Configuring the Management Interface and Security

Revised: February 07, 2014, OL-29134-02

Introduction

This chapter describes how to configure the physical management interfaces (ports) as well as the various management interface applications, such as SNMP, SSH, and TACACS+. It also explains how to configure users, passwords, IP configuration, clock and time zone, and domain name settings.

- Management Interface and Security, page 5-2
- Configuring the Management Ports, page 5-3
- Configuring Management Interface VLANs, page 5-11
- Mapping of VLAN ID to Virtual Gi ID, page 5-14
- TACACS+ Authentication, Authorization, and Accounting, page 5-18
- Configuring Access Control Lists (ACLs), page 5-35
- Managing the Telnet Interface, page 5-38
- Configuring the SSH Server, page 5-40
- Configuring and Managing the SNMP Interface, page 5-44

Management Interface and Security

The Cisco SCE 8000 platform is equipped with two RJ-45 management ports (Port1 and Port2 on the Cisco SCE 8000-SCM-E module in slot 1). These ports provide access from a remote management console to the Cisco SCE platform via a LAN.

The two management ports support management interface redundancy, providing the possibility for a backup management link.

Note The second management port is reflected in all objects related to it in the SNMP interface.

Note Cisco SCE 8000 does not support IPv6 addresses or connectivity on the management interfaces.

Perform the following tasks to configure the management interface and management interface security:

- Configure the management port:
  - Physical parameters
  - Specify active port (if not redundant installation)
  - Redundancy (if redundant installation)
- Configure management interface security
  - Configure the permitted and not-permitted IP addresses

Configuring the Management Ports

- Entering the Management Interface Configuration Mode, page 5-3
- Configuring the Management Port Physical Parameters, page 5-4
- Management Interface Redundancy, page 5-8
- Monitoring the Management Interface, page 5-10

Perform the following tasks to configure the management ports:

- Configure the IP address and subnet mask (only one IP address for the management interface, not one IP address per port).
- Configure physical parameters:
  - Duplex
  - Speed
  - active port (optional)
- Configure redundant management interface behavior (optional):
  - Failover mode

Step 1 Cable the desired management port, connecting it to the remote management console via the LAN. If connecting both management ports for redundancy, connect the to the LAN using a switch.

Step 2 Configure the management port physical parameters. (See "Configuring the Management Port Physical Parameters" section on page 5-4.)

Step 3 (Optional) Configure the system with management interface redundancy. (see "Management Interface Redundancy" section on page 5-8.)

Entering the Management Interface Configuration Mode

When entering Management Interface Configuration Mode, you must indicate the number of the management port to be configured:

- 0/1—Port1
- 0/2—Port2

The following Management Interface commands are applied only to the port specified when entering Management Interface Configuration Mode. Therefore, each port must be configured separately:

- **speed**
- **duplex**

The following Management Interface commands are applied to both management ports, regardless of which port had been specified when entering Management Interface Configuration Mode. Therefore, both ports are configured with one command:

- **ip address**
- **auto-failover**

The GBE management interface is configured as follows:

- mode: MNG Interface configuration mode
- interface designation: 0/1 or 0/2

Step 1 Enter **configure** and press **Enter**.

Enters Global Configuration mode.

The command prompt changes to SCE(config)#.

Step 2 Enter **interface mng (0/1 | 0/2)** and press **Enter**.

Enters Management Interface Configuration mode.

The command prompt changes to SCE(config if)#

Configuring the Management Port Physical Parameters

This interface has a transmission rate of 10, 100, or 1000 Mbps and is used for management operations and for transmitting RDRs, which are the output of traffic analysis and management operations.

- Setting the IP Address and Subnet Mask of the Management Interface, page 5-4
- Configuring the Management Interface Speed and Duplex Parameters, page 5-5
- Specifying the Active Management Port, page 5-7

Setting the IP Address and Subnet Mask of the Management Interface

You must define the IP address of the management interface.

When both management ports are connected, providing a redundant management port, this IP address always acts as a virtual IP address for the currently active management port, regardless of which port is the active port.

Options

The following options are available:

- **IP address—**The IP address of the management interface.

  If both management ports are connected, so that a backup management link is available, this IP address will be act as a virtual IP address for the currently active management port, regardless of which physical port is currently active.

  The following IP addresses are used internally by the Cisco SCE 8000 platform and cannot be assigned to the management interface:

  - 192.168.207.241 to 192.168.207.255
  - 92.168.207.145 to 192.168.207.159

- **subnet mask—**Subnet mask of the management interface.

Step 1 On a physically connected local console, access the interface configuration mode for either management interface. The specified IP address is configured for both interfaces.

From the SCE(config)# prompt, type **interface Mng (0/1 | 0/2)** and press **Enter**.

Step 2 From the SCE(config if)# prompt, type **ip address** *ip-address subnet-mask* and press **Enter**.

The command might fail if there is a routing table entry that is not part of the new subnet defined by the new IP address and subnet mask.

Caution Changing the IP address of the management interface via telnet will result in loss of the telnet connection and inability to reconnect with the interface.

Note After changing the IP address, you must reload the Cisco SCE platform so that the change will take effect properly in all internal and external components of the Cisco SCE platform. (See "Rebooting and Shutting Down the Cisco SCE Platform" section on page 3-23.)

Setting the IP Address and Subnet Mask of the Management Interface: Example

The following example shows how to set the IP address of the Cisco SCE platform to 10.1.1.1 and the subnet mask to 255.255.0.0.

```
SCE#config
SCE(config)#interface mng 0/1
SCE(config if)#ip address 10.1.1.1 255.255.0.0
```

Configuring the Management Interface Speed and Duplex Parameters

This section presents sample procedures that describe how to configure the speed and the duplex of the management interface.

Both these parameters must be configured separately for each port.

- Interface State Relationship to Speed and Duplex, page 5-6
- How to Configure the Speed of the Management Interface, page 5-6
- How to Configure the Duplex Operation of the Management Interface, page 5-7

Interface State Relationship to Speed and Duplex

Table 5-1 summarizes the relationship between the interface state and speed and duplex.

Note It is not possible to set one parameter to "Auto" and to specify the other parameter. If either speed or duplex is set to "Auto", then both parameters will behave as if set to "Auto".

Table 5-1 Interface State Relationship to Speed and Duplex

Speed	Duplex	Actual GBE Interface State
Auto	Auto	Auto negotiation
Auto	Full/Half	Auto negotiation
10/100/1000	Auto	Auto negotiation
10	Full	10 Mbps and full duplex
10	Half	10 Mbps and half duplex
100	Full	100 Mbps and full duplex
100	Half	100 Mbps and half duplex

How to Configure the Speed of the Management Interface

Options

The following options are available:

- **speed—**Speed in Mbps of the currently selected management port (0/1 or 0/2):
  - **10**
  - **100**
  - **auto** (default)—Auto-negotiation (do not force speed on the link)

If the duplex parameter is configured to **auto**, changing the speed parameter has no effect.

Step 1 Access the interface configuration mode for the management interface you want to configure.

From the SCE(config)# prompt, type **interface Mng (0/1 | 0/2)** and press **Enter**.

Step 2 From the SCE(config if)# prompt, type **speed (10|100|auto)** and press **Enter**.

Specify the desired speed option.

Configuring the Speed of the Management Interface: Example

The following example shows how to use this command to configure the Management port to 100 Mbps speed.

```
SCE#config
SCE(config)#interface mng 0/1
SCE(config if)#speed 100
```

How to Configure the Duplex Operation of the Management Interface

Options

The following options are available:

- **duplex—**Duplex operation of the management port (0/1 or 0/2):
  - full
  - half
  - auto (default)—Auto-negotiation (do not force duplex on the link)

If the speed parameter is configured to **auto**, changing the duplex parameter has no effect.

Step 1 Access the interface configuration mode for the management interface you want to configure.

From the SCE(config)# prompt, type **interface Mng (0/1 | 0/2)** and press **Enter**.

Step 2 From the SCE(config if)# prompt, type **duplex auto|full|half** and press **Enter**.

Specify the desired duplex option.

Configuring the Duplex Operation of the Management Interface: Example

The following example shows how to use this command to configure the management port to half duplex mode.

```
SCE#config
SCE(config)#interface mng 0/2
SCE(config if)#duplex half
```

Specifying the Active Management Port

This command explicitly specifies which management port is currently active. Its use varies slightly, depending on whether the management interface is configured as a redundant interface (auto failover enabled) or not (auto failover disabled).

- auto failover enabled (automatic mode)—The specified port becomes the currently active port, in effect forcing a failover action even if a failure has not occurred.
- auto failover disabled (manual mode)—The specified port should correspond to the cabled Mng port, which is the only functional port and therefore must be and remain the active management port.

Step 1 Access the interface configuration mode for the management interface you want to configure as the active management port.

From the SCE(config)# prompt, type **interface Mng (0/1 | 0/2)** and press **Enter**.

Step 2 Type **active-port** and press **Enter**

Specifying the Active Management Port: Example

The following example shows how to use this command to configure Mng port 2 as the currently active management port.

```
SCE#config
SCE(config)#interface mng 0/2
SCE(config if)#active-port
```

Management Interface Redundancy

- Configuring the Management Ports for Redundancy, page 5-8
- Configuring the Fail-Over Mode, page 5-9

The Cisco SCE platform contains two RJ-45 management ports. The two management ports provide the possibility for a redundant management interface, thus ensuring management access to the Cisco SCE platform even if there is a failure in one of the management links. If a failure is detected in the active management link, the standby port automatically becomes the new active management port.

