Simple Network Management Protocol

- Simple Network Management Protocol Support, on page 1
- SNMP Configuration Task Flow, on page 21
- SNMP Trap Settings, on page 36
- SNMP Trace Configuration, on page 39
- Troubleshooting SNMP, on page 40

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes and routers. As part of the TCP/IP suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

You use the serviceability GUI to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. The SNMP settings that you configure apply to the local node; however, if your system configuration supports clusters, you can apply settings to all servers in the cluster with the "Apply to All Nodes" option in the SNMP configuration windows.

Tip Unified Communications Manager only: SNMP configuration parameters that you specified in Cisco Unified CallManager or Unified Communications Manager 4.X do not migrate during a Unified Communications Manager 6.0 and later upgrade. You must perform the SNMP configuration procedures again in Cisco Unified Serviceability.

SNMP supports IPv4 and IPv6, the CISCO-CCM-MIB includes columns and storage for both IPv4 and IPv6 addresses, preferences, and so on.

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device - A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  Unified Communications Manager and IM and Presence Service only: In a configuration that supports clusters, the first node in the cluster acts as the managed device.

- Agent - A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  The master agent and subagent components are used to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few Management Information Base (MIB) variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Unified Communications Manager subagent interacts with the local Unified Communications Manager only. The Unified Communications Manager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

  The IM and Presence Service subagent interacts with the local IM and Presence Service only. The IM and Presence Service subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- Network Management System (NMS) - An SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. The following NMSs are supported:
  - CiscoWorks LAN Management Solution
  - HP OpenView
  - Third-party applications that support SNMP and Unified Communications Manager SNMP interfaces

SNMP Management Information Base

SNMP allows access to the Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

Observe the following limitations:

- Unified Communications Manager does not support CISCO-UNITY-MIB.
- Cisco Unity Connection does not support CISCO-CCM-MIB.
- IM and Presence Service does not support CISCO-CCM-MIB and CISCO-UNITY-MIB.

The SNMP extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In case of a cluster configuration, the SNMP extension

agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables the SNMP managed device to advertise themself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

Note The CISCO-CDP-MIB depends on the presence of the following MIBs: CISCO-SMI, CISCO-TC, CISCO-VTP-MIB.

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun

- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

Table 1: SYSAPPL-MIB Commands

Command	Description
Device-Related Queries	
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.
sysApplElmPastRunUser	Provides the process owner's login name (for example, root).
Memory, Storage, and CPU-Related Queries	
sysApplElmPastRunMemory	Provides the last-known total amount of real system memory measured in kilobytes that was allocated to this process before it terminated.
sysApplElmtPastRunCPU	Provides the last known number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may increment by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallElmtCurSizeLow	Provides the current file size modulo 2^32 bytes. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplInstallElmtSizeLow	Provides the installed file size modulo 2^32 bytes. This is the size of the file on disk immediately after installation. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplElmRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.

sysApplElmRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
Process-Related Queries	
sysApplElmtRunState	Provides the current state of the running process. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).
sysApplElmtRunNumFiles	Provides the number of regular files currently opened by the process. Transport connections (sockets) should *not* be included in the calculation of this value, nor should operating-system-specific special file types.
sysApplElmtRunTimeStarted	Provides the time the process was started.
sysApplElmtRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.
sysApplElmtPastRunInstallID	Provides the index into the installed element table. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a previously executed process.
sysApplElmtPastRunUser	Provides the process owner's login name (for example, root).
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplRunStarted	Provides the date and time that the application was started.
sysApplElmtRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.

Software Component-Related Queries	
sysApplInstallPkgProductName	Provides the name that the manufacturer assigned to the software application package.
sysApplElmtRunParameters	Provides the starting parameters for the process.
sysApplElmtRunName	Provides the full path and filename of the process. For example, '/opt/MYYpkg/bin/myyproc' would be returned for process 'myyproc' whose execution path is 'opt/MYYpkg/bin/myyproc'.
sysApplInstallElmtName	Provides the name of this element, which is contained in the application.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplInstallElmtPath	Provides the full path to the directory where this element is installed. For example, the value would be '/opt/EMPuma/bin' for an element installed in the directory '/opt/EMPuma/bin'. Most application packages include information about the elements that are contained in the package. In addition, elements are typically installed in subdirectories under the package installation directory. In cases where the element path names are not included in the package information itself, the path can usually be determined by a simple search of the subdirectories. If the element is not installed in that location and no other information is available to the agent implementation, then the path is unknown and null is returned.

sysApplMapInstallPkgIndex	Provides the value of this object and identifies the installed software package for the application of which this process is a part. Provided that the parent application of the process can be determined, the value of this object is the same value as the sysApplInstallPkgIndex for the entry in the sysApplInstallPkgTable that corresponds to the installed application of which this process is a part. If, however, the parent application cannot be determined (for example, the process is not part of a particular installed application), the value for this object is then '0', signifying that this process cannot be related back to an application, and in turn, an installed software package.
sysApplElmtRunInstallID	Provides the index into the sysApplInstallElmtTable. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a running instance. If this process cannot be associated with an installed executable, the value should be '0'.
sysApplRunCurrentState	Provides the current state of the running application instance. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5). This value is based on an evaluation of the running elements of this application instance (see sysApplElmRunState) and their Roles as defined by sysApplInstallElmtRole. An agent implementation may detect that an application instance is in the process of exiting if one or more of its REQUIRED elements are no longer running. Most agent implementations will wait until a second internal poll is completed to give the system time to start REQUIRED elements before marking the application instance as exiting.
sysApplInstallPkgDate	Provides the date and time this software application was installed on the host.
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.

sysApplInstallElmtType	Provides the type of element that is part of the installed application.
Date/Time-Related Queries	
sysApplElmtRunCPU	The number of centi-seconds of the total system CPU resources consumed by this process **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallPkgDate	Provides the date and time this software application is installed on the host.
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplRunStarted	Provides the date and time that the application was started.

