CLI Reference Guide for Cisco Secure Access Control System 5.4

October 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26227-01

CLI Reference Guide for Cisco Secure Access Control System 5.4

CONTENTS

CONTENTS

Preface

This guide describes how you can configure and maintain Cisco Secure Access Control System (ACS) 5.4 by using the command-line interface (CLI). Each topic provides a high-level summary of the tasks required for using the CLI in the Cisco Application Deployment Engine (ADE) OS 2.0 that, in combination with ACS 5.4, runs on the CSACS-1121 or Cisco SNS-3415 appliance.

This preface includes:

Note Use this guide in conjunction with the documentation listed in Related Documentation, page xi.

Who Should Read This Guide

The majority of the instructions in this guide are straightforward; however, a few are complex. Therefore, only experienced users should use these instructions.

Note Use this guide in conjunction with the documentation listed in Related Documentation, page xi.

How to Use This Guide

Cisco makes the following recommendations for using this document:

- Read the document in its entirety. Subsequent sections build on information and recommendations discussed in previous sections.
- Use this document for all-inclusive information about the ACS appliance.
- Do not vary the command-line conventions (see Document Conventions, page x).

How This Guide Is Organized

This table lists the major sections of this guide.

Title	Description
Chapter 1, "Overview of the ACS CLI"	Provides an overview of the ACS CLI environment and command modes.
Chapter 2, "Using the ACS CLI"	Describes how you can access and administer ACS from the CLI.
Chapter 3, "ACS Command Reference"	Provides a complete description of all the commands.

Document Conventions

This guide uses the following conventions to convey instructions and information.

Convention	Description
bold font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`courier` font	Examples of information displayed on the screen.
`bold courier` font	Examples of information you must enter.
< >	Nonprinting characters (for example, passwords) appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. A tip might not consist of an action or troubleshooting help, but could still contain useful information.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Documentation Updates

Table 1 Updates to CLI Reference Guide for Cisco Secure Access Control System 5.4

Date	Description
10/30/2012	Updated the guide with Cisco 3415 Secure Access Control System information.
10/23/2012	Cisco Secure Access Control System, Release 5.4

Related Documentation

Note It is possible for the printed and electronic documentation to be updated after original publication. Therefore, you should also review the documentation on http://www.cisco.com for any updates.

Table 2 lists the product documentation that is available for ACS 5.4. To find end-user documentation for all the products on Cisco.com, go to: http://www.cisco.com/go/techdocs

Select **Products > Security > Access Control and Policy > Policy and Access Management > Cisco Secure Access Control System**.

Table 2 Product Documentation

Document Title	Available Formats
Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps9911/products_documentation_roadmaps_list.html
Release Notes for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/prod_release_notes_list.html
User Guide for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/products_user_guide_list.html
Installation and Upgrade Guide for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/prod_installation_guides_list.html
Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/products_device_support_tables_list.html
Migration Guide for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/prod_installation_guides_list.html
Software Developer's Guide for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/products/ps9911/products_programming_reference_guides_list.html
Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.4	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/regulatory/compliance/csacsrcsi.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Overview of the ACS CLI

Cisco Secure Access Control System (ACS) 5.4 uses the CSACS-1121 appliance or Cisco SNS-3415 appliance running the Cisco Application Deployment Engine (ADE) OS 2.0. 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 5.4 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 Chapter 2, "Using the ACS CLI."

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 or Cisco SNS-3415 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 5.4, 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 1-5).

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

Table 1-1 Command Privileges

	User Account	
Command	**Admin**	**Operator (User)**
access-setting accept-all	✓	
acs commands	✓	
acs config-web-interface	✓	
acs-config	✓	
acs troubleshoot adcheck	✓	
acs troubleshoot adinfo	✓	
acs troubleshoot ldapsearch	✓	
application commands	✓	
backup	✓	
backup-logs	✓	
cdp run	✓	
clock	✓	
configure terminal	✓	
copy commands	✓	
debug	✓	
debug-adclient	✓	
debug-log	✓	
delete	✓	
dir	✓	
end	✓	
exit	✓	✓
export-data	✓	
forceout	✓	
halt	✓	
host-key sync	✓	

Table 1-1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
hostname	✓	
icmp	✓	
import-data	✓	
import-export-abort	✓	
import-export-status	✓	
interface	✓	
ip default-gateway	✓	
ip domain-name	✓	
ip name-server	✓	
ip route	✓	
ipv6 route	✓	
kron	✓	
logging commands	✓	
mkdir	✓	
nslookup	✓	✓
ntp server	✓	
password policy	✓	
patch	✓	
ping	✓	✓
reload	✓	
replication	✓	
repository	✓	
reset-management-interface-certificate	✓	
restore commands	✓	
rmdir	✓	
service	✓	
show acs-cores	✓	✓
show acs-logs	✓	✓
show acs-config-web-interface	✓	
show application	✓	✓
show backup	✓	
show cdp	✓	✓
show clock	✓	✓
show cpu	✓	✓
show debug-adclient	✓	

Table 1-1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
show debug-log	✓	
show disks	✓	✓
show icmp_status	✓	✓
show interface	✓	✓
show inventory	✓	✓
show ip route	✓	
show ipv6 route	✓	
show logging	✓	✓
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	✓	✓
tech	✓	
telnet	✓	✓
terminal	✓	✓
traceroute	✓	✓
undebug	✓	
username	✓	
write	✓	

When you log into 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.

The ACS configuration mode requires a specific, authorized user role to execute each ACS configuration command; see ACS Configuration Commands, page 1-9.

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 1-5.
- 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 1-9.
- Configuration—Use the commands in this mode to perform additional configuration tasks in ACS. See Configuration Commands, page 1-12.

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 1-2 lists the EXEC commands and provides a short description of each.
- Table 1-3 lists the show commands in the EXEC mode and provides a short description of each.

For detailed information on EXEC commands, see Understanding Command Modes, page 2-7.

EXEC or System-Level Commands

Table 1-2 describes the EXEC mode commands.

Table 1-2 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 troubleshoot adcheck	Tests the Active Directory (AD) configuration and checks for compatibility with AD agent.
acs troubleshoot adinfo	Retrieves the information from AD regarding join settings, status, domain users, and domain controllers.
acs troubleshoot ldapsearch	Performs a Lightweight Directory Access Protocol (LDAP).
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.
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.
clock	Sets the system clock on the ACS server.
configure	Enters the Configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.

Table 1-2 Summary of EXEC Commands (continued)

Command	Description
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.
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.
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 1-3 for a summary of the **show** commands.

The commands in Table 1-3 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 1-3 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.
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.
logins (requires keyword)	Displays the login history of an ACS server.
memory	Displays memory usage by all running processes.
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.

Table 1-3 Summary of Show Commands (continued)

Command	Description
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's or Cisco SNS-3415's 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.
ip route	Displays information for specific IP addresses, network masks or protocols.
ipv6 route	Displays information for specific IPv6 addresses, prefix or protocols.

ACS Configuration Commands

Use ACS configuration commands 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.

The ACS configuration mode requires a specific, authorized user role to execute each ACS configuration command. These commands are briefly described in Table 1-4. For detailed information on roles in ACS 5.4, refer to the *User Guide for Cisco Secure Access Control System 5.4*.

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

Table 1-4 lists the ACS Configuration commands and provides a short description of each.

Table 1-4 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.

Table 1-4 Summary of ACS Configuration Commands (continued)

Command	Description	Required User Role
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make 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.
ad-agent-configuration	Adds the parameter to the end of the file, if the parameter is not found in the Centrify configuration file. **Note** There is no validity check on the parameter values.	Any authorized user, irrespective of role, can run this command.
ad-agent-reset-configuration	Resets the configuration of the AD Agent.	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 GUI can export that particular configuration data 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 GUI can import that particular configuration data to an ACS local store.
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.

Table 1-4 Summary of ACS Configuration Commands (continued)

Command	Description	Required User Role
import-export-status	Displays the status of the import and export processes.	Any authorized user, irrespective of role, can run this command.
no ad-agent-configuration	It comments out the lines that contain the parameter name.	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 ad-agent-configuration	Prints the lines that contain the parameter name in the Centrify configuration file.	Any authorized user, irrespective of role, can run this command.
show ad-agent-configuration-changes	Prints all the configuration changes that are made (local or distribute) in a node of a particular deployment.	Any authorized user, irrespective of role, 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.
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.

For detailed information on ACS Configuration mode commands, see Understanding Command Modes, page 2-7.

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 1-5 lists the configuration commands and provides a short description of each.

Table 1-5 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.
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 the EXEC mode.
exit	Exits the Configuration mode.
host-key sync	Generates RSA keys between the host and ACS machines when you configure Secure File Transfer Protocol (SFTP) repository.
hostname	Sets the hostname of the system. **Note** When you intend to use the AD ID store and set up multiple ACS instances with same name prefix, use a maximum of 15 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.
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 name-server	Sets the Domain Name System (DNS) servers for use during a DNS query.
kron occurrence	Schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level.
kron policy-list	Specifies a name for a Command Scheduler policy.

Table 1-5 Summary of Configuration Commands (continued)

Command	Description
logging	Enables the system to forward logs to a remote system.
logging loglevel	Configures the log level for the **logging** command.
no	Disables or removes the function associated with the command.
ntp	Synchronizes the software clock through the NTP server for the system.
password-policy	Enables and configures the password policy.
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.
username	Adds a user to the system with a password and a privilege level.

Note The modifications done to the Centrify configuration file are not distributed. They are done for each ACS instance.

For detailed information on configuration mode and submode commands, see Understanding Command Modes, page 2-7.

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 configurational changes in the ACS server, the information related to those changes is logged in the ACS operational logs.

Table 1-7 lists the configuration mode commands that, when executed, generate operational logs.

Table 1-6 Configuration Mode Commands for the Operation Log

Command	Description
clock	Sets the system clock on the ACS server.
ip name-server	Sets the DNS servers for use during a DNS query.
hostname	Sets the hostname of the system.
ip address	Sets the IP address and netmask for the Ethernet interface.
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 3-72.

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 1-7 and Table 1-8:

Table 1-7 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.
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.
restore	Restores from backup the file contents of a specific repository.
acs backup	Performs a backup of an ACS configuration.
acs restore	Performs a restoration of an ACS configuration.
acs reset-config	Resets the ACS configuration to factory defaults.
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.
backup-logs	Backs up system logs.
acs patch	Installs and removes ACS patches.
acs support	Gathers information for ACS troubleshooting.

Table 1-8 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.
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.
reset-management-interface-certificate	Resets the management interface certificate to the default self-signed certificate.
replication	Synchronizes configuration information between the primary and secondary ACS.

CHAPTER 2

Using the ACS CLI

This chapter provides helpful tips for understanding and configuring the Cisco Secure ACS 5.4 from the CLI. It contains:

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 or Cisco SNS-3415 appliances. For detailed information, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*.

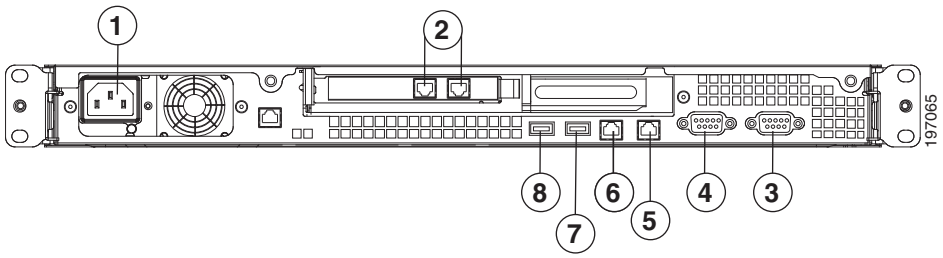
1. Starting the CSACS-1121 or Cisco SNS-3415 appliance, page 2-2
2. Running Setup to Configure ACS, page 2-3

Starting the CSACS-1121 or Cisco SNS-3415 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 5.4*.

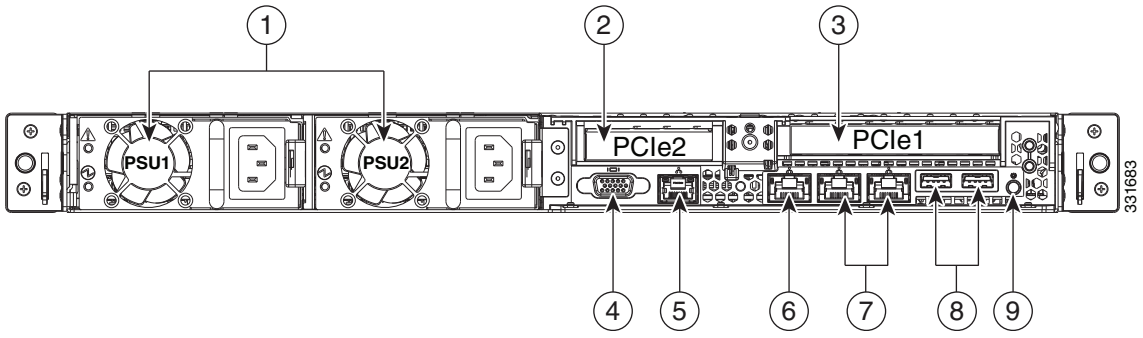
Step 3 Power up the CSACS-1121.

The appliance boots automatically and the setup utility appears (see Running Setup to Configure ACS, page 2-3).

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

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

Figure 2-2 Cisco SNS-3415 Series Appliance Rear View



1	Power supplies (up to two)	6	1 GbE dedicated management port
2	Slot 2: Low-profile PCIe slot on riser (half-height, half-length, x16 connector, x8 lane width)	7	Dual 1 GbE ports (LAN1 and LAN2)
3	Slot 1: Standard-profile PCIe slot on riser (full-height, half-length, x24 connector, x16 lane width)	8	USB ports
4	VGA video connector	9	Rear Identification button/LED
5	Serial port (RJ-45 connector)	-	

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

The setup utility (that appears when the Cisco SNS-3415 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 5.4*.

Step 3 Power up the Cisco SNS-3415.

The appliance boots automatically and the setup utility appears (see Running Setup to Configure ACS, page 2-3).

Running Setup to Configure ACS

When you power up the CSACS-1121 or Cisco SNS-3415 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]:
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, this 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 2-4.

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 into 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 2-7).

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 or Cisco SNS-3415 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 or Cisco SNS-3415 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, then press **Enter**.

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

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

Understanding Command Modes

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

- EXEC Mode, page 2-7
- ACS Configuration Mode, page 2-8
- Configuration Mode, page 2-9
- Configuration Submodes, page 2-10

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 2-8.

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# config t
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.
	Enter **?** to display what you must enter next on the command line.
	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 IP address`
`acs/admin(config-GigabitEthernet)# ipv6`
	Enter the command that you want to configure for the interface. This example uses the **ip** and **ipv6** command.
	Enter **?** to display what you must enter next on the command line.
	This example shows the available **ip** and **ipv6** configuration submode commands.

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

Command	Comment
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. Enter **?** to display what you must enter next on the command line. In this example, you must enter an required IPv4 and IPv6 addresses accordingly to configure it. A carriage return <cr> does not appear; therefore, you must enter additional arguments to complete the command.
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 2001:10::21/64 ?** <cr> Carriage Return acs/admin(config-GigabitEthernet)# **ipv6 address 2001:10::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 2001:10::21/64 IPv6 address. Enter **?** to display what you must 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 the 255.255.255.224 IP address. Enter **?** to display what you must enter next on the command line. In this example, you can press **Enter**. A carriage return <cr> displays; you can press **Enter** 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, page 2-13
- Command-Line Completion, page 2-13
- Continuing Output at the --More-- Prompt, page 2-14

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-configuration** command:

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

You could have used:

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

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

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-configuration
                ^
% 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, then 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.

CHAPTER 3

ACS Command Reference

This chapter contains an alphabetical listing of the commands that are specific to Cisco Secure ACS 5.4. The commands comprise these modes:

- EXEC
  - System-level
  - Show
- ACS Configuration

  Use the EXEC mode system-level **acs-config** command to access the ACS Configuration mode.
- Configuration
  - Configuration submode

  Use the EXEC mode system-level **configure** command to access the Configuration mode.

Each of the commands in this appendix is followed by a brief description of its use, command syntax, usage guidelines, and one or more examples. Throughout this appendix, the ACS server uses the name *acs* in place of the ACS server's hostname.

Note If an error occurs in any command usage, use the **debug** command to determine the cause of the error.

Before proceeding to use the ACS CLI commands, familiarize yourself with disk space management in CSACS-1121 or Cisco SNS-3415. This section describes disk space management for the purpose of managing logs that you can view or download from the ACS CLI and includes:

- Debug logs.
- Debug backup logs.
- Platform logs.

Managing disk space on the CSACS-1121 or Cisco SNS-3415 is important to enable you to use ACS efficiently. Table 3-1 describes the disk space allocated for each set of log files.

Table 3-1 Disk Space Allocation for ACS Process Logs

Process	Log File	Maximum Disk Space (in MB)
ADE OS 2.0	/var/log/ade/ADE.log	50
Monit	/opt/CSCOacs/logs/monit.log	55

Table 3-1 Disk Space Allocation for ACS Process Logs (continued)

Process	Log File	Maximum Disk Space (in MB)
Management	/opt/CSCOacs/logs/ACSManagementAudit.log	55
	/opt/CSCOacs/logs/ACSManagement.log	1000
	/opt/CSCOacs/mgmt/apache-tomcat-5.5.20/logs/*	55
Runtime	/opt/CSCOacs/logs/acsRuntime.log*	1000
	/opt/CSCOacs/runtime/config/*startup_cache*	1000
	/opt/CSCOacs/runtime/core.*	2000
	/opt/CSCOacs/logs/localStore/*	95000
Config Database	/opt/CSCOacs/db/acs.db	> 5120
	/opt/CSCOacs/db/acs*.log	100
	/opt/CSCOacs/db/dberr.log	100
Viewer	/opt/CSCOacs/logs/*	155
Viewer database	/opt/CSCOacs/view/data/db/acsview.db	150000
	/opt/CSCOacs/view/data/db/acsview.log	100
	/opt/CSCOacs/view/data/db/acsview.errlog	100
AD Agent	/var/log/centrifydc.log	50
	/opt/CSCOacs/logs/ACSADAgent.log	55
Backup	Packaged files within a temporary directory	105000
	/var/log/backup.log	50
	/var/log/backup-success.log	50
Upgrade/Patch	/opt/CSCOacs/patches/*	500
	/opt/CSCOacs/logs/acsupgrade.log	50

Log files in ACS are managed using various utilities, such as logrotate, log4j, and log4cxx. The log files are numbered and rolled over based on a configured maximum file size. Once a log file touches the configured limit, the data is rolled over to another file. This file is renamed in the *XXX.N*.log format, where:

- *XXX*—Specifies the name of the log file.
- *N*—Specifies any value from 1 to 10. This value varies depending on the log file. While some utilities roll over up to 10 log files, others roll over up to 9 log files. For information on these log files, see Table 3-2.

For instance, the default maximum file size for log files that logrotate manages is 5 MB. When a log file (for example, acsupgrade.log) reaches the 5-MB limit, it is renamed as acsupgrade.log.1. With every 5-MB increase in file size, the latest file is renamed as acsupgrade.log.2, acsupgrade.log.3, and so on.

Logrotate stores up to 10 log files at a given time. The latest log information, however, is always stored in acsupgrade.log. In ACS, logrotate runs as an hourly kron job and verifies the disk space allocated for the log files.

Table 3-2 Log File Rotation

Process	Log File	Number of Rotated Versions
Monit	/opt/CSCOacs/logs/monit.log	10
Upgrade	/opt/CSCOacs/logs/acsupgrade.log	10
Management	/opt/CSCOacs/mgmt/apache-tomcat-5.5.20/logs/catalina.out	10
	/opt/CSCOacs/logs/ACSManagement.log	9
	/opt/CSCOacs/logs/ACSManagementAudit.log	10
	/opt/CSCOacs/logs/MonitoringAndReportingProcess.log	10
AD Agent	/opt/CSCOacs/logs/ACSADAgent.log	10
Runtime	/opt/CSCOacs/logs/acsRuntime.log	9

For detailed information on logging in ACS 5.4, refer to the *User Guide for Cisco Secure Access Control System 5.4*.

This appendix describes:

EXEC Commands

Each EXEC command includes a brief description of its use, command syntax, usage guidelines, and sample output.

Table 3-3 lists the EXEC commands that this section describes.

Table 3-3 List of EXEC Commands[1]

• acs (instance) *	• application install	• mkdir
• acs (process) *	• application remove	• nslookup
• acs backup *	• application reset-config	• ping
• acs-config *	• application start	• reload
• acs config-web-interface	• application stop	• restore *
• acs delete core *	• application upgrade	• rmdir
• acs delete log *	• backup *	• show (see Show Commands)
• acs patch *	• backup-logs	• shutdown
• acs reset-config *	• clock	• ssh
• acs reset-password *	• configure	• tech
• acs restore *	• copy *	• telnet
• acs support *	• debug	• terminal length
• acs troubleshoot adcheck	• delete	• terminal session-timeout
• acs troubleshoot adinfo	• dir	• terminal session-welcome
• acs troubleshoot ldapsearch	• exit	• terminal terminal-type
• acs zeroize-machine *	• forceout	• traceroute
	• halt	• undebug
	• help	• write

1. Commands marked with an asterisk (*) represent those that are specific to ACS functionality.

acs (instance)

To start or stop an ACS instance, use the **acs** command in the EXEC mode.

acs {**start** | **stop**}

Syntax Description

start	Starts an ACS instance.
stop	Stops an ACS instance.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you use the **acs stop** command to stop your ACS, the ACS instance automatically starts the next time the CSACS-1121 or Cisco SNS-3415 appliance boots up.

Examples

Example 1

```
acs/admin# acs start

Starting ACS ............................

To verify that ACS processes are running, use the
'show application status acs' command.
```

Example 2

```
acs/admin#

acs/admin# acs stop

Stopping ACS ......................

acs/admin#
```

Related Commands

Command	Description
acs (process)	Starts or stops an ACS process.
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
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.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs (process)

To start or stop an individual process of an ACS instance, use the **acs** command in the EXEC mode.

acs {**start** | **stop**} {**adclient** | **database** | **management** | **runtime** | **view-logprocessor** | **view-alertmanager** | **view-collector** | **view-database** | **view-jobmanager**}

Syntax Description

start	Starts an ACS process.
stop	Stops an ACS process.
adclient	Starts or stops the adclient process of an ACS server.
database	Starts or stops the database process of an ACS server.
management	Starts or stops the management process of an ACS server.
runtime	Starts or stops the runtime process of an ACS server.
view-logprocessor	Starts or stops the view-logprocessor process of an ACS server.
view-alertmanager	Starts or stops the view-alertmanager process of an ACS server.
view-collector	Starts or stops the view-collector process of an ACS server.
view-database	Starts or stops the view-database process of an ACS server.
view-jobmanager	Starts or stops the view-jobmanager process of an ACS server.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you use the **acs stop** command to stop any ACS process, it automatically starts the next time the CSACS-1121 or Cisco SNS-3415 appliance boots up.

When ACS cannot start or stop the ACS process that you want to start or stop, it prompts you with a relevant message.

The ACS processes may fail to start or stop in the following scenarios:

- Watchdog is not running.
- If you do not configure an active directory and you start the **adclient** process, the CLI displays the following message:

  ```
  'adclient' is not configured, therefore will not be started.
  ```

- If you do not configure an active directory and you stop the **adclient** process, the CLI displays the following message:

  ```
  'adclient' is not configured. Attempting to stop it anyway.
  ```

- If you start a view-based ACS process on an ACS server that is not a log collector, the CLI displays the following error message:

  ```
  % Error: This is not a log collector node. Cannot start 'proc-name'.
  ```

Where *proc-name* refers to the specific view process that you attempted to start.

- If you stop a view-based ACS process on an ACS server that is not a log collector, the CLI displays the following message:

  ```
  This is not a log collector node. Attempting to stop 'proc-name' anyway.
  ```

Where *proc-name* refers to the specific view process that you attempted to stop.

Caution Use this command only when you need to troubleshoot the operations of an ACS node; otherwise, Cisco recommends that you maintain all of the ACS processes in running status, because ACS has high dependency on the ACS processes.

Examples

Example 1

```
acs/admin# acs start database

Starting database
acs/admin#
```

Example 2

```
acs/admin# acs stop database

Stopping database
acs/admin#
```

Related Commands

Command	Description
acs (instance)	Starts or stops an ACS instance.
show application	Shows application status and version information.

acs backup

To back up an ACS configuration (not including the ADE OS data), use the **acs backup** command in the EXEC mode.

acs backup *backup-filename* **repository** *repository-name*

Syntax Description

backup-filename	Name of the backup file. This can be a maximum of 100 alphanumeric characters.
repository	Repository command.
repository-name	Location where files should be backed up to. This can be a maximum of 30 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Performs a backup of ACS data and places the backup in a repository.

