Configuring Administrative Login Authentication, Authorization, and Accounting

This chapter describes how to configure administrative login authentication, authorization, and accounting for Cisco Wide Area Application Services (WAAS) devices.

This chapter contains the following sections:

- About Administrative Login Authentication and Authorization
- Configuring Administrative Login Authentication and Authorization
- Configuring AAA Command Authorization
- Configuring Cisco Prime Network Control System Single Sign-On
- Configuring AAA Accounting for WAAS Devices
- Viewing Audit Trail Logs

Use the WAAS Central Manager GUI to centrally create and manage two different types of administrator user accounts (device-based CLI accounts and roles-based accounts) for your Cisco WAAS devices. For more information, see Chapter 8, "Creating and Managing Administrator User Accounts and Groups."

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

About Administrative Login Authentication and Authorization

In the WAAS network, administrative login authentication and authorization are used to control login requests from administrators who want to access a WAAS device for configuring, monitoring, or troubleshooting purposes.

Login authentication is the process by which WAAS devices verify whether an administrator who is attempting to log in to the device has a valid username and password. An administrator who is logging in must have a user account registered with the device. User account information serves to authorize a user for administrative login and configuration privileges. The user account information is stored in an authentication, authorization and accounting (AAA) database, and the WAAS devices must be configured to access the particular authentication server (or servers) where the AAA database is located. When a user attempts to log in to a device, the device compares the person's username, password, and privilege level to the user account information that is stored in the database.

The WAAS software provides the following AAA support for users who have external access servers, for example, RADIUS or TACACS+ servers, and for users who require a local access database with AAA features:

- Authentication (or login authentication) is the action of determining who a user is. It checks the username and password.
- Authorization (or configuration) is the action of determining what a user is allowed to do. It permits or denies privileges for authenticated users in the network. Generally, authentication precedes authorization. Both authentication and authorization are required for a user login.
- Accounting is the action of keeping track of administrative user activities for system accounting purposes. In the WAAS software, AAA accounting through TACACS+ is supported. For more information, see Configuring AAA Accounting for WAAS Devices.

Note An administrator can log in to the WAAS Central Manager device through the console port or the WAAS Central Manager GUI. An administrator can also log in to a WAAS device that is functioning as a data center or branch WAE through the console port.

When the system administrator logs in to a WAAS device before authentication and authorization have been configured, the administrator can access the WAAS device by using the predefined superuser account (the predefined username is **admin** and the predefined password is **default**). When you log in to a WAAS device using this predefined superuser account, you are granted access to all the WAAS services and entities in the WAAS system.

Note Each WAAS device must have one administrator account with the username **admin**. You cannot change the username of the predefined superuser account. The predefined superuser account must have the username **admin**.

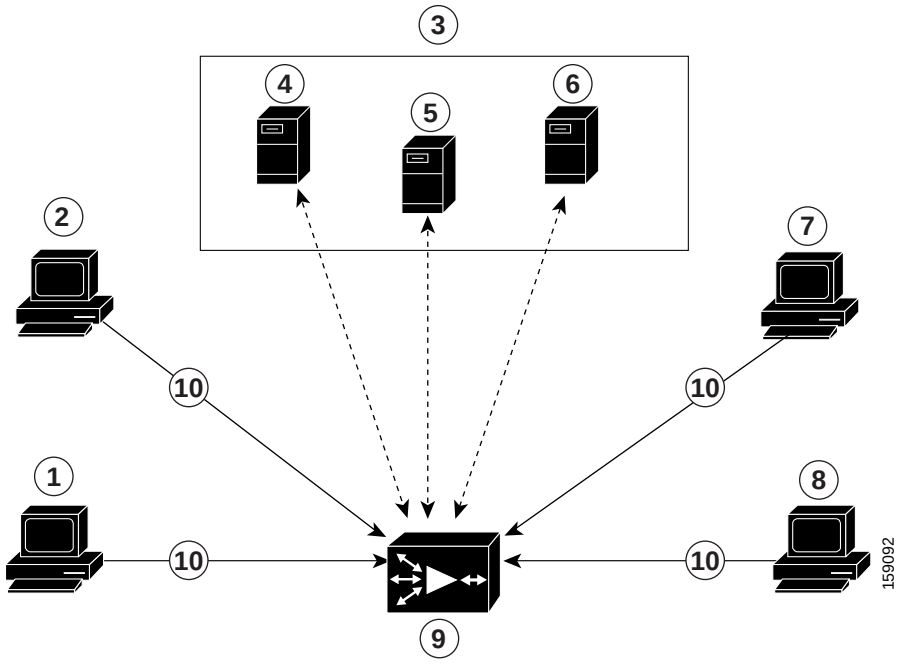
All AAA interfaces, now support IPv6 configurations.

After you have initially configured your WAAS devices, we strongly recommend that you immediately change the password for the predefined superuser account (the predefined username is **admin**, the password is **default**, and the privilege level is superuser, privilege level 15) on each WAAS device.

For instructions on using the WAAS Central Manager GUI to change the password for a predefined superuser account, see Changing the Password for Your Own Account in Chapter 8, “Creating and Managing Administrative Groups.”

Figure 7-1 shows how an administrator can log in to a WAE through the console port or the WAAS Central Manager GUIs. When the WAAS device receives an administrative login request, the WAE can check its local database or a remote third-party database (TACACS+, RADIUS, or Windows domain database) to verify the username with the password and to determine the access privileges of the administrator.

Figure 7-1 Authentication Databases and a WAE



1	FTP/SFTP client	**6**	Windows domain server
2	WAAS Central Manager GUI	**7**	Console or Telnet clients
3	Third-party AAA servers	**8**	SSH client
4	RADIUS server	**9**	WAE that contains a local database and the default primary authentication database
5	TACACS+ server	**10**	Administrative login requests

The user account information is stored in an AAA database, and the WAAS devices must be configured to access the particular authentication server (or servers) that contains the AAA database. You can configure any combination of these authentication and authorization methods to control administrative login access to a WAAS device:

- Local authentication and authorization
- RADIUS
- TACACS+
- Windows domain authentication

Note Even if you configure authentication using an external authentication server, you must create a role-based user or user group account in the WAAS Central Manager, as described in Chapter 8, "Creating and Managing Administrator User Accounts and Groups."

For more information on the default AAA configuration, see Default Administrative Login Authentication and Authorization Configuration. For more information on configuring AAA, see Configuring Administrative Login Authentication and Authorization.

Default Administrative Login Authentication and Authorization Configuration

By default, a WAAS device uses the local database to obtain login authentication and authorization privileges for administrative users.

Table 7-1 lists the default configuration for administrative login authentication and authorization.

Table 7-1 Default Configuration for Administrative Login Authentication and Authorization

Feature	Default Value
Administrative login authentication	Enabled
Administrative configuration authorization	Enabled
Authentication server failover because the authentication server is unreachable	Disabled
TACACS+ port	Port 49
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ login authorization (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ server timeout	5 seconds
TACACS+ retransmit attempts	2 times
RADIUS login authentication (console and Telnet)	Disabled
RADIUS login authorization (console and Telnet)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP authorization port	Port 1645
RADIUS key	None specified
RADIUS server timeout	5 seconds
RADIUS retransmit attempts	2 times
Windows domain login authentication	Disabled
Windows domain login authorization	Disabled
Windows domain password server	None specified
Windows domain realm (Kerberos realm used for authentication when Kerberos authentication is used). **Note** When Kerberos authentication is enabled, the default realm is DOMAIN.COM and security is the Active Directory Service (ADS).	Null string
Hostname or IP address of the Windows Internet Naming Service (WIN) server for Windows domain	None specified
Window domain administrative group	There are no predefined administrative groups.
Windows domain NETBIOS name	None specified
Kerberos authentication	Disabled

Table 7-1 Default Configuration for Administrative Login Authentication and Authorization (continued)

Feature	Default Value
Kerberos server hostname or IP address (host that is running the Key Distribution Center (KDC) for the given Kerberos realm	None specified
Kerberos server port number (port number on the KDC server)	Port 88
Kerberos local realm (default realm for WAAS)	kerberos-realm: null string
Kerberos realm (maps a hostname or DNS domain name to a Kerberos realm)	Null string

Note If you configure a RADIUS or TACACS+ key on a WAAS device (the RADIUS and or TACACS+ client), make sure that you configure an identical key on the external RADIUS or TACACS+ server.

Change these defaults through the WAAS Central Manager GUI, as described in Configuring Administrative Login Authentication and Authorization.

Multiple Windows domain utilities are included in the WAAS software to assist with Windows domain authentication configuration. You can access these utilities through the WAAS CLI by using the **windows-domain diagnostics** EXEC command.

Configuring Administrative Login Authentication and Authorization

To centrally configure administrative login authentication and authorization for a WAAS device or a device group (a group of WAEs), follow these steps:

Step 1 Determine the login authentication scheme that you want to configure for the WAAS device to use when authenticating administrative login requests, for example, use the local database as the primary login database and your RADIUS server as the secondary authentication database.