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

Table 2: MIB-II Commands

Command	Description
Device-Related Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully qualified domain name of the node. If the name is unknown, the value is the zero-length string.

sysDescr	Provides a textual description of the entity. This value should include the full name and version identification of the system hardware type, software operating-system, and networking software.
SNMP Diagnostic Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully-qualified domain name of the node. If the name is unknown, the value is the zero-length string.
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.
snmpInTotalReqVars	Provides the total number of MIB objects that were retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpOutPkts	Provides the total number of SNMP Messages that were passed from the SNMP entity to the transport service.
sysServices	Provides a value that indicates the set of services that this entity potentially offers. The value is a sum. This sum initially takes the value zero, then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which is a host offering application services would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). **Note** In the context of the Internet suite of protocols, calculate: layer 1 physical (for example, repeaters), layer 2 datalink/subnetwork (for example, bridges), layer 3 internet (supports IP), layer 4 end-to-end (supports TCP), layer 7 applications (supports SMTP). For systems including OSI protocols, you can also count layers 5 and 6.

snmpEnableAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** We strongly recommend that this object be stored in nonvolatile memory so that it remains constant across reinitializations of the network management system.
Syslog-Related Queries	
snmpEnabledAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** Cisco strongly recommends that this object be stored in a nonvolatile memory so that it remains constant across reinitializations of the network management system.
Date/Time-Related Queries	
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and the installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

Table 3: HOST-RESOURCES MIB Commands

Command	Description
Device-Related Queries	

hrFSMountPoint	Provides the path name of the root of this file system.
hrDeviceDescr	Provides a textual description of this device, including the device manufacturer and revision, and optionally, the serial number.
hrStorageDescr	Provides a description of the type and instance of the storage.
Memory, Storage, and CPU Related Queries	
hrMemorySize	Provides the amount of physical read-write main memory, typically RAM, that the host contains.
hrStorageSize	Provides the size of the storage, in units of hrStorageAllocationUnits.This object is writable to allow remote configuration of the size of the storage area in those cases where such an operation makes sense and is possible on the underlying system. For example, you can modify the amount of main memory allocated to a buffer pool or the amount of disk space allocated to virtual memory.
Process-Related Queries	
hrSWRunName	Provides a textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software is installed locally, it must be the same string as used in the corresponding hrSWInstalledName.
hrSystemProcesses	Provides the number of process contexts that are currently loaded or running on this system.
hrSWRunIndex	Provides a unique value for each piece of software that is running on the host. Wherever possible, use the native, unique identification number of the system.
Software Component-Related Queries	
hrSWInstalledName	Provides a textual description of this installed piece of software, including the manufacturer, revision, the name by which it is commonly known, and optionally, the serial number.
hrSWRunPath	Provides a description of the location of long-term storage (for example, a disk drive) from which this software was loaded.
Date/Time-Related Queries	
hrSystemDate	Provides the host local date and time of day.

hrFSLastPartialBackupDate	Provides the last date at which a portion of this file system was copied to another storage device for backup. This information is useful for ensuring that backups are being performed regularly. If this information is not known, then this variable will have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Note The CISCO-SYSLOG-MIB is dependent on the presence of the CISCO-SMI MIB.

Table 4: CISCO-SYSLOG-MIB Commands

Command	Description
Syslog-Related Queries	
clogNotificationEnabled	Indicates whether clogMessageGenerated notifications will be sent when the device generates a syslog message. Disabling notifications does not prevent syslog messages from being added to the clogHistoryTable.
clogMaxSeverity	Indicates which syslog severity levels will be processed. The agent will ignore any syslog message with a severity value greater than this value. **Note** Severity numeric values increase as their severity decreases. For example, error (4) is more severe than debug (8).

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the Unified Communications Manager and its associated devices, such as phones, gateways, and so on, that are

visible on this Unified Communications Manager node. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

SNMP supports IPv4 and IPv6, the CISCO-CCM-MIB includes columns and storage for both IPv4 and IPv6 addresses, preferences, and so on.

Note Unified Communications Manager supports this MIB in Unified Communications Manager systems. IM and Presence Service and Cisco Unity Connection do not support this MIB.

To view the support lists for the CISCO-CCM-MIB and MIB definitions, the MIB dependencies and MIB contents, including obsolete objects, across Unified Communications Manager releases, go to the following link: https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2 .

Dynamic tables get populated only if the Cisco CallManager service is up and running (or the local Cisco CallManager service in case of a Unified Communications Manager cluster configuration); static tables get populated when the Cisco CallManager SNMP Service is running.

