CHAPTER 17

Configuring SNMP Monitoring

This chapter describes how to configure SNMP traps, recipients, community strings and group associations, user security model groups, and user access permissions.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances, WAE Network Modules (the NME-WAE family of devices), and SM-SRE modules running WAAS.

This chapter contains the following sections:

About SNMP

Simple Network Management Protocol (SNMP) is an interoperable standards-based protocol that allows for external monitoring of WAAS devices through an SNMP agent.

An SNMP-managed network consists of the following primary components:

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers. Each WAAS device running the WAAS software has an SNMP agent.

- SNMP agent—A software module that resides on a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the Management Information Base (MIB), which is the repository for information about device parameters and network data. The agent can also send traps, or notification of certain events, to the management system.
- Management station—Also known as the SNMP host, the management station uses SNMP to send the agent an SNMP Get request to obtain information from the WAAS device. The managed devices then collect and store management information and use SNMP to make this information available to the management station.

Before you can access this SNMP information, you must have deployed an SNMP management application on a management station. This SNMP management station is referred to as the SNMP host because it uses SNMP to send the device agent an SNMP Get request to obtain information from the WAAS device.

This section contains the following topics:

SNMP Communication Process

The SNMP management station and the SNMP agent that resides on a WAAS device use SNMP to communicate as follows:

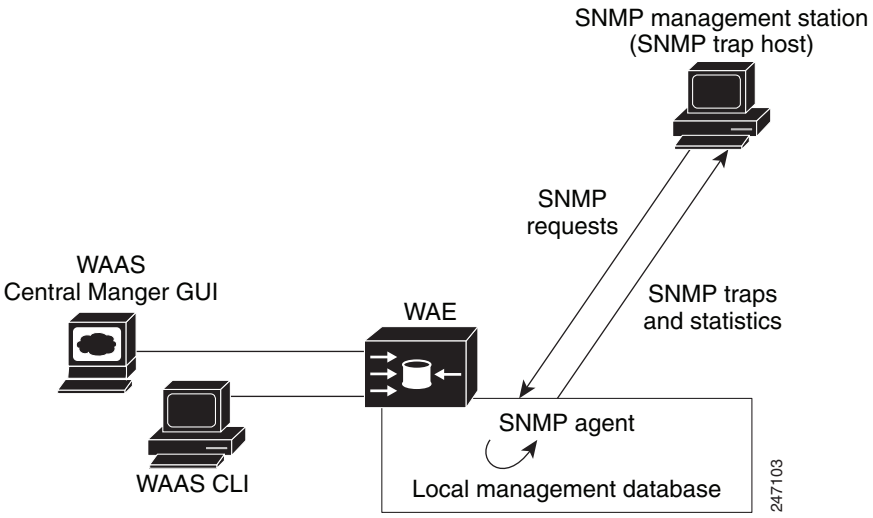
1. The SNMP management station (the SNMP host) uses SNMP to request information from the WAAS device.
2. After receiving these SNMP requests, the SNMP agent on the WAAS device accesses a table that contains information about the individual device. This table, or database, is called a Management Information Base (MIB).

   Note The SNMP agent on the WAAS device only initiates communication with the SNMP host under unusual conditions; it will initiate communication when it has a trap it needs to send to the host. For more information on this topic, see the "Enabling SNMP Traps" section on page 17-10.

3. After locating the specified information in the MIB, the agent uses SNMP to send the information to the SNMP management station.

Figure 17-1 illustrates these SNMP operations for an individual WAAS device.

Figure 17-1 SNMP Components in a WAAS Network



Supported SNMP Versions

The WAAS software supports the following versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. See the RFC 1157 for a full description of its functionality.
- Version 2 (SNMPv2c)—This is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP, defined in RFC 2271 through RFC 2275.

Each Cisco device running WAAS software contains the software necessary to communicate information about device configuration and activity using the SNMP protocol.

SNMP Security Models and Security Levels

SNMPv1 and SNMPv2c do not have any security (that is, authentication or privacy) features to keep SNMP packet traffic confidential. As a result, packets on the wire can be detected and SNMP community strings compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to WAAS devices by authenticating and encrypting packets over the network. The SNMP agent in the WAAS software supports SNMPv3 as well as SNMPv1 and SNMPv2c.

The following security features are provided in SNMPv3:

- Message integrity—Ensures that nothing has interfered with a packet during transmission.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models as well as security levels. A security model is an authentication process that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security process is used when an SNMP packet is handled. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Table 17-1 describes the combinations of security models and security levels.

