Release Notes for Cisco Secure Access Control System 5.8

Revised: October 5, 2018

This release notes pertain to the Cisco Secure Access Control System (ACS), Release 5.8, hereafter referred to as ACS 5.8. 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.

Note: ACS 5.8 and ACS 5.8.1 releases are functionally equivalent, except that the ACS 5.8.1 release supports additional hardware platforms. These two releases leverage common patches and the details for patches included in this document apply to both ACS 5.8 and 5.8.1 releases.

This document contains:

Introduction

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

The ACS 5.8 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 5.8 ships on Cisco SNS-3495 and Cisco SNS-3415 appliances. However, ACS 5.8 continues to support CSACS-1121 appliance. For more information on upgrade paths, see Upgrading Cisco Secure ACS Software, page 14.

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.

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.

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

Supported Hardware

Cisco Secure ACS 5.8 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
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*.

Cisco Secure ACS 5.8.1 supports the following two additional platforms in addition to the above mentioned hardware platforms:

Table 2 Hardware Platforms Additionally Supported by ACS 5.8.1

Hardware Platform	Configuration
Cisco SNS-3595-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-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

For more information about the supported hardware platforms for ACS 5.8.1, see *Release Notes 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 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
- VMware ESXi 6.0 Update 2
- VMware ESXi 6.0 Update 3 (validated with ACS 5.8 patch 9)

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*.

Supported Browsers

You can access the ACS 5.8 administrative user interface using the following browsers:

- MAC OS
  - 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* (supported only after installing ACS 5.8 patch 3 or later)
  - Mozilla Firefox version 47.*x*
  - Mozilla Firefox version 48.*x*
  - Mozilla Firefox version 49.*x*
  - Mozilla Firefox version 50.*x*
  - Mozilla Firefox version 51.*x*
  - Mozilla Firefox version 52.*x* (supported only after installing ACS 5.8 patch 7 or later)
  - Mozilla Firefox version 53.*x* (supported only after installing ACS 5.8 patch 8)
  - Mozilla Firefox version 54.*x*
  - Mozilla Firefox version 55.*x* (supported only after installing ACS 5.8 patch 9 or later)
  - Mozilla Firefox version 56.*x*

- Mozilla Firefox version 57.*x*
- Mozilla Firefox version 58.*x*
- Mozilla Firefox version 60.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 61.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 62.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 38.2.0 ESR
- Mozilla Firefox version 45.0.2 ESR
- Mozilla Firefox version 45.4 ESR
- Mozilla Firefox version 45.5 ESR
- Mozilla Firefox version 45.6 ESR
- Mozilla Firefox version 45.7 ESR
- Mozilla Firefox version 45.8 ESR (supported only after installing ACS 5.8 patch 8)
- Mozilla Firefox version 45.9 ESR
- Mozilla Firefox version 52.0 ESR
- Mozilla Firefox version 52.1 ESR
- Mozilla Firefox version 52.2 ESR
- Mozilla Firefox version 52.3.0 ESR (supported only after installing ACS 5.8 patch 9)
- Mozilla Firefox version 52.4.0 ESR
- Mozilla Firefox version 52.5.0 ESR
- Mozilla Firefox version 52.6.0 ESR
- Mozilla Firefox version 60.2.2 ESR (supported only after installing ACS 5.8 patch 10 or later)

- Windows 7 32-bit and Windows 7 64-bit
  - Internet Explorer version 11.*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* (supported only after installing ACS 5.8 patch 3 or later)

- Mozilla Firefox version 47.*x*
- Mozilla Firefox version 48.*x*
- Mozilla Firefox version 49.*x*
- Mozilla Firefox version 50.*x*
- Mozilla Firefox version 51.*x*
- Mozilla Firefox version 52.*x* (supported only after installing ACS 5.8 patch 7 or later)
- Mozilla Firefox version 53.*x* (supported only after installing ACS 5.8 patch 8)
- Mozilla Firefox version 54.*x*
- Mozilla Firefox version 55.*x* (supported only after installing ACS 5.8 patch 9)
- Mozilla Firefox version 56.*x*
- Mozilla Firefox version 57.*x*
- Mozilla Firefox version 58.*x*
- Mozilla Firefox version 60.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 61.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 62.*x* (supported only after installing ACS 5.8 patch 10 or later)
- Mozilla Firefox version 38.1.0 ESR
- Mozilla Firefox version 38.2.0 ESR
- Mozilla Firefox version 45.0.2 ESR
- Mozilla Firefox version 45.4 ESR
- Mozilla Firefox version 45.5 ESR
- Mozilla Firefox version 45.6 ESR
- Mozilla Firefox version 45.7 ESR
- Mozilla Firefox version 45.8 ESR (supported only after installing ACS 5.8 patch 8)
- Mozilla Firefox version 45.9 ESR
- Mozilla Firefox version 52.0 ESR
- Mozilla Firefox version 52.1 ESR
- Mozilla Firefox version 52.2 ESR
- Mozilla Firefox version 52.3.0 ESR (supported only after installing ACS 5.8 patch 9)
- Mozilla Firefox version 52.4.0 ESR
- Mozilla Firefox version 52.5.0 ESR
- Mozilla Firefox version 52.6.0 ESR
- Mozilla Firefox version 60.2.2 ESR (supported only after installing ACS 5.8 patch 10 or later)

- Windows 8.*x*
  - Internet Explorer version 11.*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* (supported only after installing ACS 5.8 patch 3 or later)
  - Mozilla Firefox version 47.*x*
  - Mozilla Firefox version 48.*x*
  - Mozilla Firefox version 49.*x*
  - Mozilla Firefox version 50.*x*
  - Mozilla Firefox version 51.*x*
  - Mozilla Firefox version 52.*x* (supported only after installing ACS 5.8 patch 7 or later)
  - Mozilla Firefox version 53.*x* (supported only after installing ACS 5.8 patch 8)
  - Mozilla Firefox version 54.*x*
  - Mozilla Firefox version 55.*x* (supported only after installing ACS 5.8 patch 9)
  - Mozilla Firefox version 56.*x*
  - Mozilla Firefox version 57.*x*
  - Mozilla Firefox version 58.*x*
  - Mozilla Firefox version 60.*x* (supported only after installing ACS 5.8 patch 10 or later)
  - Mozilla Firefox version 61.*x* (supported only after installing ACS 5.8 patch 10 or later)
  - Mozilla Firefox version 62.*x* (supported only after installing ACS 5.8 patch 10 or later)
  - Mozilla Firefox version 38.2.0 ESR
  - Mozilla Firefox version 45.0.2 ESR
  - Mozilla Firefox version 45.4 ESR
  - Mozilla Firefox version 45.5 ESR
  - Mozilla Firefox version 45.6 ESR
  - Mozilla Firefox version 45.7 ESR
  - Mozilla Firefox version 45.8 ESR (supported only after installing ACS 5.8 patch 8)
  - Mozilla Firefox version 45.9 ESR

- Mozilla Firefox version 52.0 ESR
- Mozilla Firefox version 52.1 ESR
- Mozilla Firefox version 52.2 ESR
- Mozilla Firefox version 52.3.0 ESR (supported only after installing ACS 5.8 patch 9)
- Mozilla Firefox version 52.4.0 ESR
- Mozilla Firefox version 52.5.0 ESR
- Mozilla Firefox version 52.6.0 ESR
- Mozilla Firefox version 60.2.2 ESR (supported only after installing ACS 5.8 patch 10 or later)

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*.