Table 5: Cisco-CCM-MIB Dynamic Tables

Table(s)	Contents
ccmTable	This table stores the version and installation ID for the local Unified Communications Manager. The table also stores information about all the Unified Communications Manager in a cluster that the local Unified Communications Manager knows about but shows “unknown” for the version detail. If the local Unified Communications Manager is down, the table remains empty, except for the version and installation ID values.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match the Unified Communications Manager/RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone. The ccmPhoneExtnTable uses a combined index, ccmPhoneIndex and ccmPhoneExtnIndex, for relating the entries in the ccmPhoneTable and ccmPhoneExtnTable.
ccmCTIDevice, ccmCTIDeviceDirNum	The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Unified Communications Manager MIB get updated.
ccmSIPDevice	The CCMSIPDeviceTable stores each SIP trunk as one device.

Table(s)	Contents
ccmH323Device	The ccmH323DeviceTable contains the list of H.323 devices for which Unified Communications Manager contains information (or the local Unified Communications Manager in case of a cluster configuration). For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Unified Communications Manager. Unified Communications Manager generates the H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H.323 trunk information.
ccmVoiceMailDevice, ccmVoiceMailDirNum	For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable includes one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisc MIB get updated.
ccmGateway	The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively. Unified Communications Manager generates alarms at the device or port level. The ccmGatewayTable, based on CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track the number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports. Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.
ccmMediaDeviceInfo	The table contains a list of all media devices which have tried to register with the local Unified Communications Manager at least once.
ccmGroup	This table contains the Unified Communications Manager groups in a Unified Communications Manager cluster.
ccmGroupMapping	This table maps all Unified Communications Manager's in a cluster to a Unified Communications Manager group. The table remains empty when the local Unified Communications Manager node is down.

Table 6: CISCO-CCM-MIB Static Tables

Table(s)	Content
ccmProductType	The table contains the list of product types that are supported with Unified Communications Manager (or cluster, in case of a Unified Communications Manager cluster configuration), including phone types, gateway types, media device types, H.323 device types, CTI device types, voice-messaging device types, and SIP device types.
ccmRegion, ccmRegionPair	ccmRegionTable contains the list of all geographically separated regions in a Cisco Communications Network (CCN) system. The ccmRegionPairTable contains the list of geographical region pairs for a Unified Communications Manager cluster. Geographical region pairs are defined by Source region and Destination region.
ccmTimeZone	The table contains the list of all-time zone groups in a Unified Communications Manager cluster.
ccmDevicePool	The tables contains the list of all device pools in a Unified Communications Manager cluster. Device pools are defined by Region, Date/Time Group, and Unified Communications Manager Group.

Note 'The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that are described.

CISCO-UNITY-MIB

The CISCO-UNITY-MIB uses the Connection SNMP Agent to get information about Cisco Unity Connection.

To view the CISCO-UNITY-MIB definitions, go to the following link and click **SNMP V2 MIBs**:

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

Note Cisco Unity Connection supports this MIB. Unified Communications Manager and IM and Presence Service do not support this MIB.

The Connection SNMP Agent supports the following objects.

Table 7: CISCO-UNITY-MIB Objects

Object	Description
ciscoUnityTable	This table contains general information about the Cisco Unity Connection servers such as hostname and version number.
ciscoUnityPortTable	This table contains general information about the Cisco Unity Connection voice messaging ports.
General Unity Usage Info objects	This group contains information about the capacity and utilization of the Cisco Unity Connection voice messaging ports.

SNMP Configuration Requirements

The system provides no default SNMP configuration. You must configure SNMP settings after installation to access MIB information. Cisco supports SNMP V1, V2c, and V3 versions.

SNMP agent provides security with community names and authentication traps. You must configure a community name to access MIB information. The following table provides the required SNMP configuration settings.

Table 8: SNMP Configuration Requirements

Configuration	Cisco Unified Serviceability Page
V1/V2c Community String	**SNMP** > **V1/V2c** > **Community String**
V3 Community String	**SNMP** > **V3** > **User**
System Contact and Location for MIB2	**SNMP** > **SystemGroup** > **MIB2 System Group**
Trap Destinations (V1/V2c)	**SNMP** > **V1/V2c** > **Notification Destination**
Trap Destinations (V3)	**SNMP** > **V3** > **Notification Destination**

SNMP Version 1 Support

SNMP Version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In the serviceability GUI, you configure SNMPv1 support in the **V1/V2c Configuration** window.

SNMP Version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in

SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In the serviceability GUI, you configure SNMPv2c support in the **V1/V2c Configuration** window.

SNMP Version 3 Support

SNMP Version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the requested objects). To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Note From Release 12.5(1)SU1 onwards, the MD5 or DES encryption methods are not supported in Unified Communications Manager. You can choose either SHA or AES as the authentication protocols while adding an SNMPv3 user.

Instead of using community strings like SNMPv1 and v2, SNMPv3 uses SNMP users.

In the serviceability GUI, you configure SNMPv3 support in the **V3Configuration** window.

SNMP Services

The services in the following table support SNMP operations.

Note
SNMP Master Agent serves as the primary service for the MIB interface. You must manually activate Cisco CallManager SNMP service; all other SNMP services should be running after installation.