Note Before you use this command, you may want to create an NFS staging area as a temporary location to perform your backup packaging, because backing up data requires a lot of disk space. For more information, see **backup-staging-url, page 3-140**.

When you are using the **acs backup** command, the backup files include:

- Database—Database files include data related to ACS as well as the ADE OS. You can view backup files of the ADE-OS at:
  - /storedconfig
  - /storeddata
- Database password file—dbcred.cal, located at */opt/CSCOacs/db*.
- Certificate store—Located at */opt/CSCOacs/conf*.

You can access the */opt/CSCOacs/logs/acsbackup_instance.log* file for information about the last backup operation.

You can use the **show backup history** command to display the backup operations and determine whether they succeeded. If the backup fails, you may be able to use the **show logging** command (or the **show acs-logs** command if you are backing up ACS logs) to view troubleshooting information. Failures in the ACS aspect of the backup are clearly described on the terminal.

If you use this command on a secondary ACS, no backup occurs. You can use the ACS web interface to designate an ACS node to collect logs.

After you use this command, a time stamp is added to the end of the *backup-name* filename, to enable periodic backups. For more information, see acs restore, page 3-19.

Examples

```
acs/admin# acs backup mybackup repository myrepository
ACS backup file 'mybackup-081007-2055.tar.gpg' successfully copied to repository
'myrepository'
acs/admin#
```

Related Commands

Command	Description
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
backup-staging-url	Configures a Network File System (NFS) location that backup and restore operations will use as a staging area to package and unpackage backup files.
debug-log	Defines the local debug logging level for the ACS components.
delete	Deletes a file from the ACS server.
dir	Lists a file from the ACS server.
kron occurrence	Schedules one or more Command Scheduler commands to run at a specific date and time or a recurring level.
export-data	Exports configuration data from an ACS local store to a remote repository.
reload	Reboots the system.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
repository	Enters the repository submode for configuration of backups.
restore	Restores the file contents of a specific repository from the backup.
show acs-logs	Displays ACS server debug logs.
show backup history	Displays the backup history of the system.
show debug-adclient	Shows the debug log-level status for subsystems (enabled or disabled).
show repository	Displays the available backup files located on a specific repository.

acs-config

To enter the ACS Configuration mode, use the **acs-config** command in the EXEC mode.

acs-config

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines You must have privileges to enter ACS configuration mode, and you must supply the username and the 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.

It is recommended 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.

Up to six users can access the ACS Configuration mode at a time; six users equal six sessions. When one of the six sessions ends, you must wait up to five minutes for the session to be available to another user.

To leave the ACS Configuration mode, type **`exit`** or press **Ctrl-d**.

After you provide valid login credentials, ACS prompts you to change your password for any of the following reasons:

- Password expiration.
- Account inactivity.
- **acs reset-password** command run.
- Super administrator has selected **Change password on next login** for an admin account through GUI.

When ACS prompts you to change your password, enter your old password, then a new password (conforming to the password policy), and confirm your new password (repeat the new password that you specified).

If you fail to change your password when you are requested to, you cannot log in to ACS Configuration mode.

Examples

Example 1 – Success

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

Username: user1
Password:

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

Example 2 – Failure

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

This command requires ACS to be running.
Issue 'acs start' command and try again.

acs/admin
```

Example 3 – Failure

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

Username: user1
Password:

Authentication failed.

Username:
```

Example 4 – Failure

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

Username: acsadmin
Password:

Failed to login with the default password.
Use the web interface to modify the default password

acs/admin#
```

Example 5 – Success

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

Username: acsadmin
Password:

Administrator must change password.
Old password:
New password:
Confirm new password:

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

Example 6 – Failure

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

```
Username: acsadmin
Password:

Administrator must change password.
Old password:

Invalid value.

acs/admin#
```

Example 7 – Failure

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

Username: acsadmin
Password:

Administrator must change password.
Old password:
New password:
Confirm new password:

Cannot change password:
Password and confirm password must be the same

acs/admin#
```

Example 8 – Failure

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

Username: acsadmin
Password:

Administrator must change password.
Old password:
New password:
Confirm new password:

Cannot change password:
Value is out of range (4 - 32)

acs/admin#
```

If the new password does not conform with the password policy, ACS displays the password policy details as shown in the previous example.

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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.

Command	Description
acs restore	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
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.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs config-web-interface

To enable or disable an interface for ACS configuration web, use the **acs config-web-interface** command in the EXEC mode.

acs config-web-interface [**migration | ucp | view | rest**] {**enable | disable**}

Syntax Description

migration | ucp | view | rest	(Optional) Specify one of the interfaces, to enable or disable that specific interface alone.
enable	Enables the interface for ACS migration, password change, or Representational State Transfer (REST) services for the user.
disable	Disables the interface for ACS migration, password change, or REST services for the user.

Defaults

Enabled.

Command Modes

EXEC

Usage Guidelines

Enables or disables an interface to migrate the ACS database, change the user password, or use REST services through the CLI.

If you do not want to migrate your ACS database, change the user password or use REST services. Cisco recommends that you disable these interfaces.

Examples

Example 1

```
acs/admin# acs config-web-interface migration enable
acs/admin#
```

Example 2

```
acs/admin# acs config-web-interface [migration | ucp | view | rest] disable
acs/admin#
```

Related Commands

Command	Description
show acs-config-web-interface	Indicates whether the ACS configuration web interface is enabled or disabled.

acs delete core

To delete an ACS run-time core file or JVM core log, use the **acs delete core** command in the EXEC mode.

acs delete core {*filename*}

Syntax Description

filename	Name of the run-time core file or JVM core log. You can use up to 255 alphanumeric characters to specify the filename.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To view the list of available run-time core files and JVM core logs, use **show acs-cores** command.

Examples

Example 1

```
acs/admin# acs delete core xyz.log

% Error: Invalid core file 'xyz.log'
Use 'show acs-cores' to list the core files
acs/admin(config-acs)#
```

Example 2

```
acs/admin# acs delete core hs_err_pid12477.log

Core file 'hs_err_pid12477.log' deleted successfully
acs/admin
```

Related Commands

Command	Description
acs delete log	Deletes an ACS run-time core file or JVM core log excluding the latest one.
show acs-logs	Displays ACS server debug logs.
show acs-cores	Displays ACS run-time core files and JVM core logs.

acs delete log

To delete an ACS run-time core file or JVM core log excluding the latest one, use the **acs delete log** command in the EXEC mode.

acs delete log {*filename*}

Syntax Description

filename	Name of the run-time core file or JVM core log. You can use up to 255 alphanumeric characters to specify the filename.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To view the list of available run-time core files and JVM core logs, use the **show acs-cores** command. To delete the latest run-time core file or JVM core log, use the **acs delete core** command.

Examples

Example 1

```
acs/admin# acs delete log  xyz.log

% Error: Invalid log file 'xyz.log'
Use 'show acs-logs' to list the log files
acs/admin
```

Example 2

```
acs/admin# acs delete log catalina.out

% Error: most recent log files cannot be deleted, only older logs.
acs/admin
```

Example 3

```
acs/admin# acs delete log catalina.2008-12-10.log

Log file 'catalina.2008-12-10.log' deleted successfully
acs/admin
```

Related Commands

Command	Description
acs delete core	Deletes an ACS run-time core file or JVM core log.
show acs-logs	Displays ACS server debug logs.
show acs-cores	Displays ACS run-time core files and JVM core logs.

acs patch

To install and remove ACS patches, use the **acs patch** command in the EXEC mode.

acs patch {**install** | **remove**} *patch-name*.**tar.gpg repository** *repository-name*

Syntax Description

install	Install command.
remove	Remove command.
patch-name.tar.gpg	Name of the patch, which always has the .tar.gpg filename extension.
repository	Repository command.
repository-name	Location where files should installed from or removed to. This can be a maximum of 30 alphanumeric characters.

Defaults

Patch installations and removals are logged to */opt/CSCOacs/logs/acsupgrade.log*.

Command Modes

EXEC

Usage Guidelines

ACS patches contain small fixes that include isolated files, not a full version of the ACS software. ACS patch installations and removals require that you restart ACS.

Examples

Example 1

```
acs/admin# acs patch install acspatch.tar.gpg repository myrepository
Installing an ACS patch requires a restart of ACS services.
Would you like to continue? Y/N
```

Example 2

```
acs/admin# acs patch remove acspatch
Removing an ACS patch requires a restart of ACS services.
Would you like to continue? Y/N
```

Related Commands

Command	Description
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs reset-config

To reset the ACS configuration to factory defaults, use the **acs reset-config** command in the EXEC mode.

acs reset-config

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you use the **acs reset-config** command to reset your ACS to the factory default configuration, any configurations you have performed are lost; however, the appliance settings (such as network settings and backup repositories) are not affected.

ACS does not need to be running when you use this command.

Examples

```
acs/admin# acs reset-config
This command will reset the ACS configuration.
Would you like to continue? Y/N
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
acs patch	Installs and removes ACS patches.
acs reset-password	Resets the ‘acsadmin’ administrator password to the default setting.
acs restore	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
application reset-config	Resets an application configuration to factory defaults.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
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.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.

Command	Description
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs reset-password

To reset the 'acsadmin' administrator password to the default setting, use the **acs reset-password** command in the EXEC mode.

acs reset-password

Syntax Description

No arguments or keywords.

Defaults

This command resets the ACS administrator 'acsadmin' password to the default setting (**default**). Resetting this password does not affect other ACS administrators.

Command Modes

EXEC

Usage Guidelines

You cannot use this command on a secondary ACS node.

After you use this command, you must access your primary ACS node via the web interface and change the password. If you use the default password for the web interface (**default**) to access the ACS Configuration mode (which requires you to provide the web interface username and password), the login fails and the system prompts you to change the default password.

Examples

```
acs/admin# acs reset-password
This command resets the 'ACSAdmin' password to its original value.
Are you sure you want to continue?  (yes/no) y
Password was reset successfully
acs/admin#
```

Related Commands

Command	Description
acs (instance)	Starts or stops an ACS instance.
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
acs patch	Installs and removes ACS patches.
acs reset-config	Resets the ACS configuration to factory defaults.
acs restore	Performs a restoration of an ACS configuration.

Command	Description
acs support	Gathers information for ACS troubleshooting.
backup	Backs up the system (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
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.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs restore

To restore an ACS configuration (not including the ADE OS data) from one ACS node to another, use the **acs restore** command in the EXEC mode.

acs restore *backup-file-name* **repository** *repository-name*

Syntax Description

backup-file-name	Name of backup file. This can be a maximum of 100 alphanumeric characters. A time stamp in the format -*yymmdd-hhMM*.tar.gpg is added to the backup filename to generate a unique backup filename, where: • yy—Two-digit representation of the year (the last two digits). • mm—Two-digit representation of the month. Single-digit months are preceded by zero (0). • dd—Two-digit representation of the day of the month. Single digit months are preceded by zero (0). • hh—Two-digit representation of the hour of the day of a 24-hour clock. Single-digit hours are preceded by zero (0). • MM—Two-digit representation of the minute of the hour. Single-digit minutes are preceded by zero (0). For example, if you type **`dailyBackup`** as the filename, the resulting file may be named dailyBackup-080229-2335.tar.gpg.
repository	Repository command.
repository-name	Location where files should be restored from. This can be a maximum of 30 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Restores an ACS configuration from one ACS node to another. The restoration is performed from a temporary directory (the repository).

If you are restoring an primary ACS node configuration to a secondary, you must configure the secondary to local mode before you use this command (deregister from the primary node).

Caution The **acs restore** command causes ACS to restart.

If you are restoring the backup file on a node that was part of the ACS deployment when the backup was performed, ACS replaces the database. This includes:

- Old certificates and certificate requests, if any exist
- Database password file
- Viewer database

The prikeypwd.key is not included, because this file can be associated only with the private keys of the original ACS primary node.

Note In ACS 5.4, the ACS database does not contain the prikeypwd.key; it is available only in the file system.

You need not restore the backup file on a node that was *not* part of the deployment when the backup was performed, as the new ACS node might not have any local certificates to associate with.

After a restoration is complete, you must use the ACS web interface to designate an ACS node as a log collector.

Examples

```
acs/admin# acs restore mybackup-080229-2335.tar.gpg repository myrepository
Restore requires a restart of ACS services. Continue?  (yes/no)
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
backup-staging-url	Configures a Network File System (NFS) location that backup and restore operations use as a staging area to package and unpackage backup files.
debug-log	Defines the local debug logging level for the ACS components.
delete	Deletes a file from the ACS server.
dir	Lists a file in the ACS server.
export-data	Exports configuration data from an ACS local store to a remote repository.
reload	Reboots the system.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
repository	Enters the repository submode for configuration of backups.
restore	Restores the file contents of a specific repository from the backup.
show acs-logs	Displays ACS server debug logs.
show backup history	Displays the backup history of the system.
show debug-adclient	Shows the debug log-level status for subsystems (enabled or disabled).
show repository	Displays the available backup files located on a specific repository.

acs support

To gather information for ACS troubleshooting, use the **acs support** command in the EXEC mode.

acs support *filename* **repository** *repository-name* **encryption-passphrase** <*password*>
[**description** {*"text"*}] [**include-cores** {*number-days*}] [**include-db** {**original** | **secure**}]
[**include-debug-logs** {*number-logs*}] [**include-local-logs** {*number-logs*}]
[**include-system-logs** {*number-logs*}] [**include-logs** {*number-days*} {**all-categories** |
log-categories [**aaa-accounting** | **aaa-audit** | **aaa-diagnostics** | **administrative-audit** |
system-diagnostics]}]

Syntax Description

filename	The filename (up to 100 characters) of the support file; ACS stores the file in the format *filename*.tar.gz to the repository.
repository	Repository command.
repository-name	Location where files should be restored from. This can be a maximum of 30 alphanumeric characters.
encryption-passphrase	Encryption command to encrypt the support bundle.
password	Password to dycrypt the support bundle.
description	Description command.
"text"	Text, between quotation marks, which is saved in a readme.txt file that is included in the ACS support bundle.
include-cores	Includes core files in the ACS support bundle.

number-older-days	Includes core files in the ACS support bundle that are older than the number of days that you specify with this argument. By default, or if you specify 0, the core files are not included. Specify a value between 0 and 365.
include-db	Includes the ACS database in the ACS support bundle.
Original	Includes all the data from the ACS database.
Secure	Includes the data from the ACS database excluding any sensitive information.
include-debug-logs	Includes debug log files in the ACS support bundle.
number-logs	Includes the number of recent debug log files in the ACS support bundle of ACS management and runtime subsystems and the ACS Viewer that you specify with this argument. For example, if you specify 1, the most recent logs are included. Specify a value between 0 and 999.
include-local-logs	Includes logs that a customer can view via the CLI or the ACS web interface in the ACS support bundle.
number-logs	Includes the number of log files in the ACS support bundle that you specify with this argument. By default, logs are not included. Specify a value between 0 and 999.
include-system-logs	Includes recent system logs in the ACS support bundle.
number-logs	Includes the number of recent system log files from each node in the ACS support bundle that you specify with this argument. By default, or if you specify 0, the core files are not included. Specify a value between 0 and 365.
include-logs	Includes logs from the Viewer database in the ACS support bundle.
number-recent-days	Includes Viewer database logs of the most recent number of days that you specify with this argument in the ACS support bundle. Specify a value between 0 and 365. If you specify 0, no logs are included.
all-categories	Includes messages from all logging categories in the ACS support bundle.
log-categories	Includes messages from a subset of logging categories in the ACS support bundle.
aaa-accounting	Includes messages from the AAA accounting logging category in the ACS support bundle.
aaa-audit	Includes messages from the AAA audit logging category in the ACS support bundle.
aaa-diagnostics	Includes messages from the AAA diagnostic logging category in the ACS support bundle.
administrative-audit	Includes messages from the administrative audit logging category in the ACS support bundle.
system-diagnostics	Includes messages from the system diagnostics logging category in the ACS support bundle.

Defaults

The command generates a tar.gz file, which can contain the following components:

- ACS (non-sensitive data) and Viewer (as text) configuration data.
- All core files, if any exist.
- The output of **show version, show udi, show tech-support, show running-config,** and **show startup-config** commands.

- The log files, as you specify in your command structure.
- The monitoring and reporting logs, if any exist.
- The most recent copy of system logs from each node.
- A readme.txt file.
- The encrypted support bundle with .tar.gpg as the file extension (if you have used the **encryption-passphrase** command)

Command Modes

EXEC

Usage Guidelines

Note Before you use this command, you may want to create an Network File System (NFS) staging area as a temporary location to perform your backup packaging, because backing up data requires a lot of disk space. For more information, see **backup-staging-url, page 3-140**.

You are prompted for a username and password that can access the remote location.

ACS 5.4 encrypts the support bundle if the **encryption-passphrase** command is used. You can decrypt the support bundle outside the ACS 5.4 machine, using the password provided.

To decrypt the support bundle outside the ACS 5.4 machine, you should have a decrypter program that can decrypt the .gpg files, for example, the GnuPG program. If you do not want to encrypt the support bundle, you can enter the password value as *null*.

Possible errors are standard FTP and SCP error messages.

Table 3-4 Protocol Prefix Keywords

Keyword	Source of Destination
ftp	Source or destination URL for FTP network server. The syntax for this alias: **ftp:**[[[*//username* [**:***password*]@]*location*]*/directory*]*/filename*
scp	Source or destination URL for SCP network server. The syntax for this alias: **scp:**[[[*//username* [**:***password*]@]*location*]*/directory*]*/filename*
sftp[1]	Source or destination URL for an SFTP network server. The syntax for this alias: **sftp:**[[*//location*]*/directory*]*/filename*
tftp[1]	Source or destination URL for a TFTP network server. The syntax for this alias: **tftp:**[[*//location*]*/directory*]*/filename*

1. Not available for ACS file transfers.

Examples

```
acs/admin# acs support file01 repository myrepository encryption-passphrase xyz
description "files to bundle for assistance" include-cores 3 include-db secure
include-debug-logs 10 include-local-logs 5 include-system-logs 1 include-logs 7
log-categories aaa-audit administrative-audit
Collecting support information ...(file01.tar.gz)
ACS support file 'file01.tar.gz' successfully copied to repository 'myrepository'
acs/admin#
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
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.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

acs troubleshoot adcheck

To test the AD configuration and chek for compatability with the AD Agent, use the **acs troubleshoot adcheck** command in the EXEC mode. This also scans ACS for possible AD issues that may impair proper functionality.

acs troubleshoot adcheck {*parameter*}

Syntax Description

parameter	Enter a parameter from the list of parameters that are available, to check the connection or the compatability of ACS with the AD Agent.

Defaults

No default behavior or values

Command Modes

EXEC

Usage Guidelines

When you enter this command, ACS prompts you for a confirmation, and this message is displayed:

```
This command is only for advanced troubleshooting and may incur a lot of network traffic
```

```
Do you want to continue?  (yes/no)
```

You need to enter **yes** to continue. If you enter **no**, ACS stops executing the command.

Table 3-5 lists all the parameters that are used with the **adcheck** command and its description.

Table 3-5 adcheck Parameters

Parameter	Description
-s <*domain controller*>	Connects to a specified domain controller while doing network diagnostics. This option suppresses -a, -S, and -b, if it is combined with them.
-a	Forces scan of all domain controllers. This option suppresses -S and -b, if it is combined with them.
-S	Forces scan of all domain controllers in the first detected site. This option suppresses -b if both are specified.
-b <*n*>	The scan stops if the specified number of domain controllers are reached. The default is 10.
-x <*filename*>	Writes output in XML format. -x - writes xml to standard output.
-m <*path*>	The directory in which adcheck creates temporary files during check. You need to set execute permission on this directory, otherwise adcheck fails to run. The default is /tmp.
-t <*os* | *net* | *ad*>	Runs a subset of tests; multiple subsets can be specified as -t os, -t net, and -t ad. ad and net require the domain to be specified, while os does not.
-T	Specifies the DNS marginal threshold time. The default is 0.1 second.
-X	Checks the trusts.
-u	The user name. If the username is not specified, ACS looks for a Kerberos credential cache for the current user. If none is found, then it uses “Administrator”.
-p	Password for user. ACS prompts for a password if the password is not set already.
-P	Displays a warning message if there is only one domain controller for a domain.
-V	May be combined with the above options. Sends diagnostics to stderr and keeps the temp directory that is created by adcheck.
-v	Shows version information.
-h	Shows the help text.

Examples

```
acs/admin# acs troubleshoot adcheck -v
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no) yes
adcheck (CentrifyDC 4.5.0-357)
```

Related Commands

Command	Description
acs troubleshoot adinfo	Retrieves the information from AD regarding join settings, status, domain users, and domain controllers.
acs troubleshoot ldapsearch	Performs an LDAP search.

acs troubleshoot adinfo

To retrive the AD join settings and status, use the **acs troubleshoot adinfo** command in the EXEC mode. This also can be used to retrieve detailed information regarding the domain, users, and domain controllers.

acs troubleshoot adinfo {*parameter*}

Syntax Description

parameter	Enter a parameter from the list of parameters that are available. to display the join settings and the AD status.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you enter this command, ACS prompts you for a confirmation, and the following message is displayed:

```
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no)
```

You need to enter **yes** to continue. If you enter **no**, ACS stops executing the command.

Table 3-6 adinfo Parameters

Parameter	Description
-a	Shows current join settings and status. It shows the default option if the settings and status are not available.
-s [*domain*]	Shows detailed network information for the specified domain. It uses the domain to which ACS is joined, if you do not specify the domain along with the command.
-s <*user*>	Identifies Active Directory users who can read the computer account data.
-p <*password*>	Supplies a password for the user. If the password is not already set, then it prompts you for the password.
-d	Shows only the joined domain name.
-G	Shows only the connected global catalog.
-z	Shows only the joined zone name.
-Z	Shows only the domain name of the joined zone.
-s	Shows only the joined site name.
-r	Shows only the domain controller.
-n	Shows only the joined -as name.
-c	Shows parsed contents of the centrifydc.conf file.

Table 3-6 adinfo Parameters (continued)

Parameter	Description
-C	Shows the computer diagnostics, which include tthe Keberos key version and Service Principle Names (SPNs).
-t [*domain*]	Produces output for Centrify technical support for the specified domain. It uses the joined domain if the domain is not specified. A compressed file is created that includes the support for output, log file, gp report, centrifydc folder contents, and additional paths. The Support output goes to the */tmp/adinfo_support.txt* path. However, you can redirect the output using the parameter -o.
-D	Collects the cache and Network Information Service (NIS) map files for analysis. A compressed file is created that includes all the files that are collected.
-o <*filename*>	Sends the output from the -support to a different file. If you add the '-', then the output goes to the stdout file.
-P <*paths*>	Specifies the additional paths for --support.
-m	Shows the Centrify Direct Control running mode.
-A [*domain*]	Validates the user and the password against a given domain. A username must be specified via the --user option. It uses the domain to which ACS is joined, if you do not specify the domain along with the command.
-N [*domain*]	Validates the NT LAN Manager (NTLM) user and password against a given NTLM domain. A username must be specified via the --user option. It uses the domain to which ACS is joined, if you do not specify the domain along with the command.
-s <domain controller>	Connects to a specified domain controller while doing network diagnostics.
-T [*domain*]	Tests the state of the ports that were used by CDC.
-j	Returns the count of the number of machines that are joined to each zone.
-y <*all|dns,domain, netstate,adagent, config*>	Shows the current system information. You can specify multiple modules, separated by commas. The modules are: • all—Show all system information • dns—Show dns cache contents • domain—Show domain information • netstate—Show network states • adagent—Show adagent internal information • config—Show the in-memory configuration parameters of the adclient.
-V	Sends the diagnostics to stderr when you combine this option with the above options.
-v	Shows version information.
-h	Shows the help text.

Examples

Example 1

```
acs/admin# acs troubleshoot adinfo -v
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no) yes
adcheck (CentrifyDC 4.5.0-357)
```

Example 2

```
acs/admin# acs troubleshoot adinfo -ynetstate
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no) yes
System Diagnostic
  Not joined to any domain
```

Example 3

```
acs/admin# acs troubleshoot adinfo -a
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no) yes
Not joined to any domain
Licensed Features: Enabled
```

Related Commands

Command	Description
acs troubleshoot adcheck	Tests the AD configuration and the compatibility with the AD agent.
acs troubleshoot ldapsearch	Performs an LDAP search.

acs troubleshoot ldapsearch

To perform an LDAP search in AD, use the **acs troubleshoot ldapsearch** command in the EXEC mode.

acs troubleshoot ldapsearch {*parameter*}

Syntax Description

parameter	Enter a parameter from the list of parameters that are available to perform an LDAP search in AD.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you enter this command, ACS prompts you for a confirmation, and the following message is displayed.

```
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no)
```

You need to enter **yes** to continue. If you enter **no**, ACS stops executing the command.