New Features in ACS 5.8 Release

The following sections briefly describe the new features in the 5.8 release:

Active Directory Enhancements

ACS 5.8 web interface includes the following new options in the Active Directory page:

- **Advanced Tuning**—The advanced tuning feature provides node-specific changes and settings to adjust parameters deeper in the system. This tab allows configuration of preferred Domain Controllers, Global Catalogs, Domain Controller fail over parameters, and timeouts. This page also provides troubleshooting options such as disabling encryption. These settings are not intended for normal administration flow and should be used only under Cisco Support guidance.
- **Authentication Domains**—This option allows you to restrict ACS to a subset of authentication domains while interacting with the Active Directory deployments. Configuring authentication domains enables you to select specific domains so that the authentications are performed against the selected domains only. Authentication domains improve security because they instruct ACS to authenticate users only from selected domains and not from all trusted domains.

- **Diagnostic Tool**—The Diagnostic Tool is a service that runs on every Cisco ACS node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when ACS uses Active Directory. It helps you to detect the problems with networking, firewall configurations, clock sync, user authentication, and so on when ACS uses Active Directory.
- **Ambiguous Identity Resolution**—If the user or machine name received by ACS is ambiguous, that is, it is not unique, it can cause problems for users when they try to authenticate. Identity clashes occur in cases when the user does not have a domain markup, or when there are multiple identities with the same username in more than one domain. For example, userA exists on domain1 and another userA exists on domain2. You can use the identity resolution setting to define the scope for the resolution for such users. Cisco highly recommends you to use qualified names such as UPN or NetBIOS. Qualified name reduces chances of ambiguity and increases performance by reducing delays.
- **Enable Kerberos for PAP authentications**—Prior to version 5.8, ACS used Kerberos protocol for PAP authentications. But, ACS 5.8 uses MS-RPC protocol for PAP authentications by default. If you want to use Kerberos protocol for PAP authentications in ACS 5,8, then you must check the **Use Kerberos for Plain Text** check box in **User and Identity Stores > External Identity Stores > Active Directory** page.

ACS 5.8 introduces the following new alarms and reports to monitor and troubleshoot Active Directory-related activities.

The following alarms are triggered for Active Directory errors and issues:

- Configured name server not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ACS account password update failed
- AD: Machine TGT refresh failed

You can monitor Active Directory-related activities using the following reports:

- RADIUS Authentications Report—This report shows detailed steps of the Active Directory RADIUS authentication and authorization. You can find this report here: Launch **Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > RADIUS Authentications**.
- TACACS+ Authentications Report—This report shows detailed steps of the Active Directory TACACS+ authentication and authorization. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > TACACS Authentications**.
- AD Connector Operations Report—The AD Connector Operations report provides a log of background operations performed by AD connector, such as ACS server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > ACS Instance > AD Connector Operations**.

For more information on Active Directory integration in ACS 5.8, see Active Integration in ACS 5.8 Guide and User Guide for Cisco Secure Access Control System 5.8.

Note: When you face permission issue for tokenGroups in ACS 5.8, run the below command in the Active Directory servers:

```
dscals "DC=medaille,DC=edu" /I:T /G "acsServerHostName$":rp;tokenGroups
```

Note: In ACS 5.8, you must manually join ACS to Active Directory after upgrading ACS 5.x to ACS 5.8. See Installation and Upgrade Guide for Cisco Secure Access Control System for more information on upgrade methods.

Note: Prior to Release 5.8, ACS started the adclient process only after joining the Active Directory domain to ACS. But, ACS 5.8 starts the adclient process soon after installing it.

Note: Previous releases of ACS disconnects the Active Directory domain and displays the status as “joined but disconnected” in the Active Directory connection details page, when you stop the ad-client process manually from ACS CLI. But in ACS 5.8, when you stop the ad-client process manually from ACS CLI, ACS disconnects Active Directory domain and displays the status as “None” in Active Directory connection details page. If you start the ad-client process again from ACS CLI, ACS gets connected to the Active Directory domain and displays the status as “joined and connected” in AD connection details page.

Authenticating Administrators against RADIUS Identity and RSA SecurID Servers

Previous releases of ACS support authenticating ACS administrators only against AD or LDAP external identity stores. But, ACS 5.8 supports authenticating administrators against RADIUS Identity and RSA SecurID servers. This feature is available in both the ACS web interface and ACS configuration mode of ACS CLI. This feature provides additional security to administrator authentications by using an One Time Password (OTP) that the RADIUS Identity or RSA SecurID server generates. For information on how to authenticate administrators against RSA Identity and RADIUS SecurID servers, see the User Guide for Cisco Secure Access Control System 5.8.

Exporting Policies from ACS Web Interface

ACS 5.8 allows you to export policies and policy elements from the ACS web interface as an XML file to a remote repository or to email ids that you have configured. You can perform an instant export or schedule it for a future day and time. ACS exports the policies as an XML file and encrypts it with a password that you can use for decrypting the XML file. You must have an administrator account with SuperAdmin role to export policies from the ACS web interface. ACS does not export access service policies of type external proxy. Fore more information on exporting policies, see the User Guide for Cisco Secure Access Control System 5.8.

Changing Internal User Passwords using REST API

ACS allows you to change the user password using REST APIs. You can use the **GET** method from REST API to retrieve the change password XML file from ACS. You can enter the old password and new password in the retrieved XML file and use the **PUT** method to update the password in ACS. This feature is applicable only for internal users. For more information on changing internal user password using the from REST API, see the Software Developer’s Guide Cisco Secure Access Control System.

Internal Administrator Password Hashing

To enhance security, ACS 5.8 introduces a new feature, “Enable Password Hash.” ACS runtime process must be up and running properly for this option to work. For information on hashing administrator password, see the User Guide for Cisco Secure Access Control System 5.8.

EAP-FAST Authentications with Cisco IP Phone

Cisco IP phone implements a specific use case of EAP-FAST for conducting certificate based authentications. Cisco IP phone expects the authentication server to send a certificate request during EAP-FAST authentication tunnel establishment and responds back with the certificate. ACS validates the certificate and if the certificate validation is successful, then ACS skips the inner method. Therefore, ACS must differentiate the EAP-FAST authentication with Cisco IP phone and other supplicants. To enable certificate request for EAP-FAST authentication with Cisco IP phones, ACS introduces new options under **Access Policies > Access Services > Create > Allowed Protocols >Allow EAP-FAST** page.

- If you use PACs, then you must check the **Accept Client Certificate For Provisioning** check box for ACS to differentiate Cisco IP phones from other supplicants.
- If you do not use PACs, you must check the **Accept Client Certificate** check box in ACS to differentiate Cisco IP phones from other supplicants.

