Release Notes for Cisco Secure Access Control System 5.6

Revised: November 9, 2016

These release notes pertain to the Cisco Secure Access Control System (ACS), Release 5.6, hereafter referred to as ACS 5.6. This release notes describes the features, limitations and restrictions (caveats), and related documentation for Cisco Secure ACS. The release notes supplement the Cisco Secure ACS documentation that is included with the product hardware and software release.

This document contains:

Cisco Systems, Inc.
www.cisco.com

Introduction

ACS is a policy-driven access control system and an integration point for network access control and identity management.

The ACS 5.6 software runs on a dedicated Cisco SNS-3495 appliance, on a Cisco SNS-3415 appliance, on a Cisco 1121 Secure Access Control System (CSACS-1121) or on a VMware server. ACS 5.6 ships on Cisco SNS-3495 and Cisco SNS-3415 appliances. However, ACS 5.6 continues to support CSACS-1121 appliance. You can upgrade to ACS 5.6 from any of the previous releases of ACS that runs on CSACS-1121 appliance. For more information on upgrade paths, see Upgrading Cisco Secure ACS Software, page 10.

This release of ACS provides new and enhanced functionality. Throughout this document, Cisco SNS-3495, Cisco SNS-3415 and CSACS-1121 refer to the appliance hardware, and ACS server refers to ACS software.

Note Cisco runs a security scan on the ACS application during every major release. We do not recommend you to run a vulnerability scanning in the ACS production environment because such an operation carries risks that could impact the ACS application. You can execute the vulnerability scan operation in a preproduction environment.

System Requirements

Note For more details on Cisco Secure ACS hardware platform and installation, see the Installation and Upgrade Guide for Cisco Secure Access Control System 5.6.

Note No third-party software such as anti-virus or anti-malware, is supported in Cisco Secure ACS.

Supported Hardware

Cisco Secure ACS is packaged with your appliance or image for installation. Cisco Secure ACS 5.6 ships on the following platforms:

Table 1 Supported Hardware Platforms

Hardware Platform	Configuration
Cisco SNS-3495-K9 (Large UCS)	• Cisco UCS C220 M3 • Dual socket Intel E5-2609 2.4Ghz CPU 8 total cores, 8 total threads • 32 GB RAM • 2 x 600-GB disks • RAID 0+1 • 4 GE network interfaces
Cisco SNS-3415-K9 (Small UCS)	• Cisco UCS C220 M3 • Single socket Intel E5-2609 2.4Ghz CPU 4 total cores, 4 total threads • 16 GB RAM • 1 x 600-GB disk • Embedded Software RAID 0 • 4 GE network interfaces

Table 1 Supported Hardware Platforms (continued)

Hardware Platform	Configuration
Cisco 1121 Secure Access Control System Hardware (CSACS-1121)	• Intel Core 2 Duo 2.4-GHz processor with an 800-MHz front side bus (FSB) and 2 MB of Layer 2 cache. • 4GB SDRAM • 2 x 250-GB SATA disks • 4 x 1 GB network interface
Cisco Secure ACS-VM-K9 (VMware)	• 2 CPUs (dual CPU, Xeon, Core2 Duo or 2 single CPUs) • 4 GB RAM • NIC—1 GB NIC interface required (You can install up to 4 NICs.) • For supported VMware versions, see Supported Virtual Environments. For information on VMware requirements, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*.

Supported Virtual Environments

ACS 5.6 supports the following VMware versions:

- VMware ESXi 5.0
- VMware ESXi 5.0 Update 2
- VMware ESXi 5.1
- VMware ESXi 5.1 Update 2
- VMware ESXi 5.5
- VMware ESXi 5.5 Update 1

For information on VMware machine requirements and installation procedures, see the "Installing ACS in a VMware Virtual Machine" chapter in the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*.

Supported Browsers

You can access the ACS 5.6 administrative user interface using the following browsers:

- MAC OS
  - Mozilla Firefox version 28.*x*
  - Mozilla Firefox version 29.*x*
  - Mozilla Firefox version 31.*x*
  - Mozilla Firefox version 32.*x*
  - Mozilla Firefox version 33.*x*
  - Mozilla Firefox version 34.*x*

  - Mozilla Firefox version 35.*x*
  - Mozilla Firefox version 36.*x*
  - Mozilla Firefox version 37.*x*
  - Mozilla Firefox version 38.*x*
  - Mozilla Firefox version 39.*x*
  - Mozilla Firefox version 40.*x*
  - Mozilla Firefox version 41.*x*
  - Mozilla Firefox version 42.*x*
  - Mozilla Firefox version 43.*x*
  - Mozilla Firefox version 44.*x*
  - Mozilla Firefox version 45.*x*
  - Mozilla Firefox version 46.*x*
  - Mozilla Firefox version 47.*x*
  - Mozilla Firefox version 48.*x*
  - Mozilla Firefox version 49.*x*
  - Mozilla Firefox version 24.4 ESR
  - Mozilla Firefox version 45.0.2 ESR
- Windows 7 32-bit and Windows 7 64-bit
  - Internet Explorer version 10.*x*
  - Internet Explorer version 11.*x*
  - Mozilla Firefox version 17.*x*
  - Mozilla Firefox version 21.*x*
  - Mozilla Firefox version 22.*x*
  - Mozilla Firefox version 25.*x*
  - Mozilla Firefox version 26.*x*
  - Mozilla Firefox version 28.*x*
  - Mozilla Firefox version 29.*x*
  - Mozilla Firefox version 31.*x*
  - Mozilla Firefox version 32.*x*
  - Mozilla Firefox version 33.*x*
  - Mozilla Firefox version 34.*x*
  - Mozilla Firefox version 35.*x*
  - Mozilla Firefox version 36.*x*
  - Mozilla Firefox version 37.*x*
  - Mozilla Firefox version 38.*x*
  - Mozilla Firefox version 39.*x*
  - Mozilla Firefox version 40.*x*
  - Mozilla Firefox version 41.*x*