Table 17-1 SNMP Security Models and Security Levels

Model	Level	Authentication	Encryption	Process
v1	noAuthNoPriv	Community string	No	Uses a community string match for user authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for user authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for user authentication.
v3	AuthNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
v3	AuthPriv	MD5 or SHA	Yes	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption (packet authentication) based on the cipher block chaining (CBC)-DES (DES-56) standard.

The SNMPv3 agent can be used in the following modes:

- noAuthNoPriv mode (that is, no security mechanisms turned on for packets)
- AuthNoPriv mode (for packets that do not need to be encrypted using the privacy algorithm [DES 56])
- AuthPriv mode (for packets that must be encrypted; privacy requires that authentication be performed on the packet)

Using SNMPv3, users can securely collect management information from their SNMP agents without worrying that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a Content Engine's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Supported MIBs

This section describes the Cisco-specific MIBs that are supported by WAAS. MIBs are listed in alphabetical order. The following Cisco-specific MIBs are supported:

- ACTONA-ACTASTOR-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-SMI

- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- MIB-II
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2-MIB
- SNMP-VACM-MIB

ACTONA-ACTASTOR-MIB

This MIB provides statistics for the CIFS transparent accelerator and statistics and log traps for the legacy mode WAFS component in WAAS. The following objects are included:

- cfIsConfigured
- cfIsAlive
- cfUpTime
- cfTotalBytesRead
- cfTotalWrittenBytes
- cfRemoteRequestCount
- cfLocalRequestCount
- cfTotalRemoteTime
- cfTotalLocalTime
- cfConnectedSessionCount
- cfCifsOpenFiles
- cfMaxCacheVolume
- cfCurrentCacheVolume
- cfMaxCacheResources
- cfCurrentCacheResources
- cfResourceEvictedNum
- cfLastEvictedTime
- cfVolHiWatermark
- cfVolLoWatermark
- cfAmntHiWatermark
- cfAmntLoWatermark
- cfEvictedAge

- cfEvictedLastAccess

CISCO-CDP-MIB

This MIB displays the ifIndex value of the local interface. For 802.3 repeaters on which the repeater ports do not have ifIndex values assigned, this value is a unique value for the port and is greater than any ifIndex value supported by the repeater. In this example, the specific port is indicated by the corresponding values of cdpInterfaceGroup and cdpInterfacePort, where these values correspond to the group number and the port number values of RFC 1516.

CISCO-CONFIG-MAN-MIB

This MIB represents a model of configuration data that exists in various locations:

- running—In use by the running system
- terminal—Saved to whatever hardware is attached as the terminal
- local—Saved locally in NVRAM or in flash memory
- remote—Saved to a server on the network

This MIB includes only operations that are specifically related to configuration, although some of the system functions can be used for general file storage and transfer.

CISCO-CONTENT-ENGINE-MIB

This is the MIB module for the Cisco WAE device from Cisco Systems, Inc. The following objects from this MIB are supported:

- cceAlarmCriticalCount
- cceAlarmMajorCount
- cceAlarmMinorCount
- cceAlarmHistTable

CISCO-ENTITY-ASSET-MIB

This MIB monitors the asset information of items in the ENTITY-MIB (RFC 2037) entPhysicalTable. This MIB lists the orderable part number, serial number, hardware revision, manufacturing assembly number and revision, firmware ID and revision (if any) and software ID and revision (if any) of relevant entities listed in ENTITY-MIB entPhysicalTable.

Entities that have none of this data available are not listed in this MIB. The table in this MIB is sparsely populated, so some variables may not exist for a particular entity at a particular time. For example, a row that represents a powered-off module may have no values for software ID (ceAssetSoftwareID) and revision (ceAssetSoftwareRevision). Similarly, a power supply would probably never have firmware or software information listed in the table.

Although the data may have other items encoded in it (for example, a manufacturing date in the serial number), consider all data items to be a single unit. Do not decompose the items or parse them. Use only string equal and unequal operations on them.

CISCO-SMI

This is the MIB module for Cisco Enterprise Structure of Management Information. There is nothing to query in this MIB; it describes the structure of Cisco MIBs.

ENTITY-MIB

This is the MIB module for representing multiple logical entities supported by a single SNMP agent. This MIB is documented in RFC 2737. The following groups from this MIB are supported:

- entityPhysicalGroup
- entityLogicalGroup

The entConfigChange notification is supported.