FIPS 140-2 Level 1 Compliance

ACS 5.8 is compliant with Federal Information Processing Standard (FIPS) 140-2 Level 1. ACS uses an embedded FIPS 140-2 Level 1 implementation using validated C3M and NSS modules, per the FIPS 140-2 Implementation Guidance section G.5 guidelines. The key size of Certificate Authority certificates and server certificates that are used in ACS should be greater than or equal to 2048 bits. The key size of client

certificate should be greater than or equal to 1024 bits. In FIPS mode, ACS does not support PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-MD5, LEAP, and Anonymous PAC Provisioning in EAP-FAST protocols. For more information on how to enable FIPS in ACS, see the User Guide for Cisco Secure Access Control System 5.8.

New Features Introduced in ACS 5.8 Patch 4

ACS 5.8 Patch 4 introduces the following new features:

TLS 1.2 Settings

ACS 5.8 after installing patch 4, enables TLS 1.2 for both browser access and runtime (AAA) access by default. For compatibility reasons, ACS allows you to enable and disable TLS 1.0 using the configuration available in **System Administration > Configuration > Global System Options > Security Settings** page.

For HTTPS, TLS 1.0 can be enabled/disabled using the “Enable TLS 1.0 for https access” option. This configuration will restart the management in Primary ACS. However, management services needs to be restarted manually in all the other secondary nodes in the ACS deployment for the changes to take effect.

By default, TLS 1.1 and 1.2 are enabled for GUI access and it is not possible to disable TLS 1.1.

For AAA access, runtime is enabled with all the TLS protocol versions 1.0, 1.1 and 1.2. ACS allows you to enable/disable TLS 1.0 using the “Enable TLS 1.0 only for legacy clients” option.

To disable SHA-1 specific ciphers for AAA access, uncheck the **Enable SHA-1 only for legacy clients** check box in the security settings page.

For more information on configuring security settings, see *User Guide for Cisco Secure Access Control System,* 5.8.

Allowing Weak Ciphers for EAP

ACS 5.8 after installing patch 4, allows using weak ciphers such as RC4-SHA and RC4-MD5 for legacy clients. This option is disabled by default.

To enable the weak ciphers, ACS introduces an option “Allow weak ciphers for EAP” in the list of authentication protocols under the Allowed Protocols. For more information, see *User Guide for Cisco Secure Access Control System, 5.8*.

Note: If FIPS is enabled, ACS will not allow you to enable this option and vice-versa.

Support for Elliptic Curve Cryptography (ECC) Certificates

ACS 5.8 patch 4 supports ECC ciphers in the authentication flow to provide high security. Following are few relaxations for ECC certificates if FIPS is enabled.

- The minimum supported key size for ECC certificate is 224 (which is equal to 2048 of RSA key size).
- There is no check for PKCS#8 format for private key. Non-PKCS#8 format for EC type should be allowed even in FIPS mode.

Note: ECC ciphers are supported only for AAA flows.

New Features Introduced in ACS 5.8 Patch 7

The following sections briefly describe the new features in ACS 5.8 Patch 7 release:

Authorizing Internal Users When the Password Type is set to RSA SecurID Token Server/RADIUS Identity Server

When the **Treat authorization is passed for internal user with password type set to this identity source** option (under **Advanced** tab in RSA SecurID token server/RADIUS identity server page) is enabled, authorization is passed for an unknown user if the user is found in the internal identity store and the password type is set to RSA SecurID token server/RADIUS identity server. When this option is enabled, authorization is passed always even if the user is not authenticated by this node previously and there is no corresponding entry in cache. This option is disabled by default.

Note: We strongly recommend that you enable this option only when you are using a NAS (such as, Cisco 5508 Wireless controller) that sends authentication and authorization requests to different AAA servers in a high-availability setup. Otherwise, we recommend that you always disable this option.

In a high-availability configuration, sometimes NAS sends TACACS+ authentication and authorization requests to different AAA servers. NAS sends authentication request to a AAA server and at the same time, sends the authorization/accounting request for the same user to another AAA server that is configured in the Authentication/Authorization Servers list on NAS. In this case, authentication succeeds, but the authorization fails with “User record was not found in the cache” message.

The user details are cached during authentication because User Lookups are not supported by RSA SecurID servers. ACS caches results of successful authentications and will process User Lookup requests against the cache. The authorization fails when the request is sent to a different ACS server (where authentication was not performed), because the cache (local to a server) is not replicated among ACS nodes in the deployment and hence user details would not be available in that cache. In such cases, you can enable this option to prevent this issue.

Internal Users Cache Mechanism

The cache mechanism is applicable only for TACACS+ authorization flow for internal users.

When this option is enabled, the username and user specific attributes read from the internal database are stored in the cache after the first successful authorization request, for the specified time period. You can also specify the time (TTL) for which the user details are to be stored in the cache. The valid range is from 1 to 5 minutes. Till the TTL expires, the authorization is passed if the user entry is found in the cache. The user entry is removed from the cache when the TTL is expired.

This option is disabled by default. You can enable this option to improve performance especially when scripts generating TACACS+ requests at high rate are used.

Configuring Log Accounting Updates

When the **Skip Log Accounting Updates** option (under **System Administration > Configuration > Log Configuration > Logging Categories > Global**) is enabled, accounting update packets are not sent to the log collector. This feature is applicable only for Accounting (update packets)—Radius Accounting (interim–update) and TACACS accounting (watchdog) logging category type.

This reduces the volume of logs stored and can be used for better data storage resiliency.

New Features Introduced in ACS 5.8 Patch 8

The following sections briefly describe the new features in ACS 5.8 Patch 8 release:

Exporting Reports to Local Machine

After installing ACS 5.8 patch 8, you can also export the reports to your local system as a .csv file and a pdf file in addition to exporting the reports to a repository. The reports that have multiple tables or graph can be exported only as a pdf file.

ACS allows you to export only 25000 records when you export the reports to your local system as a .csv or pdf file.

Wild Card Character Support for MAC Address of End Station or Destination

After installing ACS 5.8 patch 8, you can use the wildcard character ? for the MAC addresses of end stations or destinations that you want to permit or deny access to. For example, 1?-22-33-44-55-66, 1A-2?-3C-4D-5E-6F, or AA-BB-CC-D?-EE-FF.

Upgrading Cisco Secure ACS Software

Cisco Secure Access Control System (ACS) supports upgrades from different versions of ACS 5.*x* to ACS 5.8. 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

Follow the upgrade instructions in the Installation and Upgrade Guide for *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8*. to upgrade to Cisco Secure ACS, Release 5.8.

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.

This section contains:

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*.

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*

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*.

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* 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.*

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* 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*.

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 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*

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*.

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* 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.*

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.