  - Mozilla Firefox version 42.*x*
  - Mozilla Firefox version 43.*x*
  - Mozilla Firefox version 44.*x*
  - Mozilla Firefox version 45.*x*
  - Mozilla Firefox version 46.*x*
  - Mozilla Firefox version 47.*x*
  - Mozilla Firefox version 48.*x*
  - Mozilla Firefox version 49.*x*
  - Mozilla Firefox version 17.0.6 ESR
  - Mozilla Firefox version 24.1.1 ESR
  - Mozilla Firefox version 24.4 ESR
  - Mozilla Firefox version 24.5 ESR
  - Mozilla Firefox version 24.7.0 ESR
  - Mozilla Firefox version 31.0 ESR
  - Mozilla Firefox version 38.0.1 ESR
  - Mozilla Firefox version 45.0.2 ESR
- Windows 8.*x*
  - Internet Explorer version 11.*x*
  - Mozilla Firefox version 31.*x*
  - Mozilla Firefox version 32.*x*
  - Mozilla Firefox version 33.*x*
  - Mozilla Firefox version 34.*x*
  - Mozilla Firefox version 35.*x*
  - Mozilla Firefox version 36.*x*
  - Mozilla Firefox version 37.*x*
  - Mozilla Firefox version 38.*x*
  - Mozilla Firefox version 39.*x*
  - Mozilla Firefox version 40.*x*
  - Mozilla Firefox version 41.*x*
  - Mozilla Firefox version 42.*x*
  - Mozilla Firefox version 43.*x*
  - Mozilla Firefox version 44.*x*
  - Mozilla Firefox version 45.*x*
  - Mozilla Firefox version 46.*x*
  - Mozilla Firefox version 47.*x*
  - Mozilla Firefox version 48.*x*
  - Mozilla Firefox version 49.*x*
  - Mozilla Firefox version 24.7.0 ESR

- Mozilla Firefox version 31.0 ESR
- Mozilla Firefox version 45.0.2 ESR

Note Mozilla Firefox version 46.x or later is supported only after installing ACS 5.6 patch 5 or later.

The above mentioned browsers are supported only with one of the following cipher suits:

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

  The above cipher suits are not supported if you use Internet Explorer version 8.*x* on a Windows XP operating system in compatibility mode to access ACS web interface.

Adobe Flash Player 11.2.0.0 or above must be installed on the system running the client browser.

Note
- When you import or export a .csv file from ACS 5.*x*, you must turn off the pop-up blocker.

Note
- You can launch the ACS web interface using IPv6 addresses only in Internet Explorer 7.*x* or later and Mozilla Firefox 3.*x* versions.

Supported Device and User Repositories

For information on supported devices, 802.1X clients, and user repositories, see *Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.6*.

New Features in ACS 5.6 Release

The following sections briefly describe the new features in the 5.6 release:

Enhanced Reports

The reports in Cisco Secure ACS, Release 5.6 are enhanced to have a new look and feel that is more simple and easy to use. The reports are grouped into logical categories to provide information related to authentication, session traffic, device administration, ACS server configuration and administration, and troubleshooting. The enhanced dynamic export option allows you to export the selected reports to an excel spreadsheet as a comma-separated values (.csv) file. The enhanced scheduling service allows you to queue reports and receive notifications when the reports are available.

The report names and their filters are displayed on the left pane and the reports are displayed on the right pane of the Reports web interface. The enhanced web interface helps you to navigate through the reports easily and to have a better control over different types of reports from left pane. ACS 5.6 reports provides an enhanced performance and are easy to use, but does not support the Interactive Viewer feature as a whole; however, the “show or hide columns” and “fixing columns” (constituents of the Interactive Viewer feature) are supported. You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation. A few Interactive Viewer customization options that are missing in ACS 5.6 will be available to customers either in the upcoming ACS releases or ACS 5.6 patches.

Note ACS 5.6 patch 2 introduces two new interactive viewer functionalities, sorting and filtering reports data. After installing AC S 5.6 patch 2, you can filter and sort the data items after generating the reports from Reports web interface.

Advantages of ACS 5.6 Flex Reports

- A significant improvement in performance is observed with respect to the time taken for generating the reports.
- Flex-based reports provide the applications developer a better control of their code base. This allows the developers to mitigate the security issues especially in web-server based applications.
- If you require a new feature or a fix for any existing issue in the current version of Actuate reports, you need to upgrade Actuate to its latest version. A significant amount of effort and money is required to upgrade the current version of Actuate to its latest version. These issues are minimal in Flex reports and it preserves sustainability in the long run.
- Actuate a requires re distributable license, whereas, Flex requires only a developer license.
- Navigating through different types of reports is now better controlled from the left pane, rather than going to the right pane and selecting reports and its filter values. This left pane navigation improves the user experience.
- The look and feel, and the layout of the flex reports are much better than Actuate reports.
- Cisco Identity Services Engine (ISE) uses the Flex framework for generating reports and the ISE reports are similar to the ACS 5.6 reports. This similarity will help you to perform a smoother transition from ACS to ISE in future.

Limitations of ACS 5.6 Flex Reports

Table 2 lists the limitations and the differences between the feature implementation in ACS 5.5 and 5.6 Reports web interface.

Table 2 Limitations in ACS 5.6 Reports Compared to ACS 5.5 Reports

Functionality in ACS 5.5	Features Implemented in ACS 5.6	Workaround
In the Query & Run page, you can search for users, ACS nodes, and identity groups to generate a customized report. You can select a user or group from the list of all users or groups.	This feature is addressed in ACS 5.6 such that you do not have to remember the users or groups. The users or groups are auto populated when you enter the first three characters in the input field.	None
The Scheduled and Favorite reports in ACS 5.4 can be reused in ACS 5.5. However, these reports cannot be reused in ACS 5.6 as the Flex framework cannot understand the actuate-based Scheduled and Favorite reports format that are stored in the disk.	The Scheduled and Favorite reports generated in ACS 5.4 or 5.5 can be reused in ACS 5.6. The Scheduled and Favorite reports of ACS 5.4 or 5.5 are stored under Saved reports in ACS 5.6.	None
Sorting Columns—In the Interactive Viewer, you can sort the columns in ascending or descending order.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet, and use the excel options to sort the data.
In the Interactive Viewer, you can aggregate values of the numerical columns. For example, you can sum up the number of passed authentications and see the total number of passed authentications. Similarly, you can search and find the minimum, maximum, first, last values, and so on.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.
In the Interactive Viewer, you can add a new column by merging the values of two columns. You can also use expressions to merge the values in the columns.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.
In the Interactive Viewer, you can filter the column values based on conditions such as equal to, less than, greater than, between, not null, and so on.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.

Table 2 Limitations in ACS 5.6 Reports Compared to ACS 5.5 Reports

Functionality in ACS 5.5	Features Implemented in ACS 5.6	Workaround
In Interactive Viewer, you can edit the reports by applying a page break, changing the alignment, changing the font, style, color, case (upper/lower), and so on.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.
In Interactive Viewer, you can rearrange a report or group an entire report based on the value of a particular column. For example, rearranging the report such that all the users whose failed attempts count is more than three.	Not available	You can export the report to a CSV file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.

Upgrading Cisco Secure ACS Software

Cisco Secure Access Control System (ACS) supports upgrades from different versions of ACS 5.*x* to ACS 5.6. The supported upgrade paths include:

- Cisco Secure ACS, Release 5.4, recommended with latest patch applied
- Cisco Secure ACS, Release 5.5, recommended with latest patch applied

Follow the upgrade instructions in the Installation and Upgrade Guide for *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*. to upgrade to Cisco Secure ACS, Release 5.6.

