SNMP Agent Setup

Simple Network Management Protocol Support

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth. The Unified CVP SNMP agent lets customers and partners to integrate with their existing SNMP network management system to provide instantaneous feedback on the health of their Unified CVP system.

The Call server, Unified CVP VXML Server, and Reporting server can send SNMP traps and statistics to any standard SNMP management station. You can configure a link to the administration web page for an SNMP monitoring tool and then access it by selecting SNMP Monitor from the Tools menu.

The SNMP menus from the Operations Console enable you to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. SNMP V3 offers improved security features.

SNMP Basics

An SNMP-managed network is comprised of managed devices, agents, and network management systems.

Key SNMP Components

- 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.

- 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. Unified CVP uses a primary agent and subagent components to support SNMP. The primary agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the primary agent contains a few MIB variables that relate to MIB-II. The SNMP primary agent listens on port 161 and forwards SNMP packets for Vendor MIBs. The Unified CVP subagent interacts with the local Unified CVP only. The Unified CVP subagent sends notifications and SNMP response messages to the primary agent for forwarding to a Network Management Station. The SNMP primary agent communicates with the SNMP trap receiver (notification destination).
- Network Management System (NMS) - A 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 runs applications that monitor and control managed devices. Unified CVP works with any standard SNMP-based NMS.

SNMP Management Information Base (MIB)

SNMP allows access to 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 Unified CVP Simple Network Management Protocol (SNMP) agent resides in each component and exposes the CISCO-CVP-MIB that provides detailed information about devices that are known to the Unified CVP subagent. The CISCO-CVP-MIB provides device information such as device registration status, IP address, description, and model type for the component.

The AIX Native agent by default listens on port 161 for Network Management Station requests. Upon installation of CVP, the AIX Native agent is reconfigured to listen on port 8161. The CVP SNMP Agent takes over listening on port 161. The CVP SNMP Agent acts as a proxy to the Native AIX Agent. The CVP SNMP Agent handles the forwarding of traps and statistics. SNMP Traps generated by the Native AIX Agent are sent to the CVP SNMP Agent and forwarded to all SNMP Notification targets that are configured using the Operations Console.

Unified CVP supports the following MIBs:

Supported MIBs:

- CISCO-CVP-MIB - Provides general information; server name and version number; and status and statistics for each component.
- HOST-RESOURCES-MIB - The Host Resources MIB found in Cisco SNMP is an implementation of the Host Resources MIB document, proposed standard RFC 1514 (https://www.ietf.org/rfc/rfc1514.txt). It is also compliant with Host Resources MIB, draft standard RFC 2790 (https://www.ietf.org/rfc/rfc2790.txt). This MIB defines objects that are useful for managing host systems and allows SNMP access to useful host information, such as the storage resources, process table, device information, and the installed software base.
- The System-level Managed Objects for Applications (SYSAPPL) MIB, RFC 2287 (https://www.ietf.org/rfc/rfc2287.txt), supports configuration, fault detection, performance monitoring, and control of application software. It provides for tables that define an application as a series of processes and services. This includes objects for applications installed on the system, elements and processes that are included in an application, and current and previously run applications.

Set Up SNMP

Table 1: SNMP Configuration Checklist

Configuration Steps	Related Procedures and Topics
Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS.
Import all previous SNMP configurations to the Operations Console.	Import Previously Configured Windows SNMP v1 Community Strings
If you are using SNMP v1/v2c, configure the community string.	SNMP v1/v2c Community String Setup
If you are using SNMP v3, configure the SNMP user.	SNMP v3 User Setup
Configure the notification destinations.	SNMP v1/v2 Notification Destination Setup
Configure the system contact and location for the MIB2 system group.	SNMP MIB2 System Group Setup

Import Previously Configured Windows SNMP v1 Community Strings

To import previously configured Windows SNMP V1 Community Strings:

Procedure

Step 1 View the list of previously configured Windows SNMP V1 community strings by performing the following:

a) Open the Windows Services viewer.
b) Right-click **SNMP Service** and select **Properties**.
c) Select the **Security** tab. This tab lists the accepted V1 community strings and the access granted for each string, and also lists the hosts from which SNMP packets are accepted.

Note The accepted hosts apply to all community strings, whereas the Operations Console provides more granularity, allowing you to specify accepted hosts on a per-community string basis.

Note If **Security** tab is not displayed, install the SNMP tools using the Powershell command: `Install-WindowsFeature -Name RSAT-SNMP` and restart the Service Manager before opening the **Properties** page again.