Table 9: SNMP Services

MIB	Service	Window
CISCO-CCM-MIB	Cisco CallManager SNMP service	**Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**. Choose a server; then, choose Performance and Monitoring category.

MIB	Service	Window
SNMP Agent	SNMP Master Agent	**Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category. **CiscoUnifiedIM and Presence Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category.
CISCO-CDP-MIB	CiscoCDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
Hardware MIBs	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**Cisco Unity Connection Serviceability** > **Tools** > **Service Management.** Choose a server; then, choose Base Services category.

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the Unified Communications Manager or Cisco Unity Connection network. Do not stop the services unless your technical support team tells you to do so.

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMPv1 and v2c only.

SNMPv3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In the serviceability GUI, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination, whereas informs do receive acknowledgments. You configure the notification destinations by using the SNMP Notification Destination Configuration windows in the serviceability GUI.

Note Unified Communications Manager supports SNMP traps in Unified Communications Manager and IM and Presence Service systems.

For SNMP notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, alarms and system level log messages get sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages get logged locally in the syslog files and also get converted into SNMP traps/notifications.

The following list contains Unified Communications Manager SNMP trap/inform messages that are sent to a configured trap destination:

- Unified Communications Manager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

Tip Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string/user correctly.

You configure the SNMP trap destination by choosing **SNMP** > **V1/V2** > **Notification Destination** or **SNMP** > **V3** > **Notification Destination** in the serviceability GUI.

The following table provides information about trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in the table by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note All the parameters that are listed in the table are part of CISCO-CCM-MIB except for the last two parameters. The last two, clogNotificationsEnabled and clogMaxSeverity, comprise part of CISCO-SYSLOG-MIB.

For IM and Presence Service, you configure only clogNotificationsEnabled and clogMaxSeverity trap/inform parameters on the NMS.

Table 10: Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Although you can configure a CiscoATA 186 device as a phone in Cisco Unified Communications Manager Administration, when Unified Communications Manager sends SNMP traps for the CiscoATA device, it sends a gateway type trap; for example, ccmGatewayFailed.	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.
ccmQualityReportAlarmEnable	True	This trap gets generated only if the CiscoExtended Functions service is activated and running on the server, or, in the case of a cluster configuration (Unified Communications Manager only), on the local Unified Communications Manager server. ccmQualityReport	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when applications generate a syslog message with at least a warning severity level.

SFTP Server Support

For internal testing, we use the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Table 11: SFTP Server Support

SFTP Server	Support Description
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These SFTP servers from a technology partner are third-party provided and third-party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible.
SFTP Server from another Third Party	These SFTP servers are provided by a third party and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

SNMP Configuration Task Flow

Complete these tasks to configure the Simple Network Management Protocol. Make sure that you know which SNMP version you are going to configure as the tasks may vary. You can choose from SNMP V1, V2c, or V3..

Before you begin

Install and configure the SNMP Network Management System.

Procedure

	Command or Action	Purpose
Step 1	Activate SNMP Services, on page 22	Confirm that essential SNMP services are running.
Step 2	Complete one of the following tasks, according to your SNMP version:	For SNMP V1 or V2, configure a community string.

	Command or Action	Purpose
	• Configure SNMP Community String, on page 23 • Configure an SNMP User, on page 25	For SNMP V3, configure an SNMP User.
Step 3	Get Remote SNMP Engine ID, on page 28	For SNMP V3, obtain the address of the remote SNMP engine, which is required in Notification Destination configuration. **Note** This procedure is mandatory for SNMP V3, but is optional for SNMP V1 or V2c.
Step 4	Configure SNMP Notification Destination, on page 29	For all SNMP versions, configure a Notification Destination for SNMP Traps and Informs.
Step 5	Configure MIB2 System Group, on page 33	Configure a system contact and system location for the MIB-II system group.
Step 6	CISCO-SYSLOG-MIB Trap Parameters, on page 34	Configure trap settings for CISCO-SYSLOG-MIB.
Step 7	CISCO-CCM-MIB Trap Parameters, on page 35	Unified Communications Manager only: Configure trap settings for CISCO-CCM-MIB.
Step 8	Restart SNMP Master Agent, on page 35	After completing your SNMP configuration, restart the SNMP Master Agent.
Step 9	On the SNMP Network Management System, configure the Unified Communications Manager trap parameters.	

Activate SNMP Services

Use this procedure to ensure that SNMP Services are up and running.

Procedure

Step 1 Log in to Cisco Unified Serviceability.

Step 2 Confirm that the **Cisco SNMP Master Agent** network service is running. The service is on by default.

a) Choose **Tools** > **Control Center - Network Services**.
b) Choose the publisher node and click **Go**.
c) Verify that the **Cisco SNMP Master Agent** service is running.

Step 3 Start the **Cisco Call Manager SNMP Service**.

a) Choose **Control Center** > **Service Activation**.
b) From the **Server** drop-down, choose the publisher node and click **Go**.

c) Confirm that the **Cisco Call Manager SNMP Service** is running. If it's not running, check the corresponding check box and click **Save**.

What to do next

If you are configuring SNMP V1 or V2c, Configure SNMP Community String, on page 23.

If you are configuring SNMP V3, Configure an SNMP User, on page 25.