Monitoring and Reports Data Export Compatibility

Exporting monitoring and troubleshooting records to a remote database does not work if the remote database is an Oracle database and it is configured in a cluster setup.

Installation and Upgrade Notes

This section provides information on the installation tasks and configuration process for ACS 5.6.

This section contains:

Installing, Setting Up, and Configuring CSACS-1121

This section describes how to install, set up, and configure the CSACS-1121 series appliance. The CSACS-1121 series appliance is preinstalled with the software.

To set up and configure the CSACS-1121:

Step 1 Open the box containing the CSACS-1121 Series appliance and verify that it includes:

- The CSACS-1121 Series appliance
- Power cord
- Rack-mount kit
- Cisco Information Packet
- Warranty card
- *Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.6*

Step 2 Go through the specifications of the CSACS-1121 Series appliance.

For more details, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*.

Step 3 Read the general precautions and safety instructions that you must follow before installing the CSACS-1121 Series appliance.

For more details, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6* and pay special attention to all safety warnings.

Step 4 Install the appliance in the 4-post rack, and complete the rest of the hardware installation.

For more details on installing the CSACS-1121 Series appliance, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6.*

Step 5 Connect the CSACS-1121 Series appliance to the network, and connect either a USB keyboard and Video Graphics Array (VGA) monitor or a serial console to the serial port.

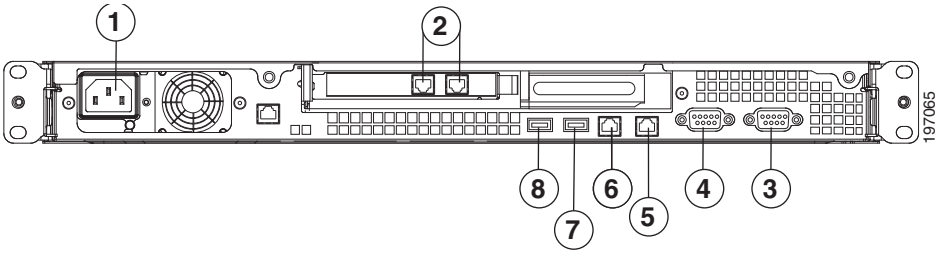
Figure 1 shows the back panel of the CSACS-1121 Series appliance and the various cable connectors.

Note For the initial setup, you must have either a USB keyboard and VGA monitor or a serial console running terminal emulation software.

For more details, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6.*

For information on installing ACS 5.6 on VMware, see the "Installing ACS in a VMware Virtual Machine" chapter in the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6.*

Figure 1 CSACS 1121 Series Appliance Rear View



The following table describes the callouts in Figure 1.

1	AC power receptacle	5	GigabitEthernet 1
2	GigabitEthernet	6	GigabitEthernet 0
3	Serial connector	7	USB 3 connector
4	Video connector	8	USB 4 connector

Step 6 After completing the hardware installation, power up the appliance.

The first time you power up the appliance, you must run the setup program to configure the appliance. For more information, see Running the Setup Program, page 13.

Installing, Setting Up, and Configuring Cisco SNS-3495 or Cisco SNS-3415

The Cisco SNS-3495 and Cisco SNS-3415 appliances do not have a DVD drive. You must use the CIMC on the appliance or a bootable USB to install, set up, and configure ACS 5.6 on this appliance. For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6*.

This section describes how to install, set up and configure the Cisco SNS-3495 and Cisco SNS-3415 appliance. The Cisco SNS-3495 and Cisco SNS-3415 appliance are preinstalled with the software.

To set up and configure the Cisco SNS-3495 and Cisco SNS-3415:

Step 1 Open the box containing the Cisco SNS-3495 and Cisco SNS-3415 appliances and verify that it includes:

- The Cisco SNS-3495 and Cisco SNS-3415 appliance
- Power cord
- KVM cable
- Cisco information packet
- Warranty card
- *Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.6*

Step 2 Go through the specifications of the Cisco SNS-3495 or Cisco SNS-3415 appliance.

For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6*.

Step 3 Read the general precautions and safety instructions that you must follow before installing the Cisco SNS-3415 or Cisco SNS-3495 appliance.

For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6* and pay special attention to all safety warnings.

Step 4 Install the appliance in the 4-post rack, and complete the rest of the hardware installation.

For more details on installing the Cisco SNS-3495 or Cisco SNS-3415 appliance, see the

Installation and Upgrade guide for the Cisco Secure Access Control System 5.6.

Step 5 Connect the Cisco SNS-3495 or Cisco SNS-3415 appliance to the network and connect either a USB keyboard and Video Graphics Array (VGA) monitor or a serial console to the serial port.

See the *Installation and Upgrade guide for Cisco Secure Access Control System 5.6* for illustrations of the front and back panel of the Cisco SNS-3495 and Cisco SNS-3415 appliance and the various cable connectors.

Note For the initial setup, you must have either a USB keyboard and VGA monitor or a serial console running terminal-emulation software.

For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6*.

For information on installing ACS 5.6 on VMware, see the" Installing ACS in a VMware Virtual Machine" chapter in the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6.*

Step 6 After completing the hardware installation, power up the appliance.

The first time you power up the appliance, you must run the setup program to configure the appliance. For more information, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.6*.

Running the Setup Program

The setup program launches an interactive CLI that prompts you for the required parameters. An administrator can use the console or a dumb terminal to configure the initial network settings and enter the initial administrator credentials for the ACS 5.6 server that is using the setup program. The setup process is a one-time configuration task.

To configure the ACS server:

Step 1 Power up the appliance.

The setup prompt appears:

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

At the login prompt, enter **setup** and press **Enter**.

The console displays a set of parameters. You must enter the parameters as described in Table 3.

Note You can interrupt the setup process at any time by typing **Ctrl-C** before the last setup value is entered.

Table 3 Network Configuration Prompts

Prompt	Default	Conditions	Description
Hostname	*localhost*	The first letter must be an ASCII character. The length must be from 3 to 15 characters. Valid characters are alphanumeric (A-Z, a-z, 0-9) and the hyphen (-), and the first character must be a letter. **Note** When you intend to use the AD ID store and set up multiple ACS instances with the same name prefix, use a maximum of 15 characters as the hostname so that it does not affect the AD functionality.	Enter the hostname.
IPv4 IP Address	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter the IP address.
IPv4 Netmask	None, network specific	Must be a valid IPv4 netmask between 0.0.0.0 and 255.255.255.255.	Enter a valid netmask.
IPv4 Gateway	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter a valid IP address for the default gateway.
Domain Name	None, network specific	Cannot be an IP address. Valid characters are ASCII characters, any numbers, the hyphen (-), and the period (.).	Enter the domain name.
IPv4 Primary Name Server Address	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter a valid name server address.
Add Another Name Server	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255. **Note** You can configure a maximum of three name servers from the ACS CLI.	To configure multiple name servers, enter `y`.
NTP Server	time.nist.gov	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255 or a domain name server. **Note** You can configure a maximum of three NTP servers from the ACS CLI.	Enter a valid domain name server or an IPv4 address.
Time Zone	UTC	Must be a valid local time zone.	Enter a valid system time zone.
SSH Service	None, network specific	None.	To enable SSH service, enter `y`.

