Overview of the ACS CLI

Cisco Secure Access Control System (ACS) 5.8 uses the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance running the Cisco Application Deployment Engine (ADE) OS 2.2.2.011. This chapter provides an overview of how to access the ACS CLI, the different command modes, and the commands that are available in each mode.

You can configure and monitor ACS 5.8 through the web interface. You can also use the CLI to perform the configuration and monitoring tasks that this guide describes.

The following sections describe the ACS CLI:

Accessing the ACS Command Environment

You can access the ACS CLI through a secure shell (SSH) client or the console port using one of the following machines:

- Windows PC running Windows 7/XP/Vista.
- Apple computer running Mac OS X 10.4 or later.
- PC running Linux.

For detailed information on accessing the CLI, see Using the ACS CLI, page 1

User Accounts and Modes in ACS

Two different types of accounts are available on the ACS server:

- Admin (administrator)
- Operator (user)

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. During this setup process, an administrator user account, also known as an Admin account, is created.

After you enter the initial configuration information, the appliance automatically reboots and prompts you to enter the username and the password that you specified for the Admin account. It is this Admin account that you must use to log in to the ACS CLI for the first time.

While an Admin can create and manage Operator (user) accounts (which have limited privileges and access to the ACS server), an Admin account provides you the functionality you require to use the ACS CLI. In ACS 5.8, you have one more role, called R/O Admin (read only Admin). R/O Admin can run all the **show** commands but cannot modify the configurations.

To create more users (with admin and operator privileges) with SSH access to the ACS CLI, you must run the **username** command in the configuration mode (see Types of Command Modes in ACS, page 4).

Table 1 on page 2 lists the command privileges for each type of user account: Admin and Operator (user).

Table 1 Command Privileges

Command	User Account	
	Admin	Operator (User)
access-setting accept-all	✓	
acs commands	✓	
acs config	✓	
acs-config-web-interface	✓	
application commands	✓	
backup	✓	
backup-logs	✓	
banner	✓	
cdp run	✓	
clock	✓	
configure terminal	✓	
copy commands	✓	
crypto	✓	✓
debug	✓	
debug-adclient	✓	
debug-log	✓	
delete	✓	
dir	✓	
end	✓	
exit	✓	✓
export-data	✓	
export-data-message-catalog	✓	
forceout	✓	
halt	✓	
hostname	✓	
icmp	✓	
import-data	✓	
import-export-abort	✓	
import-export-status	✓	
interface	✓	
ip default-gateway	✓	
ip domain-name	✓	
ip domain round-robin	✓	
ip domain timeout	✓	
ip name-server	✓	

Table 1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
ip route	✓	
ipv6 enable	✓	
ipv6 route	✓	
kron	✓	
logging commands	✓	
mkdir	✓	
nslookup	✓	✓
ntp	✓	
password	✓	✓
password policy	✓	
patch	✓	
ping	✓	✓
reload	✓	
replication	✓	
repository	✓	
reset-management-interface-certificate	✓	
restore commands	✓	
rmdir	✓	
service	✓	
show acs-cores	✓	✓
show acs-config-web-interface	✓	
show acs-logs	✓	✓
show application	✓	✓
show backup	✓	
show cdp	✓	✓
show clock	✓	✓
show cpu	✓	✓
show crypto	✓	✓
show debug-adclient	✓	
show debug-log	✓	
show disks	✓	✓
show icmp_status	✓	✓
show interface	✓	✓
show inventory	✓	✓
show ip route	✓	
show ipv6 route	✓	
show logging	✓	✓

Table 1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
show logins	✓	✓
show memory	✓	✓
show ntp	✓	✓
show ports	✓	✓
show process	✓	✓
show repository	✓	
show restore	✓	
show running-configuration	✓	
show startup-configuration	✓	
show tac	✓	
show tech-support	✓	
show terminal	✓	✓
show timezone	✓	✓
show timezones	✓	✓
show udi	✓	✓
show uptime	✓	✓
show users	✓	
show version	✓	✓
snmp-server commands	✓	
ssh	✓	✓
tcp	✓	
tech	✓	
telnet	✓	✓
terminal	✓	✓
traceroute	✓	✓
undebug	✓	
username	✓	
write	✓	

When you log in to the ACS server, it places you in the Operator (user) mode or the Admin (EXEC) mode. Typically, logging in requires a username and password.

