Configuring Other System Settings

This chapter describes how to perform other system tasks such as setting the system clock, modifying the default system configuration settings, and enabling alarm overload detection, after you have done a basic configuration of your WAAS device. This chapter also describes how to register and manage Cisco IOS routers running AppNav-XE and WAAS Express.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE and WAVE appliances, SM-SRE modules running WAAS, and vWAAS instances.

This chapter contains the following sections:

Modifying Device Properties

The WAAS Central Manager GUI allows you to make the following changes to the properties of a WAE device:

- Rename the device
- Assign a new location to the device
- Assign an IP address to be used for management traffic to the device

- Deactivate or activate the device

You can also use the WAAS Central Manager GUI to check the status of a device to determine if it is online, pending, or inactive.

You can only rename a WAAS Central Manager device from the GUI.

To modify a device's properties, follow these steps:

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

Step 2 Choose *device-name* > **Activation**.

The Device Activation window appears with fields for editing the properties of the selected device.

For a WAAS Central Manager device, the only fields that you can change in this window are the name and NetBIOS name of the device. In addition, the device IP address and role are displayed.

Step 3 Under the General Configuration heading, set or modify the following device properties:

- To change the hostname of the device, enter a new name in the Name field. This name must conform to the following rules:
  - The name must use only alphanumeric characters and hyphens (-).
  - The first and last character must be a letter or a digit.
  - Maximum length is 30 characters.
  - Names are case insensitive.
  - The following characters are considered illegal and cannot be used when naming a device: @, #, $,%, ^, &, *, (), |, \””/, <>.
- To activate or deactivate the device, check or uncheck the **Activate** check box.When this box is checked, the device is activated for centralized management through the WAAS Central Manager GUI.

  You can also click the **Deactivate** icon in the task bar to deactivate the device. Deactivating a device allows you to replace the device in the event of a hardware failure without losing all of its configuration settings.
- To change the NetBIOS name of the device, enter the new NetBIOS name for the device in the provided field. The NetBIOS name must not consist of only numbers; it must include some letters. This field is not displayed for WAAS Express devices.

Step 4 Under the Locality heading, set or change the location by choosing a new location from the **Location** drop-down list. To create a location for this device, see the "Creating Locations" section on page 3-10.

Step 5 Under the Management Interface Configuration with NAT heading, configure the NAT settings using the following fields:

- Check the **Use WAE's primary IP Address** check box to enable the WAAS Central Manager to use the IP address configured on the primary interface of the device to communicate with devices in the WAAS network that are behind a NAT firewall. This check box is not displayed for WAAS Express devices.
- Allow the WAAS Central Manager to communicate with devices in the WAAS network that are behind the NAT firewall using an explicitly configured IP address, by entering the IP address of the device in the Management IP field. You also need to enter this address in scenarios where the primary interface for a WAE is set to an inline group interface and management traffic is configured on a separate IP address (either on a secondary IP address on the same inline group interface or on a built-in interface).

- In the Port field, enter the port number for the management IP address. If the HTTPS server configured on a WAAS Express device is using a different port than the default of 443, configure the same port here.

Note If the WAAS Central Manager cannot contact a device using the primary IP address, it attempts to communicate using the Management IP address.

Step 6 In the Comments field, enter any comments that you want to appear for this device.

Step 7 Click **Submit**.

Managing Software Licenses

WAAS software version 4.1.1 introduces software licenses that enable specific WAAS optimization and acceleration features. A software license must be installed and configured before the features that it enables will operate.

Table 10-1 lists the software licenses that may be purchased and the features that each license enables.

Table 10-1 WAAS Software Licenses

License	Description
Transport	Enables basic DRE, TFO, and LZ optimization. Cannot be configured if the Enterprise license is configured.
Enterprise	Enables the EPM, HTTP, MAPI, NFS, SSL, CIFS, SMB, ICA, and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization. Cannot be configured if the Transport license is configured.
Video	Enables the video application accelerator. Requires the Enterprise license to be configured first.
Virtual-Blade	Enables the virtualization feature. Requires the Enterprise license to be configured first.

Licenses are installed and managed only on individual WAE devices, not device groups. Not all licenses are supported on all devices. A WAAS Central Manager device requires only the Enterprise license and no other licenses can be configured.

Note WAAS Express licenses are managed by using the router CLI command **license install**, not from the WAAS Central Manager. WAAS Express devices do not use the same kind of licenses as WAAS devices do. They use a single license that enables the WAAS Express optimization feature.

Note If you are upgrading the WExp devices to PI22 image, as part of the new Appxk9 license support in WExp PI22 images, you need to upgrade the WAAS Central Manager to 5.3.1 OR later. Else the devices go offline.

To add a license to a WAE from the WAAS Central Manager, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name*. (Do not choose a Central Manager device because you must use the CLI to manage licenses on Central Managers.)

Step 2 Choose **Admin** > **History** > **License Management**.

Step 3 Check the check box next to each license that you want to add.

Step 4 Click **Submit**.

To add licenses from the CLI, you can use the **license add** EXEC command.

To remove licenses from the CLI, you can use the **clear license** EXEC command.

To display the status of all licenses from the CLI, you can use the **show license** EXEC command.

The setup utility also configures licenses when you first set up a new WAAS device.

Enabling the Inetd RCP and FTP Services

Remote Copy Protocol (RCP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection oriented. Inetd (an Internet daemon) is a program that listens for connection requests or messages for certain ports and starts server programs to perform the services associated with those ports. RCP copies files between devices.

RCP is a subset of the UNIX rshell service, which allows UNIX users to execute shell commands on remote UNIX systems. It is a UNIX built-in service. This service uses TCP as the transport protocol and listens for requests on TCP port 514. RCP service can be enabled on WAAS devices that use WAAS software.

To enable RCP and FTP services on a WAAS device, 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** > **Network Services**. The Network Services window appears.

Step 3 Check the **Enable RCP** check box to enable Inetd RCP services. By default, this option is disabled.

Note The Inetd daemon listens for FTP, RCP, and TFTP services. For Inetd to listen to RCP requests, it must be explicitly enabled for RCP service.

Step 4 Check the **Enable FTP** check box to enable the Inetd FTP service. By default, this option is disabled.

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

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 the Reset button. The Reset button is visible only when you have applied default or group settings to change the current device settings but you have not yet submitted the changes.

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

Configuring Date and Time Settings

This section explains how to configure date and time settings for your WAAS network devices and contains the following topics:

Configuring NTP Settings

The WAAS Central Manager GUI allows you to configure the time and date settings using a Network Time Protocol (NTP) host on your network. NTP allows the synchronization of time and date settings for the different geographical locations of the devices in your WAAS network, which is important for proper system operation and monitoring. On each WAAS device, be sure to set up an NTP server to keep the clocks synchronized.

To configure NTP settings, 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** > **Date/Time** > **NTP**. The NTP Settings window appears.

Step 3 In the NTP Server field, enter up to four hostnames or IP addresses, separated by spaces.

Step 4 Click **Submit**.

Note Unexpected time changes can result in unexpected system behavior. We recommend reloading the system after configuring an NTP server or changing the system clock.

Configuring Time Zone Settings

If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not need to set the system clock manually. When manually setting the clock, enter the local time.

Note Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

To configure the time zone on a 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** > **Date/Time** > **Time Zone**. The Time Zone Settings window appears.

Step 3 To configure a standard time zone, follow these steps:

a. Under the Time Zone Settings section, click the **Standard Time Zone** radio button. The default is UTC (offset = 0) with no summer time configured. When you configure a standard time zone, the system is automatically adjusted for the UTC offset, and the UTC offset need not be specified.

The standard convention for time zones uses a *Location/Area* format in which *Location* is a continent or a geographic region of the world and *Area* is a time zone region within that location.

b. From the drop-down list, choose a location for the time zone. (For an explanation of the abbreviations in this list, see Table 10-2.)