Table 3 Network Configuration Prompts (continued)

Prompt	Default	Conditions	Description
Username	*admin*	The name of the first administrative user. You can accept the default or enter a new username. Must be from 3 to 8 characters and must be alphanumeric (A-Z, a-z, 0-9).	Enter the username.
Admin Password	None	No default password. Enter your password. The password must be at least six characters in length and have at least one lower-case letter, one upper-case letter, and one digit. In addition: • Save the user and password information for the account that you set up for initial configuration. • Remember and protect these credentials, because they allow complete administrative control of the ACS hardware, the CLI, and the application. • If you lose your administrative credentials, you can reset your password by using the ACS 5.6 installation CD.	Enter the password.

After you enter the parameters, the console displays:

```
localhost login: setup
Enter hostname[]: acs54-server-1
Enter IP address[]: 192.0.2.177
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 192.0.2.1
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: 192.0.2.6
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: 192.0.2.2
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH Service? Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Virtual machine detected, configuring VMware tools...
File descriptor 4 (/opt/system/etc/debugd-fifo) leaked on lvm.static invocation
Parent PID 3036: /bin/bash
Do not use `Ctrl-C' from this point on...
debugd[2455]: [2809]: config:network: main.c[252] [setup]: Setup is complete.
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

After the ACS server is installed, the system reboots automatically. Now, you can log into ACS with the CLI username and password that was configured during the setup process.

You can use this username and password to log in to ACS only through the CLI. To log in to the web interface, you must use the predefined username *ACSAdmin* and password *default*.

When you access the web interface for the first time, you are prompted to change the predefined password for the administrator. You can also define access privileges for other administrators who will access the web interface.

Licensing in ACS 5.6

To operate ACS, you must install a valid license. ACS prompts you to install a valid license when you first access the web interface.

Each ACS instance (primary or secondary) in a distributed deployment requires a unique base license.

This section contains:

Types of Licenses

Table 4 lists the types of licenses that are available in ACS 5.6.

Table 4 ACS License Support

License	Description
Base License	The base license is required for all deployed software instances and for all appliances. The base license enables you to use all ACS functions except license-controlled features, and it enables standard centralized reporting features. The base license: • Is required for all primary and secondary ACS instances. • Is required for all appliances. • Supports deployments that have a maximum of 500 NADs. The following are the types of base licenses: • Permanent—Does not have an expiration date. Supports deployments that have a maximum of 500 NADs. • Evaluation—Expires 90 days from the time the license is issued. Supports deployments that have a maximum of 50 NADs. The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses; thus the number of devices is 256.
Add-On Licenses	Add-on licenses can be installed only on an ACS server with a permanent base license. A large deployment requires the installation of a permanent base license. The Security Group Access feature licenses are of two types: Permanent and NFR. However, the permanent Security Group Access feature license can be used only with a permanent base license.

ACS 5.6 does not support auto installation of the evaluation license. Therefore, if you need an evaluation version of ACS 5.6, then you must obtain the evaluation license from Cisco.com and install ACS 5.6 manually.

If you do not have a valid SAS contract with any of the ACS products, you will not be able to download the ISO image from Cisco.com. In such case, you need to contact your local partner or the Cisco representative to get the ISO image.

Upgrading an ACS Server

If you have ACS 5.4 or ACS 5.5 installed on your machine, you can upgrade to ACS 5.6 using one of the following two methods:

- Upgrading an ACS server using the Application Upgrade Bundle
- Re imaging and upgrading an ACS server

You can perform an application upgrade on a Cisco appliance or a virtual machine only if the disk size is greater than or equal to 500 GB. If your disk size is lesser than 500 GB, you must re image to ACS 5.6, followed by a restore of the backup taken in ACS 5.4 or ACS 5.5, to move to ACS 5.6 Release.

See the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.6* for information on upgrading your ACS server.

Note Upgrading to ACS 5.6 may fail if any LDAP identity store is configured without groups or attributes in it and AD identity store is not configured. To avoid this issue, before upgrading to ACS 5.6, you need to either add groups or attributes to the LDAP identity store or configure an AD identity store.

Note You must provide full permission to NFS directory when you configure the NFS location using the **backup-stagging-url** command in ACS 5.6 to perform a successful On Demand Backup.

Applying Cumulative Patches

Periodically, patches will be posted on Cisco.com that provide fixes to ACS 5.6. These patches are cumulative. Each patch includes all the fixes that were included in previous patches for the release.

You can download ACS 5.6 cumulative patches from the following location:

http://software.cisco.com/download/navigator.html

To download and apply the patches:

Step 1 Log in to Cisco.com and navigate to **Products > Security > Access Control and Policy > Secure Access Control System > Secure Access Control System 5.6 > Secure Access Control System Software-5.6.0.22**.

Step 2 Download the patch.

Step 3 Install the ACS 5.6 cumulative patch. To do so:

Enter the following **acs patch** command in EXEC mode to install the ACS patch:

`acs patch install` *patch-name*`.tar.gpg` **`repository`** *repository-name*

ACS displays the following confirmation message:

```
Installing an ACS patch requires a restart of ACS services.
Would you like to continue? yes/no
```

Step 4 Enter **yes**.

ACS displays the following:

```
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
```

```
Getting bundle to local machine...
  md5: aa45b77465147028301622e4c590cb84
  sha256: 3b7f30d572433c2ad0c4733a1d1fb55cceb62dc1419b03b1b7ca354feb8bbcfa
% Please confirm above crypto hash with what is posted on download site.
% Continue? Y/N [Y]?
```

Step 5 The ACS 5.6 upgrade bundle displays the md5 and sha256 checksum. Compare it with the value displayed on Cisco.com at the download site. Do one of the following:

- Enter **Y** if the crypto hashes match. If you enter Y, ACS proceeds with the installation steps.

