



Creating and Managing Administrator User Accounts

This chapter describes how to create user accounts 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.

This chapter contains the following topics:

- [Overview of Administrator User Accounts, page 7-1](#)
- [Creating and Managing User Accounts, page 7-2](#)

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 7-1](#) for a description of the two types of accounts you can create from the WAAS Central Manager GUI.

Table 7-1 Account Type Descriptions

Account Type	Description
Roles-based account	<p>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.</p> <p>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.</p> <p>You create roles-based accounts from the System tab in the WAAS Central Manager GUI.</p>
Local account	<p>Provides CLI access to WAE devices and optionally allows users to access the Print Services Administration GUI and 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.</p> <p>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.</p> <p>You create local accounts in the same way as roles-based accounts, but you check the Local User check box when creating the account.</p>

Creating and Managing User Accounts

This section contains the following topics:

- [Overview for Creating an Account, page 7-2](#)
- [Working with Accounts, page 7-3](#)
- [Working with Roles, page 7-8](#)

Overview for Creating an Account

[Table 7-2](#) provides an overview of the steps you must complete to create a new roles-based administrator account.

Table 7-2 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 7-3 .
2. Create a role for the new account.	Creates a role that specifies the services an account can configure in your WAAS network. For more information, see the “Creating a New Role” section on page 7-9
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 7-10 .

Working with Accounts

When you create an administrator 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 two predefined roles, known as the admin and print roles. The admin role has access to all services. The print role has access to all print related pages.

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 7-3](#)
- [Modifying and Deleting User Accounts, page 7-6](#)
- [Changing the Password for Your Own Account, page 7-7](#)
- [Changing the Password for Another Account, page 7-8](#)
- [Viewing User Accounts, page 7-8](#)

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 7-3](#) describes the results of creating a local CLI user when setting up an account.

Table 7-3 Results of Creating a Local User

Action	Result
Creating a Local User	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 System tab > 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 GUI, choose **System > 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. (See [Figure 7-1](#).)

**Note**

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

Figure 7-1 Creating New User Account Window

The screenshot displays the 'Creating New User Account' window in the Cisco Wide Area Application Services (WAAS) configuration interface. The window is titled 'Creating New User Account' and is located within the 'Users' section of the configuration menu. The interface is divided into three main sections: Account Information, User Information, and Comments. The Account Information section includes fields for Username (required), WAE Device Manager User (checkbox), Local User (checkbox), Print Admin (checkbox), Password, and Confirm Password. The User Information section includes fields for First Name, Last Name, Phone Number, Email Address, Job Title, and Department. The Comments section is a text area. A 'Note' at the bottom indicates that fields with an asterisk are required. The interface also shows a navigation menu with options like AAA, Password, Logs, Configuration, Software Files, Users, and Roles.

- Step 3** In the Username field, enter the user account name.
User names are case-sensitive and support special characters.
- Step 4** To allow the user to access the WAE Device Manager GUI, complete the following steps:
- Check the **WAE Device Manager User** check box.
 - From the Device Manager Access drop-down list, select 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** To create a local CLI user account, complete the following steps:
- Check the **Local User** check box. See [Table 7-3 on page 7-4](#) for information about the benefits of creating a local CLI user. A local user is created on all WAE devices.
 - 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.

- 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.



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 Check the **Print Admin** check box to use this account to upload drivers to the central repository on the WAAS Central Manager and to access the Print Services Administration GUI.

For more information, see the [“Setting Up the WAAS Central Manager as the Driver Repository”](#) section on page 13-15, and the [“Using the Print Services Administration GUI”](#) section on page 13-28.

Note the following about the print admin account:

- This Print Admin checkbox is enabled only after you check the **Local User** check box.
- The print admin account must have a privilege level of 15 (super user) in order to use the account to upload drivers to the repository. If the print admin account has a privilege level of 0, it can be used only to access the Print Services Administration GUI.
- The print admin account does not have access to print related pages in the WAAS Central Manager unless it also has the print or admin roles assigned.

Step 7 (Optional) In the Username fields, enter the following information about the user: First Name, Last Name, Phone Number, Email Address, Job Title, and Department.

Step 8 (Optional) In the Comments field, enter any additional information about this account.

Step 9 Click **Submit**.

Step 10 A Changes Submitted message appears at the bottom of the window.

Step 11 Assign roles to this new account as described in the [“Working with Roles”](#) section on page 7-8.

Modifying and Deleting User Accounts



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

To modify an existing user account, follow these steps:

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

The User Accounts window appears.

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

The Modifying User Account window appears.



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

- 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 user name 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 GUI, choose **System > Password**.
The Changing Password for User Account window appears.
- Step 2** In the New Password field, enter the changed password. Passwords are case-sensitive.
- 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.

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

-
- Step 1** From the WAAS Central Manager GUI, choose **System > 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.
 - 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 **System > 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 7-3](#).

Working with Roles

The WAAS Central Manager GUI allows you to create roles for your WAAS system administrators so 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.

