Using the ACS CLI

This chapter provides helpful tips for understanding and configuring the Cisco Secure ACS 5.6 from the CLI.

- Before Accessing the ACS CLI, page 2-1
- Accessing the ACS CLI, page 2-5
- Understanding the Command Modes, page 2-7
- Navigating the CLI Commands, page 2-12
- Where to Go Next, page 2-15

Before Accessing the ACS CLI

Before logging in to the ACS CLI, review the tasks that you should have completed during hardware installation:

> **Note** These sections only provide an overview of the installation and configuration process for the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliances. For detailed information, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*.

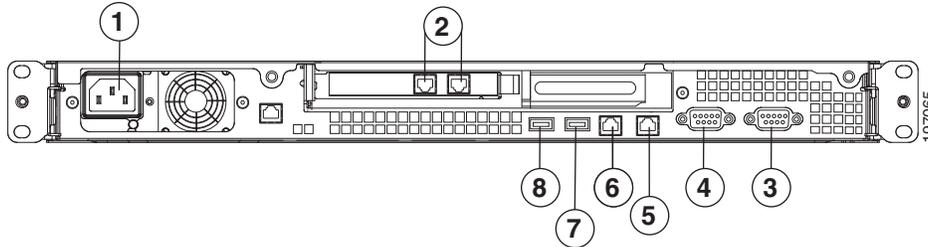1. Starting the CSACS-1121 Appliance, page 2-1
2. Starting the Cisco SNS-3415 and Cisco SNS-3495 Appliances, page 2-2
3. Running Setup to Configure ACS, page 2-4

Starting the CSACS-1121 Appliance

Complete these steps before you configure the CSACS-1121 appliance:

Step 1   Connect the power cord to the CSACS-1121 (see Figure 2-1).

Figure 2-1   *Rear View of CSACS-1121*

1	AC power receptacle	5	(Blocked) Gigabit Ethernet 1
2	(Blocked) Gigabit Ethernet	6	(In Use) Gigabit Ethernet 0
3	Serial connector	7	USB 3 connector
4	Video connector	8	USB 4 connector

Step 2   Connect the network cable to the Gigabit Ethernet 0 connector (see Figure 2-1).

The setup utility (that appears when the CSACS-1121 boots) only configures the Gigabit Ethernet 0 port. For information on connecting cables, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6.*

Step 3   Power up the CSACS-1121.

The appliance boots automatically, and the setup utility appears (see Running Setup to Configure ACS, page 2-4).

Starting the Cisco SNS-3415 and Cisco SNS-3495 Appliances

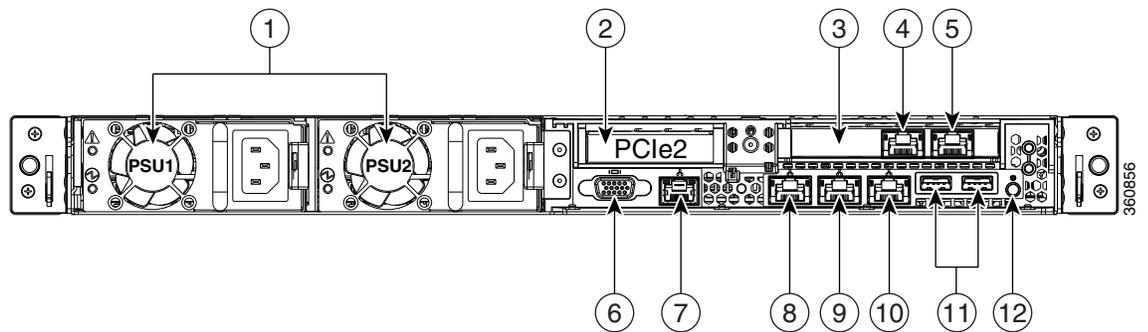Complete these steps before you configure the Cisco SNS-3415 or Cisco SNS-3495 appliance:

Step 1   Connect the power cord to the Cisco SNS-3415 or Cisco SNS-3495 appliance (see Figure 2-2).

