

SNMP

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

- About SNMP, on page 1
- Guidelines for SNMP, on page 4
- Configure SNMP, on page 7
- Monitoring SNMP, on page 13
- History for SNMP, on page 14

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 provides support for network monitoring using SNMP Versions 1, 2c, and 3, and support the use of all three versions simultaneously. The SNMP agent running on the ASA interface lets you monitor the network devices through network management systems (NMSes), such as HP OpenView. The ASA 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 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 Management Information Bases (MIBs) on the security devices. MIBs are a collection of definitions, and the ASA 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.

Note With intense workloads, deploying more than 10 NMS can impact the device's performance. To ensure device's stability and responsiveness, we recommend that you cautiously utilize NMS in conducting SNMP walk polling and in managing the trap traffic.

The ASA 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 agent also replies when a management station asks for information.

SNMP Terminology

The following table lists the terms that are commonly used when working with SNMP.

Table 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.
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 Overview

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or 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 also supports 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 SHA-1, SHA-224, SHA-256 HMAC, and SHA-384. The encryption algorithm options are 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.



Note When configuring an SNMP v3 user account, ensure that the length of authentication algorithm is equal to or greater than the length of encryption algorithm.

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. 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.



Note You can add up to 8192 hosts. However, only 128 of this number can be for traps.

Implementation Differences Between the ASA and Cisco IOS Software

The SNMP Version 3 implementation in the ASA 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 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 rule to allow incoming SNMP traffic.

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).

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 Refer to SNMP Chapter in Cisco ASA Series General Operations ASDM Configuration Guide, see the following URL:

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

Guidelines for SNMP

This section includes the guidelines and limitations that you should review before configuring SNMP.

Failover and Clustering Guidelines

- When using SNMPv3 with clustering or failover, if you add a new cluster unit after the initial cluster formation or you replace a failover unit, then SNMPv3 users are not replicated to the new unit. You must re-add the SNMPv3 users to the control/active unit to force the users to replicate to the new unit; or you can add the users directly on the new unit (SNMPv3 users and groups are an exception to the rule that you cannot enter configuration commands on a cluster data unit). Reconfigure each user by entering the **snmp-server user** *username group-name* **v3** command on the control/active unit or directly to the data/standby unit with the *priv-password* option and *auth-password* option in their unencrypted forms.

IPv6 Guidelines (All ASA Models)

SNMP can be configured over IPv6 transport so that an IPv6 host can perform SNMP queries and receive SNMP notifications from a device running IPv6 software. The SNMP agent and related MIBs have been enhanced to support IPv6 addressing.

IPv6 Guidelines for the Firepower 2100

The Firepower 2100 runs an underlying operating system called the FXOS, and supports both Appliance mode (the default) and Platform mode; see Set the Firepower 2100 to Appliance or Platform Mode.

When in Platform mode, you must configure an IPv6 management IP address in FXOS. The following example configures an IPv6 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

Additional Guidelines

- Power supply traps are not issued for systems operating in Appliance mode.
- For the Firepower 2100 in Platform mode, you cannot poll member interfaces of an EtherChannel, and traps for member interfaces are not generated. This functionality is supported if you enable SNMP directly in FXOS. Appliance mode is not affected.
- Does not support ASA traps for individual individual port members for the Firepower 2100 in Platform mode; see Cisco Firepower 2100 FXOS MIB Reference Guide.
- For the Firepower 2100 in Appliance mode, you cannot poll the hardware model and serial, and in ASA, traps are not generated for these details. Hence, configure SNMP on FXOS or Chassis Manager to poll Chassis Management IP instead of the interfaces on ASA instance.
- You must have Cisco Works for Windows or another SNMP MIB-II compliant browser to receive SNMP traps or browse a MIB.
- Management-access over a VPN tunnel is not supported with SNMP (the **management-access** command). For SNMP over VPN, we recommend enabling SNMP on a loopback interface. You don't need the management-access feature enabled to use SNMP on the loopback interface. Loopback also works for SSH.
- 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.
- The ENTITY-MIB is not available for the Firepower 9300. Instead, use CISCO-FIREPOWER-EQUIPMENT-MIB and CISCO-FIREPOWER-SM-MIB.
- On some devices, the order of interfaces (ifDescr) in the output of **snmpwalk** has been observed to change after a reboot. The ASA uses an algorithm to determine the ifIndex table that SNMP queries. When the ASA is booted up, the interfaces are added to the ifIndex table in the order loaded as the ASA reads the configuration. New interfaces added to the ASA are appended to the list of interfaces in the ifIndex table. As interfaces are added, removed, or renamed, it can affect the order of interfaces on reboot.
- When you provide an OID in the **snmpwalk** command, the snmpwalk tool queries all variables in the subtree that is below the specified OID and displays their values. Thus, to view a comprehensive output of the objects on the device, ensure to provide the OID in the **snmpwalk** command.
- 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.
- For Firepower 2100, when SNMPv3 is configured over the device management interface, all SNMPv3 users can poll the device even when they are not mapped in the Host configuration.
- For Secure Firewall models, the **snmpwalk** command polls FXOS mibs only from admin context.
- 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.
- 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.