Step 2 Configure the login access control settings for the WAAS device, as described in Configuring Login Access Control Settings for WAAS Devices.

Step 3 Configure the administrative login authentication server settings on the WAAS device (if a remote authentication database is to be used). For example, specify the IP address(IPv4/IPv6) of the remote RADIUS servers, TACACS+ servers, or Windows domain server that the WAAS device should use to authenticate administrative login requests, as described in the following sections:

- Configuring RADIUS Server Authentication Settings
- About TACACS+ Server Authentication Settings
- Configuring Windows Domain Server Authentication Settings

Step 4 Specify one or all of the following login authentication configuration schemes that the WAAS device should use to process administrative login requests:

- Specify the administrative login authentication scheme.
- Specify the administrative login authorization scheme.

- (Optional) Specify the failover scheme for the administrative login authentication server.

For example, specify which authentication database the WAAS device should check to process an administrative login request. For more information, see Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices.

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

You can enable or disable the local and the remote databases (TACACS+, RADIUS, and Windows domain) through the WAAS Central Manager GUI or the WAAS CLI. The WAAS device verifies whether all the databases are disabled, and, if so, sets the system to the default state (see Table 7-1). If you have configured the WAAS device to use one or more of the external third-party databases (TACACS+, RADIUS, or Windows domain authentication) for administrative authentication and authorization, make sure that you have also enabled the local authentication and authorization method on the WAAS device, and that the local method is specified as the last option. Otherwise, the WAAS device will not go to the local authentication and authorization method by default if the specified external third-party databases are not reachable.

By default, local login authentication is enabled first. Local authentication and authorization uses locally configured login names and passwords to authenticate administrative login attempts. The login names and passwords are local to each WAAS device and are not mapped to individual usernames. When local authentication is disabled, if you disable all the other authentication methods, local authentication is re-enabled automatically.

You can disable local login authentication only after enabling one or more of the other administrative login authentication methods. However, when local login authentication is disabled, if you disable all other administrative login authentication methods, local login authentication is re-enabled automatically. You cannot specify different administrative login authentication methods for console and Telnet connections.

We strongly recommend that you set the administrative login authentication and authorization methods in the same order. For example, configure the WAAS device to use RADIUS as the primary login method, TACACS+ as the secondary login method, Windows as the tertiary method, and the local method as the quaternary method for both administrative login authentication and authorization.

Note A TACACS+ server will not authorize a user who is authenticated by a different method. For example, if you configure Windows as the primary authentication method, but use TACACS+ as the primary authorization method, TACACS+ authorization will fail.

We strongly recommend that you specify the local method as the last method in your prioritized list of login authentication and authorization methods. By adhering to this practice, if the specified external third-party servers (TACACS+, RADIUS, or Windows domain servers) are not reachable, a WAAS administrator can still log in to a WAAS device through the local authentication and authorization method.

This section describes how to centrally configure administrative login authentication, and contains the following topics:

- Configuring Login Access Control Settings for WAAS Devices
- Configuring Remote Authentication Server Settings for WAAS Devices
- Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices

Configuring Login Access Control Settings for WAAS Devices

This section describes how to centrally configure remote login and access control settings for a WAAS device or device group, and contains the following topics:

- Configuring Secure Shell Settings for WAAS Devices
- Disabling and Re-enabling the Telnet Service for WAAS Devices
- Configuring Message-of-the-Day Settings for WAAS Devices
- Configuring EXEC Timeout Settings for WAAS Devices
- Configuring Line Console Carrier Detection for WAAS Devices

Configuring Secure Shell Settings for WAAS Devices

This section contains the following topics:

- About SSH
- Operating Guidelines for SSH and WAAS Versions
- Procedure for Configuring SSH for WAAS Devices

About SSH

Secure Shell (SSH) consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

The SSH management window in the WAAS Central Manager GUI allows you to specify the key length, login grace time, and maximum number of password guesses allowed when logging in to a specific WAAS device or device group for configuration, monitoring, or troubleshooting purposes.

Operating Guidelines for SSH and WAAS Versions

Note these operational guidelines when enabling or disabling SSH for different WAAS versions:

Table 7-2 SSH Default Status and WAAS Versions

WAAS Version	SSH Default Value
6.2.3x and later	• SSH is enabled by default. To disable SSH, check the **Disable** check box on the SSH screen (displayed on the SSH Configuration window for WAAS versions 6.2.3x and later). • If you click **Reset** to remove features that you have enabled, after reset, the SSH feature will remain enabled by default. • If you downgrade to a version earlier than 6.2.3x, the SSH default status will remain as enabled.
6.2.1x and earlier	• SSH is disabled by default. To enable SSH, check the **Enable** check box in the SSH screen (displayed on the SSH screen for WAAS versions earlier than 6.2.3x and shown in Figure 7-2). • If you click **Reset** to remove features that you have enabled, after reset, the SSH feature will remain disabled by default. • If you upgrade to version 6.2.3x or later, the SSH default status will remain as disabled.

Procedure for Configuring SSH for WAAS Devices

To centrally enable the SSH feature on a WAAS device or a device group, follow these steps:

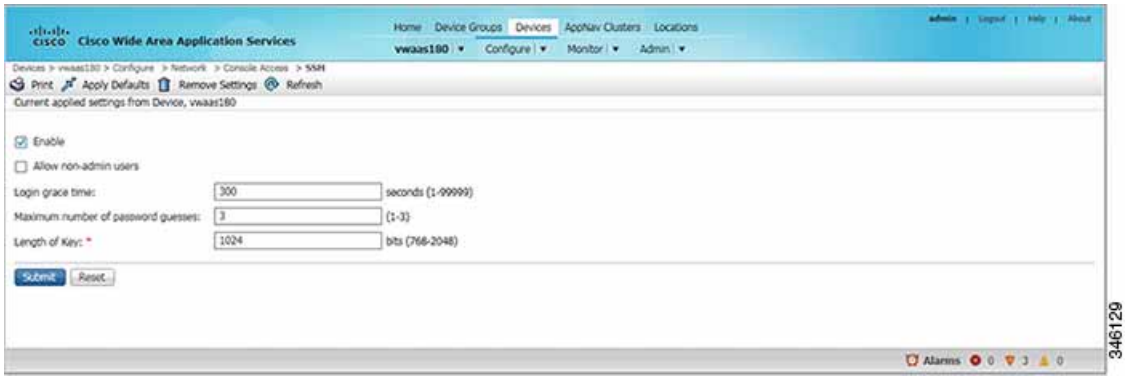
Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Network** > **Console Access** > **SSH**.

The SSH Configuration window appears. (See Figure 7-2.)

Note The SSH Version 1 protocol is no longer supported. Only the SSH Version 2 protocol is supported by the WAAS device.

Figure 7-2 SSH Configuration Window



Step 3 SSH enables login access to the chosen WAAS device (or the device group) through a secure and encrypted channel. The SSH default status is determined by your WAAS version (see Table 7-2 for descriptions of these). Depending on your WAAS version, an **Enable** or **Disable** check box is displayed in the SSH Configuration window for you to change the default status, if needed.

You can also use the CLI to enable or disable SSH, using the **sshd enable** global configuration command, or the **no sshd enable** command.

Step 4 Check the **Allow non-admin users** check box to allow nonadministrative users to gain SSH access to the chosen device (or device group). By default, this option is disabled.

Note Nonadministrative users are nonsuperuser administrators. All nonsuperuser administrators have only restricted access to a WAAS device because their login accounts have a privilege level of 0. Superuser administrators have full access to a WAAS device because their login accounts have the highest level of privileges, a privilege level of 15.

Step 5 In the Login grace time field, specify the number of seconds for which an SSH session will be active during the negotiation (authentication) phase between the client and the server before it times out. The default is 300 seconds.

Step 6 In the Maximum number of password guesses field, specify the maximum number of incorrect password guesses allowed per connection. The default is 3.

Although the value in the Maximum number of password guesses field specifies the number of password guesses allowed from the SSH server side, the actual number of password guesses for an SSH login session is determined by the combined number of allowed password guesses of the SSH server and the SSH client. Some SSH clients limit the maximum number of allowed password guesses to three (or to one in some cases), even though the SSH server allows more than this number of guesses. When you specify *n* password guesses allowed, certain SSH clients interpret this number as *n* + 1. For example, when configuring the number of guesses to two for a particular device, SSH sessions from some SSH clients will allow three password guesses.

Step 7 In the Length of key field, specify the number of bits required to create an SSH key. The default is 1024.