Figure 2-2   *Cisco SNS-3415 Appliance Rear View*
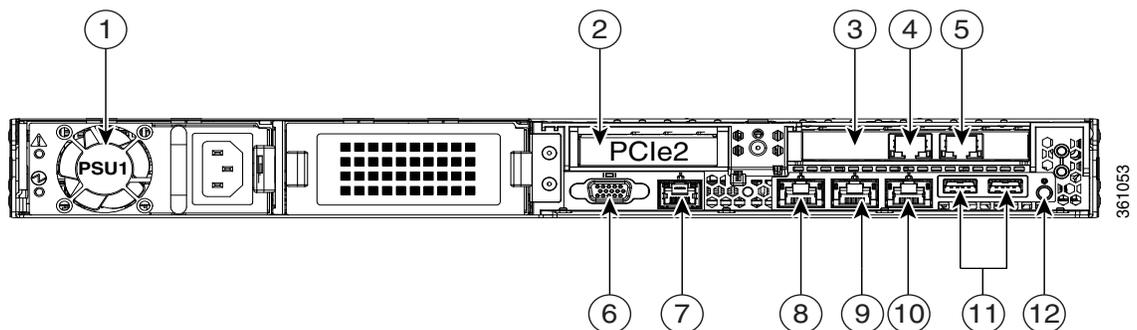
1	Power supply	7	Serial port (RJ-45 connector)
2	Slot 2: Low-profile PCIe slot on riser (half-height, half-length, x16 connector, x8 lane width)	8	1-GB Ethernet dedicated management port used to access CIMC (labeled M)
3	Slot 1: PCIe1 card containing 1-GB Ethernet ports (GigE2 and GigE3)	9	1-GB Ethernet port 1 (GigE0) for Cisco Secure ACS management communication
4	1-GB Ethernet port 3 (GigE2)	10	1-GB Ethernet port 2 (GigE1)
5	1-GB Ethernet port 4 (GigE3)	11	USB ports
6	VGA video connector	12	Rear identification button

Figure 2-3   Cisco SNS-3495 Appliance Rear View

1	Power supplies (up to two)	7	Serial port (RJ-45 connector)
2	Slot 2: Low-profile Peripheral Component Interconnect Express (PCIe) slot on riser (half-height, half-length, x16 connector, x16 lane width)	8	1-GB Ethernet dedicated management port used to access CIMC (labeled M)
3	Slot 1: PCIe1 card containing 1-GB Ethernet ports (GigE2 and GigE3)	9	1-GB Ethernet port 1 (GigE0) for Cisco Secure ACS management communication
4	1-GB Ethernet port 3 (GigE2)	10	1-GB Ethernet port 2 (GigE1)
5	1-GB Ethernet port 4 (GigE3)	11	USB ports
6	VGA video connector	12	Rear identification button

Step 2   Connect the network cable to the Gigabit Ethernet 0 connector (see Figure 2-2 and Figure 2-3).

The setup utility (which appears when the Cisco SNS-3415 or Cisco SNS-3495 appliances boots) only configures the Gigabit Ethernet 0 port. For information on connecting cables, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*.

Step 3   Power up the appliance.

The appliance boots automatically, and the setup utility appears (see Running Setup to Configure ACS, page 2-4).

Running Setup to Configure ACS

When you power up the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance for the first time, you are prompted to run the setup utility to configure the appliance. Before you run the utility using the **setup** command, ensure that you have values for the following network configuration prompts:

- Hostname
- IP address
- Netmask
- Gateway
- Domain
- Nameserver
- User ID
- Password

This example shows sample output of the **setup** command.

```
**************************************************
Please type 'setup' to configure the appliance
**************************************************
localhost login: setup

Last login: Mon Jul  2 08:45:24 on ttyS0

Press 'Ctrl-C' to abort setup
Enter hostname[]: acs
Enter IP address[]: 172.16.0.0
Enter IP default netmask[]: 255.255.255.224
Enter IP default gateway[]: 172.16.0.1
Enter default DNS domain[]: example.com
Enter Primary nameserver[]: 172.16.12.33
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: 172.16.12.33
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH Service? Y/N [N] : Y
Enter username[admin]:
Enter password:
Enter password again:
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs ...
/opt/CSCOacs/bin...
...
...
The system is going down for reboot NOW!
Application bundle (acs) installed successfully
INIT: Sending processes the TERM signal...
```

After you enter the required information, the appliance automatically reboots and the following login prompt appears:

```
machine_name login:
```

where *machine_name* identifies the hostname that you specified.

In this example, the following prompt appears:

```
ACS login:
```

To log in, use the administrator user account (and the corresponding password) that you created during the setup process. You must also use this Admin account to log in to the ACS CLI for the first time. See Accessing the ACS CLI, page 2-5.

