



Monitoring with SNMP

ACNS 5.x software supports Simple Network Management Protocol (SNMP), which is an interoperable standards-based protocol that allows external monitoring of the Content Engine through an SNMP agent.

This chapter explains how to configure SNMP traps, recipients, community strings and group associations, user security model groups, and user access permissions. It contains the following sections:

- [Supported SNMP Versions, page 22-1](#)
- [Configuring SNMP Traps, page 22-2](#)
- [Configuring SNMP Community Settings, page 22-5](#)
- [Configuring SNMP Group Settings, page 22-6](#)
- [Configuring SNMP User Settings, page 22-8](#)
- [Configuring SNMPv2 View Settings, page 22-9](#)
- [Configuring SNMP Host Settings, page 22-10](#)
- [Configuring SNMP Asset Tag Settings, page 22-11](#)
- [Supported MIBs, page 22-12](#)
- [Key SNMP CLI Commands, page 22-13](#)
- [Configuring SNMP Traps Using the CLI, page 22-5](#)

Supported SNMP Versions

ACNS 5.x software supports the following versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of its functionality.
- Version 2 (SNMPv2c)—This is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP, defined in RFC 2271 through RFC 2275.

SNMPv1 and SNMPv2c do not have any security (that is, authentication or privacy) mechanisms to keep SNMP packet traffic on the wire confidential. As a result, packets on the wire can be detected and SNMP community strings compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to Content Engines by authenticating and encrypting packets over the network. In ACNS 5.x software, SNMPv3 features are added to the SNMP agent in addition to SNMPv1 and SNMPv2c features.

**Note**

Registering a new SNMP agent with your ACNS network, as well as modifying or removing a registered SNMP agent, causes each of your ACNS nodes to restart as they register the configuration change. Restarting your ACNS devices results in a temporary interruption in service across your ACNS network for the time it takes for each of your devices to come back online—usually a few minutes.

Each Cisco device running ACNS 5.x software contains the software necessary to communicate information about device configuration and activity using the SNMP protocol. Before you can begin logging SNMP data, you must acquire and deploy an SNMP manager application for use with the ACNS network.

Configuring SNMP Traps

To enable the Content Engine to send SNMP traps, follow these steps:

- Step 1** Choose **Devices > Devices**. The Devices window appears.
- Step 2** Click the **Edit** icon next to the Content Engine that you want to enable. The Content Engine Device Home window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > General Settings**. The SNMP General Settings for Content Engine window appears. (See [Figure 22-1](#).) [Table 22-1](#) describes the fields in this window.

