Release Notes for Cisco Secure Access Control System 5.8.1

Revised: July 5, 2018

This release notes pertain to the Cisco Secure Access Control System (ACS), Release 5.8.1, hereafter referred to as ACS 5.8.1. 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:

Introduction

This release of ACS introduces new hardware platforms for the ACS product. The ACS 5.8.1 software can now run on a dedicated Cisco SNS-3595 or a Cisco SNS-3515 appliance. This is in addition to the existing platforms that continue to be supported: Cisco SNS-3495 or Cisco SNS-3415 appliance, on a Cisco 1121 Secure Access Control System (CSACS-1121) or a VMware server. For more information on upgrade procedures, see Upgrading Cisco Secure ACS Software, page 6.

This release of ACS does not provide any new or enhanced functionality and is functionally equivalent to ACS 5.8. Throughout this document, Cisco SNS-3595, Cisco SNS-3515, Cisco SNS-3495, Cisco SNS-3415 and CSACS-1121 refer to the appliance hardware, and ACS server refers to ACS software.

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 5.8.1.

Supported Hardware

Cisco Secure ACS 5.8.1 ships on the following platforms:.

Table 1 Supported Hardware Platforms

Hardware Platform	Configuration
Cisco SNS-3595-ACS-K9	■ Cisco UCS C220 M4 ■ Dual socket Intel Xeon E5-2640 v3 series CPU @ 2.60GHz, 8 total cores, 8*2 total threads ■ 64 GB RAM ■ 4 x 600-GB disks ■ RAID 10 ■ 6 GbE network interfaces
Cisco SNS-3515-ACS-K9	■ Cisco UCS C220 M4 ■ Single socket Intel Xeon E5-2620 v3 series CPU @ 2.40GHz, 6 total cores, 6*2 total threads ■ 16 GB RAM ■ 1 x 600-GB disks ■ Embedded Software RAID 0 ■ 6 GbE network interfaces
Cisco SNS-3495-ACS-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

Table 1 Supported Hardware Platforms (continued)

Hardware Platform	Configuration
Cisco SNS-3415-ACS-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
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 to 64 GB RAM ■ NIC—1 GB NIC interface required (You can install up to 4 NICs.) ■ For supported VMware versions, see Supported Virtual Environments, page 5. ■ For information on VMware requirements, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1*.

Note: Cisco recommends you to use more than a 4GB RAM platform for a deployment that has more than 100,000 devices. ACS runtime crashes when you use a machine with 4GB RAM or less in a deployment that has more than 100,000 devices.

Supported Virtual Environments

ACS 5.8.1 supports the following VMware versions:

- VMware ESXi 5.5
- VMware ESXi 5.5 Update 1
- VMware ESXi 5.5 Update 2
- VMware ESXi 5.5 Update 3
- VMware ESXi 6.0 Update 2

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 5.8.1*.

Supported Browsers

You can access the ACS 5.8.1 administrative user interface using the following browsers:

ACS 5.8.1 supports the following browser platforms:

- MAC OS
  - 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 45.0.2 ESR
- Windows 7 32-bit and Windows 7 64-bit
  - Internet Explorer version 11.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 38.4.0 ESR
- Mozilla Firefox version 38.5.2 ESR
- Mozilla Firefox version 45.0.2 ESR

- Windows 8.*x*
  - Internet Explorer version 10.x (Windows 8)
  - Internet Explorer version 11.x (Windows 8.1)
  - 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 38.5.2 ESR
  - Mozilla Firefox version 45.0.2 ESR

Note: Mozilla Firefox version 46.x or later is supported only after installing ACS 5.8 patch 3 or later on top of ACS 5.8.1 release.

Note: 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.

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 5.8.1*.

New Features in ACS 5.8.1 Release

There is no new or enhanced functionality in ACS 5.8.1 and it is functionally equivalent to ACS 5.8. However, the following sections describe the new hardware platforms supported in ACS 5.8.1 release:

- Cisco SNS 3515 and 3595 appliances support, page 6

Cisco SNS 3515 and 3595 appliances support

ACS 5.8.1 supports two new Hardware Appliances called Cisco SNS-3515 and Cisco SNS-3595. ACS 5.8.1 is shipped with SNS-3515 or SNS-3595 depending on the requirements from the customer. For more information on SNS-3515 and SNS-3595 appliances, see Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1.

