Release Notes for Cisco Secure Access Control System 5.4

Revised: January 27, 2016 OL-26234-01

These release notes pertain to the Cisco Secure Access Control System (ACS), release 5.4, hereafter referred to as ACS 5.4. These release notes provide information on the features, related documentation, resolved issues, and known issues for functionality in this release.

This document contains:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Note ACS 5.4 was originally posted as version 5.4.0.46. There were issues found while performing the final verification with the new UCS based appliance. As a result, new versions 5.4.0.46.0 and 5.4.0.46.0a were released. Note that all these versions are functionally equivalent versions. If you have installed the versions 5.4.0.46 or 5.4.0.46.0, then you do not need to switch to 5.4.0.46.0a unless you are installing ACS in the new UCS based appliance. It is possible to switch between these versions by performing a backup from one version and then a restore of the backup after the alternate version has been installed.

Introduction

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

The ACS 5.4 software runs on a dedicated Cisco 1121 Secure Access Control System (CSACS-1121) appliance, on a Cisco 3415 Secure Access Control System (CSACS-3415), or on a VMware server. However, ACS 5.4 continues to support the CSACS-1120 appliances that you have used for previous releases of ACS, which you can upgrade to ACS 5.4.

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

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

New and Changed Features

The following sections briefly describe the new and changed features in the 5.4 release:

Enhanced Access Protocol Support

The Access Protocol feature enhancement includes:

- Session resumption support for stateless EAP-TLS session

ACS 5.4 supports EAP-TLS session resumption without session state to be stored at the server. It also supports session ticket extension as described in RFC 5077. The ACS Server creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ACS to resume a session.

The stateless session resumption is supported in the distributed deployment, so that a session ticket issued by one node is accepted by another node. For more information, see the EAP-TLS Flow in ACS 5.4 section in *User Guide for Cisco Secure Access Control System 5.4*.

- PEAP cryptobinding

  ACS 5.4 supports cryptobinding TLV extension in MS PEAP. Cryptobinding TLV extension in MS PEAP authentication is used to ensure that both the EAP peer (client) and the EAP server (ACS) are participating the inner and outer EAP authentications of the PEAP authentication. For more information, see *User Guide for Cisco Secure Access Control System 5.4.*

- Name constraint extension support in issuer certificates

  ACS 5.4 now supports certificate name constraint extension. It accepts client certificates whose issuers contain the name constraint extension. The following name constraint field attributes are supported by ACS 5.4:

  - Directory Name
  - URL
  - Email
  - Domain Name Server (DNS)

  The IP address is not a supported name constraint extension field attribute.

- OCSP services

  ACS 5.4 introduces a new protocol, Online Certificate Status Protocol (OCSP), which is used to check the status of x.509 digital certificates. This protocol can be used as an alternate to the Certificate Revocation List (CRL). It can also address the issues that result in handling CRLs. For more information, see the Working with OCSP Services section in *User Guide for Cisco Secure Access Control System 5.4*.

- RADIUS proxy request attributes rewrite support

  In ACS 5.4, you have an option to define additional RADIUS attributes or update the existing ones. The updated attributes are rewritten on the RADIUS request before it is sent to the RADIUS proxy server. This attribute manipulation is configured as part of the Proxy Access Services definition. The RADIUS attributes rewrite feature is enabled only for RADIUS access requests and is not enabled for accounting requests. For more information, see *User Guide for Cisco Secure Access Control System 5.4.*

- Certificate issuer support

  ACS 5.4 supports a new field called Issuer field in client certificates to be used in the policy conditions. This Issuer certificate can be used in the Authentication, Group Mapping, and Authorization policy rules along with the ‘equals', 'contains' or 'starts/ends with' operators. The whole field value is taken to verify the DN and no further parsing is performed to extract the attributes like issuer CN and O.

Identity Store Enhancement

Active Directory ID Store

The Active Directory (AD) ID Store enhancements include:

- AD domain enhancements

  ACS 5.4 provides the support to perform the AD configuration, join, and leave operations separately. In ACS 5.4, the join or leave operations are not performed automatically. The administrator must perform the join or leave operations manually for each server in the deployment. You can perform the join or leave operations for multiple nodes. Also, in ACS 5.4, you can join the ACS nodes from same deployment to different AD domains. However, each node can be joined to a single AD domain.

- Distributed MAR cache

  ACS 5.4 supports Machine Access Restrictions Cache per ACS deployment. That is, machine authentication results can be cached among the nodes within the deployment, and you can select the MAR cache operational node. For more information, see the Distributed MAR Cache section in *User Guide for Cisco Secure Access Control System 5.4*.

