CHAPTER 74

Configuring SNMP

This chapter describes how to configure SNMP to monitor the adaptive security appliance and includes the following sections:

- Information about SNMP, page 74-1
- Licensing Requirements for SNMP, page 74-4
- Prerequisites for SNMP, page 74-5
- Guidelines and Limitations, page 74-5
- Configuring SNMP, page 74-6
- Configuration Examples for SNMP, page 74-15
- Where to Go Next, page 74-16
- Additional References, page 74-16
- Feature History for SNMP, page 74-18

Information about SNMP

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. This section describes SNMP monitoring, and includes the following topics:

- Information About SNMP Terminology, page 74-2
- Information About MIBs and Traps, page 74-2

The adaptive security appliance provides support for network monitoring using SNMP Versions 1, 2c, and 3, and supports the use of all three versions simultaneously. The SNMP interface lets you monitor the adaptive security appliance through network management systems (NMSs), such as HP OpenView. The adaptive security appliance supports SNMP read-only access through issuance of a GET request. SNMP write access is not allowed, so you cannot make changes with SNMP. In addition, the SNMP SET request is not supported.

You can configure the adaptive security appliance to send traps, which are unsolicited comments from the managed device to the management station for certain events (event notifications) to an NMS, or you can use the NMS to browse the MIBs on the adaptive security appliance. MIBs are a collection of definitions, and the adaptive security appliance maintains a database of values for each definition. Browsing a MIB means issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the NMS to determine values.

The adaptive security appliance has an SNMP agent that notifies designated management stations if events occur that are pre-defined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, which identifies itself to the management stations. The adaptive security appliance SNMP agent also replies when a management station asks for information.

Information About SNMP Terminology

Table 74-1 lists the terms that are commonly used when working with SNMP:

Table 74-1 SNMP Terminology

Term	Description
Agent	The SNMP server running on the adaptive security appliance. The agent responds to requests for information and actions from the network management station. The agent also controls access to its Management Information Base, the collection of objects that the SNMP manager can view or change.
Browsing	Monitoring the health of a device from the network management station by polling required information from the SNMP agent on the device. This activity may include issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the network management station to determine values.
Management Information Bases (MIBs)	Standardized data structures for collecting information about packets, connections, buffers, failovers, and so on. MIBs are defined by the product, protocols ,and hardware standards used by most network devices. SNMP network management stations can browse MIBs and request specific data or events be sent as they occur. Some MIB data can be modified for administrative purposes.
Network management stations (NMSs)	The PCs or workstations set up to monitor SNMP events and manage devices, such as the adaptive security appliance.
Object identifier (OID)	The system that identifies a device to its NMS and indicates to users the source of information monitored and displayed.
Trap	Predefined events that generate a message from the SNMP agent to the NMS. Events include alarm conditions such as linkup, linkdown, coldstart, authentication, or syslog events.

Information About MIBs and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. Standard traps are compiled into the adaptive security appliance software.

If needed, you can also download RFCs, standard MIBs, and standard traps from the IETF website:

http://www.ietf.org/

Download Cisco MIBs and OIDs from the following location:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Download Cisco OIDs from the following location:

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Note In software versions 7.2(1), 8.0(2), and later, the interface information accessed via SNMP refreshes about every five seconds. As a result, we recommend that you wait for at least five seconds between consecutive polls.

SNMP Version 3

This section describes SNMP Version 3 and includes the following topics:

- SNMP Version 3 Overview, page 74-3
- Security Models, page 74-3
- SNMP Groups, page 74-4
- SNMP Users, page 74-4
- SNMP Hosts, page 74-4
- Implementation Differences Between Adaptive Security Appliances and the Cisco IOS, page 74-4

SNMP Version 3 Overview

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. In addition, this version controls access to the SNMP agent and MIB objects through the User-based Security Model (USM) and View-based Access Control Model (VACM). The ASA 5500 series adaptive security appliances also support the creation of SNMP groups and users, as well as hosts, which is required to enable transport authentication and encryption for secure SNMP communications.

Security Models

For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, which are divided into the following three types:

- NoAuthPriv—No Authentication and No Privacy, which means that no security is applied to messages.
- AuthNoPriv—Authentication but No Privacy, which means that messages are authenticated.
- AuthPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.

SNMP Groups

An SNMP group is an access control policy to which users can be added. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group must match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique.

