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 Cisco WAAS device. This chapter also describes how to register and manage Cisco IOS routers running Cisco AppNav-XE and Cisco WAAS Express.

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

This chapter contains the following sections:

Modifying Device Properties

Use the Cisco WAAS Central Manager GUI to make the following changes to the properties of a Cisco 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 Cisco 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 Cisco WAAS Central Manager device from the GUI.

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

Step 1 From the Cisco 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 Cisco 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 Cisco 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 Cisco 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 Creating Locations, page 3-12 in the chapter "Using Device Groups and Device Locations".

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 Cisco 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 Cisco 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 Cisco 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 display for this device.

Step 7 Click **Submit**.

Managing Cisco WAAS Software Licenses

This section contains the following topics:

About Managing Cisco WAAS Software Licenses

Cisco WAAS Version 4.1.1 and later provides software licenses that enable specific Cisco 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 Cisco 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, SSL, SMB, ICA, and Windows Print application accelerators, the Cisco WAAS Central Manager, and basic DRE, TFO, and LZ optimization. Cannot be configured if the Transport license is configured.

Consider the following operating guidelines for Cisco WAAS software licenses:

- Licenses are installed and managed only on individual Cisco WAE devices, *not* device groups. Not all licenses are supported on all devices.

- A Cisco WAAS Central Manager device requires only the Enterprise license and no other licenses can be configured.
- Cisco WAAS Express licenses cannot be managed via the Cisco WAAS Central Manager, because Cisco WAAS Express devices do not use the same kind of licenses as Cisco WAAS devices. Cisco WAAS Express licenses are managed via the router CLI only.

  The exact WAAS Express licensing process depends on the version of IOS running on your WAAS Express router:

  – Prior to Cisco IOS Version 15.3(3), the Cisco WAAS Express license is managed by using the router CLI command **license install.** This uses a single license that enables the Cisco WAAS Express optimization feature.

  – For Cisco IOS Version 15.3(3)M, the Cisco WAAS Express feature no longer requires a separate license, but is a Right To Use (RTU) feature included in the AppxK9 license.

  – For Cisco IOS Version 15.4(1)T and later, Cisco WAAS Express is a Right To Use (RTU) feature that is included in the default license that is delivered with the router; no specific license needs to be installed.
- Regardless of the specific Cisco IOS version used, you must purchase the Cisco WAAS Express feature license.

Note If you are upgrading the Cisco WAAS Express devices to Cisco IOS Version 15.3(3)Mn, as part of the new Appxk9 license support in Cisco WAAS Express IOS 15.3(3)M, you need to upgrade the Cisco WAAS Central Manager to Cisco WAAS Version 5.3.1 or later. or else the devices will go off offline.

Adding a Cisco WAAS Software License from the Cisco WAAS Central Manager

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

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

Do not choose a Cisco WAAS Central Manager device to add a license, because you must use the Cisco WAAS CLI to manage licenses on Cisco WAAS 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**.

Adding and Managing Cisco WAAS Software Licenses from the Cisco WAAS CLI

Consider the following guidelines to add, remove, manage, or display Cisco WAAS software licenses:

- To add licenses from the CLI, run the **license add** EXEC command.
- To remove licenses from the CLI, run the **clear license** EXEC command.

- To display the status of all licenses from the CLI, run the **show license** EXEC command.
- To display the smart license status, run the **show license tech-support** EXEC command.
- You can also use the Cisco WAAS setup utility for basic Cisco WAE configuration when you set up a new Cisco WAAS device. Note that the Setup utility is only used for a new installation, because the running configuration of the existing system would not be reflected in the Setup tool).

  Consider the following recommendations, restrictions, and requirements when using the Cisco WAAS setup utility:

  – For Cisco WAAS Version 6.0 and later, the Cisco WAAS setup utility will accept IPv6 address for **Interface**, **Cisco WAAS Central Manager**, **Domain Name Server Entry** and **Network Time Protocol** settings. You can configure IPv4 only, IPv6 only or dual stack network using the Cisco WAAS setup utility.

  – The Cisco WAAS setup utility requires a minimum 25 row x 80 column terminal window for proper display (terminal length, if configured, must be 24).

  – For hyper terminal:

  - Set the emulation to **vt100**, so that all lines show up properly.

  - Set the **Input Translation** to **Shift-JIS** on the **File > Properties** menu.

  – When executing the Cisco WAAS setup utility from the Cisco WAAS CLI, disable console logging, to avoid system message flooding on the screen.

  – After a restore factory-default, we recommend that you follow the system prompt to run the Cisco WAAS setup utility.

Smart Licensing

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license, hardware and software usage trends. Smart Licensing enables you to automate time-consuming, manual licensing tasks by simplifying the three core functions of purchasing, managing and reporting of licenses. Smart Licensing on the device works with the Cisco Smart Software Manager (CSSM), the portal that enables you to manage all of your Cisco Smart software licenses from one centralized website.

Smart Licensing is available when you upgrade your Cisco WAAS Central Manager and all other devices registered with it to release version 6.4.3 and later. Table 10-2 shows the models considered for smart licensing as part of this release.

Table 10-2 Cisco Device Models Considered for Smart Licensing

Cisco WAE and WAVE Devices	Cisco ISR-WAAS	Cisco ENCS 5400-W Series	Cisco vWAAS	Cisco vCM
• OE294 • OE594 • OE694 • OE7541 • OE7571 • OE8541	• OE-ISRWAAS-200 • OE-ISRWAAS-750 • OE-ISRWAAS-1300 • OE-ISRWAAS-2500	• WAAS_ENCSW_200 • WAAS_ENCSW_750 • WAAS_ENCSW_1300 • WAAS_ENCSW_2500 • WAAS_ENCSW_6000	• vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-12000 • vWAAS-50000 • vWAAS-150000	• vCM-100 • vCM-500 • vCM-1000 • vCM-2000

Table 10-3 provides an overview of the steps you must complete to set up and enable Smart Licensing.

Table 10-3 Checklist for Configuring Smart Licensing

Task	Additional Information and Instructions
1. Create a Smart Account	Identifies the information that you need to setup before configuring Smart licenses for your WAAS devices. For more information, see Creating a Smart Account, page 10-6.
2. Enable Smart Licensing	Describes the steps to enable smart licensing for the device. For more information, see Enabling Smart License for a device, page 10-7.
3. Obtain token from Cisco Smart Software Manager (CSSM).	Describes how to obtain tokens to be used for registering your device. For more information, see Creating a New Token, page 10-7.
4. Register/de-register device with CSSM.	Describes the steps to register and de-register the device from the CSSM portal. For more information, see Enabling Smart License for a device, page 10-7.

Creating a Smart Account

A Smart Account provides a single location for all Smart License-enabled products and entitlements. It assists in speed procurement, deployment and maintenance of Cisco Software. When creating a Smart Account the submitter must have the authority to represent the requesting organization. After submitting the request goes through a brief approval.