The window refreshes, displaying all area time zones for the chosen location in the second drop-down list.

c. Choose an area for the time zone. The UTC offset is automatically set for standard time zones.

Summer time is built-in for some standard time zones (mostly time zones within the United States), and will result an automatic change in the UTC offset during summer time. For a list of standard time zones that can be configured and their UTC offsets, see Table 10-3.

Step 4 To configure a customized time zone on the device, follow these steps:

a. Under the Time Zone Settings section, click the **Customized Time Zone** radio button.

b. In the Customized Time Zone field, specify the name of the time zone. The time zone entry is case-sensitive and can contain up to 40 characters including spaces. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.

c. For UTC Offset, choose the + or – sign from the first drop-down list to specify whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (0–23) and minutes (0–59) offset from UTC for the customized time zone. The range for the UTC offset is from –23:59 to 23:59, and the default is 0:0.

Step 5 To configure customized summer time, follow these steps under the Customized Summer Time Savings section.

Note You can specify a customized summer time for both standard and customized time zones.

a. To configure absolute summer time, click the **Absolute Dates** radio button.

You can configure a start date and end date for summer time in absolute dates or recurring dates. Absolute date settings apply only once and must be set every year. Recurring dates apply repeatedly for many years.

b. In the Start Date and End Date fields, specify the month (January through December), day (1–31), and year (1993–2032) on which summer time must start and end in mm/dd/yyyy format. Make sure that the end date is always later than the start date.

Alternatively, click the **Calendar** icon next to the Start Date and End Date fields to display the Date Time Picker popup window. By default the current date is highlighted in yellow. In the Date Time Picker popup window, use the left or right arrow icons to choose the previous or following years, if

required. Choose a month from the drop-down list. Click a day of the month. The chosen date is highlighted in blue. Click **Apply**. Alternatively, click **Set Today** to revert to the current day. The chosen date will be displayed in the Start Date and End Date fields.

c. To configure recurring summer time, click the **Recurring Dates** radio button.

d. From the Start Day drop-down list, choose a day of the week (**Monday**-**Sunday**) to start.

e. From the Start Week drop-down list, choose an option (**first**, **2nd**, **3rd**, or **last**) to set the starting week. For example, choose **first** to configure summer time to recur beginning the first week of the month or **last** to configure summer time to recur beginning the last week of the month.

f. From the Start Month drop-down list, choose a month (**January**–**December**) to start.

g. From the End Day drop-down list, choose a day of the week (**Monday**–**Sunday**) to end.

h. From the End Week drop-down list, choose an option (**first**, **2nd**, **3rd**, or **last**) to set the ending week. For example, choose **first** to configure summer time to end beginning the first week of the month or **last** to configure summer time to stop beginning the last week of the month.

i. From the End Month drop-down list, choose a month (**January**–**December**) to end.

Step 6 From the Start Time drop-down lists, choose the hour (0–23) and minute (0–59) at which daylight saving time should start. From the End Time drop-down lists, choose the hour (0–23) and minute (0–59) at which daylight saving time should end.

Start Time and End Time fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start and end times are set at 00:00.

Step 7 In the Offset field, specify the minutes offset from UTC (0–1439). (See Table 10-3.)

The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.

Step 8 Click the **No Customized Summer Time Configured** radio button to not specify a summer or daylight saving time for the corresponding time zone.

Step 9 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 the Reset button. The Reset button is visible only when you have applied default or group settings to change the current device settings but have not yet submitted the changes.

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

Table 10-2 Timezone Location Abbreviations

Time Zone	Expansion
CET	Central European Time
CST6CDT	Central Standard/Daylight Time
EET	Eastern European Time
EST	Eastern Standard Time
EST5EDT	Eastern Standard/Daylight Time
GB	Great Britain
GB-Eire	Great Britain/Ireland
GMT	Greenwich Mean Time
HST	Hawaiian Standard Time

Table 10-2 Timezone Location Abbreviations (continued)

Time Zone	Expansion
MET	Middle European Time
MST	Mountain Standard Time
MST7MDT	Mountain Standard/Daylight Time
NZ	New Zealand
NZ-CHAT	New Zealand, Chatham Islands
PRC	People's Republic of China
PST8PDT	Pacific Standard/Daylight Time
ROC	Republic of China
ROK	Republic of Korea
UCT	Coordinated Universal Time
UTC	Coordinated Universal Time
WET	Western European Time
W-SU	Middle European Time

Table 10-3 Timezone—Offset from UTC

Time Zone	Offset from UTC (in hours)
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	–3
America/Caracas	–4
America/Mexico_City	–6
America/Lima	–5
America/Santiago	–4
Atlantic/Azores	–1
Atlantic/Cape_Verde	–1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30

Table 10-3 Timezone—Offset from UTC (continued)

Time Zone	Offset from UTC (in hours)
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	–4
Canada/Newfoundland	–3.30
Canada/Saskatchewan	–6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	+12
Pacific/Samoa	–11
US/Alaska	–9

Table 10-3 Timezone—Offset from UTC (continued)

Time Zone	Offset from UTC (in hours)
US/Central	–6
US/Eastern	–5
US/East–Indiana	–5
US/Hawaii	–10
US/Mountain	–7
US/Pacific	–8

UTC was formerly known as Greenwich Mean Time (GMT). The offset time (number of hours ahead or behind UTC) as displayed in the table is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.

Configuring Secure Store Settings

Secure store encryption provides strong encryption and key management for your WAAS system. The WAAS Central Manager and WAE devices use secure store encryption for handling passwords, managing encryption keys, and for data encryption.

This section contains the following topics:

Secure Store Overview

With secure store encryption on the Central Manager or a WAE device, the WAAS system uses strong encryption algorithms and key management policies to protect certain data on the system. This data includes encryption keys used by applications in the WAAS system, CIFS accelerator passwords for prepositioning, user login passwords, NAM credentials, and certificate key files.

Secure store encryption on the Central Manager is always enabled and uses a password that is auto-generated or user-provided. This password is used to generate the *key encryption key* according to secure standards. The WAAS system uses the key encryption key to encrypt and store other keys

generated on the Central Manager or WAE devices. These other keys are used for WAAS functions including disk encryption, SSL acceleration, or to encrypt and store CIFS accelerator credentials, and user passwords.

Data on the Central Manager is encrypted using a 256-bit key encryption key generated from the password and using SHA1 hashing and an AES 256-bit algorithm. When secure store is enabled on a WAE device the data is encrypted using a 256-bit key encryption key generated using SecureRandom, a cryptographically strong pseudorandom number generator.

Secure store encryption on a Central Manager uses one of the following modes:

- Auto-generated passphrase mode—The passphrase is automatically generated by the Central Manager and used to open the secure store after each system reboot. This is the default mode for new Central Manager devices or after the system has been reinstalled.
- User-provided passphrase mode—The passphrase is supplied by the user and must be entered after each system reboot to open the secure store. You can switch to this mode, and systems upgraded from versions prior to 4.4.1, with secure store initialized, are configured in this mode after upgrading to 4.4.1 or later.

To implement secure store your system must meet the following requirements:

- You must have a Central Manager configured for use in your network.
- Your WAE devices must be registered with the Central Manager.
- Your WAE devices must be online (have an active connection) with the Central Manager. This requirement applies only if you are enabling secure store on WAE devices.
- All Central Managers and WAE devices must be running WAAS software version 4.0.19 or higher.

To implement strong store encryption, follow these steps:

Step 1 Enable strong storage encryption on your primary Central Manager. See Enabling Secure Store Encryption on the Central Manager.

Step 2 Enable strong storage encryption on any standby Central Managers. See Enabling Secure Store Encryption on a Standby Central Manager.

Step 3 Enable strong storage encryption on WAE devices or WAE device groups. See Enabling Secure Store Encryption on a WAE Device. (Secure store must be enabled on the Central Manager before you enable it on the WAE devices.)