- The ASA supports an unlimited number of SNMP server trap hosts per context. The **show snmp-server host** command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts.

Configure SNMP

This section describes how to configure SNMP.

Procedure

Step 1 Configure an SNMP management station to receive requests from the ASA.
Step 2 Configure SNMP traps.
Step 3 Configure SNMP Version 1 and 2c parameters or SNMP Version 3 parameters.

Configure an SNMP Management Station

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

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Management Access** > **SNMP**. By default, the SNMP server is enabled.
Step 2 Click **Add** in the **SNMP Management Stations** pane.

The **Add SNMP Host Access Entry** dialog box appears.

Step 3 Choose the interface on which the SNMP host resides.
Step 4 Enter the SNMP host IP address.
Step 5 Enter the SNMP host UDP port, or keep the default, port 162.
Step 6 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 Choose the SNMP version used by the SNMP host.
Step 8 If you have selected SNMP Version 3 in the previous step, 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 Refer to SNMP Chapter in Cisco ASA Series General Operations ASDM Configuration Guide, see the following URL:

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

Configure SNMP Traps

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

Note When you enable all SNMP or syslog traps, it is possible for the SNMP process to consume excess resources in the agent and in the network, causing the system to hang. If you notice system delays, unfinished requests, or timeouts, you can selectively enable SNMP and syslog traps. For example, you can skip *Informational* syslog trap severity level.

Procedure

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

Step 2 Click **Configure Traps**.

The **SNMP Trap Configuration** dialog box appears.

Step 3 Check the **SNMP Server traps configuration** check box.

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.

The traps are divided into the following categories:

a) **Standard SNMP Traps**, check all that apply.

Choose from **Critical CPU temperature**, **Chassis temperature**, and **Chassis Fan Failure**.

Note
The default configuration has all SNMP standard traps enabled.

b) **Environment Traps**, check all that apply.

Choose from **Authentication**, **Link up**, **Link down**, **Cold start**, and **Warm start**.

c) **Ikev2 Traps** check all that apply.

Choose from **Start** and **Stop**.

d) **Entity MIB Notifications**.

Check this item to receive notifications about field-replaceable units.

e) **IPsec Traps**, check all that apply.

Choose from **Start** and **Stop**.

f) **Remote Access Traps**.

Check this item to receive notifications when the number of sessions established exceeds the set threshold.

g) **Resource Traps**, check all that apply.

Choose from **Connection limit reached**, **Memory threshold reached**, and **Interface threshold reached**.

h) **NAT Traps**.

Check this item to receive notifications when IP packets are discarded by NAT because mapping space is not available.

i) **Syslog**.

Check **Enable syslog traps** to receive notifications when the number of sessions established exceeds the set threshold.

To configure the **syslog** trap severity level, choose **Configuration** > **Device Management** > **Logging** > **Logging Filters**

j) **CPU Utilization Traps**.

Check **CPU rising threshold reached** to receive notifications when the CPU usage is greater than the configured **CPU Utilization threshold** value for the configured **Monitoring interval**.

k) **SNMP interface threshold**.

Check **Configure threshold and interval** to receive notifications when the interface bandwidth utilization is greater than the configured **SNMP interface threshold** value.

Valid threshold values range from 30 to 99 percent. The default value is 70 percent.

l) **SNMP Memory threshold**.

Check **Configure memory threshold** to receive notifications when the CPU usage is greater than the configured threshold value for the **SNMP memory threshold** value.