Note that both ports must be connected to the management console via a switch. In this way, the IP address of the MNG port is always the same, regardless of which physical port is currently active.

Important information:

- Only one port is active at any time.
- The same virtual IP address and MAC address are assigned to both ports.
- Default:
  - Port 1 = active
  - Port 2 = standby
- The standby port sends no packets to the network and packets from the network are discarded.
- When a problem in the active port is encountered, the standby port automatically becomes the new active port.
- Link problem, with switch to standby MNG port, is declared after the link is down for 300 msec.
- Service does not revert to the default active port if/when that link recovers. The currently active MNG port remains active until link failure causes a switch to the other MNG port.

Configuring the Management Ports for Redundancy

Step 1 Cable both management ports (Mng 1 and Mng 2), connecting them both to the remote management console via the LAN and via a switch.

Using the switch ensures that the IP address of the MNG port is always the same, regardless of which physical port is currently active

Step 2 Configure the automatic failover mode.

See Configuring the Fail-Over Mode, page 5-9.

Step 3 Configure the IP address for the management interface.

The same IP address will always be assigned to the active management port, regardless of which physical port is currently active.

See Setting the IP Address and Subnet Mask of the Management Interface, page 5-4.

Step 4 Configure the speed and duplex for both management ports.

See Configuring the Management Interface Speed and Duplex Parameters, page 5-5.

Configuring the Fail-Over Mode

- Options, page 5-9
- How to Enable the Automatic Fail-Over Mode, page 5-9
- How to Disable the Automatic Fail-Over Mode, page 5-9

Use the following command to enable automatic failover. The automatic mode must be enabled to support management interface redundancy. This mode automatically switches to the backup management link when a failure is detected in the currently active management link.

This parameter can be configured when in management interface configuration mode for either management port, and is applied to both ports with one command.

Options

The following options are available:

- **auto/ no auto—**Enable or disable automatic failover switching mode
  - Default—Auto (automatic mode)

How to Enable the Automatic Fail-Over Mode

From the SCE(config if)# prompt, type:

Command	Purpose
auto-fail-over	Enables automatic failover mode.

How to Disable the Automatic Fail-Over Mode

From the SCE(config if)# prompt, type:

Command	Purpose
no auto-fail-over	Disables automatic failover mode.

Monitoring the Management Interface

Use this command to display the following information for the management interface.

- speed
- duplex
- IP address
- auto-failover configuration

From the SCE# prompt, type:

Command	Purpose
show mng interface Mng (0/1 | 0/2) [speed | duplex | |ip address | auto-fail-over]	Displays the specified GBE management interface configuration for the specified interface. If no option is specified, all management interface information is displayed for the specified interface.

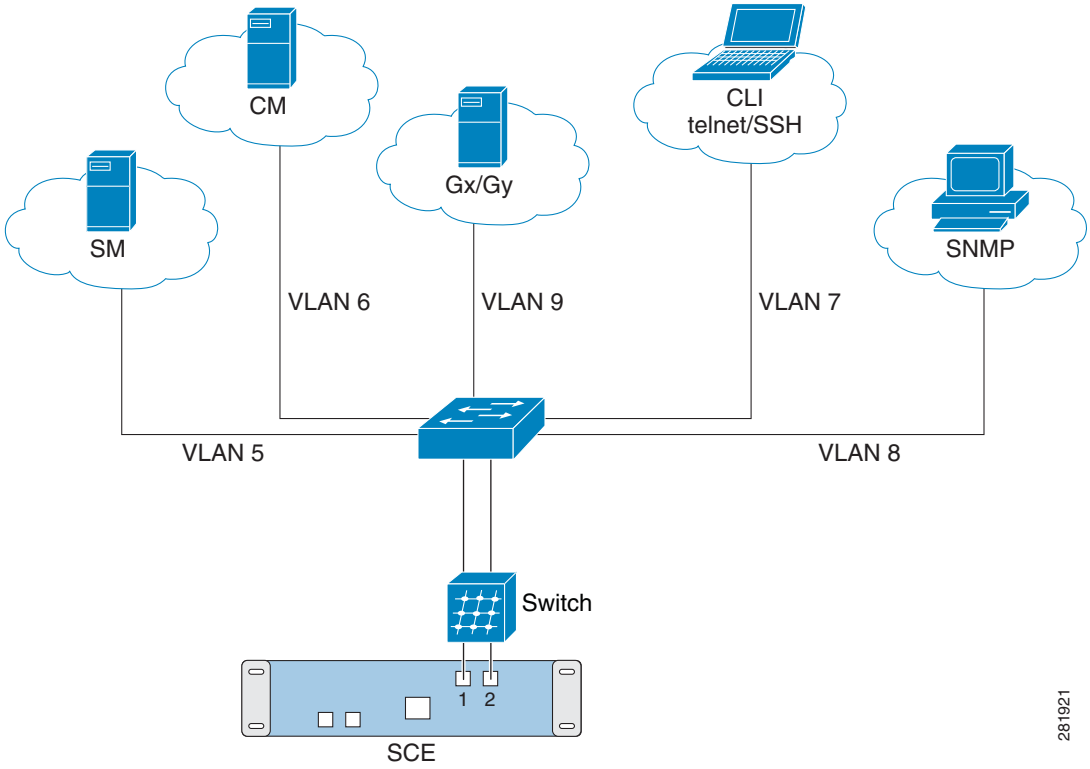
Configuring Management Interface VLANs

The Cisco SCE management network interface is used for various management services such as:

- Accessing the Cisco SCE shell through Telnet or SSH.
- SNMP

Management interface VLANS provide a way to distinguish between these management services (Telnet, SSH, SNMP) by using separate VLANs carried over same physical port (see Figure 5-1).

Figure 5-1 Management Interface VLANS



There are two steps in configuring management VLANs:

1. Create the VLAN and assign an IP address (**mng-vlan** command).
2. Assign the VLAN to a management or control service. Use one of the following commands:
   - **ip ssh mng-vlan**
   - **vty mng-vlan**
   - **snmp-server mng-vlan**

When a new management VLAN is configured, the device adds a new routing entry in the routing table. So, each configured IP address should be routable from the Cisco SCE.

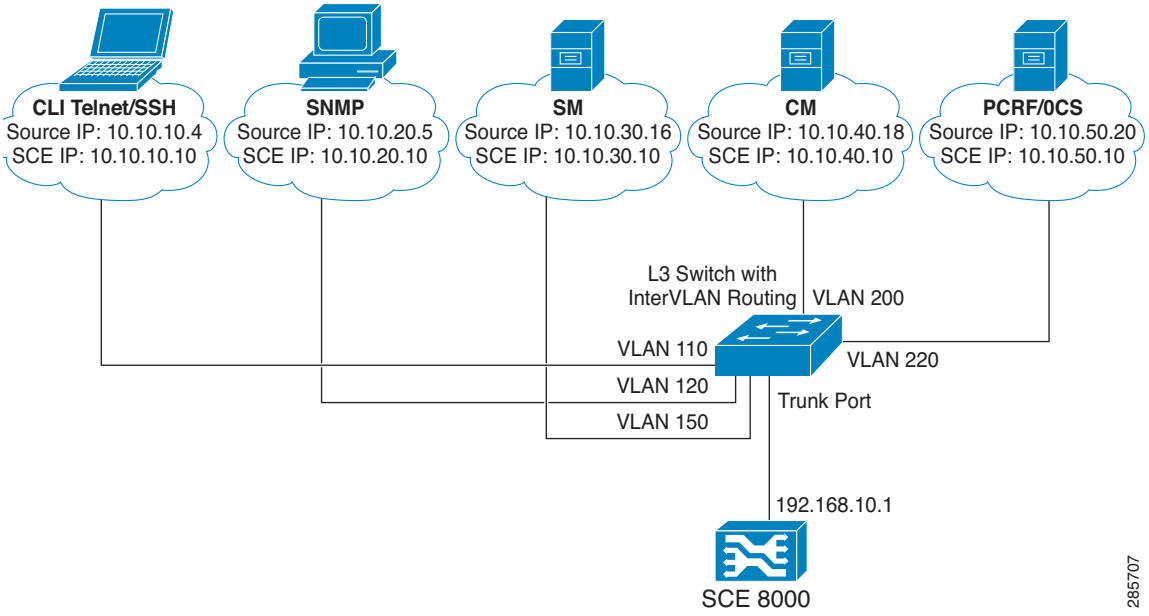
Here is an example of a sample configuration.

The following are some of the valid IP entries:

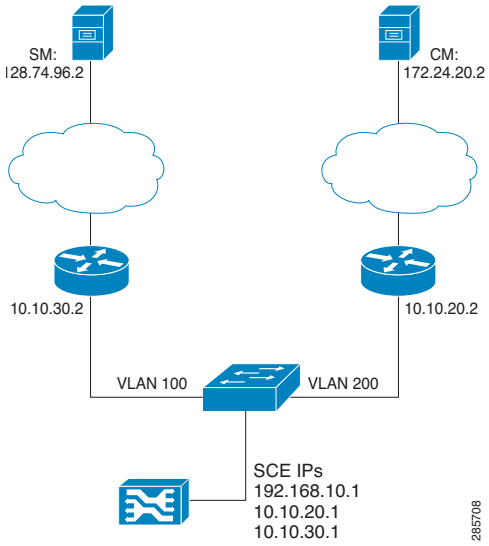
- 10.10.10.10/255.255.255.192 - VLAN ID 100
- 10.10.20.10/255.255.255.192 - VLAN ID 120
- 10.10.30.10/255.255.255.192 - VLAN ID 150

If the IP addresses listed above are added, the device creates the following entries in the routing table:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.20.0	*	255.255.255.192	U	0	0		0bond0.120
10.10.30.0	*	255.255.255.192	U	0	0		0bond0.150
10.10.10.0	*	255.255.255.192	U	0	0		0bond0.100



The following diagram provides another view of the configured management VLAN:



SUMMARY STEPS

1. **enable**
2. **configure**
3. **mng-vlan** *vlan-id* **address** *ip-address* **mask** *mask*
4. **<service> mng-vlan** *vlan-id*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `SCE> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure** **Example:** `SCE#> configure`	Enters global configuration mode.

