CHAPTER 79

Configuring SNMP

This chapter describes how to configure SNMP to monitor the ASA and includes the following sections:

- Information About SNMP, page 79-1
- Licensing Requirements for SNMP, page 79-17
- Prerequisites for SNMP, page 79-17
- Guidelines and Limitations, page 79-17
- Configuring SNMP, page 79-18
- Troubleshooting Tips, page 79-24
- Monitoring SNMP, page 79-26
- Configuration Examples for SNMP, page 79-28
- Where to Go Next, page 79-29
- Additional References, page 79-29
- Feature History for SNMP, page 79-31

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. This section describes SNMP and includes the following topics:

- Information About SNMP Terminology, page 79-2
- Information About MIBs and Traps, page 79-2
- SNMP Object Identifiers, page 79-3
- SNMP Physical Vendor Type Values, page 79-5
- Supported Tables in MIBs, page 79-11
- Supported Traps (Notifications), page 79-12
- SNMP Version 3, page 79-15

The ASA provides 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 through network management systems (NMSs), such as HP OpenView. The ASA 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 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 MIBs on the ASA. MIBs are a collection of definitions, and the ASA 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 ASA has 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 ASASNMP agent also replies when a management station asks for information.

Information About SNMP Terminology

Table 79-1 lists the terms that are commonly used when working with SNMP:

Table 79-1 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.

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. SNMP traps are compiled into the ASA software.

If needed, you can also download RFCs, standard MIBs, and standard traps from the following locations:

http://www.ietf.org/

ftp://ftp-sj.cisco.com/pub/mibs

Download a complete list of Cisco MIBs, traps, and OIDs from the following location:

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

In addition, download Cisco OIDs by FTP 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 through SNMP refreshes about every 5 seconds. As a result, we recommend that you wait for at least 5 seconds between consecutive polls.

SNMP Object Identifiers

Each Cisco system-level product has an SNMP object identifier (OID) for use as a MIB-II sysObjectID. The CISCO-PRODUCTS-MIB includes the OIDs that can be reported in the sysObjectID object in the SNMPv2-MIB. You can use this value to identify the model type. Table 79-2 lists the sysObjectID OIDs for ASA models.

Table 79-2 SNMP Object Identifiers

Product Identifier	sysObjectID	Model Number
ASA 5505	ciscoASA5505 (ciscoProducts 745)	Cisco ASA 5505
ASA 5510	ciscoASA5510 (ciscoProducts 669)	Cisco ASA 5510
ASA 5510	ciscoASA5510sc (ciscoProducts 773)	Cisco ASA 5510 security context
ASA 5510	ciscoASA5510sy (ciscoProducts 774)	Cisco ASA 5510 system context
ASA 5520	ciscoASA5520 (ciscoProducts 670)	Cisco ASA 5520
ASA 5520	ciscoASA5520sc (ciscoProducts 671)	Cisco ASA 5520 security context
ASA 5520	ciscoASA5520sy (ciscoProducts 764)	Cisco ASA 5520 system context
ASA 5540	ciscoASA5540 (ciscoProducts 672)	Cisco ASA 5540
ASA 5540	ciscoASA5540sc (ciscoProducts 673)	Cisco ASA 5540 security context
ASA 5540	ciscoASA5540sy (ciscoProducts 765)	Cisco ASA 5540 system context
ASA 5550	ciscoASA5550 (ciscoProducts 753)	Cisco ASA 5550
ASA 5550	ciscoASA5550sc (ciscoProducts 763)	Cisco ASA 5550 security context
ASA 5550	ciscoASA 5550sy (ciscoProducts 766)	Cisco ASA 5550 system context
ASA5580	ciscoASA5580 (ciscoProducts 914)	Cisco ASA 5580
ASA5580	ciscoASA5580 (ciscoProducts 915)	Cisco ASA 5580 security context
ASA5580	ciscoASA5580 (ciscoProducts 916)	Cisco ASA 5580 system context
ASA5585-SSP10	ciscoASA5585Ssp10 (ciscoProducts 1194)	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20 (ciscoProducts 1195)	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40 (ciscoProducts 1196)	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60 (ciscoProducts 1197)	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc (ciscoProducts 1198)	ASA 5585-X SSP-10 security context

Table 79-2 SNMP Object Identifiers (continued)