EVENT-MIB

This MIB defines event triggers and actions for network management purposes. The MIB is published as RFC 2981.

HOST-RESOURCES-MIB

This MIB manages host systems. The term “host” implies any computer that communicates with other similar computers connected to the Internet. The HOST-RESOURCES-MIB does not necessarily apply to devices whose primary function is communications services (terminal servers, routers, bridges, monitoring equipment). This MIB provides attributes that are common to all Internet hosts, for example, personal computers and systems that run variants of UNIX. The following objects from this MIB are not supported:

- HrPrinterEntry
- hrSWOSIndex
- hrSWInstalledGroup

IF-MIB

This MIB supports querying for interface-related statistics including 64-bit interface counters. These counters include received and sent octets, unicast, multicast, and broadcast packets on the device interfaces. All the objects from ifXEntry are supported except for ifCounterDiscontinuityTime. This MIB is documented in RFC 2233.

MIB-II

MIB-II is the Internet Standard MIB. The MIB-II is documented in RFC 1213 and is for use with network management protocols in TCP/IP-based internets. This MIB is found in the RFC1213-MIB file in the v1 directory on the download site (other MIBs are in the v2 directory). The following objects from this MIB are not supported:

- ifInUnknownProtos
- ifOutNUcastPkts
- ipRouteAge
- TcpConnEntry group
- egpInMsgs
- egpInErrors
- egpOutMsgs
- egpOutErrors
- EgpNeighEntry group

- egpAs

SNMP-COMMUNITY-MIB

This MIB is documented in RFC 2576.

SNMP-FRAMEWORK-MIB

This MIB is documented in RFC 2571.

SNMP-NOTIFICATION-MIB

This MIB is documented in RFC 3413.

SNMP-TARGET-MIB

This MIB is documented in RFC 3413.

SNMP-USM-MIB

This MIB is documented in RFC 2574.

SNMPv2-MIB

This MIB is documented in RFC 1907. WAAS supports the following notifications from this MIB:

- coldStart
- linkUp
- linkDown
- authenticationFailure

SNMP-VACM-MIB

This MIB is documented in RFC 2575.

Downloading MIB Files

You can download the MIB files for most of the MIBS that are supported by a device that is running the WAAS software from the following Cisco FTP site:

ftp://ftp.cisco.com/pub/mibs/v2

You can download the RFC1213-MIB file (for MIB-II) from the following Cisco FTP site:

ftp://ftp.cisco.com/pub/mibs/v1

The MIB objects that are defined in each MIB are described in the MIB files at the above FTP sites and are self-explanatory.

Enabling the SNMP Agent on a WAAS Device

By default, the SNMP agent on WAAS devices is disabled and an SNMP community string is not defined. The SNMP community string is used as a password for authentication when accessing the SNMP agent on a WAAS device. To be authenticated, the Community Name field of any SNMP message sent to the WAAS device must match the SNMP community string defined on the WAAS device.

The SNMP agent on a WAAS device is enabled when you define the SNMP community string on the device. The WAAS Central Manager GUI allows you to define the SNMP community string on a device or device group.

If the SNMPv3 protocol is going to be used for SNMP requests, the next step is to define an SNMP user account that can be used to access a WAAS device through SNMP. For more information on how to create an SNMPv3 user account on a WAAS device, see the "Creating an SNMP User" section on page 17-20.

Checklist for Configuring SNMP

Table 17-2 describes the process for enabling SNMP monitoring on a WAAS device or device group.

Table 17-2 Checklist for Configuring SNMP

Task	Additional Information and Instructions
1. Prepare for SNMP monitoring.	For more information, see the "Preparing for SNMP Monitoring" section on page 17-10.
2. Select the SNMP traps that you want to enable.	The WAAS Central Manager provides a wide-range of traps that you can enable on a WAAS device or device group. For more information, see the "Enabling SNMP Traps" section on page 17-10. To define additional traps, see the "Defining SNMP Traps" section on page 17-13.
3. Specify the SNMP host that receives the SNMP traps.	Specify the SNMP host to that the WAAS device or device group should send their traps to. You can specify multiple hosts so different WAAS devices send traps to different hosts. For more information, see the "Specifying the SNMP Host" section on page 17-15.
4. Specify the SNMP community string.	Specify the SNMP community string so external users can read or write to the MIB. For more information, see the "Specifying the SNMP Community String" section on page 17-16.
5. Set up SNMP views.	To restrict an SNMP group to a specific view, you must create a view that specifies the MIB subtree that you want the group to view. For more information, see the "Creating SNMP Views" section on page 17-17.
6. Create an SNMP group.	You must set up an SNMP group if are going to create any SNMP users or want to restrict a group to view a specific MIB subtree. For more information, see the "Creating an SNMP Group" section on page 17-18.