  ```
  % Installing an ACS patch requires a restart of ACS services.
  Would you like to continue? yes/no
  ```

- Enter **N** if the crypto hashes do not match. If you enter N, ACS stops the installation process.

Step 6 Enter **yes**.

The ACS version is upgraded to the applied patch. Check whether all services are running properly, using the **show application status acs** command from EXEC mode.

Step 7 Enter the **show application version acs** command in EXEC mode and verify if the patch is installed properly or not.

ACS displays a message similar to the following one:

```
acs/admin# show application version acs
CISCO ACS VERSION INFORMATION
-----------------------------
Version: 5.6.0.22
Internal Build ID: B.225
acs/admin #
```

Note During patch installation, if the patch size exceeds the allowed disk quota, a warning message is displayed in the ACS CLI, and an alarm is displayed in the ACS Monitoring and Reports page.

Resolved ACS Issues

Table 5 lists the issues that are resolved in ACS 5.6.

Table 5 Resolved Issues in ACS 5.6

Bug ID	Description
CSCuj91631	Launching the secondary instance's web interface from the primary ACS instance does not work if the secondary hostname is not resolvable.
CSCuj53935	Certificate Authority edit page is susceptible to XSS.
CSCuj80866	Collecting the support bundle from the web interface does not work if the ACS instance is not a log collector server.
CSCul09022	ACS does not respond when the TACACS requests are sent in segmented packets.

Table 5 Resolved Issues in ACS 5.6 (continued)

Bug ID	Description
CSCth35755	Group mapping in Active Directory fails if the group name has a "/" character.
CSCul29675	Newly created authorization rule does not hold the customized position.
CSCul32497	Clear filter option in ACS does not display more than 200 authorization rules.
CSCul64484	ACS View NBAPI does not have detailed debug logs.
CSCuh63873	ACS View should implement syslog messages over TLS or TCP protocols.
CSCum03625	Scripting vulnerability in ACS.
CSCum13044	Active Directory loses its connectivity with ACS after a password change.
CSCuj94585	Active Directory authentications fails in ACS when the same user is present in two different organizational units.
CSCum26584	After upgrading to ACS 5.5, a few features on ACS web interface does not work properly when you have multiple CLI administrators in ACS 5.4.
CSCuj01135	Active Directory client restarts frequently with an exceptional error while communicating with the LDAP server.
CSCum68228	Changing the internal user password fails while importing the user details using a CSV file in ACS 5.5.
CSCum86948	In ACS 5.5, the minimum password length is changed to 4.
CSCum86626	Cannot register the secondary ACS instances to the primary ACS instance over WAN after upgrading to ACS 5.5.
CSCum51180	In ACS 5.4, there is no alarm when the configuration database size is over 1GB.
CSCty13296	Importing users with the same password does not display an error message.
CSCum67932	ACS 5.5 does not start after upgrading from ACS 5.4 due to a unknown encryption algorithm.
CSCun37608	Secondary ACS instance ignores the new primary ACS instance when the old primary instance comes back online.
CSCun85949	ACS 5.5 fails to start its services when the RADIUS attributes 150, 151, and 152 are configured.
CSCun71995	ACS web interface does not display the network device group locations when you click the NDG:Location option.
CSCun67769	Creating or editing the Favorites option fails when the length of the attribute is big in size.
CSCun81726	Unable to retrieve the user attribute "userAccountControl" from Active Directory in ACS 5.5.
CSCun92213	ACS 5.x opens too many TCP connections with the remote DB at a time.
CSCun98622	Exporting MAC address from the End Station filter logs out the user from ACS web interface.
CSCtx99385	ACS displays an incorrect alert report that the incremental backup is not configured.
CSCun84823	In ACS, non-authenticated users can see the input validation code.
CSCuo54517	Overriding the global log configuration option fails in ACS.

Table 5 Resolved Issues in ACS 5.6 (continued)

Bug ID	Description
CSCuo88797	ACS 5.*x* does not display an appropriate error message when you use an unsupported browser to access the ACS web interface.
CSCuj41395	After restarting the ACS services, you can find that the scheduled backup is added twice when you run the **show running configuration** command in ACS CLI.
CSCuo93378	ACS database gets corrupted when you make configuration changes through ACS web interface using Chrome and Safari browsers.
CSCuo82841	It is mandatory to have a shared secret key while adding AAA clients for TACACS+ authentication.
CSCuo60270	ACS fails to join Active Directory domains with a very large number of domain controllers.
CSCum60476	ACS 5.4 does not fetch internal groups.
CSCun05712	The RSA agent in ACS gets exhausted if the load is too heavy.
CSCuo68704	Check status monitoring functionality has to be improved in ACS 5.*x*.
CSCuo78625	ACS 5.5 does not allow the special characters in the shared secret of TACACS+ and RADIUS authentications.
CSCuo88163	Fetching the user information using the programmatic interface does not working properly in ACS 5.5.
CSCuo63302	Changing the user password through the REST services fails if the user is created using the duplicate option.
CSCuo19733	Customized reports based on the start and end dates of ACS 5.5 View displays the last 500 pages of records for the end date.
CSCuo89864	In ACS 5.5, there are issues in cross frame scripting and session tokens in the URL.
CSCuo89889	In ACS 5.5, the session related cookies does not use a HTTP - only or secure keywords.
CSCuo89946	In ACS 5.5, unapproved hash algorithm is used to store sensitive data.
CSCuo93378	Using the Chrome and Safari web browsers results in database corruption.
CSCup00818	ACS 5.5 CLI interface displays an error when you execute the **show application status acs** command.
CSCup10509	A security administrator can change his role to be a super administrator in ACS 5.5.
CSCup32287	In ACS 5.5, the TCP port 6514 for syslog messages is open by default.
CSCup34695	In ACS 5.5, exporting data to a remote database fails with an error due to a data type mismatch between the ACS server and the remote database.
CSCup77077	ACS does not retrieve the userAccountControl attribute from Active Directory when you use userAccountControl as a condition in authorization rules.
CSCuq00890	An unexpected behavior is observed in a deployment when you execute the **halt** command in ACS command line interface.
CSCtx65471	ACS fails to send syslog messages to the remote database when you restart the log collector server multiple times in a deployment.

Table 5 Resolved Issues in ACS 5.6 (continued)

Bug ID	Description
CSCup75144	The authorization policy page in ACS web interface is not displayed properly when you use Internet Explorer 11.*x* version.
CSCuq64564	Configuration issues occur when you use Internet Explorer 11.*x* to open ACS 5.5 web interface. The issues are now resolved.
CSCul06939	LDAP authentication fails in ACS 5.x while using a DNS server name and the first DNS server is down.
CSCum05372	ACS activity logs do not display anything after upgrading to ACS 5.5.
CSCum28910	ACS runtime services do not come up when you have missing entries in Active Directory Group.
CSCum93359	SFTP server does not work after upgrading ACS 5.*x* to ACS 5.5 version.
CSCun45555	Active Directory user password that is used to join ACS to Active Directory is displayed in the logs as clear text.
CSCun89799	REST API services prompts for a password when you select the external identity stores.
CSCuo45648	ACS 5.*x* sends the syslog messages to the remote log target with the wrong timezone entries during daylight saving.
CSCup40317	ACS View job-manager processes are stopped unexpectedly during disk space calculation.
CSCup79536	ACS ignores logging configuration after reloading.
CSCup79591	ACS ignores the **no cdp run** command after reloading.
