SNMP

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

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.

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.

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/

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

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

In addition, download Cisco OIDs by FTP from the following location:

https://github.com/cisco/cisco-mibs/tree/main/oid

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.

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:

```
ciscoasa(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:

```
ciscoasa(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--
```

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 and the CISCO-ENTITY-VENDORTYPE-OID-MIB includes the OIDs that can be reported in the sysObjectID object in the SNMPv2-MIB, Entity Sensor MIB and Entity Sensor Threshold Ext MIB. You can use this value to identify the model type. The following table lists the sysObjectID OIDs for ASA and ISA models.

Table 2: SNMP Object Identifiers

Product Identifier	sysObjectID	Model Number
ASA Virtual	ciscoASAv (ciscoProducts 1902)	Cisco Adaptive Security Virtual Appliance (ASA virtual)
ASA Virtual System Context	ciscoASAvsy (ciscoProducts 1903)	Cisco Adaptive Security Virtual Appliance (ASA virtual) System Context
ASA Virtual Security Context	ciscoASAvsc (ciscoProducts 1904)	Cisco Adaptive Security Virtual Appliance (ASA virtual) Security Context.
ISA 30004C Industrial Security Appliance	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C with 4 GE Copper Security Context	ciscoProducts 2139	ciscoISA30004Csc
CISCO ISA30004C with 4 GE Copper System Context	ciscoProducts 2140	ciscoISA30004Csy

Product Identifier	sysObjectID	Model Number
ISA 30002C2F Industrial Security Appliance	ciscoProducts 2267	ciscoISA30002C2F
CISCO ISA30002C2F with 2 GE Copper ports + 2 GE Fiber Security Context	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F with 2 GE Copper ports + 2 GE Fiber System Context	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco Industrial Security Appliance (ISA) 30004C Chassis	cevChassis 1677	cevChassisISA30004C
Cisco Industrial Security Appliance (ISA) 30002C2F Chassis	cevChassis 1678	cevChassisISA30002C2F
Central Processing Unit Temperature Sensor for ISA30004C Copper SKU	cevSensor 187	cevSensorISA30004CCpuTempSensor
Central Processing Unit Temperature Sensor for ISA30002C2F Fiber	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
Processor Card Temperature Sensor for ISA30004C Copper SKU	cevSensor 192	cevSensorISA30004CPTS
Processor Card Temperature Sensor for ISA30002C2F Fiber SKU	cevSensor 193	cevSensorISA30002C2FPTS
Power Card Temperature Sensor for ISA30004C Copper SKU	cevSensor 197	cevSensorISA30004CPowercardTS
Power Card Temperature Sensor for ISA30002C2F Fiber SKU	cevSensor 198	cevSensorISA30002C2FPowercardTS
Port Card Temperature Sensor for ISA30004C	cevSensor 199	cevSensorISA30004CPortcardTS
Port Card Temperature Sensor for ISA30002C2F	cevSensor 200	cevSensorISA30002C2FPortcardTS
Central Processing Unit for ISA30004C Copper SKU	cevModuleCpuType 329	cevCpuISA30004C
Central Processing Unit for ISA30002C2F Fiber SKU	cevModuleCpuType 330	cevCpuISA30002C2F
Modules ISA30004C, ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F Industrial Security Appliance Solid State Drive	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64

Product Identifier	sysObjectID	Model Number
Cisco ISA30004C/ISA30002C2F Hardware Bypass	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
FirePOWER 4140 Security Appliance, 1U with embedded security module 36	ciscoFpr4140K9 (ciscoProducts 2293)	FirePOWER 4140
FirePOWER 4120 Security Appliance, 1U with embedded security module 24	ciscoFpr4120K9 (ciscoProducts 2294)	FirePOWER 4120
FirePOWER 4K Fan Bay	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K Power Supply Bay	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Secure Firewall Threat Defense Virtual, VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Threat Defense Virtual, AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

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, ASA virtual, or ASASM SNMP agent. You can use this value to identify the type of component (module, power supply, fan, sensors, CPU, and so on). The following table lists the physical vendor type values for the ASA models.

Table 3: Physical Vendor Type Values

Item	entPhysicalVendorType OID Description
Gigabit Ethernet port	cevPortGe (cevPort 109)
Cisco Adaptive Security Virtual Appliance	cevChassisASAv (cevChassis 1451)

Supported Tables and Objects in MIBs

The following table lists the supported tables and objects for the specified MIBs.

In multi-context mode, these tables and objects provide information for a single context. If you want data across contexts, you need to sum them. For example, to get overall memory usage, sum the cempMemPoolHCUsed values for each context.

Table 4: Supported Tables and Objects in MIBs

MIB Name and OID	Supported Tables and Objects
CISCO-ENHANCED-MEMPOOL-MIB; OID:1.3.6.1.4.1.9.9.221	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid. For a 32-bit memory system, poll using the 32-bit memory counters—cempMemPoolUsed, cempMemPoolFree,cempMemPoolUsedOvrflw, cempMemPoolFreeOvrflw, cempMemPoolLargestFree, cempMemPoolLowestFree, cempMemPoolUsedLowWaterMark, cempMemPoolAllocHit, cempMemPoolAllocMiss, cempMemPoolFreeHit, cempMemPoolFreeMiss, cempMemPoolLargestFreeOvrflw, cempMemPoolLowestFreeOvrflw, cempMemPoolUsedLowWaterMarkOvrflw, cempMemPoolSharedOvrflw. For a 64-bit memory system, poll using the 64-bit memory counters—cempMemPoolHCUsed, cempMemPoolHCFree, cempMemPoolHCLargestFree, cempMemPoolHCLowestFree, cempMemPoolHCUsedLowWaterMark, cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID:1.3.6.1.4.1.9.9.392 **Note** These three MIB OIDs can be used to track why remote access connections fail.	crasNumTotalFailures, crasNumSetupFailInsufResources, crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB; OID:1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB; OID:1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB; OID:1.3.6.1.4.1.9.9.720 **Note** Not supported on the ASA virtual.	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects
DISMAN-EVENT-MIB; OID:1.3.6.1.2.1.88	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB; OID:1.3.6.1.2.1.90	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB; OID: 1.3.6.1.2.1.99 **Note** Provides information related to physical sensors, such as chassis temperature, fan RPM, power supply voltage, etc. Not supported on the ASA virtual platform.	entPhySensorTable