	Command	Purpose
Step 3	**mng-vlan** *vlan-id* **address** *ip-address* **mask** *mask* **Example:** `SCE(config)#> mng-vlan 10 address 10.10.10.20 mask 255.255.255.0`	Creates the VLAN and assigns the IP address to the VLAN. Range for VLAN tag: 1-4094
Step 4	**<service> mng-vlan** *vlan-id* **Example:** `SCE(config)#> snmp-server mng-vlan 10`	Assigns the VLAN to the specified service. Service options are: • ip ssh • vty • snmp-server **Note** The **snmp-server mng-vlan** command, in either the positive or negative form, restarts the SNMP process in order for the changes to take effect. This generates a cold-start trap.

Monitoring Management VLANs

To monitor managment VLANs, use one or more of the following commands.

These commands are in viewer mode.

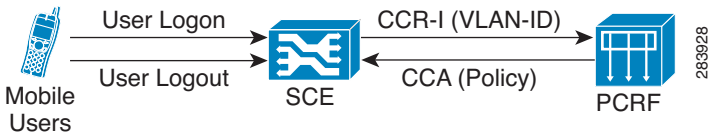
Command	Purpose
show mng-vlan [*vlan-id* **| all]**	Displays the IP configuration and configured management service for the specified management VLAN.
show vlan *vlan-id* **service-bind**	Displays the management service assigned to the specified management VLAN.
show vlan *vlan-id* **statistics**	Displays the traffic statistics for the specified VLAN.
show vty mng-vlan	Displays the management interface VLAN configured for Telnet services.
show ip ssh mng-vlan	Displays the management interface VLAN configured for SSH services.

Mapping of VLAN ID to Virtual Gi ID

The mapping of VLAN ID to virtual Gi ID feature enables Cisco SCE to map the VLAN ID retrieved from the subscriber traffic to a virtual Gi ID; thus, allowing the PCRF to fetch the policy corresponding to the VLAN ID and IP address, and send it to Cisco SCE. The physical VLAN ID received from the subscriber side traffic is in the range of 1-4094. This range (1-4094) is mapped to a static virtual ID that is of the range 1-255, and is used by the PCRF server to fetch the policy.

The mapped virtual ID is sent to the PCRF server as part of the CCR-I request. The corresponding policy is sent back to the Cisco SCE as part of the CCA answer.

Figure 5-2 Mapping of VLAN ID to Virtual ID



Gi AVP

Table 5-2 defines the Gi AVP that carries the mapped Virtual Gi ID as part of a CCR-I request:

Table 5-2 Gi Interface AVP

AVP Name	AVP Code	Value Type	Used In			
TMO-Virtual-Gi-ID	120	Uint32	CCR-I	CCA	RAR	RAA
			O (optional)	—	—	—
Subscriber-ID	443	—	—	—	—	—
Subscription-ID-Type	450	—	—	—	—	—
Subscription-ID-Data	444	—	—	—	—	—

The optional flag (O) is set for TMO-Virtual-Gi-ID and is used in CCR-I. The value type (unsigned integer 32) carries the value of the mapped virtual-ID.

Configuring VLAN ID Mapping to Virtual Gi ID

This section contains the information and instructions to configure and monitor the feature.

Following are the steps for configuring the mapping of VLAN ID to a virtual Gi interface ID.

1. Configure the VLAN ID mapping to a virtual Gi ID.
2. Configure the Gx server.
3. Enable the virtual Gi mode in the interface configuration mode.
4. Enable VLAN symmetric classification.

SUMMARY STEPS

1. **enable**
2. **configure**
3. **diameter gx virtual-gi vlan-id mapping**
4. **diameter peer**
5. **interface linecard 0**
6. **subscriber virtual-gi-mode**
7. **VLAN symmetric classify**

8. **show interface linecard 0 subscriber virtual-gi-mode**
9. **show diameter gx virtual-gi all**
10. **show running-config | include subscriber**
11. **show running-config | include diameter**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `SCE> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure** **Example:** `SCE#> configure`	Enables the global configuration mode.
Step 3	**diameter gx virtual-gi vlan-id** *vlan-id* **mapping** *value1* **Example:** `SCE(config)#> diameter Gx virtual-gi vlan-id 2 mapping 3`	Configures the VLAN-ID to virtual-Gi-ID mapping in the global configuration mode. • *vlan-id*—Specifies the vlan-id to be mapped. • *value1*—Specifies the virtual Gi ID.
Step 4	**diameter peer** *name* **peer-host** *ip-address* **[port** <*port#*>**]** **Example:** `SCE(config)#> diameter peer GX peer-host 10.78.241.155 port 3868`	Configures the Gx server (PCRF server) in the global configuration mode. • *name*—Name to be assigned to the entry in the peer table. • *ip-address*—IP address of the host. A peer is defined by an URI. This means that the same IP can not be used on different ports to distinguish between two servers except when a DNS is used. • *port#*—Port number used.
Step 5	**interface linecard 0** **Example:** `SCE(config)#> interface linecard 0`	Enables the interface configuration mode.
Step 6	**subscriber virtual-gi-mode** **Example:** `SCE(config-if)#> subscriber virtual-gi-mode`	Enables the virtual Gi mode.
Step 7	**VLAN symmetric classify** **Example:** `SCE(config-if)#> VLAN symmetric classify`	Enables VLAN symmetric classification in the interface configuration mode. This command enables VLAN-ID to be retieved from the subscriber traffic.

	Command	Purpose
Step 8	**show interface linecard 0 subscriber virtual-gi-mode** **Example:** `SCE(config)#> show interface linecard 0 subscriber virtual-gi-mode`	Enter this command in the global configuration mode. Displays the status of the virtual Gi mode.
Step 9	**show diameter gx virtual-gi all** **Example:** `SCE(config)#> show diameter gx virtual-gi all`	Displays the virtual Gi mapping table having all the existing VLAN ID to virtual Gi ID mapping.
Step 10	**show running-config | include subscriber** **Example:** `SCE(config)#> show running-config | include subscriber`	Displays the status of virtual Gi.
Step 11	**show running-config | include diameter**	Displays diameter related configurations made in the system.

Monitoring Mapping of VLAN ID to Virtual ID

To monitor mapping of VLAN ID to Virtual ID, use one or more of the following commands.

These commands are in viewer mode.

Command	Purpose
show diameter gx virtual-gi all	Displays all the VLAN ID to virtual Gi ID mappings.
show diameter gx virtual-gi vlan-id *vlan-id*	Displays a particular VLAN ID and virtual ID mapping.
show interface linecard 0 VLAN	Displays the VLAN configuration mode.
show interface linecard 0 subscriber virtual-gi-mode	Displays the status of the virtual Gi mode.

TACACS+ Authentication, Authorization, and Accounting

- Information About TACACS+ Authentication, Authorization, and Accounting, page 5-18
- Configuring the Cisco SCE Platform TACACS+ Client, page 5-22
- Managing the User Database, page 5-25
- Configuring AAA Login Authentication, page 5-29
- Configuring AAA Privilege-Level Authorization Methods, page 5-31
- Configuring AAA Command-Level Authorization Methods, page 5-31
- Configuring AAA Accounting, page 5-32
- Monitoring TACACS+, page 5-33
- Monitoring TACACS+ Users, page 5-34

Information About TACACS+ Authentication, Authorization, and Accounting

- Login Authentication, page 5-18
- Accounting, page 5-19
- Privilege-Level Authorization, page 5-19
- General AAA Fallback and Recovery Mechanism, page 5-20
- About Configuring TACACS+, page 5-21

TACACS+ is a security application that provides centralized authentication of users attempting to gain access to a network element. The implementation of TACACS+ protocol allows customers to configure one or more authentication servers for the Cisco SCE platform, providing a secure means of managing the Cisco SCE platform, as the authentication server will authenticate each user. This then centralizes the authentication database, making it easier for the customers to manage the Cisco SCE platform.

TACACS+ services are maintained in a database on a TACACS+ server running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network element are available.

The TACACS+ protocol provides authentication between the network element and the TACACS+ ACS, and it can also ensure confidentiality, if a key is configured, by encrypting all protocol exchanges between a network element and a TACACS+ server.

The TACACS+ protocol provides the following three features:

- Login authentication
- Privilege level authorization
- Accounting

Login Authentication

The Cisco SCE platform uses the TACACS+ ASCII authentication message for CLI, Telnet and SSH access.

TACACS+ allows an arbitrary conversation to be held between the server and the user until the server receives enough information to authenticate the user. This is usually done by prompting for a username and password combination.

The login and password prompts may be provided by the TACACS+ server, or if the TACACS+ server does not provide the prompts, then the local prompts will be used.

The user log in information (user name and password) is transmitted to the TACACS+ server for authentication. If the TACACS+ server indicates that the user is not authenticated, the user will be re-prompted for the user name and password. The user is re-prompted a user-configurable number of times, after which the failed login attempt is recorded in the Cisco SCE platform user log and the telnet session is terminated (unless the user is connected to the console port.)