Table 3-7 adcheck Parameter

Parameter	Description
Search Options	
-a deref	One of never (default), always, search, or find.

Table 3-7 adcheck Parameter (continued)

Parameter	Description
-A	Retrieves attribute name only (no values).
-b basedn	Base DN for search.
-E [!]<ext>	<extparam>] search extensions (! indicates criticality) [!]domainScope (domain scope) [!]mv=<filter> (matched values filter) [!]pr=[<size>[/prompt|noprompt]|disable] (default is pr=100|noprompt) [!]subentries[=true|false] (subentries) [!]sync=ro[/<cookie>] (LDAP Sync refreshOnly) rp[/<cookie>][/<slimit>] (LDAP Sync refreshAndPersist)
-F prefix	URL prefix for files (default: file:///tmp/)
-l limit	Searches using the time limits that are provided (in seconds, or "none" or "max").
-L	Prints the responses in LDAP Directory Interchange Format Version 1 (LDIFv1) format.
-LL	Prints the responses in LDIF format without comments.
-LLL	Prints the responses in LDIF format without comments and versions.
-r	Disables line wrap when printing out LDIF entries.
-s scope	One of the base, one, or sub. (search scope).
-S attr	Sorts the results using the given attribute.
-t	Writes binary values to files in the temporary directory.
-tt	Writes all values to files in the temporary directory.
-T path	Writes the file to the directory that is specified by the given path. If the path is not provided, then it writes the file into the default path. The default path is /tmp.
-u	Includes the user-friendly entry names in the output.
-z limit	Limits the size of entries while performing the search.
Common Options	
-C	Does the chase referrals.
-d level	Sets LDAP debugging level to the given level.
-D binddn	Binds the DN.
-e [!]<ext>	[=<extparam>] general extensions (! indicates criticality) [!]assert=<filter> (an RFC 2254 Filter) [!]authzid=<authzid> ("dn:<dn>" or "u:<user>") [!]manageDSAit [!]noop [!]postread[=<attrs>] (a comma-separated attribute list) [!]preread[=<attrs>] (a comma-separated attribute list)
-f file	Reads the operations from the given file.

Table 3-7 adcheck Parameter (continued)

Parameter	Description
-h host	LDAP server.
-H URI	LDAP Uniform Resource Indentifier(s).
-k	Uses Kerberos authentication.
-K	Is similar to the parameter -k, but goes only to step 1 of the Kerberos bind.
-m	Uses the machine credentials. Access to krb5.keytab and typically root permission is required.
-M	Enables the Manage DSA IT control (-MM to make critical).
-n	Shows what would be done, but does not actually perform the action.
-O props	Simple Authentication and Security Layer (SASL) security properties.
-o <opt>[=<optparam>] general options	apitimeout=<timeout> (in seconds, or "none" or "max", default:15s) Timeout value for synchronous OPENLDAP API call nettimeout=<timeout> (in seconds, or "none" or "max", default:15s) Network timeout value for ldap_pvt_connect.
-p port	Port on LDAP server.
-P version	Searches for the procotol version (default: 3).
-Q	Uses SASL Quiet mode.
R realm	SASL realm.
-v	Runs in verbose mode (diagnostics to standard output).
-V	Prints the version info.
-w passwd	Binds the password (for simple authentication).
-W	Prompts for the bind password.
-x	Simple authentication.
-y file	Reads password from file.
-Y mech	SASL mechanism (Only (Generic Security Services Application Programming Interface (GSSAPI) is supported).
-Z	Starts a Transport Layer Security (TLS) request (use -ZZ to require a successful response)

Examples

```
acs/admin# acs troubleshoot ldapsearch -V
This command is only for advanced troubleshooting and may incur a lot of network traffic
Do you want to continue?  (yes/no) yes
ldapsearch: @(#) $OpenLDAP: ldapsearch 2.2.26 (May 21 2012 18:10:23) $
        Centrify DirectControl 4.5.0
        (LDAP library: OpenLDAP 20226)
ldap_sasl_interactive_bind_s: Can't contact LDAP server (-1)
```

Related Commands

Command	Description
acs troubleshoot adcheck	Tests the AD configuration and compatibility with the AD Agent.
acs troubleshoot adinfo	Retrieves the information from the AD regarding join settings, status, domain users, and domain controllers.

acs zeroize-machine

Use the **acs zeroize-machine** command in the EXEC mode to trigger the zeroization and delete key and sensitive files, the running memory and, the swap files. This command securely deletes the partition on which ACS is installed.

It also securely deletes the swap partition and restarts the machine to clear all information in the RAM. After execution of the command is complete, ACS will no longer function on the appliance. You have to reinstall ACS on the appliance.

acs zeroize-machine

Syntax Description

No arguments or keywords.

Defaults

None.

Command Modes

EXEC mode

Usage Guidelines

When you enter this command, ACS will prompt you for confirmation for three times before running the command. The command performs the following steps:

1. Stops ACS processes so that the device is not busy and secure deletion happens.
2. Deletes the following devices:
   - /dev/smosvg/home
   - /dev/smosvg/localdiskvol
   - /dev/smosvg/optvol
   - /dev/smosvg/recvol
   - /dev/smosvg/storeddatavol
   - /dev/smosvg/tmpvol
   - /dev/smosvg/swapvol

   The optvol is the partition on which ACS is installed and all the sensitive information in ACS is stored here. The swap is maintained in swapvol.
3. Scans each partition type internally, using the fstab file.
4. Turns off the journaling, otherwise data zeroization might not happen.
5. Overwrites each partition twice with random bytes and zeroes at the end.
6. Restarts the machine to delete the RAM content.

It is recommended not to use the ACS machine after you run this command.

Examples

```
cd-acs5-13-50/admin# acs zeroize-machine
This command performs key zeroization of the ACS machine

Warning: This operation is irreversible - it completely deletes the ACS machine!

Are you sure you want to perform key zeroization now?  (yes/no)
Please enter 'yes' or 'no'
Are you sure you want to perform key zeroization now?  (yes/no) yes
Are you absolutely sure you want to perform key zeroization now?  (yes/no) no
```

application install

To install a specific application, use the **application install** command in the EXEC mode. To remove this function, use the **application remove** command.

application install *application-bundle remote-repository-name*

Syntax Description

install	Installs a specific application.
application-bundle	Application bundle filename. This can be a maximum of 255 alphanumeric characters.
remote-repository-name	Remote repository name. This can be a maximum of 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Installs the specified application bundle on the appliance. The application bundle file is pulled from the specified repository.

If you run the **application install** or **application remove** command when another installation or removal operation of an application is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress.  Try again shortly.
```

The ACS machine will be rebooted automatically soon after the installation gets completed.

Examples

```
acs/admin# application install acs.tar.gz myremoterepository

Do you want to save the current configuration ? (yes/no) [yes] ?
Generating configuration...
Saved the running configuration to startup successfully
acs/admin#
```

Related Commands

Command	Description
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

application remove

To remove a specific application, use the **application remove** command in the EXEC mode. To remove this function, use the **no** form of this command.

application remove *application-name*

Syntax Description

remove	Removes or uninstalls an application.
application-name	Application name. This can be a maximum of 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Removes or uninstalls an application.

Examples

```
acs/admin# application remove acs
acs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application start	Starts or enables an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

application reset-config

To reset an application configuration to factory defaults, use the **application reset-config** command in the EXEC mode.

application reset-config *application-name*

Syntax Description

application-name	Name of the application to reset its configuration to factory defaults. Up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

You can use the **application reset-config** command to reset the ACS configuration to factory defaults without reimaging the ACS appliance or VM.

Examples

```
acs/admin# application reset-config acs

Application successfully reset configuration
acs/admin#
```

Related Commands

Command	Description
acs reset-config	Resets the ACS configuration to factory defaults.

application start

To enable a specific application, use the **application start** command in the EXEC mode. To remove this function, use the **no** form of this command.

application start *application-name*

Syntax Description

start	Enables an application bundle.
application-name	Name of the predefined application that you want to enable. This can be a maximum of 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes EXEC

Usage Guidelines Enables an application.

You cannot use this command to start ACS.

Examples

```
acs/admin# application start acs
acs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

application stop

To disable a specific application, use the **application stop** command in the EXEC mode. To remove this function, use the **no** form of this command.

application stop *application-name*

Syntax Description

stop	Disables an application.
application-name	Name of the predefined application that you want to disable. This can be a maximum of 255 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Disables an application.

You cannot use this command to stop ACS.

Examples

```
acs/admin# application stop acs
acs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
show application	Shows application information for the installed application packages on the system.

application upgrade

To upgrade a specific application bundle, use the **application upgrade** command in the EXEC mode. To remove this function, use the **application remove** command.

application upgrade *application-bundle remote-repository-name*

Syntax Description

upgrade	Upgrades a specific application bundle.
application-bundle	Application name. Up to 255 alphanumeric characters.
remote-repository-name	Remote repository name. Up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC.

Usage Guidelines

Upgrades an application bundle, preserving any application configuration data.

If you issue the **application upgrade** command when another application upgrade operation is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress. Try again shortly.
```

Note The ACS appliance is rebooted during the application upgrade process.

Note You can use the application upgrade command to upgrade from ACS 5.1 or 5.2 patch releases to ACS 5.4. You can perform an ACS upgrade only on a standalone machine. To learn more about the upgrade process, refer *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*.

backup

To perform a backup (including the ADE OS data like hostname, IP address) and place the backup in a repository, use the **backup** command in the EXEC mode.

backup *backup-name* **repository** *repository-name*

Syntax Description

backup-name	Name of backup file. This can be a maximum of 100 alphanumeric characters.
repository	Repository command.
repository-name	Location where the files should be backed up to. This can be a maximum of 30 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Performs a backup of ACS data and places the backup in a repository.

When you are using this command for ACS, the backup files include:

- Database—Database files include data related to ACS.
- Database password file—dbcred.cal, located at /opt/CSCOacs/conf.
- Certificate store—Located at /opt/CSCOacs/conf.
- Viewer database—If the ACS node you are backing up has Viewer enabled.

You can use the **show backup history** command to display the backup operations and determine whether they succeeded.

If the backup fails, you may be able to use the **show logging** command (or the **show acs-logs** command if you are backing up ACS logs) to view troubleshooting information. Failures in the ACS aspect of the backup are clearly described in messages that are displayed on the terminal.

Examples

```
acs/admin# backup mybackup repository myrepository
% Creating backup with timestamped filename: myback2-081007-2129.tar.gpg
acs/admin#
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
acs patch	Installs and removes ACS patches.

Command	Description
acs reset-config	Resets the ACS configuration to factory defaults.
acs reset-password	Resets the 'acsadmin' administrator password to the default setting.
acs restore	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
debug-log	Defines the local debug logging level for the ACS components.
delete	Deletes a file from the ACS server.
dir	Lists a file from the ACS server.
export-data	Exports configuration data from an ACS local store to a remote repository.
reload	Reboots the system.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
repository	Enters the repository submode for configuration of backups.
restore	Restores the file contents of a specific repository from the backup.
show acs-logs	Displays ACS server debug logs.
show backup history	Displays the backup history of the system.
show debug-adclient	Shows the debug log-level status for subsystems (enabled or disabled).
show repository	Displays the available backup files located on a specific repository.

backup-logs

To back up system logs, use the **backup-logs** command in the EXEC mode. To remove this function, use the **no** form of this command.

backup-logs *backup-name* **repository** *repository-name*

Syntax Description

backup-name	Name of one or more files to back up. This can be a maximum of 100 alphanumeric characters.
repository	Repository command.
repository-name	Location where files should be backed up to. This can be a maximum of 30 alphanumeric characters.

Defaults

This command backs up these log files, which are located in specific directories:

- ACS server files located in the /var/log directory.
- ACS debug, audit, and diagnostic files located in the /opt/CSCSacs/logs directory.
- ACS Tomcat files located in the /opt/CSCOacs/mgmt/apache/<*version*>/logs directory, where <*version*> identifies the Tomcat version that you are running.

- ACS database files located in the /opt/CSCOacs/db directory.

Command Modes EXEC

Usage Guidelines Backs up system logs.

Examples

```
acs/admin# backup-logs mysyslogs repository myrepository
% Creating log backup with timestamped filename: mysyslogs-081007-2130.tar.gz
acs/admin#
```

Related Commands

Command	Description
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Restores the file contents of a specific repository from the backup.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

clock

To set the system clock, use the **clock** command in the EXEC mode. To remove this function, use the **no** form of this command.

clock {**set**} [*month day hh:min:ss yyyy*]

Syntax Description

set	Sets the system clock.
month	Current month of the year by name. This can be a maximum of three alphabetic characters. For example, Jan for January.
day	Current day (by date) of the month. Value = 0 to 31. Up to two numbers.
hh:mm:ss	Current time in hours (24-hour format), minutes, and seconds.
yyyy	Current year (no abbreviation).

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Sets the system clock. You must restart the ACS server to take effect of the changes after setting the clock.

Examples

```
acs/admin# clock set Jan 4 05:05:05 2007
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS ..................
Starting ACS ......................

acs/admin#
```

Related Commands

Command	Description
show clock	Displays the time and date set on the system software clock.

configure

To enter the Configuration mode, use the **configure** command in the EXEC mode. If using the **replace** option, this command copies a remote configuration to the system, overwriting the existing configuration.

configure {**terminal**}

Syntax Description

terminal	Runs configuration commands from the terminal.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use this command to enter the Configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them (press **Enter**).

To exit the Configuration mode and return to the EXEC mode, enter **end**, **exit**, or **Ctrl-z**.

To view the changes that you have made to the configuration, use the **show running-config** command in the EXEC mode.

Examples

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

Related Commands

Command	Description
show running-configuration	Displays the contents of the currently running configuration file or the configuration.
show startup-configuration	Displays the contents of the startup configuration file or the configuration.

copy

To copy any file from a source to a destination, use the **copy** command in the EXEC mode. The **copy** command in ACS copies a configuration (running or startup).

Running Configuration

The ACS active configuration stores itself in the ACS RAM. Every configuration command you enter resides in the running configuration. If you reboot your ACS server, you lose the configuration. If you make changes that you want to save, you must copy the running configuration to a safe location, such as a network server, or save it as the ACS server startup configuration.

Startup Configuration

You cannot edit a startup configuration directly. All commands that you enter store themselves in the running configuration, which you can copy into the startup configuration.

In other words, when you boot an ACS server, the startup configuration becomes the initial running configuration. As you modify the configuration, the two diverge:

- The startup configuration remains the same.
- The running configuration reflects the changes that you have made.

If you want to make your changes permanent, you must copy the running configuration to the startup configuration.

The following command lines show some of the **copy** command scenarios available:

copy running-configuration startup-configuration

Copies the running configuration to the startup configuration. Replaces the startup-configuration with the running configuration.

Note If you do not save the running configuration, you will lose all your configuration changes during the next reboot of the ACS server. Once you are satisfied that the current configuration is correct, copy your configuration to the startup configuration with the preceding command.

copy startup-configuration running-configuration

Copies the startup configuration to the running configuration. Merges the startup configuration on top of the running configuration.

copy [*protocol***://***hostname/location*] **startup-configuration**

Copies but does not merge a remote file to the startup configuration.

copy [*protocol*:*//hostname/location*] **running-configuration**

Copies and merges a remote file to the running configuration.

copy startup-configuration [*protocol*:*//hostname/location*]

Copies the startup configuration to a remote system.

copy running-configuration [*protocol*:*//hostname/location*]

Copies the running configuration to a remote system.

copy logs [*protocol*:*//hostname/location*]

Copies log files from the system to another location.

Note The **copy** command is supported only for the local disk and not for a repository.

Syntax Description

running-configuration	Represents the current running configuration file.
startup-configuration	Represents the configuration file used during initialization (startup).
protocol	See Table 3-4 for protocol keyword options.
hostname	Hostname of destination.
location	Location of destination.
logs	System log files.
acs-logs	ACS log files.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The fundamental function of the **copy** command allows you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file specified uses the ACS file system, through which you can specify any supported local or remote file location. The file system being used (a local memory source or a remote system) dictates the syntax used in the command.

You can enter on the command line all necessary source and destination information and the username and password to use, or you can enter the **copy** command and have the ACS server prompt you for any missing information.

Timesaver Aliases reduce the amount of typing that you need to do. For example, type **copy run start** (the abbreviated form of the **copy running-config startup-config** command).

The entire copying process might take several minutes and differs from protocol to protocol and from network to network.

Use the filename relative to the directory for file transfers.

Examples

Example 1

```
acs/admin# copy run start
Generating configuration...
acs/admin#
```

Example 2

```
acs/admin# copy logs ftp://host01/ldir01
```

Related Commands

Command	Description
acs (instance)	Starts or stops an ACS instance.
acs (process)	Starts or stops an ACS process.
acs-config	Enters the ACS Configuration mode.
acs reset-config	Resets the ACS configuration to factory defaults.
acs support	Gathers information for troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
debug-log	Defines the local debug logging level for the ACS components.
delete	Deletes a file from the ACS server.
dir	Lists a file from the ACS server.
export-data	Exports configuration data from an ACS local store to a remote repository.
reload	Reboots the system.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

debug

To display errors or events for command situations, use the **debug** command in the EXEC mode.

```
debug {all | application | backup-restore | cdp | | config | icmp | copy | locks |
    logging | snmp | system | transfer | user | utils}
```

Syntax Description

all	Enables all debugging.
application	Application files. • *all*—Enables all application debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *install*—Enables application install debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *operation*—Enables application operation debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *uninstall*—Enables application uninstall debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
backup-restore	Backs up and restores files. • *all*—Enables all debug output for backup-restore. Set level between 0 and 7 with 0 being severe and 7 being all. • *backup*—Enables backup debug output for backup-restore. Set level between 0 and 7 with 0 being severe and 7 being all. • *backup-logs*—Enables backup-logs debug output for backup-restore. Set level between 0 and 7 with 0 being severe and 7 being all. • *history*—Enables history debug output for backup-restore. Set level between 0 and 7 with 0 being severe and 7 being all. • *restore*—Enables restore debug output for backup-restore. Set level between 0 and 7 with 0 being severe and 7 being all.
cdp	CDP configuration files. • *all*—Enables all CDP configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *config*—Enables configuration debug output for CDP. Set level between 0 and 7 with 0 being severe and 7 being all. • *infra*—Enables infrastructure debug output for CDP. Set level between 0 and 7 with 0 being severe and 7 being all.

config	Configuration files. • *all*—Enables all configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *backup*—Enables backup configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *clock*—Enables clock configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *infra*—Enables configuration infrastructure debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *kron*—Enables command scheduler configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *network*—Enables network configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *repository*—Enables repository configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *service*—Enables service configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
copy	Copy commands. Set level between 0 and 7 with 0 being severe and 7 being all.
locks	Resource locking. • *all*—Enables all resource locking debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *file*—Enables file locking debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
logging	Logging configuration files. *all*—Enables all logging configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
snmp	SNMP configuration files. *all*—Enables all SNMP configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
system	System files. • *all*—Enables all system files debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *id*—Enables system ID debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *info*—Enables system info debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *init*—Enables system init debug output. Set level between 0 and 7 with 0 being severe and 7 being all.
transfer	File transfer. Set level between 0 and 7 with 0 being severe and 7 being all.

user	User management. • *all*—Enables all user management debug output. Set level between 0 and 7 with 0 being severe and 7 being all. • *password-policy*—Enables user management debug output for password-policy. Set level between 0 and 7 with 0 being severe and 7 being all.
utils	Utilities configuration files. *all*—Enables all utilities configuration debug output. Set level between 0 and 7 with 0 being severe and 7 being all.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **debug** command to identify various failures within the ACS server; for example, setup failures or configuration failures.

Examples

```
acs/admin# debug all
acs/admin# mkdir disk:/1
acs/admin# 6 [7178]: utils: vsh_root_stubs.c[2301]: mkdir operation success

acs/admin# rmdir disk:/1
acs/admin# 6 [7180]: utils: vsh_root_stubs.c[2171]: Invoked Remove Directory disk:/1
command 6 [7180]: utils: vsh_root_stubs.c[2228]: Remove Directory operation success

acs/admin# undebug all
acsvw-test8/admin# 7 [2826]: cdp:infra: ether-write.c[87]: WriteEther(): wrote len: 192
7 [2826]: cdp:infra: ether-write.c[112]: cdpd write succeed...
7 [2826]: cdp:infra: main.c[128]:
Writing with retransmissiontime 60...
```

Related Commands

Command	Description
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations.

delete

To delete a file from the ACS server, use the **delete** command in the EXEC mode. To remove this function, use the **no** form of this command.

delete *filename*

Syntax Description

filename	Filename. This can be a maximum of 80 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you attempt to delete the configuration file or image, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image, the system prompts you to confirm the deletion.

Examples

```
acs/admin# delete myfile
acs/admin#
```

Related Commands

Command	Description
dir	Lists all the files on the ACS server.

dir

To list a file from the ACS server, use the **dir** command in the EXEC mode. To remove this function, use the **no** form of this command.

dir [*word*] [**recursive**]

Syntax Description

word	Directory name. This can be a maximum of 80 alphanumeric characters. Requires **disk:/** preceding the directory name.
recursive	Lists a local directory or filename recursively.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# dir

Directory of disk:/

      16384  Jul 02 2008 08:34:49  lost+found/
       4096  Jul 16 2008 02:10:20  mytest/
       4096  Jul 11 2008 09:12:12  save-config/

           Usage for disk: filesystem
                  49741824 bytes total used
                6815842304 bytes free
                7233003520 bytes available
acs/admin#
```

Example 2

```
acs/admin# dir disk:/mytest

Directory of disk:/mytest

           Usage for disk: filesystem
                  49741824 bytes total used
                6815842304 bytes free
                7233003520 bytes available
acs/admin#
```

Example 3

```
acs/admin# dir recursive

Directory of disk:/

       4096  Jul 16 2008 02:10:20  mytest/
      16384  Jul 02 2008 08:34:49  lost+found/
       4096  Jul 11 2008 09:12:12  save-config/

Directory of disk:/mytest

No files in directory

Directory of disk:/lost+found

No files in directory

Directory of disk:/save-config

        555  Jul 11 2008 09:12:12  running-config

           Usage for disk: filesystem
                  49741824 bytes total used
                6815842304 bytes free
                7233003520 bytes available
```

Related Commands

Command	Description
delete	Deletes a file from the ACS server.

exit

To close an active terminal session by logging out of the ACS server or to move up one mode level from the Configuration mode, use the **exit** command in the EXEC mode.

exit

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use the **exit** command in EXEC mode to exit an active session (log out of the ACS server) or to move up from the Configuration mode.

Examples

```
acs/admin# exit
```

Related Commands

Command	Description
end	Exits the Configuration mode.
exit	Exits the Configuration mode or EXEC mode.
Ctrl-z	Exits the Configuration mode.

forceout

To force users out of an active terminal session by logging them out of the ACS server, use the **forceout** command in the EXEC mode.

forceout *username*

Syntax Description

username	Name of the user. This can be a maximum of 31 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use the **forceout** command in EXEC mode to force a user from an active session.

Examples

```
acs/admin# forceout user1
```

halt

To shut down and power off the system, use the **halt** command in EXEC mode.

```
halt
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Before you run the **halt** command, ensure that ACS is not performing any backup, restore, installation, upgrade, or remove operation. If you run the halt command while ACS is performing any of these operations, you will get one of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

If you get any of these warnings, enter **YES** to halt the operation, or enter **NO** to cancel the halt.