CSCup90014	Entries in /CSCOacs/view/decap/data/ are duplicated and it is stored in /opt, that result in more space usage in /opt.
CSCuq36829	Files in /var occupy the complete disk space and make ACS unstable.
CSCuq26876	Exporting remote database to Microsoft SQL fails in ACS 5.5.
CSCul38172	SNMP walk does not work properly after configuring NIC bonding in ACS 5.x.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.1

Table 6 lists the issues that are resolved in the ACS 5.6.0.22.1 cumulative patch.

You can download the ACS 5.6.0.22.1 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 6 Resolved Issues in Cumulative Patch ACS 5.6.0.22.1

Bug ID	Description
CSCur00511	ACS evaluation for CVE-2014-6271 and CVE-2014-7169. This fix addresses the vulnerabilities identified in the bash shell by upgrading to the required system libraries. This patch fix includes security fixes, and as a result, ACS server prompts a reboot which is highly recommended for a successful installation of the patch.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.2

Table 7 lists the issues that are resolved in the ACS 5.6.0.22.2 cumulative patch.

You can download the ACS 5.6.0.22.2 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 7 Resolved Issues in Cumulative Patch ACS 5.6.0.22.2

Bug ID	Description
CSCur10264	ACS 5.6 introduces Sorting and Filtering functionalities in Reports web interface.
CSCuq67241	The "Disable account if date exceeds" feature does not work in ACS 5.6.
CSCuq13294	ACS 5.3 nodes are automatically registered in ACS 5.6 standalone node while retrieving the database back up that was taken from ACS 5.3 deployment in ACS 5.6 standalone node.
CSCuq35410	Unable to search for username that contains the " ' " character.
CSCuq11378	ACS 5.6 displays IP addresses or IP ranges overlapping error message when first, second, and third octets are same.
CSCuq06377	All default filters are displayed in Saved Reports when some filters are disabled while creating Saved Reports from Reports web interface.
CSCuq21543	Day-wise Authentication details are not displayed in the SGT Assignment Report.
CSCuq21559	The selected time ranges are not displayed when you cross launch reports from Reports web interface.
CSCuq22094	The scheduled report details page in ACS Reports web interface displays the last viewed report.

Table 7 Resolved Issues in Cumulative Patch ACS 5.6.0.22.2

Bug ID	Description
CSCuq46862	The scheduled reports in ACS Reports web interface do not display the customized time ranges.
CSCuq56757	From and To time ranges are incorrectly displayed when you generate Session Directory Reports.
CSCur30345	SSLv3 Poodle vulnerability evaluation is found in ACS.
CSCur27402	Unable to Schedule reports in ACS 5.6 Reports web interface.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.3

Table 8 lists the issues that are resolved in the ACS 5.6.0.22.3 cumulative patch.

You can download the ACS 5.6.0.22.3 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 8 Resolved Issues in Cumulative Patch ACS 5.6.0.22.3

Bug ID	Description
CSCuq62466	Exporting remote database to Microsoft SQL database fails when you have junk characters in the data.
CSCur42721	Improvement is required in ACS 5.*x* TACACS+ threading.
CSCur59417	ACS 5.*x* web interface fields does not allow the single quotes, apostrophe, and plus symbols.
CSCur68196	ACS 5.*x* jobs stops running automatically after one or two days from the date of configuring remote database.
CSCur98716	ACS 5.4 displays "GC overhead limit exceeded" exception and the Monitoring and Reports web interface fails to load.
CSCus17482	The primary instance sends an incorrect reference to the secondary instances after deleting an object from the primary instance.
CSCus38676	ACS 5.6 displays an internal error after submitting the changes in AAA health alarm.
CSCus42056	Incremental backup issues in ACS View.
CSCus42060	Clear the log collector bugger pro-actively when logs are not running.
CSCus55169	ACS 5.4 to 5.6 application upgrade is not starting due to an encryption problem
CSCus68826	ACS 5.*x* is vulnerable to CVE-2015-0235.
CSCut55144	Issues with special characters in ACS 5.*x*.
CSCut05442	ACS displays the IP subnet overlap error message incorrectly.
CSCut20508	Configuring excluded IP range for a network device can cause an overlap with the other subnets in ACS.
CSCut01441	Runtime crashes if ACS receives a SIGPIPE (broken pipe) signal.

Table 8 Resolved Issues in Cumulative Patch ACS 5.6.0.22.3

Bug ID	Description
CSCus52928	Scheduled backup creates many files on same name at the same time on FTP server.
CSCus80750	Service selection rule fails to match if the first TACACS+ ASCII request does not have the username.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.4

Table 9 lists the issues that are resolved in the ACS 5.6.0.22.4 cumulative patch.

You can download the ACS 5.6.0.22.4 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 9 Resolved Issues in Cumulative Patch ACS 5.6.0.22.4

Bug ID	Description
CSCuu94829	ACS 5.x displays an incorrect device name when ACS identifies an overlapping IP range.
CSCuu93287	The report links that are provided in an email notification for alarms does not work in ACS.
CSCuu57091	ACS runtime process are stuck and in not monitored state after applying ACS 5.6 patch 3.
CSCuu43343	ACS does not allow special characters for KEK and MACK keys of Network devices.
CSCuu30320	ACS server does not identify the passcode cache timeout option that is configured from ACS web interface.
CSCuu59807	Replication issues are identified due to administrator account password change in ACS 5.x.
CSCus63338	ACS View dashboard displays an error when you add a new layouts.
CSCuv88723	Issues are found while changing ACS administrator password if the password includes < or > characters.
CSCuu81221	Unable to delete the old subordinate CAs after installing a new CA certificate.
CSCuc16427	Exporting records to a.csv file using the timestamps option does not work properly.
CSCuv99693	ACS 5.6 does not allow special characters in command sets.
CSCuw09481	ACS 5.*x is* vulnerable to CVE2015-5600.
CSCuv39328	ACS management process fails to respond when there are huge number of AAA clients and you search for reports with the network device name in ACS.
CSCuw21552	ACS 5.*x* displays incorrect results for all filters that you use on configuration Audit Scheduled Report.
CSCuw70238	Unable to save scheduled reports in ACS 5.*x* with clock time zone set as ETC/GMT+/-7.

Table 9 Resolved Issues in Cumulative Patch ACS 5.6.0.22.4

Bug ID	Description
CSCuv95363	Scheduled reports in ACS 5.*x* are not working after reloading the ACS server.
CSCuv63197	ACS runtime crashes when the last EAP fragment length is greater than the total EAP fragment length.
CSCuv42038	The advanced drop option does not drop the TACACS+ requests in ACS 5.x.
CSCus42781	OpenSSL Vulnerabilities were found in ACS during January 2015.
CSCus43434	Context limit is reached if ACS receives a reset request during packet processing.
CSCut94394	Unable to start temporary database when you restart ACS services.
CSCuu11002	Reflected XSS vulnerability is found in ACS 5.x.
CSCuu11005	Local file inclusion vulnerability is found in ACS 5.x
CSCus64212	Scheduled reports in ACS 5.6 does not display all columns.
CSCut87378	ACS runtime crashes frequently during authentications.
CSCus97002	Favorite reports in ACS 5.6 does not display any data.
CSCto56190	Active Directory interface operations take a long time if LDAP SSL is not enabled in Active Directory.
CSCut75184	ACS considers the parentheses as an invalid character.
CSCut46073	OpenSSL Vulnerabilities were found in ACS during March 2015.
CSCuu82493	OpenSSL Vulnerabilities were found in ACS during June 2015.
CSCuu67914	Purging fails in ACS after installing ACS 5.6 patch 3.
CSCuu42929	End Station Filters limitation has to be relaxed in ACS 5.x.
CSCuv20514	Issues were found when you restore ACS 5.5 View database.
CSCuv03303	ACS does not properly send emails when you export reports from ACS web interface.