- LDAP ID store

  ACS 5.4 supports password change operation for users authenticated against the LDAP ID store in TACACS+ ASCII/PAP and EAP-GTC flows. Users can trigger the password change operation. Check the Enable Password Change option in the LDAP edit page to modify the password, detect the password expiration, and reset the password. ACS 5.4 also supports definitions of LDAP groups and references from policies to LDAP groups using LDAP group attributes other than DNS.

- Disable internal users based on date

  ACS 5.4 supports an account disablement policy for each individual user. This option allows you to disable user accounts when the configured date is exceeded. This option overrides the global account disablement policy of the users. This means that the administrator can configure different expiration dates for different users, as required. The default value for this option is 60 days from the account creation date.

System Administration Enhancements

The System Administration enhancement includes:

- Administrative Access Control

  ACS 5.4 introduces a new service type called the Administrative Access Control (AAC) service. The AAC service processes the authentication and authorization of the ACS administrators. The AAC service also processes the configuration of roles and permissions for ACS management and different administration operations. Only AD and LDAP are supported as the external databases for AAC. The RSA database is not supported. For more information, see *User Guide for Cisco Secure Access Control System 5.4.*

  The enhanced AAC web interface includes:

  - Policy-based authentication and authorization.

  ACS 5.4 includes authentication against an external database, feasible by password type on administrator accounts in the administrators internal ID store and the ability to map between external groups and admin roles.

- Read-only (R/O) CLI administrators

  ACS 5.4 introduces a new user role called R/O Admin. This user can run the **show** commands in the CLI but cannot modify the ACS configurations. Also, users who are not administrators are able to execute the **show app status acs**, and **show timezones** commands to monitor the health of the active ACS processes.

Note Administrator accounts created in external identity stores cannot access CARS mode of ACS CLI. But, they can access acs-config mode of ACS CLI.

- Programmatic interface enhancements

  ACS 5.4 supports these new object types: Network Device, Network Device Groups, and Internal Hosts. These operations are done using the Representational State Transfer (REST) programmatic interface. For more information, see *Software Developer's Guide for Cisco Secure Access Control System 5.4.*

System Operations Enhancements

The system operations enhancement in ACS 5.4 include:

- Multiple network interface connector support

  ACS 5.4 supports up to four network interfaces: Ethernet 0, Ethernet 1, Ethernet 2, and Ethernet 3. ACS management functions use only the Ethernet 0 interface, but AAA protocols use all configured network interfaces. You must connect the ACS nodes in the distributed deployment only to the Ethernet 0 interface. Therefore, the syslog messages are sent and received at the log collector's Ethernet 0 interface. Data forwarding from one interface to another interface is prohibited to prevent potential security issues. The external identity stores are supported only on the Ethernet 0 interface. In ACS 5.4, multiple network interface connectors are also supported for proxies.

- New and enhanced CLI commands

ACS 5.4 introduces the following CLI commands to support IPv6 addresses.

- **ping**—This command is used to diagnose the connectivity to a remote system, In ACS 5.4, this command is enhanced to support IPv6 addresses. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*
- **traceroute**—This command is used to trace the route that the packets are traveling to reach their destination. In ACS 5.4, this command is enhanced to support IPv6 addresses. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*
- **show ipv6 route**—This command is used to display the available IPv6 routes on the server. This command is introduced in ACS 5.4. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*
- **ipv6 route**—This command is used to configure static IPv6 routes. This command is introduced in ACS 5.4. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*
- **ipv6 address**—This command is used to set the IPv6 address and prefix length for the Ethernet interface. This command is introduced in ACS 5.4. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*

ACS 5.4 introduces the following CLI commands to troubleshoot AD connectivity issues.

- **adinfo**—This command is used to retrieve the AD join settings and status. This command can also be used to retrieve detailed information regarding the domain, users, and domain controllers. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*

  - **adcheck**—This command is used to check AD configuration and check for compatibility with the AD agent. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*
  - **ldapsearch**—This command is used to perform an LDAP search in AD. For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.4.*

- Data purging enhancements

  In ACS 5.4, the size of the view database is allocated based on the /opt partition size. That is, 42 percent of the /opt partition size is the view database size. In ACS 5.3, the lower limit, upper limit, and maximum limit are hard coded. But, in ACS 5.4, these are not hard coded.