Table 17-2 Checklist for Configuring SNMP (continued)

Task	Additional Information and Instructions
7. Create an SNMP user.	If the SNMPv3 protocol is going to be used for SNMP requests, you must create at least one SNMPv3 user account on the WAAS device in order for the WAAS device to be accessed through SNMP. For more information, see the "Creating an SNMP User" section on page 17-20.
8. Configure SNMP contact settings.	For more information, see the "Configuring SNMP Contact Settings" section on page 17-21.

Preparing for SNMP Monitoring

Before you configure your WAAS network for SNMP monitoring, complete the following preparation tasks:

- Set up the SNMP host (management station) that the WAAS devices will use to send SNMP traps.
- Determine if all your WAAS devices will be sending traps to the same host, or to different hosts. Write down the IP address or hostname of each SNMP host.
- Obtain the community string used to access the SNMP agents.
- Determine if you want to create SNMP groups so you can restrict views by group.
- Determine what additional SNMP traps you need.
- Clock synchronization between the devices in a WAAS network is important. On each WAAS device, be sure to set up a Network Time Protocol (NTP) server to keep the clocks synchronized.

Enabling SNMP Traps

To enable a WAAS device to send SNMP traps, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears depending on your selection.

Step 2 Click the **Edit** icon next to the device or device group that you want to configure SNMP traps for. The Device Dashboard window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > General Settings**. The SNMP General Settings window appears. (See Figure 17-2.) Table 17-3 describes the fields in this window.