When you enable SSH, be sure to generate both a private and a public host key, which client programs can use to verify the server's identity. When you use an SSH client and log in to a WAAS device, the public key for the SSH daemon running on the device is recorded in the client machine known_hosts file in your home directory. If the WAAS administrator subsequently regenerates the host key by specifying the number of bits in the Length of key field, you must delete the old public key entry associated with the WAAS device in the known_hosts file before running the SSH client program to log in to the WAAS device. When you use the SSH client program after deleting the old entry, the known_hosts file is updated with the new SSH public key for the WAAS device.

Step 8 Click **Submit** to save the settings.

A **`Click Submit to Save`** message appears in red in the Current Settings line when there are pending changes to be saved after you have applied the default or device group settings. You can also revert to the previously configured settings by clicking **Reset** button, which is visible only if you have applied default or group settings to change the current device settings, but have not yet submitted the changes.

If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

To configure SSH settings from the CLI, you can use the **sshd** and **ssh-key-generate** global configuration commands.

Disabling and Re-enabling the Telnet Service for WAAS Devices

By default, the Telnet service is enabled on a WAAS device. You must use a console connection instead of a Telnet session to define device network settings on a WAAS device. However, after you have used a console connection to define the device network settings, you can use a Telnet session to perform subsequent configuration tasks.

You must enable the Telnet service before you can use the Telnet button in the Device Dashboard window to use Telnet to connect to a device.

Note Telnet is not supported in Internet Explorer. If you want to use the Telnet button from the Device Dashboard, use a different web browser.

To centrally disable the Telnet service on a WAAS device or a device group, 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** > **Network** > **Console Access** > **Telnet**.

The Telnet Settings window appears.

Step 3 Uncheck the **Telnet Enable** check box to disable the terminal emulation protocol for remote terminal connection for the chosen device (or device group).

Step 4 Click **Submit** to save the settings.

A **`Click Submit to Save`** message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking **Reset**, which is visible only if you have applied default or group settings to change the current device settings, but have not yet submitted the changes.

If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

To centrally re-enable the Telnet service on the device (or device group) at a later time, check the **Telnet Enable** check box in the Telnet Settings window, and click **Submit**.

From the CLI, use the **no telnet enable** global configuration command to disable Telnet, or the **telnet enable** global configuration command to enable it.

Configuring Message-of-the-Day Settings for WAAS Devices

The Message of the Day (MOTD) feature enables you to provide information bits to the users when they log in to a device that is a part of your WAAS network. There are three types of messages that you can set up:

- MOTD banner
- EXEC process creation banner
- Login banner

To configure the MOTD settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure > Network > Console Access > Message of the day**.

The MOTD Configuration window for the chosen device appears.

Step 3 To enable the MOTD settings, check the **Enable** check box.
The Message of the Day (MOTD) banner, EXEC process creation banner, and Login banner fields become enabled.

Step 4 In the Message of the Day (MOTD) Banner field, enter a string that you want displayed as the MOTD banner after a user logs in to the device.

In the Message of the Day (MOTD) Banner, EXEC Process Creation Banner, and Login Banner fields, you can enter a maximum of 1024 characters. A new line character (or Enter) is counted as two characters, as it is interpreted as \n by the system. You cannot use special characters such as `, % ,^ , and " in the MOTD text. If your text contains any of these special characters, WAAS software removes it from the MOTD output.

Step 5 In the EXEC Process Creation Banner field, enter a string to be displayed as the EXEC process creation banner when a user enters into the EXEC shell of the device.

Step 6 In the Login Banner field, enter a string to be displayed after the MOTD banner, when a user attempts to log in to the device.

Step 7 To save the configuration, click **Submit**.

Configuring EXEC Timeout Settings for WAAS Devices

To centrally configure the length of time for which an inactive Telnet session remains open on a WAAS device or device group, follow these steps:

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

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to configure the EXEC timeout.

Step 3 Choose **Configure > Network > Console Access > Exec Timeout**.

Step 4 In the Exec Timeout field, specify the number of minutes after which an active session times out. The default is 15 minutes.

A Telnet session with a WAAS device can remain open and inactive for the period specified in this field. When the EXEC timeout period elapses, the WAAS device automatically closes the Telnet session.

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

A **`Click Submit to Save`** message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking **Reset**, which is visible only if you have applied default or group settings to change the current device settings, but have not yet submitted the changes.

If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

To configure the Telnet session timeout from the CLI, use the **exec-timeout** global configuration command.

Configuring Line Console Carrier Detection for WAAS Devices

You should enable carrier detection if you plan to connect the WAAS device to a modem for receiving calls.

Note By default, this feature is disabled on a WAAS device.

To centrally enable Console Line Carrier Detection for a WAAS device or device group, 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** > **Network** > **Console Access** > **Console Carrier Detect**.

The Console Carrier Detect Settings window appears.

Step 3 Check the **Enable console line carrier detection before writing to the console** check box to enable the window for configuration.

Step 4 Click **Submit** to save the settings.

A message appears that explains that if a null-modem cable that does not have a carrier detect pin wired is being used, the WAE may appear unresponsive on the console until the carrier detect signal is asserted. To recover from a misconfiguration, the WAE should be rebooted and the 0x2000 bootflag should be set to ignore the carrier detect setting.

Step 5 Click **OK** to continue.

To configure console line carrier detection from the CLI, you can use the **line console carrier-detect** global configuration command.

Configuring Remote Authentication Server Settings for WAAS Devices

If you have determined that your login authentication scheme should include one or more external authentication servers, you must configure these server settings before you can configure the authentication scheme in the WAAS Central Manager GUI. The section contains the following topics:

- Configuring RADIUS Server Authentication Settings
- About TACACS+ Server Authentication Settings
- Configuring TACACS+ Server Settings
- Configuring Windows Domain Server Authentication Settings
- LDAP Server Signing

Configuring RADIUS Server Authentication Settings

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

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

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

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

RADIUS authentication usually occurs when an administrator first logs in to the WAAS device to configure the device for monitoring, configuration, or troubleshooting purposes. RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can also specify which method to use first.

You can configure multiple RADIUS servers; authentication is attempted on the servers in order. If the first server is unreachable, then authentication is attempted on the other servers in the farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm.

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

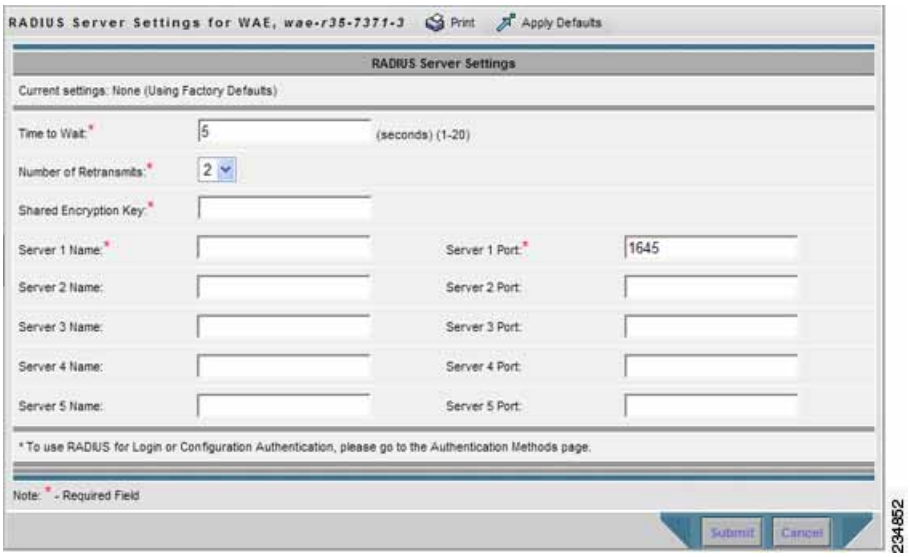
To centrally configure RADIUS server settings for a WAAS device or device group, follow these steps:

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

Step 2 Choose **Configure** > **Security** > **AAA** > **RADIUS**.

The RADIUS Server Settings window appears. (See Figure 7-3.)

Figure 7-3 RADIUS Server Settings Window



Step 3 In the Time to Wait field, specify how long the device or device group should wait for a response from the RADIUS server before timing out. The range is from 1 to 20 seconds. The default value is 5 seconds.

Step 4 In the Number of Retransmits field, specify the number of attempts allowed to connect to a RADIUS server. The default value is 2 times.

Step 5 In the Shared Encryption Key field, enter the secret key that is used to communicate with the RADIUS server.

Note If you configure a RADIUS key on the WAAS device (the RADIUS client), make sure that you configure an identical key on the external RADIUS server. Do not use the following characters: space, backwards single quote (`), double quote ("), pipe (|), or question mark (?).

Step 6 In the Server Name field, enter an IP address (IPv4/IPv6) or hostname of the RADIUS server. Five different hosts are allowed.

Step 7 In the Server Port field, enter a UDP port number on which the RADIUS server is listening. You must specify at least one port. Five different ports are allowed.

Step 8 Click **Submit** to save the settings.

You can now enable RADIUS as an administrative login authentication and authorization method for this WAAS device or device group, as described in Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices.