You can enable secure store independently on the Central Manager and on the WAE devices. To ensure full protection of your encrypted data, enable secure store on both the Central Manager and the WAE devices. You must enable secure store on the Central Manager first.

Note When you reboot the Central Manager, if secure store is in user-provided passphrase mode, you must manually open secure store encryption. All services that use the secure store (disk encryption, CIFS prepositioning, SSL acceleration, AAA, and so on) on the remote WAE devices do not operate properly until you enter the secure store password on the Central Manager to open secure store encryption.

Note the following considerations regarding the secure store:

- Passwords stored in the Central Manager database are encrypted using strong encryption techniques.
- CIFS prepositioning credentials are encrypted using the strong encryption key on the Central Manager and the WAE devices.

- Certificate key files are encrypted using the strong encryption key on the Central Manager.
- If a primary Central Manager fails, secure store key management is handled by the standby Central Manager. (Secure store mode must be enabled manually on the standby Central Manager.)
- Backup scripts back up the secure store passphrase mode (user-provided or auto-generated) of the device at the time of backup. Backup and restore are supported only on the Central Manager.
- If you have a backup made when the secure store was in user-provided passphrase mode and you restore it to a system where the secure store is in auto-generated passphrase mode, you must enter the user passphrase to proceed with the restore. After the restore, the system is in user-provided passphrase mode. If you have a backup made when the secure store was in auto-generated passphrase mode and you restore it to a system where the secure store is in user-provided passphrase mode, you do not need to enter a password. After the restore, the system is in auto-generated passphrase mode.
- When you enable secure store on a WAE device, the system initializes and retrieves a new encryption key from the Central Manager. The WAE uses this key to encrypt data such as CIFS prepositioning credentials and information on the disk (if disk encryption is also enabled).
- When you reboot the WAE after enabling secure store, the WAE retrieves the key from the Central Manager automatically, allowing normal access to the data that is stored in WAAS persistent storage. If key retrieval fails, a critical alarm is raised and secure store should be reopened manually. Until secure store is reopened, the WAE rejects configuration updates from the Central Manager if the updates contain CIFS preposition, dynamic share, or user configuration. Also, the WAE does not include preposition configuration in the updates that it sends to the Central Manager.
- While secure store encrypts certain system information, it does not encrypt the data on the hard drives. To protect the data disks, you must enable disk encryption separately. See the "Enabling Disk Encryption" section on page 16-31.

Enabling Secure Store Encryption on the Central Manager

Secure store is enabled by default on a new Central Manager, with a system-generated password that opens the secure store after the system boots. You do not need to do anything to enable secure store.

If a Central Manager is configured in user-provided passphrase mode, you must manually open the secure store after the system boots. To open secure store encryption on the Central Manager, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Secure Store**. The Configure CM Secure Store window appears.

Step 2 Enter the secure store passphrase in the Current passphrase field under Open Secure Store.

Step 3 Click the **Open** button.

The secure store is opened. Data is encrypted using the key derived from the password.

To open the secure store from the CLI, use the **cms secure-store open** EXEC command.

Note Whenever you reboot a Central Manager that is configured in user-provided passphrase mode, you must reopen the secure store manually. All services that use the secure store (disk encryption, CIFS prepositioning, SSL acceleration, AAA, and so on) on the remote WAE devices do not operate properly until you enter the secure store password on the Central Manager to reopen the secure store. Switch to auto-generated passphrase mode to avoid having to reopen the secure store after each reboot.

Note When you enable secure store on the primary Central Manager in user-provided passphrase mode, you should enable secure store on the standby Central Manager as well. See Enabling Secure Store Encryption on a Standby Central Manager, page 10-13.

You can check the status of secure store encryption by entering the **show cms secure-store** command.

Enabling Secure Store Encryption on a Standby Central Manager

Note A standby Central Manager provides limited encryption key management support. If the primary Central Manager fails, the standby Central Manager provides only encryption key retrieval to the WAE devices but does not provide new encryption key initialization. Do not enable disk encryption or secure store on WAE devices when the primary Central Manager is not available.

The secure store passphrase mode on the primary Central Manager is replicated to the standby Central Manager (within the standard replication time). If the primary Central Manager is switched to auto-generated passphrase mode, the standby Central Manager secure store changes to the open state. If the primary Central Manager is switched to user-provided passphrase mode or the passphrase is changed, the standby Central Manager secure store changes to the initialized but not open state and an alarm is raised. You must manually open the secure store on the standby Central Manager.

To enable secure store encryption on a standby Central Manager when the primary Central Manager is in user-provided passphrase mode, open the secure store on the primary Central Manager and then use the CLI to execute the **cms secure-store open** EXEC mode command on the standby Central Manager:

Step 1 Enable secure store encryption on the primary Central Manager. See the "Enabling Secure Store Encryption on the Central Manager" section on page 10-12.

Step 2 Wait until the standby Central Manager replicates the data from the primary Central Manager.

The replication should occur in 60 seconds (default) or as configured for your system.

Step 3 Enter the **cms secure-store open** command on the standby Central Manager to activate secure store encryption.

The standby Central Manager responds with the "please enter pass phrase" message.

Step 4 Type the password and press **Enter**.

The standby Central Manager encrypts the data using secure store encryption.

Note Repeat Steps 3 and 4 for each standby Central Manager on your system.

You can check the status of secure store encryption by entering the **show cms secure-store** command.

Enabling Secure Store Encryption on a WAE Device

To enable secure store encryption on a WAE device, follow these steps:

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

Note The secure store status must be the same for all WAE devices in a device group. Either all WAE devices in the group must have secure store enabled, or all must have secure store disabled. Before you add a WAE device to a device group, set its secure store status to match the others. See the "Working with Device Groups" section on page 3-2.

Step 2 Choose **Configure** > **Security** > **Secure Store**. The Secure Store Settings window appears

Step 3 Check the **Initialize CMS Secure Store** box. (The Open CMS Secure Store box will be checked automatically.)

Step 4 Click **Submit** to activate secure store encryption.

A new encryption key is initialized on the Central Manager, and the WAE encrypts the data using secure store encryption.

To enable secure store from the CLI, use the **cms secure-store init** EXEC command.

Note If you have made any other CLI configuration changes on a WAE within the datafeed poll rate time interval (5 minutes by default) before executing the **cms secure-store** command, those prior configuration changes are lost and you must redo them.

Note When you enable or disable secure store on a device group, the changes do not take effect on all WAE devices simultaneously. When you view the WAE devices be sure to give the Central Manager enough time to update the status of each WAE device.

Changing Secure Store Passphrase Mode

The secure store can operate either in user-provided or auto-generated passphrase mode and you can switch between these modes.

To change from user-provided to auto-generated passphrase mode, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin** > **Secure Store**.

Step 2 In the Switch to CM auto-generated passphrase mode area, enter the password in the Current passphrase field.

Step 3 Click the **Switch** button.

Step 4 Click **OK** in the confirmation message that appears.

The secure store is changed to auto-generated passphrase mode and remains in the open state.

To change from auto-generated to user-provided passphrase mode, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin** > **Secure Store**.

Step 2 In the Switch to User-provided passphrase mode area, enter a password in the New passphrase field and reenter the password in the Confirm passphrase field.

The password must conform to the following rules:

- Be 8 to 64 characters in length
- Contain characters only from the allowed set: A-Za-z0-9~%'!#$^&*()|;:,"<>/
- Contain at least one digit
- Contain at least one lowercase and one uppercase letter

Step 3 Click the **Switch** button.

Step 4 Click **OK** in the confirmation message that appears.

The secure store is changed to user-provided passphrase mode and remains in the open state. If you have a standby Central Manager, you must manually open its secure store (see the "Enabling Secure Store Encryption on a Standby Central Manager" section on page 10-13).

To change secure store passphrase mode from the CLI, use the **cms secure-store mode** EXEC command.