  Limits in ACS 5.4 are:

  - Lower limit—60 percent of the allocated view database size
  - Upper limit—80 percent of the allocated view database size
  - Maximum limit—100 percent of the allocated view database size

  For more information, see *User Guide for Cisco Secure Access Control System 5.4.*

- Database compress enhancements

  In ACS 5.4, the database compress operation is automated. You need to check the **Enable ACS View Database Compress** check box to compress the ACS View database automatically every day at 5 A.M. whenever there is a need. For more information, see *User Guide for Cisco Secure Access Control System 5.4.*

- VMware enhancements

  ACS 5.4 supports VMware disk space from 60 GB to 750 GB. ACS 5.4 also supports VMware tools. The ACS 5.4 image includes the VMware tools, which are installed automatically when you install ACS 5.4. The ACS 5.4 image includes the CARS kernel (Linux stock kernel) optimized for operation on the VMware ESX. The ACS 5.4 CARS kernel includes a new kernel option that allows you to adjust the system clock rate. Using this option, you can reduce the clock rate from the default of 1000 HZ to 100 HZ which is desirable in a virtual machine. By default, this option is switched on in CARS. For more information, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*

- Login banner

  In ACS 5.4, you can see two different login banners. One banner is displayed before logging in and another is displayed after logging in to the web interface and CLI. You can also edit the default text of the banners in the ACS 5.4 web interface.

- Network Time Protocol (NTP)

  ACS 5.4 supports authenticated NTP mode and the existing nonauthenticated NTP mode.

Enhanced Monitoring and Troubleshooting Reports

The Monitoring and Troubleshooting Report viewer enhancement includes:

- Network Time Protocol Daemon (NTPD) Process Monitoring

  ACS 5.4 monitors the NTPD process. When the NTPD process goes down, it restarts automatically. You can check the NTPD process status in two ways:

  - Issue the **sh app status acs** command in the CLI interface.

  - Choose **Monitoring and Reports > Reports > Catalog > ACS Instance > ACS_Health_Summary** in the ACS web interface.

- Scheduled export of logs

  In ACS 5.4, you can schedule export of logs to a remote database job based on days/hours/minutes.

- Report generation enhancements

  In ACS 5.4, you can filter the data and generate reports based on timestamps. The Start time and End time options are provided to extract the reports based on timestamps. Also, while generating reports, if there are more than 5000 records, then ACS notifies the user to use the .csv file to export the records and saves them in its local disk. Login to ACS CLI and use the **dir** command to view the exported file. You can copy the exported file to a remote repository using the **copy** command. You can track the record status in the scheduler page. For more information, see *User Guide for Cisco Secure Access Control System 5.4.*.

IPv6 Support

ACS 5.4 supports the IPv6 version of IP addresses, along with IPv4 addresses. The following features include IPv6 support:

- ACS Management Web Access—ACS 5.4 supports HTTPS access (GUI) over IPv6.
- Connectivity Tests—ACS 5.4 supports IPv6 troubleshooting tools (ping and traceroute).
- Support Bundle Downloading—ACS 5.4 supports downloading support bundles to an IPv6 destination.
- Expert Troubleshooting—ACS 5.4 supports expert troubleshooting of IPv6 network devices.
- Collection Filters—ACS 5.4 supports IPv6 addresses in collection filters based on Network Access Server (NAS) IP addresses.
- Reports—ACS 5.4 supports the display of IPv6 addresses in proper report format.
- OS Services—CARS provides several IPv6 services (such as static IPv6 address, DNS, Secure Shell [SSH], and firewall). IPv6 can be configured using the following two methods:
  - Static Global Unicast method
  - Automatic Configuration (Auto Config) method
- TACACS+ Server—ACS 5.4 supports full TACACS+ server over IPv6.
- TACACS+ Proxy—ACS 5.4 supports full TACACS+ proxy over IPv6.
- IP Address Attributes in Identity Stores and Policies—ACS 5.4 supports IP address attributes as dual-type (IPv4 and IPv6). Identity stores and policies support these dual-type IP address attributes.

Note Simple Network Management Protocol (SNMP) and Dynamic Host Configuration Protocol (DHCP) are not supported in IPv6 addresses.

Note Remote Database with cluster setup is not supported in ACS 5.4.

CSACS-3415 Appliance Hardware Support

ACS 5.4 supports a new Hardware Appliance called Cisco 3415 Secure Access Control System Hardware or CSACS-3415. Now, ACS 5.4 can be installed in the new CSACS-3415 appliance.

The CSACS-3415 appliance is designed for performance and density over a wide range of business workloads, from web serving to distributed databases. Building on the success of CSACS-3415, the enterprise-class CSACS-3415 appliance further the capabilities of the CSACS-1121 portfolio in a 1U form factor. The CSACS-3415 appliance server does this with the addition of the Intel Xenon processor E5-2600 product family, which delivers significant performance and efficiency gains. In addition, CSACS-3415 appliance offers up to 256 GB of RAM, 8 drivers, and 2 x 1 EbE lights-out management (LOM) prots that deliver outstanding levels of density and performance in a compact package. For more information on the CSACS-3415 hardware appliance see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*

Supported Virtual Environments

ACS 5.4 supports the following VMware versions.

- VMware ESXi 5.0
- VMware ESXi 5.1 is supported after ACS 5.4 patch 3

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 5.4*.