A Virtual Account exists as a sub-account within the Smart Account. Virtual Accounts are a customer defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator(s).

The creation of a new Smart Account is a one-time event and subsequent management of users is a capability provided through the tool.

To request a Smart Account, follow these steps:

Step 1 Log into the software.cisco.com and select **Administration>Request a Smart Account**.

Step 2 Select the type of Smart Account to create. There are two options:

- Individual Smart Account requiring agreement to represent your company. By creating this Smart Account you agree to authorization to create and manage product and service entitlements, users and roles on behalf of your organization.
- Create the account on someone else's behalf.

Step 3 Provide the required domain identifier and the preferred account name.

The account request will be pending an approval of the Account Domain Identifier. A subsequent email will be sent to the requester to complete the setup process.

Adding users to a Smart Account

Smart Account user management is available in the **Administration** section of **software.cisco.com**. To add a new user to a Smart Account, follow these steps:

Step 1 Log in to software.cisco.com and choose **Manage Smart Account> Administration**.

Step 2 From the **Administration** window, choose **Users** > **New User** and provide the required email address, Cisco ID and role. Roles may be defined to manage the entire Smart Account or specific Virtual Accounts.

Step 3 Click **Continue** to complete the process.

Creating a New Token

A token is required for registering a device to the Cisco Smart Software Manager (CSSM).

To create a new token:

Step 1 Log into the CSSM, select the appropriate **Virtual Account** and in the **General** tab, select **New Token**.

Step 2 Follow the dialog to provide a name, duration and export compliance applicability before accepting the terms and responsibilities. Choose **Create Token** to continue.

Step 3 Copy the token ID. The Cisco Smart Software Manager will respond with a dialogue, indicating that the token has been copied to your clipboard

Enabling Smart License for a device

From release 6.4.3, WAAS devices support both traditional licensing and smart software licensing. Eventually all devices in WAAS will support only the smart software licensing model in which case it will be enabled by default and the product instance will start in Evaluation Mode. Evaluation Mode means that a product instance has enabled Smart Licensing (either manually or by default and has not registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite).

To enable smart license on a device for the first time, follow these steps:

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

Step 2 Choose **Admin** > **Licenses**> **Smart License.**
The Smart License Configuration window appears.

Step 3 Select **Enable Smart License** under **Smart License Registration**.

Step 4 View/Edit the **Transport Settings** to see how your device communicates with the CSSM. The Transport methods are

- Direct- The product communicates directly with Cisco's Licensing Servers. If you selected this the url is automatically populated.
- HTTP Proxy- The product communicates via a HTTP or HTTPs Proxy. Enter the **Proxy Host** and **Proxy Port** details in the respective fields and click **OK**.
- Smart Software Satellite - The product communicates via proxy via Transport Gateway or Smart Software Manager Satellite. Enter the url of the gateway and click **OK**.
  Before configuring Smart Software Satellite, ensure that the Smart Software Manager Satellite is installed and is in running state. The recommended version for the Smart Software Manager satellite is ISO 5.0.1. See, the *Smart Software Manager Satellite Installation Guide* for more information.

Step 5 Click **Submit**. The product is in **Evaluation mode** after enabling Smart Software License and you can see the **Authorization Status** reflecting the same. The evaluation mode is for 90 days. You can continue to use the product in the Evaluation mode state.

Register the device with Cisco Smart Software Manager

A functioning Smart Account is required to complete the registration process. If you do not have a smart account, you can create and account. For more information, see Creating a Smart Account, page 10-6.

Three key elements are exchanged with the Cisco Smart Software Manager (CSSM) over https during the registration process.

- Trusted Unique Identifier – This is the device ID (SUDI/SUVI/ID).
- Organizational Identifier – In a numerical format to associate product with a Smart / Virtual Account.
- Licenses consumed – Allows the CSSM to understand the license type and level of consumption

To register an unregistered device with CSSM, follow the steps:

Step 1 Ensure that you have completed steps 1-5 in Enabling Smart License for a device, page 10-7.

Step 2 A token id is required to register your device to CSSM. If you do not have a token, log into the Cisco Smart Software Manager and do the needful. For more information, see Creating a New Token, page 10-7.

Step 3 On the WAAS Central Manager GUI, enter the token id obtained earlier, in the **ID Token** field and trigger the smart license registration by selecting the **Register** action from the dropdown.

- If you are initiating a fresh device registration, the license information is updated on the CSSM > **Smart Account Name** > **Virtual Account Name** > **Inventory** > **Licenses** tab.
- If your product instance is already registered; based on the license consumption, the following status is shown:

  •Authorized- If the license is available in the Cisco Smart Account.

  •Out of Compliance - If there is no license available in the Cisco Smart Virtual Account for that particular model. After license conversion process is complete the status changes to Authorized.

Note Conversion status and wait time for next poll will be updated in Smart Agent after 1 hour and the same will be updated in WAAS Central Manager GUI. This is because the Smart Agent running on the WAAS device takes one hour to check with the CSSM portal. Please ensure not to perform any actions (re-register/reload/restart) on the device when conversion is in progress state.

Device is smart-enabled and accounted for after completion of this process. Table 10-4 shows the refreshed details of the following under the **Smart Licensing Status** after the registration is complete.

You can select the **Refresh** button to see latest device smart license status in the WAAS Central manager GUI after each **Submit** action.

Table 10-4 Smart License Status Field Details

Field	Description
Registration Status	The registration status can be Registered, Unregistered, or Registration Expired: • Registered: The product is registered. The display shows **License Registered** and the registration date. • Unregistered: Smart Software Licensing is enabled but this Product Instance is not registered with CSSM. If any licenses are in use, it will run in Evaluation Mode until the evaluation period expires. • Registration Expired: Indicates that the device has been unable to communicate with the Cisco Smart Software Manager for an extended period of time. The device will attempt to contact the CSSM six months once in order to renew the ID certificate. If the Agent cannot communicate with the Cisco Smart Software Manager it will continue to try and renew the ID certificate until the expiration date (one year). Typically after one year this state will be present if failed to renew ID certificate.
Authorization Status	The Smart License authorization status can be Unconfigured, Unidentified, Evaluation Mode, Authorized, Out-of-Compliance, or Authorization Expired: • Unconfigured: Smart Software Licensing has not been configured. • Unidentified: Smart Software Licensing has been enabled but the registration has not taken place. • Evaluation Mode: Product is not registered with CSSM. If any licenses are in use, they are in Evaluation Mode and will run till the Evaluation period expires. • Authorized: Registration has been completed with a valid Smart Account and license consumption has begun.This is an indication of being in compliance. • Out-Of-Compliance: The virtual account containing your product instance has a license shortage for this type. You must buy additional licenses. • Authorization Expired: The device has been unable to communicate with the Cisco Smart Software Manager for an extended period of time. Typically after ninety days this state will be present. The device will attempt to contact the CSSM every hour in order to renew the authorization until the registration period expires.
Smart Account	A collection of virtual accounts that is accessible for you.
Virtual Account	A collection of licenses and product instances.
Product Instance	Unique Device Identifier used to identify an individual device registered with CSSM using a product instance registration token.
Transport Settings	Communication method with CSSM.