To configure RADIUS settings from the CLI, you can use the **radius-server** global configuration command.

About TACACS+ Server Authentication Settings

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

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication. TACACS+ authentication usually occurs when an administrator first logs in to the WAAS device to configure the WAE for monitoring, configuring, or troubleshooting.

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

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

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

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

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

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time.

You can configure one primary and two backup TACACS+ servers; authentication is attempted on the primary server first. If the primary server is unreachable, authentication is attempted on the other servers in the farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm.

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

If you are using TACACS+ for user authentication, you can create WAAS user group names that match the user groups that you have defined on the TACACS+ server. WAAS can then dynamically assign roles and domains to users based on their membership in the groups defined on the TACACS+ server. (See Working with Accounts in Chapter 8, “Creating and Managing Administrative Groups.”) You must specify associated group names for each user in the TACACS+ configuration file, as follows:

```
user = tacusr1 {
 default service = permit
 service = exec
 {
   waas_rbac_groups = admin,groupname1,groupname2
   priv-lvl = 15
```

```
 }
 global = cleartext "tac"
}
```

For each user, list the groups they belong to in the waas_rbac_groups attribute, separating each group from the next with a comma.

The dynamic assignment of roles and 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.

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

Configuring TACACS+ Server Settings

The WAAS software CLI EXEC mode allows you to set, view, and test system operations. The mode is divided into two access levels: user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access-level prompt and specify the admin password when prompted for a password.

In TACACS+, the enable password feature allows an administrator to define a different enable password per administrative-level user. If an administrative-level user logs in to the WAAS device with a normal-level user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), that user must enter the admin password to access privileged EXEC mode.

```
WAE> enable
Password:
```

Note This caveat applies even if the WAAS users are using TACACS+ for login authentication.

To centrally configure TACACS+ server settings on a WAAS device or device group, 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** > **TACACS+**.

The TACACS+ Server Settings window appears.

Note The TACACS+ server configuration cannot be modified or deleted when AAA Command Authorization is enabled.

Step 3 Check the **Use ASCII Password Authentication** check box to use the ASCII password type for authentication.

The default password type is PAP (Password Authentication Protocol). However, you can change the password type to ASCII when the authentication packets are to be sent in ASCII cleartext format.

Step 4 In the Time to Wait field, specify how long the device should wait before timing out. The range is from 1 to 20 seconds. The default value is 5 seconds.

Step 5 In the Number of Retransmits field, specify the number of attempts allowed to connect to a TACACS+ server. The range is 1 to 3 times. The default value is 2 times.

Step 6 In the Security Word field enter the secret key that is used to communicate with the TACACS+ server. The secret key value can contain a maximum of 32 alphanumeric characters. The following characters are not allowed: space, backwards single quote (`), double quote ("), pipe (|), number sign (#), question mark (?), or backslash (\).

Note
- The Security Word field is a mandatory field.
- When you configure a TACACS+ key on the WAAS device (the TACACS+ client), you must also configure an identical key on the external TACACS+ server.

Step 7 In the Primary Server field, enter an IP address (IPv4/IPv6) or hostname for the primary TACACS+ server.

To change the default port (49), enter the port in the Primary Server Port field.

Step 8 In the Secondary Server field, enter an IP address (IPv4/IPv6) or hostname for a secondary TACACS+ server.

To change the default port (49), enter the port in the Secondary Server Port field.

Step 9 In the Tertiary Server field, enter an IP address (IPv4/IPv6) or hostname for a tertiary TACACS+ server.

To change the default port (49), enter the port in the Tertiary Server Port field.

Note You can specify up to two backup TACACS+ servers.

Step 10 Click **Submit** to save the settings.

You can now enable TACACS+ as an administrative login authentication and authorization method for this WAAS device or device group, as described in Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices.

To configure TACACS+ settings from the CLI, use the **tacacs** global configuration command.

Configuring Windows Domain Server Authentication Settings

A Windows domain controller can be configured to control access to the WAAS software services using either a challenge/response or shared secret authentication method. The system administrator can log in to the WAAS device by using an FTP, SSH, or Telnet session, the console, or the WAAS Central Manager GUI with a single user account (username/password/privilege). RADIUS and TACACS+ authentication schemes can be configured simultaneously with Windows domain authentication. Logging of a variety of authentication login statistics can be configured when Windows domain authentication is enabled. The log files and the statistical counters and related information can be cleared at any time.

In a WAAS network, Windows domain authentication is used in the following scenarios:

- Logging in to the WAAS Central Manager GUI
- CLI configuration on any WAAS device

You can configure Windows authentication for the WAAS Central Manager device, a single WAAS device, or a group of devices. To configure Windows domain authentication on a WAAS device, configure a set of Windows domain authentication settings.

Note Windows domain authentication is not performed unless a Windows domain server is configured on the WAAS device. If the device is not successfully registered, authentication and authorization do not occur. WAAS supports authentication by a Windows domain controller running only on Windows Server 2000, Windows Server 2003, or Windows Server 2008.

This section contains the following topics:

- Configuring Windows Domain Server Settings on a WAAS Device
- Unregistering a WAE from a Windows Domain Controller

Configuring Windows Domain Server Settings on a WAAS Device

You should know the name and IP address, or hostname, of the Windows domain controller that will be used for authentication.

Note If the Central Manager is Version 4.2.3a or later, and you want to configure the Windows domain settings on a WAAS device that is running Version 4.2.3 or 4.2.1, you cannot use the Windows Domain Server Settings page on the Central Manager. You must use the **windows-domain diagnostics net** CLI command, as described in this procedure.

To configure Windows Domain server settings on a WAAS device or device group, 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** > **Windows User Authentication**.

The Windows User Authentication window appears. (See Figure 7-4.)

Note Workgroup settings are only required for Windows domain authentication, not for a domain join. You can skip to workgroup settings if you are only performing a domain join.

Figure 7-4 Windows User Authentication

Step 3 In the Windows group for authorizing normal users field, specify an administrative group for normal users (nonsuperuser administrators), who only have restricted access to the chosen device (or device group) because their administrator user account has a privilege level of 0.

Note By default, there are no predefined user groups for Windows domain authorization configured on a WAE.

Step 4 In the Windows group for authorizing super users field, specify an administrative group for superusers (superuser administrators), who have unrestricted access to the chosen device (or device group) because their administrator user account has a privilege level of 15.

Note In addition to configuring Windows domain administrative group on a WAE, you must configure the Windows domain administrative group on your Microsoft Windows 2000, 2003, or 2008 server. You must create a Windows Domain administrative superuser group and a normal user group. Make sure that the group scope for the superuser group is set to global, assign user member to newly created administrative group, and add the user account, for example, the winsuper user, to the Windows domain superuser group. For more information about how to configure the Windows domain administrative group on your Windows server, see the corresponding Microsoft documentation.

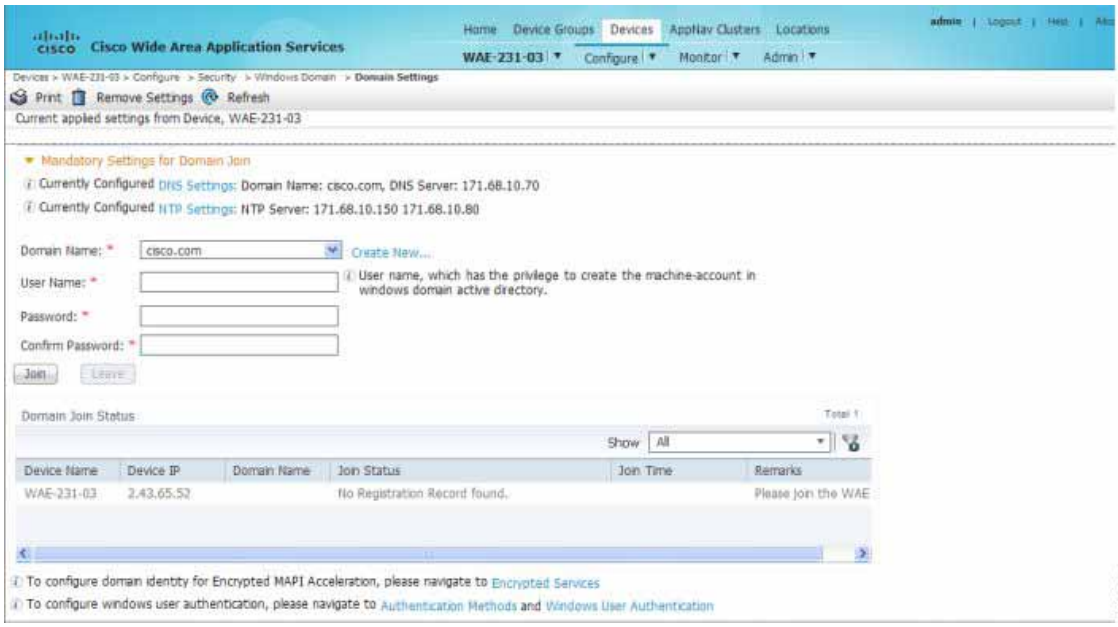
When a user attempts to access this WAE through a Telnet session, FTP, or SSH session, the WAE is configured to use the Active Directory user database to authenticate a request for administrative access.