Supported Browsers

You can access the ACS 5.4 administrative user interface using the following web clients and browsers:

- MAC OS
  - Mozilla Firefox version 3.*x*
  - Mozilla Firefox version 10.*x*
- Windows 7
  - Internet Explorer version 8.*x*
  - Internet Explorer version 9.*x*
  - Mozilla Firefox version 3.*x*
  - Mozilla Firefox version 8.*x*
- Windows XP
  - Internet Explorer version 8.x
  - Mozilla Firefox version 8.x
  - Mozilla Firefox version 9.x
  - Mozilla Firefox version 10.x

  The above mentioned browsers are supported only with one of the following cipher suits:
  - –TLS_RSA_WITH_AES_256_CBC_SHA

- –TLS_RSA_WITH_AES_128_CBC_SHA
- –RSA_WITH_3DES_EDE_CBC_SHA

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

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

Installation and Upgrade Notes

This section provides information on the installation tasks and configuration process for ACS 5.4. This section contains:

Installing, Setting Up and Configuring CSACS-1121

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

To set up and configure the CSACS-1121:

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

- The CSACS-1121 Series appliance
- Power cord
- Rack-mount kit
- Cisco Information Packet
- Warranty card
- *Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.4*

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

For more details, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*.

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

For more details, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4* and pay special attention to all safety warnings.

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

For more details on installing the CSACS-1121 Series appliance, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*

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

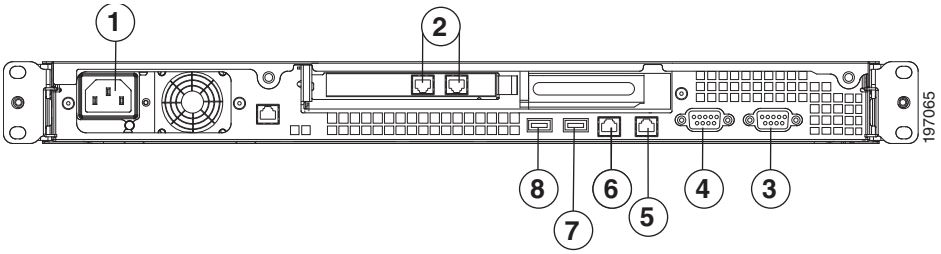
Figure 1 shows the back panel of the CSACS-1121 Series appliance and the various cable connectors.

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

For more details, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*

For information on installing ACS 5.4 on VMware, see the Installing ACS in a VMware Virtual Machine chapter in *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4.*

Figure 1 CSACS 1121 Series Appliance Rear View



The following table describes the callouts in Figure 1.

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

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

The first time you power up the appliance, you must run the setup program to configure the appliance. For more information, see Running the Setup Program, page 11.

Installing, Setting Up and Configuring CSACS-3415

The CSACS-3415 appliance does not contain a DVD drive. You must use the CIMC on the appliance or a Bootable USB to install, set up, and configure ACS 5.4 on this appliance. For more details, see *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4.*

This section describes how to install, set up and configure the CSACS-3415 appliance. The CSACS-3415 appliance is preinstalled with the software.

To set up and configure the CSACS-3415:

Step 1 Open the box containing the CSACS-3415 appliance and verify that it includes:

- The CSACS-3415 appliance
- Power cord
- KVM cable
- Cisco Information Packet
- Warranty card
- *Regulatory Compliance and Safety Information for Cisco Secure Access Control System 5.4.*

Step 2 Go through the specifications of the CSACS-3415 appliance.

For more details, see *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4*.

Step 3 Read the general precautions and safety instructions that you must follow before installing the CSACS-3415 appliance.

For more details, see *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4* and pay special attention to all safety warnings.

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

For more details on installing the CSACS-3415 appliance, see

Installation and Upgrade guide for the Cisco Secure Access Control System 5.4.

Step 5 Connect the CSACS-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 *Installation and Upgrade guide for the Cisco Secure Access Control System 5.4* views of CSACS-3415 appliance to know information about the front and back panel of the CSACS-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 *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4*.

For information on installing ACS 5.4 on VMware, see Installing ACS in a VMware Virtual Machine chapter in the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4.*

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

The first time you power up the appliance, you must run the setup program to configure the appliance. For more information, see *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.4*.

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

To configure the ACS Server:

Step 1 Power up the appliance.

The setup prompt appears:

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

Step 2 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 1.

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

Table 1 Network Configuration Prompts

Prompt	Default	Conditions	Description
Hostname	*localhost*	First letter must be an ASCII character. Length must be from 3 to 15 characters. Valid characters are alphanumeric (A-Z, a-z, 0-9), 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 host name 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 address 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 default gateway.
Domain Name	None, network specific	Cannot be an IP address. Valid characters are ASCII characters, any numbers, hyphen (-), and 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 nameserver	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	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.	Enter a valid domain name server or an IPv4 address.
Timezone	UTC	Must be a valid local time zone.	Enter a valid system timezone.