The Cisco SCE platform will eventually receive one of the following responses from the TACACS+ server:

- ACCEPT – The user is authenticated and service may begin.
- REJECT – The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ server.
- ERROR – An error occurred at some time during authentication. This can be either at the server or in the network connection between the server and the Cisco SCE platform. If an ERROR response is received, the Cisco SCE platform will try to use an alternative method\server for authenticating the user.
- CONTINUE – The user is prompted for additional authentication information.

If the server is unavailable, the next authentication method is attempted, as explained in "General AAA Fallback and Recovery Mechanism" section on page 5-20.

Accounting

The TACACS+ accounting supports the following functionality:

- Each executed command (the command must be a valid one) will be logged using the TACACS+ accounting mechanism (including login and exit commands).
- The command is logged both before and after it is successfully executed.
- Each accounting message contains the following:
  - User name
  - Current time
  - Action performed
  - Command privilege level

TACACS+ accounting is in addition to normal local accounting using the Cisco SCE platform dbg log.

Privilege-Level Authorization

After a successful login the user is granted a default privilege level of 0, giving the user the ability to execute a limited number of commands. Changing privilege level is done by executing the "enable" command. This command initiates the privilege level authorization mechanism.

Privilege level authorization in the Cisco SCE platform is accomplished by the use of an "enable" command authentication request. When a user requests an authorization for a specified privilege level, by using the "enable" command, the Cisco SCE platform sends an authentication request to the TACACS+ server specifying the requested privilege level. The Cisco SCE platform grants the requested privilege level only after the TACACS+ server does the following:

- Authenticates the " **enable** " command password

- Verifies that the user has sufficient privileges to enter the requested privilege level.

Once the user privilege level has been determined, the user is granted access to a specified set of commands according to the level granted.

As with login authentication, if the server is unavailable, the next authentication method is attempted, as explained in "General AAA Fallback and Recovery Mechanism" section on page 5-20.

Command-Level Authorization

When command level authorization is enabled, each CLI command that is issued must be authorized by the external TACACS server before the system actually executes the command. You can configure the authorization level at which command level authorization is required. For example, you can require command level authorization only at root level.

As with login and privilege level authentication, if the TACACS+ server is unavailable, the regular fall back mechanism will be used.

General AAA Fallback and Recovery Mechanism

The Cisco SCE platform uses a fall-back mechanism to maintain service availability in case of an error.

The AAA methods available are:

- **TACACS+** – AAA is performed by the use of a TACACS+ server, allows authentication, authorization and accounting.
- **Local** – AAA is performed by the use of a local database, allows authentication and authorization.
- **Enable** – AAA is performed by the use of user configured passwords, allows authentication and authorization.
- **None** – no authentication\authorization\accounting is performed.

In the current implementation the order of the methods used isn't configurable but the customer can choose which of the methods are used. The current order is:

- **TACACS+**
- **Local**
- **Enable**
- **None**

Caution If the server goes to AAA fault, the Cisco SCE platform will not be accessible until one of the AAA methods is restored. In order to prevent this, it is advisable to use the "none" method as the last AAA method. If the Cisco SCE platform becomes inaccessible, the shell function "AAA_MethodsReset" will allow you to delete the current AAA method settings and set the AAA method used to "enable".
To run the "AAA_MethodsReset" shell function, complete the following steps:
1. Connect to AUX with username "root"
2. Run the debug shell: **scos_xinetd --service debug-shell --on**
3. Use Telnet to access the shell: **telnet localhost 2301**
4. Run the shell function: **AAA_MethodsReset**

About Configuring TACACS+

The following is a summary of the procedure for configuring TACACS+. All steps are explained in detail in the remainder of this section.

1. Configure the remote TACACS+ servers.

   Configure the remote servers for the protocols. Keep in mind the following guidelines

   – Configure the encryption key that the server and client will use.

   – The maximal user privilege level and enable password (password used when executing the enable command) should be provided.

   – The configuration should always include the root user, giving it the privilege level of 15.

   – Viewer (privilege level 5) and superuser (privilege level 10) user IDs should be established at this time also.

1. For complete details on server configuration, refer to the appropriate configuration guide for the particular TACACS+ server that you will be using.
2. Configure the Cisco SCE client to work with TACACS+ server:

   – hostname of the server

   – port number

   – shared encryption key (the configured encryption key must match the encryption key configured on the server in order for the client and server to communicate.)
3. (Optional) Configure the local database, if used.

   – add new users

   If the local database and TACACS+ are both configured, it is recommended to configure the same user names in both TACACS+ and the local database. This will allow the users to access the Cisco SCE platform in case of TACACS+ server failure.

Note If TACACS+ is used as the login method, the TACACS+ username is used automatically in the enable command. Therefore, it is important to configure the same usernames in both TACACS+ and the local database so that the enable command can recognize this username.

   – specify the password

   – define the privilege level
4. Configure the authentication methods on the Cisco SCE platform.

   – login authentication methods

   – privilege level authorization methods

   – command level authorization methods
5. Review the configuration.

   Use the " **show running-config** " command to view the configuration.

Configuring the Cisco SCE Platform TACACS+ Client

- Adding a New TACACS+ Server Host, page 5-22
- Removing a TACACS+ Server Host, page 5-23
- Configuring the Global Default Key, page 5-23
- Configuring the Global Default Timeout, page 5-24

The user must configure the remote servers for the TACACS+ protocol. Then the Cisco SCE platform TACACS+ client must be configured to work with the TACACS+ servers. The following information must be configured:

- TACACS+ server hosts definition—A maximum of three servers is supported.

  For each sever host, the following information can be configured:

  - hostname (required)
  - port
  - encryption key
  - timeout interval
- Default encryption key (optional)—A global default encryption key may be defined. This key is defined as the key for any server host for which a key is not explicitly configured when the server host is defined.

  If the default encryption key is not configured, a default of no key is assigned to any server for which a key is not explicitly configured.
- Default timeout interval (optional)—A global default timeout interval may be defined. This timeout interval is defined as the timeout interval for any server host for which a timeout interval is not explicitly configured when the server host is defined.

  If the default timeout interval is not configured, a default of five seconds is assigned to any server for which a timeout interval is not explicitly configured.

The procedures for configuring the Cisco SCE platform TACACS+ client are explained in the following sections:

- Adding a New TACACS+ Server Host, page 5-22
- Removing a TACACS+ Server Host, page 5-23
- Configuring the Global Default Key, page 5-23
- Configuring the Global Default Timeout, page 5-24

Adding a New TACACS+ Server Host

Use this command to define a new TACACS+ server host that is available to the Cisco SCE platform TACACS+ client.

The Service Control solution supports a maximum of three TACACS+ server hosts.

Options

The following options are available:

- **host-name—**Name of the server
- **port number—**TACACS+ port number
  - Default = 49
- **timeout interval—**Time in seconds that the server waits for a reply from the server host before timing out
  - Default = 5 seconds or user-configured global default timeout interval (see "To define the global default timeout, do the following:" section on page 5-24.)
- **key-string—**Encryption key that the server and client will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server host.
  - Default = no key or user-configured global default key (see "To define a global default key, do the following:" section on page 5-24.)

From the SCE(config)# prompt, type:

Command	Purpose
tacacs-server host *host-name* **[port** *portnumber***] [timeout** *timeout-interval***] [key** *key-string***]**	Define a new TACACS+ server host that is available to the Cisco SCE platform TACACS+ client.

Removing a TACACS+ Server Host

Options

The following options are available:

- **host-name—**Name of the server to be deleted

From the SCE(config)# prompt, type:

Command	Purpose
no tacacs-server host *host-name*	Removes a TACACS+ server host.

Configuring the Global Default Key

Use this command to define the global default key for the TACACS+ server hosts. This default key can be overridden for a specific TACACS+ server host by explicitly configuring a different key for that TACACS+ server host.

Options

The following options are available:

- **key-string—**Default encryption key that all TACACS+ servers and clients will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server hosts.
  - Default = no encryption

To define a global default key, do the following:

From the SCE(config)# prompt, type:

Command	Purpose
tacacs-server key *key-string*	Defines the global default key for the TACACS+ server hosts.

To clear a global default key, do the following:

From the SCE(config)# prompt, type:

Command	Purpose
no tacacs-server key	No global default key is defined. Each TACACS+ server host may still have a specific key defined. However, any server host that does not have a key explicitly defined (uses the global default key) is now configured to use no key.

Configuring the Global Default Timeout

Use this command to define the global default timeout interval for the TACACS+ server hosts. This default timeout interval can be overridden for a specific TACACS+ server host by explicitly configuring a different timeout interval for that TACACS+ server host.

Options

The following options are available:

- **timeout interval—**Default time in seconds that the server waits for a reply from the server host before timing out.
  - Default = 5 seconds

To define the global default timeout, do the following:

From the SCE(config)# prompt, type:

Command	Purpose
tacacs-server timeout *timeout-interval*	Defines global default timeout.

To clear the global default timeout, do the following:

From the SCE(config)# prompt, type:

Command	Purpose
no tacacs-server timeout	No global default timeout interval is defined. Each TACACS+ server host may still have a specific timeout interval defined. However, any server host that does not have a timeout interval explicitly defined (uses the global default timeout interval) is now configured to a five second timeout interval.

Managing the User Database

TACACS+ maintains a local user database. Up to 100 users can be configured in this local database, which includes the following information for all users:

- Username
- Password—May be configured as encrypted or unencrypted
- Privilege level

The procedures for managing the local user database are explained in the following sections:

- Adding a New User to the Local Database, page 5-25
- Defining the User Privilege Level, page 5-27
- Adding a New User with Privilege Level and Password, page 5-27
- Deleting a User, page 5-29

Adding a New User to the Local Database

Use these commands to add a new user to the local database. Up to 100 users may be defined.