You can always tell when you are in the Operator (user) mode or Admin (EXEC) mode by looking at the prompt. A right angle bracket (>) appears at the end of the Operator (user) mode prompt; a pound sign (#) appears at the end of the Admin mode prompt, regardless of the submode.

ACS configuration mode requires a specific, authorized user role to execute each ACS configuration command; see ACS Configuration Commands, page 8.

Types of Command Modes in ACS

ACS supports these command modes:

- EXEC—Use the commands in this mode to perform system-level configuration. In addition, certain EXEC mode commands have ACS-specific abilities. See EXEC Commands, page 5.
- ACS configuration—Use the commands in this mode to import or export configuration data, synchronize configuration information between the primary and secondary ACS, reset IP address filtering and management interface certificate, define debug logging and show the logging status.

  This mode requires an administrator user account to log in and perform the ACS configuration-related commands. See ACS Configuration Commands, page 8.
- Configuration—Use the commands in this mode to perform additional configuration tasks in ACS. See Configuration Commands, page 10.

EXEC Commands

EXEC commands primarily include system-level commands such as **show** and **reload** (for example, application installation, application start and stop, copy files and installations, restore backups, and display information).

In addition, certain EXEC-mode commands have ACS-specific abilities (for example, start an ACS instance, display and export ACS logs, and reset an ACS configuration to factory default settings.

- Table 2 on page 5 lists the EXEC commands and provides a short description of each.
- Table 3 on page 7 lists the show commands in the EXEC mode and provides a short description of each.

For detailed information on EXEC commands, see Understanding the Command Modes, page 7.

EXEC or System-Level Commands

Table 2 Summary of EXEC Commands

Command	Description
acs start | stop	Starts or stops an ACS server.
acs start | stop *process*	Starts or stops a process in ACS.
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
acs delete core	Deletes an ACS run-time core file or JVM core log.
acs delete log	Deletes an ACS run-time core file or JVM core log excluding the latest log.
acs config-web-interface	Enables or disables an interface for ACS configuration web.
acs patch	Installs and removes ACS patches.
acs reset-config	Resets the ACS configuration to factory defaults.
acs reset-password	Resets the ‘acsadmin’ administrator password to the default setting.
acs restore	Restores an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
acs zeorize-machine	Starts the zeroization; deletes key and sensitive files, running memory, and swap files.
application install	Installs a specific application bundle.
application remove	Removes a specific application.

Table 2 Summary of EXEC Commands (continued)

Command	Description
application reset-config	Resets an ACS configuration to factory defaults.
application start	Starts or enables a specific application.
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application bundle.
backup	Performs a backup and places the backup in a repository.
backup-logs	Performs a backup of all the logs on ACS to a remote location.
banner	Displays the banner text before and after logging in to ACS CLI.
clock	Sets the system clock on the ACS server.
configure	Enters the Configuration mode.
copy	Copies any file from a source to a destination.
crypto	Performs crypto key operations.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
delete	Deletes a file in the ACS server.
dir	Lists the files in the ACS server.
exit	Exits from the EXEC mode.
forceout	Forces the logout of all the sessions of a specific ACS server system user.
halt	Disables or shuts down the ACS server.
help	Describes the help utility and how to use it in the ACS server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 address or hostname of a remote system.
ping	Determines the network connectivity to a remote system.
password	Updates the CLI password.
reload	Reboots the ACS server.
restore	Restores a previous backup.
rmdir	Removes an existing directory.
show	Provides information about the ACS server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Technical Assistance Center (TAC) commands.
telnet	Telnets to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.