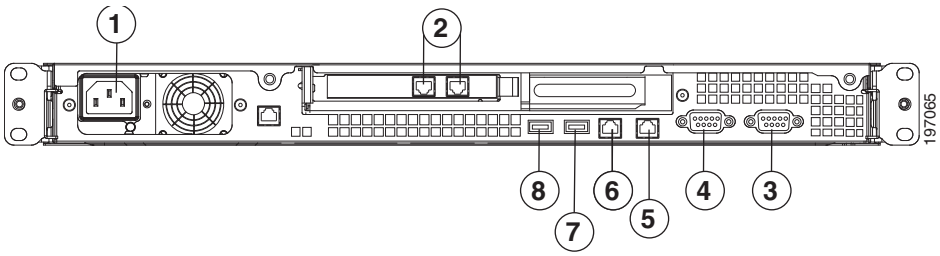
Figure 1 on page 16 shows the back panel of the CSACS-1121 Series appliance and the various cable connectors.

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.*

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 Cisco Secure Access Control System 5.8.*

Figure 1 CSACS 1121 Series Appliance Rear View



The following table describes the callouts in Figure 1 on page 16.

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 17.

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 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 3 on page 18.

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.

Table 3 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 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

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 on page 20 lists the types of licenses that are available in ACS 5.8.

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

See the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8* 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-stagging-url** command in ACS 5.8 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 and 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 5.8/5.8.1 cumulative patches from the following location:

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

To download and apply the patches:

1. Log in to Cisco.com and navigate to **Products > Security > Access Control and Policy > Secure Access Control System > Secure Access Control System 5.8 > Secure Access Control System Software-5.8.0.32**.
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 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.

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: 5.8.0.32
Internal Build ID: B.442
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.

Note: When you upgrade from ACS 5.8 patch 1 to ACS 5.8 patch 2, PUT CLEAR operation requires the password field even if the password value is not updated.

Limitations in ACS Deployments

Table 5 on page 22 describes the limitations in ACS deployments.

Table 5 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

Table 5 Limitations in ACS Deployments

Object Type	ACS System Limits
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

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**.
   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).

Resolved Issues in ACS 5.8

Table 6 on page 25 lists the issues that are resolved in ACS 5.8.

Table 6 Resolved Issues in ACS 5.8

Bug ID	Description
CSCua13802	The system status and the AAA status are shown as not available and zero in the dashboard.
CSCuc16427	Exporting records to a.csv file using the timestamps option does not work properly.
CSCuq62466	Remote database export operation fails while exporting data from ACS to Microsoft SQL due to the presence of junk characters in the data. This issue is now resolved.
CSCur27402	Unable to Schedule reports in ACS 5.6 Reports web interface.
CSCur57298	Need to increase the up-delay timer to 10 seconds while configuring bond 0 in ACS.
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.
CSCus42781	OpenSSL Vulnerabilities were found in ACS during January 2015. This issue is now resolved.
CSCus43434	Context limit is reached if ACS receives a reset request during packet processing. This issue is now resolved.
CSCus45389	ACS drops the RADIUS requests when Vendor Specific Attribute field is empty and VendorTypeField size is 1.
CSCus63338	ACS View dashboard displays an error when you add a new layouts.
CSCus64232	Customizing TACACS+ policy elements logs the user session out in ACS 5.*x* web interface.
CSCus79395	In ACS, the coaport:integer field is missing in the resulting file while exporting devices.
CSCus84600	ACS displays an error while resetting user passwords.
CSCus87461	Unable to use multiple filters for filtering AAA clients in ACS.
CSCus97002	Favorite reports in ACS 5.6 does not display any data.
CSCut05442	ACS displays the IP subnet overlap error message incorrectly. This issue is now resolved.
CSCut06874	ACS logs out the session if the authorization profile contains double quotes.
CSCut20508	Configuring excluded IP range for a network device can cause an overlap with the other subnets in ACS.
CSCut46073	OpenSSL Vulnerabilities were found in ACS during March 2015. This issue is now resolved.
CSCut55144	Issues with special characters in ACS 5.x.
CSCut75184	ACS considers the parentheses as an invalid character.
CSCut87378	ACS runtime crashes frequently during authentications. This issue is now resolved.
CSCut94394	Unable to start temporary database when you restart ACS services. This issue is now resolved.
CSCut98350	Read only administrators in ACS are unable to see the Active Directory Status.
CSCuu11002	Reflected XSS vulnerability is found in ACS 5.x.
CSCuu11005	Local file inclusion vulnerability is found in ACS 5.x
CSCuu30320	ACS server does not identify the passcode cache timeout option that is configured from ACS web interface. This issue is now resolved.
CSCuu42929	End Station Filters limitation has to be relaxed in ACS 5.x. This issue is now resolved.
CSCuu43343	ACS does not allow special characters for KEK and MACK keys of Network devices. This issue is now resolved.
CSCuu59807	Replication issues are identified due to administrator account password change in ACS 5.x. This issue is now resolved.
CSCuu81221	Unable to delete the old subordinate CAs after installing a new CA certificate. This issue is now resolved.

Table 6 Resolved Issues in ACS 5.8 (continued)

Bug ID	Description
CSCuu85461	The “acs patch install” command is not working in ACS 5.*x*.
CSCuu91166	ACS displays a blank page for reports when you open a user report whose username is provided with NetBIOS name.
CSCuu93287	The report links that are provided in an email notification for alarms does not work in ACS.
CSCuu94829	ACS 5.x displays an incorrect device name when ACS identifies an overlapping IP range. This issue is now resolved.
CSCuv03303	ACS does not properly send emails when you export reports from ACS web interface.
CSCuv12144	Identity policy with “UseCase=Host Lookup' is now working properly in ACS.
CSCuv20514	Issues were found when you restore ACS 5.5 View database. This issue is now resolved.
CSCuv22775	Unable to add static routes after enabling NIC bonding in ACS.
CSCuv32799	TCP dumps stops working after upgrading ACS to ACS 5.7.
CSCuv39328	The management services in ACS fails to respond when you search reports in ACS using filtering options.
CSCuv42038	The advanced drop option does not drop the TACACS+ requests in ACS 5.x. This issue is now resolved.
CSCuv46911	The default configuration of ACS 5.*x* includes SNMPv2 read community public string.
CSCuv63197	ACS runtime crashes when the last EAP fragment length is greater than the total EAP fragment length. This issue is now resolved.
CSCuv72012	ACS 5.*x* fails to add duplicate certificates.
CSCuv73286	ACS fails to upgrade successfully when you upgrade ACS 5.3 on a VMware appliance to ACS 5.7.
CSCuv88723	Issues are found while changing ACS administrator password if the password includes < or > characters.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.1

Table 7 on page 26 lists the issues that are resolved in the ACS 5.8.0.32.1 cumulative patch. You can download the ACS 5.8.0.32.1 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.1 patch can also be installed on ACS 5.8.1.4.

Table 7 Resolved Issues in Cumulative Patch ACS 5.8.0.32.1

Bug ID	Description
CSCuv67311	Improve TPS for MS-RPC based multiple simultaneous requests through Active Directory.
CSCux66025	Memory increased while retrieving Active Directory groups or attributes from ACS web interface.
CSCux66660	ACS management services are not responding after restoring a full back up.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.2

Table 8 on page 27 lists the issues that are resolved in the ACS 5.8.0.32.2 cumulative patch. You can download the ACS 5.8.0.32.2 cumulative patch from the following location: Download Software location. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.2 patch can also be installed on ACS 5.8.1.4.