- How to Add a User with a Clear Text Password, page 5-26
- How to Add a User with No Password, page 5-26
- How to Add a User with an MD5 Encrypted Password Entered in Clear Text, page 5-26
- How to Add a User with an MD5 Encrypted Password Entered as an MD5 Encrypted String, page 5-27

Options

The password is defined with the username. There are several password options:

- No password—Use the **nopassword** keyword.
- Password—Password is saved in clear text format in the local list.

  Use the *password* parameter.

- Encrypted password—Password is saved in encrypted (MD5) form in the local list. Use the secret keyword.

  Password may be defined by either of the following methods:

  - Specify a clear text password, which is saved in MD5 encrypted form
  - Specify an MD5 encryption string, which is saved as the user MD5-encrypted secret password

The following options are available:

- **name—**Name of the user to be added
- **password—**A clear text password. May be saved in the local list in either of two formats:
  - as clear text
  - in MD5 encrypted form if the secret keyword is used
- **encrypted-secret—**An MD5 encryption string password

The following keywords are available:

- **nopassword—**There is no password associated with this user
- **secret—**The password is saved in MD5 encrypted form. Use with either of the following keywords to indicate the format of the password as entered in the command:
  - **0—**Use with the **password** option to specify a clear text password that will be saved in MD5 encrypted form
  - **5—**Use with the **encrypted-secret** option to specify an MD5 encryption string that will be saved as the user MD5-encrypted secret password

How to Add a User with a Clear Text Password

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **password** *password*	Adds a user with a clear text password.

How to Add a User with No Password

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **nopassword**	Adds a user with no password.

How to Add a User with an MD5 Encrypted Password Entered in Clear Text

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **secret 0** *password*	Adds a user with an MD5 encrypted password entered in clear text.

How to Add a User with an MD5 Encrypted Password Entered as an MD5 Encrypted String

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **secret 5** *encrypted-secret*	Adds a user with an MD5 encrypted password entered as an MD5 encrypted string.

Defining the User Privilege Level

Privilege level authorization in the Cisco SCE platform is accomplished by the use of an " **enable** " command authentication request. When a user requests an authorization for a specified privilege level, by using the " **enable** " command, the Cisco SCE platform sends an authentication request to the TACACS+ server specifying the requested privilege level. The Cisco SCE platform grants the requested privilege level only after the TACACS+ server authenticates the " **enable** " command password and verifies that the user has sufficient privileges the enter the requested privilege level.

Options

The following options are available:

- **name—**Name of the user whose privilege level is set
- **level—**The privilege level permitted to the specified user. These levels correspond to the CLI authorization levels, which are entered via the **enable** command:
  - 0—User
  - 10—Admin
  - 15 (default)—Root

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **privilege** *level*	Defines user privilege level.

Adding a New User with Privilege Level and Password

Use these commands to define a new user, including password and privilege level, in a single command.

Note In the config files (**running config** and **startup config**), this command will appear as two separate commands.

- How to Add a User with a Privilege Level and a Clear Text Password, page 5-28
- How to Add a User with a Privilege Level and an MD5 Encrypted Password Entered in Clear Text, page 5-28
- How to Add a User with a Privilege Level and an MD5 Encrypted Password Entered as an MD5 Encrypted String, page 5-29

Options

The following options are available:

- **name—**Name of the user whose privilege level is set
- **level—**The privilege level permitted to the specified user. These levels correspond to the CLI authorization levels, which are entered via the **enable** command:
  - 0—User
  - 10—Admin
  - 15 (default)—Root
- **password—**A clear text password. May be saved in the local list in either of two formats:
  - as clear text I
  - n MD5 encrypted form if the secret keyword is used
- **encrypted-secret—**An MD5 encryption string password

The following keywords are available:

- **secret—**The password is saved in MD5 encrypted form. Use with either of the following keywords to indicate the format of the password as entered in the command:
  - **0—**Use with the **password** option to specify a clear text password that will be saved in MD5 encrypted form
  - **5** = use with the **encrypted-secret** option to specify an MD5 encryption string that will be saved as the user MD5-encrypted secret password

How to Add a User with a Privilege Level and a Clear Text Password

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **privilege** *level* **password** *password*	Adds a user with a privilege level and a clear text password.

How to Add a User with a Privilege Level and an MD5 Encrypted Password Entered in Clear Text

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **privilege** *level* **secret 0** *password*	Adds a user with a privilege level and an MD5 encrypted password entered in clear text.

How to Add a User with a Privilege Level and an MD5 Encrypted Password Entered as an MD5 Encrypted String

From the SCE(config)# prompt, type:

Command	Purpose
username *name* **privilege** *level* **secret 5** *encrypted-secret*	Adds a user with a privilege level and an MD5 encrypted password entered as an MD5 encrypted string.

Deleting a User

Options

The following options are available:

- **name—**Name of the user to be deleted

From the SCE(config)# prompt, type:

Command	Purpose
no username *name*	Deletes a user.

Configuring AAA Login Authentication

There are two features to be configured for login authentication:

- Maximum number of permitted Telnet login attempts
- The authentication methods used at login (see "General AAA Fallback and Recovery Mechanism" section on page 5-20.)

The procedures for configuring login authentication are explained in the following sections:

- Configuring Maximum Login Attempts, page 5-29
- Configuring the AAA Login Authentication Methods, page 5-30

Configuring Maximum Login Attempts

Use this command to set the maximum number of login attempts that will be permitted before the session is terminated.

Options

The following options are available:

- **number-of-attempts—**The maximum number of login attempts that will be permitted before the telnet session is terminated.

  This is relevant only for Telnet sessions. From the local console, the number of re-tries is unlimited.

  - Default = three

From the SCE(config)# prompt, type:

Command	Purpose
aaa authentication attempts login *number-of-attempts*	Configures maximum login attempts.

Configuring the AAA Login Authentication Methods

You can configure "backup" login authentication methods to be used if failure of the primary login authentication method (see "General AAA Fallback and Recovery Mechanism" section on page 5-20).

Use this command to specify which login authentication methods are to be used, and in what order of preference.

- How to Specify the Login Authentication Methods, page 5-30
- How to Delete the Login Authentication Methods List, page 5-30

Options

The following options are available:

- **method—**The login authentication methods to be used. You may specify up to four different methods, in the order in which they are to be used.
  - **group TACACS+—**Use TACACS+ authentication.
  - **local—**Use the local username database for authentication
  - **enable** (default)—Use the " **enable** " password for authentication
  - **none—**Use no authentication.

How to Specify the Login Authentication Methods

From the SCE(config)# prompt, type:

Command	Purpose
aaa authentication login default method1 [method2...]	Specifies login authentication methods. You may list a maximum of four methods; all four methods explained above. List them in the order of priority.

How to Delete the Login Authentication Methods List

From the SCE(config)# prompt, type:

Command	Purpose
no aaa authentication login default	Deletes login authentication methods list. If the login authentication methods list is deleted, the default login authentication method only (enable password) will be used. TACACS+ authentication will not be used.

Configuring AAA Privilege-Level Authorization Methods

- How to Specify AAA Privilege-Level Authorization Methods, page 5-31
- How to Delete the AAA Privilege Level Authorization Methods List, page 5-31

Options

The following options are available:

- **method—**The login authorization methods to be used. You may specify up to four different methods, in the order in which they are to be used.
  - **group TACACS+—**Use TACACS+ authorization.
  - **local—**Use the local username database for authorization
  - **enable** (default)—Use the " **enable** " password for authorization
  - **none—**Use no authorization.

How to Specify AAA Privilege-Level Authorization Methods

From the SCE(config)# prompt, type:

Command	Purpose
aaa authorization enable default method1 [method2...]	Specifies AAA privilege level authorization methods. You may list a maximum of four methods; all four methods explained above. List them in the order of priority.

How to Delete the AAA Privilege Level Authorization Methods List

From the SCE(config)# prompt, type:

Command	Purpose
no aaa authorization enable default	Deletes AAA privilege level authorization methods list. If the privilege level authorization methods list is deleted, the default login authentication method only (enable password) will be used. TACACS+ authentication will not be used.

Configuring AAA Command-Level Authorization Methods

- How to Specify AAA Command-Level Authorization Methods, page 5-32
- How to Delete the AAA Command-Level Authorization Methods List, page 5-32

Options

The following options are available:

- **level—**The privilege level for which to enable the TACACS+ command level authorizarion (0, 5, 10, 15)
- **method—**The command authorization methods to be used. You may specify up to two methods, in the order in which they are to be used.
  - **group TACACS+—**Use TACACS+ authorization.
  - **none—**Use no authorization.

How to Specify AAA Command-Level Authorization Methods

From the SCE(config)# prompt, type:

Command	Purpose
aaa authorization command *level* **default** *method1 [method2]***]**	Specifies AAA command level authorization methods. You may list a maximum of two methods. List them in the order of priority.

How to Delete the AAA Command-Level Authorization Methods List

From the SCE(config)# prompt, type:

Command	Purpose
no aaa authorization command *level* **default**	Deletes AAA command level authorization methods list. If the command level authorization methods list is deleted, the default login authentication method only (enable password) will be used. TACACS+ authentication will not be used.

Configuring AAA Accounting

Use this command to enable or disable TACACS+ accounting.

- How to Enable AAA Accounting, page 5-33
- How to Disable AAA Accounting, page 5-33

If TACACS+ accounting is enabled, the Cisco SCE platform sends an accounting message to the TACACS+ server after every command execution. The accounting message is logged in the TACACS+ server for the use of the network administrator.