ASA5585-SSP20	ciscoASA5585Ssp20sc (ciscoProducts 1199)	ASA 5585-X SSP-20 security context
ASA5585-SSP40	ciscoASA5585Ssp40sc (ciscoProducts 1200)	ASA 5585-X SSP-40 security context
ASA5585-SSP60	ciscoASA5585Ssp60sc (ciscoProducts 1201)	ASA 5585-X SSP-60 security context
ASA5585-SSP10	ciscoASA5585Ssp10sy (ciscoProducts 1202)	ASA 5585-X SSP-10 system context
ASA5585-SSP20	ciscoASA5585Ssp20sy (ciscoProducts 1203)	ASA 5585-X SSP-20 system context
ASA5585-SSP40	ciscoASA5585Ssp40sy (ciscoProducts 1204)	ASA 5585-X SSP-40 system context
ASA5585-SSP60	ciscoASA5585Ssp60sy (ciscoProducts 1205)	ASA 5585-X SSP-60 system context
ASA Services Module for Catalyst switches	ciscoAsaSm1 (ciscoProducts 1277)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches
ASA Services Module for Catalyst switches security context	ciscoAsaSm1sc (ciscoProducts 1275)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches security context
ASA Services Module for Catalyst switches security context with No Payload Encryption	ciscoAsaSm1K7sc (ciscoProducts 1334)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches security context with No Payload Encryption
ASA Services Module for Catalyst switches system context	ciscoAsaSm1sy (ciscoProducts 1276)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches system context
ASA Services Module for Catalyst switches system context with No Payload Encryption	ciscoAsaSm1K7sy (ciscoProducts 1335)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches system context with No Payload Encryption
ASA Services Module for Catalyst switches system context with No Payload Encryption	ciscoAsaSm1K7 (ciscoProducts 1336)	Adaptive Security Appliance (ASA) Services Module for Catalyst switches with No Payload Encryption
ASA 5512	ciscoASA5512 (ciscoProducts 1407)	ASA 5512 Adaptive Security Appliance
ASA 5525	ciscoASA5525 (ciscoProducts 1408)	ASA 5525 Adaptive Security Appliance
ASA 5545	ciscoASA5545 (ciscoProducts 1409)	ASA 5545 Adaptive Security Appliance
ASA 5555	ciscoASA5555 (ciscoProducts 1410)	ASA 5555 Adaptive Security Appliance
ASA 5512 Security Context	ciscoASA5512sc (ciscoProducts 1411)	ASA 5512 Adaptive Security Appliance Security Context
ASA 5525 Security Context	ciscoASA5525sc (ciscoProducts 1412)	ASA 5525 Adaptive Security Appliance Security Context
ASA 5545 Security Context	ciscoASA5545sc (ciscoProducts 1413)	ASA 5545 Adaptive Security Appliance Security Context
ASA 5555 Security Context	ciscoASA5555sc (ciscoProducts 1414)	ASA 5555 Adaptive Security Appliance Security Context
ASA 5512 System Context	ciscoASA5512sy (ciscoProducts 1415)	ASA 5512 Adaptive Security Appliance System Context
ASA 5515 System Context	ciscoASA5515sy (ciscoProducts 1416)	ASA 5515 Adaptive Security Appliance System Context

Table 79-2 SNMP Object Identifiers (continued)

ASA 5525 System Context	ciscoASA5525sy (ciscoProducts1417)	ASA 5525 Adaptive Security Appliance System Context
ASA 5545 System Context	ciscoASA5545sy (ciscoProducts 1418)	ASA 5545 Adaptive Security Appliance System Context
ASA 5555 System Context	ciscoASA5555sy (ciscoProducts 1419)	ASA 5555 Adaptive Security Appliance System Context
ASA 5515 Security Context	ciscoASA5515sc (ciscoProducts 1420)	ASA 5515 Adaptive Security Appliance System Context
ASA 5515	ciscoASA5515 (ciscoProducts 1421)	ASA 5515 Adaptive Security Appliance

SNMP Physical Vendor Type Values

Each Cisco chassis or standalone system has a unique type number for SNMP use. The entPhysicalVendorType OIDs are defined in the CISCO-ENTITY-VENDORTYPE-OID-MIB. This value is returned in the entPhysicalVendorType object from the ASA SNMP agent. You can use this value to identify the type of component (module, power supply, fan, sensors, CPU, and so on). Table 79-3 lists the physical vendor type values for the ASA models.