Step 5 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 6 Choose **Configure > Security > Windows Domain > Domain Settings**.

The Domain Settings window appears. (See Figure 7-5.)

Figure 7-5 Domain Settings



Note In WAAS versions earlier than 5.1.1, if the related WINS server and the workgroup or domain name have not been defined for the chosen device (or device group), an informational message is displayed at the top of this window to inform you that these related settings are currently not defined, as shown in Figure 7-5. To define these settings, choose **Configure** > **Network** > **WINS**.

Domain name, DNS server, and NTP configuration are mandatory prerequisites for the Windows domain join. The Windows domain controller and the WAAS device must be in time sync for Kerberos authentication to succeed. For full AAA functionality, workgroup and WINS server must also be configured.

In WAAS versions earlier than 5.1.1, NetBIOS name does not have to be configured for Windows domain join. If left unconfigured, the first 15 characters of the hostname are automatically assigned as the NetBIOS name during the join. For WAAS versions later than 5.1.1, NetBIOS name, WINS server, and workgroup configuration settings are not required for Windows domain authentication configuration.

Step 7 From the Domain Name drop-down list, choose a name or click **Create New** to create a new Local Domain Name.

Step 8 If your WAAS device (or device group) is a previous version of the software.

a. Choose **Kerberos, NTLM**1 plus ESS (Extended Session Security), or **NTLM2** as a shared secure authentication method for administrative logins to the chosen device (or device group). The default authentication protocol is kerberos.

Note In WAAS version 5.0.1 onwards, Windows domain user login authentication using NTLM protocol is deprecated. We recommend that you use Kerberos protocol for Windows domain user login authentication.

In WAAS Version 5.1.1 onwards, Windows domain user authentication using NTLM protocol is not supported.

You can use the Kerberos protocol, NTLMv1 plus ESS (Extended Session Security), or NTLMv2 for encrypted MAPI acceleration.

Click **Auto Detect The Parameters** when using Kerberos to automatically obtain the kerberos realm, kerberos server, and domain controller. Domain, DNS, and NTP parameters must be configured first. This option is not supported with NTLM.

After the device is queried for the parameters, a status message is displayed on the screen indicating either success or failure. The process may not be immediate and the status message will not appear until the auto detection process is completed.

When successful, the parameters can be reviewed and edited, if required. After the parameters are reviewed, the values can be submitted.

If auto detection fails, check the configured domain/DNS configuration and enter them manually. The values can then be submitted.

Note Kerberos Version 5 is used for Windows systems running Windows 2000 or later, with users logging in to domain accounts.

For Windows domain join using Kerberos authentication, you must have the following ports open on the firewall for outgoing traffic: 53 UDP/TCP, 88 UDP/TCP, 123 UDP, 135 TCP, 137 UDP, 139 TCP, 389 UDP/TCP, 445 TCP, 464 UDP/TCP, and 3268 TCP.

b. (Skip this step for Kerberos) For NTLM, choose **version 1** or **version 2** from the drop-down list. NTLM Version 1 is selected by default.

Note For WAAS v5.3.1, NTLM is also supported for encrypted MAPI (EMAPI). Note the following about NTLM for EMAPI:

NTLM for EMAPI does not require any additional configuration other than what is required for Kerberos. However, the client must be joined to the domain.

NTLM with EMAPI uses a key for each NTLM user. These keys are stored in memory and removed after a reload. If, for example, a core WAE is rebooted during the night, all NTLM keys need to be gathered again at startup, which may cause an increase in latency in establishing the client-server connection.

- NTLM Version 1 is used for all Windows systems, including legacy systems such as Windows 98 with Active Directory, Windows NT, and more recent Windows systems, such as Windows 2000, Windows XP, and Windows 2003. We recommend the use of Kerberos if you are using a Windows 2000 SP4 or Windows 2003 domain controller.
- NTLM Version 2 is used for Windows systems running Windows 98 with Active Directory, Windows NT 4.0 (Service Pack 4 or later), Windows XP, Windows 2000, and Windows 2003. Enabling NTLM Version 2 support on the WAAS print server will not allow access to clients who use NTLM or LM.

Caution Enable NTLM Version 2 support in the print server only if all the clients' security policy has been set to Send NTLMv2 responses only/Refuse LM and NTLM.

c. (Skip this step for NTLM) In the Kerberos Realm field, enter the fully qualified name of the realm in which the WAAS device resides. In the Key Distribution center, enter the fully qualified name or the IP address of the distribution center for the Kerberos key. If you clicked **Auto Detect The Parameters** when you selected the Kerberos authentication method, these fields will already be populated.

All Windows 2000 domains are also Kerberos realms. Because the Windows 2000 domain name is also a DNS domain name, the Kerberos realm name for the Windows 2000 domain name is always in uppercase letters. This capitalization follows the recommendation for using DNS names as realm names in the Kerberos Version 5 protocol document (RFC-4120) and affects only interoperability with other Kerberos-based environments.

d. In the Domain Controller field, enter the name of the Windows Domain Controller.

When you click **Submit**, the Central Manager validates this name by requesting the WAAS device (if Version 4.2.x or later) to resolve the domain controller name. If the domain controller is not resolvable, you are asked to submit a valid name. If the device is offline, you are asked to verify

device connectivity. If you are configuring a device group, the domain controller name is not validated on each device before this page is accepted and if it is not resolvable on a device, the configuration changes on this page are not applied to that device.

e. Click **Submit**.

Note Make sure that you click **Submit** now so that the specified changes are committed to the WAAS Central Manager database. The Domain Administrator's username and password, which you will enter in Step 9, are not stored in the WAAS Central Manager's database.

Step 9 Register the chosen device (or device group) with the Windows Domain Controller as follows:

a. In the User Name field, enter a username (the domain\username or the domain name plus the username) for the specified Windows Domain Controller. This must be the username and password of a user who has administrative privileges in Active Directory (permission to add a computer to a domain).

If your WAAS device (or device group) is running a previous version of the software, click the **Domain Join** tab.

For NTLM, the user credentials can be that of any normal user belonging to the Domain Users group. For Kerberos, it is preferable that the user credentials belong to the Domain Administrators group, but need not be the system default Administrator user.

By default, a Windows Domain Administrator user is part of following groups - Administrators, Domain Administrators, Domain Users, Enterprise Administrators, Group policy creator owners and Schema Administrators.

However, only Administrators and Domain/Enterprise Administrators have the privileges to join a device to the Windows Active Directory.

If users do not want to use the administrative privileges, they can be a part of the default group called Account Operators, which has the privilege to join the device to a Windows Active Directory (AD). However, since the Account Operators group has wide access to the AD, we recommend to use AD Delegation to grant permissions using ACLs as described below.

1) Go to Active Directory Users and Computers and select **Computers>Action>Delegate Control** to open the **Delegate Control Wizard**. Select **Users and Groups>Create custom task to Delegate.**

2) Verify that the user/group is added to the AD. Click **Computers> Properties> Security** and view if the user/group is added.

3) Select **Advanced** and add ACL for **Create** and **Delete Computer Objects** by selecting the check-boxes.

To join the Windows domain successfully, the Windows domain user should either be a part of the **Account Operators** group or should have been granted permission to join the domain through AD delegation

Note To use Windows domain server authentication, the WAAS device must join the Windows domain. For registration, you will require a user credential with permission to join a machine to the Windows domain. The user credential used for registration is not shown in clear text anywhere, including log files. WAAS does not modify the structure or schema of the Windows Active Directory.

Note A domain join is required for encrypted MAPI acceleration using a machine account.

b. In the Password field, enter the password of the specified Windows Domain Controller account.

c. In the Confirm password field, re-enter the password of the specified Windows Domain Controller.

d. (Optional, if your WAAS device [or device group] is running a previous version of the software) If necessary, enter the name of the organizational unit in the Organizational Unit field (for Kerberos authentication only).

e. Click **Join**.

Note When you click **Join**, WAAS Central Manager immediately sends a registration request to the WAAS device (or all of the devices in the device group) using SSH (the specified domain administrator password is encrypted by SSH). The registration request instructs the device to perform domain registration with the specified Windows Domain Controller using the specified domain username and password. If the device is accessible (if it is behind a NAT and has an external IP address), the registration request is performed by the device (or device group).

The status of the registration request is shown in the Domain Join Status table.

f. If your WAAS device (or device group) is running a version of the software that is earlier than latest version of WAAS, click the **Show Join Status** button to view the status of the registration request.

It may take a few moments for the results to be updated. If the join request fails, the result is shown in the Domain Join Status table.

g. Wait for a few more minutes and try again to see the updated authentication status.