After accessing the CLI as an administrator, you can create more users (with admin and operator privileges) with SSH access to the CLI by running the username command in the configuration mode.

Note   Any users that you create from the ACS web interface cannot automatically log in to the ACS CLI. You must explicitly create users with access to the CLI. To create these users, you must log in to the CLI using the Admin account that you created during setup; then, enter the configuration mode, and run the **username** command.

Accessing the ACS CLI

Before logging in to the ACS CLI, ensure that you have completed the hardware installation and configuration process outlined in Before Accessing the ACS CLI, page 2-1.

To log into ACS server and access the CLI, use an SSH secure shell client or the console port. You can log in from:

- A PC running Windows XP/Vista.
- A PC running Linux.
- An Apple computer running Mac OS X 10.4 or later.
- Any terminal device compatible with VT100 or ANSI characteristics. On the VT100-type and ANSI devices, you can use cursor-control and cursor-movement key.

    Keys include left arrow, up arrow, down arrow, right arrow, Delete, and Backspace. The CLI senses the use of the cursor-control keys and automatically uses the optimal device characteristics (see Supported Hardware and Software Platforms, page 2-5, for more information).

To exit the CLI, use the **exit** command from the EXEC mode. If currently in one of the configuration modes and you want to exit the CLI, enter the **end, exit, Ctrl-d** or **Ctrl-z** command to return to the EXEC mode, and then enter the **exit** command (see EXEC Mode, page 2-8).

Supported Hardware and Software Platforms

The following valid terminal types can access ACS:

- 1178
- 2621
- 5051
- 6053
- 8510
- altos5
- amiga

- ansi
- apollo
- Apple_Terminal
- att5425
- ibm327x
- kaypro
- vt100

See the terminfo database for a complete listing.

You can also access ACS through an SSH client or the console port.

Opening the CLI with Secure Shell

Note   To access the ACS CLI environment, use any SSH client that supports SSH v2.

The following example shows you how to log in with a Secure Shell (SSH) client (connecting to a wired WAN) via a PC by using Windows XP. Assuming that ACS is preconfigured through the setup utility to accept an Admin (administrator) user, log in as Admin.

Step 1   Use any SSH client and start an SSH session.

The SSH window appears.

Step 2   Press **Enter** or **Spacebar** to connect.

The Connect to Remote Host window appears.

Step 3   Enter a hostname, username, port number, and authentication method.

In this example, you enter **acs** for the hostname, **admin** for the username, and **22** for the port number; and, for the authentication method, choose **Password** from the drop-down list.

Step 4   Click **Connect**, or press **Enter**.

The Enter Password window appears, overlapping the Connect to Remote Host window.

Step 5   Enter your assigned password for the administrator.

The SSH with the Add Profile window appears.

Step 6   (Optional) Enter a profile name in the text box and click **Add to Profile**.

Step 7   Click **Close** on the Add Profile window.

The ACS prompt acs/admin# appears. You can now enter ACS CLI commands.

Opening the CLI Using a Local PC

If you need to configure ACS locally (without connecting to a wired LAN), you can connect a PC to the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance's console port (see Figure 2-1) by using a null-modem cable.

The serial console connector (port) provides access to the CLI locally by connecting a terminal—a PC running terminal-emulation software or an ASCII terminal—to the console port. The console port (EIA/TIA-232 asynchronous) requires only a null-modem cable.

To connect a PC running terminal-emulation software to the console port, use a DB-9 female to DB-9 female null-modem cable.

To connect an ASCII terminal to the console port, use a DB-9 female to DB-25 male straight-through cable with a DB-25 female to DB-25 female gender changer.

The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

✎
Note   If using a Cisco switch on the other side of the connection, set the switchport to duplex auto, speed auto (the default).

To open the CLI by connecting to the console port:

Step 1   Connect a null-modem cable to the console port on the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance and to the COM port on your PC.

Step 2   Set up a terminal emulator to communicate with ACS. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3   When the terminal emulator activates, press **Enter**.

Step 4   At the window, enter your username, and press **Enter**.

Step 5   Enter the password, and press **Enter**.

When the CLI activates, you can enter CLI commands to configure ACS.

Understanding the Command Modes

This section describes the ACS command modes in detail. The primary modes of operation are:

EXEC Mode

When you start a session on ACS, you begin in the Admin or EXEC mode. From the EXEC mode, you can enter the configuration mode. Most of the EXEC commands (one-time commands), such as **show** commands, display the current configuration status. The Admin or EXEC mode prompt consists of the device name or hostname before a pound sign (#), as shown:

```
acs/admin# (Admin or EXEC mode)
```

Note   Throughout this guide, the ACS server uses the name *acs* in place of the ACS server's hostname and *admin* for the user account.