Figure 22-1 SNMP General Settings Window

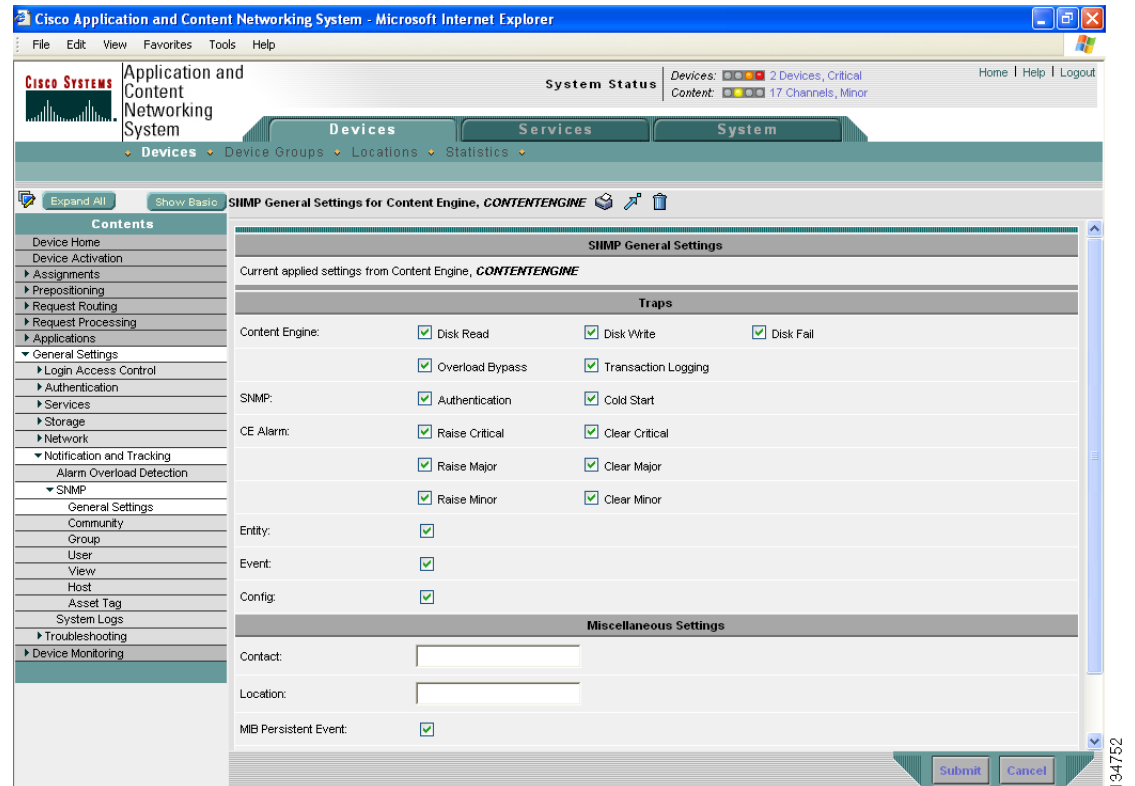


Table 22-1 SNMP General Settings

GUI Parameter	Function	CLI Command
Traps		
Content Engine	Enables SNMP Content Engine traps: <ul style="list-style-type: none"> Disk Read—Enables disk read error trap. Disk Write—Enables disk write error trap. Disk Fail—Enables disk failure error trap. Overload Bypass—Enables WCCP overload bypass error trap. Transaction Logging—Enables transaction log write error trap. 	snmp-server enable traps content-engine
SNMP	Enables SNMP-specific traps: <ul style="list-style-type: none"> Authentication—Enables authentication trap. Cold Start—Enables cold start trap. 	snmp-server enable traps snmp authentication snmp-server enable traps snmp cold-start

Table 22-1 SNMP General Settings (continued)

GUI Parameter	Function	CLI Command
CE Alarm	Enables Content Engine alarm traps: <ul style="list-style-type: none"> • Raise Critical—Enables raise-critical alarm trap • Clear Critical—Enables clear-critical alarm trap • Raise Major—Enables raise-major alarm trap • Clear Major—Enables clear-major alarm trap • Raise Minor—Enables raise-minor alarm trap • Clear Minor—Enables clear-minor alarm trap 	snmp-server enable traps alarm [clear-critical clear-major clear-minor raise-critical raise-major raise-minor]
Entity	Enables SNMP entity traps.	snmp-server enable traps entity
Event	Enables the Event MIB.	snmp-server enable traps event
Config	Enables CiscoConfigManEvent error traps.	snmp-server enable traps config
Miscellaneous Settings		
Contact	Specifies a string for the MIB-II object sysContact. The name identifies the contact person for this managed node.	snmp-server contact line
Location	Specifies a string for the MIB-II object sysLocation. The name identifies the physical location of the node.	snmp-server location line
MIB Persistent Event	Enables persistence for the SNMP Event MIB.	snmp-server mib persist event
Notify Inform	Enables the SNMP notify inform request.	snmp-server notify inform

Step 4 To enable SNMP traps, check the appropriate check boxes.

Step 5 To save the settings, click **Submit**.

A “Click Submit to Save” message appears in red next to the current settings when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured window settings by clicking **Reset**. The Reset button is visible only when you apply default or device group settings to change the current device settings but the settings have not yet been submitted.

Configuring SNMP Traps Using the CLI

To enable the Content Engine to send SNMP traps, use the **snmp-server enable traps** global configuration command. If you do not enter the **snmp-server enable traps** command, no traps are sent. Use the **no** form of this command to disable all SNMP traps or only SNMP authentication traps.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which hosts or hosts receive SNMP traps. To send traps, you must configure at least one host.

For a host to receive a trap, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be used.

In addition, SNMP must be enabled with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, you must enter the command **no snmp-server enable traps snmp authentication**.

The following example enables the Content Engine to send all traps to the host 172.31.2.160 by using the community string *public*:

```
ContentEngine(config)# snmp-server enable traps
ContentEngine(config)# snmp-server host 172.31.2.160 public
```

The following example disables all traps:

```
Content Engine (config)# no snmp-server enable traps
```

Configuring SNMP Community Settings



Note

Community strings are listed in the order in which they have been created. The maximum number of SNMP communities that can be created is ten. By default, an SNMP agent is disabled, and a community string is not configured. When a community string is configured, it permits read-only access to all agents by default.