Table 79-3 SNMP Physical Vendor Type Values

Item	entPhysicalVendorType OID Description
ASA Services Module for Catalyst switches	cevCat6kWsSvcAsaSm1 (cevModuleCat6000Type 169)
ASA Services Module for Catalyst switches with No Payload Encryption	cevCat6kWsSvcAsaSm1K7 (cevModuleCat6000Type 186)
ASA 5505 chassis	cevChassisASA5505 (cevChassis 560)
ASA 5510 chassis	cevChassisASA5510 (cevChassis 447)
Cisco Adaptive Security Appliance (ASA) 5512 Adaptive Security Appliance	cevChassisASA5512 (cevChassis 1113)
Cisco Adaptive Security Appliance (ASA) 5512 Adaptive Security Appliance with No Payload Encryption	cevChassisASA5512K7 (cevChassis 1108)
Cisco Adaptive Security Appliance (ASA) 5515 Adaptive Security Appliance	cevChassisASA5515 (cevChassis 1114)
Cisco Adaptive Security Appliance (ASA) 5515 Adaptive Security Appliance with No Payload Encryption	cevChassisASA5515K7 (cevChassis 1109)
ASA 5520 chassis	cevChassisASA5520 (cevChassis 448)
Cisco Adaptive Security Appliance (ASA) 5525 Adaptive Security Appliance	cevChassisASA5525 (cevChassis 1115)
Cisco Adaptive Security Appliance (ASA) 5525 Adaptive Security Appliance with No Payload Encryption	cevChassisASA5525K7 (cevChassis 1110)
ASA 5540 chassis	cevChassisASA5540 (cevChassis 449)

Table 79-3 SNMP Physical Vendor Type Values (continued)

Cisco Adaptive Security Appliance (ASA) 5545 Adaptive Security Appliance	cevChassisASA5545 (cevChassis 1116)
Cisco Adaptive Security Appliance (ASA) 5545 Adaptive Security Appliance with No Payload Encryption	cevChassisASA5545K7 (cevChassis 1111)
ASA 5550 chassis	cevChassisASA5550 (cevChassis 564)
Cisco Adaptive Security Appliance (ASA) 5555 Adaptive Security Appliance	cevChassisASA5555 (cevChassis 1117)
Cisco Adaptive Security Appliance (ASA) 5555 Adaptive Security Appliance with No Payload Encryption	cevChassisASA5555K7 (cevChassis 1112)
ASA 5580 chassis	cevChassisASA5580 (cevChassis 704)
Central Processing Unit for Cisco Adaptive Security Appliance 5512	cevCpuAsa5512 (cevModuleCpuType 229)
Central Processing Unit for Cisco Adaptive Security Appliance 5512 with no Payload Encryption	cevCpuAsa5512K7 (cevModuleCpuType 224)
Central Processing Unit for Cisco Adaptive Security Appliance 5515	cevCpuAsa5515 (cevModuleCpuType 230)
Central Processing Unit for Cisco Adaptive Security Appliance 5515 with no Payload Encryption	cevCpuAsa5515K7 (cevModuleCpuType 225)
Central Processing Unit for Cisco Adaptive Security Appliance 5525	cevCpuAsa5525 (cevModuleCpuType 231)
Central Processing Unit for Cisco Adaptive Security Appliance 5525 with no Payload Encryption	cevCpuAsa5525K7 (cevModuleCpuType 226)
Central Processing Unit for Cisco Adaptive Security Appliance 5545	cevCpuAsa5545 (cevModuleCpuType 232)
Central Processing Unit for Cisco Adaptive Security Appliance 5545 with no Payload Encryption	cevCpuAsa5545K7 (cevModuleCpuType 227)
Central Processing Unit for Cisco Adaptive Security Appliance 5555	cevCpuAsa5555 (cevModuleCpuType 233)
Central Processing Unit for Cisco Adaptive Security Appliance 5555 with no Payload Encryption	cevCpuAsa5555K7 (cevModuleCpuType 228)
CPU for ASA 5580	cevCpuAsa5580 (cevModuleType 200)
CPU for ASA 5585 SSP-10	cevCpuAsa5585Ssp10 (cevModuleCpuType 204)
CPU for ASA 5585 SSP-10 No Payload Encryption	cevCpuAsa5585Ssp10K7 (cevModuleCpuType 205)
CPU for ASA 5585 SSP-20	cevCpuAsa5585Ssp20 (cevModuleCpuType 206)
CPU for ASA 5585 SSP-20 No Payload Encryption	cevCpuAsa5585Ssp20K7 (cevModuleCpuType 207)
CPU for ASA 5585 SSP-40	cevCpuAsa5585Ssp40 (cevModuleCpuType 208)
CPU for ASA 5585 SSP-40 No Payload Encryption	cevCpuAsa5585Ssp40K7 (cevModuleCpuType 209)
CPU for ASA 5585 SSP-60	cevCpuAsa5585Ssp60 (cevModuleCpuType 210)
CPU for ASA 5585 SSP-60 No Payload Encryption	cevCpuAsa5585Ssp60K (cevModuleCpuType 211)

Table 79-3 SNMP Physical Vendor Type Values (continued)