Step 2 Configure these community strings using the Operations Console:

a) Open the Operations Console and select **SNMP | V1/V2C | Community String**.
b) For each community string discovered above that has not already been configured in the Operations Console, add it by clicking **Add New**.

Perform the following actions:

- Enter the community string exactly as it appeared in step 1 above.
- Select **V1** as the version.
- For Windows community strings with permission other than "Read Only," select **Read Write** in the Operations Console.
- Select the device(s) on which this community string was seen in step 1.

SNMP v1/v2c Agent Setup

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 management information base 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 to allow SNMP to 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.

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.

You need to compile the Cisco CVP MIB with your SNMP network management application. The CVP MIB is located in the %CVP_HOME%\conf folder. You can also find the current list of supported MIBS at: https://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Note The CVP MIB is defined using version 2 of the Structure of Management Information (SMI) and contains "Counter64" (64-bit integer) object types. While the CVP SNMP infrastructure supports version 1 of the SNMP protocol, SNMP v1 cannot query Counter64 object values. Hence, you must use SNMP v3 or SNMP v2c.

You can configure SNMP v1 support from the SNMP V1/V2c menu.

You can perform the following tasks:

- SNMP v1/v2c Community String Setup, on page 4
- SNMP v1/v2 Notification Destination Setup, on page 9

SNMP v1/v2c Community String Setup

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. Typically, one community string is used for read-only access to a network element.

You configure SNMP community strings for SNMP v1 and v2c only. SNMP v3 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.

Add SNMP v1/v2C Community String

Related Topics

SNMP v1/v2c Community String Settings, on page 6
Find SNMP v1/v2c Community String, on page 8

Procedure

To add an SNMP v1/v2c community string:

Procedure

Step 1 Select **SNMPV1/V2cCommunity String**.

The Find, Add, Delete, Edit window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select **Add New**.

The V1/V2c SNMP Community String Configuration window opens to the General tab.

Step 3 Fill in the community string and verify that the default values for other fields are correct.

Step 4 Select the **Devices** tab and assign an SNMP community string to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or select **Save & Deploy** to save the changes and apply the changes to the selected devices.

Edit SNMP v1/v2C Community String

Related Topics

SNMP v1/v2c Community String Settings, on page 6
Find SNMP v1/v2c Community String, on page 8

Procedure

You can change the name, the hosts to accept SNMP packets from, and the access privileges for an SNMP V1/V2C community string.

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select the SNMP community string to edit by checking the check box preceding it and selecting **Edit**.

The Community String Configuration window opens to the General tab.

Step 3 Make the desired changes to the community string settings. You cannot change the name of the SNMP community string.

Step 4 Select the **Devices** tab and make desired changes to the assignment of the SNMP community string to a device.

Step 5 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply the changes to the selected devices.

SNMP v1/v2c Community String Settings

The following table describes the fields that you can change to configure an SNMP v1/v2c community string.

Table 2: SNMP v1/v2c Community String Configuration

Field	Description	Default	Range	Restart Required
Community String Information				
Community String Name	You cannot change this name if you are editing a Community String.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
SNMP Version Information				
V1 or V2c	Select SNMP Version 1 or 2c agent	V1	V1 or 2c	No
Host IP Addresses Information				
Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts	Select hosts that are allowed to query or access the configured devices using this community string.	Accept SNMP Packets From Any Host	From any host or from only these hosts	No
Host IP Address	Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click **Add** to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click **Remove**.	None	Valid IP address	No
Access Privileges				

Field	Description	Default	Range	Restart Required
Access Privileges	Choose the appropriate access level from the following list: Access Privileges: • **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.	ReadOnly	ReadOnly, ReadWrite	No

Assign SNMP Entity to Device

Procedure

While you add or edit any of the following SNMP entities, you can add them to or remove them from one or more devices:

SNMP Entities:

- SNMP V1/V2C community strings
- SNMP V1/V2C or V3 notification destinations
- SNMP MIB-2 user groups
- SNMP V3 users

Procedure

Step 1 Select the **Devices** tab.

Step 2 To add an SNMP V1/V2 community string to a device, perform the following steps:

a) Select the device from the **Available** pane.
b) Select the right arrow to move the device to the **Selected** pane.

Step 3 To remove an SNMP V1/V2 community string from a device, perform the following steps:.

a) Select the device from the **Selected** pane.
b) Select the left arrow to move the device to the **Available** pane.

Step 4 Select **Save** to save the configuration to the Operations Console database. Select **Save & Deploy** to save the changes and apply the changes to the selected devices.