Table 1 Network Configuration Prompts (continued)

Prompt	Default	Conditions	Description
Username	*admin*	The name of the first administrative user. You can accept the default or enter a new username. Must be from 3 to 8 characters, and must be alphanumeric (A-Z, a-z, 0-9).	Enter the username.
Admin Password	None	No default password. Enter your password. The password must be at least six characters in length and have at least one lower case letter, one upper case letter, and one digit. In addition: • Save the user and password information for the account that you set up for initial configuration. • Remember and protect these credentials, because they allow complete administrative control of the ACS hardware, the CLI, and the application. • If you lose your administrative credentials, you can reset your password by using the ACS 5.4 installation CD.	Enter the password.

After you enter the parameters, the console displays:

```
localhost login: setup
Enter hostname[]: acs54-server-1
Enter IP address[]: 10.77.243.177
Enter IP default netmask[]: 255.255.255.128
Enter IP default gateway[]: 10.77.243.129
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: 10.77.242.86
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: 10.77.242.86
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
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 into ACS using only the CLI. To log into 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 application.

Licensing in ACS 5.4

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 2 lists the types of licenses that are available in ACS 5.4.

Table 2 ACS License Support

License	Description
Base License	The base license is required for all deployed software instances, as well as 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 network devices (AAA clients). The following are the types of base licenses: • Permanent—Does not have an expiration date. Supports deployments that have a maximum of 500 network devices (AAA clients). • Evaluation—Expires 90 days from the time the license is issued. Supports deployments that have a maximum of 50 managed devices. 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 5.4 does not support the auto installation of evaluation license. Therefore, if you need an evaluation version of ACS 5.4, then you need to obtain the evaluation license from Cisco.com and install ACS 5.4 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 either ACS 5.2 or ACS 5.3 installed on your machine, you can upgrade to ACS 5.4 using one of the following two methods:

- Upgrading an ACS Server using the Application Upgrade Bundle
- Reimaging and Upgrading an ACS Server

You can only perform an application upgrade bundle, on either a Cisco appliance or a virtual machine, if the disk size is greater than or equal to 500 GB. If you have a smaller disk size, you need to reimage to ACS 5.4 followed by a restore of the backup taken in ACS 5.2 or ACS 5.3 version to trigger the upgrade.

When you upgrade from ACS 5.3 to 5.4, it is mandatory to install ACS 5.3.0.40.8 prior to the upgrade or the upgrade may fail. If you use the version prior to ACS 5.3.0.40.6, then you might hit an error and the upgrade will not proceed. Note that ACS 5.4 does not include all fixes that are included in 5.3.0.40.8. Therefore, if any of these fixes in 5.3.0.40.8 are required in your deployment, then you should install patch 5.4.0.46.1 after you upgrade to ACS 5.4.

See *Installation and Upgrade Guide for Cisco Secure Access Control System 5.4* for information on upgrading your ACS Server.

Note Upgrading to ACS 5.4 may fail if any LDAP identity store is configured without groups or attributes in it and AD identity store is not configured. To avoid this issue, before upgrading to ACS 5.4, you need to either add groups or attributes to the LDAP identity store or you need to configure an AD.

Applying Cumulative Patches

Periodically, patches will be posted on Cisco.com that provide fixes to ACS 5.4. These patches are cumulative. Each path includes all the fixes that were included in previous patches for the release.

You can download ACS 5.4 cumulative patches from the following location:
http://www.cisco.com/cisco/web/download/index.html

To download and apply the patches:

Step 1 Log into Cisco.com and navigate to **Products > Security > Access Control and Policy > Policy and Access Management > Cisco Secure Access Control System > Cisco Secure Access Control System 5.4**.

Step 2 Download the patch.

Step 3 Install the ACS 5.4 cumulative patch. To do this:

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

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

ACS displays the following confirmation message:

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

Step 4 Enter **`yes`**.

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

Step 5 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: 5.4.0.46.1
Internal Build ID: B.225
Patches:
5-4-0-46-1
acs/admin #
```

Resolved ACS Issues

Table 3 lists the issues that are resolved in ACS 5.4.