Step 4 In the case of **Registration** or **Authorization** failure: After viewing the failure message in the Cisco WAAS Central Manager GUI, use the **Force Register** button to register the product (in case there is an issue with the registration).

Step 5 Table 10-5 shows the actions you can choose to initiate after the device is in **Registered** state.

Table 10-5 Registered State Actions

Action	Description
Renew ID Certificate	Smart Software Licensing registration certificate is renewed automatically by the agent every six months, so you may not need to use the **Renew ID Certificate** option in the page-level actions menu. • If you want to manually renew the Smart Software Licensing registration certificate, selecting the option that displays a progress dialog box as the product attempts to contact the Smart Software Manager or satellite. • After initiated, the operation runs in the background.
Renew Authorization	License authorization is renewed automatically by the agent every thirty days, so you may not need to use the **Renew Authorization** option in the page-level actions menu. • If you want to manually renew license authorization, selecting the option that displays a progress dialog box as the product attempts to contact the Smart Software Manager or satellite. • After initiated, the operation runs in the background.
Deregister	**Product Instance** no longer appears in the Smart Software Manager and the licenses being used will be made available (for use) to other products in the **Virtual Account**.
Disable	Disables the smart licensing for this product and de-registers from CSSM or satellite.

Step 6 You can choose to disable or de-register the device from CSSM. by selecting the **Deregister/Disable** option from the **Action** drop-down list and click **Submit**. This will release the license from CSSM portal after successful deregistration.

After each action the details under the **Smart Licensing Status** are updated.

Periodic synchronization between Cisco WAAS and CSSM every 24 hrs, ensures that the Smart Licensing status for the devices is up to date and in sync with the CSSM.

Note You can monitor the smart license logs in the **smart-license.log** file under **errorlog**.

To display the smart license status, run the **show license tech-support** EXEC command.

EnablingFTP Services

File Transfer Protocol (FTP) 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, FTP 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. FTP copies files between devices.

FTP 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. FTP service can be enabled on Cisco WAAS devices that use Cisco WAAS software.

To enableFTP services on a Cisco WAAS device, follow these steps:

Note For the FTP transfer to be successful, configure a Pass-Through policy for the FTP server. If an Optimized policy is configured for the FTP server, the FTP transfer will fail.

Step 1 From the Cisco 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 FTP** check box to enable Inetd FTP services. By default, this option is disabled.

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

Step 4 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. The **Warning** dialog box appears only 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 Cisco WAAS network devices and contains the following topics:

Configuring NTP Settings

The Cisco 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 Cisco WAAS network, which is important for proper system operation and monitoring. On each Cisco 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 Cisco 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.This field now accepts IPv6 addresses.

Step 4 Click **Submit**.

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 an 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 Cisco 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 **Standard Timezone** drop-down list, choose a location for the time zone. (For an explanation of the abbreviations in this list, see Table 10-6.)

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 10-7.

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, from the first drop-down list choose the plus sign (**+**) or minus sign (**–**) sign to specify whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (**0** to **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 This step shows how to configure two types of customized summer time, Absolute Summer Time and Recurring Summer Time.

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

Configuring Absolute Summer Time

a. From the **Customized Summer Time Savings** section, 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** to **31**), and year (**1993** to **2032**) on which summer time must start and end, in the **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.

Configuring Recurring Summer Time

a. From the **Customized Summer Time Savings** section, click the **Recurring Dates** radio button.

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

c. From the **Start Week** drop-down list, choose an option to set the starting week (**first**, **2nd**, **3rd**, or **last**).

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.

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

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

f. From the **End Week** drop-down list, choose an option to set the ending week (**first**, **2nd**, **3rd**, or **last**).

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.

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

Step 6 **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 time and end time are set to **00:00**.

To configure start time and end time:

a. From the **Start Time** drop-down lists, choose the hour (**0** to **23**) and minute (**0** to **59**) at which daylight saving time should start.

b. From the **End Time** drop-down lists, choose the hour (**0** to **23**) and minute (**0** to **59**) at which daylight saving time should end.

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

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 10-6 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
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

Table 10-6 Timezone Location Abbreviations (continued)

Time Zone	Expansion
ROK	Republic of Korea
UCT	Coordinated Universal Time
UTC	Coordinated Universal Time
WET	Western European Time
W-SU	Middle European Time

Table 10-7 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
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

Table 10-7 Timezone—Offset from UTC (continued)

Time Zone	Offset from UTC (in hours)
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
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 Encryption Settings

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

This section contains the following topics:

About Secure Store Encryption

With Secure Store encryption on the Cisco WAAS Central Manager or a Cisco WAE device, the Cisco 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 Cisco WAAS system, user login passwords and certificate key files.

Secure Store encryption on the Cisco WAAS 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 Cisco WAAS system uses the key encryption key to encrypt and store other keys generated on the Cisco WAAS Central Manager or Cisco WAE devices. These other keys are used for Cisco WAAS functions including disk encryption, SSL acceleration, or to encrypt user passwords.

Data on the Cisco WAAS 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 pseudo random number generator.

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

- Auto-generated passphrase mode: The passphrase is automatically generated by the Cisco WAAS Central Manager and used to open the Secure Store after each system reboot. This is the default mode for new Cisco WAAS 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 Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1, with Secure Store initialized, are configured in this mode after upgrading to Cisco WAAS Version 4.4.1 or later.

To implement Secure Store your system must meet the following requirements:

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

To implement strong Secure Store encryption, follow these steps:

Step 1 Enable strong storage encryption on your primary Cisco WAAS Central Manager. See Enabling Secure Store Encryption on the Cisco WAAS Central Manager, page 10-19.

Step 2 Enable strong storage encryption on any standby Cisco WAAS Central Managers. See Enabling Secure Store Encryption on a Standby Central Manager, page 10-20.

Step 3 Enable strong storage encryption on Cisco WAE devices or Cisco WAE device groups. See Enabling Secure Store Encryption on a Cisco WAE Device, page 10-21. (Secure Store must be enabled on the Cisco WAAS Central Manager before you enable it on the Cisco WAE devices.)

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

Note When you reboot the Cisco 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 (such as disk encryption, SSL acceleration, or AAA) on the remote Cisco WAE devices do not operate properly until you enter the Secure Store password on the Cisco WAAS Central Manager to open Secure Store encryption.

