Creating and Managing Administrator User Accounts and Groups

This chapter describes how to create user accounts and groups from the Cisco Wide Area Applications Services Central Manager GUI (Cisco WAAS Central Manager GUI).

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the WAAS Central Managers and WAEs (Cisco Wide Area Application Engines) in your network. The term WAE refers to WAE appliances and WAE Network Modules (the Cisco WAAS NME-WAE family of devices).

This chapter contains the following sections:

About Administrator User Accounts

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

If you want to create additional administrator user accounts, see the following list for a description of the two types of accounts you can create from the Cisoc WAAS Central Manager GUI.

- **Roles-based account**
  - Allows you to create accounts that manage and configure specific Cisco 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** windows in the Cisco WAAS Central Manager GUI.
  - 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 Cisco WAAS Central Manager GUI.

- **Local account**
  - Provides CLI access to Cisco WAE devices. A user with this account type can log in to the Cisco WAAS Central Manager but they have the access rights assigned to the default account, which initially has no access to GUI functionality.
  - We recommend that you create a local account if there is an administrator that only needs CLI access to Cisco WAE devices.
  - You should create local accounts the same way as roles-based accounts, but you should check the **Local User** check box when creating the account.

Administrator Account User Name and Strong Password Guidelines

The Cisco WAAS administrator account username is **admin** and the password is initially set to **default**.

Note For how to change the devices administrator account username and password for Cisco vWAAS, see the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series" in the Cisco Virtual Wide Area Application Services Configuration Guide.

For Cisco WAAS Version 6.4.3d and earlier: Changing the password of the administrator account is recommended but *optional* after your initial login.

For Cisco WAAS Version 6.4.3e and later: Changing the password of the administrator account to a strong password is *required* after your initial login, regardless of device mode (Application Accelerator, Appnav or Central Manager).

Consider the following operating guidelines for the **strong password** feature for Cisco WAAS Version 6.4.3e and later:

- **Strong password and Administrator account**: Strong password enforcement is applicable *only* to the Administrator account with the username **admin**. For more information on creating a strong password, see Working with Passwords, on page 9.
- **Strong password and registered Cisco vWAAS devices in upgrade from Cisco WAAS Version 6.4.1b to Cisco WAAS Version 6.4.3e or later**: to ensure that a new strong password is reflected in both the Cisco WAAS Central Manager and the Cisco vWAAS, follow these steps:
  1. Use the Cisco WAAS Central Manager GUI to upgrade the Cisco WAAS Central Manager from Cisco WAAS Version 6.4.1b to 6.4.3e or later.
  2. Change the strong password.
  3. Login with the new strong password.
  4. Choose **Home** > **Security** > **Password** and submit the new strong password.
  5. Verify that the new strong password is reflected in the Cisco vWAAS as well as the Cisco WAAS Central Manager.

6. Upgrade the Cisco vWAAS from Cisco WAAS Version 6.4.1b to 6.4.3e or later.

To update the password on the Cisco Wide Area Virtualization Engine Console:

1. In the **Username** field, enter admin or a username of your choice.
2. In the **Password** field, enter a password that contains the following parameters:
   - At least one lowercase character (a-z)
   - At least one uppercase character (A-Z)
   - At least one number (0-9)
   - At least one special character
   - A password length of 8 to 31 characters

To update the password using the CLI:

NO-HOSTNAME(config)# **username** *username* **passwd**

The following message will be displayed:

```
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New WAAS password:
Retype new WAAS password:
NO-HOSTNAME#
```

Note To ensure the new password gets reflected to all devices, after you change the password using the Cisco WAAS Central Manager CLI, you must then change the password in **Home > Admin > Security**. This new password should not be the same password used in the Cisco WAAS CLI.

Creating and Managing User Accounts

This section contains the following topics:

Workflow for Creating and Managing a User Account

The following list provides a workflow of the steps you must complete to create a new roles-based administrator account.

1. Create a new account.

   Creates an account on the system with a specific username, password, and privilege level. For more information, see Creating a New Account .

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 Creating a New Role. If you are using an external authentication server, you can define matching user groups that automatically assign roles to users.

3. Assign the role to the new account.

   Assigns the new role to the new account. For more information, see Assigning a Role to a User Account. 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 Creating a New Domain.

5. Add an entity to the domain.

   Adds one or more WAEs, device groups, or AppNav Clusters to the domain. For more information, see Adding an Entity to a Domain.

6. Assign a domain to a user account.

   Assigns the domain to the new user account. For more information, see Assigning a Domain to a User Account. 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 Cisco WAAS Central Manager.

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

Two default user accounts are preconfigured in the Cisco 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 Cisco 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, although you can use the default account to log in to the Cisco WAAS Central Manager GUI.

This section contains the following topics:

Creating a New Account

Before you begin

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, which determine the WAAS services and devices that the account can manage and configure.

The following table describes the outcome of creating a local CLI user when setting up an account.