Table 2 Summary of EXEC Commands (continued)

Command	Description
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations. For example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Copies, displays, or erases the running ACS server information.

Show Commands

The show commands are used to view the ACS settings and are among the most useful commands. See Table 3 on page 7 for a summary of the **show** commands.

The commands in Table 3 on page 7 require the **show** command to be followed by a keyword; for example, **show application**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

Table 3 Summary of Show Commands

Command	Description
acs-cores	Displays ACS run-time core files and JVM core logs.
acs-logs	Displays ACS server debug logs.
acs config-web-interface	Indicates whether an interface is disabled or enabled for ACS configuration web.
application (requires keyword)	Displays information about the installed application. For example, status information or version information.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol (CDP) interfaces.
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
crypto	Displays crypto key information.
disks	Displays file-system information of the disks.
icmp_status	Displays the Internet Control Message Protocol (ICMP) echo/response configuration information.
interface	Displays statistics for all the interfaces configured on ACS.
inventory	Displays information about the hardware inventory, including the ACS appliance model and serial number.
logging (requires keyword)	Displays ACS server logging information.
ip route	Displays the static ip routes.
ipv6 route	Displays the ipv6 routes.
logins (requires keyword)	Displays the login history of an ACS server.
memory	Displays memory usage by all running processes.

Table 3 Summary of Show Commands

Command	Description
ntp	Displays the status of the Network Time Protocol (NTP) servers.
ports	Displays all the processes listening on the active ports.
process	Displays information about the active processes of the ACS server.
repository (requires keyword)	Displays the file contents of a specific repository.
restore (requires keyword)	Displays the restore history in ACS.
running-config	Displays the contents of the configuration file that currently runs in ACS.
startup-config	Displays the contents of the startup configuration in ACS.
tech-support	Displays system and configuration information that you can provide to the Cisco Technical Assistance Center (TAC) when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the current time zone in ACS.
timezones	Displays all the time zones available for use in ACS.
udi	Displays information about the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 Unique Device Identifier (UDI).
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information about the system users.
version	Displays information about the currently loaded software version, along with hardware and device information.

ACS Configuration Commands

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

The ACS configuration mode requires a specific, authorized user role to execute each ACS configuration command. These commands are briefly described in Table 4 on page 9. For detailed information on the roles in ACS 5.8, see the *User Guide for Cisco Secure Access Control System 5.8.*

To access the ACS configuration mode, enter the **acs-config** command in EXEC mode.

Table 4 on page 9 lists the ACS configuration commands and provides a short description of each.

Table 4 Summary of ACS Configuration Commands

Command	Description	Required User Role
access-setting accept-all	Resets IP address filtering to allow all IP addresses to access the management pages of an ACS server.	Only the super admin can run this command on a primary ACS node.
acsview-db-compress	Compresses the ACS View database by rebuilding each table in the database and releasing the unused space. As a result, the physical size of the database is reduced.	Any authorized user, irrespective of role, can run this command.
acsview merge-from-supportbundle	Merges the ACS View database with the specified support bundle data.	Only the super admin or system admin can run this command.
acsview rebuild-database	Rebuilds the ACS View database and keeps the log data only for the specified number of days.	Only the super admin or system admin can run this command.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS View database and makes it as a fresh database.	Only the super admin or system admin can run this command.
acsview replace-cleandb	Removes all data from the ACS View database and makes the current View database as a fresh View database.	Only the super admin or system admin can run this command.
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.	Only the super admin or system admin can run this command.
acsview truncate-log	Truncates the ACS view database transaction logs.	Only the super admin or system admin can run this command.
database-compress	Reduces the ACS database size by removing unused disk space from within the ACS database file.	Any authorized user, irrespective of role, can run this command.
debug-adclient	Enables debug logging of an Active Directory client.	Only the network-device admin can run this command.
debug-log	Defines the local debug logging level for the ACS components.	Any authorized user, irrespective of role, can run this command.
export-data	Exports configuration data from an ACS local store to a remote repository.	Only users who have Read permission to a specific configuration object in the web interface can export that particular configuration data to a remote repository.
export-data-message-catalog	Exports the message catalog messages from the ACS message catalog to a remote repository.	Only users who have Read permission to the message catalog messages in ACS web interface can export those particular log messages to a remote repository.
import-data	Imports configuration data from a remote repository to an ACS local store.	Only users who have Create, Read, Update, and Delete (CRUD) permissions to a specific configuration object in the web interface can import that particular configuration data to an ACS local store.

