CHAPTER 46

SNMP

This chapter describes how to configure Simple Network Management Protocol (SNMP) to monitor the ASA.

Information About SNMP

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices and is part of the TCP/IP protocol suite.

The ASA, ASAv, and ASASM provide support for network monitoring using SNMP Versions 1, 2c, and 3, and supports the use of all three versions simultaneously. The SNMP agent running on the ASA interface lets you monitor the ASA and ASASM through network management systems (NMSs), such as HP OpenView. The ASA, ASAv, and ASASM support 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 ASA, ASAv, and ASASM to send traps, which are unsolicited messages 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 ASA. MIBs are a collection of definitions, and the ASA, ASAv, and ASASM maintain 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 ASA, ASAv, and ASASM have an SNMP agent that notifies designated management stations if events occur that are predefined 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 ASA, ASAv, or ASASM SNMP agent also replies when a management station asks for information.

Information About SNMP Terminology

Table 46-1 lists the terms that are commonly used when working with SNMP:

Table 46-1 SNMP Terminology

Term	Description
Agent	The SNMP server running on the ASA. The SNMP agent has the following features: • Responds to requests for information and actions from the network management station. • Controls access to its Management Information Base, the collection of objects that the SNMP manager can view or change. • Does not allow set operations.
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.
Network management stations (NMSs)	The PCs or workstations set up to monitor SNMP events and manage devices, such as the ASA, ASAv, and ASASM.
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, warmstart, authentication, or syslog messages.

SNMP Version 3

This section describes SNMP Version 3.

- SNMP Version 3 Overview, page 46-3
- Security Models, page 46-3
- SNMP Groups, page 46-3
- SNMP Users, page 46-3
- SNMP Hosts, page 46-3
- Implementation Differences Between the ASA, ASA Services Module, and the Cisco IOS Software, page 46-4

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 and ASASM 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

ASA and ASA Services Module. Each SNMP host can have only one username associated with it. To receive SNMP traps, configure the SNMP NMS, and make sure that you configure the user credentials on the NMS to match the credentials for the ASA and ASASM.

Implementation Differences Between the ASA, ASA Services Module, and the Cisco IOS Software

The SNMP Version 3 implementation in the ASA and ASASM differs from the SNMP Version 3 implementation in the Cisco IOS software in the following ways:

- The local-engine and remote-engine IDs are not configurable. The local engine ID is generated when the ASA or ASASM 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 ASA, ASAv, or ASASM rule to allow incoming SNMP traffic.

Licensing Requirements for SNMP

Model	License Requirement
ASAv	Standard or Premium License.
All other 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

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Failover Guidelines

- Supported in SNMP Version 3.

- The SNMP client in each ASA, ASAv, or ASASM shares engine data with its peer. Engine data includes the engineID, engineBoots, and engineTime objects of the SNMP-FRAMEWORK-MIB. Engine data is written as a binary file to flash:/snmp/*contextname*.

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.
- The ENTITY-MIB is not available in the non-admin context. Use the IF-MIB instead to perform queries in the non-admin context.
- Does not support SNMP Version 3 for the AIP SSM or AIP SSC.
- Does not support SNMP debugging.
- Does not support retrieval of ARP information.
- Does not support SNMP SET commands.
- 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 AES256 or AES192.
- Changes to the existing configuration are rejected if the result places the SNMP feature in an inconsistent state.
- 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.
- The connection-limit-reached trap is generated in the admin context. To generate this trap. you must have at least one SNMP server host configured in the user context in which the connection limit has been reached.
- You cannot query for the chassis temperature on the ASA 5585 SSP-40 (NPE).
- If the NMS cannot successfully request objects or is not correctly handling incoming traps from the ASA, performing a packet capture is the most useful method for determining the problem. Choose **Wizards > Packet Capture Wizard**, and follow the on-screen instructions.
- You can add up to 4000 hosts. However, only 128 of this number can be for traps.
- The total number of supported active polling destinations is 128.
- You can specify a network object to indicate the individual hosts that you want to add as a host group.
- You can associate more than one user with one host.