Find SNMP v1/v2c Community String

If you have several SNMP community strings in your network, the Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP community string.

Procedure

To find an SNMP V1/V2c community string:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 To scroll through the list, select **Next** to view the next group of available community strings.

Step 3 Select **Previous** to view the previous group of available community strings.

Step 4 To filter the list:

a) Using the filter at the top right of the list, select a field to search.
b) Select a modified (such as Starts with).
c) Select **Find**.

Note The filter is not case-sensitive and wildcards are not allowed.

Step 5 From the second window drop-down list box, select one of the following search criteria:

- begins with
- contains
- ends with
- is exactly

Step 6 Specify the appropriate search text, if applicable, and select **Find**.

Delete SNMP v1/v2c Community String

Procedure

To delete one or more SNMP V1/V2c community strings:

Procedure

Step 1 Selec **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 To select the SNMP community string to delete, perform the following steps:

a) Select the check box preceding the string.

b) Select **Delete**.

Step 3 When prompted to confirm the delete operation, perform one of the following steps:

- Select **OK** to delete the operation.
- Select **Cancel** to cancel the delete operation.

Related Topics

Find SNMP v1/v2c Community String, on page 8

SNMP v1/v2 Notification Destination Setup

You can configure different community strings for SNMP v1 and v2c depending on which protocol they wish to use on their network. If you use both SNMP v1 and v2c, you can configure one community string for v1 and another for v2.

You might have one management station (using SNMP v1) collecting notifications from one part of the network and another management station (using SNMP v2) collecting notifications from another part. In this case, when configuring a destination, you must specify the community string that correlates the SNMP version used to send the notification.

SNMP v1/v2 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

Table 3: Notification Destination Configuration Settings

Field	Description	Default	Range	Restart Required
Host IP Address Information				
Host IP Address	IP address of host to receive SNMP notifications.	None	Valid IP address	No
Port Number	Port number to receive SNMP notifications.	162	Any available port number. Valid port numbers are integers between 1 and 65535	No
Notification Destination Information				

Field	Description	Default	Range	Restart Required
Notification Destination Name	When you are adding a notification destination, assign a name. You cannot change the Notification Destination Name.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
Community String Information				
Community String	Select the community string from the drop-down list.	None	Not applicable	No

Add SNMP v1/v2c Notification Destination

Procedure

To add an SNMP v1/v2c notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2c Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The V1/V2c Notification Destination Configuration window opens to the Configuration tab.

Step 3 Fill in the fields on the configuration tab.

Step 4 Select the **Devices** tab and assign the SNMP notification destination to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save and apply the changes to the selected devices.

Related Topics

SNMP v1/v2 Notification Destination Settings, on page 9

Edit SNMP v1/v2C Notification Destination

Related Topics

SNMP v1/v2 Notification Destination Settings, on page 9
Assign SNMP Entity to Device, on page 7
Find SNMP v1/v2C Notification Destination, on page 11

Procedure

To change an SNMP V1/V2C notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To select the SNMP notification destination to edit, perform the following steps:

a) Select the check box preceding the destination.
b) Select **Edit**.

The Notification Destination Configuration window opens to the Configuration tab.

Step 3 Make the desired changes to the fields on the Configuration tab.

Note You cannot change the name of the notification destination.

Step 4 Select the **Devices** tab and assign an SNMP entity to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save and apply the changes to the selected devices.

Delete SNMP v1/v2C Notification Destination

Procedure

To delete one or more SNMP V1/V2c notification destinations:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To select the SNMP notification destination to delete, perform the following steps:

a) Select the check box preceding the destination.
b) Select **Delete**.

Step 3 When prompted to confirm the delete operation, select **OK** to delete or select **Cancel** to cancel the delete operation.

Find SNMP v1/v2C Notification Destination, on page 11

Find SNMP v1/v2C Notification Destination

The Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

Procedure

To find an SNMP V1/V2c notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2c Notification Destinations window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To scroll through many pages of the list, click the first, previous, next, and last page icons on the bottom left to view the next group of available notification destinations.

Step 3 You can filter the list by performing the following steps:

a) Using the filter at the top right of the list, select a field to search.
b) Select a modifier (such as Starts With).
c) Select **Find**.

Note The filter is not case-sensitive and wildcards are not allowed.

SNMP v3 Agent Setup

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 objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3. Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the SNMP Community Strings and Users topic.

Configure SNMP v3 support from the SNMP V3 menu.

You can perform the following tasks:

- SNMP v3 User Setup, on page 12
- SNMP v3 Notification Destination Setup, on page 17

SNMP v3 User Setup

When you create SNMP users, match their SNMP user names to the user names you have already configured for the NMS.