CPU for Cisco ASA Services Module for Catalyst switches	cevCpuAsaSm1 (cevModuleCpuType 222)
CPU for Cisco ASA Services Module with No Payload Encryption for Catalyst switches	cevCpuAsaSm1K7 (cevModuleCpuType 223)
Chassis Cooling Fan in Adapative Security Appliance 5512	cevFanASA5512ChassisFan (cevFan 163)
Chassis Cooling Fan in Adapative Security Appliance 5512 with No Payload Encryption	cevFanASA5512K7ChassisFan (cevFan 172)
Chassis Cooling Fan in Adapative Security Appliance 5515	cevFanASA5515ChassisFan (cevFan 164)
Chassis Cooling Fan in Adapative Security Appliance 5515 with No Payload Encryption	cevFanASA5515K7ChassisFan (cevFan 171)
Chassis Cooling Fan in Adapative Security Appliance 5525	cevFanASA5525ChassisFan (cevFan 165)
Chassis Cooling Fan in Adapative Security Appliance 5525 with No Payload Encryption	cevFanASA5525K7ChassisFan (cevFan 170)
Chassis Cooling Fan in Adapative Security Appliance 5545	cevFanASA5545ChassisFan (cevFan 166)
Chassis Cooling Fan in Adapative Security Appliance 5545 with No Payload Encryption	cevFanASA5545K7ChassisFan (cevFan 169)
Power Supply Fan in Adapative Security Appliance 5545 with No Payload Encryption	cevFanASA5545K7PSFan (cevFan 161)
Power Supply Fan in Adapative Security Appliance 5545	cevFanASA5545PSFan (cevFan 159)
Chassis Cooling Fan in Adapative Security Appliance 5555	cevFanASA5555ChassisFan (cevFan 167)
Chassis Cooling Fan in Adapative Security Appliance 5555 with No Payload Encryption	cevFanASA5555K7ChassisFan (cevFan 168)
Power Supply Fan in Adapative Security Appliance 5555	cevFanASA5555PSFan (cevFan 160)
Power Supply Fan in Adapative Security Appliance 5555 with No Payload Encryption	cevFanASA5555PSFanK7 (cevFan 162)
Fan type for ASA 5580	cevFanASA5580Fan (cevFan 138)
Power supply fan for ASA 5585-X	cevFanASA5585PSFan (cevFan 146)
ASA 5580 4-port GE copper interface card	cevModuleASA5580Pm4xlgeCu (cevModuleASA5580Type 1)
10-Gigabit Ethernet interface	cevPort10GigEthernet (cevPort 315)
Gigabit Ethernet port	cevPortGe (cevPort 109)
Power Supply unit in Adapative Security Appliance 5545	cevPowerSupplyASA5545PSInput (cevPowerSupply 323)
Presence Sensor for Power Supply input in Adaptive Security Appliance 5545	cevPowerSupplyASA5545PSPresence (cevPowerSupply 321)

Table 79-3 SNMP Physical Vendor Type Values (continued)

Power Supply unit in Adapative Security Appliance 5555	cevPowerSupplyASA5555PSInput (cevPowerSupply 324)
Presence Sensor for Power Supply input in Adaptive Security Appliance 5555	cevPowerSupplyASA5555PSPresence (cevPowerSupply 322)
Power supply input for ASA 5580	cevPowerSupplyASA5580PSInput (cevPowerSupply 292)
Power supply input for ASA 5585	cevPowerSupplyASA5585PSInput (cevPowerSupply 304)
Cisco Adaptive Security Appliance (ASA) 5512 Chassis Fan sensor	cevSensorASA5512ChassisFanSensor (cevSensor 120)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5512	cevSensorASA5512ChassisTemp (cevSensor 107)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5512	cevSensorASA5512CPUTemp (cevSensor 96)
Cisco Adaptive Security Appliance (ASA) 5512 with No Payload Encryption Chassis Fan sensor	cevSensorASA5512K7ChassisFanSensor (cevSensor 125)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5512 with No Payload Encryption	cevSensorASA5512K7CPUTemp (cevSensor 102)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5512 with No Payload Encryption	cevSensorASA5512K7PSFanSensor (cevSensor 116)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5512	cevSensorASA5512PSFanSensor (cevSensor 119)
Cisco Adaptive Security Appliance (ASA) 5515 Chassis Fan sensor	cevSensorASA5515ChassisFanSensor (cevSensor 121)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5515	cevSensorASA5515ChassisTemp (cevSensor 98)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5515	cevSensorASA5515CPUTemp (cevSensor 97)
Cisco Adaptive Security Appliance (ASA) 5515 with No Payload Encryption Chassis Fan sensor	cevSensorASA5515K7ChassisFanSensor (cevSensor 126)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5515 with No Payload Encryption	cevSensorASA5515K7CPUTemp (cevSensor 103)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5515 with No Payload Encryption	cevSensorASA5515K7PSFanSensor (cevSensor 115)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5515	cevSensorASA5515PSFanSensor (cevSensor 118)
Cisco Adaptive Security Appliance (ASA) 5525 Chassis Fan sensor	cevSensorASA5525ChassisFanSensor (cevSensor 122)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5525	cevSensorASA5525ChassisTemp (cevSensor 108)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5525	cevSensorASA5525CPUTemp (cevSensor 99)