- You can specify overlapping network objects in different **host-group** commands. The values that you specify for the last host group take effect for the common set of hosts in the different network objects.
- If you delete a host group or hosts that overlap with other host groups, the hosts are set up again using the values that have been specified in the configured host groups.
- The values that the hosts acquire depend on the specified sequence that you use to run the commands.
- The limit on the message size that SNMP sends is 1472 bytes.
- Members of a cluster do not synchronize their SNMPv3 engine IDs. Because of this, each unit in the cluster should have a unique SNMPv3 user configuration.

Configuring SNMP

This section describes how to configure SNMP.

- Enabling SNMP, page 46-6
- Configuring an SNMP Management Station, page 46-6
- Configuring SNMP Traps, page 46-7
- Using SNMP Version 1 or 2c, page 46-8
- Using SNMP Version 3, page 46-9

Enabling SNMP

The SNMP agent that runs on the ASA 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, see the following pane:

Path	Purpose
Configuration > Device Management > Management Access > SNMP	Ensures that the SNMP server on the ASA, ASAv, or ASASM is enabled. By default, the SNMP server is enabled.

What to Do Next

See Configuring an SNMP Management Station, page 46-6.

Configuring an SNMP Management Station

To receive requests from the ASA. you must configure an SNMP management station in ASDM.

To configure an SNMP management station, perform the following steps:

Step 1 Choose **Configuration > Device Management > Management Access > SNMP**.

Step 2 In the SNMP Management Stations pane, click **Add**.

The Add SNMP Host Access Entry dialog box appears.

Step 3 From the Interface Name drop-down list, choose the interface on which the SNMP host resides.

Step 4 In the IP Address field, enter the SNMP host IP address.

Step 5 In the UDP Port field, enter the SNMP host UDP port, or keep the default, port 162.

Step 6 In the Community String field, add the SNMP host community string. If no community string is specified for a management station, the value set in the Community String (default) field on the SNMP Management Stations pane is used.

Step 7 From the SNMP Version drop-down list, choose the SNMP version used by the SNMP host.

Step 8 If you have selected SNMP Version 3 in the previous step, from the Username drop-down list, choose the name of a configured user.

Step 9 To specify the method for communicating with this NMS, check either the **Poll** or **Trap** check box.

Step 10 Click **OK**.

The Add SNMP Host Access Entry dialog box closes.

Step 11 Click **Apply**.

The NMS is configured and changes are saved to the running configuration. For more information about SNMP Version 3 NMS tools, see the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

What to Do Next

See Configuring SNMP Traps, page 46-7.

Configuring SNMP Traps

To designate which traps that the SNMP agent generates and how they are collected and sent to NMSs, perform the following steps:

Step 1 Choose **Configuration > Device Management > Management Access > SNMP**.

Step 2 Click **Configure Traps**.

The SNMP Trap Configuration dialog box appears.

Step 3 The traps are divided into the following categories: standard, IKEv2, entity MIB, IPsec, remote access, resource, NAT, syslog, CPU utilization, CPU utilization and monitoring interval, and SNMP interface threshold. Check the applicable check boxes for the SNMP events to notify through SNMP traps. The default configuration has all SNMP standard traps enabled. If you do not specify a trap type, the default is the syslog trap. The default SNMP traps continue to be enabled with the syslog trap. All other traps are disabled by default. To disable a trap, uncheck the applicable check box. To configure the syslog trap severity level, choose **Configuration > Device Management > Logging > Logging Filters**.

Step 4 Click **OK** to close the SNMP Trap Configuration dialog box.

Step 5 Click **Apply**.

The SNMP traps are configured and the changes are saved to the running configuration.

What to Do Next

Choose one of the following:

- See Using SNMP Version 1 or 2c, page 46-8.
- See Using SNMP Version 3, page 46-9.