Configure SNMP Community String

If you are deploying SNMP V1 or V2c, use this procedure to set up an SNMP community string.

Note This procedure is required for SNMP V1 or V2c. For SNMP V3, configure an SNMP User instead of a community string.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Snmp** > **V1/V2c** > **Community String**.

Step 2 Select a **Server** and click **Find** to search for existing community strings. Optionally, you can enter search parameters to locate a specific community string.

Step 3 Do either of the following:

- To edit an existing SNMP community string, select the string.
- To add a new community string, click **Add New**.

Note
To delete an existing community string, select the string and click **Delete Selected**. After you delete the user, restart the Cisco SNMP Master Agent.

Step 4 Enter the **Community String Name**.

Step 5 Complete the fields in the **SNMP Community String Configuration** window. For help with the fields and their settings, see Community String Configuration Settings, on page 24.

Step 6 From the **Access Privileges** drop-down, configure the privileges for this community string.

Step 7 If you want these settings to apply to all cluster nodes, check the **Apply to All Nodes** check box.

Step 8 Click **Save**.

Step 9 Click **OK** to restart the SNMP master agent service and effect the changes.

What to do next

Configure SNMP Notification Destination, on page 29

Community String Configuration Settings

The following table describes the community string configuration settings.

Table 12: Community String Configuration Settings

Field	Description
Server	This setting in the Community String configuration window displays as read only because you specified the server choice when you performed the procedure in find a community string. To change the server for the community string, perform the find a community string procedure.
Community String	Enter a name for the community string. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Choose community string names that are hard for outsiders to figure out. When you edit a community string, you cannot change the name of the community string.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click this button.
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Hostname/IPv4/IPv6 Address field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets and click **Insert**. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334. Repeat this process for each address from which you want to accept SNMP packets. To delete an address, choose that address from the Host IPv4/IPv6 Addresses list box and click **Remove**.

Field	Description
Access Privileges	From the drop-down list box, select the appropriate access level from the following list: **ReadOnly** The community string can only read the values of MIB objects. **ReadWrite** The community string can read and write the values of MIB objects. **ReadWriteNotify** The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** The community string can only send MIB object values for a trap and inform messages. **ReadNotifyOnly** The community string can read values of MIB objects and also send the values for trap and inform messages. **None** The community string cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, configure a community string with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges. IM and Presence Service does not support ReadNoticyOnly.
Apply To All Nodes	To apply the community string to all nodes in the cluster, check this check box. This field applies to Unified Communications Manager and IM and Presence Service clusters only.

Configure an SNMP User

If you are deploying SNMP V3, use this procedure to set up an SNMP User.

Note This procedure is required for SNMP V3 only. For SNMP V1 or V2c, configure a community string instead.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Snmp** > **V3** > **User**.

Step 2 Select a **Server** and click **Find** to search for existing SNMP users. Optionally, you can enter search parameters to locate a specific user.

Step 3 Do either of the following::

- To edit an existing SNMP user, select the user.
- To add a new SNMP user, click **Add New**.

Note
To delete an existing user, select the user and click **Delete Selected**. After you delete the user, restart the Cisco SNMP Master Agent.

Step 4 Enter the **SNMP User Name**.

Step 5 Enter the SNMP User configuration settings. For help with the fields and their settings, see SNMP V3 User Configuration Settings, on page 26.

Tip
Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 6 From the **Access Privileges** drop-down, configure the access privileges that you want to assign to this user.

Step 7 If you want to apply this configuration to all cluster nodes, check the **Apply to all Nodes** check box.

Step 8 Click **Save**.

Step 9 Click **OK** to restart the SNMP Master Agent.

Note
To access the server with the user that you configured, make sure that you configure this user on the NMS with the appropriate authentication and privacy settings.

What to do next

Get Remote SNMP Engine ID, on page 28

SNMP V3 User Configuration Settings

The following table describes the SNMP V3 user configuration settings.

Table 13: SNMP V3 User Configuration Settings

Field	Description
Server	This setting displays as read only because you specified the server when you performed the find notification destination procedure. To change the server where you want to provide access, perform the procedure to find an SNMP user.

Field	Description
User Name	In the field, enter the name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS). For existing SNMP users, this setting displays as read only.
Authentication Required	To require authentication, check the check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, choose **SHA** as the protocol.
Privacy Required	If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the check box, enter the password in the Password and Reenter Password fields, and check the protocol check box. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, choose **AES128** as the protocol.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Hostname/IPv4/IPv6 Address field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets and click **Insert**. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334. Repeat this process for each address from which you want to accept SNMP packets. To delete an address, choose that address from the Host IPv4/IPv6 Addresses list box and click **Remove**.

Field	Description
Access Privileges	From the drop-down list box, choose one of the following options for the access level: **ReadOnly** You can only read the values of MIB objects. **ReadWrite** You can read and write the values of MIB objects. **ReadWriteNotify** You can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** You can only send MIB object values for trap and inform messages. **ReadNotifyOnly** You can read values of MIB objects and also send the values for trap and inform messages. **None** You cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
Apply To All Nodes	To apply the user configuration to all nodes in the cluster, check this check box. This applies to Unified Communications Manager and IM and Presence Service clusters only.