CSCuu75750	Updating end station filters using a .csv file fails in ACS.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.5

Table 10 lists the issues that are resolved in the ACS 5.6.0.22.5 cumulative patch.

You can download the ACS 5.6.0.22.5 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 10 Resolved Issues in Cumulative Patch ACS 5.6.0.22.5

Bug ID	Description
CSCuz48986	Adding or editing the Service Selection Rules in ACS using Firefox 46 browser erases all the rules.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.6

Table 11 lists the issues that are resolved in the ACS 5.6.0.22.6 cumulative patch.

You can download the ACS 5.6.0.22.6 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 11 Resolved Issues in Cumulative Patch ACS 5.6.0.22.6

Bug ID	Description
CSCus45389	If the VendorTypeField size is set to 1, ACS drops the RADIUS requests when Vendor Specific Attribute field is empty.
CSCut99902	ACS does not list the identity group if there is a "\" in the identity group description field.
CSCuv10632	ACS displays an error message intermittently when you execute the acs config-web-interface migration enable command.
CSCuv10688	ACS primary node shows the status of the secondary node as "Node not responding" though the secondary node is connected.
CSCuw24655	Protection vulnerability impacts the integrity of the system due to improper RBAC validation in ACS.
CSCuw24661	Protection vulnerability due to improper RBAC validation in ACS while accessing the Launch Monitoring and Report Viewer.
CSCuw24694	Denial of Service vulnerability is found in Secure Shell connections with ACS.
CSCuw24700	SQL injection vulnerability in ACS.
CSCuw24705	Reflective XSS vulnerability in ACS.
CSCuw24710	DOM-based XSS vulnerability in ACS.
CSCuw24714	XML injection vulnerability in ACS.

Table 11 Resolved Issues in Cumulative Patch ACS 5.6.0.22.6

Bug ID	Description
CSCuw89910	ACS fails to join the Active Directory domain when the password includes "<" or ">" characters.
CSCux33426	ACS 5.7 fails to import a CSV file having "&" symbol in the Network Device Group filters.
CSCux34781	Apache Common Collections Java library vulnerability was found in ACS during December 2015.
CSCux44063	Secure Syslog feature is not working properly when you restart the log collector server in ACS 5.7.
CSCuy09740	ACS View report does not display the latest records when the report has more than 25K records.
CSCuy13890	Log Recovery is stuck when a syslog message attribute length is greater than 1024.
CSCuz48986	Adding or editing the Service Selection Rules in ACS using Firefox 46 browser erases all the rules.
CSCuz52505	OpenSSL Vulnerabilities were found in ACS during May 2016.

Resolved Issues in Cumulative Patch ACS 5.6.0.22.7

Table 12 lists the issues that are resolved in the ACS 5.6.0.22.7 cumulative patch.

You can download the ACS 5.6.0.22.7 cumulative patch from the following location:

http://software.cisco.com/download/navigator.html?a=a&i=rpm

Refer to "Applying Cumulative Patches" section on page 18 for instructions on how to apply the patch to your system.

Table 12 Resolved Issues in Cumulative Patch ACS 5.6.0.22.7

Bug ID	Description
CSCva81649	ACS needs to update "tzdata" for December 2016 leap second.

Limitations in ACS Deployments

Table 13 describes the limitations in ACS deployments.

Table 13 Limitations in ACS Deployments

Object Type	ACS System Limits
ACS Instances	22
Hosts	150,000
Users	300,000
Identity Groups	1,000
Active Directory Group Retrieval	1,500
Network Devices	100,000
Network Device Groups	Unique top-level NDGs: 12 Network Device Group Child Hierarchy: 6 All Locations: 10,000 All Device Types: 350
Services	25
Authorization Rules	320
Conditions	8
Authorization Profile	600
Service Selection Policy (SSP)	50
Network Conditions (NARs)	3,000
ACS Admins	50
	9 static roles
dACLs	600 dACL with 100 ACEs each

Known ACS Issues

Table 14 lists the known issues in ACS 5.6. You can also use the Bug Toolkit on Cisco.com to find any open bugs that do not appear here.

Table 14 Known Issues in ACS 5.6

Bug ID	Description
CSCuo38291 Extra information that appear in the error messages of ACS Reports web interface are not removed.	If the ACS session is logged out when you are generating reports in the Reports web interface, an error message is displayed. The extra information in this error message should be removed. This problem occurs when you log out from the main ACS window and the reports viewer is open in another window. **Workaround:** 1. Close the Reports web interface. 2. Log into ACS web interface and click **Launch Monitoring and Report Viewer**. The Monitoring and Reports web interface opens in a new window. 3. Click **Reports** to open the Reports Web interface in a new window.
CSCuq61449 Start time and End time filters are not displayed in saved reports.	The Start time and End time filter values have to be entered when you run any Saved reports. This problem occurs when you run a report with Start time and End time filters and save it. **Workaround:** Enter the values for the Start time and End time filters manually.
CSCuq24311 Filter options of the Favorite reports change automatically when you set a User Report as Favorite report.	In ACS 5.6, when you set a User Report as a Favorite report, the filter values that are customized in the Favorite reports are not displayed properly. This problem occurs when you generate a favorite report with customized filters and select that favorite report to view its details after generating the same report with default filters from ACS Reports section. **Workaround:** Refresh the Reports web interface.
CSCuq24409 Filter values displayed in the Saved Reports are incorrect.	The filter values for the Saved reports, ACS reports, and Favorite reports are displayed incorrectly. This problem occurs when you run Saved reports, ACS Reports, or Favorite reports with customized filter values. **Workaround:** Close the Reports web interface and open it again from ACS web interface. The filter values are displayed incorrectly in the Reports web interface, but, the generated report displays the correct information as ACS fetches the filter data from the database.
CSCuo87567 ACS 5.6 Reports web interface does not support a few Interactive viewer functionalities.	ACS 5.6 Reports web interface does not support the Interactive Viewer feature as a whole; however, the “show or hide columns” and “fixing columns” (constituents of Interactive Viewer feature) are supported. This problem occurs after you upgrade ACS to ACS 5.6 version. **Workaround:** Export the generated report to a CSV file. Open the CSV file with Microsoft Excel spreadsheet and use the excel options to obtain the missing interactive viewer functionalities.

Table 14 Known Issues in ACS 5.6 (continued)

Bug ID	Description
CSCuq06377 ACS displays all filters for saved reports even though some of the filters are disabled while saving the report.	ACS displays all filters for saved reports even though some of the filters are disabled while saving the report in Reports web interface. In general, for any saved reports, ACS displays only the customized filters. This problem occurs when you save a report with customized filters and select that saved report to view its details after generating the same report with default filters from ACS reports section. **Workaround:** Refresh the Reports web interface.
CSCuq21543 Day-wise authentication information is not displayed in the SGT Assignment Report.	ACS does not display the day-wise authentication information for SGT Assignment Report. This problem occurs when you generate SGT Assignment Report. **Workaround:** Generate the SGT Assignment Report with From and To date filters.
CSCuq21559 Incorrect time ranges are displayed when you cross launch reports from ACS Reports web interface.	Incorrect time ranges are displayed when you cross launch RADIUS and TACACS+ reports in ACS Reports web interface. This problem occurs when you cross launch RADIUS and TACACS reports from ACS Reports web interface. **Workaround:** The time ranges are displayed incorrectly in the Reports web interface, but, the generated report displays the correct information as ACS fetches the filter data from the database.