You can always tell when you are in the EXEC mode, the ACS configuration mode, or the configuration mode by looking at the prompt. In the:

- EXEC mode, a pound sign (#) appears after the ACS server hostname and your username. For example:

  ```
  acs/admin#
  ```

- ACS configuration mode, the (config-acs) keyword and the pound sign (#) appear after the hostname of the ACS server and your username.

  You must have privileges to enter the ACS configuration mode, and must supply the username and the password that you use to log in to the ACS web interface. See ACS Configuration Mode, page 2-9.

  For example:

  ```
  acs/admin# acs-config
  Escape character is CNTL/D.

  Username: acsadmin
  Password: <pwd>

  acs/acsadmin(config-acs)# (ACS configuration mode)
  ```

- Configuration mode, the (config) keyword and a pound sign (#) appear after the hostname of the ACS server and your username.

  For example:

  ```
  acs/admin# configure
  Enter configuration commands, one per line.  End with CNTL/Z.
  acs/admin(config)# (configuration mode)
  ```

If you are familiar with UNIX, you can equate the EXEC mode to *root* access. You could also equate it to the administrator level in Windows NT or the supervisor in NetWare. In this mode, you have permission to access everything in the ACS server, including the configuration commands.

However, you cannot enter configuration commands directly. Before you can change the ACS server's actual configuration, you must enter the configuration mode by running the **configure** or **configure terminal (conf t)** command. Enter this command only when in the EXEC mode.

For example:

```
acs/admin# configure
Enter configuration commands, one per line. End with CNTL-Z.
acs(config)# (configuration mode)
```

The configuration mode has several submodes; each has its own prompt. To enter these submodes, you must first enter the configuration mode by entering the **configure terminal** command.

To exit the configuration mode, enter the **end**, **exit**, or **Ctrl-z** command. To exit the EXEC mode, enter the **exit** command.

To exit both configuration and EXEC modes, enter this sequence of commands:

```
acs/admin(config)# exit
acs/admin# exit
```

To obtain a listing of commands in the EXEC mode, enter a question mark (**?**):

```
acs/admin# ?
```

ACS Configuration Mode

Use the ACS configuration mode to set the debug log level for the ACS management and runtime components, show system settings, reset server certificate and IP address access list, and manage import and export processes.

You must have privileges to enter the ACS configuration mode. To do so, run the **acs-config** command in the EXEC mode; then, enter the administrative username and password that you use to log in to the ACS web interface.

The default username and password to access the ACS web interface are **acsadmin** and **default**, and the first time you log in to the web interface, you will be prompted to change the default password. Cisco recommends that you do so for security reasons. You can change your password for the first time only by logging into the web interface. You will also be prompted to install the license.

Note You cannot delete the default **acsadmin** user. You can, however, create other users with admin privileges from the web interface.

After resetting your password and installing a valid license, use the default username (**acsadmin**) and changed password, or the username and password for a newly created admin user, to access the ACS CLI in the ACS configuration mode.

When in the ACS configuration mode, ACS expects ACS configuration commands.

From this level, you can enter commands directly into the ACS configuration. To obtain a list of commands in this mode, enter a question mark (**?**). For example:

```
acs/admin(config-acs)# ?
```

You can enter **exit** or press **Ctrl-d** to leave the ACS configuration mode and return to the EXEC mode.

Some ethernet interface related attributes will be missing in the output while executing the CLI command **ethernet-interface show-configuration** in **acs-config mode** on the ESX machine. This is because the ESX does not support displaying all regular interface attributes.

For example:

```
Output in ESX server:
acs243-254/acsadmin(config-acs)# ethernet-interface show-configuration
Settings for eth0:
        Current message level: 0x00000007 (7)
        Link detected: yes
acs243-254/acsadmin(config-acs)#
```

Configuration Mode

Use the configuration mode to make changes to the existing configuration. When you save the configuration, these commands remain across ACS server reboots, but only if you run either of these commands:

- copy running-config startup-config
- write memory

To enter the configuration mode, run the **configure** or **configure terminal (conf t)** command in the EXEC mode. When in the configuration mode, ACS expects configuration commands.