Get Remote SNMP Engine ID

If you are deploying SNMP V3, use this procedure to obtain the remote SNMP engine ID, which is required for Notification Destination configuration.

Note This procedure is mandatory for SNMP V3, but is optional for SNMP V1 or 2C.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the `utils snmp walk 1` CLI command.

Step 3 Enter the configured community string (with SNMP V1/V2) or configured user (with SNMP V3).

Step 4 Enter the ip address of the server. For example, enter `127.0.0.1` for localhost.

Step 5 Enter `1.3.6.1.6.3.10.2.1.1.0` as the Object ID (OID).

Step 6 For the file, enter `file`.

Step 7 Enter `y`.
The HEX-STRING that the system outputs represents the Remote SNMP Engine ID.

Step 8 Repeat this procedure on each node where SNMP is running.

What to do next

Configure SNMP Notification Destination, on page 29

Configure SNMP Notification Destination

Use this procedure to configure a Notification Destination for SNMP Traps and Informs. You can use this procedure for either SNMP V1, V2c, or V3.

Before you begin

If you haven't set up an SNMP community string or SNMP user yet, complete one of these tasks:

- For SNMP V1/V2, see Configure SNMP Community String, on page 23
- For SNMP V3, see Configure an SNMP User, on page 25

Procedure

Step 1 From Cisco Unifeid Serviceability, choose one of the following:

- For SNMP V1/V2, choose **Snmp** > **V1/V2** > **Notification Destination**
- For SNMP V3, choose **Snmp** > **V3** > **Notification Destination**

Step 2 Select a **Server** and click **Find** to search for existing SNMP Notification Destinations. Optionally, you can enter search parameters to locate a specific destination.

Step 3 Do either of the following::

- To edit an existing SNMP notification destination, select the notification destination.
- To add a new SNMP notification destination, click **Add New**.

Note
To delete an existing SNMP notification destination, select the destination and click **Delete Selected**. After you delete the user, restart the **Cisco SNMP Master Agent**.

Step 4 From the **Host IP Addresses** drop-down, select an existing address or click **Add New** and enter a new host IP address.

Step 5 SNMP V1/V2 only. From the **SNMP Version** field, check the V1 or V2C radio buttons, depending on whether you are configuring SNMP V1 or V2c.

Step 6 For SNMP V1/V2, complete these steps:

a) SNMP V2 only. From the **Notification Type** drop-down, select **Inform** or **Trap**.
b) Select the **Community String** that you configured.

Step 7 For SNMP V3, complete these steps:

a) From the **Notification Type** drop-down select **Inform** or **Trap**.
b) From the **Remote SNMP Engine ID** drop-down, select an existing Engine ID or select **Add New** and enter a new ID.
c) From the **Security Level** drop-down, assign the appropriate security level.

Step 8 If you want to apply this configuration to all cluster nodes, check the **Apply to all Nodes** check box.

Step 9 Click **Insert**.

Step 10 Click **OK** to restart the SNMP Master Agent.

Example

Note For field description help in the Notification Destination Configuration window, see one of the following topics:

- Notification Destination Settings for SNMP V1 and V2c, on page 30
- Notification Destination Settings for SNMP V3, on page 31

What to do next

Configure MIB2 System Group, on page 33

Notification Destination Settings for SNMP V1 and V2c

The following table describes the notification destination configuration settings for SNMP V1/V2c.

Table 14: Notification Destination Configuration Settings for SNMP V1/V2c

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure to find a notification destination. To change the server for the notification destination, perform the procedure to find a community string.
Host IPv4/IPv6 Addresses	From the drop-down list box, select the Host IPv4/IPv6 address of the trap destination or click **Add New**. If you click **Add New**, enter the IPv4/IPv6 address of the trap destination in the Host IPv4/IPv6 Address field. For existing notification destinations, you cannot modify the host IP address configuration.

Field	Description
Host IPv4/IPv6 Address	In the field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334.
Port Number	In the field, enter the notification-receiving port number on the destination server that receives SNMP packets.
V1 or V2c	From the SNMP Version Information pane, click the appropriate SNMP version radio button, either V1 or V2c, which depends on the version of SNMP that you are using. • If you choose V1, configure the community string setting. • If you choose V2c, configure the notification type setting and then configure the community string.
Community String	From the drop-down list box, choose the community string name to be used in the notification messages that this host generates. Only community strings with minimum notify privileges (ReadWriteNotify or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click **Create New uiCommunity String** to create a community string. IM and Presence only: Only community strings with minimum notify privileges (ReadWriteNotify, ReadNotifyOnly, or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click **Create New Community String** to create a community string.
Notification Type	From the drop-down list box, choose the appropriate notification type.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Notification Destination Settings for SNMP V3

The following table describes the notification destination configuration settings for SNMP V3.

Table 15: Notification Destination Configuration Settings for SNMP V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure to find an SNMP V3 notification destination. To change the server for the notification destination, perform the procedure to find an SNMP V3 notification destination and select a different server.