SNMP Users

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, and AES (which is available in 128, 192, and 256 versions). When you create a user, you must associate it with an SNMP group. The user then inherits the security model of the group.

SNMP Hosts

An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMP Version 3 hosts, along with the target IP address, you must configure a username, because traps are only sent to a configured user. SNMP target IP addresses and target parameter names must be unique on the adaptive security appliance. Each SNMP host can have only one username associated with it. To receive SNMP traps, after you have added the **snmp-server host** command, make sure that you configure the user credentials on the NMS to match those configured on the adaptive security appliance.

Implementation Differences Between Adaptive Security Appliances and the Cisco IOS

The SNMP Version 3 implementation in adaptive security appliances differs from the SNMP Version 3 implementation in the Cisco IOS in the following ways:

- The local-engine and remote-engine IDs are not configurable. The local engine ID is generated when the adaptive security appliance starts or when a context is created.
- No support exists for view-based access control, which results in unrestricted MIB browsing.
- Support is restricted to the following MIBs: USM, VACM, FRAMEWORK, and TARGET.
- You must create users and groups with the correct security model.
- You must remove users, groups, and hosts in the correct sequence.
- Use of the **snmp-server host** command creates an adaptive security appliance rule to allow incoming SNMP traffic.

Licensing Requirements for SNMP

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Prerequisites for SNMP

SNMP has the following prerequisite:

You must have Cisco Works for Windows or another SNMP MIB-II compliant browser to receive SNMP traps or browse a MIB.

Guidelines and Limitations

Context Mode Guidelines

Supported in single and multiple context modes.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

Failover Guidelines

- Supported in SNMP Version 3.
- The SNMP client in each adaptive security appliance shares engine data with its peer. Engine data includes the engineID, engineBoots, and engineTime objects of the SNMP-FRAMEWORK-MIB.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

- Does not support view-based access control, but the VACM MIB is available for browsing to determine default view settings.
- Does not support SNMP Version 3 for the AIP SSM or AIP SSC.
- Does not support SNMP debugging.
- When using NET-SNMP Version 5.4.2.1, only supports the encryption algorithm version of AES128. Does not support the encryption algorithm versions of AES246 or AES192.
- For SNMP Version 3, configuration must occur in the following order: group, user, host.
- Before a group is deleted, you must ensure that all users associated with that group are deleted.
- Before a user is deleted, you must ensure that no hosts are configured that are associated with that username.
- If users have been configured to belong to a particular group with a certain security model, and if the security level of that group is changed, you must do the following in this sequence:
  - Remove the users from that group.
  - Change the group security level.
  - Add users that belong to the new group.
- The creation of custom views to restrict user access to a subset of MIB objects is not supported.
- All requests and traps are available in the default Read/Notify View *only.*

Configuring SNMP

This section describes how to configure SNMP and includes the following topics:

- Enabling SNMP, page 74-6
- Configuring SNMP Traps, page 74-7
- Compiling Cisco Syslog MIB Files, page 74-7
- Using SNMP Version 1 or 2c, page 74-9
- Using SNMP Version 3, page 74-10

Enabling SNMP

The SNMP agent that runs on the adaptive security appliance performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the SNMP server, enter the following command:

Command	Purpose
snmp-server enable **Example:** `hostname(config)# snmp-server enable`	Ensures that the SNMP server on the adaptive security appliance is enabled. By default, the SNMP server is enabled.

What to Do Next

See the "Configuring SNMP Traps" section on page 74-7.

Configuring SNMP Traps

To designate which traps the SNMP agent generates and how they are collected and sent to NMSs, enter the following command:

Detailed Steps

Command	Purpose
snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]] **Example:** `hostname(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart`	Sends individual traps, sets of traps, or all traps to the NMS. Enables syslog messages to be sent as traps to the NMS. The default configuration has all SNMP core traps enabled, as shown in the example. To disable these traps, use the **no snmp-server enable traps snmp** command. If you enter this command and do not specify a trap type, the default is the syslog trap. By default, the syslog trap is enabled. The default SNMP traps continue to be enabled with the syslog trap. To restore the default enabling of SNMP traps, use the **clear configure snmp-server** command.

What to Do Next

See the "Compiling Cisco Syslog MIB Files" section on page 74-7.