Note Whenever you reboot a Central Manager that is configured in user-provided passphrase mode, you must reopen the secure store manually. All services that use the secure store (disk encryption, CIFS prepositioning, SSL acceleration, AAA, and so on) on the remote WAE devices do not operate properly until you enter the secure store password on the Central Manager to reopen the secure store. Switch to auto-generated passphrase mode to avoid having to reopen the secure store after each reboot.

Changing the Secure Store Encryption Key and Password

The secure store encryption password is used by the Central Manager to generate the encryption key for the encrypted data. If the Central Manager is configured for user-provided passphrase mode, you can change the password.

To change the password and generate a new encryption key on the Central Manager, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin** > **Secure Store**.

Step 2 In the Change Secure Store passphrase area, in the Current passphrase field, enter the current password.

Step 3 In the New passphrase field, enter the new password.

The password must conform to the following rules:

- Be 8 to 64 characters in length
- Contain characters only from the allowed set: A-Za-z0-9~%'!#$^&*()|;:,"<>/

- Contain at least one digit
- Contain at least one lowercase and one uppercase letter

Step 4 In the Confirm passphrase field, enter the new password again.

Step 5 Click the **Change** button.

The WAAS device reencrypts the stored data using a new encryption key derived from the new password.

To change the password and generate a new encryption key on the Central Manager from the CLI, use the **cms secure-store change** EXEC command.

To generate a new encryption key for a WAE device from the WAAS Central Manager, 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** > **Secure Store**.

Step 3 Check the **Change CMS Secure Store** box and then click **Submit**.

A new encryption key is generated in the Central Manager. The Central Manager replaces the encryption key in the WAE with the new key. The WAE re-encrypts the stored data using the new encryption key.

To configure the secure store encryption key from the CLI, use the **cms secure-store change** EXEC command.

Resetting Secure Store Encryption on a Central Manager

You can reset the secure store if you reload the Central Manager and you cannot open the secure store because it is configured in user-provided passphrase mode and you forget the secure store password. This procedure deletes all encrypted data, certificate and key files, and key manager keys. The secure store is reinitialized, configured in auto-generated passphrase mode, and opened.

To reset secure store encryption on a Central Manager, follow these steps:

Step 1 At the primary Central Manager CLI, enter the **cms secure-store reset** command to reset secure store encryption.

Step 2 Wait until the standby Central Manager replicates the data from the primary Central Manager.

The replication should occur in 60 seconds (default) or as configured for your system.

Step 3 Enter the **cms secure-store reset** command on the standby Central Manager if secure store is in the initialized and open state.

Step 4 From the primary Central Manager, reset all user account passwords, CIFS credentials, and NAM credentials.

For information on resetting user passwords, see the "Changing the Password for Another Account" section on page 8-7. For information on resetting dynamic share passwords, see the "Creating Dynamic Shares for the CIFS Accelerator" section on page 12-9. For information on resetting preposition passwords, see the "Creating a New Preposition Directive" section on page 12-12. For information on resetting NAM credentials, see the "Configuring the Basic Setup" section on page 15-3.

Step 5 On each WAE registered to the Central Manager, follow these steps:

a. If secure store is initialized and open, from the Central Manager, clear secure store (see the "Disabling Secure Store Encryption on a WAE Device" section on page 10-17). Or, from the CLI, enter the **cms secure-store clear** EXEC command.

b. From the Central Manager, initialize secure store (see the "Enabling Secure Store Encryption on a WAE Device" section on page 10-14) or from the CLI, enter the **cms secure-store init** EXEC command. (This step is needed only if you performed Step 5a.)

c. Enter the **crypto pki managed-store initialize** command and restart the SSL accelerator.

d. If disk encryption is enabled, from the Central Manager, disable disk encryption (see the "Enabling Disk Encryption" section on page 16-31) or from the CLI, enter the **no disk encrypt enable** global configuration command.

e. If disk encryption had been enabled before Step 5d, reload the device. After the reload, reenable disk encryption and reload the device again.

Note If the WAE is reloaded before doing Step 5, disk encryption, SSL acceleration, and secure store does not function properly. In this case, you must restore the WAE to factory defaults.

Step 6 From the primary Central Manager, reimport all certificate and key files for all the accelerated and peering services which are configured on the WAEs.

Disabling Secure Store Encryption on a WAE Device

To disable secure store encryption on a WAE device, 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** > **Secure Store**. The Secure Store Settings window appears.

Step 3 Check the **Clear CMS Secure Store** box and then click Submit to disable secure store encryption and return to standard encryption.

You can also enter the **cms secure-store clear** command to disable secure store encryption and return to standard encryption.

Note If a Windows Domain User account identity has been configured on the device or the device group for encrypted-mapi acceleration, you will not be able to clear the secure store on the device. You must remove the Windows domain user account identity configuration from the device or device group before you can clear secure store.

Note You cannot clear secure store on a device that contains an encrypted services user account domain identity. See the "Configuring Encrypted MAPI Acceleration" section for more information on user account domain identities.

To disable secure store on a WAE from the CLI, use the **cms secure-store clear** EXEC command.

Note Secure store cannot be disabled on a Central Manager.

Modifying the Default System Configuration Properties

The WAAS software comes with preconfigured system properties that you can modify to alter the default behavior of the system.

Table 10-4 describes the system configuration properties that you can modify.

Table 10-4 Descriptions for System Configuration Properties

System Property	Description
cdm.remoteuser.deletionDaysLimit	Maximum number of days since their last login after which external users will be deleted from the WAAS Central Manager database. For example, if cdm.remoteuser.deletionDaysLimit is set to 5, external users will be deleted from the database if the difference between their last login time and the current time is more than 5 days. The default is 60 days. External users are users that are defined in an external AAA server and not in the WAAS Central Manager. Any reports scheduled by such users are also deleted when the users are deleted.
cdm.session.timeout	Timeout in minutes of a WAAS Central Manager GUI session. The default is 10 minutes. If the session is idle for this length of time, the user is automatically logged out.
DeviceGroup.overlap	Status of whether a device can belong to more than one device group. The default is true (devices can belong to more than one device group).
System.datafeed.pollRate	Poll rate between a WAAS (or WAAS Express) device and the WAAS Central Manager (in seconds). The default is 300 seconds.
System.device.recovery.key	Device identity recovery key. This property enables a device to be replaced by another node in the WAAS network.
System.guiServer.fqdn	Scheme to use (IP address or FQDN) to launch the Device Manager GUI.
System.healthmonitor.collectRate	Collect and send rate in seconds for the CMS device health (or status) monitor. If the rate is set to 0, the health monitor is disabled. The default is 120 seconds.
System.lcm.enable	This setting controls propagation of device CLI configuration changes back to the CM. If disabled, configuration changes done in device's CLI will not be communicated to the Central Manager. This setting is system wide and applies to all managed WAAS devices. Note that disabling this setting may result in Central Manager and WAAS device(s) configuration to go out of sync. You can customize this setting for specific device in Device -> Admin -> Config Synchronization UI page.