For example:

```
acs/admin# configure
    Enter configuration commands, one per line. End with CNTL-Z.
acs/admin(config)# (configuration mode)
```

From this level, you can enter commands directly into the ACS configuration. To obtain a listing of commands in this mode, enter a question mark (**?**):

```
acs/admin(config)# ?
```

The configuration mode has several configuration submodes. Each of these submodes places you deeper in the prompt hierarchy. When you enter **exit**, ACS backs you out one level and returns you to the previous level. When you enter **exit** again, ACS backs you out to the EXEC level.

Note In the configuration mode, you can alternatively enter **Ctrl-z** instead of the **end** or **exit** command.

Configuration Submodes

In the configuration submodes, you can enter commands for specific configurations. For example:

```
acs/admin# configure terminal
acs/admin(config)# interface GigabitEthernet 0
acs/admin(config-GigabitEthernet)#
```

To obtain a list of commands in this mode, enter a question mark (**?**):

```
acs/admin(config-GigabitEthernet)# ?
```

Use the **exit** or **end** command to exit this prompt and return to the configuration prompt.

For the previous example, Table 2-1 lists the commands in that configuration submode. There are other configuration submodes, including those specific to the **kron**, **repository**, and **password policy** commands.

Table 2-1   Command Options for Configuration Submodes

Command	Comment
| ```
acs/admin(config)# interface GigabitEthernet 0
acs/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  do       EXEC command
  end      Exit from configure mode
  exit     Exit from this submode
  ip       Configure IP features
  ipv6     Configure IPv6 features
  no       Negate a command or set its defaults
  shutdown Shutdown the interface
acs/admin(config-ethernet)#
``` | Enter the command that you want to configure for the interface. This example uses the **interface GigabitEthernet** command. <br><br> Enter **?** to display what you can enter next on the command line. <br><br> This example shows the available **interface GigabitEthernet** configuration submode commands. |
| ```
acs/admin(config-GigabitEthernet)# ip ?
  address  Configure IP address
acs/admin(config-GigabitEthernet)# ip

acs/admin(config-GigabitEthernet)# ipv6 ?
  address  Configure IPv6 address
Enable/Disable IPv6 for the interface
``` | Enter the command that you want to configure for the interface. This example uses the **ip** and **ipv6** commands. <br><br> Enter **?** to display what you can enter next on the command line. <br><br> This example shows the available **ip** and **ipv6** configuration submode commands. |
| ```
acs/admin(config-GigabitEthernet)# ip address ?
  <A.B.C.D>  IPv4 address
acs/admin(config-GigabitEthernet) ip address