By default, TACACS+ accounting is disabled.

Options

The following options are available:

- **level—**The privilege level for which to enable the TACACS+ accounting

How to Enable AAA Accounting

From the SCE(config)# prompt, type:

Command	Purpose
aaa authentication accounting commands *level* **default stop-start group tacacs+**	Enables AAA accounting. The **start-stop** keyword (required) indicates that the accounting message is sent at the beginning and the end (if the command was successfully executed) of the execution of a CLI command.

How to Disable AAA Accounting

From the SCE(config)# prompt, type:

Command	Purpose
aaa authentication accounting commands *level* **default**	Disables AAA accounting.

Monitoring TACACS+

- Displaying Statistics for TACACS+ Servers, page 5-33
- Displaying Statistics, Keys, and Timeouts for TACACS+ Servers, page 5-33
- Monitoring TACACS+ Users, page 5-34

Displaying Statistics for TACACS+ Servers

From the SCE# prompt, type:

Command	Purpose
show tacacs	Displays statistics for TACACS+ servers.

Displaying Statistics, Keys, and Timeouts for TACACS+ Servers

From the SCE# prompt, type:

Command	Purpose
show tacacs all	Displays statistics, keys, and timeouts for TACACS+ servers. Note that, although most show commands are accessible to viewer level users, the ' **all** ' option is available only at the admin level. Use the command ' **enable 10** ' to access the admin level.

Monitoring TACACS+ Users

Use this command to display the users in the local database, including passwords.

From the SCE# prompt, type:

Command	Purpose
show users	Displays the users in the local database, including passwords. Note that, although most show commands are accessible to viewer level users, this command is available only at the admin level. Use the command ' **enable 10** ' to access the admin level.

Configuring Access Control Lists (ACLs)

- Adding Entries to an ACL, page 5-36
- Removing an ACL, page 5-36
- Defining a Global ACL, page 5-37

The Cisco SCE platform can be configured with Access Control Lists (ACLs), which are used to permit or deny incoming connections on the management interface. An access list is an ordered list of entries, each consisting of an IP address and an optional wildcard "mask" defining an IP address range, and a permit/deny field.

The order of the entries in the list is important. The default action of the first entry that matches the connection is used. If no entry in the Access List matches the connection, or if the Access List is empty, the default action is deny.

Configuration of system access is done in two stages:

1. Creating an access list. ("Adding Entries to an ACL" section on page 5-36).
2. Associating the ACL with a management service. (See "Defining a Global ACL" section on page 5-37.)

Creating an access list is done entry by entry, from the first to the last.

When the system checks for an IP address on an access list, the system checks each line in the ACL for the IP address, starting at the first entry and moving towards the last entry. The first match that is detected (that is, the IP address being checked is found within the IP address range defined by the entry) determines the result, according to the permit/deny flag in the matched entry. If no matching entry is found in the ACL, access is denied.

You can create up to 99 ACLs. ACLs can be associated with system access on the following levels:

- Global (IP) level: If a global list is defined using the **ip access-class** command, when a request comes in, the Cisco SCE platform first checks if there is permission for access from that IP address. If not, the Cisco SCE does not respond to the request. Configuring the Cisco SCE platform to deny a certain IP address would preclude the option of communicating with that address using any IP-based protocol including Telnet, FTP, ICMP, RPC, SSH, and SNMP. The basic IP interface is low-level, blocking the IP packets before they reach the interfaces.
- Service level: Access to each management service (Telnet, SNMP, and SSH) can be restricted to an ACL. Interface-level lists are, by definition, a subset of the global list defined. If access is denied at the global level, the IP will not be allowed to access using one of the interfaces. Once an ACL is associated with a specific management service, that service checks the ACL to find out if there is permission for a specific external IP address trying to access the management interface.

  Use the following CLI commands to assign an ACL to the specified management service:

  - Telnet–**access-class in**
  - SSH—**ip ssh access-class**
  - SNMP—**snmp-server community**

It is possible to configure several management services to the same ACL, if this is the desired behavior of the Cisco SCE platform.

If no ACL is associated to a management service or to the global IP level, access is permitted from all IP addresses.

Note The Cisco SCE Platform will respond to **ping** commands only from IP addresses that are allowed access. Pings from a non-authorized address will not receive a response from the Cisco SCE platform, as ping uses ICMP protocol.

Options

The following options are available:

- **number—**The ID number assigned to the Access Control List
- **ip-address—**The IP address of the interface to be permitted or denied. Enter in x.x.x.x format.
- **ip-address/mask—**Configures a range of addresses in the format x.x.x.x y.y.y.y where x.x.x.x specifies the prefix bits common to all IP addresses in the range, and y.y.y.y is a wildcard-bits mask specifying the bits that are ignored. In this notation, '0' means bits to ignore.

The following keywords are available:

- **permit—**The specified IP addresses have permission to access the Cisco SCE platform.
- **deny—**The specified IP addresses are denied access to the Cisco SCE platform.

Adding Entries to an ACL

Step 1 Type **configure** and press **Enter**.

Enables Global Configuration mode.

Step 2 Enter the desired IP address or addresses.

- To configure one IP address type:

  access-list *number* **permit|deny** *ip-address* and press **Enter**.

- To configure more than one IP address type:

  access-list *number* **permit|deny** *ip-address/mask* and press **Enter**.

When you add a new entry to an ACL, it is always added to the end of the list.

Adding Entries to an ACL: Example

The following example adds an entry to the access list number 1, that permits access only to IP addresses in the range of 10.1.1.0–10.1.1.255.

```
SCE(config)#access-list 1 permit 10.1.1.0 0.0.0.255
```

Removing an ACL

Use this command to remove an ACL with all its entries.

From the SCE(config)# prompt, type:

Command	Purpose
no access-list *number*	Removes the specified ACL with all its entries.

Defining a Global ACL

A global ACL for permits or denies all traffic to the Cisco SCE platform.

From the SCE(config)# prompt, type:

Command	Purpose
ip access-class *number*	Applies the specified ACL to all traffic attempting to access the Cisco SCE platform, rather than to a specific type of traffic, such as Telnet traffic.

Managing the Telnet Interface

- Preventing Telnet Access, page 5-38
- Assigning an ACL to the Telnet Interface, page 5-38
- Configuring Telnet Timeout, page 5-39

This section discusses the Telnet interface of the Cisco SCE platform. A Telnet session is the most common way to connect to the Cisco SCE platform CLI interface.

You can set the following parameters for the Telnet interface:

- Enable/disable the interface
- Assign an ACL to permit or deny incoming connections.
- Timeout for Telnet sessions, that is, if there is no activity on the session, how long the Cisco SCE platform waits before automatically cutting off the Telnet connection.

The following commands are relevant to Telnet interface:

- **access-class in**
- **line vty**
- **[no] access list**
- **[no] service telnetd**
- **[no] timeout**
- **show line vty access-class in**
- **show line vty timeout**

Preventing Telnet Access

Use this command to disable access by Telnet altogether.

From the SCE(config)# prompt, type:

Command	Purpose
no service telnetd	Disables access by Telnet. Current Telnet sessions are not disconnected, but no new Telnet sessions are allowed.

Assigning an ACL to the Telnet Interface

From the SCE(config-line)# prompt, type:

Command	Purpose
access-class *acl-number* **in**	The specified ACL controls access to the Telnet interface. *acl-number* is the ID number of an existing ACL.

Assigning an ACL to the Telnet Interface: Example

The following example shows how to assign ACL #1 to the Telnet interface.

```
SCE#configure
SCE(config)#line vty 0
SCE(config-line)#access-class 1 in
```

Removing ACL Assignment from the Telnet Interface

From the SCE(config-line)# prompt, type:

Command	Purpose
no access-class in	Removes the ACL assignment from the Telnet interface, so that any IP address may now access the Telnet interface.

Configuring Telnet Timeout

The Cisco SCE platform supports timeout of inactive Telnet sessions.

Options

The following options are available:

- **timeout—**The length of time in minutes before an inactive Telnet session will be timed-out.
  - Default—30 minutes

From the SCE(config-line)# prompt, type:

Command	Purpose
timeout *timeout*	Configures Telnet timeout.

Configuring the SSH Server

- The SSH Server, page 5-40
- Key Management, page 5-40
- Managing the SSH Server, page 5-41
- Monitoring the Status of the SSH Server, page 5-43

The SSH Server

A shortcoming of the standard telnet protocol is that it transfers password and data over the net unencrypted, thus compromising security. Where security is a concern, using a Secure Shell (SSH) server rather than telnet is recommended.

An SSH server is similar to a telnet server, but it uses cryptographic techniques that allow it to communicate with any SSH client over an insecure network in a manner which ensures the privacy of the communication. CLI commands are executed over SSH in exactly the same manner as over telnet.

The SSH server supports both the SSHv1 and SSHv2 protocols. You can disable SSHv1, so that only SSHv2 is running.

The SSH server supports the following encryption ciphers:

- aes256-ctr, aes192-ctr, aes128-ctr (RFC-4344, section 4).
- 3des-cbc, blowfish-cbc, aes256-cbc, aes192-cbc, aes128-cbc, arcfour, cast128-cbc (RFC-4253, section 6.3)
- arcfour128, arcfour256 (RFC-4345, section 4).
- rijndael-cbc@lysator.liu.se (as provided by OpenSSH 4.7p1).