Table 10-4 Descriptions for System Configuration Properties (continued)

System Property	Description
System.pcm.enable	This setting controls whether WAAS devices accept or ignore configuration changes received from the Central Manager. It could be used in deployments where WAAS devices are not managed by Central Manager but other entity(i.e. directly via CLI). Note that disabling this setting may result in Central Manager and WAAS device(s) configuration to go out of sync. You can customize this setting for specific device in Device -> Admin -> Config Synchronization UI page.
System.monitoring.collectRate	Rate at which a WAE collects and sends the monitoring report to the WAAS Central Manager (in seconds). For a WAAS Express device, this is the rate at which the Central Manager collects the monitoring data from the WAAS Express device. The default is 300 seconds (5 minutes). Reducing this interval impacts the performance of the WAAS Central Manager device.
System.monitoring.dailyConsolidationHour	Hour at which the WAAS Central Manager consolidates hourly and daily monitoring records. The default is 1 (1:00 a.m.).
System.monitoring.enable	WAAS and WAAS Express statistics monitoring (enable or disable). The default is true.
System.monitoring.maxDevicePerLocation	Maximum number of devices for which monitoring is supported in location level reports. The default is 25.
System.monitoring.maxReports	Maximum number of completed or failed report instances to store for each custom report. The default is 10 report instances.
System.monitoring.monthlyConsolidationFrequency	How often (in days) the WAAS Central Manager consolidates daily monitoring records into monthly records. If this setting is set to 1, the WAAS Central Manager checks if consolidation needs to occur every day, but only performs consolidation if there is enough data for consolidation to occur. The default is 14 days. When a monthly data record is created, the corresponding daily records are removed from the database. Consolidation occurs only if there is at least two calendar months of data plus the consolidation frequency days of data. This ensures that the WAAS Central Manager always maintains daily data records for the past month and can display data on a day level granularity for the last week. For example, if data collection starts on February 2nd, 2006 and System.monitoring.monthlyConsolidationFrequencyis set to 14, then the WAAS Central Manager checks if there is data for the past two calendar months on the following days: Feb 16th, March 2nd, March 16th, and March 30th. No consolidation will occur because there is not enough data on these days. On April 13th, however, two calendar months of data exists. The WAAS Central Manager then consolidates data for the month of February and deletes the daily data records for that month.
System.monitoring.recordLimitDays	Maximum number of days of monitoring data to maintain in the system. The default is 1825 days.

Table 10-4 Descriptions for System Configuration Properties (continued)

System Property	Description
System.monitoring.timeFrameSettings	Default time frame to be used for plotting all the charts. Settings saved by the user will not be changed. The default is Last Hour.
System.registration.autoActivation	Status of the automatic activation feature, which automatically activates WAAS and WAAS Express devices that are registered to the Central Manager. The default is true (devices are automatically registered).
System.rpc.timeout.syncGuiOperation	Timeout in seconds for the GUI synchronization operations for the Central Manager to WAE connection. The default is 50 seconds.
System.security.maxSimultaneousLogins	Maximum number of concurrent WAAS Central Manager sessions permitted for a user. Specify 0 (zero, the default) for unlimited concurrent sessions. A user must log off the Central Manager to end a session. If a user closes the browser without logging off, the session is not closed until after it times out after 120 minutes (the timeout is not configurable). If the number of concurrent sessions permitted also is exceeded for that user, there is no way for that user to regain access to the Central Manager GUI until after the timeout expires. This setting does not affect CLI access to the Central Manager device.
System.security.webApplicationFilter	Status of the web application filter, which rejects any javascript, SQL, or restricted special characters in input. The default is false.
System.standby.replication.maxCount	Maximum number of statistics data records (in thousands) that will be replicated to a standby Central Manager. The range is 10 to 300. The default is 200 (200,000 records). We do not recommend increasing this number.
System.standby.replicationTimeout	Maximum number of seconds to wait for replication to a standby Central Manager. The range is 300 to 3600 seconds. The default is 900 seconds. We do not recommend decreasing this timeout.
System.WcmIosUser.enable	Enables creation of WCM user on the registered IOS device. Global / device level / DG level IOS Router credential pages will be hidden if this system property is enabled.

To view or modify the value of a system property, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure > Global > System Properties**. The Config Properties window appears.

Step 2 Click the **Edit** icon next to the system property that you want to change. The Modifying Config Property window appears.

Step 3 From a drop-down list, enter a new value or choose a new parameter, depending on the system property that you want to change.

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

Configuring the Web Application Filter

Web Application Filter is a security feature that protects the WAAS Central Manager GUI against Cross-Site Scripting (XSS) attacks. XSS security issues can occur when an application sends data that originates from a user to a web browser without first validating or encoding the content, which can allow malicious scripting to be executed in the client browser, potentially compromising database integrity.

This security feature verifies that all application parameters sent from WAAS users are validated and/or encoded before populating any HTML pages.

This section contains the following topics:

Enabling the Web Application Filter

To enable the Web Application Filter, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure > Global > System Properties**. The Config Properties window appears.

Note You cannot enable this feature using the CLI. This feature is disabled by default.

Step 2 Click the Edit icon next to the system.security.webApplicationFilter entry.

The Modifying Config Property window appears.

Step 3 Choose **true** from the Value drop-down list to enable this feature.

A confirmation message appears to advise Central Manager and Device Manager users to log out and then back in after enabling this feature.

Step 4 Click **OK** and then **Submit**.

Step 5 Log out and then back in again.

Security Verification

The Web Application Filter feature verifies security using two methods, input verification and sanitization. Input validation validates all input data before accepting data. Sanitization prevents malicious configuration and scripts already present in the data from getting executed.

This section contains the following topics:

Input Validation

Input validation scans all data that is input to the Central/Device Manager database and is only configurable by the admin user.

Any input submitted using the Central Manager GUI that is suspicious of XSS is blocked. Blocked input results in a warning.

Input data is checked against the following XSS filter rules:

- Input is rejected if it contains a semicolon (;)
- Input is rejected if it is enclosed in angle brackets (<>)
- Input is rejected if it can be indirectly used to generate the above tags (&#60, &#62, %3c, %3e)

Sanitization

The sanitizer prevents malicious configuration and scripts from getting executed in the browser when there is an XSS attack on the database. Sanitization is not configurable by the user.

Configuration data coming from the Central Manager that is suspect for XSS is shown in red on the Device Groups > All Device Groups page.

Configuring Faster Detection of Offline WAAS Devices

You can detect offline WAAS devices more quickly if you enable the fast detection of offline devices. A WAAS device is declared as offline when it has failed to contact the WAAS Central Manager for a getUpdate (get configuration poll) request for at least two polling periods. (See the "About Faster Detection of Offline Devices" section on page 10-23 for more information about this feature.)

To configure fast detection of offline WAAS devices, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure > Global > Fast Device Offline Detection**. The Configure Fast Offline Detection window appears.

Note The fast detection of offline devices feature is in effect only when the WAAS Central Manager receives the first UDP heartbeat packet and a getUpdate request from a device.

Step 2 Check the **Enable Fast Offline Detection** check box to enable the WAAS Central Manager to detect the offline status of devices quickly.

Step 3 In the Heartbeat Rate field, specify how often devices should transmit a UDP heartbeat packet to the WAAS Central Manager, in seconds. The default is 30 seconds.

Step 4 In the Heartbeat Fail Count field, specify the number of UDP heartbeat packets that can be dropped during transmission from devices to the WAAS Central Manager before a device is declared offline. The default is 1.

Step 5 In the Heartbeat UDP Port field, specify the port number using which devices will send UDP heartbeat packets to the primary WAAS Central Manager. The default is port 2000.

The Maximum Offline Detection Time field displays the product of the failed heartbeat count and heartbeat rate.

Maximum Offline Detection Time = Failed heartbeat count * Heartbeat rate

If you have not enabled the fast detection of offline devices feature, then the WAAS Central Manager waits for at least two polling periods to be contacted by the device for a getUpdate request before declaring the device to be offline. However, if you enable the fast detection of offline devices feature, then the WAAS Central Manager waits until the value displayed in the Maximum Offline Detection Time field is exceeded.

If the WAAS Central Manager receives the Cisco Discovery Protocol (CDP) from a device, then the WAAS Central Manager GUI displays the device as offline after a time period of 2* (heartbeat rate) * (failed heartbeat count).

Step 6 Click **Submit**.

Note Any changes to the Configure Fast WAE offline detection page in the Central Manager could result in devices temporarily appearing to be offline. Once the configuration changes are propagated to the devices, they show as online again.

About Faster Detection of Offline Devices

Communication between the WAAS device and WAAS Central Manager using User Datagram Protocol (UDP) allows faster detection of devices that have gone offline. UDP heartbeat packets are sent at a specified interval from each device to the primary WAAS Central Manager in a WAAS network. The primary WAAS Central Manager tracks the last time that it received a UDP heartbeat packet from each device. If the WAAS Central Manager has not received the specified number of UDP packets, it displays the status of the nonresponsive devices as offline. Because UDP heartbeats require less processing than a getUpdate request, they can be transmitted more frequently, and the WAAS Central Manager can detect offline devices much faster.