To enable the SNMP agent and configure a community string to permit access to the SNMP agent, follow these steps:

- Step 1** Choose **Devices > Devices**. The Devices window appears.
- Step 2** Click the **Edit** icon next to the Content Engine for which you want to configure an SNMP community setting. The Contents pane appears on the left.
- Step 3** In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > Community**. The SNMP Community Strings for Content Engine window appears.
- Step 4** In the taskbar, click the **Create New SNMP Community String** icon. The Creating New SNMP Community String for Content Engine window appears. [Table 22-2](#) describes the fields in this window.

Table 22-2 *SNMP Community Settings*

GUI Parameter	Function
Community* ¹	Community string used as a password for authentication when you access the SNMP agent of the Content Engine. The “Community Name” field of any SNMP message sent to the Content Engine must match the community string defined here in order to be authenticated. Entering a community string enables the SNMP agent. You can enter a maximum of 256 characters in this field.
Groupname/rw*	Group to which the community string belongs. The rw option allows a read or write group to be associated with this community string. The rw option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list: <ul style="list-style-type: none"> • None—Choose this option if you do not want to specify a group name to be associated with the community string. If you enter a group name after selecting this option, an error message is displayed. The Group Name field remains disabled if you select this option. • Rw—Choose this option if you want to allow read-write access to the group associated with a community string. The Group Name field remains disabled if you select this option. • Group—Choose this option if you want to specify a group name.
Group Name*	Name of the group to which the community string belongs. You can enter a maximum of 256 characters in this field. This field is available only if you have chosen the group option in the previous field.

1. * = Required field.

Step 5 In the appropriate fields, enter the community string, choose whether or not read-write access to the group is allowed, and enter the group name.

Step 6 To save the settings, click **Submit**.

To enable the SNMP agent and configure a community string from the CLI, use the following global configuration command:

```
snmp-server community string [group groupname | rw]
```

Configuring SNMP Group Settings



Note

Groups are listed in the order in which they have been created. The maximum number of SNMP groups that can be created is ten.

To define a user security model group, follow these steps:

Step 1 Choose **Devices > Devices**. The Devices window appears.

- Step 2** Click the **Edit** icon next to the Content Engine for which you want to create an SNMP group. The Device Home window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > Group**. The SNMP Group Strings for Content Engine window appears.
- Step 4** In the taskbar, click the **Create New SNMP Group String** icon. The Creating New SNMP Group String for Content Engine window appears. [Table 22-3](#) describes the fields in this window.

Table 22-3 *SNMP Group Settings*

GUI Parameter	Function
Name	Name of the SNMP group. You can enter a maximum of 256 characters.
Sec Model	Security model for the group. Choose one of the following options from the drop-down list: <ul style="list-style-type: none"> v1—Version 1 security model (SNMP Version 1 [noAuthNoPriv]). v2c—Version 2c security model (SNMP Version 2 [noAuthNoPriv]). v3-auth—User security level SNMP Version 3 AuthNoPriv. v3-noauth—User security level SNMP Version 3 noAuthNoPriv. v3-priv— User security level SNMP Version 3 AuthPriv.
Read View	Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. In order to provide read access to users of the group, a view must be specified.
Write View	Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined.
Notify View	Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined.

- Step 5** In the appropriate fields, enter the SNMP group configuration name, the security model, and the names of the read, write, and notify views.
- Step 6** To save the settings, click **Submit**.

To define a user security model group from the CLI, use the following global configuration command:

```
snmp-server group name { v1 [notify name] [read name] [write name] | v2c [notify name] [read name] [write name] | v3 { auth [notify name] [read name] [write name] | noauth [notify name] [read name] [write name] | priv [notify name] [read name] [write name] } }
```

Configuring SNMP User Settings



Note

Users are listed in the order in which they have been created. The maximum number of users that can be created is ten.

To define a user who can access the SNMP engine, follow these steps:

- Step 1** Choose **Devices > Devices**. The Devices window appears.
- Step 2** Click the **Edit** icon next to the Content Engine for which you want to create an SNMP user. The Contents pane appears on the left.
- Step 3** In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > User**. The SNMP Users for Content Engine window appears.
- Step 4** In the taskbar, click the **Create New SNMP User** icon. The Creating New SNMP User window appears. [Table 22-4](#) describes the fields in this window.