Table 79-3 SNMP Physical Vendor Type Values (continued)

Cisco Adaptive Security Appliance (ASA) 5525 with No Payload Encryption Chassis Fan sensor	cevSensorASA5525K7ChassisFanSensor (cevSensor 127)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5525 with No Payload Encryption	cevSensorASA5525K7CPUTemp (cevSensor 104)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5525 with No Payload Encryption	cevSensorASA5525K7PSFanSensor (cevSensor 114)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5525	cevSensorASA5525PSFanSensor (cevSensor 117)
Cisco Adaptive Security Appliance (ASA) 5545 Chassis Fan sensor	cevSensorASA5545ChassisFanSensor (cevSensor 123)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5545	cevSensorASA5545ChassisTemp (cevSensor 109)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5545	cevSensorASA5545CPUTemp (cevSensor 100)
Cisco Adaptive Security Appliance (ASA) 5545 with No Payload Encryption Chassis Fan sensor	cevSensorASA5545K7ChassisFanSensor (cevSensor 128)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5545 with No Payload Encryption	cevSensorASA5545K7ChassisTemp (cevSensor 90)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5545 with No Payload Encryption	cevSensorASA5545K7CPUTemp (cevSensor 105)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5545 with No Payload Encryption	cevSensorASA5545K7PSFanSensor (cevSensor 113)
Presence Sensor for Power Supply input in Adaptive Security Appliance 5545 with No Payload Encryption	cevSensorASA5545K7PSPresence (cevSensor 87)
Temperature Sensor for Power Supply Fan in Adapative Security Appliance 5545 with No Payload Encryption	cevSensorASA5545K7PSTempSensor (cevSensor 94)
Sensor for Power Supply Fan in Adapative Security Appliance 5545 with No Payload Encryption	cevSensorASA5545PSFanSensor (cevSensor 89)
Presence Sensor for Power Supply input in Adaptive Security Appliancce 5545	cevSensorASA5545PSPresence (cevSensor 130)
Presence Sensor for Power Supply input in Adaptive Security Appliancce 5555	cevSensorASA5545PSPresence (cevSensor 131)
Temperature Sensor for Power Supply Fan in Adapative Security Appliance 5545	cevSensorASA5545PSTempSensor (cevSensor 92)
Cisco Adaptive Security Appliance (ASA) 5555 Chassis Fan sensor	cevSensorASA5555ChassisFanSensor (cevSensor 124)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5555	cevSensorASA5555ChassisTemp (cevSensor 110)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5555	cevSensorASA5555CPUTemp (cevSensor 101)

Table 79-3 SNMP Physical Vendor Type Values (continued)

Cisco Adaptive Security Appliance (ASA) 5555 with No Payload Encryption Chassis Fan sensor	cevSensorASA5555K7ChassisFanSensor (cevSensor 129)
Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5555 with No Payload Encryption	cevSensorASA5555K7ChassisTemp (cevSensor 111)
Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5555 with No Payload Encryption	cevSensorASA5555K7CPUTemp (cevSensor 106)
Sensor for Chassis Cooling Fan in Adapative Security Appliance 5555 with No Payload Encryption	cevSensorASA5555K7PSFanSensor (cevSensor 112)
Presence Sensor for Power Supply input in Adaptive Security Appliance 5555 with No Payload Encryption	cevSensorASA5555K7PSPresence (cevSensor 88)
Temperature Sensor for Power Supply Fan in Adapative Security Appliance 5555 with No Payload Encryption	cevSensorASA5555K7PSTempSensor (cevSensor 95)
Sensor for Power Supply Fan in Adapative Security Appliance 5555	cevSensorASA5555PSFanSensor (cevSensor 91)
Temperature Sensor for Power Supply Fan in Adapative Security Appliance 5555	cevSensorASA5555PSTempSensor (cevSensor 93)
Sensor type for ASA 5580	cevSensorASA5580FanSensor (cevSensor 76)
Sensor for power supply input for ASA 5580	cevSensorASA5580PSInput (cevSensor 74)
Sensor for power supply fan for ASA 5585-X	cevSensorASA5585PSFanSensor (cevSensor 86)
Sensor for power supply input for ASA 5585-X	cevSensorASA5585PSInput (cevSensor 85)
CPU temperature sensor for ASA 5585 SSP-10	cevSensorASA5585SSp10CPUTemp (cevSensor 77)
CPU temperature sensor for ASA 5585 SSP-10 No Payload Encryption	cevSensorASA5585SSp10K7CPUTemp (cevSensor 78)
CPU temperature sensor for ASA 5585 SSP-20	cevSensorASA5585SSp20CPUTemp (cevSensor 79)
CPU temperature sensor for ASA 5585 SSP-20 No Payload Encryption	cevSensorASA5585SSp20K7CPUTemp (cevSensor 80)
CPU temperature sensor for ASA 5585 SSP-40	cevSensorASA5585SSp40CPUTemp (cevSensor 81)
CPU temperature sensor for ASA 5585 SSP-40 No Payload Encryption	cevSensorASA5585SSp40K7CPUTemp (cevSensor 82)
CPU temperature sensor for ASA 5585 SSP-60	cevSensorASA5585SSp60CPUTemp (cevSensor 83)
CPU temperature sensor for ASA 5585 SSP-60 No Payload Encryption	cevSensorASA5585SSp60K7CPUTemp (cevSensor 84)