You can enable or disable this feature, specify the interval between two UDP packets, and configure the failed heartbeat count. Heartbeat packet rate is defined as the interval between two UDP packets. Using the specified heartbeat packet rate and failed heartbeat count values, the WAAS Central Manager GUI displays the resulting offline detection time as a product of heartbeat rate and failed heartbeat count. If the fast detection of offline devices is enabled, the WAAS Central Manager detects devices that are in network segments that do not support UDP and uses getUpdate (get configuration poll) request to detect offline devices.

By default, the feature to detect offline devices more quickly is not enabled.

Configuring Alarm Overload Detection

WAAS devices can track the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM), then the WAAS device enters an alarm overload state. This situation occurs when multiple applications raise alarms at the same time to report error conditions. When a WAAS device is in an alarm overload state, the following occurs:

- SNMP traps for subsequent alarm raise and clear operations are suspended. The trap for the raise alarm-overload alarm and the clear alarm-overload alarm are sent; however, traps related to alarm operations between the raise alarm-overload alarm and the clear alarm-overload alarm operations are suspended.

- Alarm overload raise and clear notifications are not blocked. The alarm overload state is communicated to SNMP and the Configuration Management System (CMS). However, in the alarm overload state, SNMP and the CMS are not notified of individual alarms. The information is only available by using the CLI.
- The WAAS device remains in an alarm overload state until the rate of incoming alarms decreases to the point that the alarm rate is less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the WAAS device comes out of the alarm overload state and begins to report the alarm counts to SNMP and the CMS.

When the WAAS device is in an alarm overload state, the Node Health Manager continues to record the alarms being raised on the WAAS device and keeps a track of the incoming alarm rate. Alarms that have been raised on a WAAS device can be listed using the **show alarm** CLI commands that are described in the *Cisco Wide Area Application Services Command Reference.*

To configure alarm overload 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** > **Monitoring** > **Alarm Overload Detection**. The Alarm Overload Detection Settings window appears.

Step 3 Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the WAAS device (or device group) to suspend alarm raise and clear operations when multiple applications report error conditions. This check box is checked by default.

Step 4 In the Alarm Overload Low Water Mark (Clear) field, enter the number of incoming alarms per second below which the WAAS device comes out of the alarm overload state.

The low-water mark is the level up to which the number of alarms must drop before alarms can be restarted. The default value is 1. The low-water mark value should be less than the high-water mark value.

Step 5 In the Alarm Overload High Water Mark (Raise) field, enter the number of incoming alarms per second above which the WAAS device enters the alarm overload state. The default value is 10.

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

To configure alarm overload detection from the CLI, you can use the **alarm overload-detect** global configuration command.

Configuring the E-mail Notification Server

You can schedule reports to be generated periodically, and when they are generated, a link to the report can be e-mailed to one or more recipients. (For details, see the "Managing Reports" section on page 17-48.)

To enable e-mail notification, you must configure e-mail server settings for the WAAS Central Manager by following these steps:

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

Step 2 Choose **Configure** > **Monitoring** > **Email Notification**. The Configure Email Server Details window appears.

Step 3 In the Mail Server Hostname field, enter the hostname of the SMTP e-mail server that is to be used to send e-mail.

Note Only SMTP mail servers are supported. If any other type of mail server is configured, the email notification fails.

Step 4 In the Mail Server Port field, enter the port number. The default is port 25.

Step 5 In the Server Username field, enter a valid e-mail account username.

Step 6 In the Server Password field, enter the password for the e-mail account.

Step 7 In the From Address field, enter the e-mail address shown as the sender of the e-mail notification.

Step 8 Click **Submit**.

Using IPMI over LAN

Intelligent Platform Management Interface (IPMI) over LAN provides remote platform management service for WAVE-294/594/694/7541/7571/8541 appliances. IPMI is an open standard technology that defines how administrators monitor system hardware and sensors, control system components, and retrieve logs of important system events to conduct remote management and recovery. IPMI runs on the Baseboard Management Controller (BMC) and operates independently of WAAS. After IPMI over LAN is set up and enabled on WAAS, authorized users can access BMC remotely even when WAAS becomes unresponsive or the device is powered down but connected to a power source. You can use an IPMI v2 compliant management utility, such as ipmitool or OSA SMbridge, to connect to the BMC remotely to perform IPMI operations.

The IPMI over LAN feature provides the following remote platform management services:

- Supports the power on, power off, and power cycle of the WAAS appliance.
- Monitors the health of the WAAS hardware components by examining Field Replaceable Unit (FRU) information and reading sensor values.
- Retrieves logs of important system events to conduct remote management and recovery.
- Provides serial console access to the WAAS appliance over the IPMI session.
- Support for IPMI Serial over LAN (SoL)—IPMI SoL enables a remote user to access a WAAS appliance through a serial console through an IPMI session.

IPMI over LAN and IPMI SoL features can be configured using CLI commands and include the following:

- Configuring IPMI LAN interface
- Configuring IPMI LAN users
- Configuring security settings for remote IPMI access
- Enabling/disabling IPMI over LAN
- Enabling/disabling IPMI SoL
- Restoring the default settings for the BMC LAN channel

- Displaying the current IPMI over LAN and IPMI SoL configurations

For more information on configuring IPMI over LAN, see the "Configuring BMC for Remote Platform Management" section on page 10-27.

BMC Firmware Update

IPMI over LAN requires that a specific BMC firmware version be installed on the device. The minimum supported BMC firmware versions are:

- WAVE-294/594/694—48a
- WAVE-7541/7571/8541—26a

WAAS appliances shipped from the factory with WAAS version 4.4.5 or later do have the correct firmware installed. If you are updating a device that was shipped with an earlier version of WAAS software, you must update the BMC firmware, unless it was updated previously.

To determine if you are running the correct firmware version, use the **show bmc info** command. The following example displays the latest BMC firmware version installed on the device (48a here):

```
wave# show bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.48                    <<<<< version 48
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 160 (0x00a0)
Product Name              : Unknown (0xA0)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
    0x0c
    0x08
    0x0a                                            <<<<< a
. . .
```

If a BMC firmware update is needed, you can download it from cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image is named waas-bmc-installer-48a-48a-26a-k9.bin or a newer version may be available. Use the latest firmware update that is available.

You can use the following command to update the firmware from the image file that is available through FTP on your network:

copy ftp install *ip-address remotefiledir* **waas-bmc-installer-48a-48a-26a-k9.bin**

The update process automatically checks the health status of the BMC firmware. If BMC firmware corruption is detected, BMC is recovered during the BMC firmware update procedure. The complete update process can take several minutes and the device may appear unresponsive but do not interrupt the process or power cycle the device. After the update is complete, you must reload the device.

After the device reboots, you can verify the firmware version by using the **show bmc info** command.

BMC recovery and BMC firmware update restores the factory defaults on the BMC and all the current IPMI over LAN configurations are erased.

If BMC firmware corruption happens, a critical alarm is raised.

Configuring BMC for Remote Platform Management

This section describes the minimum steps needed to enable IPMI over LAN and IPMI SoL to conduct remote platform management. This section includes the following topics:

Enabling IPMI Over LAN

To enable IPMI over LAN, perform the following steps using the **bmc lan** command:

Step 1 Change the default BMC LAN IP address.

Step 2 Change the password for the BMC default user, which is user 2.

Step 3 Enable IPMI over LAN.

Step 4 Access the BMC from a remote client over IPMI session v2.0 using the username and password for the number 2 user. The default cipher suite used to access the BMC is 3, which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.

Step 5 To access the BMC over a IPMI session v1.5, change the user 2 IPMI-session-version setting from v2.0 to v1.5.

Enabling IPMI SoL

To enable IPMI SoL, perform the following steps:

Step 1 On the WAAS device, configure and enable IPMI over Lan (IoL).