You can perform the following tasks:

- Find SNMP v3 User, on page 13
- Add SNMP v3 User, on page 13
- Edit SNMP v3 User, on page 14

Find SNMP v3 User

Procedure

To find an SNMP user:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit Users window lists the available SNMP v3 users, sorted by name, 10 at a time.

Step 2 If the list is long, you can click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, you can enter a page number in the **Page** field and press **enter** to go to the numbered page.

Step 3 You can filter the list by selecting an attribute such as **V3 Username**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Add SNMP v3 User

Related Topics

SNMP v3 User Settings, on page 14
Assign SNMP Entity to Device, on page 7

Procedure

To add an SNMP v3 user:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit V3 Users window lists the available SNMP users, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The SNMP V3 User Configuration window opens to the Configuration tab.

Step 3 Fill in the username and verify that the default values for other fields are correct.

Step 4 Select the **Devices** tab and assign the user to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the change to the selected devices.

Edit SNMP v3 User

Related Topics

SNMP v3 User Settings, on page 14
Assign SNMP Entity to Device, on page 7
Find SNMP v3 User, on page 13

Procedure

You can change the access privileges, authentication and privacy information for an SNMP V3 user.

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit Users window lists the available SNMP users, sorted by name, 10 at a time.

Step 2 Select the SNMP user name to edit by selecting the check box preceding it or highlighting the user name and then clicking **Edit**.

The SNMP User Configuration window opens to the Configuration tab.

Step 3 Make the desired changes to SNMP V3 users settings. You cannot change the username for the SNMP V3 user.

Step 4 Select the **Devices** tab and change the assignment of the user to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the change to the selected devices.

SNMP v3 User Settings

The following table describes the fields that you can change to configure an SNMP v3 user.

Field	Description	Default	Range	Restart Required
User Information				
Username	Enter the SNMP v3 user name. You cannot change this name when editing an SNMP v3 user.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No

Field	Description	Default	Range	Restart Required
Access Privileges	Select the appropriate access level from the following list: Access Privileges: • **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.	ReadOnly	ReadOnly, ReadWrite	No
Host IP Addresses Information				
Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts	Select hosts that are allowed to query or access the configured devices using this community string.	Accept SNMP Packets From Any Host	From any host or from only these hosts	No
Host IP Address	Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click **Add** to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click **Remove**.	None	Valid IP address	No
Authentication Information				
Authentication Required	Select to require authentication for this user. This offers an additional level of security not provided with SNMP v1 and v2c. The SNMP user only gains access to the device when using both a valid user name and password. If authentication is not required, security is no better with v3 than it would be for SNMP v1/v2c using community strings.	Disabled	Enabled or Disabled	No
Password	Password for the SNMP Version 3 user. This password is required to accept incoming SNMP v3 packets.	None	Any text that follows the security guidelines for passwords.	No

Field	Description	Default	Range	Restart Required
Re-enter Password	Retype the password for this user account to verify that you typed the password correctly.	None	The same text that was entered in the Password field.	No
Protocol	Choose MD5 or SHA-1 protocols to encrypt the password.	None	MD5 or SHA-1	No
Privacy Information				
Privacy Required	Select to require privacy for the SNMP user. Enabling privacy causes the SNMP message data to be encrypted during transmission. This provides an additional level of security over authentication (only) in that it protects the data, rendering it unreadable by would-be snoopers while traveling over the wire.	Disabled	Enabled or disabled.	No
Password	Password the SNMP user must enter.	None	Any text that follows the security guidelines for passwords.	No
Re-enter Password	Re-type the same text entered in the Password field.	None	The same text entered in the Password field.	No
Protocol	Select the protocol to encrypt the user password.	None	3DES, AES-192 , AES-256	No

Delete SNMP v3 User

Procedure

To delete one or more SNMP users:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit window lists the available users, sorted by name, 10 at a time.

Step 2 Select the SNMP users to delete by selecting the check box preceding it or highlighting the user name, and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP v3 User, on page 13

SNMP v3 Notification Destination Setup

A notification destination identifies the target host and port to receive SNMP notifications sent by the Unified CVP SNMP agent on the devices you specify. You can specify an SNMP v3 user and associated authorization for an SNMP v3 notification destination.

Add SNMP v3 Notification Destination

Related Topics

SNMP v3 Notification Destination Settings, on page 18
Assign SNMP Entity to Device, on page 7

Procedure

To add an SNMP V3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The SNMP Notification Destination Configuration window opens to the Configuration tab.