Table 3 Resolved Issues in ACS 5.4

Bug ID	Description
CSCtx53223	ACS 5.3 fails to join AD domain, and the Centrify license is missing when you upgrade ACS from its previous versions.
CSCtx53340	The NIL-CONTEXT error in the ACS 5.3 TCP Listener Process causes TACACS+ failure.
CSCub60424	Unable to register ACS in the deployment when the import operation is in progress.
CSCty01094	In ACS 5.3, the # sign in the AD group name produces an error.
CSCuc06451	ACS cannot find Global Catalogs.
CSCtw56213	In ACS 5.x, AD1: pwdLastSet attribute condition is not saved and shows an error when you use a long value for it.
CSCub98158	The replication is not working when you register or deregister a secondary ACS instance.
CSCtt24620	The delete host operation in SSH fails, with an "% Internal error during command execution" error.
CSCtx56129	The ACS 5.x replication service fails because it cannot bind to port 2030.
CSCtx65488	Add the TACACS+ protocol argument as an attribute on conditions in authorization policies.
CSCtx99378	Unable to log in to the ACS 5.x web interface if the hostname has a dot (.) in it.
CSCty10523	ACS 5.x does not allow blank spaces around separators in AV pairs.
CSCuc57160	Upgrade fails when you use the Enum definition for ACS Reserved Authentication ID Store attribute.
CSCty68058	Database restore error: the ACS database integrity check failed.
CSCty70612	The ACS 5.x migration utility fails to export all ACS 4.x users.
CSCua63063	The ACS view does not show the 30 days report.
CSCua66744	The ACS view database transaction log reaches more than 50 GB, which fills the /opt partition size.
CSCua67150	The network device is not recorded in the RADIUS Authentication logs.
CSCua90369	ACS 5.x is creating the error message: ShellProfile..ERROR...DeviceAttrFactory.cpp:29.
CSCub15396	ACS 5.3 does not support blank spaces in the TACACS shared secret key.
CSCub20366	ACS 5.3 does not retrieve the local groups when you install patch 3 or later.
CSCub27718	The system alarm message list should be documented in ACS 5.x documents.
CSCub40498	The password field in ACS 5.3 has the autocomplete operation enabled.
CSCub46074	ACS 5.3 response is very slow with a large number of identity groups.
CSCub61366	ACS does not strip the LDAP username prefix to the last occurrence.

Table 3 Resolved Issues in ACS 5.4 (continued)

Bug ID	Description
CSCub84814	In the ACS 5.3 primary server, promoting a secondary server to a primary server is not working.
CSCtz51830	Cannot edit a group name that contains the “}” character.
CSCtz76233	ACS 5.3 fails to join the AD when the username or password has a dollar ”$” symbol.
CSCtz80879	Unable to create a MAC address with the wildcard mask * in the end station filters.
CSCua06098	Unable to run the "show logging" command.
CSCua28423	The ACS 5.x system clock does not support the next leap second on June 30, 2012.
CSCtw84073	Unable to enter acs-config in the ACS CLI.
CSCua98027	The ACS documentation needs to show more information about the Statistics Polling Period.
CSCub31641	New purge limits should be added or updated in the online help files and the User Guide.
CSCsm00425	Unable to create authorization profiles with maximum value for unsigned integers.
CSCtx05302	ACS 5.x fails to generate reports and displays the "Report generation failed. Cause: null” error.
CSCtz24314	ACS 5.x runs out of disk space.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.1

Table 4 lists the issues that are resolved in the ACS 5.4.0.46.1 cumulative patch.

You can download the ACS 5.4.0.46.1 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 4 Resolved Issues in Cumulative Patch ACS 5.4.0.46.1

Bug ID	Description
CSCuc60457	Users created prior to adding the ACS-RESERVED-Never-Expired ignore the default value if set to TRUE.
CSCud17220	Maximum user session is case sensitive.
CSCuc13958	ACS web pages are not displayed properly when you use Firefox version 15.x.
CSCuc68843	Secondary ACS server is reported to be in Local mode incorrectly.
CSCub82913	ADclient cache issue - Authentication fails when you change the OU in multiple domain controller environment.
CSCtn99545	Administrators with numerical username are unable to use the dashboard.
CSCuc80049	Editing device filters results in validation error and ACS runtime to crash.
CSCuc28306	Unable to export the ACS_Log_Information from ACS view to a .csv file.
CSCub98880	Sometimes, the details icon in the troubleshooting reports page is not shown.
CSCuc93106	Upgrading from ACS 5.3 to ACS 5.4 fails.
CSCud06310	TCP socket exhaustion causes ACS 5.x to crash.
CSCub40278	XSS vulnerabilities were found in ACS view pages.
CSCub40291	CSRF vulnerabilities were found in ACS 5.3.
CSCub40480	Cookie vulnerabilities were found in ACS 5.3.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.2

Table 5 lists the issues that are resolved in the ACS 5.4.0.46.2 cumulative patch.

You can download the ACS 5.4.0.46.2 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

ACS 5.4 patch 2 supports Windows 2012 AD.