CSCuq22094 The filters of previously generated scheduled report is displayed when you view the details of another scheduled report.	The filters of previously generated scheduled report is displayed in the right pane when you select any scheduled report from Saved and Scheduled Report section to view its details on the right pane. This problem occurs when you have multiple scheduled reports and select a scheduled report to view its details on the right pane immediately after generating another scheduled report. **Workaround:** Refresh the Reports web interface.
CSCuq46862 From and To dates are not displayed on the right pane when you click a scheduled report from Reports web interface.	The From and To dates are not displayed on the right pane.when you select a scheduled report under Saved and Scheduled reports section to view its details on the right pane. This problem occurs when you schedule any ACS report with customized time range. **Workaround:** None This issue does not affect the scheduled report.

Table 14 Known Issues in ACS 5.6 (continued)

Bug ID	Description
CSCuq51480 ACS displays additional filters for saved reports even though some of the filters are disabled while saving the report.	ACS displays additional filters for saved reports even though some of the filters are disabled while saving the report in Reports web interface. In general, for any saved reports, ACS displays only the customized filters. This problem occurs when you save a report with customized filters and select that saved report to view its details after generating the same report with default filters from ACS reports section. **Workaround:** Refresh the Reports web interface and open the saved report from Saved reports section.
CSCuq56757 Incorrect From and To dates are displayed in ACS Reports web interface.	After generating a report, the From and To dates are displayed in the report web interface when you use the time range filter. But in ACS 5.6, the From and To date values are incorrectly displayed when you generate session directory reports with time range filter. This problem occurs when you generate the Session Directory reports with the time range filter applied. **Workaround:** The time ranges are displayed incorrectly in the Reports web interface, but, the generated report displays the correct information as ACS fetches the filter data from the database.

Documentation Updates

Table 15 lists the updates to *Release Notes for Cisco Secure Access Control System 5.6*.

Table 15 Updates to Release Notes for Cisco Secure Access Control System 5.6

Date	Description
10/27/2016	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.7, page 29
7/27/2016	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.6, page 27
5/24/2016	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.5, page 27
11/19/2015	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.4, page 25
4/27/2015	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.3, page 24.
11/27/2014	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.2, page 23.
10/08/2014	Added Resolved Issues in Cumulative Patch ACS 5.6.0.22.1, page 23.
9/26/2014	Cisco Secure Access Control System, Release 5.6.

Product Documentation

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

Table 16 lists the product documentation that is available for ACS 5.6. 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 16 Product Documentation

Document Title	Available Formats
Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
Migration Guide for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
User Guide for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html
CLI Reference Guide for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-command-reference-list.html
Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-device-support-tables-list.html
Installation and Upgrade Guide for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
Software Developer's Guide for Cisco Secure Access Control System 5.6	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-programming-reference-guides-list.html
Regulatory Compliance and Safety Information for Cisco Secure Access Control System	http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/regulatory/compliance/csacsrcsi.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Supplemental License Agreement

END USER LICENSE AGREEMENT SUPPLEMENT FOR CISCO SYSTEMS ACCESS CONTROL SYSTEM SOFTWARE:

IMPORTANT: READ CAREFULLY

This End User License Agreement Supplement ("Supplement") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this Supplement but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this Supplement, the terms and conditions of this Supplement will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this Supplement. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD

PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

1. Product Names

For purposes of this Supplement, the Product name(s) and the Product description(s) you may order as part of Access Control System Software are:

A. Advanced Reporting and Troubleshooting License

Enables custom reporting, alerting and other monitoring and troubleshooting features.

B. Large Deployment License

Allows deployment to support more than 500 network devices (AAA clients that are counted by configured IP addresses). That is, the Large Deployment license enables the ACS deployment to support an unlimited number of network devices in the enterprise.

C. Advanced Access License (not available for Access Control System Software 5.0, will be released with a future Access Control System Software release)

Enables Security Group Access policy control functionality and other advanced access features.

2. ADDITIONAL LICENSE RESTRICTIONS

- Installation and Use. The Cisco Secure Access Control System (ACS) Software component of the Cisco SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms are preinstalled. CDs containing tools to restore this Software to the SNS 3495, SNS 3415, and CSACS 1121 hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported Cisco Secure Access Control System Software Products on the Cisco SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms designed for its use. No unsupported Software product or component may be installed on the Cisco SNS 3495, SNS 3415, and CSACS 1121 Hardware Platform.
- Software Upgrades, Major and Minor Releases. Cisco may provide Cisco Secure Access Control System Software upgrades for the Cisco SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms as Major Upgrades or Minor Upgrades. If the Software Major Upgrades or Minor Upgrades can be purchased through Cisco or a recognized partner or reseller, the Customer should purchase one Major Upgrade or Minor Upgrade for each Cisco SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms. If the Customer is eligible to receive the Software release through a Cisco extended service program, the Customer should request to receive only one Software upgrade or new version release per valid service contract.
- Reproduction and Distribution. Customer may not reproduce nor distribute software.

3. DEFINITIONS

Major Upgrade means a release of Software that provides additional software functions. Cisco designates Major Upgrades as a change in the ones digit of the Software version number [(x).x.x].

Minor Upgrade means an incremental release of Software that provides maintenance fixes and additional software functions. Cisco designates Minor Upgrades as a change in the tenths digit of the Software version number [x.(x).x].

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc., End User License Agreement.

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Release Notes for Cisco Secure Access Control System 5.6