Table 22-4 *SNMP User Settings*

GUI Parameter	Function
Name	String representing the name of the user (256 characters maximum) who can access the Content Engine.
Group	Name of the group (256 characters maximum) to which the user belongs.
Remote SNMP ID	Globally unique identifier for a remote SNMP entity. To send an SNMPv3 message to the Content Engine, at least one user with a remote SnpID must be configured on the Content Engine. The SnpID must be entered in octet string format.
Authentication Algorithm	Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list: <ul style="list-style-type: none"> • No-auth—Requires no security mechanism to be turned on for SNMP packets. • MD5—Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm. • SHA—Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.
Authentication Password	String (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display. This field is optional if the no-auth option is chosen for the authentication algorithm. Otherwise, this field must contain a value.

Table 22-4 SNMP User Settings (continued)

GUI Parameter	Function
Confirmation Password	Authentication password for confirmation. The reentered password must be the same as the one entered in the previous field.
Private Password	String (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters will be adjusted to fit the display area if it exceeds the limit for display.
Confirmation Password	Private password for confirmation. The reentered password must be the same as the one entered in the previous field.

- Step 5** In the appropriate fields, enter the user name, the group to which the user belongs, the engine identity of the remote entity to which the user belongs, the authentication algorithm used to protect SNMP traffic from tampering, the user authentication parameters, and the authentication parameters for the packet.
- Step 6** To save the settings, click **Submit**.

To define a user who can access the SNMP engine from the CLI, use the following global configuration command:

```
snmp-server user name group [auth {md5 password [priv password] | sha password [priv password]} | remote octetstring [auth {md5 password [priv password] | sha password [priv password]}]]
```

Configuring SNMPv2 View Settings



Note

Views are listed in the order in which they have been created. The maximum number of views that can be created is ten.

To define a Version 2 SNMP (SNMPv2) MIB view, follow these steps:

- Step 1** Choose **Devices > Devices**. The Devices window appears.
- Step 2** Click the **Edit** icon next to the Content Engine for which you want to create an SNMPv2 view. The Contents pane appears on the left.
- Step 3** In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > View**. The SNMP Views for Content Engine window appears.
- Step 4** In the taskbar, click the **Create New View** icon. The Creating New SNMP View window appears. [Table 22-5](#) describes the fields in this window.

Table 22-5 *SNMPv2 View Settings*

GUI Parameter	Function	CLI Command
Name	String representing the name of this family of view subtrees (256 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB.	snmp-server view <i>viewname</i>
Family	Object identifier (256 characters maximum) that identifies a subtree of the MIB.	snmp-server view <i>viewname</i> <i>MIBfamily</i>
View Type	View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list: <ul style="list-style-type: none"> Included—The MIB family is included in the view. Excluded—The MIB family is excluded from the view. 	snmp-server view <i>viewname</i> <i>MIBfamily</i> { excluded included }

Step 5 In the appropriate fields, enter the view name, the family name, and the view type.

Step 6 To save the settings, click **Submit**.

Configuring SNMP Host Settings



Note Hosts are listed in the order in which they have been created. The maximum number of SNMP hosts that can be created is four.

To configure SNMP host settings, follow these steps:

Step 1 Choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the Content Engine for which you want to define an SNMP host. The Device Home window appears with the Contents pane on the left.

Step 3 In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > Host**. The SNMP Hosts for Content Engine window appears.

Step 4 In the taskbar, click the **Create New SNMP Host** icon. The Creating New SNMP Host window appears. [Table 22-6](#) describes the fields in this table.

Table 22-6 *SNMP Host Settings*

GUI Parameter	Function	CLI Command
Trap Host	Host name or IP address of the SNMP trap host that is sent in SNMP trap messages from the Content Engine.	snmp-server host { <i>hostname</i> <i>ipaddress</i> }
Community/User	Name of the SNMP community or user (256 characters maximum) that is sent in SNMP trap messages from the Content Engine.	snmp-server host { <i>hostname</i> <i>ipaddress</i> } <i>communitystring</i>
Authentication	Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list: <ul style="list-style-type: none"> No-auth—Sends notification without any security mechanism. v2c-noauth—Sends notification using Version 2c security. Model v3-auth—Sends notification using SNMP Version 3 AuthNoPriv. Security Level v3-noauth—Sends notification using SNMP Version 3 NoAuthNoPriv security. Level v3-priv—Sends notification using SNMP Version 3 AuthPriv security. 	snmp-server host { <i>hostname</i> <i>ipaddress</i> } <i>communitystring</i> [v2c [retry num] [timeout seconds]] v3 { auth [retry num] [timeout seconds]} noauth [retry num] [timeout seconds]} priv [retry num] [timeout seconds]}}
Retry	Number of retries (1–10) allowed for the inform request. The default is 2 tries.	
Timeout	Timeout for the inform request in seconds (1–1000). The default is 15 seconds.	