Using SNMP Version 1 or 2c

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

Step 1 Choose **Configuration > Device Management > Management Access > SNMP.**

Step 2 Enter a default community string in the Community String (default) field if you are using SNMP Version 1 or 2c. Enter the password used by the SNMP NMSs when they send requests to the ASA. The SNMP community string is a shared secret among the SNMP NMSs and the network nodes being managed. The ASA uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive value up to 32 alphanumeric characters long. Spaces are not permitted. The default is public. SNMP Version 2c allows separate community strings to be set for each NMS. If no community string is configured for any NMS, the value set here is used by default.

Step 3 In the Contact field, enter the name of the ASA system administrator. The text is case-sensitive and can be up to 127 alphabetic characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Step 4 In the ASA Location field, enter the location of the ASA being managed by SNMP. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Step 5 In the Listening Port field, enter the number of the ASA port that listens for SNMP requests from NMSs; or keep the default, port number 161.

Step 6 In the SNMP Host Access List pane, click **Add** to display the Add SNMP Host Access Entry dialog box.

Step 7 Choose the interface name from which traps are sent from the drop-down list.

Step 8 Enter the IP address of the NMS or SNMP manager that can connect to the ASA.

Step 9 Enter the UDP port number. The default is 162.

Step 10 Choose the SNMP version that you are using from the drop-down list. If you choose Version 1 or Version 2c, you must enter the community string. If you choose Version 3, you must choose the username from the drop-down list.

Step 11 In the Server Poll/Trap Specification area, check the **Poll** check box to limit the NMS to sending requests (polling) only. Check the **Trap** check box to limit the NMS to receiving traps only. You may check both check boxes to perform both functions of the SNMP host.

Step 12 Click **OK** to close the Add SNMP Host Access Entry dialog box.

The new host appears in the SNMP Host Access List pane.

Step 13 Click **Apply**.

SNMP parameters for Versions 1, 2c, or 3 are configured and the changes are saved to the running configuration.

What to Do Next

See Monitoring SNMP, page 46-11.

Using SNMP Version 3

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

Step 1 Choose **Configuration > Device Management > Management Access > SNMP.**

Step 2 In the SNMPv3 Users pane, to add a configured user or a new user to a group, on the SNMPv3 User/Group tab, click **Add > SNMP User**. To change user parameters, click **Edit > SNMP User**. To remove a configured user from a group, select the user, then click **Delete > SNMP User**. When you remove the last user in a group, ASDM deletes the group.

Note After a user has been created, you cannot change the group to which the user belongs.

The Add SNMP User Entry dialog box appears.

Step 3 From the Group Name drop-down list, choose the group to which the SNMP user belongs. The available groups are as follows:

- Auth&Encryption, in which users have authentication and encryption configured
- Authentication_Only, in which users have only authentication configured
- No_Authentication, in which users have neither authentication nor encryption configured

Note You cannot change the group names.

Step 4 To use the user security model (USM) groups, click the **USM Model** tab.

Step 5 To add a USM group, click **Add**. To modify an existing USM group, select it, then click **Edit**. To remove an existing USM group, select it, then click **Delete**.

The Add or Edit SNMP USM Entry dialog box appears.

Step 6 In the Group Name field, enter the group name.

Step 7 Choose the security level from the drop-down list. This setting allows you to assign a configured USM group as a security level to SNMPv3 users.

Step 8 In the Username field, enter the name of a configured user or a new user. The username must be unique for the SNMP server group selected.

Step 9 Indicate the type of password you want to use by clicking one of the two radio buttons: **Encrypted** or **Clear Text**.

Step 10 Indicate the type of authentication you want to use by clicking one of the two radio buttons: **MD5** or **SHA**.

Step 11 In the Authentication Password field, type the password to use for authentication.

Step 12 Indicate the type of encryption you want to use by clicking one of these three radio buttons: **DES**, **3DES**, or **AES**.

Step 13 If you chose AES encryption, then from the AES Size drop-down list, choose the level of AES encryption to use: **128**, **192**, or **256**.