MIB Name and OID	Supported Tables and Objects
NAT-MIB; OID:1.3.6.1.2.1.123	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus
CISCO-PTP-MIB; OID:1.3.6.1.4.1.9.9.760 **Note** Only MIBs corresponding to E2E Transparent Clock mode are supported.	ciscoPtpMIBSystemInfo, cPtpClockDefaultDSTable, cPtpClockTransDefaultDSTable, cPtpClockPortTransDSTable

Supported Traps (Notifications)

The following table lists the supported traps (notifications) and their associated MIBs.

Table 5: Supported Traps (Notifications)

Trap and MIB Name	Varbind List	Description
authenticationFailure (SNMPv2-MIB)	—	For SNMP Version 1 or 2, the community string pr request is incorrect. For SNMP Version 3, a report instead of a trap if the auth or priv passwords or use The **snmp-server enable traps snmp authenticati** to enable and disable transmission of these traps.
bgpBackwardTransition	bgpPeerLastError, bgpPeerState	The **snmp-server enable traps peer-flap** comman transmission of BGP peer-flap related trap.
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged, ccmHistoryEventTerminalType	The **snmp-server enable traps config** command is transmission of this trap.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL -MIB)	entPhysicalContainedIn	The **snmp-server enable traps entity fru-insert** c enable this notification.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL -MIB)	entPhysicalContainedIn	The **snmp-server enable traps entity fru-remove** enable this notification.

Trap and MIB Name	Varbind List	Description
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT -MIB)	entPhysicalName, entPhysicalDescr, entPhySensorValue, entPhySensorType, ceSensorExtThresholdValue	The **snmp-server enable traps entity** [**power-** **fan-failure** | **cpu-temperature**] command is use of the entity threshold notifications. This notifi supply failure. The objects sent identify the fan The **snmp-server enable traps entity fan-failu** enable transmission of the fan failure trap.This t Firepower 2100 series. The **snmp-server enable traps entity power-s** is used to enable transmission of the power sup does not apply to the Firepower 2100 series. The **snmp-server enable traps entity chassis-** used to enable transmission of the chassis fan f The **snmp-server enable traps entity cpu-tem** used to enable transmission of the high CPU te does not apply to the Firepower 2100 series. The **snmp-server enable traps entity power-su** is used to enable transmission of the power supp The **snmp-server enable traps entity power-s** command is used to enable transmission of the p threshold trap. The **snmp-server enable traps entity chassis-** is used to enable transmission of the chassis am This trap does not apply to the Firepower 2100 The **snmp-server enable traps entity accelera** command is used to enable transmission of the temperature trap.
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunLifeTime	The **snmp-server enable traps ikev2 start** con transmission of ikev2 start trap.
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunActiveTime	The **snmp-server enable traps ikev2 stop** con transmission of ikev2 stop trap.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR -MIB)	cipSecTunLifeTime, cipSecTunLifeSize	The **snmp-server enable traps ipsec start** con transmission of this trap.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR -MIB)	cipSecTunActiveTime	The **snmp-server enable traps ipsec stop** com transmission of this trap.
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	The **snmp-server enable traps config** comma transmission of this trap.

Trap and MIB Name	Varbind List	Description
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 e these traps.
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	The **snmp-server enable traps failover-state** comm transmission of failover-state trap.
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Syslog messages are generated. The value of the clogMaxSeverity object is used to messages are sent as traps. The **snmp-server enable traps syslog** command i disable transmission of these traps.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE -LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	The **snmp-server enable traps connection-limit-** used to enable transmission of the connection-limit- The clogOriginID object includes the context name originated.
coldStart (SNMPv2-MIB)	—	The SNMP agent has started. The **snmp-server enable traps snmp coldstart** co enable and disable transmission of these traps.
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	The **snmp-server enable traps cpu threshold risi** to enable transmission of the CPU threshold rising cpmCPURisingThresholdPeriod object is sent with
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	The **snmp-server enable traps cluster-state** comm transmission of cluster-state trap.
entConfigChange (ENTITY-MIB)	—	The **snmp-server enable traps entity config-char fru-remove** command is used to enable this notific **Note** This notification is only sent in multim context is created or removed.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	The linkdown trap for interfaces. The **snmp-server enable traps snmp linkdown** c 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** comm and disable transmission of these traps.

Trap and MIB Name	Varbind List	Description
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	The **snmp-server enable traps memory-thres** to enable the memory threshold notification. Th cempMemPoolHCUsed. The cempMemPoolNa cempMemPoolHCUsed objects are sent with th
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	The **snmp-server enable traps interface-thre** to enable the interface threshold notification. T objects are sent with the other objects.
natPacketDiscard (NAT-MIB)	ifIndex	The **snmp-server enable traps nat packet-dis** to enable the NAT packet discard notification. T limited for 5 minutes and is generated when IP NAT because mapping space is not available. T of the mapped interface.
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	The **snmp-server enable traps peer-flap** comm transmission of OSPF peer-flap related trap.
warmStart (SNMPv2-MIB)	—	The **snmp-server enable traps snmp warmsta** enable and disable transmission of these traps.

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 the following table 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 6: SNMP Traffic Statistics for Physical and VLAN Interfaces

Example 1