acs/admin(config-GigabitEthernet)# ipv6 address ?
  <X:X:X::X(/n)> Configure IPv6 address
  autoconfig Configure IPv6 auto-configuration address
acs/admin(config-GigabitEthernet) ip address
``` | Enter the command that you want to configure for the interface. This example uses the **ip address** and **ipv6 address** command. <br><br> Enter **?** to display what you must enter next on the command line. In this example, you must enter the required IPv4 and IPv6 addresses. <br><br> A carriage return <cr> does not appear; therefore, you must enter additional arguments to complete the command. |

Table 2-1   Command Options for Configuration Submodes (continued)

Command	Comment

`acs/admin(config-GigabitEthernet)# ip address`
`172.16.0.1 ?`
`  <A.B.C.D>  Network mask`
`acs/admin(config-GigabitEthernet)# ip address`
`172.16.0.1`
 	
`acs/admin(config-GigabitEthernet)# ipv6 address`
`2001:DB8::21/64 ?`
`<cr>  Carriage Return`
`acs/admin(config-GigabitEthernet)# ipv6 address`
`2001:DB8::21/64`
 	
`acs/admin(config-GigabitEthernet)# ipv6 address`
`autoconfig ?`
`<cr>  Carriage Return`
`acs/admin(config-GigabitEthernet)# ipv6 address`
`autoconfig`
	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IPv4 address and 2001:DB8::21/64 IPv6 address.
	
	Enter **?** to display what you can enter next on the command line.
	
	A carriage return <cr> does not display; therefore, you must enter additional arguments to complete the command.

`acs/admin(config-GigabitEthernet)# ip address`
`172.16.0.1 255.255.255.224 ?`
`  <cr>  Carriage Return`
`acs/admin(config-GigabitEthernet)# ip address`
`172.16.0.1 255.255.255.224`
	Enter the network mask. This example uses 255.255.255.224.
	
	Enter **?** to display what you can enter next on the command line.
	
	Press **Enter**. A carriage return <cr> displays; press **Enter** again to complete the command.

Navigating the CLI Commands

This section describes how to navigate the commands and modes on ACS.

Getting Help

Use the question mark (**?**) and the arrow keys to help you enter commands:

- For a list of available commands, enter a question mark (**?**):

  `acs/admin# ?`

- To complete a command, enter a few known characters before **?** (with no space):

  `acs/admin# s?`

- To display keywords and arguments for a command, enter **?** at the prompt or after entering part of a command followed by a space:

  `acs/admin# show ?`

  ACS displays a list and brief description of available keywords and arguments.

The <cr> symbol in command help stands for "carriage return" (**Return** or **Enter** key). The <cr> at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional.

The <cr> symbol by itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

- To redisplay a command that you previously entered, press the **Up Arrow** key. Continue to press the **Up Arrow** key to see more commands.

Using the No and Default Forms of Commands

Some EXEC or configuration commands have a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function disabled by default; for example, an IP address enabled by default. To disable the IP address, use the **no ip address** command; to re-enable the IP address, use the **ip address** command.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands disable by default, so in such cases using the **default** form has the same result as using the **no** form of the command.

However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values.

See Chapter 3, "ACS Command Reference," for a description of the complete syntax of the configuration commands, and the **no** and default forms of a command.

Command-Line Conventions

While reading this document, you might not understand some of the information if you do not know certain basic conventions of CLI usage.

Note the following sections:

Command-Line Editing Key Conventions

ACS provides a number of keyboard shortcuts that you can use to edit an entered line.

Tab

Tries to finish the current command.

Pressing the **Tab** key:

- At the beginning of a line, lists all the short-form options.
- When you enter a partial command, the system lists all the short form options beginning with those characters.
- When only one possible option is available, the system fills in the option automatically.

Ctrl-C

Aborts the sequence. Breaks out of any executing command and returns to the previous mode.

Ctrl-D

Exits the ACS configuration mode and returns to the EXEC mode.

Ctrl-Z

Exits the configuration mode and returns to the previous configuration mode.

?

You can get a list of the available commands by entering a question mark (**?**) at the prompt (see Getting Help, page 2-12).

Command-Line Completion

Command-line completion makes the ACS CLI more user-friendly. It saves you extra key strokes and helps out when you cannot remember a command's syntax.

For example, in the **show running-config** command:

```
acs/admin# show running-config
```

You could have used:

```
acs/admin# sh run
```

ACS expands the command **sh run** to **show running-config**.

Another shortcut is pressing the **Tab** key after you type **sh**; the ACS CLI fills in the best completion, in this case **show**.

If the ACS CLI does not understand a command, it repeats the entire command line and places a caret symbol (^) under the point at which it could not parse the command.

For example:

```
acs/admin# show running-config
                  ^
% Invalid input detected at '^' marker.
```

The caret symbol (^) points to the first letter in the command line that ACS does not understand. Usually, this means that you need to provide additional arguments to complete the command or you mispelled the command. In this case, you omitted the "r" in the "unning" command. To fix the error, retype the command.

In another form of command-line completion, you can start a command by entering the first few characters, and pressing the **Tab** key. As long as you can match one command, the ACS CLI will complete the command.

For example, if you type **sh** and press **Tab**, ACS completes the **sh** with **show**. If ACS does not complete the command, you can enter a few more letters and press **Tab** again. For more information, see Tab, page 2-13.

Continuing Output at the --More-- Prompt

When working with the ACS CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?** or **show** commands, the output pauses and a **--More--** prompt appears at the bottom of the screen.

To resume output, press **Return** to scroll down one line, or press the **spacebar** to display the next full screen of output.

Tip   If output pauses on your screen but you do not see the **--More--** prompt, try entering a smaller value for the screen length by using the **terminal length** EXEC command. Command output will not pause if you set the length value to zero (0).

Where to Go Next

Now that you are familiar with some of the ACS CLI basics, you can begin to configure ACS by using the CLI.

Remember that:

- You can use the question mark (**?**) and arrow keys to help you enter commands.

- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (**?**) to see a list of available commands.

- To disable a feature, enter the keyword **no** before the command; for example, **no ip address**.

- You must save your configuration changes so that you preserve them during a system reload or power outage.

Proceed to Chapter 3, "ACS Command Reference," for command listings, descriptions, syntax, usage guidelines, and sample output.