If no processes are running when you use the **halt** command or you enter **YES** in response to the warning message displayed, ACS asks you to respond to the following option:

```
Do you want to save the current configuration ?
```

Enter **YES** to save the existing ACS configuration. ACS displays the following message:

```
Saved the running configuration to startup successfully
```

Examples

```
acs/admin# halt
acs/admin#
```

Related Commands

Command	Description
reload	Reboots the system.

help

To describe the interactive help system for the ACS server, use the **help** command in the EXEC mode.

```
help
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

All configuration modes

Usage Guidelines

The **help** command provides a brief description of the context-sensitive help system. To:

- List all commands available for a particular command mode, enter a question mark (**?**) at the system prompt.
- Obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (**?**). This form of help is called word help, because it lists only the keywords or arguments that begin with the abbreviation that you entered.
- List the keywords and arguments associated with a command, enter a question mark (**?**) in place of a keyword or argument on the command line. This form of help is called command syntax help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments that you have already entered.

Examples

```
acs/admin# help
Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
acs/admin#
```

mkdir

To create a new directory on the ACS server, use the **mkdir** command in the EXEC mode.

mkdir *directory-name* [*disk:/path*]

Syntax Description

directory-name	Name of the directory to create. Use *disk:/path* with the directory name. This can be a maximum of 80 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use *disk:/path* with the directory name; otherwise, an error indicating that the *disk:/path* must be included appears.

Examples

```
acs/admin# mkdir disk:/test/
acs/admin# dir

Directory of disk:/

      16384  Jun 28 2007 00:09:50  lost+found/
       4096  Jun 28 2007 14:34:27  test/

           Usage for disk: filesystem
                  88150016 bytes total used
               44585803776 bytes free
               47064707072 bytes available

acs/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the ACS server.
rmdir	Removes an existing directory.

nslookup

To look up the hostname of a remote system and its services on the ACS server, use the **nslookup** command in the EXEC mode.

nslookup *word*

Syntax Description

word	IPv4 address or hostname of a remote system. This can be a maximum of 64 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# nslookup 1.2.3.4
Trying "4.3.2.1.in-addr.arpa"
Host 4.3.2.1.in-addr.arpa not found: 3(NXDOMAIN) Received 105 bytes from
209.165.200.225#53 in 5 ms
```

Example 2

```
acs/admin# nslookup 209.165.200.225
Trying "225.200.165.209.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15007 ;; flags: qr aa rd ra; QUERY: 1,
ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;225.200.165.209.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
225.200.165.209.in-addr.arpa. 86400 IN      PTR     ACS.cisco.com.

;; AUTHORITY SECTION:
165.209.in-addr.arpa.    86400   IN      NS      ns2.cisco.com.
165.209.in-addr.arpa.    86400   IN      NS      ns1.cisco.com.

;; ADDITIONAL SECTION:
ns1.cisco.com.          86400   IN      A       209.165.200.225
ns2.cisco.com.          86400   IN      A       209.165.200.225

Received 146 bytes from 172.69.2.133#53 in 5 ms
```

Example 3

```
acs149/admin# nslookup _finger._tcp.child1.apkacs-dev.com
```

```
Trying "_finger._tcp.child1.apkacs-dev.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34964
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;_finger._tcp.child1.apkacs-dev.com. IN ANY

;; ANSWER SECTION:
_finger._tcp.child1.apkacs-dev.com. 3600 IN SRV 0 0 79.
_finger._tcp.child1.apkacs-dev.com. 3600 IN SRV 10 0 79.

Received 90 bytes from 10.77.243.169#53 in 0 ms
acs/admin#
```

ping

To diagnose basic network connectivity to a remote system, use the **ping** command in the EXEC mode.

ping ip {*ipv4-address* | *hostname*}[**df** *df*] [**packetsize** *packetsize*] [**pingcount** *pingcount*]

ping ipv6 {*ipv6-address* | *hostname*} [**GigabitEthernet** *GigabitEthernet*] [**pingcount** *pingcount*]

Syntax Description

ipv4-address	IPv4 address of the system to ping. This can be a maximum of 32 alphanumeric characters.
ipv6-address	IPv6 address of the system to ping. This can be a maximum of 32 alphanumeric characters.
hostname	Hostname of the system to ping. This can be a maximum of 32 alphanumeric characters.
df	Specification for packet fragmentation.
df	Specify the value as **1** to prohibit packet fragmentation, or **2** to fragment the packets locally, or **3** to not set DF.
Packetsize	Size of the ping packet.
packetsize	Specify the size of the ping packet; the value can be between 0 and 65507.
Pingcount	Number of ping echo requests.
pingcount	Specify the number of ping echo requests; the value can be between 1 and 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

Examples

Example 1

```
acs/admin# ping 172.16.0.1 df 2 packetsize 10 pingcount 2
PING 172.16.0.1 (172.16.0.1) 10(38) bytes of data.
18 bytes from 172.16.0.1: icmp_seq=0 ttl=40 time=306 ms
18 bytes from 172.16.0.1: icmp_seq=1 ttl=40 time=300 ms

--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 300.302/303.557/306.812/3.255 ms, pipe 2
acs/admin#
```

Example 2

```
ACS143/admin# ping ip 10.56.24.191 df 2 packetsize 10 pingcount 2
PING 10.56.24.191 (10.56.24.191) 10(38) bytes of data.
18 bytes from 10.56.24.191: icmp_seq=0 ttl=43 time=259 ms
18 bytes from 10.56.24.191: icmp_seq=1 ttl=43 time=259 ms

--- 10.56.24.191 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 259.376/259.450/259.525/0.514 ms
acs/admin#
```

Example 3

```
ACS143/admin# ping ipv6 5abe::20c:29ff:feac:cbbe gigabitEthernet 0 packet size 10
pingcount 2
PING 5abe::20c:29ff:feac:cbbe (5abe::20c:29ff:feac:cbbe) from 5abe::bd1d:4b94:8884:27ca
etho 10 data bytes.
18 bytes from 5abe::20c:29ff:feac:cbbe: icmp_seq=0 ttl=64 time=3.41 ms
18 bytes from 5abe::20c:29ff:feac:cbbe: icmp_seq=1 ttl=64 time=0.856 ms

--- 5abe::20c:29ff:feac:cbbe ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.856/2.134/3.412/1.278 ms pipe 2
acs/admin#
```

reload

To reload the ACS operating system, use the **reload** command in the EXEC mode.

```
reload
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **reload** command halts the system. Use the command after you enter configuration information into a file and save it to the startup configuration.

Before you run the **reload** command, ensure that ACS is not performing any backup, restore, installation, upgrade, or remove operation. If ACS performs any of these operations and you try to run the **reload** command, you will see any of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with reload?

WARNING: An install/upgrade/remove is currently in progress! Continue with reload?
```

If you get any of these warnings, enter **YES** to halt the operation, or enter **NO** to cancel the halt.

If no processes are running when you use the **reload** command or you enter **YES** in response to the warning message displayed, ACS asks you to respond to the following option:

```
Do you want to save the current configuration ?
```

Enter **YES** to save the existing ACS configuration. ACS displays the following message:

```
Saved the running configuration to startup successfully
```

Examples

```
acs/admin# reload
Continue with reboot? [y/n] y

Broadcast message from root (pts/0) (Tue Oct  7 23:01:46 2008):

The system is going down for reboot NOW!

acs/admin#
```

Related Commands

Command	Description
halt	Disables the system.

restore

To perform a restore of a previous backup, use the **restore** command in the EXEC mode. A restore operation restores data related to ACS as well as the ADE OS. To remove this function, use the **no** form of this command.

restore *filename* **repository** *repository-name*

Syntax Description

filename	Name of the backed-up file that resides in the repository. This can be a maximum of 120 alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository-name	Name of the repository you want to restore from backup.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines When you use this command for ACS, the ACS server reboots automatically.

Examples

```
acs/admin# restore backup1.tar.gpg repository repository1
acs/admin#
```

Related Commands

Command	Description
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.

rmdir

To remove an existing directory, use the **rmdir** command in the EXEC mode.

rmdir *word*

Syntax Description

word	Directory name. This can be a maximum of 80 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
acs/admin# mkdir disk:/test/
acs/admin# dir
```

```
Directory of disk:/

      16384  Jun 28 2007 00:09:50  lost+found/
       4096  Jun 28 2007 14:34:27  test/

           Usage for disk: filesystem
                  88150016 bytes total used
               44585803776 bytes free
               47064707072 bytes available CAM/admin#
acs/admin# rmdir disk:/test
acs/admin# dir

Directory of disk:/

      16384  Jun 28 2007 00:09:50  lost+found/

           Usage for disk: filesystem
                  88145920 bytes total used
               44585807872 bytes free
               47064707072 bytes available CAM/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the ACS server.
mkdir	Creates a new directory.

show

To show the running system information, use the **show** command in the EXEC mode. For detailed information on all the ACS **show** commands, see Show Commands, page 3-70.

show *keyword*

Syntax Description

Table 3-8 provides a summary of the **show** commands.

Table 3-8 Summary of Show Commands

Command[1]	Description
application (requires keyword)[2]	Displays information about the installed application; for example, status or version.
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.
disks	Displays file-system information of the disks.

Table 3-8 Summary of Show Commands (continued)

Command[1]	Description
interface	Displays statistics for all the interfaces configured on the ADE OS 1.0.2 system.
logging (requires keyword)	Displays system logging information.
logins (requires keyword)	Displays login history.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP).
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 restore history on the ACS server.
running-config	Displays the contents of the currently running configuration file on the ACS server.
startup-config	Displays the contents of the startup configuration on the ACS server.
tech-support	Displays system and configuration information that you can provide to the Cisco Technical Assistance Center (TAC) when reporting a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the time zone of the ACS server.
timezones	Displays all the time zones available for use on the ACS server.
udi	Displays information about the system's Unique Device Identifier (UDI).
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information for currently logged in users.
ip route	Displays information for specific IP addresses, network masks or protocols.

1. The commands in this table require that the **show** command precedes a keyword; for example, **show application**.
2. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**. This **show** command displays the version of the application that is installed on the system (see show application, page 3-75).

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

All **show** commands require at least one keyword to function.

Examples

```
acs/admin# show application
<name>          <Description>
acs              Cisco ACS 5.4
acs/admin#
```

shutdown

To shut down an interface, use the **shutdown** command in the interface configuration mode. To disable this function, use the **no** form of this command.

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface Configuration

Usage Guidelines

When you shut down an interface using this command, you lose connectivity to the CSACS-1121 or Cisco SNS-3415 appliance through that interface (even though the appliance is still powered on). However, if you have configured the second interface on the appliance with a different IP and have not shut down that interface, you can access the appliance through that second interface.

To shut down an interface, you can also modify the ifcfg-eth[0,1] file, which is located at */etc/sysconfig/network-scripts,* using the ONBOOT parameter:

- Disable an interface, set ONBOOT="no"
- Enable an interface, set ONBOOT="yes"

You can also use the **no shutdown** command to enable an interface.

Examples

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

Related Commands

Command	Description
interface	Configures an interface type and enters the interface mode.
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.
show interface	Displays information about the system IP interfaces.
ip default-gateway	Sets the IP address of the default gateway of an interface.

ssh

To start an encrypted session with a remote system, use the **ssh** command in the EXEC mode.

Note An Admin or Operator (user) can use this command (see Table 1-1).

ssh <host *ip-address* | *hostname*> <*username*> **port** <*port number*> **version** <*version number*>

or

ssh delete host <host *ip-address* | *hostname*>

Syntax Description

ip-address	IP address of the remote system. This can be a maximum of 64 alphanumeric characters.
hostname	Hostname of the remote system. This can be a maximum of 64 alphanumeric characters.
username	Username of the user logging in through SSH.
port [*number*]	(Optional) Indicates the port number of the remote host. From 0 to 65,535. Default 22.
version [1 | 2]	(Optional) Indicates the version number. Default 2.
delete host	Deletes the SSH fingerprint of a specific host.
word	IPv4 address or hostname of a remote system. This can be a maximum of 64 alphanumeric characters.

Defaults

Disabled.

Command Modes

EXEC (Admin or Operator)

Usage Guidelines

The **ssh** command enables a system to make a secure, encrypted connection to another remote system or server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an insecure network.

Examples

Example 1

```
acs/admin# ssh delete host <ipaddress or hostname>
acs/admin#
```

Example 2

```
acs/admin# ssh acs2 admin
admin@acs2's password:
Last login: Wed Jul 11 05:53:20 2008 from ACS.cisco.com

acs2/admin#
```

tech

To dump a Transmission Control Protocol (TCP) package to the console, use the **tech** command in the EXEC mode.

tech {**dumptcp**} *gigabit-ethernet*

Syntax Description

dumptcp	Dumps TCP package to console.
gigabit-ethernet	Gigabit Ethernet interface number 0 to 1.

Defaults

Disabled.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# tech dumptcp 0
140816:141088(272) ack 1921 win 14144
08:26:12.034630 IP ACS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P
141088:141248(160) ack 1921 win 14144
08:26:12.034635 IP dhcp-64-102-82-153.cisco.com.2221 > ACS.cisco.com.ssh: . ack 139632 win
64656
08:26:12.034677 IP ACS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P
141248:141520(272) ack 1921 win 14144
08:26:12.034713 IP ACS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P
141520:141680(160) ack 1921 win 14144
08:26:12.034754 IP ACS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P
141680:141952(272) ack 1921 win 14144
08:26:12.034756 IP dhcp-64-102-82-153.cisco.com.2221 > ACS.cisco.com.ssh: . ack 140064 win
65520
08:26:12.034796 IP ACS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P
141952:142112(160) ack 1921 win 14144
1000 packets captured
1000 packets received by filter
0 packets dropped by kernel
acs/admin#
```

telnet

To log in to a host that supports Telnet, use the **telnet** command in Operator (user) or EXEC mode.

telnet [*ip-address* | *hostname*] **port** *number*

Syntax Description

ip-address	IP address of the remote system. Can be a maximum of 64 alphanumeric characters.
hostname	Hostname of the remote system. Can be a maximum of 64 alphanumeric characters.
port *number*	(Optional) Indicates the port number of the remote host. From 0 to 65,535.

Defaults

No default behavior or values.

Command Modes

Operator

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# telnet 172.16.0.11 port 23
ACS.cisco.com login: admin
password:
Last login: Mon Jul  2 08:45:24 on ttyS0
acs/admin#
```

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** command in the EXEC mode.

terminal length *integer*

Syntax Description

integer	Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output.

Defaults

24 lines

Command Modes

EXEC

Usage Guidelines The system uses the length value to determine when to pause during multiple-screen output.

Examples

```
acs/admin# terminal length 0
acs/admin#
```

terminal session-timeout

To set the inactivity timeout for all sessions, use the **terminal session-timeout** command in the EXEC mode.

terminal session-timeout *minutes*

Syntax Description

minutes	Sets the number of minutes for the inactivity timeout. From 0 to 525,600. Zero (0) disables the timeout.

Defaults 30 minutes

Command Modes EXEC

Usage Guidelines Setting the **terminal session-timeout** command to zero (0) results in no timeout being set.

Examples

```
acs/admin# terminal session-timeout 40
acs/admin#
```

Related Commands

Command	Description
terminal session-welcome	Sets a welcome message on the system for all users who log in to the system.

terminal session-welcome

To set a welcome message on the system for all users who log in to the system, use the **terminal session-welcome** command in EXEC mode.

terminal session-welcome *string*

Syntax Description

string	Welcome message. This can be a maximum of 2,048 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Specify a message using up to 2,048 characters.

Examples

```
acs/admin# terminal session-welcome Welcome
acs/admin#
```

Related Commands

Command	Description
terminal session-timeout	Sets the inactivity timeout for all sessions.

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** command in EXEC mode.

terminal terminal-type *type*

Syntax Description

type	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. This can be a maximum of 80 alphanumeric characters.

Defaults VT100

Command Modes EXEC

Usage Guidelines Indicate the terminal type if it is different from the default of VT100.

Examples

```
acs/admin# terminal terminal-type vt220
acs/admin#
```

traceroute

To discover the routes that packets take when traveling to their destination address, use the **traceroute** command in EXEC mode.

traceroute {ip | ipv6} [*ip-address* | *hostname*]

Syntax Description

ip-address	IP address of the remote system. This can be a maximum of 32 alphanumeric characters.
hostname	Hostname of the remote system. This can be a maximum of 32 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# traceroute 172.16.0.1
traceroute to 172.16.0.1 (172.16.0.1), 30 hops max, 38 byte packets
 1  172.16.0.1 0.067 ms  0.036 ms  0.032 ms
acs/admin#
```

Example 2

```
ACS143/admin# traceroute ip 10.77.243.152
traceroute to 10.77.243.152 (10.77.243.152), 30 hops max, 40 byte packets
 1 10.77.243.152 ms  2.661 ms 2.666 ms 2.661 ms
acs/admin#
```

Example 3

```
ACS143/admin# traceroute ipv6 5abe::20c:29ff:feac:cbbe
traceroute to 5abe::20c:29ff:feac:cbbe (5abe::20c:29ff:feac:cbbe), 30 hops max, 40 byte
packets
 1 5abe::20c:29ff:feac:cbbe  2.684 ms  2.681 ms  2.676 ms
acs/admin#
```

undebug

To disable debugging functions, use the undebug command in EXEC mode.

undebug {**all | application | backup-restore | cdp | config | copy | locks | logging | snmp | system | transfer | user | utils**} *level*

Syntax Description

all	Disables all debugging.
application	Application files. • *all*—Disables all application debug output. • *install*—Disables application install debug output. • *operation*—Disables application operation debug output. • *uninstall*—Disables application uninstall debug output.
backup-restore	Backs up and restores files. • *all*—Disables all debug output for backup-restore. • *backup*—Disables backup debug output for backup-restore. • *backup-logs*—Disables backup-logs debug output for backup-restore. • *history*—Disables history debug output for backup-restore. • *restore*—Disables restore debug output for backup-restore.
cdp	CDP configuration files. • *all*—Disables all CDP configuration debug output. • *config*—Disables configuration debug output for CDP. • *infra*—Disables infrastructure debug output for CDP.
config	Configuration files. • *all*—Disables all configuration debug output. • *backup*—Disables backup configuration debug output. • *clock*—Disables clock configuration debug output. • *infra*—Disables configuration infrastructure debug output. • *kron*—Disables command scheduler configuration debug output. • *network*—Disables network configuration debug output. • *repository*—Disables respository configuration debug output. • *service*—Disables service configuration debug output.
copy	Copy commands.
locks	Resource locking. • *all*—Disables all resource locking debug output. • *file*—Disables file locking debug output.
logging	Logging configuration files. *all*—Disables all debug output for logging configuration.

snmp	SNMP configuration files. *all*—Disables all debug output for SNMP configuration.
system	System files. • *all*—Disables all system files debug output. • *id*—Disables system ID debug output. • *info*—Disables system info debug output. • *init*—Disables system init debug output.
transfer	File transfer.
user	User management. • *all*—Disables all user management debug output. • *password-policy*—Disables user management debug output for password-policy.
utils	Utilities configuration files. *all*—Disables all utilities configuration debug output.
level	Number of the priority level at which you set the undebug output. Set level between 0 and 7 with 0 being severe and 7 being all.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# undebug all
acs/admin#
```

Related Commands

Command	Description
debug	Displays errors or events for command situations.

write

To copy, display, or erase ACS server configurations, use the **write** command with the appropriate argument in the EXEC mode.

```
write {erase | memory | terminal}
```

Syntax Description

erase	Erases the startup-configuration.
memory	Copies running-configuration to startup-configuration.
terminal	Copies the running-configuration to console.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# write memory
Generating configuration...
acs/admin#
```

Example 2

```
acs/admin# write terminal
Generating configuration...
!
hostname ACS
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet 1
  shutdown
!
ip name-server 209.165.201.1
!
ip default-gateway 209.165.202.129
!
clock timezone UTC
!
username admin password hash $1$UMCQIJy1$8Z.9tkpO1QzCo4zyc1jso0 role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
```

```
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
acs/admin#
```

Show Commands

Each **show** command includes a brief description of its use, command syntax, usage guidelines, and sample output.

Table 3-9 lists the Show commands in the EXEC mode, which are described in this section.

Table 3-9 List of EXEC Show Commands[1]

• show acs-config-web-interface • show acs-cores • show acs-logs * • show application *[2] • show backup history • show cdp • show clock • show cpu • show disks • show icmp_status • show interface • show inventory • show ip route • show ipv6 route • show logging • show logins	• show memory • show ntp • show ports • show process • show repository • show restore • show running-configuration • show startup-configuration • show tech-support • show terminal • show timezone • show timezones • show udi • show uptime • show users • show version *

1. Commands marked with an asterisk (*) represent those that are specific to ACS functionality.
2. The **show application status acs** and **show application version acs** commands are specific to ACS.

show acs-config-web-interface

To see whether an interface is disabled or enabled for ACS configuration web, use the **show acs-config-web-interface** command in the EXEC mode.

```
show acs-config-web-interface
```

Syntax Description No arguments or keywords.

Defaults The interface for ACS configuration web is enabled by default.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
acs/admin# show acs-config-web-interface
migration interface is enabled
ucp interface is disabled
view interface is disabled
```

Related Commands

acs config-web-interface	Enables or disables an interface for ACS configuration web.

show acs-cores

To display the list of ACS run-time core files and Java Virtual Machine (JVM) core logs, use the **show acs-cores** command in the EXEC mode.

```
show acs-cores [details]
```

Syntax Description

details	Displays the modification time and size (in KB) for each core and log file.

Defaults The ACS core files are located at /opt/CSCOacs/runtime/core and the JVM core logs are located at /hs_err_pid.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
acs/admin# show acs-cores

core.2464
core.3535
hs_err_pid12477.log
acs/admin#
```

Example 2

```
acs/admin# show acs-cores details

Filesize (kb)   Date   Time   Filename
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
4562             Nov 18 13:45 core.2464
6788             Nov 10 12:33 core.3535
1193             Apr 29 11:59 hs_err_pid12477.log
acs/admin#
```

Example 3

```
acs/admin# show acs-cores

No ACS core files exist
acs/admin#
```

Related Commands

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.
show acs-logs	Displays ACS server debug logs.

show acs-logs

To display ACS server debug logs, use the **show acs-logs** command in the EXEC mode.

show acs-logs {**details** | **filename** [*filename*]}

Syntax Description

details	Displays the modification time and size (in KB) for each log file. Also lists the available logfiles.
filename	Specifies a file whose contents you want to view.

filename	Name of the logfile (up to 255 characters) whose contents you want to view.
|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table 3-11). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

The ACS logs are located at /opt/CSCOacs/logs, and include the logs displayed in Table 3-10:

Table 3-10 ACS Logs

Logs	Description
ACSADAgent.log*	Stores the logs of an Active Directory client.
acsLogForward.log	Stores the debug log of log-forwarding processes.
ACSManagementAudit.log	Stores the details of the operations and configuration that are performed by administrators when using the ACS web interface or CLI.
ACSManagement.log	Stores information, warning, and debug messages from ACS web interface, CLI, and UCP web-service components.
acsRuntime.log	Stores the debug logs from runtime subsystem.
acsupgrade.log	Stores the patch installation and upgrade operation logs.
monit.log	Stores information about the health of various ACS processes. These include: • Web interface • Runtime process that processes the authentication and authorization requests • ACS database • ACS Monitoring and Report Viewer
MonitoringAndReportingAlert.log	Stores the logs from view-alertmanager process.
MonitoringAndReportingCollector.log	Stores the logs from view-logprocessor process.
MonitoringAndReportingDatabase.log	Stores the logs from view-database process.
MonitoringAndReportingExpertTroubleshooting.log	Stores the debug logs from the expert-troubleshooting feature of the Monitoring and Report Viewer web interface.
MonitoringAndReportingProcess.log	Stores the logs from all of the ACS view processes.

Table 3-10 ACS Logs

Logs	Description
MonitoringAndReportingScheduler.log	Stores the logs from view-jobmanager process.
MonitoringAndReportingUI.log	Stores the logs from Monitoring and Report Viewer web interface.
acsLocalStore.log*	Stores the logs from the local system.
catalina.out*	Stores information and debug messages from ACS, and Monitoring and Report Viewer web interfaces of the web server.
dberr.log	Stores the error logs from ACS database.

The log files that are marked with an asterisk (*) are numbered and rolled over based on a configured maximum file size. Once a log file touches the configured limit, the data is rolled over to another file. The new files are named by suffixing the time stamp or sequential numbers to the log filename.

Using the **show acs-logs** and **show acs-logs details** commands, you can view the list of available logfiles. To view the contents of a specific logfile, use the **show acs-logs filename** *filename* command.

Command Modes

EXEC

Usage Guidelines

You can use this command when ACS is not running.