Table 1: Outcome of Creating a Local User

Action	Result
Creating a Local User	• The account can be used to access the Cisco WAAS CLI and the Cisco WAAS Central Manager GUI (with the default role). • Users can change their own passwords, and the password change will propagate to standby Cisco WAAS Central Managers. • The account is stored in the Cisco WAAS Central Manager database and is also propagated to the standby Cisco WAAS Central Managers.
Not Creating a Local User	• The user account is created in the primary and standby Cisco 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 Cisco 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 Cisco 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 Cisco WAAS Central Manager GUI for the first time, the Centralized Management System (CMS) automatically creates a user account (with the same username as that configured in the CLI) with default authorization and access control. An account created from the CLI will initially be unable to access any configuration pages in the Cisco WAAS Central Manager GUI. You must use an admin account to give the account created from the CLI the roles it requires to perform configuration tasks from the WAAS Central Manager GUI.

Procedure

Step 1 From the Cisco 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.

Step 4 Usernames are case sensitive and cannot contain characters other than letters, numbers, period, hyphen, and underscore. Complete the following steps to create a local CLI user account:

a) Check the **Local User** check box. See the above table for information about the benefits of creating a local CLI user. A local user is created on all Cisco WAE devices.

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

b) In the **Password** field, enter a password for the local user account, and re-enter 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 Cisco WAAS Central Manager GUI user with the **admin** role can perform.

Note Use the Cisco WAAS CLI EXEC mode 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, see the Cisco Wide Area Application Services Command Reference .

Step 5 (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 6 (Optional) In the **Comments** field, enter any additional information about this account.

Step 7 Click **Submit**.

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

Step 8 Assign roles to this new account, as described in Working with Roles, on page 11 and assign domains, as described in Working with Domains, on page 15.

Modifying and Deleting a User Account

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:

Procedure

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.

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

The Modifying User Account window appears. You can delete or edit user accounts as follows:

- 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

Before you begin

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

- Your account and password were created in the Cisco 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 Cisco 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 Cisco WAAS Central Manager GUI is that both the primary and the standby Cisco WAAS Central Managers will be synchronized, and GUI users will not have to access the CLI to change their password.

Procedure

Step 1 From the Cisco 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, and 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, re-enter 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 Cisco WAAS Central Manager GUI, it changes the password for all Cisco WAE devices managed by the Cisco WAAS Central Manager.

Changing the Password for Another Account

If you log in to the Cisco 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:

Procedure

Step 1 From the Cisco 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 a User Account

To view all user accounts, choose **Admin > AAA> Users** from the Cisco 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 Creating a New Account .

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.

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

Unlocking a User Account

Before you begin

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.

Procedure

Step 1 From the Cisco 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 in which you want to unlock the account.

The list of device users appears.

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

Working with Passwords

Before you begin

The Cisco WAAS system features two levels of password policy: **Standard** and **Strong**. By default, the **Standard** password policy is enabled.

Procedure

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

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

Step 3 To enable the strong password policy, check the **Enforce stringent password** check box.

Step 4 In the **Maximum login retries** field, enter the maximum number of login attempts to be allowed before a user is locked out. The user remains locked out until cleared by the administrator. For more information, see Unlocking a User Account, on page 9.

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

Note The MAPI process terminates abruptly when you try to upgrade to version 6.4.3e and higher. This happens when the **admin** user uses the **default**password and enforces password checking using the **Enforce stringent password** checkbox. To avoid this, either change the password or disable stringent password checking while upgrading the device.

Step 6 (Optional) To configure a password policy from the CLI, run 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 to 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. However, the minimum password length can vary depending on the following conditions:
  - The minimum password length must be 10 characters if all characters are the same type of characters: all lowercase letters. all uppercase letters, all numbers, or all special characters.
  - The minimum password length must be 9 characters if you use any two different types of characters.
  - The minimum password length must be 8 characters if you use any three different types of characters.
  - The minimum password length must be 7 if you use any four different types of characters.
- The password can include both uppercase and lowercase letters (A-Z and a-z), numbers (0 to 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.

Note When you enable the strong password policy, existing standard-policy passwords will still work. However, these passwords are subject to expiration under the strong password policy.

A user account will be locked out after the configured number of failed login attempts (the default is **3**). The user remains locked out until cleared by the administrator. For more information, see Unlocking a User Account, on page 9.

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. After you create a 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 a predefined role, known as the admin role. The admin role has access to all services, similar to a CLI user having privilege level 15. Without the admin role, a user will not be able to perform all the 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.

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 assign a role to the user groups on the WAAS Central Manager. For more information on user groups, see Working with User Groups, on page 19.

This section contains the following topics:

Creating a New Role

Procedure

Step 1 From the Cisco 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 you want this role to manage.

- The check boxes in this window are tri-state check boxes. When there is a check in a check 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.
- To expand the listing of services under a category, click the **folder** icon, and then check the check box next to the services 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.
- The following table lists the services that you can enable for a role.