Figure 17-2 SNMP General Settings Window

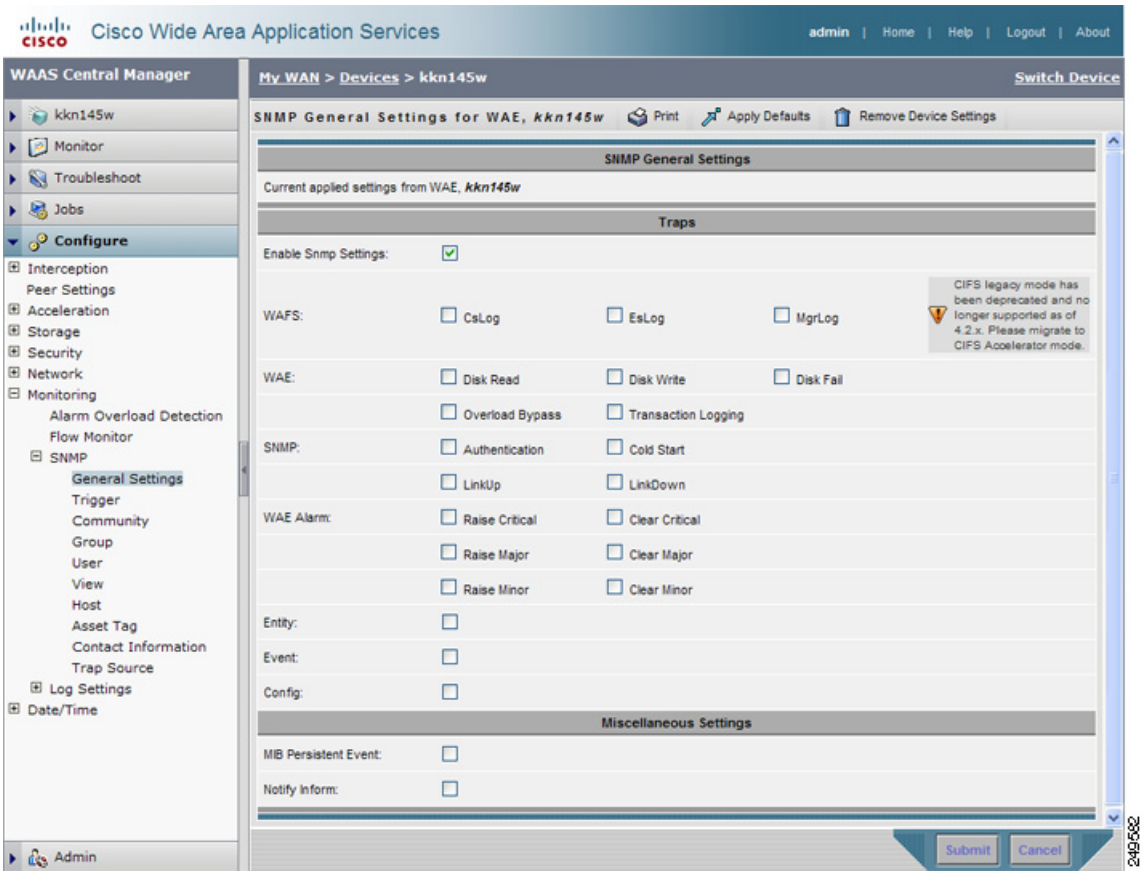


Table 17-3 SNMP General Settings

GUI Parameter	Function
Traps	
Enable Snmp Settings	Enables SNMP traps.
WAFS	Enables SNMP WAFS traps: • CsLog—Enables WAFS legacy mode Core Server error log traps. • EsLog— Enables WAFS legacy mode Edge Server error log traps. • MgrLog—Enables WAAS Central Manager error log traps.
WAE	Enables SNMP WAE traps: • Disk Read—Enables disk read error trap. • Disk Write—Enables disk write error trap. • Disk Fail—Enables disk failure error trap. • Overload Bypass—Enables WCCP overload bypass error trap. • Transaction Logging—Enables transaction log write error trap.

Table 17-3 SNMP General Settings (continued)

GUI Parameter	Function
SNMP	Enables SNMP-specific traps: • Authentication—Enables authentication trap. • Cold Start—Enables cold start trap. • LinkUp—Link up trap. • LinkDown—Link down trap.
WAE Alarm	Enables WAE alarm traps: • Raise Critical—Enables raise-critical alarm trap • Clear Critical—Enables clear-critical alarm trap • Raise Major—Enables raise-major alarm trap • Clear Major—Enables clear-major alarm trap • Raise Minor—Enables raise-minor alarm trap • Clear Minor—Enables clear-minor alarm trap
Entity	Enables SNMP entity traps.
Event	Enables the Event MIB.
Config	Enables CiscoConfigManEvent error traps.
Miscellaneous Settings	
MIB Persistent Event	Enables persistence for the SNMP Event MIB. (This check box is not shown when the selected device is a Central Manager.)
Notify Inform	Enables the SNMP notify inform request. Inform requests are more reliable than traps but consume more resources in the router and in the network. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

Step 4 Check the appropriate check boxes to enable SNMP traps.

Step 5 Click **Submit**.

A “Click Submit to Save” message appears in red next to the current settings 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 window settings by clicking **Reset**. The Reset button is visible only when you apply default or device group settings to change the current device settings but the settings have not yet been submitted.

To enable SNMP traps from the CLI, you can use the **snmp-server enable traps** global configuration command.

To control access to the SNMP agent by an external SNMP server, use the **snmp-server access-list** global configuration command to apply an SNMP ACL.

Note If you are using an SNMP server ACL, you must permit the loopback interface.

To define additional SNMP traps for other MIB objects of interest to your particular configuration, see the "Defining SNMP Traps" section on page 17-13.

Defining SNMP Traps

To define additional SNMP traps for other MIB objects of interest to your particular configuration, follow these steps to create additional SNMP triggers:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears depending on your selection.

Step 2 Click the **Edit** icon next to the device or device group that you want to define SNMP traps for. The Device Dashboard window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Trigger**. The SNMP Trigger List Entries window appears. The columns in this window are the same as the parameters described in Table 17-4.

Step 4 In the taskbar, click the **Create New SNMP Trigger List Entry** icon. The Creating New SNMP Trigger window appears. Table 17-4 describes the fields in this window.

Table 17-4 Creating New SNMP Trigger Settings

GUI Parameter	Function
MIB Name	MIB variable name of the object that you want to monitor.
Wild Card	(Optional) Check this check box if the MIB Name value is a wildcard. Note that this check box is disabled when editing the SNMP Trigger.
Frequency	Number of seconds (60–600) to wait between trigger samples.