Table 4 Summary of ACS Configuration Commands (continued)

Command	Description	Required User Role
import-export-abort	Aborts specific (or all) import and export processes.	Only the super admin can simultaneously abort a running process and all pending import and export processes. However, a user who owns a particular import or export process can terminate that particular process by using the process ID, or by stopping the process when it is in progress.
import-export-status	Displays the status of the import and export processes.	Any authorized user, irrespective of role, can run this command.
no debug-adclient	Disables debug logging of an Active Directory client.	Only the network-device admin can run this command.
no debug-log	Restores the default local debug logging level of the ACS components.	Any authorized user, irrespective of role, can run this command.
replication force-sync	Synchronizes configuration information between the primary and secondary ACS.	Only the super admin or system admin can run this command on a secondary ACS node.
replication status	Shows the replication status of the ACS database.	Only the super admin or system admin can run this command.
reset-management-interface-certificate	Resets the management interface certificate to the default self-signed certificate.	Only the super admin or system admin can run this command.
show debug-adclient	Displays debug logging status for an Active Directory client.	Any authorized user, irrespective of role, can run this command.
show debug-log	Displays the local debug logging status for subsystems.	Any authorized user, irrespective of role, can run this command.

For detailed information on ACS Configuration mode commands, see Understanding the Command Modes, page 7.

Configuration Commands

Configuration commands include **interface** and **repository**. To access the configuration mode, run the **configure** command in the EXEC mode.

Some of the configuration commands will require you to enter the configuration submode to complete the configuration.

Table 5 on page 10 lists the configuration commands and provides a short description of each.

Table 5 Summary of Configuration Commands

Command	Description
backup-staging-url	Specifies a Network File System (NFS) temporary space or staging area for the remote directory for backup and restore operations.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from the ACS server before discarding it.
cdp run	Enables CDP.
cdp timer	Specifies how often the ACS server sends CDP updates.
clock	Sets the time zone for display purposes.
conn-limit	Configures the TCP connection limit from the source IP.

Table 5 Summary of Configuration Commands (continued)

Command	Description
do	Executes an EXEC-level command from the configuration mode or any configuration submode. To initiate, the **do** command precedes the EXEC command.
end	Returns to EXEC mode.
exit	Exits the configuration mode.
hostname	Sets the hostname of the system. **Note:** When you intend to use the AD ID store and set up multiple ACS instances with the same name prefix, use a maximum of 19 characters for the hostname, so that it does not affect AD functionality.
icmp echo	Configures the ICMP echo requests.
interface	Configures an interface type and enters the interface configuration mode.
ip address	Sets the IP address and netmask for the Ethernet interface. This is an interface configuration command.
ipv6 address	Sets the IPv6 address and prefix length for the Ethernet interface. This is an interface configuration command.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration in the interface configuration mode.
ip default-gateway	Defines or sets a default gateway with an IP address.
ip domain-name	Defines a default domain name that an ACS server uses to complete hostnames.
ip domain round-robin	Defines a round robin selection of name servers from the available list of name servers.
ip domain timeout	Defines a default amount of time the resolver will wait for a response from a remote name server before retrying the query via a different name server
ip name-server	Sets the Domain Name System (DNS) servers for use during a DNS query.
ip route	Configures the static IPv4 address routes.
ipv6 enable	Enables the IPv6 stack globally or for a specific interface.
ipv6 route	Configures the static IPv6 address routes.
kron occurrence	Schedules one or more Command Scheduler commands to run at a specific date and time or at a recurring level.
kron policy-list	Specifies a name for a Command Scheduler policy.
logging	Enables the system to forward logs to a remote system.
logging loglevel	Configures the log level for the **logging** command.
max-ssh	Configures the number of concurrent SSH sessions with a remote system.
no	Disables or removes the function associated with the command.
ntp	Synchronizes the software clock through the NTP server for the system.
ntp authenticate	Enables authentication of all time sources.
ntp authentication-key	Adds Message Digest 5 (MD5)-type authentication keys for trusted time sources.
ntp server	Specifies an NTP server to use.
ntp trusted-key	Specifies the key numbers for trusted time sources.
password-policy	Enables and configures the password policy.
rate-limit	Configures the TCP/UDP/ICMP packet-rate limit from the source IP.