Field	Description
Host IPv4/IPv6 Addresses	From the drop-down list box, select the Host IPv4/IPv6 address of the trap destination or click **Add New**. If you click **Add New**, enter the IPv4/IPv6 address of the trap destination in the Host IPv4/IPv6 Address field. For existing notification destinations, you cannot modify the host IP address configuration.
Host IPv4/IPv6 Address	In the field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334.
Port Number	In the field, enter the notification-receiving port number on the destination server.
Notification Type	From the drop-down list box, choose **Inform** or **Trap**. **Tip** Cisco recommends that you choose the Inform option. The Inform function retransmits the message until it is acknowledged, thus, making it more reliable than traps.
Remote SNMP Engine Id	This setting displays if you chose Inform from the Notification Type drop-down list box. From the drop-down list box, choose the engine ID or choose **Add New**. If you chose Add New, enter the ID in the Remote SNMP Engine Id field, which requires a hexidecimal value.
Security Level	From the drop-down list box, choose the appropriate security level for the user. **noAuthNoPriv** No authentication or privacy configured. **authNoPriv** Authentication configured, but no privacy configured. **authPriv** Authentication and privacy configured.
User Information pane	From the pane, perform one of the following tasks to associate or disassociate the notification destination with the user. 1. To create a new user, click **Create New User**. 2. To modify an existing user, click the radio button for the user and then click **Update Selected User**. 3. To delete a user, click the radio button for the user and then click **Delete Selected User**. The users that display vary depending on the security level that you configured for the notification destination.

Field	Description
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Configure MIB2 System Group

Use this procedure to configure a system contact and system location for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and SanJose, Bldg 23, 2nd floor, for the system location. You can use this procedure for SNMP V1, V2, and V3.

Procedure

Step 1 From cisco Unified Serviceability, choose **Snmp** > **SystemGroup** > **MIB2 System Group**.

Step 2 From the **Server** drop-down select a node and click **Go**.

Step 3 Complete the **System Contact** and **System Location** fields.

Step 4 If you want these settings to apply to all cluster nodes, check the **Apply to All Nodes** check box.

Step 5 Click **Save**.

Step 6 Click **OK** to restart the SNMP master agent service

Example

Note For field description help, see MIB2 System Group Settings, on page 33

Note You can click **Clear All** to clear the fields. If you click **Clear All** followed by**Save**, the record is deleted.

MIB2 System Group Settings

The following table describes the MIB2 System Group configuration settings.

Table 16: MIB2 System Group Configuration Settings

Field	Description
Server	From the drop-down list box, choose the server for which you want to configure contacts, and then click **Go**.

Field	Description
System Contact	Enter a person to notify when problems occur.
System Location	Enter the location of the person that is identified as the system contact.
Apply To All Nodes	Check to apply the system configuration to all of the nodes in the cluster. This applies to Unified Communications Manager and IM and Presence Service clusters only.

CISCO-SYSLOG-MIB Trap Parameters

Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:

- Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to True by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to True from the linux command line using:

```
snmpset -c <community string>-v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  You can also use any other SNMP management application for the SNMP Set operation.

- Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset-c public-v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>
```

  Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.

  Severity values are as follows:

  - 1: Emergency
  - 2: Alert
  - 3: Critical
  - 4: Error
  - 5: Warning
  - 6: Notice
  - 7: Info
  - 8: Debug)

  You can also use any other SNMP management application for the SNMP Set operation.

Note Before logging, Syslog truncates any trap message data that is larger than the specified Syslog buffer size. The Syslog trap message length limitation equals 255 bytes.

CISCO-CCM-MIB Trap Parameters

- Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset -c <community string> -v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

  You can also use any other SNMP management application for the SNMP Set operation.