Upgrading Cisco Secure ACS Software

Cisco Secure Access Control System (ACS) supports upgrades from different versions of ACS 5.*x* to ACS 5.8.1. The supported upgrade paths include:

- Cisco Secure ACS, Release 5.5, recommended with latest patch applied
- Cisco Secure ACS, Release 5.6, recommended with latest patch applied
- Cisco Secure ACS, Release 5.7, recommended with latest patch applied
- Cisco Secure ACS, Release 5.8, 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 5.8.1*. to upgrade to Cisco Secure ACS, Release 5.8.1.

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 5.8.1.

This section contains:

Installing, Setting Up, and Configuring Cisco SNS 3500 Series Appliances

ACS 5.8.1 is shipped with Cisco SNS-3515 or SNS-3595 appliances depending on the customer requirements. The SNS-3595 and SNS-3515 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 5.8 on this appliance. For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.8*.

This section describes how to install, set up and configure the Cisco SNS-3595 and Cisco SNS-3515 appliance. The Cisco SNS-3595 and Cisco SNS-3515 appliance are preinstalled with the software.

To set up and configure the Cisco SNS-3595 and Cisco SNS-3515:

1. Open the box containing the Cisco SNS-3595 and Cisco SNS-3515 appliances and verify that it includes:

- The Cisco SNS-3595 and Cisco SNS-3515 appliance
- Power cord
- KVM cable
- Cisco information packet
- Warranty card

- *Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.8*

2. Go through the specifications of the Cisco SNS-3595 or Cisco SNS-3515 appliance.

For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.8*.

3. Read the general precautions and safety instructions that you must follow before installing the Cisco SNS-3515 or Cisco SNS-3595 appliance.

For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.8* and pay special attention to all safety warnings.

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-3595 or Cisco SNS-3515 appliance, see the *Installation and Upgrade guide for the Cisco Secure Access Control System 5.8*.

5. Connect the Cisco SNS-3595 or Cisco SNS-3515 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 5.8* for illustrations of the front and back panel of the Cisco SNS-3595 and Cisco SNS-3515 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 5.8*.

For information on installing ACS 5.8 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 5.8*.

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 5.8*.

Installing, Setting Up, and Configuring Cisco SNS 3400 Series Appliances

You can install ACS software on Cisco SNS-3495 and SNS-3415 appliances. These 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 software on this appliance. For more details, see the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.8.1*.

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:

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 5.8.1*

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 5.8.1*.

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 5.8.1* and pay special attention to all safety warnings.

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 5.8.1.*

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 5.8.1* 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 5.8.1*.

For information on installing ACS 5.8.1 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 5.8.1*.

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 5.8.1*.

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:

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 5.8.1*

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 5.8.1*.

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 5.8.1* and pay special attention to all safety warnings.

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 5.8.1.*

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.

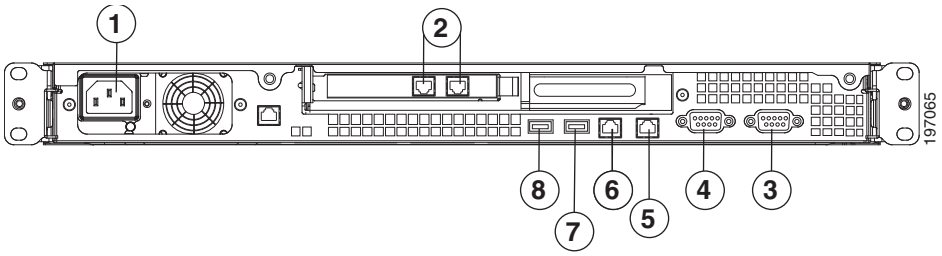
Figure 1 on page 10 shows the back panel of the CSACS-1121 Series appliance and the various cable connectors.

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 5.8.1.*

For information on installing ACS 5.8.1 on VMware, see the "Installing ACS in a VMware Virtual Machine" chapter in the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1.*

Figure 1 CSACS 1121 Series Appliance Rear View



The following table describes the callouts in Figure 1 on page 10.

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

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 10.

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 5.8.1 server that is using the setup program. The setup process is a one-time configuration task.

To configure the ACS server:

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 2 on page 11.

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

Table 2 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.

Table 2 Network Configuration Prompts (continued)

Prompt	Default	Conditions	Description
SSH Service	None, network specific	None.	To enable SSH service, enter **y**.
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 5.8.1 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 5.8.1

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 3 on page 13 lists the types of licenses that are available in ACS 5.8.1.