An ACL can be configured for SSH as for any other management protocol, limiting SSH access to a specific set of IP addresses (see "Configuring Access Control Lists (ACLs)" section on page 5-35)

Key Management

Each SSH server should define a set of keys (DSA2, RSA2 and RSA1) to be used when communicating with various clients. The key sets are pairs of public and private keys. The server publishes the public key while keeping the private key in non-volatile memory, never transmitting it to SSH clients. Note that the keys are kept on the tffs0 file system, which means that a person with knowledge of the 'enable' password can access both the private and public keys. The SSH server implementation provides protection against eavesdroppers who can monitor the management communication channels of the Cisco SCE platform, but it does not provide protection against a user with knowledge of the 'enable' password.

Key management is performed by the user via a special CLI command. A set of keys must be generated at least once before enabling the SSH server.

Size of the encryption key is always 2048 bits.

Managing the SSH Server

Use these commands to manage the SSH server. These commands do the following:

- Generate an SSH key set
- Enable/disable the SSH server
- Enable/disable SSHv1. (Disabling SSHv1 allows you to run SSHv2 only.)
- Delete existing SSH keys

Generating a Set of SSH Keys

Remember that you must generate a set of SSH keys before you enable the SSH server.

From the SCE(config)# prompt, type:

Command	Purpose
ip ssh key generate	Generates a new SSH key set and immediately saves it to non-volatile memory. (Key set is not part of the configuration file). Key size is always 2048 bits.

Enabling the SSH Server

SSH allows you to login only when the user password and AAA authentication

are configured.

- Configure at least one user name and password.

  SCE8000(config)# username <username> password <password>

- Configure AAA authentication for login.

  SCE8000(config)# aaa authentication login default none

From the SCE(config)# prompt, type:

Command	Purpose
ip ssh	Enables SSH server.

Disabling the SSH Server

From the SCE(config)# prompt, type:

Command	Purpose
no ip ssh	Disables SSH server.

Running Only SSHv2

Step 1 From the SCE(config)# prompt, type **ip ssh** and press **Enter**.

Step 2 From the SCE(config)# prompt, type **no ip ssh sshv1** and press **Enter**

To re-enable SSHv1, use the command **ip ssh SSHv1.**

Assigning an ACL to the SSH Server

From the SCE(config)# prompt, type:

Command	Purpose
ip ssh access-class *acl-number*	The specified ACL controls access to the SSH server. *acl-number* is the ID number of an existing ACL

Removing the ACL Assignment from the SSH Server

rom the SCE(config)# prompt, type:

Command	Purpose
no ip ssh access-class	Removes the ACL assignment from the SSH server, so that any IP address may now access the SSH server.

Deleting the Existing SSH Keys

From the SCE(config)# prompt, type:

Command	Purpose
ip ssh key remove	Removes the existing SSH key set from non-volatile memory.

If the SSH server is currently enabled, it will continue to run, since it only reads the keys from non-volatile memory when it is started. However, if the startup-configuration specifies that the SSH server is enabled, the Cisco SCE platform will not be able to start the SSH server on startup if the keys have been deleted. To avoid this situation, after executing this command, always do one of the following before the Cisco SCE platform is restarted (using **reload**):

- Generate a new set of keys.
- Disable the SSH server and save the configuration.

Monitoring the Status of the SSH Server

Use this command to monitor the status of the SSH sever, including current SSH sessions.

From the SCE> prompt, type:

Command	Purpose
show ip ssh	Monitors the status of SSH server.

Configuring and Managing the SNMP Interface

- About the SNMP Interface, page 5-44
- Enabling the SNMP Interface, page 5-47
- Configuring SNMP Community Strings, page 5-47
- Configuring SNMP Notifications, page 5-49

About the SNMP Interface

This section explains how to configure the SNMP agent parameters. It also provides a brief overview of SNMP notifications and relevant CLI commands.

- SNMP Protocol, page 5-44
- Security Considerations, page 5-45
- About CLI, page 5-45
- About MIBs, page 5-46
- Configuration via SNMP, page 5-46

SNMP Protocol

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Cisco SCE platform supports the original SNMP protocol (also known as SNMPv1), and a newer version called Community-based SNMPv2 (also known as SNMPv2C).

- **SNMPv1—**This is the first version of the Simple Network Management Protocol, as defined in RFCs 1155 and 1157, and is a full Internet standard. SNMPv1 uses a community-based form of security.
- **SNMPv2c—**This is the revised protocol, which includes improvements to SNMPv1 in the areas of protocol packet types, transport mappings, and MIB structure elements but using the existing SNMPv1 administration structure. It is defined in RFC 1901, RFC 1905, and RFC 1906.

Cisco SCE platform implementation of SNMP supports all MIB II variables, as described in RFC 1213, and defines the SNMP traps using the guidelines described in RFC 1215.

The SNMPv1 and SNMPv2C specifications define the following basic operations that are supported by Cisco SCE platform. Table 5-3 lists the request types and descriptions.

Table 5-3 Request Types

Request Type	Description	Remarks
Set Request	Writes new data to one or more of the objects managed by an agent.	Set operations immediately affect the Cisco SCE platform running-config but do not affect the startup config
Get Request	Requests the value of one or more of the objects managed by an agent.	
Get Next Request	Requests the Object Identifier(s) and value(s) of the next object(s) managed by an agent.	
Get Response	Contains the data returned by an agent.	
Trap	Sends an unsolicited notification from an agent to a manager, indicating that an event or error has occurred on the agent system	Cisco SCE platform may be configured to send either SNMPv1 or SNMPv2 style traps.
Get Bulk Request	Retrieves large amounts of object information in a single Request / response transaction. GetBulk behaves as if many iterations of GetNext request/responses were issued, except that they are all performed in a single request/response.	This is newly defined SNMPv2c message.

Security Considerations

By default, the SNMP agent is disabled for both read and write operations. When enabled, SNMP is supported over the management port only (in-band management is not supported).

In addition, the Cisco SCE platform supports the option to configure community of managers for read-write accessibility or for read-only accessibility. Furthermore, an ACL may be associated with the SNMP agent by assigning it to one of the community strings to allow SNMP management to a restricted set of manager IP addresses. If different ACLs are assigned to different community strings, access by all community strings is controlled by all assigned ACLs. Assigning different ACLs to different community strings is not supported

About CLI

- CLI Commands for Configuring SNMP, page 5-46
- CLI Commands for Monitoring SNMP, page 5-46

The Cisco SCE platform supports the CLI commands that control the operation of the SNMP agent. All the SNMP commands are available in Admin authorization level. The SNMP agent is disabled by default and any SNMP configuration command enables the SNMP agent (except where there is an explicit disable command).

CLI Commands for Configuring SNMP

Following is a list of CLI commands available for configuring SNMP. These are Global Configuration mode commands.

- **snmp-server enable**
- **no snmp-server**
- **[no] snmp-server community [all]**
- **[no | default] snmp-server enable traps**
- **[no] snmp-server host [all]**
- **[no] snmp-server contact**
- **[no] snmp-server location**

CLI Commands for Monitoring SNMP

Following is a list of CLI commands available for monitoring SNMP. These are Viewer mode commands, and are available when the SNMP agent is enabled:

- show snmp (available when SNMP agent is disabled)
- show snmp community
- show snmp contact
- show snmp enabled
- show snmp host
- show snmp location
- show snmp MIB (available when SNMP agent enabled and community was set)
- show snmp traps

About MIBs

MIBs (Management Information Bases) are databases of objects that can be monitored by a network management system (NMS). SNMP uses standardized MIB formats that allow any SNMP tools to monitor any device defined by a MIB.

For further information concerning MIBs used by the Cisco SCE 8000 platform, see the "Cisco Service Control MIBs" section on page A-1

Configuration via SNMP

The Cisco SCE platform supports a limited set of variables that may be configured via SNMP (read-write variables). Setting a variable via SNMP (as via the CLI) takes effect immediately and affects only the running-configuration. To make this configuration stored for next reboots (startup-configuration) the user must specify it explicitly via CLI or via SNMP using the Cisco enterprise MIB objects.

It should be noted also that the Cisco SCE platform takes the approach of a single configuration database with multiple interfaces that may change this database. Therefore, executing the **copy running-config startup-config** command via CLI or SNMP makes permanent all the changes made by either SNMP or CLI.

Enabling the SNMP Interface

Use this command to explicitly enable the SNMP interface.

The SNMP interface is implicitly enabled when any **snmp-server** command is executed to configure any SNMP parameter. For more information on configuring and managing the SNMP parameters, including hosts, communities, contact, location, and trap destination hosts, see "Configuring and Managing the SNMP Interface" section on page 5-44.

- How to Enable the SNMP Interface, page 5-47
- How to Disable the SNMP Interface, page 5-47

How to Enable the SNMP Interface

You must define at least one community string to allow SNMP access. For complete information on community strings see "Configuring SNMP Community Strings" section on page 5-47.

From the SCE(config)# prompt, type:

Command	Purpose
snmp-server enable	Enables SNMP interface.

How to Disable the SNMP Interface

From the SCE(config)# prompt, type:

Command	Purpose
no snmp-server	Disables SNMP interface.

Configuring SNMP Community Strings

- Defining a Community String, page 5-48
- Removing a Community String, page 5-48
- Displaying the Configured Community Strings, page 5-49

To enable SNMP management, you must configure SNMP community strings to define the relationship between the SNMP manager and the agent.

After receiving an SNMP request, the SNMP agent compares the community string in the request to the community strings that are configured for the agent. The requests are valid under the following circumstances:

- SNMP *Get* , *Get-next* , and *Get-bulk* requests are valid if the community string in the request matches the read-only community.
- SNMP *Get* , *Get-next* , *Get-bulk* and *Set* requests are valid if the community string in the request matches the agent's read-write community.