If the request succeeds, the domain registration status is shown in the Domain Join Status table.

After configuring the Windows domain settings, to complete the process of enabling Windows authentication, you must set Windows as the authentication and authorization method for the device by using the Authentication Methods window, as described in the Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices.

We recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure the Windows Domain server settings, but if you want to use the CLI, see the following commands in the *Cisco Wide Area Application Services Command Reference*: **windows-domain join** and **kerberos** (if you are using Kerberos as a shared secure authentication method).

You must first configure the IP domain name and IP name server using the **ip** global configuration command.

Next, configure the appropriate NTP server using the **ntp** global configuration command.

Next, configure the windows domain administrative supergroup and normal group using the following global configuration commands:

```
WAE(config)# windows-domain administrative group super-user group_name
WAE(config)# windows-domain administrative group normal-user group_name
```

Next, register the WAAS device with the Windows domain server that you configured, by using the following command:

```
WAE# windows-domain join domain-name DomainName user UserName
```

To create a machine account in a specific organizational unit, use following command:

```
WAE# windows-domain join domain-name DomainName organization-unit OUName user UserName
```

Finally, enable Windows Domain as the administrative login authentication and authorization configuration by using the following commands:

```
WAE(config)# authentication login windows-domain enable primary
WAE(config)# authentication configuration windows-domain enable primary
```

Troubleshooting NTLM Authentication for EMAPI

The following CLI commands display diagnostic information on NTLM authentication for EMAPI:

```
# show windows-domain encryption-service identity
# show windows-domain encryption-service identity detail
# show windows-domain encryption-service blacklist identity
# show statistics connectoin conn-id ConnectionID
# show statistics accelerator mapi detail
```

Unregistering a WAE from a Windows Domain Controller

If you want to unregister a WAE device from a Windows domain controller, you can do that directly from the WAAS Central Manager, as long as you have used the Kerberos shared secure authentication method. If you have used the NTLM method, you cannot unregister the WAE by using the WAAS Central Manager; you must log in to the domain controller and remove the device registration manually.

Note Before you can unregister a device, you must disable Windows authentication for the device. Also, if Encrypted MAPI is utilizing the machine account domain identity, you must remove it before performing a domain leave.

To unregister a WAE device, follow these steps:

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

Step 2 Choose **Configure** > **Security** > **AAA** > **Authentication Methods**.

The Authentication and Authorization Methods window appears. (See Figure 7-6.)

Step 3 Under both the Authentication Login Methods and the Authorization Methods sections, change the value WINDOWS that is already chosen by choosing another value from the drop-down lists. For more information about changing these settings, see Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices.

Step 4 Click **Submit** to save the settings.

Step 5 Choose **Configure** > **Security** > **Windows Domain** > **Domain Settings**. If your WAAS device (or device group) is running a previous version of the software, click the **Domain Join** tab.

Step 6 (Optional) Enter the administrative username and password in the Administrator Username, Password, and Confirm Password fields. The domain controller requires the username and password to perform the unregistration.

Step 7 Click **Leave**.

Note When you click Leave, WAAS Central Manager immediately sends an unregistration request to the WAAS device (or device group) using SSH. The unregistration request instructs the device to unregister from the specified Windows Domain Controller.

Request to unregister the device is not allowed when encrypted MAPI is configured to use machine accounts. You must delete the machine account identity before proceeding with the leave.

The status of the unregistration request is shown in the Domain Join Status table.

Step 8 If your WAAS device (or device group) is running a previous version of the software, check the status of the unregistration request by waiting a few minutes and click **Show Join Status**.

If you want to use the CLI to unregister a WAE device, you must first use the following commands to disable windows authentication:

```
WAE(config)# no authentication login windows-domain enable
WAE(config)# no authentication configuration windows-domain enable
```

Note If an Encrypted MAPI machine account identity has been configured, then it has to be removed first. Use the **no windows-domain encryption-service** global configuration command to remove a machine account identity.

Next, unregister the WAAS device from the Windows domain server by using the following command (for Kerberos authentication):

```
WAE# windows-domain leave user UserName password Password
```

There is no CLI command to unregister the WAAS device if it is using NTLM authentication.

LDAP Server Signing

Lightweight Directory Access Protocol (LDAP) server signing is a configuration option of the Microsoft Windows Server's Network security settings. This option controls the signing requirements for LDAP clients. LDAP signing is used to verify that an intermediate party did not tamper with the LDAP packets on the network and to guarantee that the packaged data comes from a known source. Windows Server 2003 administration tools use LDAP signing to secure communications between running instances of these tools and the servers that they administer.

By using the Transport Layer Security (TLS, RFC 2830) protocol to provide communications privacy over the Internet, client/server applications can communicate in a way that prevents eavesdropping, tampering, or message forging. TLS v1 is similar to Secure Sockets Layer (SSL). TLS offers the same encryption on regular LDAP connections (ldap://:389) as SSL, while operating on a secure connection (ldaps://:636). A server certificate is used by the TLS protocol to provide a secure, encrypted connection to the LDAP server. A client certificate and key pair are required for client authentication.

In the WAAS software, login authentication with Windows 2003 domains is supported when the *LDAP server signing requirements* option for the Domain Security Policy is set to "Require signing." The LDAP server signing feature allows the WAE to join the domain and authenticate users securely.

Note When you configure your Windows domain controller to require an LDAP signature, you must also configure LDAP signing on the client WAE. By not configuring the client to use LDAP signatures, communication with the server is affected, and user authentication, group policy settings, and login scripts might fail. Install the Certification Authority service on the Microsoft server with the server's certificate (**Programs > Administrative Tools > Certification Authority**). Enable the LDAP server signing requirements property on the Microsoft server (**Start > Programs > Administrative Tools > Domain Controller Security Policy)**. In the window that is displayed, choose **Require signing** from the drop-down list, and click **OK**.

For information about how to configure your Windows domain controller to require an LDAP signature, see your Microsoft documentation.

This section contains the following topics:

- Configuring LDAP Signing on the Client WAEs
- Disabling LDAP Server Signing on a Client WAE

Configuring LDAP Signing on the Client WAEs

You can configure a security setting on Windows 2003 domain controllers to require clients (such as WAEs) to sign LDAP requests. Because unsigned network traffic can be intercepted and manipulated by outside parties, some organizations require LDAP server signing to prevent man-in-the-middle attacks on their LDAP servers. You configure LDAP signing only on a single WAE; it cannot be configured at a system level. In addition, you must configure LDAP signing on a WAE through the WAAS CLI; you cannot configure LDAP signing through any of the WAAS GUI.

By default, LDAP server signing is disabled on a WAE. To enable this feature on a WAE, follow these steps:

Step 1 Enable LDAP server signing on the WAE:

```
WAE# configure
WAE(config)# smb-conf section "global" name "ldap ssl" value "yes"
```

Step 2 Save the configuration on the WAE:

```
WAE(config)# exit
WAE# copy run start
```

Step 3 Verify the current running LDAP client configuration on the WAE:

```
WAE# show smb-conf
```

Step 4 Register the WAE with the Windows domain:

```
WAE# windows-domain diagnostics net "ads join -U username%password"
```

Step 5 Enable user login authentication on the WAE:

```
WAE# configure
WAE(config)# authentication login windows-domain enable primary
```

Step 6 Enable user login authorization on the WAE:

```
WAE(config)# authentication configuration windows-domain enable primary
```

Step 7 Check the current configuration for login authentication and authorization on the WAE:

```
WAE# show authentication user
Login Authentication:    Console/Telnet/Ftp/SSH Session
------------------------- -----------------------------
local                                enabled (secondary)
Windows domain           enabled (primary)
Radius                    disabled
Tacacs+                  disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
------------------------- -----------------------------
local                                enabled (primary)
Windows domain           enabled (primary)
Radius                    disabled
Tacacs+                  disabled
```

The WAE is now configured to authenticate Active Directory users, who can use Telnet, FTP, or SSH to connect to the WAE. Alternatively, they can access the WAE through the WAAS GUI.

Step 8 View statistics that are related to Windows domain user authentication. Statistics increment after each user authentication attempt:

```
WAE# show statistics windows-domain
Windows Domain Statistics
  ----------------------------------------------
  Authentication:
    Number of access requests:                    9
    Number of access deny responses:              3
    Number of access allow responses:             6
  Authorization:
    Number of authorization requests:             9
    Number of authorization failure responses:    3
    Number of authorization success responses:    6
  Accounting:
    Number of accounting requests:                0
    Number of accounting failure responses:       0
    Number of accounting success responses:       0

WAE# show statistics authentication
    Authentication  Statistics
    -------------------------------------
    Number of access requests:        9
    Number of access deny responses:  3
    Number of access allow responses: 6
```

Step 9 Use the **clear statistics** EXEC command to clear the statistics on the WAE:

- To clear all the login authentication statistics, enter the **clear statistics authentication** EXEC command.
- To clear only the statistics that are related to Windows domain authentication, enter the **clear statistics windows-domain** EXEC command.
- To clear all the statistics, enter the **clear statistics all** EXEC command.