Table 5 Resolved Issues in Cumulative Patch ACS 5.4.0.46.2

Bug ID	Description
CSCud36423	ACS 5.4 supports setting up maximum number of sessions for each user on group level.
CSCud63630	A script error is displayed when you select the authorization profile results in ACS web interface using Internet Explorer.
CSCub40412	The session ID is displayed in the error logs.
CSCub15246	ACS fails to update the UPN suffix list.
CSCuc76487	The ADclient crashes while building the trusted domain map and parsing the SRV and LOC cache records.
CSCud79530	ACS does not properly manage the root certificate authorities.
CSCue31419	"Object not found" error is displayed in the ADclient logs when you disconnect and reconnect ACS 5.3 to AD.
CSCub40331	The support bundle in ACS 5.3 has vulnerabilities.
CSCue35765	An invalid alarm is shown in ACS 5.3, as follows: The database purge is not running for the past two days.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.3

Table 6 lists the issues that are resolved in the ACS 5.4.0.46.3 cumulative patch.

You can download the ACS 5.4.0.46.3 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 6 Resolved Issues in Cumulative Patch ACS 5.4.0.46.3

Bug ID	Description
CSCud40928	The secondary instance management process remains in initializing state after deregistering it from the deployment.
CSCtq54680	ACS 5.x adds a default blank space when you configure a TACACS+ attribute manually.
CSCud98038	Incorrect records are displayed in ACS Administrator login records after restarting ACS management services.
CSCue25744	ACS 5.x interactive viewer filter is greyed out.
CSCuc93503	ACS does not send an access reject message for requests sent without user name and password.
CSCue71318	Filtering the command sets does not work properly.
CSCua34208	ACS returns a wrong username in the access-accept response for access-accept request sent by the client.
CSCuf31396	In ACS 5.4, On Demand Data Purging is not working properly and the Purge Now button is greyed out.
CSCue33753	ACS 5.x dashboard displays "Value too long" error.
CSCue68493	The collection filter operation is case sensitive in ACS. But, the ACS web interface is not case sensitive.
CSCue85453	Unable to restore a backup file which is backed up from ACS 5.4 web interface.
CSCuc58345	The ACS-RESERVED-NEVER-EXPIRED attribute in ACS counts the number of days and sends reminder mails until it expires when this attribute is set to true.
CSCuf16197	The ACS-RESERVED-Never-Expired attribute does not prevent the user account from expiring.
CSCug29901	After installing ACS 5.4 patch 2, ACS breaks the EAP-TLS protocols when the root or client certificate does not contain the SKI or AKI.
CSCue43289	Rules in Access Policies are pushed to the end of the list when you use filter to search or make any changes in them.
CSCug27046	The CLI command "tech dumptcp" does not escape the arguments properly.
CSCug21883	ACS stops logging the ACS Instance catalog reports when you select to override the logging categories.
CSCug08493	When you add a property based query in REST services, the resulting page displays some unnecessary items.

Table 6 Resolved Issues in Cumulative Patch ACS 5.4.0.46.3

Bug ID	Description
CSCuf93782	ACS window freezes when you press F5 or click refresh.
CSCug79631	Unable to delete the objects in ACS 5.*x* which has “or” in its name.
CSCud56657	ACS 5.4 user import template does not contain the date exceeds fields.
CSCud75174	Client-side filtering option in ACS leads to XSS Attack
CSCud75177	CSRF vulnerabilities found in ACS admin and ACS view pages.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.4

Table 7 lists the issues that are resolved in the ACS 5.4.0.46.4 cumulative patch.

You can download the ACS 5.4.0.46.4 cumulative patch from the following location:

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

Refer to “Applying Cumulative Patches” section on page 16 for instructions on how to apply the patch to your system.

Table 7 Resolved Issues in Cumulative Patch ACS 5.4.0.46.4

Bug ID	Description
CSCug92686	ACS marks Domain Controllers as dead after changing the password in AD.
CSCue70923	Hardening AD in ACS sometimes results in failed authentications.
CSCue30708	ACS 5.3 gets disconnected frequently with AD Domain Controllers and the error message “Cannot contact LDAP server” is displayed in the logs.
CSCuf77905	Network Device Group search takes too long to respond when the group has large number of devices in it.
CSCuh16386	Centrify white list with PAC testing.
CSCug51752	Authenticating users against LDAP fails when the root certificate is not selected on the web interface.
CSCug76945	LDAP server configuration page trusts any certificate and test bind to server passes when anonymous authentication is selected.
CSCuh22440	Service selection that references device filters fails after upgrading ACS from ACS 5.3 to ACS 5.4.
CSCto11421	ACS 5.*x* Network Device Group named service does not display the child objects in ACS web interface.
CSCuf44685	Incorrect host entry is added while adding a new interface in ACS 5.4.
CSCug86630	In ACS 5.4, logs messages are not displayed in ACS view and an error message “Garbage Collection overhead limit is exceeded” is displayed.
CSCug28561	ACS Database purging alarms are stopped.
CSCuh03584	ACS 5.x is unable to retrieve CN from BMPSTRING encoded certificate field.
CSCuh12488	A Malformed TCP packet results in runtime to crash.