Table 2: Description of Cisco WAAS Services

Service	Description
Home	Allows a role to view, configure, and manage the system dashboard and settings in the **Configure**, **Monitor**, and **Admin** menus of the Cisco 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 a role to view, configure, and manage the settings and subpages for the various device groups in the Cisco WAAS Central Manager GUI in the device group context.
Devices	Allows a role to view, configure, and manage the settings and subpages for various kinds of devices in the Cisco WAAS Central Manager GUI in the device context.
AppNav Clusters	Allows a role to view, configure, and manage the settings and subpages in the Cisco WAAS Central Manager GUI in the AppNav Cluster context.
Locations	Allows a role to view, configure, and manage the settings and subpages in the Cisco WAAS Central Manager GUI in the Location context.
All Devices	Allows a role to access all the devices in your Cisco 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.

Service	Description
All Device Groups	Allows a role to access all the device groups in your Cisco WAAS network. If this service is not enabled, 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 a role to access all the AppNav clusters in your Cisco 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.
Monitoring API	Allows a role to access monitoring APIs through HTTPS requests. For more information, see Cisco Wide Area Application Services API Reference.
System Status	Allows a role to access the device Alarms panel. For more information about device alarms, see the chapter Monitoring Your Cisco WAAS Network.

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

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

Assigning a Role to a User Account

Before you begin

After you create a role, you must assign the role to an account (or a user group). If you create an account, but do not assign a role to the account, the user for that account can log in to the Cisco 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.

Procedure

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

The **User Accounts** or **User Groups** window appears with all the 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 the configured role names listed.

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

Step 5 Click the **Unassign** icon (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 the roles in the current window to a user account or group. Alternatively, click the **Remove all Roles** icon to unassign all the roles associated with a user account or group.

Step 6 Click **Submit**.

The roles assigned to a user account or group will be listed in the **Roles** section in the **Modifying User Account** or **Modifying User Group** window.

Modifying and Deleting a Role

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

To modify or delete a role, follow these steps:

Procedure

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 corresponding service. 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:

Procedure

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

Note A Cisco 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.

Cisco 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 Cisco 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 Cisco WAAS Central Manager. For more information on user groups, see Working with User Groups, on page 19.

This section contains the following topics:

Creating a New Domain

To create a new domain, follow these steps:

Procedure

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 (Devices, Device Groups, or None) that you want to assign to the domain.

Note Choose **None** if this domain is used for a file server dynamic share.

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

Step 6 Click **Submit**.

If the entity type you chose has not 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 Adding an Entity to a Domain, on page 16. 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.

For a domain used in a dynamic share configuration, assign the domain to each user having to edit the dynamic share configuration, as described in Assigning a Domain to a User Account, on page 17. Only users assigned to the domain will be able to edit the dynamic share configuration.

Adding an Entity to a Domain

After 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 have 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:

Procedure

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 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 the 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 the 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 Assigning a Domain to a User Account, on page 17.

Assigning a Domain to a User Account

Before you begin

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 having 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 Cisco WAAS domains to users. For more information, see Working with User Groups, on page 19.

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 have to assign a domain to the account or group. The account or group can automatically access all the devices or device groups, or both, in the Cisco WAAS system. For more information, see Working with Passwords, on page 9.

Procedure

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

The **User Accounts** or **User Groups** window appears with all the 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 a domain from the user account or group, click the **Unassign** (green tick mark) next to the domain name.

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

Step 5 Click **Submit**.

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 a Domain

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

Procedure

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

Procedure

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

The **User Accounts** or **User Groups** window appears, with all the 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 have to define a role or WAAS domain for each user individually; instead, you define roles and WAAS domains for the user groups, and a 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 (Access Control Server) 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

Procedure

Step 1 From the Cisco 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. 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 comments, if any, about this user group.

Step 5 Click **Submit**.

Step 6 Assign a role or Cisco WAAS domain to this user group, as described in Assigning Roles to a User Group, on page 20 and Assigning a Domain to a User Group, on page 20.

Assigning Roles to a User Group

After you create a user group, you have 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 in to 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:

Procedure

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

The User Groups window appears with all the 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 the 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 the roles in the current window to a user group. Alternatively, click the Remove all Roles icon to unassign all the roles associated with a user group.

Step 6 Click **Submit**.

The roles assigned to a user group will be listed in the Roles section in the Modifying User Group window.

Assigning a Domain 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 that 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 have to assign a domain to the user group. The users in that group can automatically access all the devices, or device groups, or both, in the WAAS system. For more information, see Table 8-4 .

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

Procedure

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

The User Groups window appears with all the 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 the 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 a domain from the user group, click the **Unassign** (green tick mark) next to the domain name.

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

Step 5 Click **Submit**.

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:

Procedure

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 the user groups, choose **Admin > AAA > User Groups** from the Cisco 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 Creating a New User Group, on page 19.