Compiling Cisco Syslog MIB Files

To receive security and failover SNMP traps from the adaptive security appliance, compile the Cisco SMI MIB and the Cisco Syslog MIB into the SNMP management application. If you do not compile the Cisco Syslog MIB into your application, you only receive traps for linkup or linkdown, coldstart, and authentication failure.

To compile Cisco Syslog MIB files into your browser using Cisco Works for Windows, perform the following steps:

Step 1 To download the Cisco MIBs, go to the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Step 2 From the Cisco Secure and VPN Products drop-down list, choose **adaptive security appliance**.

The Adaptive Security Appliance MIB Support List appears.

Step 3 Click **CISCO-SYSLOG-MIB.my**, and save the file to your desktop.

Step 4 Start CiscoWorks for Windows.

Step 5 Choose **Config > Compile MIB**.

Step 6 Scroll to the bottom of the list, and click the last entry.

Step 7 Click **Add**.

Step 8 Locate the Cisco Syslog MIB files.

Note You must manually rename any files with the .my extension to the .mib extension, because only files with the .mib extension appear in the file selection window of CiscoWorks for Windows.

Step 9 Click **CISCO-FIREWALL-MIB.mib**, and click **OK**.

Step 10 Scroll to the bottom of the list, and click the last entry.

Step 11 Click **Add**.

Step 12 Click **CISCO-MEMORY-POOL-MIB.mib**, and click **OK**.

Step 13 Scroll to the bottom of the list, and click the last entry.

Step 14 Click **Add**.

Step 15 Click **CISCO-SMI-MIB.mib**, and click **OK**.

Step 16 Scroll to the bottom of the list, and click the last entry.

Step 17 Click **Add**.

Step 18 Click **CISCO-SYSLOG-MIB.mib**, and click **OK**.

Step 19 Click **Load All**.

Step 20 If no errors occur, restart Cisco Works for Windows.

What to Do Next

Choose one of the following:

- See the "Using SNMP Version 1 or 2c" section on page 74-9.
- See the "Using SNMP Version 3" section on page 74-10.

Using SNMP Version 1 or 2c

To configure parameters for SNMP Version 1 or 2c, perform the following steps:

Detailed Steps

	Command	Purpose

Step 1	**snmp-server host** *interface* {*hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | ***2c*** *username*}] [**udp-port** *port*]
	Example:
	`hostname(config)# snmp-server host mgmt 10.7.14.90 version 2`
	`hostname(config)# snmp-server host corp 172.18.154.159 community public`
		Specifies the recipient of an SNMP notification. Indicates the interface from which traps are sent. Identifies the name and IP address of the NMS or SNMP manager that can connect to the adaptive security appliance. The **trap** keyword limits the NMS to receiving traps only. The **poll** keyword limits the NMS to sending requests (polling) only. By default, SNMP traps are enabled. By default, the UDP port is 162. The community string is a shared secret key between the adaptive security appliance and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default community-string is “public.” The adaptive security appliance uses this key to determine whether the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the adaptive security appliance and the management station with the same string. The adaptive security appliance uses the specified string and does not respond to requests with an invalid community string. For more information about SNMP hosts, see the “SNMP Hosts” section on page 74-4.
		Note To receive traps, after you have added the **snmp-server host** command, make sure that you configure the user on the NMS with the same credentials as those configured on the adaptive security appliance.

Step 2	**snmp-server community** *community-string* **Example:** `hostname(config)# snmp-server community onceuponatime`	Sets the community string, which is for use *only* with SNMP Version 1 or 2c.

Step 3	**snmp-server** [**contact** | **location**] *text*
	Example:
	`hostname(config)# snmp-server location building 42`
	`hostname(config)# snmp-server contact EmployeeA`
		Sets the SNMP server location or contact information.

What to Do Next

See the "Monitoring SNMP" section on page 74-14.