Note the following considerations regarding the Secure Store:

- Passwords stored in the Cisco WAAS Central Manager database are encrypted using strong encryption techniques.
- Certificate key files are encrypted using the strong encryption key on the Cisco WAAS Central Manager.
- If a primary Cisco WAAS Central Manager fails, Secure Store key management is handled by the standby Cisco WAAS Central Manager. (Secure Store mode must be enabled manually on the standby Cisco WAAS 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 Cisco WAAS 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 Cisco WAE device, the system initializes and retrieves a new encryption key from the Cisco WAAS Central Manager. The Cisco WAE uses this key to encrypt data credentials and information on the disk (if disk encryption is also enabled).
- When you reboot the Cisco WAE after enabling Secure Store, the Cisco WAE retrieves the key from the Cisco WAAS Central Manager automatically, allowing normal access to the data that is stored in Cisco 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 Cisco WAE rejects configuration updates from the Cisco WAAS Central Manager if the updates contain dynamic share, or user configuration. Also, the Cisco WAE does not include preposition configuration in the updates that it sends to the Cisco WAAS 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.

Enabling Secure Store Encryption on the Cisco WAAS Central Manager

Secure Store is enabled by default on a new Cisco WAAS 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 Cisco WAAS 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 Cisco WAAS Central Manager, follow these steps:

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

Step 2 At the **Open Secure Store** area, enter the Secure Store passphrase in the **Current passphrase** field.

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 Cisco WAAS CLI, run the **cms secure-store open** EXEC command.

Note Whenever you reboot a Cisco WAAS Central Manager that is configured in user-provided passphrase mode, you must reopen the Secure Store manually. All services that use the Secure Store (such as disk encryption, SSL acceleration, or AAA) on the remote Cisco WAE devices do not operate properly until you enter the Secure Store password on the Cisco WAAS 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 Cisco WAAS Central Manager in user-provided passphrase mode, you should also enable Secure Store on the standby Cisco WAAS Central Manager. See Enabling Secure Store Encryption on a Standby Central Manager, page 10-20.

To check the status of the Secure Store encryption, run the **show cms secure-store** command.

Enabling Secure Store Encryption on a Standby Central Manager

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

The Secure Store passphrase mode on the primary Cisco WAAS Central Manager is replicated to the standby Cisco WAAS Central Manager (within the standard replication time). If the primary Cisco WAAS Central Manager is switched to auto-generated passphrase mode, the standby Cisco WAAS Central Manager Secure Store changes to the Open state. If the primary Cisco WAAS Central Manager is switched to user-provided passphrase mode or the passphrase is changed, the standby Cisco WAAS 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 Cisco WAAS Central Manager.

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

Step 1 Enable Secure Store encryption on the primary Cisco WAAS Central Manager. See Enabling Secure Store Encryption on the Cisco WAAS Central Manager, page 10-19.

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

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

Step 3 Enter the **cms secure-store open** EXEC command on the standby Cisco WAAS Central Manager to activate Secure Store encryption.

The standby Cisco WAAS Central Manager responds with the **Please enter pass phrase** message.

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

The standby Cisco WAAS Central Manager encrypts the data using Secure Store encryption.

Note Repeat Step 3 and Step 4 for each standby Cisco WAAS Central Manager on your system.

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

Enabling Secure Store Encryption on a Cisco WAE Device

To enable Secure Store encryption on a Cisco WAE device, follow these steps:

Step 1 From the Cisco 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 Cisco WAE devices in a device group. Either all Cisco WAE devices in the group must have Secure Store enabled, or all must have Secure Store disabled. Before you add a Cisco WAE device to a device group, set its Secure Store status to match the others. See Working with Device Groups, page 3-2 in the chapter "Using Device Groups and Device Locations".

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** check box will be checked automatically.)

Step 4 Click **Submit** to activate Secure Store encryption.

A new encryption key is initialized on the Cisco WAAS Central Manager, and the Cisco WAE encrypts the data using Secure Store encryption.

To enable Secure Store from the Cisco WAAS CLI, run the **cms secure-store init** EXEC command.

Note If you have made any other Cisco WAAS CLI configuration changes on a Cisco WAE within the datafeed poll rate time interval (five minutes by default) before executing the **cms secure-store** EXEC 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 Cisco WAE devices simultaneously. When you view the Cisco WAE devices be sure to give the Cisco WAAS Central Manager enough time to update the status of each Cisco WAE device.

Changing Secure Store Passphrase Mode

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

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

Step 1 From the Cisco 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 passphrase mode to user-provided passphrase mode, follow these steps:

Step 1 From the Cisco 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:

- A length of 8 to 64 characters
- 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 Cisco WAAS Central Manager, you must manually open its Secure Store (see Enabling Secure Store Encryption on a Standby Central Manager, page 10-20).

To change Secure Store passphrase mode from the Cisco WAAS CLI, run the **cms secure-store mode** EXEC command.

Note When you reboot a Cisco WAAS Central Manager that is configured in user-provided passphrase mode, you must reopen the Secure Store manually. All services that use the Secure Store (such as disk encryption, SSL acceleration, or AAA) on the remote Cisco WAE devices do not operate properly until you enter the Secure Store password on the Cisco WAAS 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 Cisco WAAS Central Manager to generate the encryption key for the encrypted data. If the Cisco WAAS 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 Cisco WAAS Central Manager, follow these steps:

Step 1 From the Cisco 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:

- A length of 8 to 64 characters
- 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 Cisco WAAS device reencrypts the stored data using a new encryption key derived from the new password.

Note There may be a delay of a few minutes after you click the **Change** button before the changes take effect.

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

To generate a new encryption key for a Cisco WAE device from the Cisco WAAS Central Manager, follow these steps:

Step 1 From the Cisco 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 Cisco WAAS Central Manager. The Cisco WAAS Central Manager replaces the encryption key in the Cisco WAE with the new key. The Cisco WAE re-encrypts the stored data using the new encryption key.

Note There may be a delay of a few minutes after you click the **Submit** button before the changes take effect.

To configure the Secure Store encryption key from the Cisco WAAS CLI, run the **cms secure-store change** EXEC command.

Resetting Secure Store Encryption on a Cisco WAAS Central Manager

You can reset the Secure Store if you reload the Cisco WAAS 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 Cisco WAAS Central Manager, follow these steps:

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

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

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

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

Step 4 From the primary Cisco WAAS Central Manager, reset all user account passwords.

For information on resetting user passwords, see Changing the Password for Another Account, page 8-8 in the chapter "Creating and Managing Administrator User Accounts and Groups".