Disabling LDAP Server Signing on a Client WAE

To disable LDAP server signing on a WAE, follow these steps:

Step 1 Unregister the WAE from the Windows domain:

```
WAE# windows-domain diagnostics net "ads leave -U Administrator"
```

Step 2 Disable user login authentication:

```
WAE# configure
WAE(config)# no authentication login windows-domain enable primary
```

Step 3 Disable LDAP signing on the WAE:

```
WAE(config)# no smb-conf section "global" name "ldap ssl" value "yes"
```

Enabling Administrative Login Authentication and Authorization Schemes for WAAS Devices

This section describes how to centrally enable the various administrative login authentication and authorization schemes (the authentication configuration) for a WAAS device or device group.

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

By default, a WAAS device uses the local database to authenticate and authorize administrative login requests. The WAAS device verifies whether all the authentication databases are disabled, and if so, sets the system to the default state. For information on this default state, see Default Administrative Login Authentication and Authorization Configuration.

Note You must configure the TACACS+, RADIUS, or Windows server settings for the WAAS device (or device group) before you configure and submit these settings. For information on how to configure these server settings on a WAAS device or device group, see About TACACS+ Server Authentication Settings, and Configuring RADIUS Server Authentication Settings, and Configuring Windows Domain Server Authentication Settings.

By default, WAAS devices fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method fails for any reason. Change this default login authentication failover method through the WAAS Central Manager GUI, as follows:

- To change the default for a WAAS device, choose **Devices** > *device-name* and then choose **Configure** > **Security** > **AAA** > **Authentication Methods** from the menu. Check the **Failover to next available authentication method** box in the displayed window and click **Submit**.
- To change the default for a device group, choose **Device Groups** > *device-group-name* and then choose **Configure** > **Security** > **AAA** > **Authentication Methods** from the menu. Check the **Failover to next available authentication method** box in the displayed window and click **Submit**.

After you enable the failover to next available authentication method option, the WAAS device (or the devices in the device group) queries the next authentication method only if the administrative login authentication server is unreachable, not if authentication fails for some other reason. The authentication server could be unreachable due to an incorrect key in the RADIUS or TACACS+ settings on the WAAS device.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **Failover to next available authentication method** check box.

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

If the failover to the next available authentication method option is *enabled*, follow these guidelines:

- You can configure only two login authentication schemes (a primary and secondary scheme) on the WAAS device.
- Note that the WAAS device (or the devices in the device group) fails over from the primary authentication scheme to the secondary authentication scheme only if the specified authentication server is unreachable.
- Configure the local database scheme as the secondary scheme for both authentication and authorization (configuration).

For example, if the failover to next available authentication method option is enabled and RADIUS is set as the primary login authentication scheme and local is set as the secondary login authentication scheme, the following events occur:

1. When the WAAS device (or the devices in the device group) receives an administrative login request, it queries the external RADIUS authentication server.
2. One of the following occurs:
   a. If the RADIUS server is reachable, the WAAS device (or the devices in the device group) uses this RADIUS database to authenticate the administrator.
   b. If the RADIUS server is not reachable, the WAAS device (or the devices in the device group) tries the secondary authentication scheme (that is, it queries its local authentication database) to authenticate the administrator.

Note The local database is contacted for authentication only if this RADIUS server is not available. In any other situation, for example, if the authentication fails in the RADIUS server, the local database is not contacted for authentication.

Conversely, if the failover to the next available authentication method option is *disabled*, the WAAS device (or the devices in the device group) contacts the secondary authentication database regardless of the reason why the authentication failed with the primary authentication database.

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

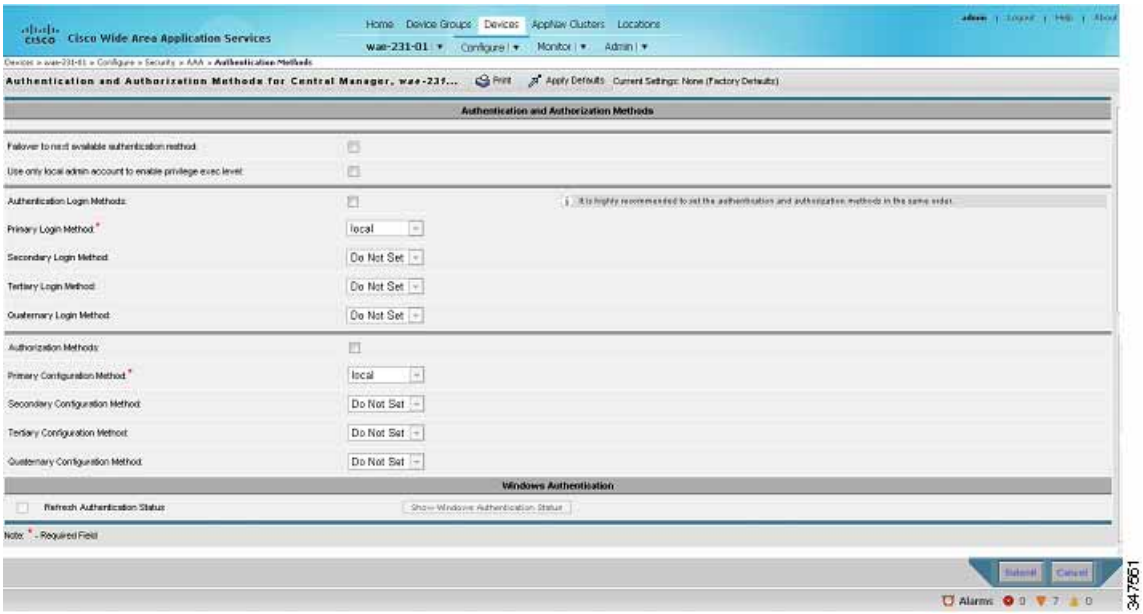
To specify the login authentication and authorization scheme for a WAAS device or device group, follow these steps:

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

Step 2 Choose **Configure** > **Security** > **AAA** > **Authentication Methods**.

The Authentication and Authorization Methods window appears. (See Figure 7-6.)

Figure 7-6 Authentication and Authorization Methods Window



Step 3 Check the **Failover to next available authentication method** check box to query the secondary authentication database only if the primary authentication server is unreachable. When the check box is unchecked, the other authentication methods are tried if the primary method fails for any reason.

To use this feature, you must set TACACS+, RADIUS, or Windows domain as the primary authentication method, and local as a secondary authentication method. Make sure that you configure the local method as a secondary scheme for both authentication and authorization (configuration).

Check the **Use only local admin account to enable privilege exec level** check box to configure enable authentication by using the local admin user account password. In this case, the request for enable access is not sent to the external authentication servers, but is processed on the WAE. It uses only the local "admin" user account password to verify the given password, and to provide access.

Step 4 Check the **Authentication Login Methods** check box to enable authentication privileges using the local, TACACS+, RADIUS, or WINDOWS databases.

Step 5 Specify the order of the login authentication methods that the chosen device or device group are to use:

a. From the Primary Login Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the first method that the chosen device (or the device group) should use for administrative login authentication.

b. From the Secondary Login Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or the device group) should use for administrative login authentication if the primary method fails.

c. From the Tertiary Login Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or the device group) should use for administrative login authentication if both the primary and the secondary methods fail.

d. From the Quaternary Login Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or device group) should use for administrative login authentication if the primary, secondary, and tertiary methods all fail.

Note We strongly recommend that you specify the local method as the last method in your prioritized list of login authentication and authorization methods. By adhering to this practice, the WAAS administrator will be able to log in to a WAAS device (or the devices in the device groups) through the local authentication and authorization method if the specified external third-party servers (TACACS+, RADIUS, or Windows domain servers) are not reachable.

Step 6 Check the **Authorization Methods** check box to enable authorization privileges using the local, TACACS+, RADIUS, or WINDOWS databases.

Note Authorization privileges apply to console and Telnet connection attempts, secure FTP (SFTP) sessions, and Secure Shell (SSH Version 2) sessions.

Step 7 Specify the order of the login authorization (configuration) methods that the chosen device (or the device group) should use:

Note We strongly recommend that you set the administrative login authentication and authorization methods in the same order. For example, configure the WAAS device (or device group) to use RADIUS as the primary login method, TACACS+ as the secondary login method, Windows as the tertiary method, and the local method as the quaternary method for both administrative login authentication and authorization.

a. From the Primary Configuration Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the first method that the chosen device (or the device group) should use to determine authorization privileges.

Note If you have checked the **Failover to next available authentication method** check box (Step 3), make sure that you choose **TACACS+ or RADIUS** from the Primary Configuration Method drop-down list to configure either the TACACS+ or RADIUS method as the primary scheme for authorization (configuration).

b. From the Secondary Configuration Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or the device group) should use to determine authorization privileges if the primary method fails.