Table 8 Resolved Issues in Cumulative Patch ACS 5.8.0.32.2

Bug ID	Description
CSCur92646	SSLv3/TLS Renegotiation Stream Injection issue in ACS 5.7.
CSCut77567	NTPD vulnerabilities in April 2015.
CSCut99902	ACS does not list the identity group if there is a "\" in the identity group description field.
CSCuu66563	Search option in ACS 5.7 and later version displays additional fields after canceling the search results.
CSCuu75750	Updating end station filters using a .csv file fails in ACS.
CSCuu82493	OpenSSL Vulnerabilities were found in ACS during June 2015.
CSCuv10632	ACS displays an error message intermittently when you enable an interface for ACS configuration web.
CSCuv10688	ACS primary node shows the status of the secondary node as "Node not responding" though the secondary node is connected.
CSCuv58437	Saved Reports in ACS does not work if you edit the name of the saved reports.
CSCuv88038	ACS 5.7 has compatibility issues with Mozilla Firefox 39.0 browser.
CSCuv95363	Scheduled reports in ACS 5.x are not working after reloading the ACS server.
CSCuv99693	ACS 5.6 does not allow special characters in command sets.
CSCuw09481	ACS 5.x is vulnerable to CVE2015-5600.
CSCuw21552	ACS 5.x displays incorrect results for all filters that you use on configuration Audit Scheduled Report.
CSCuw24655	Protection vulnerability impacting 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.
CSCuw33071	Scheduled backups in ACS 5.7 fails when you use RSA crypto keys to authenticate against SFTP repository.
CSCuw55386	Management process fails to start after restoring a full ACS View backup in ACS 5.7 web interface.
CSCuw70238	Unable to save scheduled reports in ACS 5.x with clock time zone set as ETC/GMT+/-7.
CSCuw81477	ACS has to allow the read-only user to execute the show users status command.
CSCuw81495	The password types drop-down list does not display the available options when you apply filters for user objects and try to change your password from ACS 5.7 web interface. This issue is specific to Mozilla Firefox browser versions 39 or later.
CSCuw84970	Evaluating ACS 5.x for NTP in October 2015.
CSCuw89652	Unable to edit the acsadmin account details when there is a "+" symbol in the clocks timezone.
CSCuw89910	ACS fails to join the Active Directory domain when the password includes "<" or ">" characters.
CSCux04983	Administrator Entitlement report in ACS fails to run properly when the administrator is an operational or provisional administrator.
CSCux07030	ACS displays the following error while authenticating an user after upgrading ACS from 5.4 to 5.5 version: 15020 Could not find selected Shell Profiles
CSCux33250	The User Changeable Password (UCP) fails to work after enabling the Enable Password Hash option in ACS 5.7.
CSCux33426	ACS 5.7 fails to import a CSV file that has an ampersand symbol in the Network Device Group filters.

Table 8 Resolved Issues in Cumulative Patch ACS 5.8.0.32.2 (continued)

Bug ID	Description
CSCux34781	Apache Common Collections Java library vulnerability was found in ACS during December 2015.
CSCux39905	Evaluating CVE-2015-6564 in ACS.
CSCux43519	Authentication lookup portlet feature in ACS 5.7 displays an internal error.
CSCux44063	Secure Syslog feature is not working properly when you restart the log collector server in ACS 5.7.
CSCux81584	Backup for a file size more than 2 GB fails in ACS 5.6 patch 4 while using an FTP repository.
CSCux95189	Evaluating ACS 5.x for NTP in January 2016.
CSCuy05184	User Accounts in ACS are disabled when you configure the disable user account after n days of inactivity option though there are passed authentications within the configured number of days.
CSCuy09734	Unable to edit Password Hash enabled users using password complexity feature.
CSCuy09740	ACS View reports does not display the latest records when the report has more than 25K records.
CSCuy11959	ACS 5.x reports subnets overlapping error while creating network devices using IPv6 with TACACS protocol.
CSCuy12884	Unable to retrieve AD group information after successful authentication when the Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory option is enabled, in ACS 5.8.
CSCuy13890	Log Recovery is stuck when a syslog message attribute length is greater than 1024.
CSCuy23108	User is not disabled after multiple failure authentication attempts when the password type is selected as AD.
CSCuy23574	In Radius RFC, packets are dropped when zeros are appended at the end and the packet length shows 63 bytes.
CSCuy36585	Evaluating ACS for glibc during February 2016.
CSCuy89193	AD Client fails to start after restoring ACS 5.6 backup on ACS 5.8

Resolved Issues in Cumulative Patch ACS 5.8.0.32.3

Table 9 on page 28 lists the issues that are resolved in the ACS 5.8.0.32.3 cumulative patch. You can download the ACS 5.8.0.32.3 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.3 patch can also be installed on ACS 5.8.1.4.

Table 9 Resolved Issues in Cumulative Patch ACS 5.8.0.32.3

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

Resolved Issues in Cumulative Patch ACS 5.8.0.32.4

Table 10 on page 28 lists the issues that are resolved in the ACS 5.8.0.32.4 cumulative patch. You can download the ACS 5.8.0.32.4 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.4 patch can also be installed on ACS 5.8.1.4.

Table 10 Resolved Issues in Cumulative Patch ACS 5.8.0.32.4

Bug ID	Description
CSCuu29920	ACS 5.x requires TLS 1.2 support for LDAP authentication.
CSCux98281	DBPurge fails when the Log Recovery feature is enabled.
CSCuy44452	Issues with Change password on next login in ACS 5.7 and ACS 5.8 if password hash is enabled for internal users.

Table 10 Resolved Issues in Cumulative Patch ACS 5.8.0.32.4

Bug ID	Description
CSCuy45998	ACS 5.7 does not allow unlocking of user account when the user reaches the password retries threshold due to incorrect password entered in the CLI.
CSCuy50131	ACS 5.8 supports weak ciphers for legacy clients.
CSCuy54597	Evaluating ACS 5.x for OpenSSL in March 2016.
CSCuy59628	Unable to edit Network Device entries with a IP Range.
CSCuy63004	Catalina.log file reaches 100-200GB in size.
CSCuy63906	ACS creates the database crash dumps in /home/ directory instead of database home directory.
CSCuy73706	Log files are not updated for a long time due to the following error: "failed to allocate a SYSV semaphore" while getting connection from the database.
CSCuy81798	Updating TACACS shared secret details using import/export operation throws validation error when the key exceeds 32 characters.
CSCuy92415	Runtime is not monitored when you upgrade from ACS 5.5/5.6/5.7 to ACS 5.8 without log collector or restore a backup taken without log collector.
CSCuz03320	In ACS 5.8, loginFailureCount is not reset to 0 automatically for REST call.
CSCuz27273	ACS provides support for Policy Export file download to client computer.
CSCuz40534	In ACS 5.8 patch 2, report shows a blank page for a dynamic admin user.
CSCuz45645	ACS throws the following error: "ProvisioningAdmin and OperationsAdmin Role should not combined with any of other roles. Please remove roles accordingly" while creating or editing the authorization rules on ACS by adding another external AD group.
CSCuz50074	Core files are not generated in PBIS when the AD Connector crashes.
CSCuz75323	ACS 5.8 supports Elliptic curve cryptography (ECC) ciphers only for client certificates.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.5

Table 11 on page 29 lists the issues that are resolved in the ACS 5.8.0.32.5 cumulative patch. You can download the ACS 5.8.0.32.5 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.5 patch can also be installed on ACS 5.8.1.4.