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

a. If Secure Store is initialized and open, from the Cisco WAAS Central Manager, clear Secure Store (see Disabling Secure Store Encryption on a Cisco WAE Device, page 10-24). Or, from the Cisco WAAS CLI, enter the **cms secure-store clear** EXEC command.

b. From the Cisco WAAS Central Manager, initialize Secure Store (see Enabling Secure Store Encryption on a Cisco WAE Device, page 10-21) or from the Cisco WAAS 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** EXEC command and restart the SSL accelerator.

d. If disk encryption is enabled, from the Cisco WAAS Central Manager, disable disk encryption from the Cisco WAAS CLI, enter the **no disk encrypt enable** global configuration command.

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

Note If the Cisco 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 Cisco WAE to factory defaults.

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

Disabling Secure Store Encryption on a Cisco WAE Device

To disable Secure Store encryption on a Cisco WAE device, follow these steps:

Step 1 From the Cisco 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** EXEC command to disable Secure Store encryption and return to standard encryption.

Consider the following when you disable Secure Store in the Cisco WAAS Central Manager or with the **cms secure-store clear** EXEC command:

- There may be a delay of a few minutes for the changes to take effect, after you either click **Submit** at the **Secure Store Settings** window, or enter the **cms secure-store clear** EXEC command at the Cisco WAAS CLI.
- 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 Microsoft Windows domain user account identity configuration from the device or device group before you can clear Secure Store.
- You cannot clear Secure Store on a device that contains an encrypted services user account domain identity. For more information on user account domain identities, see Configuring Encrypted MAPI Acceleration, page 12-17 in the chapter "Configuring Application Acceleration".
- To disable Secure Store on a Cisco WAE from the Cisco WAAS CLI, run the **cms secure-store clear** EXEC command.
- Secure Store cannot be disabled on a Cisco WAAS Central Manager.

Modifying the Default System Properties

This section contains the following topics:

About Default System Properties

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

The following list describes the default system properties that you can modify.

- **cdm.remoteuser.deletionDaysLimit**

  Maximum number of days since their last login after which external users will be deleted from the Cisco 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 Cisco 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 Cisco 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.clusterStatus.collectRate**

  The rate (in seconds) at which AppNav Controller collects and sends **Cluster status** to the Cisco WAAS Central Manager from the AppNav IOM. The default is **30 seconds**.

- **System.datafeed.pollRate**

  Poll rate between a Cisco WAAS (or Cisco WAAS Express) device and the Cisco 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 Cisco 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.IOS.clusterStatus.collectRate**

  The rate (in seconds) at which the Cisco WAAS Central Manager collects **Cluster Status** data from Cisco IOS Routers.

- **System.IOS.clusterTopologyView.collectRate**

  The rate (in seconds) at which the Cisco WAAS Central Manager collects **Cluster Status** data from Cisco IOS Routers for **Cluster Topology view**.

- **System.lcm.enable**

  This setting controls propagation of device CLI configuration changes back to the Cisco WAAS Central Manager. If disabled, configuration changes done in the device's CLI will not be communicated to the Cisco WAAS Central Manager. This setting is system wide and applies to all managed Cisco WAAS devices. Note that disabling this setting may result in Cisco WAAS Central Manager and Cisco WAAS device(s) configuration to go out of sync.

  To customize this setting for a specific device, choose **Device > Admin > Config Synchronization UI** page.

- **System.pcm.enable**

  This setting controls whether Cisco WAAS devices accept or ignore configuration changes received from the Cisco WAAS Central Manager. It could be used in deployments where Cisco WAAS devices are not managed by Cisco WAAS Central Manager but other entity (that is, directly via the Cisco WAAS CLI). Note that disabling this setting may result in Cisco WAAS Central Manager and Cisco WAAS device(s) configuration to go out of sync.

  To customize this setting for a specific device, choose **Device > Admin > Config Synchronization UI** page.

- **System.monitoring.collectRate**

  Rate at which a Cisco WAE collects and sends the monitoring report to the Cisco WAAS Central Manager (in seconds). For a Cisco WAAS Express device, this is the rate at which the Cisco WAAS Central Manager collects the monitoring data from the Cisco WAAS Express device. The default is **300 seconds (5 minutes)**. Reducing this interval impacts the performance of the Cisco WAAS Central Manager device.

- **System.monitoring.dailyConsolidationHour**

Hour at which the Cisco WAAS Central Manager consolidates hourly and daily monitoring records. The default is **1 (1:00 a.m.)**.

- **System.monitoring.enable**

  Cisco WAAS and Cisco WAAS Express statistics monitoring (enable or disable). The default is T**rue**.

- **System.monitoring.maxConsecutiveRpcErrorWaitCount**

  Maximum number of RPC failures after which statistics from Cisco WAE to Cisco WAAS Central Manager will not be transmitted.

- **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 Cisco WAAS Central Manager consolidates daily monitoring records into monthly records. If this setting is set to **1**, the Cisco 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 Cisco 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.monthlyConsolidationFrequency**is set to 14, then the Cisco 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 Cisco 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**.

- **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.rpc.timeout.syncGuiOperation**

  Timeout in seconds for the GUI synchronization operations for the Cisco WAAS Central Manager to the Cisco WAE connection. The default is **50 seconds**.

- **System.security.maxSimultaneousLogins**

  Maximum number of concurrent Cisco 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 is exceeded for that user, there is no way for that user to regain access to the Cisco WAAS Central Manager GUI until after the timeout expires. This setting does not affect Cisco WAAS 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 Cisco WAAS Central Manager. The range is **10** to **300 records**. 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 Cisco WAAS 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 a Cisco WAAS Central Manager user on the registered Cisco IOS device. Global or Device level or Device Group level IOS Router credential pages will be hidden if this system property is enabled.

- **System.clearedAlarm.purging.interval**

  Enables configuration of time interval for retaining alarm records. The default is **7 days** but can be configured for 365 days.

- **System.cleanUp.alarm.interval**

  Number of health monitor cycles to force a synchronization of alarm data between a Cisco WAE device and Cisco WAAS Central Manager. The default is **1 health monitor cycle**. To disable this alarm update, configure **0**.

- **System.clearedAlarm.purging.interval**

  Number of days to keep alarm email history in the table. The default is **7 days**.

Procedure to View or Modify a Default System Property

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

Step 1 From the Cisco 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 To save the settings, click **Submit**.

Configuring the Web Application Filter

Web Application Filter is a security feature that protects the Cisco 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 Cisco 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 Cisco WAAS Central Manager menu, choose **Configure > Global > System Properties**. The **Config Properties** window appears.

Note You cannot enable the Web Application Filter using the Cisco WAAS 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 To enable the **Web Application Filter** feature, choose **True** from the **Value** drop-down list.

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

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

Step 5 Log out and then back in again.

Web Application Filter 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:

Web Application Filter Input Validation

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

Any input submitted using the Cisco WAAS 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)

Web Application Filter 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 Cisco WAAS Central Manager that is suspect for XSS is shown in red on the **Device Groups > All Device Groups** window.

