Configuring SNMP Monitoring

Last Updated: July 25, 2006

This chapter describes the procedures for configuring Simple Network Monitoring Protocol (SNMP) on the Cisco Unity Express module to monitor the system's health, conduct performance monitoring, collect data, and manage traps for Cisco Unity Express voicemail and auto attendant applications.

See the *Cisco Unity Express SNMP MIB Support* guide for details about the CISCO-UNITY-EXPRESS-MIB.

The system monitoring commands are not available through the Cisco Unity Express graphical user interface (GUI).

This chapter contains the following sections:

- Prerequisites for Implementing SNMP Monitoring on Cisco Unity Express, page 325
- Enabling the SNMP Agent, Passwords, and Trap Server, page 325
- Setting Threshold Values for Subscriber Responses, page 328
- Enabling Cisco Unity Express Shutdown Requests, page 331

Prerequisites for Implementing SNMP Monitoring on Cisco Unity Express

See the *Cisco Unity Express SNMP MIB Support* guide for details about installing the CISCO-UNITY-EXPRESS-MIB on the Cisco Unity Express module.

Enabling the SNMP Agent, Passwords, and Trap Server

Activating the SNMP system monitoring on Cisco Unity Express requires the following tasks:

- Enabling the SNMP agent.
- Specifying the SNMP notification passwords.
- Specifying at least one host server that will receive the notifications.

Prerequisites

Be sure that the appropriate MIBs are installed. See the *Cisco Unity Express SNMP MIB Support* guide for details.

Required Data for This Procedure

- Passwords that permit subscribers to retrieve and change SNMP information. Specify whether these passwords will have read-only or read-write privileges. The system supports a maximum of 5 read-only and 5 read-write passwords. Each password may have a maximum of 15 alphanumeric characters, including letters A to Z, letters a to z, digits 0 to 9, underscore (_), and hyphen (-).
- IP address and password of the host server that will receive the SNMP information. If no host is defined, the system discards the trap information. The system supports a maximum of 5 servers. The password does not have to be the same as the subscriber passwords.

  No host is considered the primary host. The system sends the SNMP notifications to all enabled hosts.
- (Optional) Server contact and location information.

SUMMARY STEPS

1. **config t**
2. **snmp-server community** *community-string* {**ro** | **rw**}
3. **snmp-server enable traps**
4. **snmp-server host** *host-ipaddress community-string*
5. (Optional) **snmp-server contact** *contact-string*
6. (Optional) **snmp-server location** *location-string*
7. **end**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `se-10-0-0-0# config t`	Enters configuration mode.

Step 2	**snmp-server community** *community-string* {**ro** | **rw**}
	
	Example:
	`se-10-0-0-0(config)# snmp-server community myaccess rw`
	`se-10-0-0-0(config)# snmp-server community youraccess ro`
		Enables the SNMP agent and defines SNMP passwords.
		• *community-string*—Specifies an SNMP password. The maximum length is 15 alphanumeric characters, which includes letter A to Z, letters a to z, digits 0 to 9, underscore (_), and hyphen (-). The first character does not have to be a letter.
		• **ro**—The password has read-only capability. The system supports a maximum of 5 **ro** passwords.
		• **rw**—The password has read and write capabilities. The system supports a maximum of 5 **rw** passwords.

Step 3	**snmp-server enable traps** **Example:** `se-10-0-0-0(config)# snmp-server enable traps`	Enables SNMP traps. SNMP traps are disabled by default. Use this command in conjunction with the **snmp-server host** command to identify at least one server that will receive the SNMP notifications.

Step 4	**snmp-server host** *host-ipaddress community-string*
	
	Example:
	`se-10-0-0-0(config)# snmp-server host 172.16.100.10 iminhere`
	`se-10-0-0-0(config)# snmp-server host 172.16.100.20 bigtraps`
	`se-10-0-0-0(config)# snmp-server host 172.16.100.30 traps4cue`
		Specifies a server that accepts the SNMP notifications.
		• *host-ipaddress*—IP address of the server. Enable at least one host. The system supports a maximum of 5 hosts.
		• *community-string*—Specifies an SNMP password. The maximum length is 15 alphanumeric characters. This password does not have to be the same as those defined with the **snmp-server community** command.