Examples

Example 1

```
acs/admin# show acs-logs
ACSADAgent.log
ACSManagementAudit.log
ACSManagement.log
acsRuntime.log
monit.log
MonitoringAndReportingAlert.log
MonitoringAndReportingCollector.log
MonitoringAndReportingDatabase.log
MonitoringAndReportingProcess.log
MonitoringAndReportingScheduler.log
MonitoringAndReportingUI.log
reportService.0.acs.2008Oct08_20_02_37_Pacific_Daylight_Time.0.log
acsLocalStore.log
catalina.out
acs/admin#
```

Example 2

```
acs/admin# show acs-logs details
Filesize (kb)   Date   Time   Filename
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
26              Oct 7  19:32  ACSManagementAudit.log
65              Oct 7  19:32  ACSManagement.log
12              Oct 7  19:32  acsRuntime.log
6               Oct 7  19:33  monit.log
0               Oct 7  19:17  MonitoringAndReportingAlert.log
```

```
2               Oct 7  19:34  MonitoringAndReportingCollector.log
6               Oct 7  19:32  MonitoringAndReportingDatabase.log
3               Oct 7  19:33  MonitoringAndReportingProcess.log
0               Oct 7  19:17  MonitoringAndReportingScheduler.log
0               Oct 7  19:18  MonitoringAndReportingUI.log
0              Oct 8 20:02
reportService.0.acs.2008Oct08_20_02_37_Pacific_Daylight_Time.0.log
8               Oct 7  19:32  acsLocalStore.log
19              Oct 7  19:32  catalina.out
acs/admin#
```

Example 3

```
acs/admin# show acs-logs filename acsRuntime.log
MessageBus,07/10/2008,19:16:40:569,ERROR,66497456,MessageBusSender::connect: unable to
connect to the management;exception=Connection refused,MessageBusSender.cpp:131
Handler,07/10/2008,19:17:35:273,WARN ,67550128,NIL-CONTEXT,Posture Server did not have any
ca cert configured,PostureServerHandler.cpp:63
Handler,07/10/2008,19:17:35:274,WARN ,67550128,NIL-CONTEXT,AcsNode does *not* have an
Https Certificate,PostureServerHandler.cpp:100
--More-- (press Spacebar to continue)
```

Related Commands

Command	Description
export-data	Exports configuration data from an ACS local store to a remote repository.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.

show application

To show application information of the installed application packages on the system, use the **show application** command in the EXEC mode.

show application [**status** | **version** [*app_name*]]

Syntax Description

status	Displays the status of the installed application. For ACS usage, the display includes whether the ACS is the primary or secondary, and the status of the services.
version	Displays the application version for an installed application—the ACS.

app_name	Name of installed application. The application name is case-sensitive.
|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table 3-11). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Table 3-11 Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Here is a list of various application status displayed and their interpretation.

Status	Description
Running	When the application is in running state.
Execution Failed	When the process has failed to start but still trying to start the process.
Not Monitored	After watchdog failed to start the process as configured.
Restarting	When either the process cannot be found or the process ID file is missing and the watchdog restarts the process.
Initializing	Intermediate state when the watchdog comes up or watchdog starts again to monitor a process. This is shown also when any of the processes has failed to pass the active test.

Examples

Example 1

```
acs/admin# show application
<name>          <Description>
acs              ACS 5.4
acs/admin#
```

Example 2

```
acs/admin# show application version acs

Cisco ACS VERSION INFORMATION
-----------------------------
Version :  5.4.0.46.0a
Internal Build ID : B.221

acs/admin#
```

Example 3

```
acs/admin# show application status acs
ACS role: PRIMARY

Process 'database'                  running
Process 'management'                running
Process 'runtime'                   running
Process 'view-database'             running
Process 'view-jobmanager'           running
Process 'view-alertmanager'         running
Process 'view-collector'            running
Process 'view-logprocessor'         running

acs/admin#
```

Example 4

```
acs/admin# show application status acs
ACS role: PRIMARY

"ACS is busy applying a recent configuration change
requiring enabling/disabling of processes.
Status is unavailable.
Please check again in a minute."

acs/admin#
```

This message appears when a set of processes change because of a view node selection or Active Directory configuration.

Example 5

```
acs/admin# show application status acs

ACS is not running.
Issue 'application start acs' command to start ACS.

acs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.

show backup history

To display the backup history of the system, use the **show backup** command in the EXEC mode.

```
show backup history
```

Syntax Description

history	Displays history information about any backups on the system.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# show backup history
Wed Jul 18 12:55:21 UTC 2007: backup logs logs-0718.tar.gz to repository fileserver007:
success
Wed Jul 18 12:55:53 UTC 2007: backup full-0718.tar.gpg to repository fileserver007:
success
acs/admin#
```

Example 2

```
acs/admin# show backup history
backup history is empty
```

Related Commands

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.

show cdp

To display information about the enabled CDP interfaces, use the **show cdp** command in the EXEC mode.

```
show cdp {all | neighbors}
```

Syntax Description

all	Shows enabled CDP interfaces.
neighbors	Shows CDP neighbors.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# show cdp all

CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port GigabitEthernet0.

acs/admin#
```

Example 2

```
acs/admin# show cdp neighbors


CDP Neighbor : acs-test2
        Local Interface    : GigabitEthernet0
        Device Type        : cisco WS-C3560G-48PS
        Port               : GigabitEthernet0/36
        Address            : 209.165.200.225

acs/admin#
```

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a CDP packet from your router before discarding it.
cdp run	Enables the CDP.
cdp timer	Specifies how often the ACS server sends CDP updates.

show clock

To display the day, month, date, time, time zone, and year of the system software clock, use the **show clock** command in the EXEC mode.

```
show clock
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show clock
Tue Oct  7 20:13:22 UTC 2008
acs/admin#
```

Note The **show clock** output in the previous example includes Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), Great Britain, or Zulu time (see Tables 3-19, 3-20, and 3-21 on pages A-94 and A-95 for sample time zones).

Related Commands

Command	Description
clock	Sets the system clock for display purposes.

show cpu

To display CPU information, use the **show cpu** command in the EXEC mode.

show cpu [*statistics*] [|] [|]

Syntax Description

statistics	Displays CPU statistics.
|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table 3-12). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables (see Table 3-12).

Table 3-12 Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
acs/admin# show cpu
processor : 0
model     : Intel(R) Core(TM)2 CPU          6400  @ 2.13GHz
speed(MHz): 2133.737
cache size: 2048 KB

processor : 1
model     : Intel(R) Core(TM)2 CPU          6400  @ 2.13GHz
speed(MHz): 2133.737
cache size: 2048 KB

acs/admin#
```

Example 2

```
acs/admin# show cpu statistics
user time:               8312
kernel time:             3200
idle time:           15510748
i/o wait time:           5295
irq time:                 972

acs/admin#
```

Related Commands

Command	Description
show disks	Displays the system information of all disks.
show memory	Displays the amount of system memory that each system process uses.

show disks

To display file-system information about the disks, use the **show disks** command in the EXEC mode.

show disks [|] [|]

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table 3-13). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables (see Table 3-13).

Table 3-13 Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Only platforms that have a disk file system support the **show disks** command.

Examples

```
acs/admin# show disks
disk: 1% used (48564 of 7063480)
temp. space 2% used (35844 of 2031952)

Internal filesystems:
  all internal filesystems have sufficient free space

acs/admin#
```

Related Commands

Command	Description
show cpu	Displays CPU information.
show memory	Displays the amount of system memory that each system process uses.

show icmp_status

To display file-system information about the disks, use the **show icmp_status** command in EXEC mode.

show icmp_status {**>** *file* | |}

Syntax Description

>	Output direction.
file	Name of file to redirect standard output (stdout).
|	Output modifier commands: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word count. – |—Output modifier commands (see Table 3-14). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word last. This can be a maximum of 80 lines to display. Default 10. – |—Output modifier commands (see Table 3-14).

Table 3-14 Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
acs/admin# show icmp_status
icmp echo response is turned on
acs/admin#
```

Example 2

```
acs/admin# show icmp_status
icmp echo response is turned off
acs/admin#
```

Related Commands

Command	Description
icmp echo	Configures the Internet Control Message Protocol (ICMP) echo requests.

show interface

To display the usability status of interfaces configured for IP, use the **show interface** command in the EXEC mode.

show interface [*GigabitEthernet*] |

Syntax Description

GigabitEthernet	Shows the Gigabit Ethernet interface. Either 0 or 1.
|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show interface
eth0      Link encap:Ethernet  HWaddr 00:16:36:56:61:D2
          inet addr:209.165.200.225 Bcast:209.165.200.255 Mask:255.255.255.224
          inet6 addr: fe80::216:36ff:fe56:61d2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8783423 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4178157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:574274908 (547.6 MiB)  TX bytes:268869567 (256.4 MiB)
          Interrupt:169

eth1      Link encap:Ethernet  HWaddr 00:16:36:56:61:D1
          inet6 addr: fe80::216:36ff:fe56:61d1/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:177

lo        Link encap:Local Loopback
          inet addr:209.165.201.1 Mask:255.255.255.224
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:21617 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3587148 (3.4 MiB)  TX bytes:3587148 (3.4 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

acs/admin#
```

Related Commands

Command	Description
interface	Configures an interface type and enters the interface configuration submode.

show inventory

To display information about the hardware inventory, including the ACS appliance model and serial number, use the **show inventory** command in the EXEC mode.

```
show inventory |
```

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show inventory

NAME: "CSACS1120-K9       chassis", DESCR: "CSACS1120-K9       chassis"
PID: CSACS1120-K9      , VID: V01 , SN: CAM12345678
Total RAM Memory: 4149500 kB
CPU Core Count: 2
CPU 0: Model Info: Intel(R) Core(TM)2 CPU          6400  @ 2.13GHz
CPU 1: Model Info: Intel(R) Core(TM)2 CPU          6400  @ 2.13GHz
Hard Disk Count(*): 2
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 250.00 GB
Disk 0: Geometry: 255 heads 63 sectors/track 30401 cylinders
Disk 1: Device Name: /dev/sdb
Disk 1: Capacity: 250.00 GB
Disk 1: Geometry: 255 heads 63 sectors/track 30401 cylinders
NIC Count: 2
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:15:17:59:73:81
NIC 0: Driver Descr: e1000: eth0: e1000_probe: Intel(R) PRO/1000 Network Connect
```

```
ion
NIC 1: Device Name: eth1
NIC 1: HW Address: 00:15:17:59:73:82
NIC 1: Driver Descr: e1000: eth1: e1000_probe: Intel(R) PRO/1000 Network Connect
ion

(*) Hard Disk Count may be Logical.

acs/admin#
```

show ip route

To display the route information for specific IP addresses, network masks or protocols, use the s**how ip route** command in the EXEC mode.

```
show ip route |
```

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC.

Usage Guidelines

None.

Examples

```
acs/admin# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.77.247.64    0.0.0.0         255.255.255.224 U     0      0        0 eth0
0.0.0.0         10.77.247.65    0.0.0.0         UG    0      0        0 eth0
```

Related Commands

Command	Description
ip address	Sets the IP address and netmask for the Ethernet interface.
ip route	Configures the static routes.

show ipv6 route

To display the available IPv6 routes on the server, use the s**how ipv6 route** command in the EXEC mode.

```
show ipv6 route |
```

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC.

Usage Guidelines

None.

Examples

```
acs/admin# show ipv6 route
Kernel IPv6 routing table
Destination                    Next                    Hop    Flags  Metric Ref  Use
Iface
2001::/6                       ::                      UA     256    1058   0    eth0
2001::/64                      2001::212:44ff:fe30:bc0a UG     1024   0      0    eth0
fe80::/64                      ::                      U      256    0      0    eth0
::/0                           fe80::212:44ff:fe30:bc0a UGDA   1024   7      0    eth0
::1/128                        ::                      U      0      24     9    lo
2001::215:17ff:fe7f:7780/128   ::                      U      0      0      1    lo
2001::9893:fc06:19ee:6453/128  ::                      U      0      0      1    lo
2001::c0bf:f906:75e9:9868/128  ::                      U      0      4      1    lo
2001::c996:dafc:1419:73f3/128  ::                      U      0      0      1    lo
```

```
fe80::215:17ff:fe7f:7780/128   ::                    U     0      3      1    lo
ff00::/8                       ::                    U     256    0      0    eth0
acs240-228/admin#
```

Related Commands	Command	Description
	ip address	Sets the IP address and netmask for the Ethernet interface.
	ip route	Configures the static routes.

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in the EXEC mode.

show logging {**application** [*application-name*]} {**internal**} {**system**} |

Syntax Description		
	application	Displays application logs. *application-name*—Application name. This can be a maximum of 255 alphanumeric characters. – *tail*—Tail system syslog messages. – *count*—Tail last count messages. From 0 to 4,294,967,295. |—Output modifier variables (see below).
	internal	Displays the syslogs configuration.
	system	Displays the system syslogs.
	|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and for which, logging destinations (console, monitor, buffer, or host) logging is enabled.

Examples

Example 1

```
acs/admin# show logging system
ADEOS Platform log:
-----------------

Oct  7 13:24:41 localhost debugd[2050]: [2915]: config:network: main.c[238]: Set
up is complete
Oct  7 13:24:51 localhost debugd[2050]: hangup signal caught, configuration read
Oct  7 13:24:51 localhost debugd[2050]: successfully loaded debug config
Oct  7 13:24:51 localhost debugd[2050]: [3482]: icmp: icmputils_cli.c[139]: Generating
icmp echo response config
Oct  7 13:24:51 localhost debugd[2050]: [3482]: icmp: cars_icmpcfg.c[118]: Got the current
ICMP Echo response config as : enabled
Oct  7 13:24:51 localhost debugd[2050]: [3482]: icmp: icmputils_cli.c[160]: Got ICMP echo
config: on
Oct  7 13:24:51 localhost debugd[2050]: [3482]: icmp: icmputils_cli.c[167]: Finished icmp
echo response config generation
Oct  7 13:24:51 localhost debugd[2050]: [3482]: logging: logutils_cli.c[233]: Generating
logging config
Oct  7 13:24:51 localhost debugd[2050]: [3482]: logging: logutils_cli.c[253]: Got
Logserver: localhost
Oct  7 13:24:51 localhost debugd[2050]: [3482]: logging: logutils_cli.c[261]: Got
loglevel: 6
--More-- (press Spacebar to continue)
```

Example 2

```
acs/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Enabled

acs/admin#
```

show logins

To display the state of system logins, use the **show logins** command in the EXEC mode.

```
show logins cli
```

Syntax Description

cli	Lists the login history.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines Requires the **cli** keyword; otherwise, an error occurs.

Examples

```
acs/admin# show logins cli
admin    pts/0        dhcp-64-102-82-1 Thu May  3 05:23   still logged in
admin    pts/0        dhcp-64-102-82-1 Thu May  3 04:31 - 05:11  (00:39)
admin    pts/0        dhcp-64-102-82-1 Thu May  3 04:16 - 04:17  (00:00)
admin    pts/0        dhcp-64-102-82-1 Thu May  3 03:53 - 04:16  (00:22)

wtmp begins Tue Oct  7 13:21:14 2008

acs/admin#
```

show memory

To display the memory usage of all the running processes, use the **show memory** command in the EXEC mode.

```
show memory
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
acs/admin# show memory
total memory:    2074924 kB
free memory:     1687324 kB
cached:           162984 kB
swap-cached:           0 kB

acs/admin#
```

show ntp

To show the status of the Network Time Protocol (NTP) associations, use the **show ntp** command in the EXEC mode.

```
show ntp
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
acs/admin# show ntp
Primary NTP   : 1.ntp.esl.cisco.com
Secondary NTP : 2.ntp.esl.cisco.com

synchronised to NTP server (209.165.202.129) at stratum 2
   time correct to within 37 ms
   polling server every 128 s

acs/admin#
```

Related Commands

Command	Description
ntp server	Allows synchronization of the software clock by the NTP server for the system.

show ports

To display information about all the processes listening on active ports, use the **show ports** command in the EXEC mode.

```
show ports [|] [|]
```

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. |—Output modifier variables (see Table 3-15). • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables (see Table 3-15).

Table 3-15 Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10. |—Output modifier variables.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you run the **show ports** command, the port must have an associated active session.

Examples

```
acs/admin# show ports

Process : dbsrv10 (9253)
     tcp: 0.0.0.0:2638, :::2638
Process : portmap (2615)
     tcp: 0.0.0.0:111
     udp: 0.0.0.0:111
Process : dbsrv10 (10019)
     tcp: 0.0.0.0:43216, :::43216
Process : rt_daemon (9450)
     tcp: 172.23.245.28:49
     udp: 0.0.0.0:32771, 0.0.0.0:1812, 0.0.0.0:1813, 0.0.0.0:1645, 0.0.0.0:1646
Process : monit (6933)
     tcp: 127.0.0.1:2812
Process : java (9756)
     tcp: :::2020, ::ffff:127.0.0.1:8005, :::6666, :::2030, :::61616, :::80,
::ffff:127.0.0.1:51515, :::443
Process : sshd (2776)
     tcp: :::22
Process : java (10023)
     udp: :::20514
acs/admin#
```

show process

To display information about active processes, use the **show process** command in the EXEC mode.

```
show process |
```

Syntax Description

|	(Optional) Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the interface. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

See Table 3-16 for process field descriptions.

```
acs/admin# show process

USER       PID     TIME TT       COMMAND
root         1 00:00:00 ?        init
root         2 00:00:00 ?        migration/0
root         3 00:00:00 ?        ksoftirqd/0
root         4 00:00:00 ?        migration/1
root         5 00:00:00 ?        ksoftirqd/1
root         6 00:00:00 ?        events/0
root         7 00:00:00 ?        events/1
root         8 00:00:00 ?        khelper
root         9 00:00:00 ?        kacpid
root        36 00:00:00 ?        kblockd/0
root        37 00:00:00 ?        kblockd/1
root        55 00:00:00 ?        pdflush
root        58 00:00:00 ?        aio/0
root        59 00:00:00 ?        aio/1
root        38 00:00:00 ?        khubd
```

```
root         57 00:00:00 ?        kswapd0
root        203 00:00:00 ?        kseriod
root        320 00:00:00 ?        ata/0
root        321 00:00:00 ?        ata/1
root        325 00:00:00 ?        scsi_eh_0
root        326 00:00:00 ?        scsi_eh_1
--More-- (press Spacebar to continue)
```

Table 3-16 Show Process Field Descriptions

Field	Description
USER	Logged-in user.
PID	Process ID.
TIME	The time the command was last used.
TT	Terminal that controls the process.
COMMAND	Type of process or command used.

show repository

To display the file contents of the repository, use the **show repository** command in the EXEC mode.

show repository *repository-name*

Syntax Description

repository-name	Name of the repository whose contents you want to view. This can be a maximum of 30 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show repository myrepository
back1.tar.gpg
back2.tar.gpg
acs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.

Command	Description
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show restore

To display the restore history, use the **show restore** command in the EXEC mode.

```
show restore {history}
```

Syntax Description

history	Displays the restore history.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# show restore history
Tue Sep  4 03:42:48 PDT 2008: restore 11backup_Local.File2.tar.gpg from repository
executeBackupRepo: success Tue Sep  4 03:46:15 PDT 2008: restore
11backup_Local.File2.tar.gpg from repository executeBackupRepo: success Tue Sep  4
03:51:07 PDT 2008: restore 11backup_Local.File2.tar.gpg from repository executeBackupRepo:
success Tue Sep  4 03:54:35 PDT 2008: restore 11backup_Local.File2.tar.gpg from repository
executeBackupRepo: success Wed Sep  5 12:31:21 UTC 2008: restore cdromRestore.tar.gpg from
repository cdrom1: success admin#

acs/admin#
```

Example 2

```
acs/admin# show restore history
restore history is empty
acs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show running-configuration

To display the contents of the currently running configuration file or the configuration, use the **show running-configuration** command in the EXEC mode.

```
show running-configuration
```

Syntax Description

No arguments or keywords.

Defaults

The **show running-configuration** command displays all of the configuration information.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show running-configuration

Generating configuration...
!
hostname acs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet 1
  shutdown
!
!

clock timezone UTC
!
!
username admin password groove role admin
!
service sshd
!
repository myrepository
  url ftp://209.165.200.234/backup
  user bubba password gump
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
```

```
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
acs/admin#
```

Related Commands

Command	Description
configure	Enters the Configuration mode.
show startup-configuration	Displays the contents of the startup configuration file or the configuration.

show startup-configuration

To display the contents of the startup configuration file or the configuration, use the **show startup-configuration** command in the EXEC mode.

show startup-configuration

Syntax Description

No arguments or keywords.

Defaults

The **show startup-configuration** command displays all of the startup configuration information.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show startup-configuration

Generating configuration...
!
hostname acs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet 1
  shutdown
!
!

clock timezone UTC
!
```

```
!
username admin password groove role admin
!
service sshd
!
repository myrepository
  url ftp://209.165.200.234/backup
  user bubba password gump
!
--More-- (press Spacebar to continue)
```

Related Commands

Command	Description
configure	Enters the Configuration mode.
show running-configuration	Displays the contents of the currently running configuration file or the configuration.

show tech-support

To display technical support information, including e-mail, use the **show tech-support** command in the EXEC mode.

show tech-support file [*word*]

Syntax Description

file	Save any technical support data as a file in the local disk.
word	Filename to save. This can be a maximum of 80 alphanumeric characters.

Defaults

Passwords and other security information do not appear in the output.

Command Modes

EXEC

Usage Guidelines

The **show tech-support** command is useful for collecting a large amount of information about your ACS server for troubleshooting purposes. You can then provide output to technical support representatives when reporting a problem.

Examples

```
acs/admin# show tech-support
#####################################################
Application Deployment Engine(ADE) - Release 1.0
Technical Support Debug Info follows...
#####################################################


**************************************
Checking dmidecode Serial Number(s)
**************************************
  0x0736C7F6
```

```
 0x0736C803
 0x0736C808
 0x0736C81F
 AZAX74601334

****************************************
Displaying System Uptime...
****************************************
 20:41:46 up  6:42,  1 user,  load average: 0.45, 0.20, 0.12

****************************************
Display Memory Usage(KB)
****************************************
             total       used       free     shared    buffers     cached
Mem:       4148032    2951612    1196420          0      59440    1873920
-/+ buffers/cache:    1018252    3129780
Swap:      8191992          0    8191992

****************************************
Displaying Processes(ax --forest)...
****************************************
  PID TTY      STAT   TIME COMMAND
    1 ?        S      0:00 init [3]
    2 ?        S      0:00 [migration/0]
    3 ?        SN     0:00 [ksoftirqd/0]
    4 ?        S      0:00 [migration/1]
    5 ?        SN     0:00 [ksoftirqd/1]

--More--(Press Enter or Spacebar.)
```

Related Commands

Command	Description
show interface	Displays the usability status of the interfaces.
show process	Displays information about active processes.
show running-configuration	Displays the contents of the current running configuration.

show terminal

To obtain information about the terminal configuration parameter settings, use the **show terminal** command in the EXEC mode.

```
show terminal
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
acs/admin# show terminal
TTY: /dev/pts/0 Type: "vt100"
Length: 25 lines, Width: 80 columns
Session Timeout: 30 minutes
acs/admin#
```

Table 3-17 describes the fields of the **show terminal** output.

Table 3-17 Show Terminal Field Descriptions

Field	Description
TTY: /dev/pts/0	Displays standard output to type of terminal.
Type: “vt100“	Type of current terminal used.
Length: 24 lines	Length of the terminal display.
Width: 80 columns	Width of the terminal display, in character columns.
Session Timeout: 30 minutes	Length of time, in minutes, for a session, after which the connection closes.

show timezone

To display the time zone as set on the system, use the **show timezone** command in the EXEC mode.

```
show timezone
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show timezone
UTC
acs/admin#
```

Related Commands

Command	Description
clock timezone	Sets the time zone on the system.
show timezones	Displays the time zones available on the system.

show timezones

To obtain a list of time zones from which you can select, use the **show timezones** command in the EXEC mode.

```
show timezones
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

See clock timezone, page 3-142, for examples of the time zones available for the ACS server.

Examples

```
acs/admin# show timezones
PST8PDT
Hongkong
Etc/GMT-7
Etc/GMT-12
Etc/GMT-4
Etc/GMT-13
Etc/GMT-11
Etc/GMT-1
Etc/GMT+5
Etc/GMT-14
Etc/GMT+11
Etc/GMT+6
Etc/Zulu
Etc/GMT+7
Etc/Universal
Etc/GMT-2
Etc/GMT+10
Etc/GMT-8
Etc/GMT+8
Etc/GMT+1
Etc/GMT0
Etc/GMT+9
Etc/GMT+3
Etc/GMT-3
Etc/GMT
Etc/GMT-5
Etc/GMT-0
Etc/GMT-6
Etc/GMT+4
Etc/GMT-9
Etc/GMT+12
Etc/GMT+2
Etc/UCT
Etc/GMT-10
Etc/GMT+0
Etc/Greenwich
```

```
Etc/UTC
Pacific/Norfolk
--More-- (Press Enter or Spacebar)
```

Related Commands

Command	Description
show timezone	Displays the time zone set on the system.
clock timezone	Sets the time zone on the system.

show udi

To display information about the CSACS-1121's or Cisco SNS-3415's UDI, use the **show udi** command in the EXEC mode.

```
show udi
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
acs/admin# show udi
SPID: ADE-1010
VPID: VO1
Serial: 123455
acs/admin#
```

Example 2

```
acs/admin# sh udi
SPID:: Cisco-VM-SPID
VPID:  V01
Serial: Cisco-VM-SN
```

This output appears when you run the **show udi** command on VMware servers running VMware ESXi 4.1.0.

show uptime

To display the length of time that you have been logged in to the ACS server, use the **show uptime** command in the EXEC mode.

```
show uptime |
```

Syntax Description

|	(Optional) Output modifier variables: • *begin*—Matched pattern. This can be a maximum of 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. • *end*—End with line that matches. This can be a maximum of 80 alphanumeric characters. • *exclude*—Exclude lines that match. This can be a maximum of 80 alphanumeric characters. • *include*—Include lines that match. This can be a maximum of 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. This can be a maximum of 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
acs/admin# show uptime
4 day(s), 16:36:58
acs/admin#
```

show users

To display the list of users logged in to the ACS server, use the **show users** command in the EXEC mode.