Defining a Community String

Options

The following options are available:

- **community-string—**A security string that identifies a community of managers who are permitted to access the SNMP server
- **acl-number**—(Optional) ID number of the ACL to be assigned to the SNMP interface. It should list the IP addresses of all SNMP managers permitted to access the SNMP server.

Note Assigning different ACLs to different community strings is not supported. If you specify an ACL in this command, it is assigned to the SNMP server globally, not just to the specified community string. For example, if you configure two community strings and assign a different ACL to each, access to the SNMP agent for both communities is controlled by both ACLs.

If no ACL is specified, all IP addresses can access the SNMP service. For more information about ACLs, see "Configuring Access Control Lists (ACLs)" section on page 5-35.

The following keywords are available:

- **ro—**Read only (default accessibility)
- **rw**—Read and write

From the SCE(config)# prompt, type:

Command	Purpose
snmp-server community *community-string* **ro|rw** [*acl-number*]	Defines a community string. If you specify ACLs for any communities, all assigned ACLs in conjunction will control access for all communities. Repeat the command as necessary to define all community strings.

Defining a Community String: Example

This example shows how to configure a community string called "mycommunity" with read-only rights. ACL "1" will be assigned to the SNMP server and all configured community strings, not just "mycommunity".

Since read-only is the default, it does not need to be defined explicitly.

```
SCE(config)#snmp-server community mycommunity 1
```

Removing a Community String

From the SCE(config)# prompt, type:

Command	Purpose
no snmp-server community *community-string*	Removes a community string.

Removing a Community String: Example

The following example shows how to remove a community string called “mycommunity”. If an ACL was assigned to this community string, it is also removed.

```
SCE(config)#no snmp-server community mycommunity
```

Displaying the Configured Community Strings

From the SCE> prompt, type:

Command	Purpose
show snmp-server community *community-string*	Displays configured community strings

Displaying the Configured Community Strings: Example

The following example shows how to display the configured SNMP communities.

```
SCE>show snmp community
Community: public, Access Authorization: RO, Access List Index: 1
SCE>
```

Configuring SNMP Notifications

Use these commands to configure:

- The destinations that will receive SNMP notifications (hosts)
- Which types of notifications will be sent (traps)

Notifications are unsolicited messages that are generated by the SNMP agent that resides inside the Cisco SCE platform when an event occurs. When the Network Management System receives the notification message, it can take suitable actions, such as logging the occurrence or ignoring the signal.

By default, the Cisco SCE platform is not configured to send any SNMP notifications. You must define the Network Management System to which the Cisco SCE platform should send notifications. (See the table below, Configurable Notifications, for a list of configurable notifications). Whenever one of the events that trigger notifications occurs in the Cisco SCE platform, an SNMP notification is sent from the Cisco SCE platform to the list of IP addresses that you define.

The Cisco SCE platform supports two general categories of notifications:

- Standard SNMP notifications - As defined in RFC1157 and using the conventions defined in RFC1215.
- Proprietary service control enterprise notifications - As defined in the service control proprietary MIB (See Table A-20 on page A-21).

After a host or hosts are configured to receive notifications, by default, the Cisco SCE platform sends to the host or hosts all the notifications supported by the Cisco SCE platform except for the AuthenticationFailure notification. The Cisco SCE platform provides the option to enable or disable the sending of this notification, as well as some of the Cisco SCE enterprise notifications, explicitly.

The Cisco SCE platform can be configured to generate either SNMPv1 style or SNMPv2c style notifications. By default, the Cisco SCE platforms sends SNMPv1 notifications.

Following are some sample procedures illustrating how to do the following:

- Configure hosts (NMS) to which the SNMP agent should send notifications
- Remove/disable a host (NMS) from receiving notifications
- Enable the SNMP agent to send authentication-failure notifications
- Enable the SNMP agent to send enterprise notifications
- Reset all notifications to the default setting

Defining SNMP Hosts

Use this command to define the hosts that will receive notifications from the Cisco SCE platform.

- How to Configure the Cisco SCE Platform to Send Notifications to a Host (NMS), page 5-50
- How to Configure the Cisco SCE Platform to Stop Sending Notifications to a Host, page 5-51
- Configuring SNMP Traps, page 5-51

Options

The following options are available:

- **ip-address—**The IP address of the SNMP server host
- **community-string—**A security string that identifies a community of managers who are permitted to access the SNMP server
- **version—**SNMP version running in the system. Can be set to 1 or 2c.
  - Default—1 (SNMPv1)

How to Configure the Cisco SCE Platform to Send Notifications to a Host (NMS)

At the SCE(config)# prompt, type:

Command	Purpose
snmp-server host *ip-address community-string*	Configures Cisco SCE platform to send notifications to a host (NMS). If the version is not specified, SNMPv1 is assumed. Only one host can be specified per command. To define multiple hosts, execute one command for each host.

Configuring the Cisco SCE Platform to Send Notifications to Multiple Hosts: Example

The following example shows how to configure the Cisco SCE platform to send SNMPv1 notifications to several hosts.

```
SCE(config)#snmp-server host 10.10.10.10 mycommunity
SCE(config)#snmp-server host 20.20.20.20 mycommunity
SCE(config)#snmp-server host 30.30.30.30 mycommunity
SCE(config)#snmp-server host 40.40.40.40 mycommunity
```

How to Configure the Cisco SCE Platform to Stop Sending Notifications to a Host

At the SCE(config)# prompt, type:

Command	Purpose
no snmp-server host *ip-address*	Configures Cisco SCE platform to stop sending notifications to a host.

Configuring the Cisco SCE Platform to Stop Sending Notifications to a Host: Example

The following example shows how to remove the host with the IP Address: “192.168.0.83”.

```
SCE(config)#no snmp-server host 192.168.0.83
```

Configuring SNMP Traps

Use this command to configure the notifications that will be sent to the defined host.

- How to Enable the SNMP Server to Send Authentication Failure Notifications, page 5-52
- How to Enable the SNMP Server to Send All Enterprise Notifications, page 5-52
- How to Enable the SNMP Server to Send a specific Enterprise Notification, page 5-52
- How to Restore All Notifications to the Default Status, page 5-52

Options

The following options are available:

- **snmp—**Optional parameter that specifies that all or specific snmp traps should be enabled or disabled.

  By default, snmp traps are disabled.

  snmp trap name—Optional parameter that specifies a specific snmp trap that should be enabled or disabled.

  Currently the only accepted value for this parameter is **Authentication** .

- **enterprise—**Optional parameter that specifies that all or specific enterprise traps should be enabled or disabled.

  By default, enterprise traps are enabled.

- **enterprise trap name—**Optional parameter that specifies a specific snmp trap that should be enabled or disabled.

  Values: attack, chassis, link-bypass, logger, operational-status, port-operational-status, pull-request-failure, RDR-formatter, session, SNTP, subscriber, system-reset, telnet, vas-traffic-forwarding

Use these parameters as follows:

- To enable/disable all traps of one type: Specify only **snmp** or **enterprise** .
- To enable/disable only one specific trap: Specify **snmp** or **enterprise** with the additional trap name parameter naming the desired trap.
- To enable/disable all traps: Do not specify either **snmp** or **enterprise** .

How to Enable the SNMP Server to Send Authentication Failure Notifications

At the SCE(config)# prompt, type:

Command	Purpose
snmp-server enable traps snmp authentication	Enables SNMP server to send authentication failure notifications.

How to Enable the SNMP Server to Send All Enterprise Notifications

At the SCE(config)# prompt, type:

Command	Purpose
snmp-server enable traps enterprise	Enables SNMP server to send all enterprise notifications.

How to Enable the SNMP Server to Send a specific Enterprise Notification

At the SCE(config)# prompt, type:

Command	Purpose
snmp-server enable traps enterprise *[attack|chassis|link-bypass|logger|operational-status|port-operational-status|pull-request-failure|RDR-formatter|session| SNTP|subscriber|system-reset|telnet|vas-traffic-forwarding]*	Specify the desired enterprise trap type.

Enabling the SNMP Server to Send a Specific Enterprise Notification: Example

The following example shows how to configure the SNMP server to send the logger enterprise notification only.

```
SCE(config)#snmp-server enable traps enterprise logger
```

How to Restore All Notifications to the Default Status

At the SCE(config)# prompt, type:

Command	Purpose
default snmp-server enable traps	Resets all notifications supported by the Cisco SCE platform to their default status.

SNMP Walk Acceleration for linkServiceUsage Queries

Starting from Release 3.8.0, the time taken for the SNMP walk on any of the linkServiceUsage queries is reduced considerably.

The SNMP walk acceleration enables Cisco SCE 8000 device to perform SNMP queries for LinkUsage MIB queries in background and cache the results. This may result in more CPU utilization.

The following queries are accelerated:

- snmpbulkwalk on linkServiceUsageUpVolume
- snmpbulkwalk on linkServiceUsageDownVolume
- snmpbulkwalk on linkServiceUsageNumSessions
- snmpbulkwalk on linkServiceUsageDuration
- snmpbulkwalk on linkServiceUsageConcurrentSessions
- snmpbulkwalk on linkServiceUsageActiveSubscribers
- snmpwalk on complete linkServiceUsageTable

Use the following commands to enable, disable, and show the SNMP query acceleration for linkServiceUsage queries:

- **snmp-server accelerate-query**
- **show snmp-server accelerate-query**

How to Enable SNMP Query Acceleration

From the SCE(config)#> prompt, type:

Command	Purpose
snmp-server accelerate-query <*linkServiceUsage query*>	Enables the SNMP query acceleration.