Step 5 Enter the host name or IP address of an SNMP trap host, SNMP community or user name, security model to send notification, and retry count and timeout for inform requests.

Step 6 To save the settings, click **Submit**.

Configuring SNMP Asset Tag Settings

To configure SNMP asset tag settings, follow these steps:

Step 1 Choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the Content Engine for which you want to define an SNMP asset tag. The Contents pane appears on the left.

Step 3 In the Contents pane, choose **General Settings > Notification and Tracking > SNMP > Asset Tag**. The SNMP Asset Tag Settings for Content Engine window appears.

- Step 4** In the Asset Tag Name field, enter a name for the asset tag.
- Step 5** To save the settings, click **Submit**.
-

To configure SNMP asset tag settings from the CLI, use the **asset tag** global configuration command.

Supported MIBs

The SNMP agent supports the following MIBs:

- CISCO-CDP-MIB
- ENTITY-MIB
- CISCO-ENTITY-ASSET-MIB
- MIB-II
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB (supports streaming media-related MIB objects)
- HOST-RESOURCES-MIB
- EVENT-MIB

The EVENT-MIB can set the threshold on any MIB variables supported by ACNS 5.x software and store the threshold permanently on disk. The HOST-RESOURCES-MIB provides statistics on system resources.

The CISCO-CONTENT-ENGINE-MIB is extended to incorporate MIB objects related to streaming. The WMT, Cisco Streaming Engine, and RealProxy MIB groups incorporate statistics about the WMT server or proxy, Cisco Streaming Engine, and Real Proxy. For each 64-bit counter MIB object, a 32-bit counter MIB object is implemented so that SNMP clients using the SNMPv1 protocol can retrieve data associated with 64-bit counter MIB objects. The MIB objects of each of these groups are read-only.

- The WMT MIB group provides statistics about WMT proxy and server performance. Twenty-eight MIB objects are implemented in this group. Six of these MIB objects are implemented as 64-bit counters.
- The Cisco Streaming Engine MIB group provides statistics about RTSP streaming engine performance. Seven MIB objects are implemented in this group. Two of these MIB objects are implemented as 64-bit counters.
- The RealProxy MIB group provides statistics about RealProxy performance. Fourteen MIB objects are implemented in this group.

Use the following link to access these MIBs:

<ftp://ftp.cisco.com/pub/mibs/v2/>



Note

If your browser is located behind a firewall or you are connecting to the Internet with a DSL modem and you are unable to access this file folder, you must change your web browser compatibility settings. In the Internet Explorer (IE) web browser, choose **Tools > Internet options > Advanced**, and check the “Use Passive FTP” checkbox.

Key SNMP CLI Commands

Use the **snmp-server group** global configuration command to select one of the three SNMP versions, SNMPv1, SNMPv2c, or SNMPv3. Use the **no** form of this command to remove the specified version. Refer to the *Cisco ACNS Software Command Reference, Release 5.4* for more information on how to use this and other SNMP commands.

The **snmp-server community string** command provides view-based access control for SNMPv1, SNMPv2c, and SNMPv3 but also continues to provide backward compatibility between different versions. The previous version of this command did not have an option to create a community string that allows SNMP messages to execute a set operation on a MIB object. An **rw** option has been introduced for this purpose. Also, the previous version of the SNMP agent did not provide selective access control to MIB objects. Access to any MIB object was denied or granted based on authentication of the SNMP community string. With the introduction of view-based access control, it is now possible to configure a community string that grants access to only part of the MIB subtree. To provide backward compatibility with the previous version of this command, a default read group or default write group (if the **rw** option is specified on the command line) is associated with the community string if no group name is specified. Both of these default groups are hidden from users and not displayed in the configuration file or in the **show snmp group** command, but they are created during initialization of the SNMP agent.

**Note**

The SNMP agent is disabled by default, and a community string is not configured.

The following example enables the SNMP agent and assigns the community string *comaccess* to SNMP:

```
507-1(config)# snmp-server community comaccess
```

The preceding example defines a community string *comaccess* used as a password for authentication when you access the SNMP agent of the Content Engine. Any SNMP message sent to the Content Engine must have the “Community Name” field of the message match the community string defined here to be authenticated. Entering a community string enables the SNMP agent.

The following example disables the SNMP agent and removes the previously defined community string.

```
507-1(config)# no snmp-server community
```