Table 17-4 Creating New SNMP Trigger Settings (continued)

GUI Parameter	Function
Test	Test used to trigger the SNMP trap. Choose one of the following tests: • absent—A specified MIB object that was present at the last sampling is no longer present as of the current sampling. • equal—The value of the specified MIB object is equal to the specified threshold. • falling—The value of the specified MIB object has fallen below the specified threshold value. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value rises above the threshold value and then falls below the falling threshold value again. • greater-than—The value of the specified MIB object is greater than the specified threshold value. • less-than—The value of the specified MIB object is less than the specified threshold value. • on-change—The value of the specified MIB object has changed since the last sampling. • present—A specified MIB object is present as of the current sampling that was not present at the previous sampling. • rising—The value of the specified MIB object has risen above the specified threshold. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value falls below the threshold value and then rises above the rising threshold value again.
Sample Type	(Optional) Sample type, as follows: • absolute—The test is evaluated against a fixed integer value between zero and 2147483647. • delta—The test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.
Threshold Value	Threshold value of the MIB object. This field is not used if absent, on-change, or present is chosen in the Test drop-down list.
MIB Var1 MIB Var2 MIB Var3	(Optional) Names of up to three alternate MIB variables to add to the notification. Validation of these names is not supported, so be sure to enter them correctly.
Comments	Description of the trap.

Step 5 In the appropriate fields, enter the MIB name, frequency, test, sample type, threshold value, and comments.

Note You can create valid triggers only on read-write and read-only MIB objects. If you create a trigger on a read-create MIB object, it is deleted from the Central Manager configuration after one one data feed poll cycle.

Step 6 Click **Submit**.

The new SNMP trigger is listed in the SNMP Trigger List window.

You can edit an SNMP trigger by clicking the **Edit** icon next to the MIB name in the SNMP Trigger List Entries window.

You can delete an SNMP trigger by clicking the **Edit** icon next to the MIB name and then clicking the **Delete** taskbar icon.

Note If you delete any of the default SNMP triggers, they will be restored after a reload.

You can use the **snmp trigger** EXEC command to define SNMP traps from the CLI.

To control access to the SNMP agent by an external SNMP server, use the **snmp-server access-list** global configuration command to apply an SNMP ACL.

Note If you are using an SNMP server ACL, you must permit the loopback interface.

Aggregating SNMP Triggers

An individual WAE device can have custom SNMP triggers defined and can belong to device groups that have other custom SNMP triggers defined.

In the SNMP Trigger List Entries window, the Aggregate Settings radio button controls how SNMP triggers are aggregated for an individual device, as follows:

- Choose **Yes** if you want to configure the device with all custom SNMP triggers that are defined for itself and for device groups to which it belongs.
- Choose **No** if you want to limit the device to just the custom SNMP triggers that are defined for itself.

When you change the setting, you get the following confirmation message: “This option will take effect immediately and will affect the device configuration. Do you wish to continue?” Click **OK** to continue.

Specifying the SNMP Host

Hosts are listed in the order in which they have been created. The maximum number of SNMP hosts that can be created is four.

To specify the SNMP host, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to define an SNMP host. The Device Dashboard window or the Modifying Device Groups window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Host**. The SNMP Hosts window appears.

Step 4 In the taskbar, click the **Create New SNMP Host** icon. The Creating New SNMP Host window appears. Table 17-5 describes the fields in this window.

Table 17-5 SNMP Host Settings

GUI Parameter	Function
Trap Host	Hostname or IP address of the SNMP trap host that is sent in SNMP trap messages from the WAE. This is a required field.
Community/User	Name of the SNMP community or user (64 characters maximum) that is sent in SNMP trap messages from the WAE. This is a required field.
Authentication	Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list: • **No-auth**—Sends notification without any security mechanism. • **v2c**—Sends notification using Version 2c security. • **v3-auth**—Sends notification using SNMP Version 3 AuthNoPriv. • **v3-noauth**—Sends notification using SNMP Version 3 NoAuthNoPriv security. • **v3-priv**—Sends notification using SNMP Version 3 AuthPriv security.
Retry	Number of retries (1–10) allowed for the inform request. The default is 2 tries.
Timeout	Timeout for the inform request in seconds (1–1000). The default is 15 seconds.

Step 5 Enter the hostname or IP address of an SNMP trap host, SNMP community or user name, security model to send notification, and retry count and timeout for inform requests.

Step 6 Click **Submit**.

To specify the SNMP host from the CLI, you can use the **snmp-server host** global configuration command.