Step 14 In the Encryption Password field, type the password to use for encryption. The maximum number of alphanumeric characters allowed for this password is 64.

Step 15 Click **OK** to create a group (if this is the first user in that group), display this group in the Group Name drop-down list, and create a user for that group.

The Add SNMP User Entry dialog box closes.

Step 16 Click **Apply**.

SNMP parameters for Version 3 are configured, and the changes are saved to the running configuration.

What to Do Next

See Monitoring SNMP, page 46-11.

Configuring a Group of Users

To configure an SNMP user list with a group of specified users in it, perform the following steps:

Step 1 Choose **Configuration > Device Management > Management Access > SNMP.**

Step 2 In the SNMPv3 Users pane, to add a configured user group or a new user group, on the SNMPv3 User/Group tab, click **Add > SNMP User Group**. To change group parameters, click **Edit > SNMP Group**. To remove a configured user group, select it, then click **Delete > SNMP Group**. When you remove the last user in a group, ASDM deletes the group.

The Add SNMP User Group dialog box appears.

Step 3 Enter the user group name.

Step 4 To select an existing user or user group, click the **Existing User/User Group** radio button.

Step 5 To create a new user, click the **Create new user** radio button.

Step 6 From the Group Name drop-down list, choose the group to which the SNMP user belongs. The available groups are as follows:

- Auth&Encryption, in which users have authentication and encryption configured
- Authentication_Only, in which users have only authentication configured
- No_Authentication, in which users have neither authentication nor encryption configured

Step 7 In the Username field, enter the name of a configured user or a new user. The username must be unique for the SNMP server group selected.

Step 8 Indicate the type of password you want to use by clicking one of the two radio buttons: **Encrypted** or **Clear Text**.

Step 9 Indicate the type of authentication you want to use by clicking one of the two radio buttons: **MD5** or **SHA**.

Step 10 In the Authentication Password field, type the password to use for authentication.

Step 11 Retype the password to use for authentication.

Step 12 Indicate the type of encryption you want to use by clicking one of these three radio buttons: **DES**, **3DES**, or **AES**.

Step 13 In the Encryption Password field, type the password to use for encryption. The maximum number of alphanumeric characters allowed for this password is 64.

Step 14 Retype the password to use for encryption.

Step 15 Click **Add** to add the new user to the specified user group in the Members in Group pane. Click **Remove** to delete an existing user from the Members in Group pane.

Step 16 Click **OK** to create a new user for the specified user group.

The Add SNMP User Group dialog box closes.

Step 17 Click **Apply**.

SNMP parameters for Version 3 are configured, and the changes are saved to the running configuration.

.

Monitoring SNMP

NMSs are the PCs or workstations that you set up to monitor SNMP events and manage devices, such as the ASA.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.

- SNMP Syslog Messaging, page 46-11
- SNMP Monitoring, page 46-12

SNMP Syslog Messaging

SNMP generates detailed syslog messages that are numbered 212*nnn*. Syslog messages indicate the status of SNMP requests, SNMP traps, SNMP channels, and SNMP responses from the ASA or ASASM to a specified host on a specified interface.

For detailed information about syslog messages, see the syslog messages guide.

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

SNMP Monitoring

To monitor SNMP, perform the following steps:

Path	Purpose
Tools > Command Line Interface Enter the **show running-config snmp-server** command, then click **Send**.	Shows all SNMP server configuration information.
Tools > Command Line Interface Enter the **show running-config snmp-server group** command, then click **Send**.	Shows SNMP group configuration settings.
Tools > Command Line Interface Enter the **show running-config snmp-server host** command, then click **Send**.	Shows configuration settings used by SNMP to control messages and notifications sent to remote hosts.
Tools > Command Line Interface Enter the **show running-config snmp-server host-group** command, then click **Send**.	Shows SNMP host group configurations.
Tools > Command Line Interface Enter the **show running-config snmp-server user** command, then click **Send**.	Shows SNMP user-based configuration settings.
Tools > Command Line Interface Enter the **show running-config snmp-server user-list** command, then click **Send**.	Shows SNMP user list configurations.
Tools > Command Line Interface Type **show snmp-server engineid** command, then click **Send**.	Shows the ID of the SNMP engine configured.
Tools > Command Line Interface Enter the **show snmp-server group** command, then click **Send**.	Shows 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.
Tools > Command Line Interface Enter the **show snmp-server statistics** command, then click **Send**.	Shows the configured characteristics of the SNMP server.
Tools > Command Line Interface Enter the **show snmp-server user** command, then click **Send**.	Shows the configured characteristics of users.