Table 11 Resolved Issues in Cumulative Patch ACS 5.8.0.32.5

Bug ID	Description
CSCux16057	The NTP server status reverts back to local in ACS 5.6 and 5.7.
CSCux97425	Test configuration check returns error after setting up ACS 5.7/5.8 with LDAP servers.
CSCuy78327	DB purge on Feb 29 is deleting all the logs.
CSCuy88722	ACS displays the following error "AD Connector is not available" while joining ACS to AD.
CSCuy92367	ACS is vulnerable to CVE-2016-1907
CSCuz11125	Logging recovery process creates duplicate records in log collector.
CSCuz11163	Logging Recovery time interval needs to be fine-tuned.
CSCuz12297	Promotion fails while configuring RSA SecurID Token Servers.
CSCuz24101	Management process does not run properly after reloading ACS.
CSCuz28260	ACS Admin Access by Radius identity Server sends incorrect NAS IP address.

Table 11 Resolved Issues in Cumulative Patch ACS 5.8.0.32.5

Bug ID	Description
CSCuz41442	ACS 5.7/5.8 PAC provisioning fails with Credential Time TLV.
CSCuz43689	Restoring ACS View database from GUI fails with sudo errors.
CSCuz49536	After restoring the log collector backup, logging recovery does not work properly.
CSCuz49544	Few logs are missing during the logging recovery process.
CSCuz50048	Browser hangs while configuring CommandSet Arguments with double quotes.
CSCuz52505	OpenSSL Vulnerabilities were found in ACS during May 2016.
CSCuz69016	If the sequence number of the AD operations is more than 2147483647, an alarm is generated citing Database Failure with the ACS node name and ADOperations as the task.
CSCuz73164	Password hashing fails if TACACS enable password setting is disabled.
CSCuz86412	Unable to update Password Hash enabled users through RESTAPI
CSCuz98731	In ACS 5.7 patch 2 or 3, CLI Admin Unlock done via ISO boot remains ineffective.
CSCva00401	ACSAdmin accounts in AD are not able to view reports.
CSCva23984	ACS should not be accessible using unsupported browser.
CSCva42072	RuntimeDebugLog.config flag is not working in ACS 5.8.
CSCva42079	Runtime process is restarted when the context counter reaches 10,000.
CSCva43184	Domain becomes unusable when the following error message: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN is encountered.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.6

Table 12 on page 30 lists the issues that are resolved in the ACS 5.8.0.32.6 cumulative patch. You can download the ACS 5.8.0.32.6 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.6 patch can also be installed on ACS 5.8.1.4.

Table 12 Resolved Issues in Cumulative Patch ACS 5.8.0.32.6

Bug ID	Description
CSCuv42787	In ACS 5.6 and 5.7, the Device IP field is not displayed in the TACACS Authentication Report.
CSCux76335	Unable to restore ACS 5.5 backup on ACS 5.7/5.8 when VSA attribute changes are done.
CSCva05815	In ACS 5.7 and 5.8, static routes cause problem for the local subnet route.
CSCva43590	On restarting the ACS services, ACS View database does not start after upgrading from ACS 5.7 to ACS 5.8.
CSCva50918	ACS Monitoring and Report Viewer keeps sending alarms of High CPU every 2 minutes.
CSCva56902	In ACS 5.8, Authentication fails due to same user and computer name in AD.
CSCva79933	ACS stops processing RSA Authentication and displays the following error: "ACM_NO_SERVER".
CSCva81649	ACS needs to update “tzdata” for December 2016 leap second.
CSCvb05250	Backup Interface feature does not work in ACS 5.8.
CSCvb13970	ACS View DBPurge and incremental backups fail after upgrading to ACS 5.8.1.
CSCvb15365	Automatic AD DC failover on RPC failure receipt.
CSCvb15366	AD agent is not reconnected to DC upon receiving TCP reset request.
CSCvb15368	ACS fetches wrong information from AD query.
CSCvb15369	Enhance Concurrent Handling for DC Availability Updates.

Table 12 Resolved Issues in Cumulative Patch ACS 5.8.0.32.6

Bug ID	Description
CSCvb22800	Unable to export ACS reports with special characters in the ACS GUI account after upgrading to ACS 5.8.
CSCvb28841	Optimize User Validation based on authentication results.
CSCvb38112	ValidateUser mechanism is replaced from RPC to LDAP.
CSCvb91226	Authorization rule hits incorrectly due to duplicate AD group SID's in the ActiveDirectory group configuration.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.7

Table 13 on page 31 lists the issues that are resolved in the ACS 5.8.0.32.7 cumulative patch. You can download the ACS 5.8.0.32.7 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.7 patch can also be installed on ACS 5.8.1.4.

Table 13 Resolved Issues in Cumulative Patch ACS 5.8.0.32.7

Bug ID	Description
CSCuz11206	TACACS+ authorization fails if authentication is done against different ACS machines with the condition that the password type is RSA.
CSCuz39617	ACS sends self-signed certificate for management access if ACS cluster is upgraded from 5.x to 5.8.1
CSCva24770	SNMP daemon is not responding if snmpwalk gets MIB objects recursively without specifying the hierarchical level of OID.
CSCva88672	Evaluating ACS 5.x for TCP in August 2016.
CSCvb26372	Launch Monitoring and Report Viewer launches a new tab with the IP address of the secondary server as the URL not the hostname.
CSCvb34188	Registration to a deployment fails in ACS 5.8 patch 4 or later for specific certificate.
CSCvb48662	Evaluating ACS 5.x for OpenSSL in September 2016.
CSCvb52091	ACS services restart is required to switch to the next available DC during a DC fail over.
CSCvb62332	ACS 5.x is vulnerable to CVE-2016-6313.
CSCvb71656	Unable to locate AAA client if there is an overlap in IP Subnets.
CSCvb72704	ACS displays an incorrect URL for the "Top N Authentications By Network Device" report.
CSCvb82842	Unable to add AD user for ACS login if "Password must not contain <password> or its characters in reverse order" is set under password complexity setting.
CSCvb85658	ACS 5.x is vulnerable to CVE-2016-5195.
CSCvb91043	Recent logs are not displayed in the reports.
CSCvb98750	In ACS 5.8 patch 4 or later, LDAP server uses only TLSv1.0 for "Test Bind To Server" and "Test Configuration" options.
CSCvc04553	Scheduled policy export fails if the repository name has the word "backup".
CSCvc04593	Configurable option for accounting interim update messages under the logging categories.
CSCvc04838	XSS vulnerability is found in ACS.
CSCvc04845	XXE vulnerability is found in ACS.
CSCvc04849	Open Redirect vulnerability in found in ACS.
CSCvc04854	Information Disclosure Vulnerability is found in ACS.