Each user account can be assigned to zero or more roles. Roles are not inherited or embedded. The WAAS Central Manager provides two predefined roles, known as the admin and print roles. The admin role has access to all services. The print role has access to all print related pages. In addition, when this role is assigned to a user, the user automatically becomes a print admin with CLI Privilege Level 0 (normal user).

This section contains the following topics:

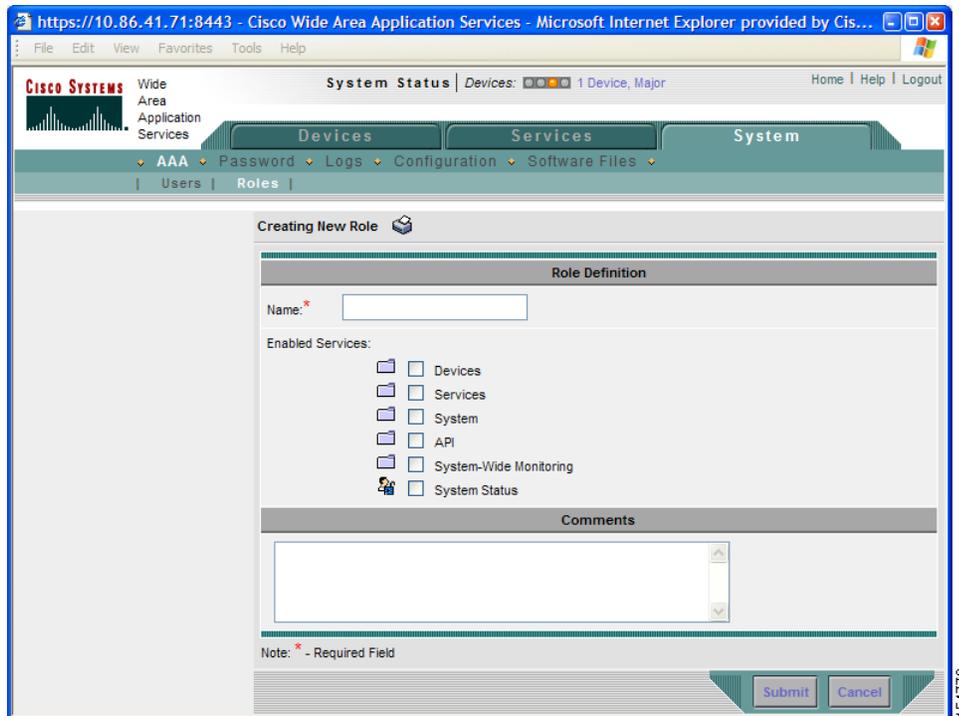
- [Creating a New Role, page 7-9](#)
- [Assigning a Role to a User Account, page 7-10](#)
- [Modifying and Deleting Roles, page 7-11](#)
- [Viewing Role Settings, page 7-11](#)

Creating a New Role

To create a new role, follow these steps:

- Step 1** From the WAAS Central Manager GUI, choose **System > AAA > Roles**.
The Roles listing window appears.
- Step 2** Click the **Create New Role** icon from the taskbar.
The Creating New Role window appears. (See [Figure 7-2](#).)

Figure 7-2 Creating New Role Window



- Step 3** In the Name field, enter the name of the role.
- Step 4** Check the check box next to the services that you want this role to manage.

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 7-4](#) lists the services that you can enable for a role.

Table 7-4 Description of the WAAS Services

Service	Description
Devices	Allows this role to configure and manage the settings on the Devices tab of the WAAS Central Manager GUI. If you do not want to enable the entire Devices tab, select the subpages that you want this role to manage.
Services	Allows this role to configure and manage the settings on the Services tab of the WAAS Central Manager GUI. If you do not want to enable the entire Services tab, select the subpages that you want this role to manage.
System	Allows this role to configure and manage the settings on the System tab of the WAAS Central Manager GUI. If you do not want to enable the entire System tab, select the subpages that you want this role to manage.
System-Wide Monitoring	Provides access to the WAAS system-wide traffic statistics report. For more information about these reports, see Chapter 15, “Monitoring and Troubleshooting Your WAAS Network.”
System Status	Displays the System Status alarm lights located at the top of the WAAS Central Manager GUI. These lights can help users troubleshoot and resolve system alarms. For more information about the System Status alarms, see Chapter 15, “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. 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, follow these steps:

-
- Step 1** From the WAAS Central Manager GUI, choose **System > AAA > Users**.
The User Accounts window appears with all configured user accounts listed.
- Step 2** Click the **Edit** icon next to the user account for which you want to assign roles.
The Modifying User Account window appears.
- Step 3** In the Contents pane, choose **Role Management**.
The Role Management for User Account 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.

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



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

- Step 6** Click **Submit**.

A green tick mark appears next to the assigned roles and a blue cross mark appears next to the unassigned roles. The roles assigned to this user account will be listed in the Roles section in the Modifying User Account window.

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 GUI, choose **System > 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.

- 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.

To view role settings, follow these steps:

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

The User Accounts window appears with all configured user accounts listed.

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

The Modifying User Account window appears.

- Step 3** In the Contents pane, choose **Role Management**.

The Role Management for User Account 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**.