Using SNMP Version 3

To configure parameters for SNMP Version 3, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**snmp-server group** *group-name* **v3** [**auth** | **noauth** | **priv**] **Example:** hostname(config)# snmp-server group *testgroup1* v3 auth	Specifies a new SNMP group, which is for use *only* with SNMP Version 3. When a community string is configured, two additional groups with the name that matches the community string are autogenerated: one for the Version 1 security model and one for the Version 2 security model. For more information about security models, see the "Security Models" section on page 74-3. The **auth** keyword enables packet authentication. The **noauth** keyword indicates no packet authentication or encryption is being used. The **priv** keyword enables packet encryption and authentication. No default values exist for the **auth** or **priv** keywords.
Step 2	**snmp-server user** *username group-name* {**v3** [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv** [**des** | **3des** | **aes**] [**128** | **192** | **256**] *priv-password* **Example:** hostname(config)# snmp-server user *testuser1 testgroup1* v3 auth md5 *testpassword* aes 128 *mypassword* hostname(config)# snmp-server user *testuser1* public v3 encrypted auth md5 *00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF*	Configures a new user for an SNMP group, which is for use *only* with SNMP Version 3. The *username* argument is the name of the user on the host that belongs to the SNMP agent. The *group-name* argument is the name of the group to which the user belongs. The **v3** keyword specifies that the SNMP Version 3 security model should be used, and enables the use of the **encrypted, priv,** and the **auth** keywords. The **encrypted** keyword specifies the password in encrypted format. Encrypted passwords must be in hexadecimal format. The **auth** keyword specifies which authentication level (**md5** or **sha**) should be used. The **priv** keyword specifies the encryption level. No default values for the **auth** or **priv** keywords nor default passwords exist. For the encryption algorithm, you can specify either **des**, **3des**, or **aes**. You can also specify which version of the AES encryption algorithm to use: **128**, **192**, or **256**. The *auth-password* specifies the authentication user password. The *priv-password* specifies the encryption user password. **Note** If you forget a password, you cannot recover it, and must reconfigure the user. You can specify a plain-text password or a localized digest. The localized digest must match the authentication algorithm selected for the user, which can be either MD5 or SHA. When the user configuration is displayed on the console or is written to a file (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed instead of a plain-text password (see the second example). The minimum length for a password is one character; however, we recommend that you use at least eight characters for security.

	Command	Purpose

Step 3	**snmp-server host** *interface* {*hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | ***2c*** | ***3*** *username*}] [**udp-port** *port*]
	Example:
	`hostname(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1`
	`hostname(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2`
		Specifies the recipient of an SNMP notification. Indicates the interface from which traps are sent. Identifies the name and IP address of the NMS or SNMP manager that can connect to the adaptive security appliance. The **trap** keyword limits the NMS to receiving traps only. The **poll** keyword limits the NMS to sending requests (polling) only. By default, SNMP traps are enabled. By default, the UDP port is 162. The community string is a shared secret key between the adaptive security appliance and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default community-string is "public." The adaptive security appliance uses this key to determine whether the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the adaptive security appliance and the NMS with the same string. The adaptive security appliance uses the specified string and does not respond to requests with an invalid community string. For more information about SNMP hosts, see the "SNMP Hosts" section on page 74-4.
		Note When SNMP Version 3 hosts are configured on the adaptive security appliance, a user must be associated with that host. To receive traps, after you have added the **snmp-server host** command, make sure that you configure the user on the NMS with the same credentials as those configured on the adaptive security appliance.

Step 4	**snmp-server** [**contact** | **location**] *text*
	Example:
	`hostname(config)# snmp-server location building 42`
	`hostname(config)# snmp-server contact EmployeeA`
		Sets the SNMP server location or contact information.

What to Do Next

See the "Monitoring SNMP" section on page 74-14.

Troubleshooting Tips

To ensure that the SNMP process that receives incoming packets from the NMS is running, enter the following command:

```
hostname(config)# show process | grep snmp
```

To capture syslog messages from SNMP and have them appear on the adaptive security appliance console, enter the following commands:

```
hostname(config)# logging list snmp message 212001-212015
hostname(config)# logging console snmp
```

To make sure that the SNMP process is sending and receiving packets, enter the following commands:

```
hostname(config)# clear snmp-server statistics
hostname(config)# show snmp-server statistics
```

The output is based on the SNMP group of the SNMPv2-MIB.