Supported Tables in MIBs

Table 79-4 lists the supported tables and objects for the specified MIBs.

Table 79-4 Supported Tables and Objects in MIBs

MIB Name	Supported Tables and Objects
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid, cempMemPoolUsed, cempMemPoolFree, cempMemPoolUsedOvrflw, cempMemPoolHCUsed, cempMemPoolFreeOvrflw, cempMemPoolHCFree
CISCO-ENTITY-SENSOR-EXT-MIB **Note** Not supported on the ASA Services Module.	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
DISMAN-EVENT-MIB	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB **Note** Not supported on the ASA Services Module.	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB **Note** Not supported on the ASA Services Module.	entPhySensorTable
NAT-MIB	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus, cnatAddrBindNumberOfEntries, cnatAddrBindSessionCount

Supported Traps (Notifications)

Table 79-5 lists the supported traps (notifications) and their associated MIBs.

Table 79-5 Supported Traps (Notifications)

Trap and MIB Name	Varbind List	Description
authenticationFailure (SNMPv2-MIB)	—	For SNMP Version 1 or 2, the community string provided in the SNMP request is incorrect. For SNMP Version 3, a report PDU is generated instead of a trap if the auth or priv passwords or usernames are incorrect. The **snmp-server enable traps snmp authentication** command is used to enable and disable transmission of these traps.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	—	The **snmp-server enable traps entity fru-insert** command is used to enable this notification.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	—	The **snmp-server enable traps entity fru-remove** command is used to enable this notification.

Table 79-5 Supported Traps (Notifications) (continued)

ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB) **Note** Not supported on the ASA Services Module.	ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName	The **snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] command is used to enable transmission of the entity threshold notifications. This notification is sent for a power supply failure. The objects sent identify the fan and CPU temperature. The **snmp-server enable traps entity fan-failure** command is used to enable transmission of the fan failure trap. The **snmp-server enable traps entity power-supply-failure** command is used to enable transmission of the power supply failure trap. The **snmp-server enable traps entity chassis-fan-failure** command is used to enable transmission of the chassis fan failure trap. The **snmp-server enable traps entity cpu-temperature** command is used to enable transmission of the high CPU temperature trap. The **snmp-server enable traps entity power-supply-presence** command is used to enable transmission of the power supply presence failure trap. The **snmp-server enable traps entity power-supply-temperature** command is used to enable transmission of the power supply temperature threshold trap. The **snmp-server enable traps entity chassis-temperature** command is used to enable transmission of the chassis ambient temperature trap.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	The **snmp-server enable traps ipsec start** command is used to enable transmission of this trap.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	The **snmp-server enable traps ipsec stop** command is used to enable transmission of this trap.
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions	The **snmp-server enable traps remote-access session-threshold-exceeded** command is used to enable transmission of these traps.

Table 79-5 Supported Traps (Notifications) (continued)

clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Syslog messages are generated. The value of the clogMaxSeverity object is used to decide which syslog messages are sent as traps. The **snmp-server enable traps syslog** command is used to enable and disable transmission of these traps.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	The **snmp-server enable traps connection-limit-reached** command is used to enable transmission of the connection-limit-reached notification. The clogOriginID object includes the context name from which the trap originated.
coldStart (SNMPv2-MIB)	—	The SNMP agent has started. The **snmp-server enable traps snmp coldstart** command is used to enable and disable transmission of these traps.
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	The **snmp-server enable traps cpu threshold rising** command is used to enable transmission of the cpu threshold rising notification. The cpmCPURisingThresholdPeriod object is sent with the other objects.
entConfigChange (ENTITY-MIB)	—	The **snmp-server enable traps entity config-change fru-insert fru-remove** command is used to enable this notification. **Note** This notification is only sent in multimode when a security context is created or removed.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	The linkdown trap for interfaces. The **snmp-server enable traps snmp linkdown** command is used to enable and disable transmission of these traps.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	The linkup trap for interfaces. The **snmp-server enable traps snmp linkup** command is used to enable and disable transmission of these traps.