Configuring Faster Detection of Offline Cisco WAAS Devices

This section contains the following topics:

About Faster Detection of Offline Cisco WAAS Devices

Communication between the Cisco WAAS device and Cisco WAAS Central Manager utilizing 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 Cisco WAAS Central Manager in a Cisco WAAS network.
  - The primary WAAS Central Manager tracks the last time that it received a UDP heartbeat packet from each device. If the Cisco WAAS Central Manager has not received the specified number of UDP packets, it displays a 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 Cisco WAAS Central Manager can detect offline devices much faster.
- You can enable or disable the UDP feature, specify the interval between two UDP packets, and configure the failed heartbeat count.
  - The default for the UDP feature is disabled.
  - Heartbeat packet rate is defined as the interval between two UDP packets. Using the specified heartbeat packet rate and failed heartbeat count values, the Cisco WAAS Central Manager GUI displays the resulting offline detection time as a product of heartbeat rate and failed heartbeat count.

– If you enable the fast detection of offline devices, the Cisco 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.

Procedure for Configuring Faster Detection of Offline Cisco WAAS Devices

You can detect offline Cisco WAAS devices more quickly if you enable the fast detection of offline devices. A Cisco WAAS device is declared as offline when it has failed to contact the Cisco WAAS Central Manager for a **getUpdate** (get configuration poll) request for at least two polling periods.

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

Step 1 From the Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco WAAS Central Manager before a device is declared offline. The default is **1 UDP heartbeat packet**.

Step 5 In the **Heartbeat UDP Port** field, specify the port number using which devices will send UDP heartbeat packets to the primary Cisco 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 Cisco 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 Cisco WAAS Central Manager waits until the value displayed in the **Maximum Offline Detection Time** field is exceeded.

If the Cisco WAAS Central Manager receives the Cisco Discovery Protocol (CDP) from a device, then the Cisco 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** window in the Cisco WAAS Central Manager could result in devices temporarily appearing to be offline. After the configuration changes are propagated to the devices, they again show as **online**.

Configuring Alarm Overload Detection

Cisco 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 Cisco 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 Cisco 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 Cisco WAAS CLI.
- The Cisco 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 Cisco WAAS device comes out of the alarm overload state and begins to report the alarm counts to SNMP and the CMS.

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

To configure alarm overload detection for a Cisco WAAS device or device group, follow these steps:

Step 1 From the Cisco 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 To save the settings, click **Submit**.

To configure alarm overload detection from the Cisco WAAS CLI, run 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 more information, see Managing Reports, page 15-53 in the chapter "Monitoring Your Cisco WAAS Network".

Note The **Enable Notification for Cleared Alarms** generates emails for cleared alarms *only if* you have cleared alarms after more than 24 hours of system time. If you clear alarms at 24 hours or less of system time, emails are not triggered for cleared alarms.

The **Enable Notification for Raised Alarms** generates emails for raised alarms independent of when alarms are cleared.

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

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

This section contains the following topics:

About 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 Cisco WAAS. After IPMI over LAN is set up and enabled on Cisco WAAS, authorized users can access BMC remotely even when Cisco 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 Cisco WAAS appliance.
- Monitors the health of the Cisco 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 Cisco WAAS appliance over the IPMI session.
- Support for IPMI Serial over LAN (SoL): IPMI SoL enables a remote user to access a Cisco WAAS appliance through a serial console through an IPMI session.

IPMI over LAN and IPMI SoL features can be configured using Cisco WAAS 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 Configuring BMC for Remote Platform Management, page 10-35.

BMC Firmware Update for IPMI over LAN

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

- Cisco WAVE-294, Cisco WAVE-594, or Cisco WAVE-694: 48a
- Cisco WAVE-7541, Cisco WAVE-7571, or Cisco WAVE-8541: 26a

Cisco WAAS appliances shipped from the factory with Cisco 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 Cisco WAAS software, you must update the BMC firmware, unless it was updated previously.

To determine if you are running the correct firmware version, run the **show bmc info** EXEC 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 Cisco Wide Area Application Service (WAAS) Software 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.

Run 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** EXEC 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 Cisco 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 Cisco WAAS console baud rate of 9600 bps.

Step 4 On the Cisco 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, run 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 Cisco WAAS device. When you are done, use the ~. escape character to terminate the connection.

Managing Cisco IOS Router Devices

This section contains the following topics:

About Managing Cisco IOS Router Devices

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

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

Registering a Cisco IOS Router Device with the Cisco WAAS Central Manager

Before You Begin

Before you register a router with the WAAS Central Manager, remove all banner configurations (with keywords such as username, password, hostname), because these banner configurations interfere with the registration process, and will generate errors.

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 Select the type of IP address (IPv4 or IPv6) that the Router will use. The IPv6 option is available only when the Cisco WAAS Central Manager is configured with a valid IPv6 address.

Step 3 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.

Note Although an IOS router can have a dot (".") in the hostname, this special character is not allowed in a Cisco WAAS device hostname. If you try to import an AppNav-XE device that has a dot in the hostname, the import will fail and the following error message is displayed: `Registration failed for the device devicename ConstraintException; Invalid AppNav-XE name: X.X since name includes invalid character '.'.`

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 4 Configure the router login credentials by entering the username and password. If you need to create a user on the router, see Configuring a User, page 10-40.

Step 5 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 6 In the **Central Manager IP Address** field, enter the IP address you want the router to use for the Cisco WAAS 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 7 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 Cisco WAAS 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 Installing a License on the Router, page 10-43.

Configuring Cisco IOS Router Credentials

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

On the Cisco WAAS 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 Configuring a User, page 10-40.

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 Enabling the HTTP Secure Server on the Router, page 10-43.)

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

Step 4 Click **Submit**.

To configure credentials at the device group or individual device level, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).The **Device/ Device Group** window appears. Go to **Admin** > **Authentication** > **WAAS Express Credentials/AppNav-XE Credentials** menu item.

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 Configuring a User, page 10-40.

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 Enabling the HTTP Secure Server on the Router, page 10-43.)

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

Step 4 Click **Submit**.

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

Registering a Cisco IOS Router Using the CLI

You can also register a Cisco IOS router device with the Cisco WAAS Central Manager using the Cisco WAAS CLI by completing the steps outlined in Table 10-8. This procedure applies to Cisco IOS routers running both WAAS Express and AppNav-XE.