Table 5 Summary of Configuration Commands (continued)

Command	Description
repository	Enters the repository submode.
service	Specifies the type of service to manage.
snmp-server community	Sets up the community access string to permit access to the Simple Network Management Protocol (SNMP).
snmp-server contact	Configures the SNMP contact MIB value on the system.
snmp-server host	Sends SNMP traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server trap dskThresholdLimit	Configures the SNMP server to receive traps when a ACS partition reaches its disk threshold utilization value.
synflood-limit	Configures the TCP SYN packet limit from the source IP.
tcp	Enables fast recycling of TIME_WAIT sockets, enables reuse of TIME_WAIT sockets, and configures the timeout value for TCP final packets.
username	Adds a user to the system with a password and a privilege level.

For detailed information on configuration mode and submode commands, see Understanding the Command Modes, page 7.

CLI Audit

You must have administrator access to execute ACS configuration commands. Whenever an administrator logs in to the configuration mode and executes a command that causes configuration changes in the ACS server, the information related to those changes is logged in the ACS operational logs.

Table 6 on page 12 lists the configuration mode commands that, when executed, generate operational logs.

Table 6 Configuration Mode Commands for the Operation Log

Command	Description
clock	Sets the system clock on the ACS server.
hostname	Sets the hostname of the system.
ip address	Sets the IP address and netmask for the Ethernet interface.
ip name-server	Sets the DNS servers for use during a DNS query.
ntp	Specifies NTP configuration.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

You can view these logs using the **show acs-logs** command. For more information on log file types and the information that is stored in each log file, see show acs-logs, page 90.

In addition to the configuration mode commands, there are some commands in the EXEC and ACS configuration mode that generate operational logs, as listed in Table 7 on page 12 and Table 8 on page 13:

Table 7 EXEC Mode Commands for the Operation Log

Command	Description
acs (Instance)	Starts or stops an ACS instance.
acs (Process)	Starts or stops an ACS process.
acs backup	Performs a backup of an ACS configuration.

Table 7 EXEC Mode Commands for the Operation Log (continued)

Command	Description
acs delete core	Deletes an ACS run-time core file or JVM core log.
acs delete log	Deletes an ACS run-time core file or JVM core log excluding the latest log.
acs patch	Installs and removes ACS patches.
acs restore	Performs a restoration of an ACS configuration.
acs reset-config	Resets the ACS configuration to factory defaults.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository. If View exists, View data will also get backed up.
backup-logs	Backs up system logs.
restore	Restores from backup the file contents of a specific repository.

Table 8 ACS Configuration Mode Commands for the Operation Log

Command	Description
access-setting accept-all	Resets the IP address filtering to allow all IP addresses to access the management pages of an ACS server.
debug-adclient	Enables debug logging of an Active Directory client.
debug-log	Defines the local debug logging level for the ACS components.
export-data	Exports configuration data from an ACS local store to a remote repository.
export-data-message -catalog	Exports the message catalog messages from ACS message catalog to a remote repository.
import-data	Imports configuration data from a remote repository to an ACS local store.
import-export-abort	Aborts specific (or all) import and export processes.
replication	Synchronizes configuration information between the primary and secondary ACS.
reset-management-interface-certificate	Resets the management interface certificate to the default self-signed certificate.