When the used system context memory reaches 80 percent of the total system memory, the memory threshold trap is generated from the admin context. For all other user contexts, this trap is generated when the used memory reaches 80 percent of the total system memory in that particular context.

m) **Failover Traps**.

Check **Enable Failover related traps** to receive SNMP syslog traps for failover.

n) **Cluster Traps**.

Check **Enable cluster related traps** to receive SNMP syslog traps for cluster members.

o) **Peer-Flap Traps**.

Check **Enable bgp/ospf peer-flap related traps** to receive SNMP syslog traps for cluster peer MAC address flapping.

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.

Configure Parameters for SNMP Version 1 or 2c

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

Procedure

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. However, if SNMP monitoring is through the management interface instead of the diagnostic interface, polling takes place without ASA validating the community string. 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.

Note
You should avoid the use of special characters (!, @, #, $, %, ^, &, *, \) in community strings. In general, using any special characters reserved for functions used by the operating system can cause unexpected results. For example, the backslash (\) is interpreted as an escape character and should not be used in the community string.

Step 3 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 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 Enter the number of the ASA port that listens for SNMP requests from NMSes; or keep the default, port number 161.

Step 6 (Optional) Check the **Enable Global-Shared pool in the walk** checkbox to query free memory and used memory statistics through SNMP walk operations.

Important
When the ASA queries memory information, the CPU may be held by the SNMP process for too long before releasing the CPU to other processes. This can result in SNMP-related CPU hogs causing packet drops.

Step 7 Click **Add** in the **SNMP Host Access List** pane.

The **Add SNMP Host Access Entry** dialog box appears.

Step 8 Choose the interface name from which traps are sent from the drop-down list.

Step 9 Enter the IP address of the NMS or SNMP manager that can connect to the ASA.

Step 10 Enter the UDP port number. The default is 162.

Step 11 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.

The version specifies the SNMP version to use for traps and requests (polling). Communication with the server is allowed using the selected version only.

Step 12 Check the **Poll** check box in the **Server Poll/Trap Specification** area 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 13 Click **OK** to close the **Add SNMP Host Access Entry** dialog box.

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

Step 14 Click **Apply**.

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

Configure Parameters for SNMP Version 3

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

Procedure

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

Step 2 Click **Add** > **SNMP User**on the **SNMPv3 User/Group** tab in the **SNMPv3 Users pane** to add a configured user or a new user to a group. 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 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 Click the **USM Model** tab to use the user security model (USM) groups.

Step 5 Click **Add**.

The **Add SNMP USM Entry** dialog box appears.

Step 6 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 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 four radio buttons: **SHA**, **SHA224**, **SHA256**, or **SHA384**.

Step 11 Enter the password to use for authentication.

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

Step 13 If you chose AES encryption, then choose the level of AES encryption to use: **128**, **192**, or **256**.

Step 14 Enter 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.

Configure a Group of Users

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

Procedure

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

Step 2 Click **Add** > **SNMP User Group** on the **SNMPv3 User/Group** tab in the **SNMPv3 Users** pane to add a configured user group or a new user 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 Click the **Existing User/User Group** radio button to select an existing user or user group.

Step 5 Click the **Create new user** radio button to create a new user.

Step 6 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 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 four radio buttons: **SHA**, **SHA224**, **SHA256**, or **SHA384**.

Step 10 Enter the password to use for authentication.

Step 11 Confirm the password to use for authentication.

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

Step 13 Enter the password to use for encryption. The maximum number of alphanumeric characters allowed for this password is 64.

Step 14 Confirm 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

See the following commands for monitoring SNMP. You can enter these commands using **Tools > Command Line Interface**.

- **show running-config snmp-server** [**default**]

  This command shows all SNMP server configuration information.

- **show running-config snmp-server group**

  This command shows SNMP group configuration settings.

- **show running-config snmp-server host**

  This command shows configuration settings used by SNMP to control messages and notifications sent to remote hosts.

- **show running-config snmp-server host-group**

  This command shows SNMP host group configurations.

- **show running-config snmp-server user**

  This command shows SNMP user-based configuration settings.

- **show running-config snmp-server user-list**

  This command shows SNMP user list configurations.

- **show snmp-server engineid**

  This command shows the ID of the SNMP engine configured.

- **show snmp-server group**

  This command shows the names of configured SNMP groups. 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**

This command shows the configured characteristics of the SNMP server. To reset all SNMP counters to zero, use the **clear snmp-server statistics** command.