Table 3 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 5.8.1 does not support auto installation of the evaluation license. Therefore, if you need an evaluation version of ACS 5.8.1, then you must obtain the evaluation license from Cisco.com and install ACS 5.8.1 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 5.5, ACS 5.6, ACS 5.7, or ACS 5.8 installed on your machine, you can upgrade to ACS 5.8.1 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 5.8.1, followed by a restore of the backup taken in ACS 5.5, 5.6, 5.7, or ACS 5.8, to move to ACS 5.8.1 Release.

See the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1* for information on upgrading your ACS server.

Note: You must provide full permission to NFS directory when you configure the NFS location using the **backup-staging-url** command in ACS 5.8.1 to perform a successful On Demand Backup.

Applying Cumulative Patches

Periodically, patches will be posted on Cisco.com that provide fixes to ACS 5.8.1. These patches are cumulative. Each patch includes all the fixes that were included in previous patches for the release.

You can download ACS 5.8.1 cumulative patches from the following location:

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

The ACS 5.8 and 5.8.1 releases are functionally equivalent and only difference is the set of hardware platforms that are supported. Therefore a common set of patches are provided that can be installed on either ACS 5.8 or ACS 5.8.1. For more information on ACS 5.8 patches, see Resolved Issues in Cumulative Patch ACS 5.8.0.32.1.

To download and apply the patches:

1. Log in to Cisco.com and navigate to **Products > Security > Access Control and Policy > Cisco Secure Access Control System > Cisco Secure Access Control System 5.8**.
2. Download the patch.
3. Install the ACS 5.8 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

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]?
```

5. The ACS 5.8 patch 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.

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.

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: 5.8.1.4
Internal Build ID: B.462
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.

Limitations in ACS Deployments

Table 4 on page 15 describes the limitations in ACS deployments.

Table 4 Limitations in ACS Deployments

Object Type	ACS System Limits
ACS Instances	22
Hosts	■ 200,000 for DelNorte appliance ■ 150,000 for other appliances
Users	■ 400,000 for DelNorte appliance ■ 300,000 for other appliances
Identity Groups	1,000
Active Directory Group Retrieval	1,500

Table 4 Limitations in ACS Deployments

Object Type	ACS System Limits
Network Devices	■ 150,000 on DelNorte appliance ■ 100,000 on other appliances
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)	20,000
ACS Admins	50
	9 static roles
dACLs	600 dACL with 100 ACEs each

Using the Bug Search Tool

This section explains how to use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Search Bugs Using the Bug Search Tool

Use the Bug Search Tool to view the list of outstanding and resolved bugs in a release.

1. Go to https://tools.cisco.com/bugsearch/search.
2. At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.

Note: If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

3. To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.
4. To search for bugs in the current release:
   a. Click **Select from list** link. The Select Product page is displayed.
   b. Choose **Security > Access Control and Policy > Cisco Secure Access Control system > Cisco Secure Access Control System 5.8.1**.
   c. Click **OK**.
   d. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs based on different criteria such as status, severity, and modified date.

Export to Spreadsheet

The Bug Search Tool provides the following option to export bugs to an Excel spreadsheet:

Click **Export Results to Excel** link in the Search Results page under the Search Bugs tab to export all the bug details from your search to the Excel spreadsheet. Presently, up to 10000 bugs can be exported at a time to an Excel spreadsheet.

If you are unable to export the spreadsheet, log in to the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Documentation Updates

Table 5 on page 17 lists the updates to *Release Notes for Cisco Secure Access Control System 5.8.1*.

Table 5 Updates to Release Notes for Cisco Secure Access Control System 5.8.1

Date	Description
3/21/2016	Cisco Secure Access Control System, Release 5.8.1.

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 6 on page 18 lists the product documentation that is available for ACS 5.8.1. 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 > Cisco Secure Access Control System > Cisco Secure Access Control System 5.8.1**.

Table 6 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 5.8.1	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 5.8.1	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 5.8.1	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 5.8.1	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 5.8.1	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 5.8.1	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/5-8-1/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:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

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 3595, SNS 3515, SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms are preinstalled. CDs containing tools to restore this Software to the SNS 3595, SNS 3515, SNS 3495, SNS 3415, and CSACS 1121 hardware are provided to Customer for re installation purposes only. Customer may only run the supported Cisco Secure Access Control System Software Products on the Cisco SNS 3595, SNS 3515, SNS 3495, SNS 3415, and CSACS 1121 Hardware Platforms designed for its use. No unsupported Software product or component may be installed on the SNS 3595, SNS 3515, 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 3595, SNS 3515, 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 3595, SNS 3515, 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.