Note If you have checked the **Failover to next available authentication method** check box (Step 3), make sure that you choose **local** from the Secondary Configuration Method drop-down list to configure the local method as the secondary scheme for authorization (configuration).

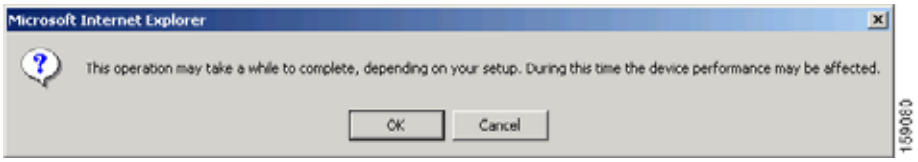
c. From the Tertiary Configuration Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or the device group) should use to determine authorization privileges if both the primary and secondary methods fail.

d. From the Quaternary Configuration Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **WINDOWS**. This option specifies the method that the chosen device (or device group) should use to determine authorization privileges if the primary, secondary, and tertiary methods all fail.

Step 8 To refresh the authentication status, check the check box and click **Show Windows Authentication Status**. This option is only available when Windows is set as the authentication and authorization methods.

A dialog box prompts you about whether or not you want to continue with this request to refresh the status of the authentication request. (See Figure 7-7.)

Figure 7-7 Confirmation Dialog Box



Step 9 Click **OK** to continue or **Cancel** to cancel the request.

If the request fails, an error dialog box is displayed. Wait for a few more minutes and try again to see the updated authentication status.

Step 10 Click **Submit** to save the settings.

Note If you have enabled the Windows authentication or authorization method, the Central Manager queries the WAE (of Version 4.2.1 or later) to ensure that it is registered to a Windows domain. This can take up to one minute after you click **Submit**. You will see a message asking you to confirm this process. Click **OK** to proceed. If you are configuring a WAE of Version 4.1.x or earlier, or a device group, the Central Manager does not query the WAEs and you must ensure that each WAE is properly registered. You will see a message informing you that system behavior is unknown (if a WAE is unregistered). Click **OK** to proceed.

Note If you have enabled the Windows authentication method, it takes about 15 seconds to activate it. Wait for at least 15 seconds before verifying the Windows authentication status or performing any operation that requires Windows authentication.

To configure the login authentication and authorization scheme from the CLI, use the **authentication** global configuration command. Before you enable Windows domain authentication or authorization for a device, the device must be registered with the Windows domain controller.

Configuring AAA Command Authorization

Command authorization enforces authorization through an external AAA server for each command executed by the CLI user. All the commands executed by a CLI user are authorized before they are executed. RADIUS, Windows domain, and local users are not affected.

Note Only commands executed through the CLI interface are subject to command authorization.

When command authorization is enabled, you must specify "permit null" on the TACACS+ server to allow authorized commands with no arguments to be executed.

To configure command authorization for a WAAS device or device group, 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** > **Command Authorization Settings**.

The Command Authorization window appears.

Step 3 Check the Command Authorization Level check box to mark the desired level:

- Level 0—Only EXEC commands are authorized by the TACACS+ server before they are executed, regardless of user level (normal or super). Global configuration commands are not allowed.
- Level 15—Both EXEC and global configuration level commands are authorized by the TACACS+ server before they are executed, regardless of user level (normal or super).

Note You must have a TACACS+ server configured before you can configure command authorization.

Step 4 Click **Submit** to save the settings.

Configuring Cisco Prime Network Control System Single Sign-On

New IOS/WAAS features, such as AppNav and kWAAS, require the use of both WAAS and Cisco Prime Network Control System (NCS) management systems at the same time. Lack of integration between the NCS and WAAS CM impairs user experience. NCS Single Sign-On (SSO) functionality provides a way to integrate these two systems and seamlessly launch the WAAS CM from NCS.

The NCS integration has the following prerequisites:

- The NCS device is running the 2.x code.
- The Cisco IOS-XE device must be running 3.10 code.
- The Cisco WAAS 5.3.0 or later Central Manager is installed and configured.
- The IOS-XE device with kWAAS instance is configured.
- The kWAAS instance is registered with the WAAS CM.

To configure the NCS, follow the steps below:

Step 1 Configure the NCS device. For more information, see Configuring the NCS Device.

Step 2 Configure the WAAS CM. For more information, see Configuring the WAAS CM to use SSO.

Step 3 Use the Single Sign-on feature. For more information, see Launching WAAS CM from NCS.

Configuring the NCS Device

To configure the NCS Server follow these steps:

Step 1 Log in to Prime NCS to add the SSO server:

a. Choose **Administration** > **Users, Roles & AAA** > **SSO servers**.

b. Enter the SSO server information, then click **Save**.

Note If you use an external Cisco Prime host for SSO, specify the IP address of that host. If you do not currently use the SSO functionality to log in to Cisco Prime, use the IP address of the Cisco Prime device itself.

Step 2 To enable SSO authentication:

a. Choose **Administration** > **Users, Roles & AAA** > **AAA mode**.

b. Click the **SSO mode** radio button. Click **Save**.

Step 3 To configure WAAS CM address:

a. Choose **Administration** > **System Settings** > **Service Container Management** and enter the WAAS CM Ip address in the **WCM IP Address** field.

b. Click **Save**.

Configuring the WAAS CM to use SSO

To configure the WAAS CM to use SSO follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin** > **AAA** > **Users** to configure a NCS user account.
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.Create a new non-local (remote) user account with the name matching exactly the name of the NCS SSO user. Assign needed roles and domains in the **Role Management** and **Domain Management** windows.

Step 3 To configure the NCS server from the WAAS CM:

a. From the WAAS Central Manager menu, choose **Devices** > **WAAS CM**> **Configure AAA**> **Cisco Prime SSO**

b. Check the **Enable NCS Single Sign-on** check box, enter the NCS SSO server URL to configure the SSO server. Click **Submit**.

c. Verify Server Certificate and click Submit.

The SSO feature is now ready for use.

Launching WAAS CM from NCS

To launch WAAS CM from NCS follow these steps:

Step 1 Go to Cisco Prime Server and select the appropriate device from the Service Container.

Step 2 Click the **WAAS CM UI** tab to launch the WAAS CM GUI.

Alternatively, select the device to launch the device instance homepage in the WAAS CM GUI.

Configuring AAA Accounting for WAAS Devices

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

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

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

Note Before you can configure the AAA accounting settings for a WAAS device, you must first configure the TACACS+ server settings for the WAAS device. (See About TACACS+ Server Authentication Settings.)

Note If you enable AAA accounting for a device, we strongly recommended that you create an IP ACL condition in the first entry position permitting access to the TACACS+ servers to avoid delay while processing the commands. For information on IP ACLs, see Chapter 9, "Creating and Managing IP Access Control Lists for Cisco WAAS Devices."

To centrally configure AAA accounting settings for a WAAS device or device group, 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** > **AAA Accounting**.

The AAA Accounting Settings window appears.

Step 3 From the **System Events** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track system-level events that are not associated with users, such as reloads, and to activate accounting for system events.

Step 4 From the **Exec Shell and Login/Logout Events** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track EXEC shell and user login and logout events and to activate accounting for EXEC mode processes. Reports include username, date, start and stop times, and the WAAS device IP address.

Step 5 From the **Normal User Commands** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track all the commands at the normal user privilege level (privilege level 0) and to activate accounting for all the commands at the nonsuperuser administrative (normal user) level.

Step 6 From the **Administrative User Commands** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track all commands at the superuser privilege level (privilege level 15) and to activate accounting for all the commands at the superuser administrative user level.

Caution Before using the **wait-start** option, ensure that the WAAS device is configured with the TACACS+ server and is able to successfully contact the server. If the WAAS device cannot contact a configured TACACS+ server, it might become unresponsive.

Table 7-3 describes the event type options.

Table 7-3 Event Types for AAA Accounting

GUI Parameter	Function
Event Type Options	
stop-only	The WAAS device sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.
start-stop	The WAAS device sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server. The start accounting record is sent in the background. The requested user service begins regardless of whether or not the start accounting record was acknowledged by the TACACS+ accounting server.
wait-start	The WAAS device sends both a start and a stop accounting record to the TACACS+ accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.
Do Not Set	Accounting is disabled for the specified event.

Step 7 Check the **Enable CMS CLI Accounting** check box to enable AAA accounting to TACACS+ server.

Step 8 Click **Submit** to save the settings.

To configure AAA accounting settings from the CLI, use the **aaa accounting** global configuration command.

Viewing Audit Trail Logs

The WAAS Central Manager device logs user activity in the system. The only activities that are logged are those activities that change the WAAS network. For more information on viewing a record of user activity on your WAAS system, see Viewing the Audit Trail Log in Chapter 16, Troubleshooting Your WAAS Network."