Where to Go Next

To configure the syslog server, see Chapter 45, "Logging."

Additional References

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

- RFCs for SNMP Version 3, page 46-13
- MIBs, page 46-13
- Application Services and Third-Party Tools, page 46-15

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 ASA, ASAv, and ASASM by release, see the following URL:

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

Not all OIDs in MIBs are supported. To obtain a list of the supported SNMP MIBs and OIDs for a specific ASA or ASASM, choose **Tools > Command Line Interface**, the following command, then click **Send**:

```
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. However, this command is for Cisco TAC use only. Contact the Cisco TAC before using this command.

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

```
hostname(config)# show snmp-server oidlist
[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 46-2 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 46-2 Feature History for SNMP

Feature Name	Platform Releases	Feature Information
SNMP Versions 1 and 2c	7.0(1)	Provides ASA, ASAv, and ASASM network monitoring and event information by transmitting data between the SNMP server and SNMP agent through the clear text community string. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
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. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
Password encryption	8.3(1)	Supports password encryption.

Table 46-2 Feature History for SNMP (continued)

Feature Name	Platform Releases	Feature Information
SNMP traps and MIBs	8.4(1)	Supports the following additional keywords: **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. The entPhysicalTable reports entries for sensors, fans, power supplies, and related components. Supports the following additional MIBs: CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. Supports the following additional traps: ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
IF-MIB ifAlias OID support	8.2(5)/8.4(2)	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description.
ASA Services Module (ASASM)	8.5(1)	The ASASM supports all MIBs and traps that are present in 8.4(1), except for the following: Unsupported MIBs in 8.5(1): • CISCO-ENTITY-SENSOR-EXT-MIB (Only objects under the entPhySensorTable group are supported). • ENTITY-SENSOR-MIB (Only objects in the entPhySensorTable group are supported). • DISMAN-EXPRESSION-MIB (Only objects in the expExpressionTable, expObjectTable, and expValueTable groups are supported). Unsupported traps in 8.5(1): • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). This trap is only used for power supply failure, fan failure, and high CPU temperature events. • InterfacesBandwidthUtilization.
SNMP traps	8.6(1)	Supports the following additional keywords for the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X: **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. We modified the following command: **snmp-server enable traps**.

Table 46-2 Feature History for SNMP (continued)

Feature Name	Platform Releases	Feature Information
VPN-related MIBs	9.0(1)	An updated version of the CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB has been implemented to support the next generation encryption feature. The following MIBs have been enabled for the ASASM: • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	Support for the following MIB was added: CISCO-TRUSTSEC-SXP-MIB.
SNMP OIDs	9.1(1)	Five new SNMP Physical Vendor Type OIDs have been added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
NAT MIB	9.1(2)	Added the cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support the xlate_count and max_xlate_count entries, which are the equivalent to allowing polling using the **show xlate count** command.
SNMP hosts, host groups, and user lists	9.1(5)	You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
SNMP message size	9.2(1)	The limit on the message size that SNMP sends has been increased to 1472 bytes.
SNMP MIB		The CISCO-VPN-LIC-USAGE-MONITOR-MIB, a new SNMP MIB for monitoring VPN shared license usage, has been added. The OID has the following index: 1.3.6.1.4.1.9.9.816.x.x. This new OID polls the number of active and max-session connections. We did not introduce or modify any commands.