Table 13 Resolved Issues in Cumulative Patch ACS 5.8.0.32.7

Bug ID	Description
CSCvc05781	Unable to do initial setup for admin after performing "write erase" on ACS 5.8/5.8.1 patch 2 or later patch bundle.
CSCvc06777	Unable to edit the IP ranges while modifying a network device.
CSCvc15446	EAP-FAST authentication is not working for weak ciphers from ACS 5.8 patch 4.
CSCvc22979	Internal users cache mechanism for TACACS+ authZ flow.
CSCvc40694	A proper message should be displayed to the user instead of a generic INTERNAL ERROR when a NULL error is encountered in ACS for the REST request.
CSCvc40734	ACS5 REST API | SDK should implement TLSv1.2 by default.
CSCvc60673	AD joining process takes more time in ACS 5.8 patch 6.
CSCvc68590	In ACS 5.6 or later, export option is not available in some report pages.
CSCvc78589	After applying ACS 5.8 patch 3 or later, executing "show tech" command does not show UDI and inventory information for Cisco SNS 3515 and 3595 appliances
CSCvd22451	Unable to launch the ACS GUI in Mozilla Firefox 52 browser.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.8

Table 14 on page 32 lists the issues that are resolved in the ACS 5.8.0.32.8 cumulative patch. You can download the ACS 5.8.0.32.8 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.8 patch can also be installed on ACS 5.8.1.4.

Table 14 Resolved Issues in Cumulative Patch ACS 5.8.0.32.8

Bug ID	Description
CSCuv56583	Proper error message must be displayed in the GUI while creating an admin user with password hash enabled when the runtime is not up.
CSCuw14444	Incorrect range for password is shown in the Internal User page.
CSCvb47838	Runtime service is not monitored after adding the user dictionary attribute.
CSCvb67339	Internal error is displayed while viewing Top N Failed Authentications By Failure Reason report.
CSCvc63681	UCP python script fails after installing patch 4 on ACS 5.8.
CSCvc70687	If the year is changed, the previous logs are purged in ACS 5.8.1.
CSCvc82625	ACS displays Server Error for specific links in the Reports page.
CSCvc94988	Unable to use a dictionary condition defined from the Internal Users page for expiration date value in the authorization policy after upgrading to ACS 5.8.
CSCvd01030	Core file is generated when EAP-FAST authentication is performed using AnyConnect.
CSCvd04752	Unable to access ACS GUI over IPv6 address after installing 5.8 patch 4 or later.
CSCvd27745	ACS 5.7 and 5.8 are vulnerable to CVE-2016-8858.
CSCvd30991	SuperAdmin users authenticated via LDAP are unable to change the passwords for other SuperAdmin users.
CSCvd34752	ACS uses the default certificate if the new server certificate name is same as default certificate.
CSCvd42702	Authorization fails with the following error "Configured operand failed to match the value type" while configuring the compound conditions in Hierarchical attribute versus String attribute.
CSCvd50631	UCP web application fails when TLS 1.0 for HTTPS Access option is disabled in the security settings page.
CSCvd65807	ACS 5.8 displays “No Data Available” in the detailed reports after merging the ViewDB from support bundle.
CSCvd70407	Runtime crashes due to incorrect LDAP directory attribute configured in ACS 5.8.

Table 14 Resolved Issues in Cumulative Patch ACS 5.8.0.32.8

Bug ID	Description
CSCvd77636	Support download of ACSView reports to local desktop.
CSCvd91391	Missing columns in the "Top N Authentications By Network Device" report in ACS 5.8.
CSCvd98956	Proper validation must be provided in End station filter > Mac address page to support the wildcard character "?".
CSCve62941	Incorrect warning message is displayed in ACSView reports.
CSCve70587	Stored Cross-site scripting (XSS) in Cisco ACS 5.8.1.4.
CSCve76165	After installing patch 7, ACS 5.8 sends incorrect NAS IP address while communicating with external RADIUS Identity Server.
CSCvf01320	ACS Management service restarts if the reports run with some filters.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.9

Table 15 on page 33 lists the issues that are resolved in the ACS 5.8.0.32.9 cumulative patch. You can download the ACS 5.8.0.32.9 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Note: The ACS 5.8.0.32.9 patch can also be installed on ACS 5.8.1.4.

Table 15 Resolved Issues in Cumulative Patch ACS 5.8.0.32.9

Bug ID	Description
CSCve70595	Cisco Access Control Server XML eXternal Entity (XXE) Injection Vulnerability - CstAction Component
CSCve70616	Cisco Access Control Server XML eXternal Entity (XXE) Injection Vulnerability - amfsecure component
CSCvf05455	ACS 5.8 patch 7 - All internal users are disabled after 45 days.
CSCvf14383	ACS MAR cache issue with upper and lower case MAC addresses string comparison.
CSCvf22363	ACS 5 impact to Apache TomCat vulnerabilities.
CSCvf25975	CRL check fails when two root CA certs from the same CA exist.
CSCvf38012	IPv6 addresses with masks other than /128 cannot be used when adding NAS.
CSCvf47906	LDAP "test configuration" function uses only TLS 1.0.
CSCvf62930	Option to be added for AD Identity Resolution only against Joined Domain in ACS 5.8 (as in ACS 5.4). This fix ensures that SAM account names are always searched in the joined domain (as in ACS 5.4). A new option, “Search only in joined domain,” is introduced in the GUI, which, if enabled, restricts the search only to the joined domain. Account name with the domain markup is searched in the respective domain.
CSCvf66155	Cisco Secure Access Control System Information Disclosure Vulnerability
CSCvf76783	ACS modifies the client NAS IP while RADIUS server is configured as an identity server.
CSCvf82233	CA authentication issue is seen when CRL is enabled on two CA certificates with the same name.

Table 15 Resolved Issues in Cumulative Patch ACS 5.8.0.32.9

Bug ID	Description
CSCvf90786	ACS fails to resolve ambiguity for AD accounts. A new advanced tuning (registry) configuration for “IdentityLookupField” is introduced with the following three options: ■ Search by SAM (Default) ■ Search by CN ■ Search by CN and SAM For authorization failures that occur because of conflicting SAM or CN accounts, you can choose either the SAM or the CN search. If further conflicts arise because of trusted domains, you can use the "no domain markup” configuration to further filter unwanted accounts. See the *User Guide for Cisco Secure Access Control System 5.8* for information on advanced tuning configuration.
CSCvg21341	ACS handling the check of TACACS+ packet's IPv6 source address against network devices incorrectly.
CSCvg29874	CVE-2017-1000364 kernel: heap/stack gap jumping via unbounded stack allocations.
CSCvg45489	Unable to log out of ACS GUI when logged in using IPv6 address.
CSCvg46693	ACS 5.8 : EAP-FAST authentication fails if Vocera supplicant provides expired/invalid PAC.
CSCvg69718	ACS patch-8 has not been installed completely at times.
CSCvg70018	ACS: Evaluate CVE-2017-1000253.