Step 5	**snmp-server contact "***contact-string***"** **Example:** `se-10-0-0-0(config)# snmp-server contact "Dial 71111 for system operator"`	(Optional) Specifies SNMP server contact information. Maximum length is 31 alphanumeric characters. This value sets the MIB's sysContact string. Enclose the text in double quotes (" ").

	Command or Action	Purpose
Step 6	**snmp-server location "***location-string***"** **Example:** `se-10-0-0-0(config)# snmp-server location "Bldg A NYC"`	(Optional) Specifies SNMP server location information. Maximum length is 31 alphanumeric characters. This value sets the MIB's sysLocation string. Enclose the text in double quotes (" ").
Step 7	**end** **Example:** `se-10-0-0-0(config)# end`	Exits configuration mode.
Step 8	**copy running-config startup-config** **Example:** `se-10-0-0-0# copy running-config startup-config`	Saves the configuration changes.

Verifying the Enabling of the SNMP Agent, Passwords, and Trap Server

Use the **show snmp configuration** command in Cisco Unity Express EXEC mode to display the SNMP agent status and passwords.

The following example shows output from the **show snmp configuration** command:

```
se-10-0-0-0# config t

Enter configuration commands, one per line.  End with CNTL/Z.
se-10-0-0-0(config)# snmp-server community myaccess rw
se-10-0-0-0(config)# snmp-server community iminhere ro
se-10-0-0-0(config)# snmp-server enable traps
se-10-0-0-0(config)# snmp-server host 172.16.160.224 bigtraps
se-10-0-0-0(config)# snmp-server contact "Dial 71111 for system operator"
se-10-0-0-0(config)# snmp-server location "Bldg A NYC"
se-10-0-0-0(config)# end

se-10-0-0-0# show snmp configuration
Contact:              Dial 71111 for system operator
Location:             Bldg A NYC
Community 1 RO:       iminhere
Community 1 RW:       admin_main
Community 2 RW:       myaccess
Traps:                enabled
Host Community 1:     172.16.160.224 bigtraps
cueShutdownRequest:   disabled
se-10-0-0-0#
```

Setting Threshold Values for Subscriber Responses

Tracking spikes in the number of failures that occur within a short period of time for certain subscriber actions helps to identify possible security breaches in the system.

Each subscriber action has a default threshold value. Use the commands in this section if you want to change the default values.

Cisco Unity Express supports setting thresholds for the number of failures in a 5-minute interval for the following subscriber actions:

- Logging in.
- Entering a password.
- Entering a personal identification number (PIN) user ID.
- Entering a PIN password.
- Resetting a PIN.

When the number of attempts reaches the action's threshold, the system sends a notification to the SNMP host.

Prerequisites

Be sure that the appropriate MIBs are installed. See the *Cisco Unity Express SNMP MIB Support* guide for details.

Required Data for This Procedure

Number of times the following can occur before the system sends a notification to the SNMP host:

- Password errors (default is 30)
- Login errors (default is 30)
- PIN password errors (default is 30)
- PIN resets (default is 5)
- PIN user ID errors (default is 30)

SUMMARY STEPS

1. **config t**
2. (Optional) **notification security login user** *threshold*
3. (Optional) **notification security login password** *threshold*
4. (Optional) **notification security pin uid** *threshold*
5. (Optional) **notification security pin password** *threshold*
6. (Optional) **notification security pin reset** *threshold*
7. **end**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `se-10-0-0-0# config t`	Enters configuration mode.
Step 2	**notification security login user** *threshold* **Example:** `se-10-0-0-0(config)# notification security login user 10`	(Optional) Sets the number of invalid login names within a 5-minute interval to *threshold*. If the number of failures exceeds this value, the system sends a notification to the SNMP host. The default value is 30. Valid values are 0 to 999.
Step 3	**notification security login password** *threshold* **Example:** `se-10-0-0-0(config)# notification security login password 6`	(Optional) Sets the number of invalid login passwords within a 5-minute interval to *threshold*. If the number of failures exceeds this value, the system sends a notification to the SNMP host. The default value is 30. Valid values are 0 to 999.
Step 4	**notification security pin uid** *threshold* **Example:** `se-10-0-0-0(config)# notification pin uid 12`	(Optional) Sets the number of invalid PIN user IDs within a 5-minute interval to *threshold*. If the number of failures exceeds this value, the system sends a notification to the SNMP host. The default value is 30. Valid values are 0 to 999.
Step 5	**notification security pin password** *threshold* **Example:** `se-10-0-0-0(config)# notification security pin password 8`	(Optional) Sets the number of invalid PIN passwords within a 5-minute interval to *threshold*. If the number of failures exceeds this value, the system sends a notification to the SNMP host. The default value is 30. Valid values are 0 to 999.
Step 6	**notification security pin reset** *threshold* **Example:** `se-10-0-0-0(config)# notification security pin rest 3`	(Optional) Sets the number of PIN password resets within a 5-minute interval to *threshold*. If the number of resets exceeds this value, the system sends a notification to the SNMP host. The default value is 5. Valid values are 0 to 999.