Step 2 On the remote client make sure that the BMC user can do IoL operations successfully over IPMI session v2.0.

Step 3 On the remote client, change the baud-rate of the terminal to match the WAAS console baud rate of 9600 bps.

Step 4 On the WAAS device, enable IPMI SoL.

Step 5 On the remote client, if the IPMI management tool is ipmitool, check the SoL payload status of the specific BMC user with the following command:
ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol payload status 1** *bmc-user-userid*

For example:

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is disabled
```

Step 6 If the SoL payload is disabled for this user, enable the SoL payload for this user with the following command:
ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol payload enable 1** *bmc-user-userid*

For example:

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload enable 1 3
Password:
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is enabled
```

Step 7 On the remote client, use the following command to open the serial console to the WAAS device: **ipmitool -I lanplus -H** *bmc-ip-address* **-U** *bmc-user-name* **sol activate**

Step 8 On the remote client, you have now entered the console session of the WAAS device. When you are done, use the ~. escape character to terminate the connection.

Managing Cisco IOS Router Devices

You can use the WAAS Central Manager to manage WAAS Express and AppNav-XE devices, which are both Cisco IOS routers deployed with WAAS related software. The Central Manager menu displays a subset of the full menu when a WAAS Express or device AppNav-XE is selected as the context, as these devices implement a subset of WAAS appliance functionality.

The Central Manager and a Cisco IOS device communicate using the HTTPS protocol. To establish communication between a WAAS Central Manager and a Cisco IOS router device, you must register the Cisco IOS router device with the Central Manager. Using the Central Manager GUI to register a Cisco IOS router device is the easiest method.

This section includes the following topics:

Registering a Cisco IOS Router Device Using the Central Manager GUI

To register a Cisco IOS router device, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Registration > Cisco IOS Routers**. The Cisco IOS Router Registration window appears.

Note To register a Cisco IOS router device using the Central Manager GUI, SSH v1 or v2 must be enabled on the router.

Step 2 In the IP Address(es) field, enter the router IP addresses to register, separated by commas. The IP address, hostname, router type, and status are displayed in the Registration Status table.

You may also upload a CSV file that contains a list of IP addresses to register. To upload a list, click the **Import CSV file** radio button and click the **Choose File** button to browse to the file and click **Open**. Each IP address must be on a separate line.

Step 3 Configure the router login credentials by entering the username, password, and enable password. If you need to create a user on the router, see the "Configuring a User" section on page 10-31.

Step 4 Choose the HTTP Authentication Type, local or AAA.

Note Be sure to choose the HTTP authentication type that is currently configured on the router. If you choose an HTTP authentication type that differs from your current configuration, your existing configuration on the router will be overwritten and you may not be able to use HTTP to communicate with the router. Communications with routers with previously established authentication credentials will fail.

Step 5 In the Central Manager IP Address field, enter the IP address you want the router to use for the Central Manager. This field is initially filled in with the current Central Manager IP address but you may need to change this in a NAT environment.

Step 6 Click the Register button and verify that the registration status was successful.

You may view the results in the log file: /local/local1/errlog/waasx-audit.log

After you successfully register a Cisco IOS router device, the Central Manager displays it in the Registration Status table and in the All Devices list.

In case your want to register additional devices, use the Reset button to clear data from all the fields, to enter the next configuration.

You may need to install a software license on the Cisco IOS router device. For details, see the "Installing a License on the Router" section on page 10-34.

Configuring Router Credentials

For the Central Manager to access a Cisco IOS router device, you must configure the router credentials in the Central Manager.

On the Central Manager, you can define global credentials that apply to all Cisco IOS router devices, or you can define credentials at the device group or individual device level by using the Admin > Authentication > WAAS Express Credentials/AppNav-XE Credentials menu item. To configure device group or individual device credentials, you must first complete the Cisco IOS router registration process and then configure credentials for a router device group or device. Device and device group credentials have precedence over global credentials.

To configure global router credentials, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Security > Cisco IOS Router Global Credentials**. The Cisco IOS Router Global Credentials window appears.

Step 2 In the Username field, enter a username that is defined on the Cisco IOS router. If you need to create a user on the router, see the "Configuring a User" section on page 10-31.

Note The username field is optional if you are not using local or AAA authentication for the HTTP server on the Cisco IOS router device; that is, if you use the default HTTP server configuration of **ip http authentication enable**. (See the "Enabling the HTTP Secure Server on the Router" section on page 10-33.)

Step 3 In the Password field, enter the password for the specified username.

Step 4 Click **Submit**.

Note Changing the router credentials on the Central Manager does not change the configuration on the router device itself. It affects only the router credentials that are stored on the Central Manager.

Registering a Cisco IOS Router Using the CLI

You can also register a Cisco IOS router device with the Central Manager using the CLI by completing the steps outlined in Table 10-5. This procedure applies to Cisco IOS routers running both WAAS Express and AppNav-XE.

Table 10-5 Checklist for Registering a Cisco IOS Router Using the CLI

Task	Additional Information and Instructions
1. Configure a username and password.	The same username and password are configured on the router and the Central Manager, so the Central Manager can log in to the router for management purposes. For more information, see the "Configuring a User" section on page 10-31.
2. Import the primary Central Manager administrative server certificate into the router.	The router requires the Central Manager certificate for secure HTTPS server communication. For more information, see the "Importing the Central Manager Certificate" section on page 10-31.
3. Configure a router certificate.	The Central Manager device requests this router certificate for secure HTTPS server communication. For more information, see the "Configuring a Router Certificate" section on page 10-32.
4. Enable the secure HTTP server with user authentication.	Enables the Central Manager and router to communicate. For more information, see the "Enabling the HTTP Secure Server on the Router" section on page 10-33.
5. Install a permanent WAAS software license.	Allows the WAAS software to operate on the router. For more information, see the "Installing a License on the Router" section on page 10-34.
6. Configure an NTP server.	Keeps the time synchronized between the router and the Central Manager. For more information, see the "Configuring an NTP Server" section on page 10-34.
7. Register the router with the Central Manager.	Registers the router with the Central Manager. For more information, see the "Registering the Router" section on page 10-34.

The following sections describe these steps in detail.

Configuring a User

The first step in setting up your router and Central Manager to communicate is to configure the same user on the router and the Central Manager.

To configure a user, follow these steps:

Step 1 Log in to the router CLI.

Step 2 Configure a local user with privilege level 15 on the router by using the **username** IOS configuration command:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#username cisco privilege 15 password 0 cisco
router(config)#exit
```

Alternatively, you can configure an external TACACS+ or RADIUS user; see details after this procedure.

Step 3 Save the running configuration:

```
router#write memory
Building configuration...
[OK]
```

Step 4 In the WAAS Central Manager, configure the router credentials as described in the "Configuring Router Credentials" section on page 10-29.

To configure an external TACACS+ user on the router, use the following configuration commands on the router:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login default group tacacs+
router(config)#aaa authorization exec default group tacacs+
router(config)#tacacs-server host host-ip
router(config)#tacacs-server key keyword
```

To configure an external RADIUS user on the router, use the following configuration commands on the router:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login default group radius
router(config)#aaa authorization exec default group radius
router(config)#radius-server host host-ip
router(config)#radius-server key keyword
```

The external authentication server for TACACS+ or RADIUS must be Cisco ACS 4.x or 5.x.

Importing the Central Manager Certificate

The next step is to import the certificate from the Central Manager into the router.

To import the certificate, follow these steps:

Step 1 Log in to the Central Manager CLI.

Step 2 Display the administrative certificate by using the show crypto EXEC command:

```
waas-cm#show crypto certificate-detail admin

...
-----BEGIN CERTIFICATE-----
TIICezCCAeSgAwIBAgIEVwMK8zANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYD
VQQLEwRDTkJVMRswGQYDVQQKExJDaXNjbyBTeXN0ZW1zLCBJbmMxHjAcBgNVBAMT
FWRvYy13YWFzLWNtLmNpc2NvLmNvbTAeFw0wODA3MjQxOTMwMjNaFw0xMzA3MjMx
OTMwMjNaMIGBMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8G
A1UEBxMIU2FuIEpvc2UxDTALBgNVBAsTBENOQlUxGzAZBgNVBAoTEkNpc2NvIFN5
c3RlbXMsIEluYzEeMBwGA1UEAxMVZG9jLXdhYXMtY20uY2lzY28uY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCy10xBfsUDTh5imYwkkterx/IqkNQO7KB/
M0wqIK2j4zj4BpR1ztKaFyEtGjqGpxPBQ54V9EHGmGUljx/Um9PORk3AXyWoUsDf
o0T2Z94FL5UoVUGzUia6/xiUrPCLNf6BLBDGPQg970QtZSU+DYUqjYHzDgv6yXFt
viHARbhZdQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADKF7aIeQ+Uh4Y2zZJwlaIF7
ON+RqDvtyy4DNerEN9iLI4EFO/QJ+uhChZZU8AKR8u3OnLPSNtNck33OWwMemcOd
QGhnsMtiUq2VuSh+A3Udm+sMLFguCw5RmJvqKTrj3ngAsmDBW3uaK0wkPGp+y3+0
2hUYMf+mCrCOwBEPfs/M
-----END CERTIFICATE-----
```

Step 3 Copy the certificate text, which is the part in between the BEGIN CERTIFICATE and END CERTIFICATE lines in the output.

Step 4 Log in to the router CLI.

Step 5 Configure a certificate for the Central Manager:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto pki trustpoint wcm

router(ca-trustpoint)#enrollment terminal pem
router(ca-trustpoint)#exit
router(config)#crypto pki authenticate wcm

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Step 6 Paste in the certificate that you copied from the Central Manager in Step 3.

Configuring a Router Certificate

The router needs a certificate that is requested by the Central Manager when establishing HTTPS communication. This procedure describes how to configure a persistent self-signed certificate on the router, but you can also use a CA signed certificate.

To configure a router certificate, follow these steps:

Step 1 Log in to the router CLI.

Step 2 Create a self-signed certificate on the router:

Note Due to CSCsy03412, you must configure **ip domain name** *name* before enrolling the certificate. If you do not configure **ip domain name**, IOS regenerates the self-signed certificate upon reload and this affects the communication with the WAAS Central Manager.

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto pki trustpoint local
router(ca-trustpoint)#enrollment selfsigned
router(ca-trustpoint)#subject-alt-name routerFQDN
router(ca-trustpoint)#exit
router(config)#crypto pki enroll local
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 10.10.10.25
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

If the router certificate changes after the router is registered with the Central Manager, you must reimport the certificate into the Central Manager. For details, see the "Reimporting a Router Device Certificate" section on page 10-35.

Enabling the HTTP Secure Server on the Router

The Central Manager and a router communicate using the HTTPS protocol. You must enable the HTTP secure server on the router.

To enable the HTTP secure server, follow these steps:

Step 1 On the router, enable the HTTP secure server:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip http secure-server
```

Note Be sure to choose the HTTP authentication type that is currently configured on the router. If you choose an HTTP authentication type that differs from your current configuration, your existing configuration on the router will be overwritten and you will not be able to use HTTP to communicate with the router.

Step 2 Configure authentication for the HTTP server for a local user as follows:

```
router(config)#ip http authentication local
```

If you are using external TACACS+ or RADIUS user authentication, configure authentication for the HTTP server as follows:

```
router(config)#ip http authentication aaa
```

Note If you do not configure local or AAA authentication for the HTTP server, only the enable password is used for authentication. (The default is **ip http authentication enable**, which uses only the enable password and no username.) If this default configuration is used, it is not necessary to define a username credential for the router on the Central Manager. (See the "Configuring a User" section on page 10-31.)

Installing a License on the Router

The router requires one or more licenses to operate the WAAS Express or AppNav-XE software. Refer to the router documentation for details.

To install a license, follow these steps:

Step 1 Obtain and copy the appropriate license to a location accessible to the **license** command on the router.

Step 2 On the router, install the license:

```
router#license install ftp://infra/licenses/FHH122500AZ_20100811190225615.lic
```

This example uses FTP to get and install the license but there are various options available for this command. Choose one that best suits your deployment.

Step 3 Save the running configuration:

```
router#write memory
Building configuration...
[OK]
```

Configuring an NTP Server

It is important to keep the time synchronized between devices in your WAAS network. You should already have an NTP server configured for the Central Manager (see the "Configuring NTP Settings" section on page 10-5).

To configure an NTP server for the router, on the router use the **ntp server** global configuration command, as follows:

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ntp server 10.10.10.55
```

Registering the Router

The final step in setting up a router with the Central Manager is to register the device. You will need to know the IP address of the Central Manager.

To register a router with the Central Manager, follow these steps:

Step 1 For a WAAS Express router, register with the Central Manager as follows:

```
router#waas cm-register https://CM_IP_Address:8443/wcm/register
```

For an AppNav-XE router, register with the Central Manager as follows:

```
router#appnav cm-register https://CM_IP_Address:8443/wcm/register
```

In the URL for this command, specify the Central Manager IP address as indicated. Be sure to include a colon and the port number of 8443.

If a permanent WAAS license is not installed on the router, you must accept the terms of the evaluation license to continue. The evaluation license is valid for 60 days.

Step 2 Save the running configuration:

```
router#write memory
Building configuration...
[OK]
```

After the successful registration of the router in the Central Manager, the Central Manager initially shows the device on the Manage Devices page with a management status of Pending and a license status of Active. After the Central Manager retrieves the device configuration and status, the management status changes to Online and the license status changes to Permanent (or Evaluation, Expires in x weeks y days).

Reimporting a Router Device Certificate

If the router device certificate changes after you have registered the router device with the Central Manager, you must reimport a matching certificate into the Central Manager.

To reimport a router device certificate, follow these steps:

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

Step 2 Choose **Admin** > **Authentication** > **Identity Certificate**. The Certificate window appears

The Certificate Info tab shows the certificate information for the device. The Certificate in PEM Encoded Format tab shows the certificate in PEM format. You can copy the certificate from this tab to use in the paste operation in the next step.

Step 3 Import this certificate into the Central Manager by selecting one of the following radio buttons that are shown above the tabs:

- **Upload PEM file**—Click **Choose File** and locate the PEM file containing the certificate.
- **Manual**—Paste the PEM-encoded certificate in the text field that appears.

Step 4 Click **Submit**.

Creating a new WAAS Central Manager IOS user on pre-registered IOS devices

A router that has already been registered with the WAAS Central Manager(WCM) before the system property was enabled needs to be migrated to communicate with the WCM. To enable this communication, you need to create a new WAAS CM IOS user so that the ongoing communication uses the same to communicate with the WCM.

The WAAS Express User Creation Tool window is visible only when the System.WcmIosUser.enable is enabled on the **Home** > **Configure** > **System Properties** > **WcmIosUser.**

To create a new WAAS Central Manager IOS user on the registered IOS device, follow the steps:

Step 1 From the WAAS Central Manager menu, choose **Home > Admin > Security > WCM Cisco IOS User Creation Tool**. The WAAS Express User Creation Tool window appears.

Step 2 Configure the router login credentials by entering the username, password, and enable.

In the IP Address(es) field, enter the WAAS Express router IP addresses to migrate, separated by commas. The IP address, hostname and status are displayed in the Status table.

You may also upload a CSV file that contains a list of IP addresses to migrate. To upload a list, click the Upload File check box and click the Choose File button to browse to the file and click Open. Each IP address must be on a separate line.

Step 3 Click the Update button to create a new WAAS CM IOS user on the router and verify that the user creation status was successful.

In case your want to migrate additional pre- registered routers, use the Reset button to clear data from all the fields, to enter the next configuration.