```
ciscoasa# 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

ciscoasa# 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

```
ciscoasa# show interface GigabitEthernet0/0
interface GigabitEthernet0/0.100
vlan 100
nameif inside
security-level 100
ip address 10.7.1.101 255.255.255.0 standby

ciscoasa# 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 Appli
IF-MIB::ifInOctets.9 = Counter32: 126318
```

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, 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.

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 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

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.
- 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 Firewall 3100 , 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.
- 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.

Troubleshooting Tips

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

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

- To capture syslog messages from SNMP and have them appear on the ASA console, enter the following commands:

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

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

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(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 and to the SNMP process, enter the following commands:

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

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

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

- If the ASA 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
  - Issue the following commands:

show block

show interface

show process

show cpu

show vm

- 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 interfaces, you might also need to permit ICMP traffic from the remote SNMP server using the **icmp permit** command.
- When doing SNMP walk operations, the ASA will query memory information from the MEMPOOL_DMA and MEMPOOL_GLOBAL_SHARED pools. This can result in SNMP-related CPU hogs causing packet drops. To mitigate this issue, avoid polling the OIDs that relate to the Global Shared pool using the **no snmp-server enable oid** command. When disabled, the mempool OIDs would return 0 bytes.
- When you use SNMPGET with a large number of OID's in a single request for polling ASP drop counters requires repeated polling of ASP drop counters that results in higher CPU usage. Hence, we recommended that you identify important counters to monitor and use SNMPGET on each counter to get these values such that there is limited cpu impact.
- For additional troubleshooting information, see the following URL: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

Configure SNMP

This section describes how to configure SNMP.

Procedure

Step 1 Enable the SNMP Agent and SNMP server.

Step 2 Configure SNMP traps.

Step 3 Configure SNMP Version 1 and 2c parameters or SNMP Version 3 parameters.