	Command or Action	Purpose
Step 7	**end** **Example:** `se-10-0-0-0(config)# end`	Exits configuration mode.
Step 8	**copy running-config startup-config** **Example:** `se-10-0-0-0# copy running-config startup-config`	Saves the configuration changes.

Verifying the SNMP Login and PIN Notification Thresholds

Use the **show notification configuration** command in Cisco Unity Express EXEC mode to display the SNMP login and password notification thresholds.

The following example shows output from the **show notification configuration** command:

```
se-10-0-0-0# config t
Enter configuration commands, one per line.  End with CNTL/Z.
se-10-0-0-0(config)# notification security login user 10
se-10-0-0-0(config)# notification security login password 6
se-10-0-0-0(config)# notification security pin uid 12
se-10-0-0-0(config)# notification security pin password 8
se-10-0-0-0(config)# notification security pin reset 3
se-10-0-0-0(config)# end
se-10-0-0-0# show notification configuration
Login user threshold:          10    (errors within a 5 minute interval)
Login password threshold:      6     (errors within a 5 minute interval)
PIN uid threshold:             12    (errors within a 5 minute interval)
PIN password threshold:        8     (errors within a 5 minute interval)
PIN reset threshold:           3     (resets within a 5 minute interval)
se-10-0-0-0#
```

Enabling Cisco Unity Express Shutdown Requests

Enabling shutdown requests allows the Cisco Unity Express module to be gracefully halted. For example, suppose an uninterruptible power supply (UPS) sends a power out alert to the Cisco Unity Express management application. The management application would send an SNMP shutdown request to bring down the Cisco Unity Express module while power is still supplied from the UPS.

For security reasons, the shutdown capability is disabled by default.

To reset the Cisco Unity Express module, use the **service-module service-engine** *slot/port* **reset** command on the router housing the module.

Prerequisites

Be sure that the appropriate MIBs are installed. See the *Cisco Unity Express SNMP MIB Support* guide for details.

SUMMARY STEPS

1. **config t**
2. **snmp-server enable cueShutdownRequest**
3. **end**
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `se-10-0-0-0# config t`	Enters configuration mode.
Step 2	**snmp-server enable cueShutdownRequest** **Example:** `se-10-0-0-0(config)# snmp-server enable cueShutdownRequest`	Enables Cisco Unity Express shutdown requests. Shutdown requests are disabled by default.
Step 3	**end** **Example:** `se-10-0-0-0(config)# end`	Exits configuration mode.
Step 4	**copy running-config startup-config** **Example:** `se-10-0-0-0# copy running-config startup-config`	Saves the configuration changes.

Verifying the Enabling of Shutdown Requests

Use the **show snmp configuration** command in Cisco Unity Express EXEC mode to display the status of the shutdown request capability.

The following example shows output from the **show snmp configuration** command:

```
se-10-0-0-0# show snmp configuration
Contact:              Dial 71111 for system operator
Location:             Bldg A NYC
Community 1 RO:       iminhere
Community 1 RW:       admin_main
Community 2 RW:       myaccess
Traps:                enabled
Host Community 1:     172.16.160.224 bigtraps
cueShutdownRequest    enabled
se-10-0-0-0#
```