```
show users
```

Syntax Description

No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
acs/admin# show users
USERNAME         ROLE   HOST                      TTY      LOGIN DATETIME
admin            Admin  209.165.200.225             pts/0    Tue Oct  7 19:21:00 2008
acs/admin#
```

show version

To display information about the software version of the system, use the **show version** command in the EXEC mode.

```
show version
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines This command displays information about the ADE-OS 2.0 software version running on the ACS server, and the ACS version.

Examples

```
acs/admin# sh ver
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.3.062
ADE-OS System Architecture: i386
Copyright (c) 2005-2012 by Cisco Systems, Inc.
All rights reserved.
Hostname: acs

Version information of installed applications
---------------------------------------------


Cisco ACS VERSION INFORMATION
```

```
-----------------------------
Version :  5.4.0.46.0a
Internal Build ID: B.221
acs/admin#
```

ACS Configuration Commands

Each ACS Configuration command includes a brief description of its use, command syntax, usage guidelines, and sample output.

To access the ACS Configuration mode, you must use the **acs-config** command in the EXEC mode.

This section describes the following Configuration commands.

- access-setting accept-all
- acsview-db-compress
- acsview merge-from-supportbundle
- acsview rebuild-database
- acsview replace-clean-activesessionsdb
- acsview replace-cleandb
- acsview show-dbsize
- acsview truncate-log
- ad-agent-configuration
- ad-agent-reset-configuration
- debug-adclient
- debug-log
- export-data
- import-data
- import-export-abort
- import-export-status
- no ad-agent-configuration
- no debug-adclient
- no debug-log
- replication force-sync
- replication status
- reset-management-interface-certificate
- show ad-agent-configuration
- show ad-agent-configuration-changes
- show debug-adclient
- show debug-adclient
- database-compress

access-setting accept-all

To reset the IP address filtering to allow any IP address to access the management pages of an ACS server, use the **access-setting accept-all** command in the ACS Configuration mode. Only the super admin has the privilege to use this command on a primary ACS node.

```
access-setting accept-all
```

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS Configuration

Usage Guidelines Use the **access-setting accept-all** command when all system administrators' access to an ACS node through the GUI is blocked. This problem occurs when an administrator defines an access list that includes all IP addresses and blocks access to the GUI.

When you run this command, IP address filtering is set to allow all IP addresses to connect the management pages, but the IP addresses defined in the IP Ranges table to allow or reject the IP addresses to access the management pages are not reset; therefore, you can reuse this table to set IP address filtering.

Examples

```
acs/admin(config-acs)# access-setting accept-all

access setting allows all IP addresses to connect
acs/admin(config-acs)#
```

acsview-db-compress

Use the acsview-db-compress command to compress the ACS View database file size. This command 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.

```
acsview-db-compress
```

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS Configuration

Usage Guidelines

ACS is stopped during the database compression process. ACS restarts automatically after the database compression. Database compression takes sometime, based on the database size. If the database size is large, then the compression happens in hours. This CLI command needs to executed only in the log collector server.

It is strongly recommended to execute this CLI only during maintenance hours, as it requires restarting the ACS services. The option to compress the view database is also mentioned in the description of one of the alerts that is sent when the databasae reaches a certain limit.

Examples

```
acs242-197/acsadmin(config-acs)# acsview-db-compress
You can chose to compress ACS View database. This operation will take more time if the
size of the database is big. During this operation, ACS services will be stopped. Services
will be started automatically when the compression is over. Do you want to continue (y/n)?
Please wait till ACS services return after the ACS View database is compressed. Refer to
ADE.log for more details about the ACS View db compress.
```

acsview merge-from-supportbundle

Use the acsview merge-from-supportbundle command to merge the existing ACS view database with the information given in the specified support bundle.

acsview merge-from-supportbundle *support-file-name*

Syntax Description

support-file-name	Holds the support bundle file name which is to be merged with the existing ACS view database. This support bundle file should be present in the local disk.

Defaults

None.

Command Modes

ACS configuration

Usage Guidelines

ACS view services are stopped during the support bundle merge operation. ACS view services restart automatically after the merge operation is successful.

You should copy the decrypted support bundle of the same version which we have specified in the support file name of the merge command including the patch version. You should copy this file using the copy command in CLI.

Examples

```
acs242-197/acsadmin(config-acs)# acsview merge-from-supportbundle clisupport.tar.gz
Do you want to clean the data first?[y/n]

Please wait till database merge operation is completed. Refer ADE.log for more details
about the status.
```

Related Commands

Command	Description
acsview rebuild-database	Rebuilds the ACS view database and keeps the log data only for the specified number of days.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make it as a fresh database.
acsview replace-cleandb	Removes all data from the ACS view database and makes the current view database as a fresh view database.
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.
acsview truncate-log	Truncates the ACS view database transaction logs.

acsview rebuild-database

Use the acsview rebuild-database command to rebuild the database with the log information up to the specified number of days. If you specify to rebuild the database for 10 days, then ACS view database keeps only the last 10 days data and erases the remaining data.

acsview rebuild-database *noofdays*

Syntax Description

number-of-days	Holds a integer value for number of days.

Defaults

None.

Command Modes

ACS configuration

Usage Guidelines

ACS view services are stopped during the database rebuild operation. ACS view services restart automatically after rebuild operation is successful.

You need to clean up the unwanted files and have enough disk space before executing the rebuild-database command in ACS view.

Examples

```
acs242-197/acsadmin(config-acs)# acsview rebuild-database 10
This operation will take more time if the number of records are more in the
database.During this operation,ACSview unloads the data for given number of days to
localdisk or opt which one is having more space,Stops view services ,replaces with clean
db,restart view services and reload the data.Do you want to continue (y/n)?
Please wait till database reload operation is completed.Refer ADE.log for more details.
```

Related Commands

Command	Description
acsview merge-from-supportbundle	Merges the ACS view database with the specified support bundle data.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make it as a fresh database.
acsview replace-cleandb	Removes all data from the ACS view database and makes the current view database as a fresh view database.
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.
acsview truncate-log	Truncates the ACS view database transaction logs.

acsview replace-clean-activesessionsdb

Use the acsview replace-clean-activesessionsdb command to clean up the active session information in the ACS view database. This command removes the active session information in the ACS view database.

```
acsview replace-clean-activesessionsdb
```

Syntax Description

No arguments or keywords.

Defaults

None.

Command Modes

ACS configuration

Usage Guidelines

ACS view services are stopped during database active sessions clean up process. ACS view services restart automatically after the active sessions clean up operation is successful.

Examples

```
acs242-197/acsadmin(config-acs)# acsview replace-clean-activesessionsdb
acs242-197/acsadmin(config-acs)#
```

Related Commands

Command	Description
acsview merge-from-supportbundle	Merges the ACS view database with the specified support bundle data.
acsview rebuild-database	Rebuilds the ACS view database and keeps the log data only for the specified number of days.
acsview replace-cleandb	Removes all data from the ACS view database and makes the current view database as a fresh view database.

Command	Description
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.
acsview truncate-log	Truncates the ACS view database transaction logs.

acsview replace-cleandb

Use the acsview replace-cleandb command to clean up the information in the ACS view database. This command removes all data from the ACS view database. That is, this command replaces the current database with a fresh view database.

```
acsview replace-cleandb
```

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS configuration

Usage Guidelines ACS view services are stopped during database clean up process. ACS view services restart automatically after the database clean up operation is successful.

Examples

```
acs242-197/acsadmin(config-acs)# acsview replace-cleandb
acs242-197/acsadmin(config-acs)#
```

Related Commands

Command	Description
acsview merge-from-supportbundle	Merges the ACS view database with the specified support bundle data.
acsview rebuild-database	Rebuilds the ACS view database and keeps the log data only for the specified number of days.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make it as a fresh database.
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.
acsview truncate-log	Truncates the ACS view database transaction logs.

acsview show-dbsize

Use the acsview show-dbsize command to display the physical and active size of the ACS view database. It also displays the physical size of the ACS view transaction log files.

```
acsview show-dbsize
```

Syntax Description

No arguments or keywords.

Defaults

None.

Command Modes

ACS configuration

Usage Guidelines

None.

Examples

```
acs242-197/acsadmin(config-acs)# acsview show-dbsize
Actual DB Size (bytes) : 63692800
Actual DB Size (GBs) :0.06
Physical DB Size (bytes):64667648
Physical DB Size (GBs) :0.06
Physical ACSviewlog file Size (GBs) :0
acs242-197/acsadmin(config-acs)#
```

Related Commands

Command	Description
acsview merge-from-supportbundle	Merges the ACS view database with the specified support bundle data.
acsview rebuild-database	Rebuilds the ACS view database and keeps the log data only for the specified number of days.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make it as a fresh database.
acsview replace-cleandb	Removes all data from the ACS view database and makes the current view database as a fresh view database.
acsview truncate-log	Truncates the ACS view database transaction logs.

acsview truncate-log

Use the acsview truncate-log command to truncate the ACS view database transaction log messages.

acsview truncate-log

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS configuration

Usage Guidelines None.

Examples

```
acs242-197/acsadmin(config-acs)# acsview truncate-log
acs242-197/acsadmin(config-acs)#
```

Related Commands

Command	Description
acsview merge-from-supportbundle	Merges the ACS view database with the specified support bundle data.
acsview rebuild-database	Rebuilds the ACS view database and keeps the log data only for the specified number of days.
acsview replace-clean-activesessionsdb	Removes the active session information from the ACS view database and make it as a fresh database.
acsview replace-cleandb	Removes all data from the ACS view database and makes the current view database as a fresh view database.
acsview show-dbsize	Displays the physical and actual size of the ACS view database and the transaction log files.

ad-agent-configuration

This command adds the parameter to the end of the file, if the given parameter is not found in the Centrify configuration file. There is no validity check on the parameter value:

ad-agent-configuration *parameter-name value* **{local | distribute}**

Syntax Description

parameter-name	Holds the parameter name that has to be added to the Centrify configuration file.
value	Holds the value of the parameter to be added or modified.
local	Applies the configuration changes to this acs node only.
distribute	Applies the configuration changes to the entire deployment.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

You can use this command to add a new parameter or modify the value of the existing parameter value in the Centrify configuration file. When you try to modify the value of the parameter, it will be uncommented if it is commented by default. You can change the configuration either local to this node or to the entire deployment. Use local to change the configuration locally and distribute to change the configuration to the entire deployment.

Examples

Example 1

```
ACS149/acsadmin(config-acs)# ad-agent-configuration distparam 89 distribute
Performing AD agent internal setting modification is only allowed with ACS support
approval. continue (y/n)?

ACS149/acsadmin(config-acs)# show ad-agent-configuration-changes
-------------------------------------------------------------------------------------
Loading the AD Agent Configuration made for the primary node acs149...
-------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:23
-------------------------------------------------------------------------------------

Loading the AD Agent Configuration made for the secondary node ACS136...
-------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:22
-------------------------------------------------------------------------------------
ACS149/acsadmin(config-acs)#
```

Example 2

```
ACS149/acsadmin(config-admin)# ad-agent-configuration localparam 90 local
Performing AD agent internal setting modification is only allowed with ACS support
approval. continue (y/n)?

ACS149/acsadmin(config-acs)# show ad-agent-configuration-changes
-------------------------------------------------------------------------------------
Loading the AD Agent Configuration made for the primary node acs149...
-------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:23
localparam 90            N/A           local       acs149   2012-09-17 07:15:23
```

```
--------------------------------------------------------------------------------
ACS149/acsadmin(config-acs)#
```

ad-agent-reset-configuration

To reset the AD Agent configurations in the Centrify configuration file to its default value, use the **ad-agent-reset-configuration** command.

ad-agent-reset-configuration

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS Configuration

Usage Guidelines Use this command when you want to reset the configuration of an AD Agent in the Centrify configuration file to its default value.

Examples

```
cd-acs5-13-74/acsadmin(config-acs)#  ad-agent-reset-configuration
Performing reset of AD agent configuration, AD agent will be restarted. continue (y/n)?
cd-acs5-13-74/acsadmin(config-acs)#
```

You have to open the file manually to check the configuration changes.

debug-adclient

To enable debug logging for an Active Directory client, use the **debug-adclient** command in the ACS Configuration mode. To disable debug logging for an Active Directory client, use the **no** form of this command. Only the network-device admin can enable or disable debug logging for an Active Directory client.

debug-adclient enable

Syntax Description No arguments or keywords.

Defaults Disabled.

Command Modes ACS Configuration

Usage Guidelines

When you set the log level of debug logs to DEBUG for the following components, the active directory client logs are automatically enabled. Similarly, when you disable the DEBUG log level on one of these components, the active directory logs are disabled:

- all
- mgmt
- runtime
- runtime-idstores

Examples

```
acs/admin(config-acs)# debug-adclient enable
acs/admin(config-acs)#
```

Related Commands

Command	Description
no debug-adclient	Disables debug logging for an Active Directory client.
debug-log	Defines the local debug logging level for the ACS components.
show debug-log	Shows the debug log level status for subsystems (enabled or disabled).
show debug-adclient	Shows the debug log level status for an Active Directory client (enabled or disabled).
show acs-logs	Displays ACS server debug logs.

debug-log

To set the local debug logging level for all or specific ACS components, use the debug-log command in the ACS Configuration mode. Any user, irrespective of role, can run this command.

debug-log {*component* | **all**} **level** {**debug** | **info** | **warn** | **error** | **fatal** | **none**}

Syntax Description

component	Selects local debug logging on the components you want, where *component* can be any of the components described in the Usage Guidelines.
all	Selects local debug logging on all components.
level	Selects local debug logging level. The options are: • debug—Selects logging messages with the DEBUG severity level. • info—Selects logging messages with the INFO severity level. • warn—Selects logging messages with the WARN severity level. • error—elects logging messages with the ERROR severity level. • fatal—Selects logging messages with the FATAL severity level. • none—Selects logging messages with the no severity level.

Defaults

All ACS debug logging is set to warn.

Command Modes ACS Configuration

Usage Guidelines You can select any of the following options (including suboptions) as a component:

- runtime—If you select this component, all runtime subcomponents are included; see *runtime-* items in the list below.
  - runtime-admin
  - runtime-authenticators
  - runtime-authorization
  - runtime-config-manager
  - runtime-config-notification-flow
  - runtime-customerlog
  - runtime-crypto
  - runtime-dataaccess
  - runtime-dbpassword
  - runtime-eap
  - runtime-event-handler
  - runtime-idstores
  - runtime-infrastructure
  - runtime-logging
  - runtime-logging-notification-flow
  - runtime-message-bus
  - runtime-message-catalog
  - runtime-radius
  - runtime-rule-engine
  - runtime-state-manager
  - runtime-tacacs
  - runtime-xml-config
- mgmt (management)—If you select this component, all other mgmt subcomponents are included; see *mgmt-* items in the list below.
  - mgmt-audit
  - mgmt-common
  - mgmt-aac
  - mgmt-bl
  - mgmt-cli
  - mgmt-gui
  - mgmt-system
  - mgmt-notification

- mgmt-bus
- mgmt-dbal
- mgmt-replication
- mgmt-distmgmt
- mgmt-validation
- mgmt-changepassword
- mgmt-license
- mgmt-acsview

The debug logging configuration remains in effect even after a reboot. To reconfigure, use the **debug-log** command again or the **no debug-log** command.

When you set the log level of debug logs to DEBUG for the following components, the active directory client logs are automatically enabled. Similarly, when you disable the DEBUG log level on one of these components, the active directory logs are disabled:

- all
- mgmt
- runtime
- runtime-idstores

Examples

```
acs/admin(config-acs)# debug-log mgmt level warn
acs/admin(config-acs)#
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
export-data	Exports configuration data from an ACS local store to a remote repository.
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores the file contents of a specific repository from the backup.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).

Command	Description
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

export-data

To export the configuration data from an ACS local store to a remote repository, use the command **export-data** in the ACS Configuration mode. Only users who have Read permission to a specific configuration object in the GUI can export that specific configuration data to a remote repository.

export-data {**user** | **host** | **device** | **idgroup** | **ndg** | **dacl** | **cmdset**} *repository file-name*
result-file-name {**full** *secret-phrase* | **none** | **only-sec-repo** | **only-sec-files** *secret-phrase*}

Syntax Description

user | host | device | idgroup | ndg | dacl | cmdset	Exports specific configuration data to the remote repository.
repository	The remote repository to which to export the configuration data.
file-name	The file name to download the configuration data and store it in the remote repository.
result-file-name	The filename to use when downloading the results of the export process to the remote repository. By default, the ACS server concatenates a unique process ID with the *result-file-name* that you provide.
full	Encrypts the export file using the GNU Privacy Guard (GPG) encryption mechanism and uses secured remote repository to export the file. If you specify the security type as full, you must specify a repository of the type SFTP.
secret-phrase	Provide a secret phrase to encrypt the export file. If you specify the security type as full or only-sec-files, you must specify the secret phrase.
none	Neither encrypts the import file nor uses the secured remote repository for export.
only-sec-repo	Uses the secured remote repository to export the file. If you specify the security type as only-sec-repo, you must specify a repository of the type SFTP.
only-sec-files	Encrypts the export file using the GPG encryption mechanism.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

When you run this command, the ACS server starts a process to export the configuration data from the local ACS node to the specified remote repository and provides you a unique process ID to track the progress of the export operation. Use the **import-export-status** command to learn the status of export operations.

If the export process violates the security constraints defined in the security type parameters (full, none, only-sec-repo, and only-sec-files), the ACS server returns a validation error similar to the following:

```
Repository 'ftp01' has low security level
```

The **export-data** command is asynchronous, which allows you to execute other CLI commands when the export operation is in progress.

Examples

```
acs/admin(config-acs)# export-data user repostiory01 file01 resultfile01 full password

Export process Id is: 1
acs/admin(config-acs)#
```

Related Commands

Command	Description
import-data	Imports configuration data from a remote repository to an ACS local store.
import-export-abort	Aborts all or specific import or export processes.
import-export-status	Displays the status of all or specific import or export processes.

import-data

To update, delete, or add an ACS configuration data to the ACS local store from the import file of the remote repository, use the command **import-data** in the ACS Configuration mode. Only users who have CRUD permissions to a specific configuration object in the GUI can import that particular configuration data to an ACS local store.

import-data {**update** | **delete** | **add**} {**user** | **host** | **device** | **idgroup** | **ndg** | **dacl** | **cmdset**} *repository file-name result-file-name* {**abort-on-error** | **cont-on-error**} {**full** *secret-phrase* | **none** | **only-sec-repo** | **only-sec-files** *secret-phrase*}

Syntax Description

update	Updates the records in the ACS local store that match the records in the specified remote repository.
delete	Deletes the records in the ACS local store that match the records in the specified remote repository.
add	Adds the records that do not match the records of the import file in the remote repository to the ACS local store.
user | host | device | idgroup | ndg | dacl | cmdset	Imports the specified type of configuration data from the import file in the remote repository.
repository	Remote repository from which to import the configuration data.
file-name	Import filename in the remote repository.

result-file-name	Filename to use when downloading the results of the import process to the remote repository. By default, the ACS server concatenates a unique process ID with the *result-file-name*.
abort-on-error	Aborts the import operation if an error occurs during the import process.
cont-on-error	Ignores errors, if any occur, and continues the import process.
full	Encrypts the import file using the GPG encryption mechanism and uses secured remote repository to import the file. If you specify the security type as full, you must specify a repository of the type SFTP.
none	Neither encrypts the import file nor uses the secured remote repository for import.
secret-phrase	Provide the secret phrase to decrypt the import file. If you specify the security type as full or only-sec-files, you must specify the secret phrase.
only-sec-repo	Uses the secured remote repository to import the file. If you specify the security type as only-sec-repo, you must specify a repository of the type SFTP.
only-sec-files	Encrypts the import file using GPG encryption mechanism.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

When you run this command, the ACS server starts a process to import the ACS configuration data to the local ACS node from the specified remote repository and provides you a unique process ID to track the progress of the import operation. Use the **import-export-status** command to learn the status of import operations.

If the import process violates the security constraints defined in the security type parameters (full, none, only-sec-repo, and only-sec-files), the ACS server returns a validation error similar to the following:

```
Repository 'ftp01' has low security level
```

The **import-data** command is asynchronous, which allows you to execute other CLI commands when the import operation is in progress.

Examples

```
acs/admin(config-acs)# import-data add user repository01 file01 resultfile01
abort-on-error full password

Import process Id is: 2
acs/admin(config-acs)#
```

Related Commands

Command	Description
export-data	Exports configuration data from an ACS local store to a remote repository.

Command	Description
import-export-abort	Aborts all or specific import or export processes.
import-export-status	Displays the status of all or specific import or export processes.

import-export-abort

To abort currently running, queued, or all import and export processes, use the **import-export-abort** command in the ACS Configuration mode. 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 abort that particular process by using the process ID, or by stopping the process when it is in progress.

import-export-abort {**running** | **all** | **id** *id*}

Syntax Description

running	Aborts if any import or export processes is in progress.
all	Aborts if any import or export processes is in progress or waiting in queue to be processed.
id	Aborts the import or export processes with the specified ID, whether it is in progress or waiting in queue to be processed. You must specify the process ID.
id	To abort a specific import or export processes, specify the process ID.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

None.

Examples

Example 1

```
acs/admin(config-acs)# import-export-abort running

Aborted process ID #5
acs/admin(config-acs)#
```

Example 2

```
acs/admin(config-acs)# import-export-abort running

No running processes.
acs/admin(config-acs)#
```

Example 3

```
acs/admin(config-acs)# import-export-abort all
```

```
Aborted process ID #20, 50 pending processes are removed.
acs/admin(config-acs)#
```

Example 4

```
acs/admin(config-acs)# import-export-abort id 3

Removed pending process ID #3 from queue.
acs/admin(config-acs)#
```

Example 5

```
acs/admin(config-acs)# import-export-abort id 201

No such process ID #201.
acs/admin(config-acs)#
```

Related Commands

Command	Description
export-data	Exports configuration data from an ACS local store to a remote repository.
import-data	Imports configuration data from a remote repository to an ACS local store.
import-export-status	Displays the status of all or specific import or export processes.

import-export-status

To view the status of running import and export processes and to verify whether there are any pending processes, use the **import-export-status** command in the ACS Configuration mode. Any user, irrespective of role, can run this command.

import-export-status {**current** | **all** | **id** *id*}

Syntax Description

current	Displays the status of the currently running processes.
all	Displays the status of all the import and export processes, including any pending processes.
id	Displays the status of an import or export process with the specified ID. You must specify the process ID.
id	To view the import or export status based on a particular process, specify the process ID.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

None.

Examples

Example 1

```
acs/admin(config-acs)# import-export-status current

20 out of 30 records are processed, 0 failed.[]
acs/admin(config-acs)#
```

Example 2

```
acs/admin(config-acs)# import-export-status id 3

Process id# 3 completed; 10 out of 10 records are processed, 0 failed.[]
acs/admin(config-acs)#
```

Example 3

```
acs/admin(config-acs)# import-export-status id 4

Process id# 3 is pending; its number in the pending queue is 8.
acs/admin(config-acs)#
```

Example 4

```
acs/admin(config-acs)# import-export-status all

Process id# is running; 10 out of 10 records are processed, 0 failed; 0 are pending.
acs/admin(config-acs)#
```

Example 5

```
acs/admin(config-acs)# import-export-status all

No process is running.
acs/admin(config-acs)#
```

Related Commands

Command	Description
export-data	Exports configuration data from an ACS local store to a remote repository.
import-data	Imports configuration data from a remote repository to an ACS local store.
import-export-abort	Aborts all or specific import or export processes.

no ad-agent-configuration

This command comments out the lines that contain the parameter name.

no ad-agent-configuration *parameter name*

Syntax Description

.

parameter name	Holds the parameter name that is used in the the Centrify configuration file.