Step 3 Fill in the name of the SNMP V3 notification destination.

Step 4 Select the **Devices** tab and assign the SNMP notification destination to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save the change and apply them to the selected devices.

Edit SNMP v3 Notification Destination

Related Topics

SNMP v3 Notification Destination Settings, on page 18
Assign SNMP Entity to Device, on page 7

Procedure

To change an SNMP v3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Edit**.

The SNMP Notification Destination Configuration window opens to the Configuration tab.

Step 3 Change the desired notification destination configuration settings. You cannot change the name of the notification destination.

Step 4 Select the **Devices** tab and add or remove devices to this notification destination.

Step 5 Click **Save** to save the settings in the Operations Console database, or click **Save & Deploy** to save the change and apply them to the selected devices.

SNMP v3 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

Field	Description	Default	Range	Restart Required
Notification Destination Information				
Notification Destination Name	Name for the notification destination. You cannot change this name when editing a notification destination.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
Host IP Addresses Information				
Host IP Address	IP address of host to receive SNMP notifications.	None	Valid IP address	No
Port Number	Port number to receive SNMP notifications.	162	Any available port number. Valid port numbers are integers between 1 and 65535	No
User Information				
User	Select a user from the drop-down list.	None	None	No

Find SNMP v3 Notification Destination

As you probably have several SNMP notification destinations in your network, the Operations Console lets you locate specific destination notifications on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

Procedure

To find an SNMP V3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, 10 at a time, sorted by name.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, you can enter a page number in the **Page** field and press enter to go directly to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **Name**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Delete SNMP v3 Notification Destination

Procedure

To delete one or more SNMP V3 notification destinations:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Select the SNMP notification destination to delete by selecting the check box preceding it or highlighting the notification destination and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP v1/v2C Notification Destination, on page 11

SNMP MIB2 System Group Setup

The Operations Console allows you to change the system contact and system location information in the SNMP MIB-II system group, and to assign that system group to a device. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

You can perform the following tasks:

Add SNMP MIB2 System Group

Procedure

To add an SNMP MIB2 system group:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit MIB2 System Groups window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time. Each device can only be associated with one system group. Only devices that are not associated with other system groups are displayed in the available system groups.

Step 2 Click **Add New**.

The MIB2 System Group Configuration window opens to the Configuration tab.

Step 3 In the **System Contact** field, enter a person to notify when problems occur.

Step 4 In the **System Location** field, enter the location of the person that is identified as the system contact.

Step 5 Select the **Devices** tab and assign the devices to this system group.

Step 6 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

Edit SNMP MIB2 System Group

Procedure

To change SNMP MIB2 system group information:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

Step 2 Click **Edit**.

The MIB2 System Group Configuration window opens to the Configuration tab.

Step 3 In the **System Contact** field, change the name of the person to notify when problems occur.

Step 4 Select the **Devices** tab and add or remove devices to this system group.

Step 5 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

Delete SNMP MIB2 System Group

Procedure

To delete one or more SNMP MIB2 system groups:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

Step 2 Select the SNMP MIB2 system group to delete by selecting the check box preceding it and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP MIB2 System Group, on page 21

Find SNMP MIB2 System Group

Procedure

To find an SNMP MIB2 system group:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, you can enter a page number in the **Page** field and press enter to go to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **System Location**. Select a modifier, such as **begins with**, enter your search term, and then click **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Syslog

Set Up Syslog Server

The instructions below describe how to adjust syslog settings for a Unified CVP Call Server, Unified CVP VXML Server, and/or Unified CVP Reporting Server using the Operations Console.

Procedure

Step 1 Open the Operations Console.

Step 2 Select the server where you want to configure syslog.

Step 3 Click **Edit**.

Step 4 Click **Infrastructure** tab.

Step 5 Edit the fields for backup severs and port numbers for secondary syslog server.

Step 6 Click **Save**.

Unified CVP allows you to configure primary and backup syslog servers. However, it is important to note that failover from primary to backup server is not guaranteed. When the primary syslog server goes down (the entire machine not just the syslog receiver application), Unified CVP relies on the host operating system and the Java Runtime Environment for notification that the destination is not reachable. As this notification does not guarantee delivery, Unified CVP cannot guarantee failover.

Unified CVP allows you to configure secondary set of syslog and backup servers. CVP sends the syslog messages to both primary syslog and secondary syslog server on the ports specified.

See the *Configuration Guide for Cisco Unified Customer Voice Portal* for additional information about Syslog Server settings.