- Set ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

```
snmpset -c <community string> -v2c
<transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

  You can also use any other SNMP management application for the SNMP Set operation.

CISCO-UNITY-MIB Trap Parameters

Cisco Unity Connection only: The Cisco Unity Connection SNMP Agent does not enable trap notifications, though traps can be triggered by Cisco Unity Connection alarms. You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability, on the **Alarm** > **Definitions** screen.

You can configure trap parameters by using the CISCO-SYSLOG-MIB.

Related Topics

CISCO-SYSLOG-MIB Trap Parameters, on page 34

Restart SNMP Master Agent

After you complete all of your SNMP configurations, restart the SNMP Master Agent service.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 Choose a **Server** and click **Go**.

Step 3 Select the **SNMP Master Agent**.

Step 4 Click **Restart**.

SNMP Trap Settings

Use CLI commands to set the configurable SNMP trap settings. SNMP trap configuration parameters and recommended configuration tips are provided for CISCO-SYSLOG-MIB, CISCO-CCM-MIB, and CISCO-UNITY-MIB.

Configure SNMP Traps

Use this procedure to configure SNMP traps.

Before you begin

Configure your system for SNMP. For details, see SNMP Configuration Task Flow, on page 21.

Make sure that the **Access Privileges** for either the SNMP community string (for SNMP V1/V2), or the SNMP user (for SNMP V3) are set to one of the following settings: **ReadWriteNotify**, **ReadNotify**, **NotifyOnly**.

Procedure

Step 1 Log in to CLI and run the `utils snmp test` CLI command to verify that SNMP is running.

Step 2 Follow Generate SNMP Traps, on page 36 to generate specific SNMP traps (for example, the ccmPhoneFailed or MediaResourceListExhausted traps).

Step 3 If the traps do not generate, perform the following steps:

- In Cisco Unified Serviceability, choose **Alarm** > **Configuration** and select **CM Services** and **Cisco CallManager**.
- Check the **Apply to All Nodes** check box.
- Under Local Syslogs, set the Alarm Event Level drop-down list box to **Informational**.

Step 4 Reproduce the traps and check if the corresponding alarm is logged in CiscoSyslog file.

Generate SNMP Traps

This section describes the process for generating specific types of SNMP traps. SNMP must be set up and running on the server in order for the individual traps to generate. Follow Configure SNMP Traps, on page 36 for instructions on how to set up your system to generate SNMP traps.

Note The processing time for individual SNMP traps varies depending on which trap you are attempting to generate. Some SNMP traps may take up to a few minutes to generate.

Table 17: Generate SNMP Traps

SNMP Traps	Process
ccmPhoneStatusUpdate	To trigger the ccmPhoneStatusUpdate trap: **1.** In the ccmAlarmConfig Info mib table, set ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 or higher. **2.** Log in to Cisco Unified Communications Manager Administration. **3.** For a phone that is in service and that is registered to Unified Communications Manager, reset the phone. The phone deregisters, and then reregisters, generating the ccmPhoneStatusUpdate trap.
ccmPhoneFailed	To trigger the ccmPhoneFailed trap: **1.** In the ccmAlarmConfigInfo mib table, set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 or higher. **2.** In Cisco Unified Communications Manager Administration, change the MAC address of the phone to an invalid value. **3.** In Cisco Unified Communications Manager Administration, reregister the phone. **4.** Set the phone to point to the TFTP server A and plug the phone into a different server.
ccmGatewayFailed	To trigger the ccmGatewayFailed SNMP trap: **1.** Confirm that ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) is set to true. **2.** In Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. **3.** Reboot the gateway.
ccmGatewayLayer2Change	To trigger the ccmGatewayLayer2Change trap on a working gateway where layer 2 is monitored (for example, the MGCP backhaul load): **1.** In the ccmAlarmConfig Info mib table, set ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true. **2.** In Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. **3.** Reset the gateway.

SNMP Traps	Process
MediaResourceListExhausted	To trigger a MediaResourceListExhausted trap: **1.** In Cisco Unified Communications Manager Administration, create a media resource group that contains one of the standard Conference Bridge resources (CFB-2). **2.** Create a media resource group list that contains the media resource group that you created. **3.** In the Phone Configuration window, set the Media Resource Group List field to the media resource group list that you have created. **4.** Stop the IP Voice Media Streaming service. This action causes the ConferenceBridge resource (CFB-2) to stop working. **5.** Make conference calls with phones that use the media resource group list. The "No Conference Bridge available" message appears in the phone screen.
RouteListExhausted	To trigger a RouteListExhausted trap: **1.** Create a route group that contains one gateway. **2.** Create a route group list that contains the route group that you just created. **3.** Create a unique route pattern that routes a call through the route group list. **4.** Deregister the gateway. **5.** Dial a number that matches the route pattern from one of the phones.
MaliciousCallFailed	To trigger a MaliciousCallFailed trap: **1.** Create a softkey template that includes all available "MaliciousCall" softkeys. **2.** Assign the new softkey template to phones in your network and reset the phones. **3.** Place a call between the phones. **4.** During the call, select the "MaliciousCall" softkey.

SNMP Traps	Process
ccmCallManagerFailed	1. Run the `show process list` CLI command to get the Process Identifier (PID) of the CallManager application ccm. This command returns a number of processes and their PIDs. You must obtain the PID for ccm specifically since this is the PID that you must stop in order to generate the alarm. 2. Run the `delete process <pid>` crash CLI command 3. Run the CLI command. The CallManager Failed Alarm is generated when internal errors are generated. These internal errors may include an internal thread quitting due to the lack of CPU, pausing the CallManager server for more than 16 seconds, and timer issues. You cannot manually generate this alarm. **Note** Generating a ccmCallManagerFailed alarm or trap shuts down the CallManager service and generates a core file. To avoid confusion, Cisco recommends that you delete the core file immediately.
syslog messages as traps	To receive syslog messages above a particular severity as traps, set the following two mib objects in the clogBasic table: 1. Set clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true(1). Default value is false(2). For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 2. Set the clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) to a level that is greater than the level at which you want your traps to be produced. The default value is warning (5). All syslog messages with alarm severity lesser than or equal to the configured severity level are sent as traps. For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP Trace Configuration

For Unified Communications Manager, you can configure trace for the Cisco CallManager SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco CallManager SNMP Service in the Performance and Monitoring Services service group. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you use the CLI to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For Cisco Unity Connection, you can configure trace for the Cisco Unity Connection SNMP agent in the Trace Configuration window in Cisco Unity Connection Serviceability by choosing the Connection SNMP Agent component.

Troubleshooting SNMP

Review this section for troubleshooting tips. Make sure that all of the feature and network services are running.

Problem

You cannot poll any MIBs from the system.

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system. By default, no community string or user is configured on the system.

Solution

Check whether the community string or snmp user is properly configured on the system by using the SNMP configuration windows.

Problem

You cannot receive any notifications from the system.

This condition means that the notification destination is not configured correctly on the system.

Solution

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.