Defaults

None.

Command Modes ACS Configuration

Usage Guidelines You can use this command to comment out the lines that contain the given parameter name.

Examples

Example 1 – Using a specific parameter name

```
1) cd-acs5-13-74/acsadmin(config-acs)# no ad-agent-configuration
adclient.get.builtin.membership
Performing AD agent internal setting modification is only allowed with ACS support
approval. continue (y/n)?
cd-acs5-13-74/acsadmin(config-acs)#
output from Centrify.conf file - #  adclient.get.builtin.membership: true
```

Example 2– Using a Wildcard character

```
cd-acs5-13-74/acsadmin(config-acs)# no ad-agent-configuration
adclient.get.builtin.membership ?
  value  value.
  <cr>
cd-acs5-13-74/acsadmin(config-acs)#
```

no debug-adclient

To disable debug logging for an Active Directory client, use the **no debug-adclient** command in the ACS Configuration mode. Only the network-device admin can enable or disable debug logging for an Active Directory client.

```
no debug-adclient enable
```

Syntax Description No arguments or keywords.

Defaults Disabled.

Command Modes ACS Configuration

Usage Guidelines None.

Examples

```
acs/admin(config-acs)# no debug-adclient enable
acs/admin(config-acs)#
```

Related Commands

Command	Description
debug-adclient	Enables debug logging for an Active Directory client.
debug-log	Defines the local debug logging level for the ACS components.

Command	Description
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show debug-adclient	Shows the debug log level status for an Active Directory client (enabled or disabled).

no debug-log

To return debug logging to the default configuration for all components or specific ACS components, use the **no debug-log** command in the ACS Configuration mode. Any user, irrespective of role, can run this command.

no debug-log {*component* | **all**} [**level** [**debug** | **info** | **warn** | **error** | **fatal** | **none**]]

Syntax Description

component	Selects local debug logging on the components you want, where *component* can be any of the components described in the Usage Guidelines.
all	Selects local debug logging on all components.

Defaults

All debug logging is disabled.

Command Modes

ACS Configuration

Usage Guidelines

You can select any of the following as a component:

- runtime—If you select this component, all other runtime subcomponents are included; see *runtime-* items in the list below:
  - runtime-admin
  - runtime-authenticators
  - runtime-authorization
  - runtime-config-manager
  - runtime-config-notification-flow
  - runtime-customerlog
  - runtime-crypto
  - runtime-dataaccess
  - runtime-dbpassword
  - runtime-eap
  - runtime-event-handler
  - runtime-idstores
  - runtime-infrastructure
  - runtime-logging

  - runtime-logging-notification-flow
  - runtime-message-bus
  - runtime-message-catalog
  - runtime-radius
  - runtime-rule-engine
  - runtime-state-manager
  - runtime-tacacs
  - runtime-xml-config
- mgmt (management)—If you select this component, all other mgmt subcomponents are included; see *mgmt-* items in the list below:
  - mgmt-audit
  - mgmt-common
  - mgmt-aac
  - mgmt-bl
  - mgmt-cli
  - mgmt-gui
  - mgmt-system
  - mgmt-notification
  - mgmt-bus
  - mgmt-dbal
  - mgmt-replication
  - mgmt-distmgmt
  - mgmt-validation
  - mgmt-changepassword
  - mgmt-license
  - mgmt-acsview

Examples

```
acs/admin(config-acs)# no debug-log all
```

Related Commands

Command	Description
acs (instance)	Starts or stops an ACS instance.
acs (process)	Starts or stops an ACS process.
acs-config	Enters the ACS Configuration mode.
acs reset-config	Resets the ACS configuration to factory defaults.
acs support	Gathers information for troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
debug-log	Defines the local debug logging level for the ACS components.

Command	Description
replication force-sync	Synchronizes the secondary ACS database to the primary ACS database.
restore	Restores from backup the file contents of a specific repository.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).
show acs-logs	Displays ACS server debug logs.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

replication force-sync

To synchronize the ACS database (configuration information) of a secondary ACS with the database of the primary ACS, use the **replication force-sync** command in the ACS Configuration mode. Only the super admin or system admin can run this command on a secondary ACS node.

```
replication force-sync
```

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

ACS Configuration

Usage Guidelines

You can use this command only on a secondary ACS. If you use this command on the primary ACS, this message appears:

```
Replication synchronization must be done on a SECONDARY instance.
```

This command stops the ACS application, which remains unavailable for the duration of the synchronization process. The duration of the synchronization process depends on the size of the ACS database—it could take a significant amount of time to complete. Ensure that you use this command when you do not need to access your ACS.

ACS restarts after the primary-to-secondary synchronization is complete.

Examples

```
acs/admin(config-acs)# replication force-sync

Success.
```

Related Commands

Command	Description
acs (instance)	Starts or stops an ACS instance.
acs (process)	Starts or stops an ACS process.

Command	Description
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
debug-log	Enables debug logging for components.
export-data	Exports configuration data from an ACS local store to a remote repository.
restore	Restores the file contents of a specific repository from the backup.
show acs-logs	Displays ACS server debug logs.
show application	Displays application status and version information.
show version	Displays information about the software version of the system.

replication status

To check the **replication status** ACS database (configuration information), use the command replication status.

```
replication staus
```

Syntax Description No arguments or keywords.

Defaults None.

Command Modes ACS Configuration

Usage Guidelines You can use this command to check the replication status of the ACS database.

Examples

```
acs205/acsadmin(config-acs)# replication_status
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.

reset-management-interface-certificate

To reset the management interface certificate to a default self-signed certificate, use the **reset-management-interface-certificate** command in the ACS Configuration mode. Only the super admin and system admin can run this command.

```
reset-management-interface-certificate
```

Syntax Description

No arguments or keywords.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

run this command when you assign an invalid GUI certificate for the management interface and your login to ACS GUI is denied, or when you want to reset the existing management interface certificate to the default self-signed certificate.

When you run this command, the ACS server performs the following process:

1. For first-time management interface certificate reset:
   a. Disconnects the association of the invalid certificate with the management interface.

      The disconnected invalid certificate remains in the database.

   b. Creates a new self-signed certificate with the subject name *host***--reset**.

   c. Associates the new self-signed certificate with the management interface.
2. For subsequent resets (for an existing certificate with the subject name *host***--reset**):
   a. Disconnects all the associations (the management interface, external policy server, and EAP server associations from the invalid certificate).

b. Creates a new self-signed certificate with the subject name *host***--reset**.

c. Associates the new self-signed certificate with the management interface and establishes the connections between the new certificate and external policy and EAP servers.

In the subject name of the certificate *host***--reset**, *host* refers to the ACS server name. If the hostname is lnx-01, then the certificate's subject name would be lnx-01--reset.

Examples

Example 1 – Success

```
acs/admin(config-acs)# reset-management-interface-certificate

Resetting ACS Management Interface Certificate...
Management Interface Certificate Reset Completed.
acs/admin(config-acs)#
```

Example 2 – Failure

```
acs/admin(config-acs)# reset-management-interface-certificate

Resetting ACS Management Interface Certificate...
Failed to Reset Management Interface Certificate.
See the logs for more details
acs/admin(config-acs)#
```

show ad-agent-configuration

This command prints the lines of the Centrify configuration file that contain the given parameter name.

show-ad-agent-configuration *parameter-name*

Syntax Description

parameter-name	Holds the parameter name that is used in the the Centrify configuration file.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

You can use this command to query for the lines that contain the given parameter name. When you query for a specific parameter, all the instances in the file that contain the given parameter name are displayed in the output.

Examples

```
cd-acs5-13-74/acsadmin(config-acs)# show ad-agent-configuration
adclient.get.builtin.membership
#adclient.get.builtin.membership: false
# adclient.get.builtin.membership: false
```

show ad-agent-configuration-changes

This command prints all the configuration changes that are made (local or distribute) in a node of a particular deployment.

show-ad-agent-configuration-changes

Syntax Description

None.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

You can use this command to query the configuration changes that are made in primary or secondary nodes, which should be part of the deployment. When you execute this command from a primary node, it lists all the configuration changes that are made in the primary and all the associated secondary nodes of the deployment. Whereas, when you execute the same command from a secondary node, it lists the configration changes that are made only on the particular node (local or distribute).

Examples

Example 1 Run from a Primary node

```
acs149/acsadmin(config-acs)# show ad-agent-configuration-changes
Loading the AD Agent Configuration made for the primary node acs149...
-------------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:23
localparam 90            N/A           local       acs149   2012-09-17 07:15:23
-------------------------------------------------------------------------------------------

Loading the AD Agent Configuration changes made for the secondary node ACS136...
-------------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:22
localparam 58            N/A           local       ACS136   2012-09-17 12:16:38
-------------------------------------------------------------------------------------------
acs149/acsadmin(config-acs)#
```

Example 2 Run from a Secondary node

```
ACS136/acsadmin(config-acs)# show ad-agent-configuration-changes
Loading the AD Agent Configuration made for the secondary node ACS136...
-------------------------------------------------------------------------------------------
Key        CurrentValue  DefaultVAlue  mode        node_id  ModifiedDate
distparam  89            N/A           distribute  acs149   2012-09-17 07:08:23
localparam 58            N/A           local       ACS136   2012-09-17 12:16:38
-------------------------------------------------------------------------------------------
ACS136/acsadmin(config-acs)#
```

show debug-adclient

To display the debug logging status for an Active Directory client, use the **show debug-adclient** command in the ACS Configuration mode. Any user, irrespective of role, can run this command.

```
show debug-adclient
```

Syntax Description No arguments or keywords.

Defaults Disabled.

Command Modes ACS Configuration

Usage Guidelines None.

Examples

```
acs/admin(config-acs)# show debug-adclient
Active Directory client debug is disabled
```

Related Commands

Command	Description
debug-adclient	Enables debug logging for an Active Directory client.
no debug-adclient	Disables debug logging for an Active Directory client.
debug-log	Defines the local debug logging level for the ACS components.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).

show debug-log

To display the local debug logging status for all components or for specific ACS components, use the **show debug-log** command in the ACS Configuration mode. Any user, irrespective of role, can run this command.

show debug-log [*component* | **all**]

Syntax Description

component	Selects local debug logging on the components you want, where *component* can be any of the components described in the Usage Guidelines.
all	Displays the currently configured local debug logging status for all components.

Defaults All ACS debug logging is set to warn.

Command Modes ACS Configuration

Usage Guidelines You can select any of the following (including the suboptions) as a component:

- runtime—If you select this component, all other runtime subcomponents are included; see *runtime-* items in the list below:
  - runtime-admin
  - runtime-authenticators
  - runtime-authorization
  - runtime-config-manager
  - runtime-config-notification-flow
  - runtime-customerlog
  - runtime-crypto
  - runtime-dataaccess
  - runtime-dbpassword
  - runtime-eap
  - runtime-event-handler
  - runtime-idstores
  - runtime-infrastructure
  - runtime-logging
  - runtime-logging-notification-flow
  - runtime-message-bus
  - runtime-message-catalog
  - runtime-radius
  - runtime-rule-engine
  - runtime-state-manager
  - runtime-tacacs
  - runtime-xml-config
- mgmt (management)—If you select this component, all other mgmt subcomponents are included; see *mgmt-* items in the list below:
  - mgmt-audit
  - mgmt-common
  - mgmt-aac
  - mgmt-bl
  - mgmt-cli
  - mgmt-gui
  - mgmt-system
  - mgmt-notification

- mgmt-bus
- mgmt-dbal
- mgmt-replication
- mgmt-distmgmt
- mgmt-validation
- mgmt-changepassword
- mgmt-license
- mgmt-acsview

Examples

```
ACS/admin(config-acs)# sh debug-log mgmt
mgmt                          warn
mgmt-acsview                  warn

ACS/admin(config-acs)# sh debug-log runtime
runtime                       warn

ACS/admin(config-acs)# sh debug-log mgmt-acsview
mgmt-acsview                  warn
```

Related Commands

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.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs support	Gathers information for ACS troubleshooting.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
debug-log	To set the local debug logging level for all or specific ACS components.
export-data	Exports configuration data from an ACS local store to a remote repository.
restore	Restores the file contents of a specific repository from the backup.
show acs-logs	Displays ACS server debug logs.
show application	Displays application status and version information.
show version	Displays information about the software version of the system.

database-compress

To reduce the ACS database size by removing unused disk space from within the ACS database file, use the **database-compress** command in the ACS Configuration mode. This command has the option to truncate ACS transaction history.

This command does not erase or modify any information during the database compression, except for the transaction history if the truncate flag is used.

When you run this command, ACS is stopped, and the process of compressing the ACS database is executed. ACS starts automatically after the process is done.

The progress of the command execution is logged in the ADE.log file.

```
database-compress [truncate_log]
```

Syntax Description

truncate_log	Truncates the transaction history.

Defaults

None.

Command Modes

ACS Configuration

Usage Guidelines

None.

Examples

```
acs/admin(config-acs)# database-compress
```

Related Commands

Command	Description
debug-adclient	Enables debug logging for an Active Directory client.
no debug-adclient	Disables debug logging for an Active Directory client.
debug-log	Defines the local debug logging level for the ACS components.
show debug-adclient	Shows the debug log level status for subsystems (enabled or disabled).

Configuration Commands

Each Configuration command includes a brief description of its use, command syntax, usage guidelines, and sample output.

Configuration commands include **interface** and **repository**.

Note Some of the Configuration commands require you to enter the configuration submode to complete the command configuration.

To access the Configuration mode, you must use the **configure** command in the EXEC mode.

Table 3-18 lists the Configuration commands that are described in this section.

Table 3-18 List of Configuration Commands

• backup-staging-url	• ip name-server
• cdp holdtime	• ip route
• cdp run	• ipv6 route
• cdp timer	• kron occurrence
• clock timezone	• kron policy-list
• do	• logging
• end	• ntp server
• exit	• password-policy
• host-key sync	• repository
• hostname	• service
• icmp echo	• snmp-server community
• interface	• snmp-server contact
• ip address	• snmp-server host
• ipv6 address	• snmp-server location
• ip default-gateway	• username
• ip domain-name	

backup-staging-url

To allow you to configure a Network File System (NFS) location that backup and restore operations will use as a staging area to package and unpackage backup files, use the **backup-staging-url** command in Configuration mode.

backup-staging-url *word*

Syntax Description

word	NFS URL for staging area. This can be a maximum of 2048 alphanumeric characters. Use **nfs://***server***:***path*[1].

1. Server is the server name and path refers to /subdir/subsubdir. Remember that a colon (:) is required after the server.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The URL is NFS only. The format of the command is **backup-staging-url nfs://***server***:***path*.

Warning **Ensure that you secure your NFS server in such a way that the directory can be accessed only by the IP address of the ACS server.**

Examples

```
acs/admin(config)# backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
acs/admin(config)#
```

cdp holdtime

To specify the amount of time for which the receiving device should hold a CDP packet from the ACS server before discarding it, use the **cdp holdtime** command in the Configuration mode. To revert to the default setting, use the **no** form of this command.

cdp holdtime *seconds*

Syntax Description

seconds	Specifies the hold time, in seconds. Value from 10 to 255 seconds.

Defaults

180 seconds

Command Modes

Configuration

Usage Guidelines

CDP packets transmit with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

The **cdp holdtime** command takes only one argument; otherwise, an error occurs.

Examples

```
acs/admin(config)# cdp holdtime 60
acs/admin(config)#
```

Related Commands

Command	Description
cdp timer	Specifies how often the ACS server sends CDP updates.
cdp run	Enables the CDP.

cdp run

To enable the CDP, use the **cdp run** command in Configuration mode. To disable the CDP, use the **no** form of this command.

```
cdp run [GigabitEthernet]
```

Syntax Description

GigabitEthernet	Specifies the GigabitEthernet interface on which to enable CDP.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The command has one optional argument, an interface name. Without an optional interface name, the command enables CDP on all interfaces.

Note The default for this command is on interfaces that are already up and running. When you are bringing up an interface, stop CDP first; then, start CDP again.

Examples

```
acs/admin(config)# cdp run GigabitEthernet 0
acs/admin(config)#
```

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a CDP packet from the ACS server before discarding it.
cdp timer	Specifies how often the ACS server sends CDP updates.

cdp timer

To specify how often the ACS server sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in Configuration mode. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

Syntax Description

seconds	Specifies how often, in seconds, the ACS server sends CDP updates. Value from 5 to 254 seconds.

Defaults

60 seconds

Command Modes

Configuration

Usage Guidelines

CDP packets transmit with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

The **cdp timer** command takes only one argument; otherwise, an error occurs.

Examples

```
acs/admin(config)# cdp timer 60
acs/admin(config)#
```

Related Commands

Command	Description
cdp holdtime	Specifies the amount of time that the receiving device should hold a CDP packet from the ACS server before discarding it.
cdp run	Enables CDP.

clock timezone

To set the time zone, use the **clock timezone** command in Configuration mode. To disable this function, use the **no** form of this command.

clock timezone *timezone*

Syntax Description

timezone	Name of the time zone visible when in standard time. This can be a maximum of 64 alphanumeric characters.

Defaults

UTC

Command Modes Configuration

Usage Guidelines The system internally keeps time in UTC. If you do not know your specific time zone, you can enter the region, country, and city (see Tables 3-19, 3-20, and 3-21 for sample time zones to enter on your system).

Table 3-19 Common Time Zones

Acronym or name	Time Zone Name
Europe	
GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu	Greenwich Mean Time, as UTC
GB	British
GB-Eire, Eire	Irish
WET	Western Europe Time, as UTC
CET	Central Europe Time, as UTC + 1 hour
EET	Eastern Europe Time, as UTC + 2 hours
United States and Canada	
EST, EST5EDT	Eastern Standard Time, as UTC -5 hours
CST, CST6CDT	Central Standard Time, as UTC -6 hours
MST, MST7MDT	Mountain Standard Time, as UTC -7 hours
PST, PST8PDT	Pacific Standard Time, as UTC -8 hours
HST	Hawaiian Standard Time, as UTC -10 hours

Table 3-20 Australia Time Zones

Australia[1]			
ACT[2]	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHI[3]	Melbourne
North	NSW[4]	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

1. Enter the country and city together with a forward slash (/) between them; for example, Australia/Currie.
2. ACT = Australian Capital Territory.
3. LHI = Lord Howe Island
4. NSW = New South Wales

Table 3-21 Asia Time Zones

Asia[1]			
Aden[2]	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

1. The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia.
2. Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

Note Several more time zones are available to you. On your ACS server, enter **show timezones**. A list of all the time zones available in the ACS server appears. Choose the most appropriate one for your time zone.

Examples

```
acs/admin(config)# clock timezone EST
Time zone was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no)
Stopping ACS ..................
Starting ACS ......................

acs/admin(config)# exit
acs/admin# show timezone
EST
acs/admin#
```

Related Commands

Command	Description
show timezones	Displays a list of available time zones on the system.
show timezone	Displays the current time zone set on the system.

do

To execute an EXEC-level command from Configuration mode or any configuration submode, use the **do** command in any configuration mode.

do *arguments*

Syntax Description

arguments	The EXEC command to execute (see Table 3-22).

Table 3-22 Command Options for Do Command

Command	Description
acs backup	Performs a backup of an ACS configuration.
acs-config	Enters the ACS Configuration mode.
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	Performs a restoration of an ACS configuration.
acs start	Starts an ACS instance.
acs stop	Stops an ACS instance.
acs support	Gathers information for ACS troubleshooting.
application install	Installs a specific application.
application remove	Removes a specific application.
application start	Starts or enables a specific application
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application.
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
backup-logs	Performs a backup of all the logs on the ACS server to a remote location.
clock	Sets the system clock on the ACS server.
configure	Enters Configuration mode.
copy	Copies any file from a source to a destination.
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 on the ACS server.
dir	Lists files on the ACS server.
forceout	Forces the logout of all the sessions of a specific ACS node user.
halt	Disables or shuts down the ACS server.

Table 3-22 Command Options for Do Command (continued)

Command	Description
help	Describes the help utility and how to use it on the ACS server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 address or hostname of a remote system.
ping	Determines the network activity on a remote system.
reload	Reboots the ACS server.
restore	Performs a restore and retrieves the backup out of a repository.
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.
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.

Command Default

No default behavior or values.

Command Modes

Configuration or any configuration submode

Usage Guidelines

Use this command to execute EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your server. After the EXEC command executes, the system will return to the configuration mode you were using.

Examples

```
acs/admin(config)# do show run
Generating configuration...
!
hostname ems-lnx106
ip domain-name cisco.com
interface ethernet 0
  ip address 209.165.200.225 255.255.255.224
interface ethernet 1
```

```
  shutdown
ip name-server 209.165.201.1
ip default-gateway 209.165.202.129
clock timezone Cuba
!
!
username admin password hash $1$hB$MxIZHvecMiey/P9mM9PvN0 role admin
!
!
logging localhost
logging loglevel 6
!
acs/admin(config)#
```

end

To end the current configuration session and return to the EXEC mode, use the **end** command in Configuration mode.

end

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

This command brings you back to EXEC mode regardless of what configuration mode or submode you are in.

Use this command when you finish configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

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

Related Commands

Command	Description
exit	Exits Configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the ACS server.

exit

To exit any configuration mode to the next-highest mode in the CLI mode hierarchy, use the **exit** command in Configuration mode.

```
exit
```

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes Configuration

Usage Guidelines The **exit** command is used in the ACS server to exit the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in Configuration mode to return to the EXEC mode. Use the **exit** command in the configuration submodes to return to Configuration mode. At the highest level, EXEC mode, the **exit** command exits the EXEC mode and disconnects from the ACS server (see exit, page 3-49 for a description of the **exit** [EXEC] command).

Examples

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

Related Commands

Command	Description
end	Exits Configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the ACS server.

host-key sync

To sync the SSH keys for an SFTP repository between ACS and an SFTP server, use the **host-key sync** command.

```
host-key sync
```

Syntax Description No arguments or keywords.

Defaults None.

Command Modes Configuration

Usage Guidelines None.

Examples

```
acs/admin(config)# repository new
acs/admin(config-Repository)# url sftp://starwars.test.com/repository/system1
acs/admin(config-Repository)# user luke password skywalker
acs/admin(config-Repository)# host-key sync
acs/admin(config)#
```

Related Commands

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Restores the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

hostname

To set the hostname of the system, use the **hostname** command in Configuration mode. To delete the hostname from the system, use the **no** form of this command. This resets the system to localhost.

hostname *word*

Syntax Description

word	Name of the host. Contains at least 2 to 64 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.

Defaults No default behavior or values.

Command Modes Configuration

Usage Guidelines A single instance type of command, **hostname** only occurs once in the configuration of the system. The hostname must contain one argument; otherwise, an error occurs.

Examples

```
acs/admin(config)# hostname myserver-1
Hostname was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS ......................
Starting ACS ....
```

```
To verify that ACS processes are running, use the
'show application status acs' command.

myserver-1/admin(config)#
```

icmp echo

To configure the Internet Control Message Protocol (ICMP) echo responses, use the **icmp echo** command in Configuration mode.

```
icmp echo {off | on}
```

Syntax Description

echo	Configures ICMP echo response.
off	Disables ICMP echo response
on	Enables ICMP echo response.

Defaults

The system will behave as if the ICMP echo response is on (enabled).

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
acs/admin(config)# icmp echo off
acs/admin(config)#
```

Related Commands

Command	Description
show icmp_status	Display ICMP echo response configuration information.

interface

To configure an interface type and enter the interface configuration mode, use the **interface** command in Configuration mode. This command does not have a **no** form.

```
interface GigabitEthernet [0 | 1]
```

Syntax Description

GigabitEthernet	Configures the Gigabit Ethernet interface.
0 | 1	Number of the Gigabit Ethernet port to configure.

Note After you enter the Gigabit Ethernet port number in the **interface** command, you enter the config-GigabitEthernet configuration submode (see the following Syntax Description).

do	EXEC command. Allows you to perform any EXEC commands in this mode (see do, page 3-145).
end	Exits the config-GigabitEthernet submode and returns you to the EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets the IP address and netmask for the Ethernet interface (see ip address, page 3-151).
no	Negates the command in this mode. Two keywords available: • ip—Sets the IP address and netmask for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface (see shutdown, page 3-60).

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

You can use this command to configure subinterfaces to support various requirements.

Examples

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

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown, page 3-60).

ip address

To set the IP address and netmask for the Ethernet interface, use the **ip address** command in interface Configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address netmask*

Note You can configure the same IP address on multiple interfaces. You might want to do this to limit the configuration steps required to switch from using one interface to another.