Enable the SNMP Agent and SNMP Server

To enable the SNMP agent and SNMP server, perform the following steps:

Procedure

Enable the SNMP agent and SNMP server on the ASA. By default, the SNMP server is enabled.

snmp-server enable

Example:

```
ciscoasa(config)# snmp-server enable
```

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

Send individual traps, sets of traps, or all traps to the NMS.

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature** **l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

Example:

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

This command 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.

Traps 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.

The **config** trap enables the ciscoConfigManEvent notification and the ccmCLIRunningConfigChanged notification, which are generated after you have exited configuration mode.

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.

Some traps are not applicable to certain hardware models. Use ? in place of a trap keyword to determine which traps are available for your device. For example:

- The Firepower 1000 series supports the following entity traps only: **chassis-temperature**, **config-change**, and **cpu-temperature**.

Note SNMP does not monitor voltage sensors.

Configure a CPU Usage Threshold

To configure a CPU usage threshold, perform the following steps:

Procedure

Configure the threshold value for a high CPU threshold and the threshold monitoring period.

snmp cpu threshold rising *threshold_value monitoring_period*

Example:

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

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.

Configure a Physical Interface Threshold

To configure the physical interface threshold, perform the following steps:

Procedure

Configure the threshold value for an SNMP physical interface.

snmp interface threshold *threshold_value*

Example:

```
ciscoasa(config)# snmp interface threshold 75%
```

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.

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.

Configure Parameters for SNMP Version 1 or 2c

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

Procedure

Step 1 Specify the recipient of an SNMP notification, indicate the interface from which traps are sent, and identify the name and IP address of the NMS or SNMP manager that can connect to the ASA.

snmp-server host {*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

Example:

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

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 long. Spaces are not permitted. The default community string is public. The ASA uses this key to determine whether or not 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 do not respond to requests with an invalid community string. However, if SNMP monitoring is through the management interface instead of the diagnostic interface, polling takes place without ASA validating the community string. After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible. The encrypted community string is always generated by the ASA; you normally enter the clear text form.

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

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 Set the community string, which is for use *only* with SNMP Version 1 or 2c.

snmp-server community *community-string*

Example:

```
ciscoasa(config)# snmp-server community onceuponatime
```

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 Set the SNMP server location or contact information.

snmp-server [**contact** | **location**] *text*

Example:

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

The *text* argument specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Step 4 Set the listening port for SNMP requests.

snmp-server listen-port *lport*

Example:

```
ciscoasa(config)# snmp-server lport 192
```

The *lport* argument is the port on which incoming requests are accepted. The default listening port is 161. The **snmp-server listen-port** command is only available in admin context, and is not available in the system context. If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Configure Parameters for SNMP Version 3

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

Procedure

Step 1 Specify a new SNMP group, which is for use *only* with SNMP Version 3.

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

Example:

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

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. 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 Configure a new user for an SNMP group, which is for use only with SNMP Version 3.

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

Example:

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(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
```

The username argument is the name of the user on the host that belongs to the SNMP agent. Enter up to 32 characters for the username. The name must begin with a letter. Valid characters include letters, numbers, _ (underscore), . (period), @ (at sign), and - (hyphen).

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 **engineID** keyword is optional and specifies the engineID of the ASA which was used to localize the user's authentication and encryption information. The engineID argument must specify a valid ASA engineID.

The **encrypted** keyword specifies the password in encrypted format. Encrypted passwords must meet the following requirements.

- Must be in hexadecimal format.
- Must contain a minimum of 8 characters and a maximum of 80 characters.

- Must contain only letters, numbers, and the following characters: ~`!@#%^&*()_-+{}[]|\:;"'<,>./
- Must not contain the following symbols: $ (dollar sign), ? (question mark), or = (equals sign).
- Must contain at least five different characters.
- Must not contain too many consecutively incrementing or decrementing numbers or letters. For example, the string "12345" has four such characters, and the string "ZYXW" has three. If the total number of such characters exceeds a certain limit (typically more than around 4-6 such occurrences), the simplicity check will fail.

  Note The consecutively incrementing or decrementing character count is not reset when non-incrementing or decrementing characters are used in between. For example, abcd&!21 will fail the password check, but abcd&!25, will not.

The **auth** keyword specifies which authentication level (**sha**, **sha224**, **sha256**, or **sha384**) 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 the **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.

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 SHA, SHA-224, SHA-256, or SHA-384. 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.

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.

If you enter a user on the control/active unit with the **encrypted** keyword, an error message appears to inform you that the SNMPv3 user commands will not be replicated. This behavior also means that existing SNMPv3 user and group commands are not cleared during replication.

For example, a control/active unit using commands entered with encrypted keys:

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

For example, a data unit during cluster replication (appears only if an **snmp-server user** commands exist in the configuration):

```
ciscoasa(cfg-cluster)#
```

```
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

Step 3 Specify the recipient of an SNMP notification. Indicate the interface from which traps are sent. Identify the name and IP address of the NMS or SNMP manager that can connect to the ASA.