Specifying the SNMP Community String

An SNMP community string is the password used to access an SNMP agent that resides on WAAS devices. There are two types of community strings: group and read-write. Community strings enhance the security of your SNMP messages.

Community strings are listed in the order in which they have been created. The maximum number of SNMP communities that can be created is ten. By default, an SNMP agent is disabled, and a community string is not configured. When a community string is configured, it permits read-only access to all agents by default.

To enable the SNMP agent and configure a community string to permit access to the SNMP agent, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure an SNMP community setting.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Community**. The SNMP Community Strings window appears.

Step 4 In the taskbar, click the **Create New SNMP Community String** icon. The Creating New SNMP Community String window appears. Table 17-6 describes the fields in this window.

Table 17-6 SNMP Community Settings

GUI Parameter	Function
Community	Community string used as a password for authentication when you access the SNMP agent of the WAE. The "Community Name" field of any SNMP message sent to the WAE must match the community string defined here in order to be authenticated. Entering a community string enables the SNMP agent on the WAE. You can enter a maximum of 64 characters in this field. This is a required field.
Group name/rw	Group to which the community string belongs. The Read/Write option allows a read or write group to be associated with this community string. The Read/Write option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list: • **None**—Choose this option if you do not want to specify a group name to be associated with the community string. The Group Name field remains disabled if you select this option. • **Group**—Choose this option if you want to specify a group name. • **Read/Write**—Choose this option if you want to allow read-write access to the group associated with a community string. The Group Name field remains disabled if you select this option. This is a required field.
Group Name	Name of the group to which the community string belongs. You can enter a maximum of 64 characters in this field. This field is available only if you have chosen the Group option in the previous field.

Step 5 In the appropriate fields, enter the community string, choose whether or not read-write access to the group is allowed, and enter the group name.

Step 6 Click **Submit**.

To configure a community string from the CLI, you can use the **snmp-server community** global configuration command.

Creating SNMP Views

To restrict a group of users to view a specific MIB tree, you must create an SNMP view using the WAAS Central Manager GUI. Once you create the view, you need to create an SNMP group and SNMP users that belong to this group as described in later sections.

Views are listed in the order in which they have been created. The maximum number of views that can be created is ten.

To create a Version 2 SNMP (SNMPv2) MIB view, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to create an SNMPv2 view.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > View**. The SNMP Views window appears.

Step 4 In the taskbar, click the **Create New View** icon. The Creating New SNMP View window appears. Table 17-7 describes the fields in this window.

Table 17-7 SNMPv2 View Settings

GUI Parameter	Function
Name	String representing the name of this family of view subtrees (64 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB. This is a required field.
Family	Object identifier (64 characters maximum) that identifies a subtree of the MIB. This is a required field.
View Type	View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list: • **Included**—The MIB family is included in the view. • **Excluded**—The MIB family is excluded from the view.

Step 5 In the appropriate fields, enter the view name, the family name, and the view type.

Step 6 Click **Submit**.

Step 7 Create an SNMP group that will be assigned to this view as described in the section that follows.

To create an SNMP view from the CLI, you can use the **snmp-server view** global configuration command.

Creating an SNMP Group

You must set up an SNMP group if you are going to create any SNMP users or want to restrict a group of users to view a specific MIB subtree.

Groups are listed in the order in which they have been created. The maximum number of SNMP groups that can be created is ten.

To define a user security model group, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to create an SNMP group. The Device Dashboard or the Modifying Device Group window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Group**. The SNMP Group Strings for WAE window appears.

Step 4 In the taskbar, click the **Create New SNMP Group String** icon. The Creating New SNMP Group String for WAE window appears. Table 17-8 describes the fields in this window.

Table 17-8 SNMP Group Settings

GUI Parameter	Function
Name	Name of the SNMP group. You can enter a maximum of 64 characters. This is a required field.
Sec Model	Security model for the group. Choose one of the following options from the drop-down list: • **v1**—Version 1 security model (SNMP Version 1 [noAuthNoPriv]). • **v2c**—Version 2c security model (SNMP Version 2 [noAuthNoPriv]). • **v3-auth**—User security level SNMP Version 3 AuthNoPriv. • **v3-noauth**—User security level SNMP Version 3 noAuthNoPriv. • **v3-priv**—User security level SNMP Version 3 AuthPriv. **Note** A group defined with the SNMPv1 or SNMPv2c security model should not be associated with SNMP users; they should only be associated with the community strings.
Read View	Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. In order to provide read access to users of the group, a view must be specified. For information on creating SNMP views, see the "Creating SNMP Views" section on page 17-17.
Write View	Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined. For information on creating SNMP views, see the "Creating SNMP Views" section on page 17-17.
Notify View	Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined. For information on creating SNMP views, see the "Creating SNMP Views" section on page 17-17.