Table 79-5 Supported Traps (Notifications) (continued)

mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	The **snmp-server enable traps memory-threshold** command is used to enable the memory threshold notification. The mteHotOID is set to cempMemPoolHCUsed. The cempMemPoolName and cempMemPoolHCUsed objects are sent with the other objects.
mteTriggerFired (DISMAN-EVENT-MIB) **Note** Not supported on the ASA Services Module.	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	The **snmp-server enable traps interface-threshold** command is used to enable the interface threshold notification. The entPhysicalName objects are sent with the other objects.
natPacketDiscard (NAT-MIB)	ifIndex	The **snmp-server enable traps nat packet-discard** command is used to enable the NAT packet discard notification. This notification is rate limited for 5 minutes and is generated when IP packets are discarded by NAT because mapping space is not available. The ifIndex gives the ID of the mapped interface.
warmStart (SNMPv2-MIB)	—	The **snmp-server enable traps snmp warmstart** command is used to enable and disable transmission of these traps.

SNMP Version 3

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

- SNMP Version 3 Overview, page 79-15
- Security Models, page 79-16
- SNMP Groups, page 79-16
- SNMP Users, page 79-16
- SNMP Hosts, page 79-16
- Implementation Differences Between the ASA, ASA Services Module, and the Cisco IOS Software, page 79-16

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 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. 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 the credentials for the ASA.

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 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.

Licensing Requirements for SNMP

The following table shows the licensing requirements for this feature:

License Requirement
Base License: Base (DES).
Optional license: Strong (3DES, AES)

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 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 retireval 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.
- The value returned for ifNumber will be larger than the number of interfaces that you can query through SNMP, because ifNumber includes hidden internal interfaces that are not viewable.
- You cannot query for the chassis temperature for the ASA 5585 SSP-40 (NPE).

Configuring SNMP

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

- Enabling SNMP, page 79-18
- Configuring SNMP Traps, page 79-20
- Configuring a CPU Usage Threshold, page 79-21
- Configuring a Physical Interface Threshold, page 79-21
- Using SNMP Version 1 or 2c, page 79-22
- Using SNMP Version 3, page 79-23

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, enter the following command:

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

What to Do Next

See the "Configuring SNMP Traps" section on page 79-20.

Configuring SNMP Traps

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

Command	Purpose
snmp-server enable traps [**all** | **syslog** | **snmp** [*authentication* | *linkup* | *linkdown* | *coldstart* | *warmstart*] | **entity** [*config-change* | *fru-insert* | *fru-remove* | *fan-failure* | *cpu-temperature* | *chassis-fan-failure* | *power-supply-failure*] | *chassis-temperature* | *power-supply-presence* | *power-supply-temperature*] **ikev2** [*start* | *stop*] |**ipsec** [*start* | *stop*] | **remote-access** [*session-threshold-exceeded*]| **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*] **Example:** `hostname(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart` **Note** The **interface-threshold** trap is not supported on the ASASM.	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 standard 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. You need to configure both the **logging history** command and the **snmp-server enable traps syslog** command to generate traps from the syslog MIB. To restore the default enabling of SNMP traps, use the **clear configure snmp-server** command. All other traps are disabled by default. Keywords available in the admin context only: • **connection-limit-reached** • **entity** • **memory-threshold** Traps generated through the admin context only for physically connected interfaces in the system context: • **interface-threshold** All other traps are available in the admin and user contexts in single mode. In multi-mode, the **fan-failure** trap, the **power-supply-failure** trap, and the **cpu-temperature** trap are generated only from the admin context, and not the user contexts (applies only to the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X). If the CPU usage is greater than the configured threshold value for the configured monitoring period, the **cpu threshold rising** trap is generated. 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. **Note** SNMP does not monitor voltage sensors.

What to Do Next

See the "Configuring a CPU Usage Threshold" section on page 79-21.

Configuring a CPU Usage Threshold

To configure the CPU usage threshold, enter the following command:

Command	Purpose
snmp cpu threshold rising *threshold_value monitoring_period* **Example:** `hostname(config)# snmp cpu threshold rising 75% 30 minutes`	Configures the threshold value for a high CPU threshold and the threshold monitoring period. To clear the threshold value and monitoring period of the CPU utilization, use the **no** form of this command. If the **snmp cpu threshold rising** command is not configured, the default for the high threshold level is over 70 percent, and the default for the critical threshold level is over 95 percent. The default monitoring period is set to 1 minute. You cannot configure the critical CPU threshold level, which is maintained at a constant 95 percent. Valid threshold values for a high CPU threshold range from 10 to 94 percent. Valid values for the monitoring period range from 1 to 60 minutes.