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

Example:

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

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 NMS with the same string. The ASA uses the specified string and do not respond to requests with an invalid community string. After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible. The encrypted community string is always generated by the ASA; you normally enter the clear text form.

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

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 Set the SNMP server location or contact information.

snmp-server [**contact** | **location**] *text*

Example:

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

The *text* argument specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Step 5 Set the listening port for SNMP requests.

snmp-server listen-port *lport*

Example:

```
ciscoasa(config)# snmp-server lport 192
```

The *lport* argument is the port on which incoming requests are accepted. The default listening port is 161. The **snmp-server listen-port** command is only available in admin context, and is not available in the system context. If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Configure a Group of Users

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

Procedure

Configure an SNMP user list.

snmp-server user-list *list_name* **username** *user_name*

Example:

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

The *listname* argument specifies the name of the user list, which may be up to 33 characters long. The **username** *user_name* keyword-argument pair specifies the users who may be configured in the user list. You configure the users in the user list with the **snmp-server user** *username* command, which is available only if you are using SNMP Version 3. The user list must have more than one user in it and can be associated with a hostname or a range of IP addresses.

Associate Users with a Network Object

To associate a single user or a group of users in a user list with a network object, perform the following steps:

Procedure

Associate a single user or a group of users in a user list with a network object.

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

Example:

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

The *net_obj_name* argument specifies the interface network object name with which a user or group of users is associated.

The **trap** keyword specifies that only traps can be sent, and that this host is not allowed to browse (poll). SNMP traps are enabled by default.

The **poll** keyword specifies that the host is allowed to browse (poll), but no traps can be sent.

The **community** keyword specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. You can use this keyword only for SNMP Version 1 or 2c. The *community-string* argument specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters.

The **version** keyword sets the SNMP notification version to Version 1, 2c, or 3 to use for sending traps and accepting requests (polling). The default version is 1.

The *username* argument specifies the name of the user if you are using SNMP Version 3.

The **user-list** *list_name* keyword-argument pair specifies the name of the user list.

The **udp-port** *port* keyword-argument pair specifies that SNMP traps must be sent to an NMS host on a non-default port and sets the UDP port number of the NMS host. The default UDP port is 162.

Monitoring SNMP

See the following commands for monitoring SNMP.

- **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.

Examples

The following example shows how to display SNMP server statistics:

```
ciscoasa(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:

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

Examples for SNMP

The following section provides examples that you can use as reference for all SNMP versions.

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:

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

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:

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

History for SNMP

Table 7: 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.
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**.

Feature Name	Version	Description
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.
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**.

Feature Name	Version	Description
VPN-related MIBs	9.0(1)	An updated version of the CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB has been implemented to support the next generation encryption feature. The following MIBs have been enabled for the ASASM: • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	Support for the following MIB was added: CISCO-TRUSTSEC-SXP-MIB.
SNMP OIDs	9.1(1)	Five new SNMP Physical Vendor Type OIDs have been added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
NAT MIB	9.1(2)	Added the cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support the xlate_count and max_xlate_count entries, which are the equivalent to allowing polling using the **show xlate count** command.
SNMP hosts, host groups, and user lists	9.1(5)	You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We introduced or modified the following commands: **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
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.

Feature Name	Version	Description
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 command: **snmp-server enable traps**.
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.
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 modified the following command: **show snmp-server host**.
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 modified the following command: **snmp-server enable traps entity**.
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.

Feature Name	Version	Description
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 command: **snmp-server host** **Note** The **snmp-server host-group** command does not support IPv6.
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. New or modified command: **snmp-server enable oid**
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. We did not modify any commands.
SNMPv3 Authentication	9.14(1)	You can now use SHA-256 HMAC for user authentication. New/Modified commands: **snmp-server user**
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.

Feature Name	Version	Description
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 commands: **snmp-server user**
SNMP over IPv6	9.17(1)	The **snmp-server host-group** command now supports IPv6 host, range, and subnet objects.
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**