Table 10-8 Checklist for Registering a Cisco IOS Router Using the Cisco WAAS CLI

Task	Additional Information and Instructions
1. Configure a username and password.	The same username and password are configured on the router and the Cisco WAAS Central Manager, so the Cisco WAAS Central Manager can log in to the router for management purposes. For more information, see Configuring a User, page 10-40.
2. Import the primary Central Manager administrative server certificate into the router.	The router requires the Cisco WAAS Central Manager certificate for secure HTTPS server communication. For more information, see Importing the Cisco WAAS Central Manager Certificate, page 10-41.
3. Configure a router certificate.	The Cisco WAAS Central Manager device requests this router certificate for secure HTTPS server communication. For more information, see Configuring a Cisco IOS Router Certificate, page 10-42.
4. Enable the secure HTTP server with user authentication.	Enables the Cisco WAAS Central Manager and router to communicate. For more information, see Enabling the HTTP Secure Server on the Router, page 10-43.
5. Install a permanent WAAS software license.	Allows the Cisco WAAS software to operate on the router. For more information, see Installing a License on the Router, page 10-43.
6. Configure an NTP server.	Keeps the time synchronized between the router and the Cisco WAAS Central Manager. For more information, see Configuring an NTP Server, page 10-44.
7. Register the router with the Central Manager.	Registers the router with the Cisco WAAS Central Manager. For more information, see Registering a Router with the Cisco WAAS Central Manager, page 10-44.

The following sections describe these steps in detail.

Configuring a User

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

To configure a user, follow these steps:

Step 1 Log in to the router Cisco WAAS 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 Cisco WAAS Central Manager, configure the router credentials as described in Configuring Cisco IOS Router Credentials, page 10-38.

Step 5 Click **Submit**.

To configure an external TACACS+ user on the router, run 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, run 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 Cisco WAAS Central Manager Certificate

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

To import the certificate, follow these steps:

Step 1 Log in to the Cisco WAAS 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
FWRvYy13YWFzLWNtLmNpc2NvLmNvbTAeFw0xODA3MjQxOTMwMjNaFw0xMzA3MjMx
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 Cisco WAAS 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 Cisco WAAS Central Manager in Step 3.

Configuring a Cisco IOS Router Certificate

The router needs a certificate that is requested by the Cisco WAAS 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**, Cisco IOS regenerates the self-signed certificate upon reload and this affects the communication with the Cisco 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
```

For a Cisco AppNav XE device, if the self signed certificate is generated with key label as hostname and if you change the hostname through the Cisco WAAS Central Manager GUI or router CLI, then there is a SSL handshake failure and the device goes offline. This is because the existing certificate is a valid only with respect to the old host name and the certificate needs to be validated against the hostname with which it was generated.

- To prevent this handshake failure, whenever you change the hostname, you need to re-generate the certificate for that hostname and reimport it.
- 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 Reimporting a Cisco Router Device Certificate, page 10-45.

Enabling the HTTP Secure Server on the Router

The Cisco WAAS 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 To configure authentication for the HTTP server, use the following options.

- To configure authentication for the HTTP server for a local user, use the following command:

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

- If you are using external TACACS+ or RADIUS user authentication, configure authentication for the HTTP server with the following command:

  ```
  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 Cisco WAAS Central Manager. (See Configuring a User, page 10-40.)

Installing a License on the Router

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

To install a license on the router, 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 Cisco WAAS network. You should already have an NTP server configured for the Cisco WAAS Central Manager (see Configuring NTP Settings, page 10-12).

To configure an NTP server for the router, on the router run 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 a Router with the Cisco WAAS Central Manager

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

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

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

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

If you want to register the Cisco WAAS Express router with an IPv6 address, register it with the following commands:

```
router#waas cm-register https://[CM_IPv6_Address]:8443/wcm/register
```

For a Cisco AppNav-XE router, register with the Cisco WAAS Central Manager as follows:

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

router#appnav cm-register https://[CM_IPV6_Address]:8443/wcm/register
```

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

If a permanent Cisco 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 with the Cisco WAAS Central Manager, the Cisco WAAS 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 Cisco WAAS 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 Cisco Router Device Certificate

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

To reimport a router device certificate, follow these steps:

Step 1 From the Cisco 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 Privacy-Enhanced Mail (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 Cisco WAAS 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 Cisco WAAS Central Manager IOS User on Preregistered Cisco IOS Devices

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

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

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

Step 1 From the Cisco 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.

Step 3 Select the Router IP address type: **IPv4** or **IPv6**.

Step 4 Select the Router IP Address entry method.

Step 5 In the **IP Address(es)** field, enter the Cisco WAAS Express router IP addresses to migrate, separated by commas. The IP address, hostname and status are displayed in the **Status** table.

You can also upload a CSV file that contains a list of IP addresses to migrate:

a. To upload a list, click the **Upload File** check box.

b. Click the **Choose File** button to browse to the file.

c. Click **Open**.

Each IP address must be on a separate line.

Step 6 Click the **Update** button to create a new Cisco WAAS Central Manager IOS user on the router.

- Verify that the user creation status was successful.
- If you want to migrate additional preregistered routers, use the **Reset** button to clear data from all the fields, to enter the next configuration.

If you create a Cisco IOS WCM user, using the **Home > Admin > Security > WCM Cisco IOS User Creation Tool** by specifying the Cisco IOS username, password and enable:

1. You must manually log in to the Cisco IOS router.
2. Save the running configuration by running the **write memory** EXEC command.

Note If you do not save the running configuration and reload the device, the Cisco IOS router goes off line in the Cisco WAAS Central Manager.

Cisco WAAS, Cisco ISR-WAAS, and Cisco IOS-XE Interoperability

Consider the following operating guidelines for Cisco WAAS, Cisco ISR-WAAS, and Cisco IOS-XE Interoperability:

- ISR4321-B/K9 is not supported for ISR-WAAS installation.
- Activating Cisco ISR-WAAS after formatting the Cisco 4000 Series ISR-router bootflash

  After you format the Cisco 4000 Series ISR-router bootflash, you must reload the router to ensure a successful activation of Cisco ISR-WAAS. If you do not reload the Cisco ISR router after formatting the bootflash, you will be unable to activate Cisco ISR-WAAS. For more information on formatting the Cisco 4000 Series ISR router bootflash, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs*.

- For Cisco ISR-4321 with Cisco IOS-XE, used with Cisco WAAS Version 6.2.3c or 6.3.1

  You must complete a new OVA deployment of Cisco WAAS version 6.2.3c or 6.3.1 for this configuration to work successfully. This configuration will not automatically work after an upgrade to Cisco WAAS Version 6.2.3c or 6.3.1 from Cisco WAAS Version 5.x or 6.x.

- Using Snort with Cisco ISR-WAAS and Cisco ISR-4000 Series, with a hard disk less than or equal to 200 GB

  To ensure a successful WAAS installation of ISR-WAAS and the intrusion detection and prevention system Snort on an ISR router, you must install ISR-WAAS *before* you install Snort. If you do not follow this installation order, ISR-WAAS will not install and a disk error will be displayed.

- VRF restriction for **VirtualPortGroup31** on Cisco ISR-WAAS

  When you configure Cisco ISR-WAAS with EZConfig: **VirtualPortGroup31**, the Cisco WAAS service and router interface, is automatically created, and you can then add or modify specific parameters for it.

  Do *not* add Virtual Routing and Forwarding (VRF) to **VirtualPortGroup31**, because VRF causes **VirtualPortGroup31** to lose its IP address and to disable Cisco AppNav. To re-establish these, you must uninstall and reinstall CIsco ISR-WAAS without VRF.

  For more information on **VirtualPortGroup31**, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs*.

Configuring the Hostname for Cisco ISR-WAAS

This section contains the following topics:

About Cisco ISR-WAAS and Cisco ISR-WAAS Hostname

For Cisco WAAS Version 5.5.5 and later, you can configure the Cisco ISR-WAAS hostname. For Cisco WAAS versions earlier than Cisco WAAS Version 5.5.1, Cisco ISR-WAAS receives a system-generated hostname from the Cisco ISR router, which cannot be edited.

Cisco ISR-WAAS is the specific implementation of Cisco vWAAS running in a Cisco IOS-XE Software container (the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router). Table 10-9 shows the Cisco ISR-WAAS models supported for vWAAS.

Table 10-9 Cisco ISR-WAAS Models Supported for vWAAS

Cisco vWAAS Model	Cisco vWAAS Model Memory	Supported Cisco ISR-WAAS Model	Cisco WAAS Version Supported
ISR-WAAS-200	3 GB	ISR-4321	5.2.1 and later
	4 GB	ISR-4321	6.2.3 and later

Cisco vWAAS Model	Cisco vWAAS Model Memory	Supported Cisco ISR-WAAS Model	Cisco WAAS Version Supported
ISR-WAAS-750	4 GB	ISR-4351	5.2.1 and later
		ISR-4331	
		ISR-4431	
		ISR-4451	
		ISR-4461	6.4.1b and later
ISR-WAAS-1300	6 GB	ISR-4431	5.2.1 and later
		ISR-4451	
		ISR-4461	6.4.1b and later
ISR-WAAS-2500	8 GB	ISR-4451	5.2.1 and later
		ISR-4461	6.4.1b and later

Consider the following guidelines for the Cisco ISR-WAAS hostname:

- The Cisco ISR-WAAS hostname is independent of the Cisco ISR router hostname. Changing the Cisco ISR router hostname does not change the Cisco ISR-WAAS hostname.
- Hostname configuration is not supported on the Cisco ISR-WAAS device when it is downgraded from Cisco WAAS Version 6.x to a Cisco WAAS version earlier than Cisco WAAS Version 5.5.5.
- Each Cisco ISR-WAAS image is shipped with multiple profiles; each profile dictates the resources used by the Cisco ISR-WAAS virtual instance and the number of connections supported. The default is the profile with the highest number of connections; you can select the profile that meets the requirements of your system.

Note To change the Cisco ISR-WAAS profile of an active Cisco ISR-WAAS, you must first uninstall and then reinstall the Cisco ISR-WAAS.

If you only deactivate the existing Cisco ISR-WAAS instance and then change the Cisco ISR-WAAS profile, the Cisco ISR-WAAS will become unstable and the TFO limit will show **Zero** on the Cisco ISR-WAAS console.

Note For information on how to deploy and register a Cisco ISR-WAAS on the Cisco ISR-4451-X, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco ISR-4451-X*.

Configuring a Cisco ISR-WAAS Hostname with the Cisco WAAS Central Manager

To configure the Cisco ISR-WAAS hostname with the Cisco WAAS Central Manager, follow these steps:

Step 1 Verify that the Cisco ISR-WAAS device is online by choosing **Devices** > *device-name*.

The **Device Dashboard** window appears, and displays information including device status: **Pending**, **Installed**, **Online**, or **Inactive**.

Note During a fresh OVA deployment of a Cisco ISR-WAAS instance, the Cisco ISR-WAAS default hostname is *router-name* **isr-waas**. After the hostname is changed on the **vwaas** instance, the **vwaas** instance does not get an update from the router until you change it in the **vwaas** instance with the Cisco WAAS CLI **no-hostname** command.

Step 2 To change the Cisco ISR WAAS hostname, choose **Devices > ISR WAAS Device > Activation**.

The **Device Activation** window appears, with fields for editing properties of the selected device. The **Name** field initially has the default Cisco ISR-WAAS hostname, *router-hostname*-**isr-waas**.

Step 3 In the **Name** field of the **Activation** window, enter the new name of the Cisco ISR-WAAS hostname.

Enter a maximum of 30 alphanumeric characters, including a hyphen. The hostname is case sensitive. Special characters such as $, #, or * are not allowed.

Step 4 Click **Submit**.

Step 5 To verify that the new hostname is saved, click the Cisco WAAS CLI **show hosts** command.

Configuring the Cisco ISR-WAAS Hostname with the Cisco Router CLI

To configure the hostname for a Cisco ISR-WAAS using the Cisco ISRO router CLI, follow these steps:

Step 1 To verify that the to verify that the Cisco ISR-WAAS device is online, run the router CLI command **show virtual-service list**. The **show virtual-service list** command displays the status for each device, as shown in Figure 10-1. Possible states are I**nitializing**, **Installing**, **Installed**, **Install Failed**, **Activating**, **Activated**, **Activated Failed**, **Deactivating**, **Deactivated**, and **Error**.

Figure 10-1 Sample Output for show virtual-service list Command

```
router# show virtual-service list

Virtual Service List:
Name               Status                              Package Name
------------------------------------------------------------------------------
multiova           Activated                           multiova-working.ova
WAAS               Installed                           ISR4451X-WAAS-5.5.5...
```

Step 2 Log in to the Cisco ISR-WAAS device.

Step 3 Enter **Configuration** mode and run the router global configuration command **hostname** *hostname* to specify a new hostname.

Enter a maximum of 30 alphanumeric characters, including a hyphen. Special characters such as $, #, or * are not allowed.

```
Router# config
Router (config)# hostname isr-waas-rs4a
```

Step 4 To verify that the new Cisco ISR-WAAS hostname has been saved, run the **show hosts** command.

Resetting a Cisco ISR-WAAS Hostname

To reset a Cisco ISR-WAAS hostname, run the **restore factory default** command.

Consider the different results generated by the **restore factory default** command and its parameters:

- To reset the Cisco ISR-WAAS hostname to its factory default (**-IRS-WAAS**): Run the **restore factory-default** command. This version of the command resets the entire device configuration and all data back to the manufacture factory status.
- To retain the Cisco ISR-WAAS hostname but reset other parts of the device configuration and data: Run the **restore factory-default preserve basic-config** command.

  The **restore factory-default preserve basic-config** version of the command resets all device configuration and all data back to the manufacture factory status but preserves the Cisco ISR-WAAS hostname, as well as domain name, name server, and network interfaces.

For more information on using the **restore factory-default** command, see the *Cisco Wide Area Application Services Command Reference Guide*.