What to Do Next

See the "Configuring a Physical Interface Threshold" section on page 79-21.

Configuring a Physical Interface Threshold

To configure the physical interface threshold, enter the following command:

Command	Purpose
snmp interface threshold *threshold_value* **Example:** `hostname(config)# snmp interface threshold 75%` **Note** Not supported on the ASA Services Module.	Configures the threshold value for an SNMP physical interface. To clear the threshold value for an SNMP physical interface, use the **no** form of this command. The threshold value is defined as a percentage of interface bandwidth utilization. Valid threshold values range from 30 to 99 percent. The default value is 70 percent. The **snmp interface threshold** command is available only in the admin context. **Note** Physical interface usage is monitored in single mode and multimode, and traps for physical interfaces in the system context are sent through the admin context. Only physical interfaces are used to compute threshold usage.

What to Do Next

Choose one of the following:

- See the "Using SNMP Version 1 or 2c" section on page 79-22.
- See the "Using SNMP Version 3" section on page 79-23.

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, and identifies the name and IP address of the NMS or SNMP manager that can connect to the ASA. 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 ASA and the NMS. The key is a case-sensitive value up to 32 alphanumeric characters. Spaces are not permitted. The default community-string is public. The ASA 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 ASA and the management station with the same string. The ASA 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 79-16.
		
		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 the credentials configured on the ASA.

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 79-26.

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 79-16. 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, or default passwords exist. For the encryption algorithm, you can specify either the **des**, **3des**, or **aes** keyword. You can also specify which version of the AES encryption algorithm to use: **128**, **192**, or **256**. The *auth-password* argument specifies the authentication user password. The *priv-password* argument specifies the encryption user password.
		
		Note If you forget a password, you cannot recover it and you 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 1 alphanumeric character; however, we recommend that you use at least 8 alphanumeric 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 ASA. 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 ASA and the NMS. The key is a case-sensitive value up to 32 alphanumeric characters. Spaces are not permitted. The default community-string is public. The ASA 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 ASAand the NMS with the same string. The ASAuses 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 79-16.
		
		Note When SNMP Version 3 hosts are configured on the ASA, 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 the credentials configured on the ASA.

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 79-26.

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 ASA or ASASM 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 ASA or ASASM 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 ASA or ASASM 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 ASA or ASASM is not performing as expected, obtain information about network topology and traffic by doing the following:

- For the NMS configuration, obtain the following information:
  - 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 ASA or ASASM 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.

Note For a physical interface that has multiple VLAN interfaces associated with it, be aware 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 79-6 show the differences in SNMP traffic statistics. Example 1 shows the difference in physical and logical output statistics for the **show interface** command and the **show traffic** command. Example 2 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.

Table 79-6 SNMP Traffic Statistics for Physical and VLAN Interfaces

Example 1

```
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
```

Example 2

```
hostname# show interface GigabitEthernet0/0.100
interface GigabitEthernet0/0.100
    vlan 100
    nameif inside
    security-level 100
    ip address 10.7.1.101 255.255.255.0 standby
    10.7.1.102

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
```

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. This section includes the following topics:

- SNMP Syslog Messaging, page 79-27
- SNMP Monitoring, page 79-27

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 to a specified host on a specified interface.

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

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

SNMP Monitoring

To monitor SNMP, enter one of the following commands:

Command	Purpose
show running-config [**default**] **snmp-server**	Shows all SNMP server configuration information.
show running-config snmp-server group	Shows SNMP group configuration settings.
show running-config snmp-server host	Shows configuration settings used by SNMP to control messages and notifications sent to remote hosts.
show running-config snmp-server user	Shows SNMP user-based configuration settings.
show snmp-server engineid	Shows the ID of the SNMP engine configured.
show snmp-server group	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.
show snmp-server statistics	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	Shows the configured characteristics of users.

Examples

The following example shows how to display SNMP server statistics:

```
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
```

The following example shows how to display the SNMP server running configuration:

```
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 79-28
- Configuration Example for SNMP Version 3, page 79-28

Configuration Example for SNMP Versions 1 and 2c

The following example shows how the ASA 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 shows how the ASA 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 77, "Configuring Logging."

Additional References

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

- RFCs for SNMP Version 3, page 79-29
- MIBs, page 79-29
- Application Services and Third-Party Tools, page 79-31

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 ASAby 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, 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. 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 79-7 lists each feature change and the platform release in which it was implemented.

Table 79-7 Feature History for SNMP

Feature Name	Platform Releases	Feature Information
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.
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 introduced or modified the following commands: **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. We modified the following commands: **snmp-server community**, **snmp-server host**.

Table 79-7 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 introduced or modified the following commands: **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
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.
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**.
NAT MIB	8.4(5)	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.