- **show snmp-server user**

  This command shows the configured characteristics of users.

History for SNMP

Table 2: History for SNMP

Feature Name	Version	Description
SNMP Versions 1 and 2c	7.0(1)	Provides ASA 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.
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.

Feature Name	Version	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**.
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.

Feature Name	Version	Description
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 OIDs and MIBs	9.2(1)	The ASA now supports the cpmCPUTotal5minRev OID. The ASA Virtual has been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID. The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASA Virtual platform. A new SNMP MIB for monitoring VPN shared license usage has been added.
SNMP OIDs and MIBs	9.3(1)	CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) support has been added for the ASASM.
SNMP MIBs and traps	9.3(2)	The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the ASA 5506-X. The ASA 5506-X has been added as new products to the SNMP sysObjectID OID and entPhysicalVendorType OID tables. The ASA now supports the CISCO-CONFIG-MAN-MIB, which enables you to do the following: • Know which commands have been entered for a specific configuration. • Notify the NMS when a change has occurred in the running configuration. • Track the time stamps associated with the last time that the running configuration was changed or saved. • Track other changes to commands, such as terminal details and command sources. We modified the following screen: Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration.
SNMP MIBs and traps	9.4(1)	The ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X have been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID tables.

Feature Name	Version	Description
Unlimited SNMP server trap hosts per context	9.4(1)	The ASA supports unlimited SNMP server trap hosts per context. The **show snmp-server host** command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts. We did not modify any ASDM screens.
Added support for ISA 3000	9.4(1.225)	The ISA 3000 family of products is now supported for SNMP. We added new OIDs for this platform. The **snmp-server enable traps entity** command has been modified to include a new variable *l1-bypass-status*. This enables hardware bypass status change. We did not modify any ASDM screens.
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	9.6(1)	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system. **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM.
Support for E2E Transparent Clock Mode MIBs for the Precision Time Protocol (PTP)	9.7(1)	MIBs corresponding to E2E Transparent Clock mode are now supported. **Note** Only SNMP get, bulkget, getnext, and walk operations are supported.
SNMP over IPv6	9.9(2)	The ASA now supports SNMP over IPv6, including communicating with SNMP servers over IPv6, allowing the execution of queries and traps over IPv6, and supporting IPv6 addresses for existing MIBs. We added the following new SNMP IPv6 MIB objects as described in RFC 8096. • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30)—Contains per-interface IPv6-specific information. • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32)—Includes all the prefixes learned by this entity. • ipAddressTable (OID: 1.3.6.1.2.1.4.34)—Contains addressing information relevant to the entity's interfaces. • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35)—Contains the mapping from IP addresses to physical addresses. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	9.10(1)	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. We did not modify any ASDM screens.

Feature Name	Version	Description
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	9.12(1)	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**
SNMPv3 Authentication	9.14(1)	You can now use SHA-256 HMAC for user authentication. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
For Failover pairs in 9.14(1)+, the ASA no longer shares SNMP client engine data with its peer.	9.14(1)	The ASA no longer shares SNMP client engine data with its peer.
SNMP polling over site-to-site VPN	9.14(2)	For secure SNMP polling over a site-to-site VPN, include the IP address of the outside interface in the crypto map access-list as part of the VPN configuration.
Support for the CISCO-MEMORY-POOL-MIB OIDs is deprecated	9.15(1)	The CISCO-MEMORY-POOL-MIB OIDs (ciscoMemoryPoolUsed, ciscoMemoryPoolFree) are deprecated for systems that use 64-bit counters. The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB provides memory pool monitoring entries for systems that use 64-bit counters.
SNMPv3 Authentication	9.16(1)	You can now use SHA-224 and SHA-384 for user authentication. You can no longer use MD5 for user authentication. You can no longer use DES for encryption. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
Loopback interface support for SNMP	9.18(2)	You can now add a loopback interface and use it for SNMP. New/Modified commands: **interface loopback**, **snmp-server host** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Loopback Interface** ASDM support was added in 7.19.
SNMP MIBs and traps	9.20(1)	The Secure Firewall 4200 model devices (FPR4215, FPR4225, FPR4245) have been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID tables. SNMP support for the two EPM cards(4X200G and 2X100G) of these Secure Firewall 4200 Series devices was added.