To make sure that SNMP packets are going through the adaptive security appliance and to the SNMP process, enter the following commands:

```
hostname(config)# clear asp drop
hostname(config)# show asp drop
```

If the NMS cannot request objects successfully or is not handing incoming traps from the adaptive security appliance correctly, use a packet capture to isolate the problem, by entering the following commands:

```
hostname (config)# access-list snmp permit udp any eq snmptrap any
hostname (config)# access-list snmp permit udp any any eq snmp
hostname (config)# capture snmp type raw-data access-list snmp interface mgmt
hostname (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

If the adaptive security appliance is not performing as expected, obtain information about network topology and traffic by doing the following:

- For the NMS configuration:
  - Number of timeouts
  - Retry count
  - Engine ID caching
  - Username and password used
- Run the following commands:
  - **show block**
  - **show interface**
  - **show process**
  - **show cpu**

If a fatal error occurs, to help in reproducing the error, send a traceback file and the output of the **show tech-support** command to Cisco TAC.

If SNMP traffic is not being allowed through the adaptive security appliance interfaces, you might also need to permit ICMP traffic from the remote SNMP server using the **icmp permit** command.

For the ASA 5580, differences may appear in the physical interface statistics output and the logical interface statistics output between the **show interface** command and the **show traffic** command.

Interface Types and Examples

The interface types that produce SNMP traffic statistics include the following:

- Logical—Statistics collected by the software driver, which are a subset of physical statistics.
- Physical—Statistics collected by the hardware driver. Each physical named interface has a set of logical and physical statistics associated with it. Each physical interface may have more than one VLAN interface associated with it. VLAN interfaces only have logical statistics. For a physical interface that has multiple VLAN interfaces associated with it, be aware of the following:

Note For a physical interface that has multiple VLAN interfaces associated with it, note that SNMP counters for ifInOctets and ifOutoctets OIDs match the aggregate traffic counters for that physical interface.

- VLAN-only—SNMP uses logical statistics for ifInOctets and ifOutOctets.

The examples in Table 74-2 show the differences in SNMP traffic statistics.

Table 74-2 SNMP Traffic Statistics for Physical and VLAN Interfaces

<table>
<tr><th>Example 1</th><th>Example 2</th></tr>
<tr>
<td>

The following example shows the difference in physical and logical output statistics for the **show interface** command and the **show traffic** command:

```
hostname# show interface GigabitEthernet3/2
interface GigabitEthernet3/2
    description fullt-mgmt
    nameif mgmt
    security-level 10
    ip address 10.7.14.201 255.255.255.0
    management-only

hostname# show traffic
(Condensed output)

Physical Statistics
GigabitEthernet3/2:
    received (in 121.760 secs)
        36 packets       3428 bytes
        0 pkts/sec      28 bytes/sec

Logical Statistics
mgmt:
    received (in 117.780 secs)
        36 packets       2780 bytes
        0 pkts/sec      23 bytes/sec
```

The following examples show the SNMP output statistics for the management interface and the physical interface. The ifInOctets value is close to the physical statistics output that appears in the **show traffic** command output, but not to the logical statistics output.

ifIndex of the mgmt interface:

```
IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt'
interface
```

ifInOctets that corresponds to the physical interface statistics:

```
IF-MIB::ifInOctets.6 = Counter32:3246
```

</td>
<td>

The following example shows output statistics for a VLAN-only interface for the **show interface** command and the **show traffic** command. The example shows that the statistics are close to the output that appears for the **show traffic** command:

```
hostname# show interface GigabitEthernet0/0.100
interface GigabitEthernet0/0.100
    vlan 100
    nameif inside
    security-level 100
    ip address 47.7.1.101 255.255.255.0 standby
    47.7.1.102

hostname# show traffic
inside
    received (in 9921.450 secs)
        1977 packets       126528 bytes
        0 pkts/sec      12 bytes/sec
    transmitted (in 9921.450 secs)
        1978 packets       126556 bytes
        0 pkts/sec      12 bytes/sec
```

ifIndex of VLAN inside:

```
IF-MIB::ifDescr.9 = Adaptive Security Appliance
'inside' interface
IF-MIB::ifInOctets.9 = Counter32: 126318
```

</td>
</tr>
</table>

Monitoring SNMP

NMSs are the PCs or workstations that you set up to monitor SNMP events and manage devices, such as the adaptive security appliance.You can monitor the health of a device from an NMS by polling required information from the SNMP agent that has been set up on the device. Predefined events from the SNMP agent to the NMS generate syslog messages. This section includes the following topics:

- SNMP Syslog Messaging, page 74-14
- SNMP Monitoring Commands, page 74-14

SNMP Syslog Messaging

SNMP generates detailed syslog messages numbered 212*nnn*. Syslog messages indicate the status of SNMP requests, SNMP traps, SNMP channels, and SNMP responses from the adaptive security appliance to a specified host on a specified interface.

For detailed information about syslog messages, see *Cisco ASA 5500 Series System Log Messages*.

Note SNMP polling will fail if SNMP syslog messages exceed a high rate (approximately 4000 per second).

SNMP Monitoring Commands

To monitor SNMP, enter one of the following commands:

Command	Purpose
`show running-config [default] snmp-server`	Displays all SNMP server configuration information.
`show running-config snmp-server group`	Displays SNMP group configuration settings.
`show running-config snmp-server host`	Displays configuration settings used by SNMP to control messages and notifications sent to remote hosts.
`show running-config snmp-server user`	Displays SNMP user-based configuration settings.
`show snmp-server engineid`	Displays the ID of the SNMP engine configured.
`show snmp-server group`	Displays the names of configured SNMP groups. **Note** If the community string has already been configured, two extra groups appear by default in the output. This behavior is normal.
`show snmp-server statistics`	Displays the configured characteristics of the SNMP server. To reset all SNMP counters to zero, enter the **clear snmp-server statistics** command.
`show snmp-server user`	Displays the configured characteristics of users.

Examples

The following examples show how to display SNMP server statistics and the SNMP server running configuration:

```
hostname(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

hostname(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

Configuration Examples for SNMP

This section includes the following topics:

- Configuration Example for SNMP Versions 1 and 2c, page 74-15
- Configuration Example for SNMP Version 3, page 74-15

Configuration Example for SNMP Versions 1 and 2c

The following example shows how the adaptive security appliance can receive SNMP requests from host 192.0.2.5 on the inside interface but does not send any SNMP syslog requests to any host:

```
hostname(config)# snmp-server host 192.0.2.5
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact EmployeeA
hostname(config)# snmp-server community ohwhatakeyisthee
```

Configuration Example for SNMP Version 3

The following example show how the adaptive security appliance can receive SNMP requests using the SNMP Version 3 security model, which requires that the configuration follow this specific order: group, followed by user, followed by host:

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

Where to Go Next

To configure the syslog server, see Chapter 72, "Configuring Logging."

Additional References

For additional information related to implementing SNMP, see the following sections:

- RFCs for SNMP Version 3, page 74-16
- MIBs, page 74-16
- Application Services and Third-Party Tools, page 74-18

RFCs for SNMP Version 3

RFC	Title
3410	Introduction and Applicability Statements for Internet Standard Management Framework
3411	An Architecture for Describing SNMP Management Frameworks
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
3413	Simple Network Management Protocol (SNMP) Applications
3414	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMP)
3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

MIBs

For a list of supported MIBs and traps for the adaptive security appliance by release, see the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To obtain a list of the supported SNMP MIBs for a specific adaptive security appliance, enter the following command:

```
hostname(config)# show snmp-server oidlist
```

Note Although the **oidlist** keyword does not appear in the options list for the **show snmp-server** command help, it is available.

The following is sample output from the **show snmp-server oidlist** command:

```
[0]      1.3.6.1.2.1.1.1.        sysDescr
[1]      1.3.6.1.2.1.1.2.        sysObjectID
[2]      1.3.6.1.2.1.1.3.        sysUpTime
```

```
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
```

```
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

Application Services and Third-Party Tools

For information about SNMP support, see the following URL:

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

For information about using third-party tools to walk SNMP Version 3 MIBs, see the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

Feature History for SNMP

Table 74-3 lists each feature change and the platform release in which it was implemented.

Table 74-3 Feature History for SNMP

Feature Name	Platform Releases	Feature Information
SNMP Versions 1 and 2c	7.0(1)	Provides adaptive security appliance network monitoring and event information by transmitting data between the SNMP server and SNMP agent through the clear text community string.
SNMP Version 3	8.2(1)	Provides 3DES or AES encryption and support for SNMP Version 3, the most secure form of the supported security models. This version allows you to configure users, groups, and hosts, as well as authentication characteristics by using the USM. In addition, this version allows access control to the agent and MIB objects, and includes additional MIB support. The following commands were introduced or modified: **show snmp-server engineid, show snmp-server group, show snmp-server user, snmp-server group, snmp-server user**, **snmp-server host**.
Password encryption	8.3(1)	Supports password encryption. The following commands were modified: **snmp-server community** and **snmp-server host**.