Syntax Description

ip-address	IPv4 version IP address.
netmask	Mask of the associated IP subnet.

Defaults

Enabled.

Command Modes

Interface configuration

Usage Guidelines

Requires exactly one address and one netmask; otherwise, an error occurs.

Examples

```
acs/admin(config)# interface GigabitEthernet 1
acs/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
IP Address was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS ......................
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
acs/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
shutdown (interface configuration mode)	Disables an interface (see shutdown, page 3-60).
ip default-gateway	Sets the IP address of the default gateway of an interface.
show interface	Displays information about the system IP interfaces.
interface	Configures an interface type and enters the interface mode.

ipv6 address

To set the IPv6 address and prefix length for the Ethernet interface, use the ipv6 address command in interface Configuration mode. To remove an IPv6 address or disable IPv6 processing, use the no form of this command.

ipv6 address *ip-address/prefix*

Note You can configure the same IPv6 address on multiple interfaces. You might want to do this to limit the configuration steps required to switch from using one interface to another.

Syntax Description

ip-address	IPv6 version IP address.
prefix	Prefix of ipv6 address.

Defaults

Enabled.

Command Modes

Interface configuration

Usage Guidelines

Requires exactly one address and one prefix; otherwise, an error occurs.

Examples

```
ACS154/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
acs/admin(config)# interface GigabitEthernet 0
acs/admin(config-GigabitEthernet)# ipv6 address 1901::20c:29ff:feb8:e4c/64
Changing the IPV6 address may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
IP Address was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS.
Stopping Management and
View.....................................................
Stopping Runtime.....................
Stopping Database.............
Stopping Ntpd.........................
Cleanup..
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
acs/admin(config-GigabitEthernet)
```

Related Commands

Command	Description
shutdown (interface configuration mode)	Disables an interface (see shutdown, page 3-60).
ip default-gateway	Sets the IP address of the default gateway of an interface.
show interface	Displays information about the system IP interfaces.
interface	Configures an interface type and enters the interface mode.

ip default-gateway

To define or set a default gateway with an IP address, use the **ip default-gateway** command in Configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the default gateway.

Defaults

Disabled.

Command Modes

Configuration

Usage Guidelines

If you enter more than one argument or no arguments at all, an error occurs.

Examples

```
acs/admin(config)# ip default-gateway 209.165.202.129
acs/admin(config)#
```

Related Commands

Command	Description
ip address(interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.

ip domain-name

To define a default domain name that the ACS server uses to complete hostnames, use the **ip domain-name** command in Configuration mode. To disable this function, use the **no** form of this command.

ip domain-name *word*

Syntax Description

word	Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.

Defaults

Enabled.

Command Modes

Configuration

Usage Guidelines If you enter more or fewer arguments, an error occurs.

Examples

```
acs/admin(config)# ip domain-name cisco.com
acs/admin(config)#
```

Related Commands

Command	Description
ip name-server	Sets the DNS servers for use during a DNS query.

ip name-server

To set the Domain Name Server (DNS) servers for use during a DNS query, use the **ip name-server** command in Configuration mode. You can configure one to three DNS servers. To disable this function, use the **no** form of this command.

Note Using the **no** form of this command removes all the name servers from the configuration. Using the **no** form of this command and one of the IP names removes only that IP name.

ip name-server *ip-address* [*ip-address**]

Syntax Description

ip-address	Address of a name server.
*ip-address**	(Optional) IP addresses of additional name servers. **Note** You can configure a maximum of three name servers.

Defaults No default behavior or values.

Command Modes Configuration

Usage Guidelines The first name server added with the **ip name-server** command will occupy the first position and the system will first use that server in resolving the IP addresses.

You can add name servers to the system one at a time or all at once, until you reach the maximum (3). If you already configured the system with three name servers, you must remove at least one server to add additional name servers.

To place a name server in the first position so that the subsystem uses it first, you must remove all name servers with the **no** form of this command before you proceed.

Examples

```
acs/admin(config)# ip name-server 209.165.201.1
Name Server was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS ......................
```

```
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
acs/admin(config)#
```

You can choose not to restart the ACS server; nevertheless, the changes will take effect.

Related Commands

Command	Description
ip domain-name	Defines a default domain name that the ACS server uses to complete hostnames.

ip route

To configure the static routes, use the **ip route** command in Configuration mode. To remove static routes, use the **no** form of this command.

Static routes are manually configured. This makes them inflexible (they cannot dynamically adapt to network topology changes) but extremely stable. Static routes optimize bandwidth utilization, because no routing updates need to be sent to maintain them. They also make it easy to enforce routing policy.

The **ipv6 route** command is meant for adding only the IPv6 default gateway. ACS acts as end host, hence, adding multiple static routes is not supported

ip route *prefix mask* **gateway** *ip-address*

no ip route *prefix mask*

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.

Defaults

No default behavior or values.

Command Modes

Configuration.

Examples

```
acs/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
```

ipv6 route

To configure the static IPv6 routes, use the **ipv6 route** command in Configuration mode. To remove static routes, use the **no** form of this command.

The **ipv6 route** command is meant for adding only the IPv6 default gateway. ACS acts as end host, hence, adding multiple static routes is not supported

ipv6 route *prefix mask* **gateway** *ip-address*

no ipv6 route *prefix mask*

Syntax Description

prefix	IPv6 route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IPv6 address of the next hop that can be used to reach that network.

Defaults

No default behavior or values.

Command Modes

Configuration.

Examples

```
acs/admin(config)# ipv6 route 2001::/64 gateway 2001::212:44ff:fe30:bc0a
acs/admin(config)#
```

kron occurrence

To schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level, use the **kron occurrence** command in Configuration mode. To delete this, use the **no** form of this command.

kron {**occurrence**} *occurrence-name*

Syntax Description

occurrence	Schedules Command Scheduler commands.
occurrence-name	Name of the occurrence. This can be a maximum of 80 alphanumeric characters. (See following note and Syntax Description.)

Note After you enter the *occurrence-name* in the **kron occurrence** command, you enter the config-occurrence configuration submode (see the following Syntax Description).

at	Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*].
do	EXEC command. Allows you to perform any EXEC commands in this mode (see do, page 3-145).
end	Exits the kron-occurrence configuration submode and returns you to the EXEC mode.
exit	Exits the kron-occurrence configuration mode.
no	Negates the command in this mode. Three keywords available: • at—Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*]. • policy-list—Specifies a policy list to be run by the occurrence. This can be a maximum of 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated.
policy-list	Specifies a Command Scheduler policy list to be run by the occurrence.
recurring	Identifies that the occurrences run on a recurring basis.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC CLI commands to be scheduled to run on the ACS server at a specified time. See kron policy-list, page 3-159.

Examples

Note When you run the **kron** command, support bundles are downloaded with a unique name (by adding a time stamp), to ensure that the files do not overwrite each other.

```
acs/admin(config)# kron occurrence daily_occurrence
acs/admin(config-Occurrence)# at 14:35
acs/admin(config-Occurrence)# policy-list daily_support
acs/admin(config-Occurrence)# recurring
acs/admin(config-Occurrence)# exit
acs/admin(config)#
```

Related Commands

Command	Description
kron policy-list	Specifies a name for a Command Scheduler policy.
acs backup	Backs up an ACS configuration.

kron policy-list

To specify a name for a Command Scheduler policy and enter the kron-Policy List configuration submode, use the **kron policy-list** command in Configuration mode. To delete this, use the **no** form of this command.

kron {**policy-list**} *list-name*

Syntax Description

policy-list	Specifies a name for Command Scheduler policies.
list-name	Name of the policy list. This can be a maximum of 80 alphanumeric characters.

Note After you enter the *list-name* in the **kron policy-list** command, you enter the config-Policy List configuration submode (see the following Syntax Description).

cli	Command to be executed by the scheduler. This can be a maximum of 80 alphanumeric characters.
do	EXEC command. Allows you to perform any EXEC commands in this mode (see do, page 3-145).
end	Exits from the config-Policy List configuration submode and returns you to the EXEC mode.
exit	Exits this submode.
no	Negates the command in this mode. One keyword available: • cli–Command to be executed by the scheduler.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC CLI commands to be scheduled to run on the ACS server at a specified time. Use the **kron occurrence** and **policy list** commands to schedule one or more policy lists to run at the same time or interval. See kron occurrence, page 3-157.

Examples

```
acs/admin(config)# kron policy-list daily_support
acs/admin(config-Policy List)# cli acs support acssupport repository local
encryption-passphrase null
acs/admin(config-Policy List)# exit
acs/admin(config)#
```

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters the config-Occurrence configuration mode.

logging

To enable the system to forward logs to a remote system or to configure the log level, use the **logging** command in Configuration mode. To disable this function, use the **no** form of this command.

logging {*ip-address* | *hostname*} {**loglevel** *level*}

Syntax Description

ip-address	IP address of remote system to which you forward logs. This can be a maximum of 32 alphanumeric characters.
hostname	Hostname of remote system to which you forward logs. This can be a maximum of 32 alphanumeric characters.
loglevel	Configures the log level for the **logging** command.
level	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0-emerg—Emergencies: System unusable. • 1-alert—Alerts: Immediate action needed. • 2-crit—Critical: Critical conditions. • 3-err—Error: Error conditions. • 4-warn—Warning: Warning conditions. • 5-notif—Notifications: Normal but significant conditions. • 6-inform—Informational messages. Default. • 7-debug—Debugging messages.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

This command requires an IP address or hostname or the **loglevel** keyword; an error occurs if you enter two or more of these arguments.

Examples

Example 1

```
acs/admin(config)# logging 209.165.200.225
acs/admin(config)#
```

Example 2

```
acs/admin(config)# logging loglevel 0
acs/admin(config)#
```

Related Commands

Command	Description
show logging	Displays list of logs for the system.

ntp server

To allow for software clock synchronization by the Network Time Protocol (NTP) server for the system, use the **ntp server** command in Configuration mode. Allows up to two servers. To disable this capability, use the **no** form of this command.

ntp server {*ip-address* | *hostname*} [*ip-address* | *hostname*]

Syntax Description

ip-address | *hostname*	IP address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters.

Defaults

No servers are configured by default.

Command Modes

Configuration

Usage Guidelines

Use this command if you want to allow the system to synchronize with a specified server.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords or arguments.

For example, if you previously ran the **ntp server** command and you now want to remove not only the server synchronization capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions disable and that the NTP service also terminates.

Note This command will give conflicting information during the sync process. The sync process can take up to 20 minutes to complete.

Examples

```
acs/admin(config)# ntp server 209.165.201.31
NTP Server was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS ......................
```

```
Starting ACS ......................

To verify that ACS processes are running, use the
'show application status acs' command.
acs/admin(config)#
```

Related Commands	Command	Description
	show ntp	Displays the status information about the NTP associations.

password-policy

To enable or configure the passwords on the system, use the **password-policy** command in Configuration mode. To disable this function, use the **no** form of this command.

password-policy *option*

Note The **password-policy** command requires a policy option (see Syntax Description).

You must enter the **password-expiration-enabled** command before the other password-expiration commands.

Syntax Description

Note After you enter the **password-policy** command, you enter the config-password-policy configuration submode.

digit-required	Requires a digit in the password.
disable-repeat-characters	Disables the password's ability to contain more than four identical characters.
disable-cisco-password	Disables the ability to use the word Cisco or any combination as the password.
lower-case-required	Requires a lowercase letter in the password.
min-password-length	Specifies a minimum number of characters for a valid password. Integer length from 0 to 4,294,967,295.
no-previous-password	Prevents users from reusing a part of their previous password.
no-username	Prohibits users from reusing their username as a part of a password.
password-expiration-days	Number of days until a password expires. Integer length from 0 to 80.
password-expiration-enabled	Enables password expiration. **Note** You must enter the **password-expiration-enabled** command before the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiration begin. Integer length from 0 to 4,294,967,295.

password-lock-enabled	Locks a password after several failures.
password-lock-retry-count	Number of failed attempts before password locks. Integer length from 0 to 4,294,967,295.
upper-case-required	Requires an uppercase letter in the password.
special-required	Requires a special character in the password.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
acs/admin(config)# password-policy
acs/admin(config-password-policy)# password-expiration-days 30
acs/admin(config-password-policy)# exit
acs/admin(config)#
```

repository

To enter the repository submode for configuration of backups, use the **repository** command in Configuration mode.

repository *repository-name*

Syntax Description

repository-name	Name of repository. This can be a maximum of 80 alphanumeric characters.

Note After you enter the name of the repository in the **repository** command, you enter the config-Repository configuration submode (see the Syntax Description).

do	EXEC command. Allows you to perform any of the EXEC commands in this mode (see do, page 3-145).
end	Exits the config-Repository mode and returns you to the EXEC mode.
exit	Exits this mode.
no	Negates the command in this mode. Two keywords available: • url—Repository URL. • user—Repository username and password for access.

url	URL of the repository. This can be a maximum of 80 alphanumeric characters (see Table 3-23).
user	Configure username and password for access. This can be a maximum of 30 alphanumeric characters.

Table 3-23 URL Keywords

Keyword	Source of Destination
word	Enter repository URL, including server and path info. This can be a maximum of 80 alphanumeric characters.
cdrom:	Local CD-ROM drive (read only).
disk:	Local storage. All local repositories are created on the /localdisk partition. When you specify disk:// in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered **disk://backup,** the directory is created at /localdisk/backup. You can run the **show repository** *repository_name* to view all the files in the local repository.
ftp:	Source or destination URL for an FTP network server. Use url ftp://*server/path*[1].
nfs:	Source or destination URL for an NFS network server. Use url nfs://*server:path*[1].
sftp:	Source or destination URL for an SFTP network server. Use url sftp://*server/path*[1].
tftp:	Source or destination URL for a TFTP network server. Use url tftp://*server/path*[1]. **Note** You cannot use a TFTP repository for performing ACS upgrade.

1. Server is the server name and path refers to /subdir/subsubdir. Remember that a colon (:) is required after the server for an NFS network server.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

In ACS 5.1/5.2, when you create an SFTP repository using the url sftp*://server/path* and use the "root" username, the backup that you take gets stored in the *root/path* directory of this repository.

ACS 5.4 uses the absolute path, and for the same commands, the backup is stored in the */path* directory. You should have permission to access this directory.

Note If you restore an ACS 5.1 ADE OS backup on ACS 5.4, the SFTP repositories that are created in ACS 5.1 do not work in ACS 5.4 because of this change in behavior.

You must use the absolute path to fetch the backup file. For windows SFTP server, the virtual path "/" should be mapped to any of the folders in the windows drive.

Examples

```
acs/admin(config)# repository myrepository
acs/admin(config-Repository)# url sftp://starwars.test.com/repository/system1
acs/admin(config-Repository)# user luke password plain skywalker
acs/admin(config-Repository)# exit
acs/admin(config)# exit
acs/admin # write memory
Generating Configuration...
acs/admin #
```

Related Commands

Command	Description
backup	Performs a backup (ACS and ADE OS) and places the backup in a repository.
restore	Performs a restore and takes the backup out of a repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

service

To specify a service to manage, use the **service** command in Configuration mode. To disable this function, use the **no** form of this command.

service sshd

Syntax Description

sshd	Secure Shell Daemon. The daemon program for SSH.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
acs/admin(config)# service sshd
acs/admin(config)#
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in Configuration mode. To disable this function, use the **no** form of this command.

snmp-server community *word* **ro**

Syntax Description

word	Accessing string that functions much like a password, allowing access to SNMP. No blank spaces allowed. This can be a maximum of 255 alphanumeric characters.
ro	Specifies read-only access.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The **snmp-server community** command requires a community string and the **ro** argument; otherwise, an error occurs.

Examples

```
acs/admin(config)# snmp-server community new ro
acs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server contact

To configure the SNMP contact MIB value on the system, use the **snmp-server contact** command in Configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *word*

Syntax Description

word	String that describes the system contact information of the node. This can be a maximum of 255 alphanumeric characters.

Defaults No default behavior or values.

Command Modes Configuration

Usage Guidelines None.

Examples

```
acs/admin(config)# snmp-server contact Luke
acs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to the SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.

snmp-server host

To send SNMP traps to a remote user, use the **snmp-server host** command in Configuration mode. To remove trap forwarding, use the **no** form of this command. This command does not display any output on the CLI.

snmp-server host {*ip-address* | *hostname*} **version** {**1** | **2c**} *community*

Syntax Description

ip-address	IP address of the SNMP notification host. This can be a maximum of 32 alphanumeric characters.
hostname	Name of the SNMP notification host. This can be a maximum of 32 alphanumeric characters.
version {1 | 2c}	(Optional) Version of the SNMP used to send the traps. Default = 1. If you use the version keyword, specify one of the following keywords: • 1—SNMPv1. • 2c—SNMPv2C.
community	Password-like community string that is sent with the notification operation.

Defaults Disabled.

Command Modes Configuration

Usage Guidelines The command takes arguments as listed; otherwise, an error occurs.

Examples

```
acs/admin(config)# snmp-server community new ro 10
acs/admin(config)# snmp-server host 209.165.202.129 version 1 password
acs/admin(config)#
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server location

To configure the SNMP location MIB value on the system, use the **snmp-server location** command in Configuration mode. To remove the system location information, use the **no** form of this command.

snmp-server location *word*

Syntax Description

word	String that describes the system's physical location information. This can be a maximum of 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Cisco recommends that you use underscores (_) or hyphens (-) between the terms within the *word* string. If you use spaces between terms within the *word* string, you must enclose the string in quotation marks (").

Examples

Example 1

```
acs/admin(config)# snmp-server location Building_3/Room_214
acs/admin(config)#
```

Example 2

```
acs/admin(config)# snmp-server location "Building 3/Room 214"
acs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server contact	Configures the SNMP location MIB value on the system.

username

To add a user who can access the CSACS-1121 or Cisco SNS-3415 using SSH, use the **username** command in Configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** *email-address*]] [**email** *email-address*]

For an existing user, use the following option:

username *username* **password role** {**admin** | **user**} *password*

Syntax Description

username	Only one word for the username argument. Blank spaces and quotation marks (“) are not allowed. This can be a maximum of 31 alphanumeric characters.
password *password*	Password character length This can be a maximum of 40 alphanumeric characters. You must specify the password for all new users.
hash | plain	Type of password. This can be a maximum of 34 alphanumeric characters.
role admin | user	Sets the privilege level for the user.
disabled	Disables the user according to the user’s e-mail address.
email *email-address*	The user’s e-mail address. For example, *user1@mydomain.com*.

Defaults

The initial user during setup.

Command Modes

Configuration

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Examples

Example 1

```
acs/admin(config)# username admin password hash ###### role admin
acs/admin(config)#
```

Example 2

```
acs/admin(config)# username admin password plain Secr3tp@swd role admin
acs/admin(config)#
```

Example 3

```
acs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@mydomain.com
acs/admin(config)#
```

Related Commands

Command	Description
password-policy	Enables and configures the password policy.
show users	Displays a list of users and their privilege level. It also displays a list of logged-in users.

GLOSSARY

A

ACS Access Control System.

ADE Application Deployment Engine.

C

CDP Cisco Discovery Protocol. A proprietary tool that network administrators use to access a summary of protocol and address information about other devices that are directly connected to the device initiating the command.

CDP runs over the data-link layer connecting the physical media to the upper-layer protocols. Because CDP operates at this level, two or more CDP devices that support different network layer protocols (for example, IP and Novell IPX) can learn about each other.

Physical media supporting the Subnetwork Access Protocol (SNAP) encapsulation connect CDP devices. These can include all LANs, Frame Relay, and other WANs, and ATM networks.

Cisco Discovery Protocol *See* CDP.

CLI Command-line interface. An interface through which the user can interact with the software operating system by entering commands and optional arguments.

client Node or software program that requests services from a server. For example, the Secure Shell (SSH) client. *See also* server.

command-line interface *See* CLI.

community string A text string that acts as a password, which is used to authenticate messages sent between a management station and an IP Transfer Point (ITP) containing a SNMP agent. The community string sends in every packet between the manager and the agent.

D

DNS Domain Name System. DNS associates various sorts of information with so-called domain names; most importantly, it serves as the "phone book" for the Internet: it translates human-readable computer hostnames (for example, *en.wikipedia.org*) into the IP addresses that networking equipment needs for delivering information. It also stores other information, such as the list of mail exchange servers that accept e-mail for a given domain. In providing a worldwide keyword-based redirection service, the DNS is an essential component of contemporary Internet use.

DNS name Initial name of a node.

domain name The style of identifier—a sequence of case-insensitive ASCII labels separated by dots (.) (for example, *bbn.com.*)—defined for subtrees in the Internet DNS [R1034] and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

Domain Name System *See* DNS.

F

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

H

host Computer system on a network. Similar to the term node; except, that host usually implies a computer system, whereas node generally applies to any network system, including access servers and ITPs.

hostname The name of the operating system's server or computer that contains the major program files.

I

IP Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.

IP address 32-bit address assigned to hosts by using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and written as 4 octets separated by periods (.) (dotted-decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. For routing, the network and subnetwork numbers stay together, while the host number addresses an individual host within the network or subnetwork. A subnet mask extracts network and subnetwork information from the IP address.

M

MIB Management Information Base. A directory listing information used and maintained by a network's management protocol, such as SNMP.

N

name server A name server is a computer server that implements a name-service protocol. It will normally map a computer-usable identifier of a host to a human-usable identifier for that host. For example, a DNS server might translate the domain name *en.wikipedia.org* to the IP address 145.97.39.155.

Network Time Protocol *See* NTP.

NTP Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. NTP is designed particularly to resist the effects of variable latency (jitter).

NTP is one of the oldest Internet protocols still in use (since before 1985). NTP was originally designed by Dave Mills of the University of Delaware, who still maintains it, along with a team of volunteers.

NTP is not related to the much simpler DAYTIME (RFC 867) and TIME (RFC 868) protocols.

P

port In IP terminology, an upper-layer process that receives information from lower layers. Each numbered port associates with a specific process. For example, SMTP associates with port 25.

S

Secure Shell *See* SSH.

server An application or device that performs services for connected clients as part of a client-server architecture. A server application, as defined by RFC 2616 (HTTP/1.1), is "an application program that accepts connections in order to service requests by sending back responses." Server computers are devices designed to run such an application or applications, often for extended periods of time, with minimal human direction. Examples of servers include web servers, e-mail servers, and file servers.

See also client.

Simple Network Management Protocol *See* SNMP.

SSH Secure Shell. A network protocol in which data is exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log in to a remote machine and execute commands; but, it also supports tunneling, forwarding arbitrary TCP ports, and X Window System (X11) connections. It can transfer files by using the associated SSH File Transfer Protocol (SFTP) or Secure Copy (SCP) protocols.

An SSH server, by default, listens on the standard TCP port 22. An SSH client program is typically used for establishing connections to an sshd daemon accepting remote connections. Both are commonly present on most modern operating systems. Proprietary, freeware, and open-source versions of various levels of complexity and completeness exist.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMPv1 SNMPv1 is a simple request/response protocol. In the SNMPv1 framework, the network-management system installed a request, and managed devices return responses.

SNMPv2C The second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations. SNMPv2C support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2C improved error-handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: No such object, No such instance, and End of MIB view.

T

TCP Transmission Control Protocol. Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack.

Telnet Telnet (TELetype NETwork). A network protocol used on the Internet or LAN connections. It was developed in 1969 beginning with RFC 0015 and standardized as IETF STD 8, one of the first Internet standards.

The term Telnet also refers to software that implements the client part of the protocol. Telnet clients have been available on most UNIX systems for many years and are available for virtually all platforms. Most network equipment and operating systems with a TCP/IP stack support some kind of Telnet service server for their remote configuration (including ones based on Windows NT). Recently, Secure Shell has begun to dominate remote access for UNIX-based machines.

Most often, a user telnets to a UNIX-like server system or a simple network device such as a switch. For example, you might “telnet in from home to check your e-mail at work.” In doing so, you would be using a Telnet client to connect from your computer to one of your servers. Once the connection is established, you would then log in with your account information and execute the operating system commands remotely on that computer, such as **ls** or **cd**.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

Transmission Control Protocol *See* TCP.

Trivial File Transfer Protocol *See* TFTP.

U

UDI Unique Device Identifier. Each identifiable product is an entity, as defined by the Entity MIB (RFC 2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a super entity like a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements: product identifier (PID), version identifier (VID), and serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." You use this identifier to order an exact replacement part.

The VID is the version of the product. Whenever a product is revised, the VID is incremented, according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. This number identifies an individual, specific instance of a product.

Unique Device Identifier *See* UDI.

INDEX

A

C

D

E

H

L

M