Step 5 In the appropriate fields, enter the SNMP group configuration name, the security model, and the names of the read, write, and notify views.

Step 6 Click **Submit**.

Step 7 Create SNMP users that belong to this new group as described in the section that follows.

To create an SNMP group from the CLI, you can use the **snmp-server group** global configuration command.

Creating an SNMP User

Users are listed in the order in which they have been created. The maximum number of users that can be created is ten.

To define a user who can access the SNMP engine, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to create an SNMP user.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > User**. A list of SNMP users for the device or device group appears.

Step 4 In the taskbar, click the **Create New SNMP User** icon. The Creating New SNMP User window appears. Table 17-9 describes the fields in this window.

Table 17-9 SNMP User Settings

GUI Parameter	Function
Name	String representing the name of the user (32 characters maximum) who can access the device or device group. This is a required field.
Group	Name of the group (64 characters maximum) to which the user belongs. This is a required field.
Remote SNMP ID	Globally unique identifier for a remote SNMP entity (10 to 64 characters). To send an SNMPv3 message to the WAE, at least one user with a remote SNMP ID must be configured on the WAE. The SNMP ID must be entered in octet string format. Only hexadecimal characters and the colon (:) are allowed in this field. If any colons appear in the entered string, they are removed when the page is submitted.
Authentication Algorithm	Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list: • **No-auth**—Requires no security mechanism to be turned on for SNMP packets. • **MD5**—Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm. • **SHA**—Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.
Authentication Password	String (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display. This field is optional if the **no-auth** option is chosen for the authentication algorithm. Otherwise, this field must contain a value.
Confirmation Password	Authentication password for confirmation. The reentered password must be the same as the one entered in the previous field.

Table 17-9 SNMP User Settings (continued)

GUI Parameter	Function
Private Password	String (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters is adjusted to fit the display area if it exceeds the limit for display.
Confirmation Password	Private password for confirmation. The reentered password must be the same as the one entered in the previous field.

Step 5 In the appropriate fields, enter the username, the group to which the user belongs, the engine identity of the remote entity to which the user belongs, the authentication algorithm used to protect SNMP traffic from tampering, the user authentication parameters, and the authentication parameters for the packet.

Step 6 Click **Submit**.

To create an SNMP user from the CLI, you can use the **snmp-server user** global configuration command.

Configuring SNMP Asset Tag Settings

To configure SNMP asset tag settings, which create values in the CISCO-ENTITY-ASSET-MIB, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to define an SNMP asset tag. The Device Dashboard or the Modifying Device Groups window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Asset Tag**. The SNMP Asset Tag Settings window appears.

Step 4 In the Asset Tag Name field, enter a name for the asset tag.

Step 5 Click **Submit**.

To configure SNMP asset tag settings from the CLI, you can use the **asset tag** global configuration command.

Configuring SNMP Contact Settings

To configure SNMP contact settings, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**). The Devices or Device Groups window appears.

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure an SNMP contact. The Device Dashboard or the Modifying Device Groups window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Contact Information**. The SNMP Contact Settings window appears.

Step 4 Enter a contact name and location in the provided fields.

Step 5 Click **Submit**.

To configure SNMP contact settings from the CLI, you can use the **snmp-server contact** global configuration command.

Configuring SNMP Trap Source Settings

To configure the source interface from which SNMP traps are sent, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**. The Devices window appears. (This setting is not supported from device groups.)

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure an SNMP trap source. The Device Dashboard or the Modifying Device Groups window appears.

Step 3 In the navigation pane, choose **Configure > Monitoring > SNMP > Trap Source**. The SNMP Trap Source Settings window appears.

Step 4 From the Trap Source drop-down list, choose the interface to be used as the trap source. From the available gigabit Ethernet, standby, and port channel interfaces, only those with IP addresses are shown in the list. For vWAAS devices, virtual interfaces with assigned IP addresses are shown in the list.

Note An interface assigned as a trap source cannot be removed until it is unassigned as a trap source.

Step 5 Click **Submit**.

To configure SNMP trap source settings from the CLI, you can use the **snmp-server trap-source** global configuration command.