Resolved Issues in Cumulative Patch ACS 5.8.0.32.10

Table 16 on page 34 lists the issues that are resolved in the ACS 5.8.0.32.10 cumulative patch. You can download the ACS 5.8.0.32.10 cumulative patch from the following location: Download Software. Refer to Applying Cumulative Patches, page 21 section for instructions on how to apply the patch to your system.

Table 16 Resolved Issues in Cumulative Patch ACS 5.8.0.32.10

Bug ID	Description
CSCvg47940	ACS disconnected from AD when ACS cannot refresh its machine account.
CSCvh81084	Make Disable Inactive User Accounts feature as case-insensitive.
CSCvh27607	ACS performs DNS SRV queries for domains disabled in "Authentication Domains" AD configuration.
CSCvi68462	ACS 5.8: Both bonded interfaces are not reachable after shut and no shut.
CSCvi85318	Cisco Secure Access Control Server XML External Entity Injection Vulnerability
CSCvj09832	SNMP OID for SN retrieves empty string for ACS 5.8.1 on SNS 3515/3595.
CSCvk69731	ACS 5.8: Evaluation against CVE-2018-5390

Known Issues in ACS 5.8

Table 17 on page 36 lists the known issues in ACS 5.8. You can also use the Bug Toolkit on Cisco.com to find any open bugs that do not appear here.

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

You can use the following bug search tool query to view all ACS 5.8 open caveats:

5.8 open bug search

Table 17 Known Issues in ACS 5.8

Bug ID	Description
CSCuv56583 ACS displays an incorrect error message for administrator password hashing errors.	ACS displays the “System Failure: Generation of password hash timeout, your changes have not been saved.” error message when you enable password hashing for an administrator account while ACS runtime process are not running. This problem occurs when you try to create an administrator account and enable password hashing option for that administrator in ACS web interface. Workaround: None. This issue does not create an impact in the functionality of the ACS web interface.
CSCuw05787 ACS displays incorrect data for a specific time range authentication trend reports.	In ACS, choose Monitoring and Reports > Reports > ACS Reports > AAA Protocol > Authentication Trend and generate report with specific time ranges. ACS retrieves the Authentication Trend Report for the selected time range (for example Last 7 days). ACS must display the appropriate data when you click on a particular days report. But, ACS does not display the time range specific data properly except for the time range option Today. This problem occurs when you try to generate authentication trend report for specific time ranges. Workaround: You can generate appropriate AAA protocol reports with required time range.
CSCuv02840 Unable to add local certificates in ACS after upgrading to ACS 5.8.	Unable to add local certificates in ACS after upgrading it from 5.5, 5.6, or 5.7 versions to 5.8 version and ACS does not display any error message for this issue. This problem occurs when you upgrade from ACS 5.5, 5.6, or 5.7 to ACS 5.8 having management certificate expired. Workaround: Execute **acs-reset-config** command from ACS CLI. (Or) You must set the ACS clock time to previous day’s date and time. After changing ACS clock time, you can add new certificates.
CSCuw06091 ACS view database fails to start after changing the IP address of a name server from ACS CLI.	View related processes in ACS fail to run after upgrading from ACS 5.7 patch 1 to ACS 5.8. This process occurs when you upgrade from ACS 5.7 patch 1 to ACS 5.8 and change the IP address of the name server from ACS CLI. Workaround: Execute the **acsview replace-clean-db** command from ACS CLI to replace the current database with a clean new database.
CSCuw14444 ACS displays an incorrect password range for creating internal users web interface.	ACS displays the password range as 4-32 in creating internal users web interface. This password range is incorrect as ACS supports up to 128 characters for internal user password. This problem occurs when you enter more than 32 characters for internal user password. ACS does not display an error messages as it supports up to 128 characters. Workaround: None. The supported range is 4 to 128.

Table 17 Known Issues in ACS 5.8 (continued)

Bug ID	Description
CSCuv58437 ACS does not allow you to edit the saved reports name.	Saved Reports in ACS does not work if you edit the name of the saved reports. This problem occurs when you edit the name of a saved reports in ACS Reports web interface. Workaround: Delete and add the report again.
CSCuv75650 ACS displays an incorrect error message for a logon restricted user when you use Kerberos protocol for PAP authentication	Kerberos authentication for logon restricted user does not display proper report logs. ACS must display the “24410 User authentication against Active Directory failed since user is considered to be in restricted logon hours.” error message. But, ACS displays the “24370 User credentials have been revoked” error message. This error message is reported, when the Kerberos PAP authentication is executed and the authentication fails with restricted hour permission. Workaround: You do not have an impact in the application functionality. ACS does not display the proper error messages when you use Kerberos protocol for PAP authentication. ACS displays the proper error message if you use MS-RPC protocol.
CSCvd01030 ACS generates core file on EAP-FAST authentication with AnyConnect	Core File is generated on EAP-FAST authentication with AnyConnect. This problem occurs when EAP-FAST Mschap authentication is performed using AnyConnect. Workaround: Disable the Allow TLS-Renegotiation option if the Accept Client Certificate option is enabled in the ACS GUI.
CSCvd34752 ACS uses the default certificate if the new server certificate name is same as the default certificate	ACS uses the default self-signed certificate if the new server certificate name is same as the default certificate. This problem occurs when the new server certificate name is same as the default certificate. Workaround: Submit the server certificate that is already mapped to management protocol.
CSCvf95674 Unable to do any action in ACS view reports when you click the details reports of RADIUS/TACACS authentication in Firefox (55.0.2).	Unable to do any action in ACS view reports when you click the details reports of RADIUS/TACACS authentication in Firefox (55.0.2). This issue is seen when you enable automatic updates in Firefox settings. Once the latest version of Firefox is updated automatically (or installed manually) in 32-bit versions of Firefox on 64-bit operating systems. Workaround: 1. Type about:config in the url of the browser and press **Enter**. The config page appears. 2. Search for the attribute “dom.ipc.plugins.asyncdrawing.enabled”. 3. By default, the value of the attribute is set to "True." Change it to "False" and close the page to save the change. We recommend that you install 64-bit Firefox versions on 64-bit operating systems, and 32-bit Firefox versions on 32-bit operating systems.
CSCvh88875 OLH is not updated for the new AD Identity Resolution added in 5.8p9.	OLH is not updated for the new AD Identity Resolution added in 5.8p9. See the *User Guide for Cisco Secure Access Control System 5.8* for the documentation updates.

Documentation Updates

Table 18 on page 38 lists the updates to *Release Notes for Cisco Secure Access Control System 5.8*.

Table 18 Updates to Release Notes for Cisco Secure Access Control System 5.8

Date	Description
02/27/2018	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.9, page 33
07/21/2017	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.8, page 32
03/03/2017	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.7, page 31
11/18/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.6, page 30
8/25/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.5, page 29.
6/7/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.4, page 28.
5/20/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.3, page 28.
4/08/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.2, page 26.
1/04/2016	Added Resolved Issues in Cumulative Patch ACS 5.8.0.32.1, page 26.
9/29/2015	Cisco Secure Access Control System, Release 5.8.

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 19 on page 39 lists the product documentation that is available for ACS 5.8. 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 19 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	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	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	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	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	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	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:

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 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 re installation 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 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.