Table 7 Resolved Issues in Cumulative Patch ACS 5.4.0.46.4

Bug ID	Description
CSCuh20183	ACS supports FF version 17.0.6 ESR.
CSCug53703	ACS gets logged ou when you create an authorization profile with a name that has a double quotes in it.
CSCuh30964	ACS5.4 is not recognizing the Subject Alternate Name value with UID.
CSCuh46765	An unexpected error occurs in ACS when you add more than 100 policies.
CSCuh47237	Unable to login to ACS with a base license or evaluation license with more than 500 devices.
CSCud74421	A wrong error message is displayed when the Domain Name Server is down. Authentications gets failed even after the Domain Name Server is up and running properly.
CSCuh06710	Centrify AD domain whitelisting breaks the ACS machine authentication.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.5

Table 8 lists the issues that are resolved in the ACS 5.4.0.46.5 cumulative patch.

You can download the ACS 5.4.0.46.5 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 8 Resolved Issues in Cumulative Patch ACS 5.4.0.46.5

Bug ID	Description
CSCuh17172	ACS needs to send an alarm for ACS configuration database size similar to the ACS View database size.
CSCuh16836	The script on the support bundle which is used to rebuild the ACS View database does not work sometimes.
CSCui15100	Invalid schema files are present in ACS 5.4 REST schema.
CSCuh14898	ACS fails to join AD domain after installing ACS 5.4 patch 2.
CSCuh98939	ACS 5.4 centrify shows that the complete domain is not accessible when one of the subdomain is not accessible.
CSCui51469	ACS displays an internal error message after installing ACS 5.4 patch 3 and 4.
CSCui41190	ACS View jobs stop running intermittently.
CSCuh87325	The options under Network Device Group NDG tab are not displayed after installing ACS 5.4 patch 3.
CSCuh30576	ACS 5.*x* Domain Name Server queries mandate authoritative responses.
CSCui55934	ACS 5.4 Centrify cannot find the machine if SPN being used by the suplicant contains a DNS suffix which does not exist on the Domain Controller Group List.
CSCuh59288	ACS 5.x fails some authentications and dis plays the errors 24429 and 24444.

Table 8 Resolved Issues in Cumulative Patch ACS 5.4.0.46.5

Bug ID	Description
CSCui73761	In ACS 5.4, you cannot change a password using the REST service.
CSCui65823	ACS 5.x does not identify the MS attributes (MS-CHAP) in bundled attributes.
CSCuj01123	AD client restarts periodically during PEAP authentications.
CSCue65957	ACS displays sensitive information in error messages.
CSCud75170	The index page of ACS online help files is susceptible to XSS Attack.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.6

Table 9 lists the issues that are resolved in the ACS 5.4.0.46.6 cumulative patch.

You can download the ACS 5.4.0.46.6 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 9 Resolved Issues in Cumulative Patch ACS 5.4.0.46.6

Bug ID	Description
CSCuj91631	Launching secondary instance's web interface from primary ACS instance does not work if the secondary hostname is not resolvable.
CSCuj53935	The Certificate Authority edit page is susceptible to XSS.
CSCul09022	ACS does not respond when the TACACS requests are sent in segmented packets.
CSCuj65655	ACS Administrator Login details does not display the correct administrator details.
CSCul64484	ACS View NBAPI must have better debug logs.
CSCuj94585	Active Directory authentications fails in ACS when same user is present in two different Organizational Units.
CSCuj01135	AD client restarts frequently with an exceptional error while communicating with LDAP server.

Note When you upgrade from ACS 5.4 to ACS 5.5, it is mandatory to install the pointed patch before you start upgrading from ACS 5.4 version. The name of the patch file is **Pointed-PreUpgrade-CSCum04132-5-4-0-46-0a.tar.gpg**. You can install this pointed patch directly on FCS candidate build or on top of any cumulative patch version.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.7

Table 10 lists the issues that are resolved in the ACS 5.4.0.46.7 cumulative patch.

You can download the ACS 5.4.0.46.7 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 10 Resolved Issues in Cumulative Patch ACS 5.4.0.46.7

Bug ID	Description
CSCur00511	ACS evaluation for CVE-2014-6271 and CVE-2014-7169.

Note It is highly recommended to execute the Reboot operation when the patch installation process prompts for it.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.8

Table 11 lists the issues that are resolved in the ACS 5.4.0.46.8 cumulative patch.

You can download the ACS 5.4.0.46.8 cumulative patch from the following location:

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

Refer to "Applying Cumulative Patches" section on page 16 for instructions on how to apply the patch to your system.

Table 11 Resolved Issues in Cumulative Patch ACS 5.4.0.46.8

Bug ID	Description
CSCus68826	ACS 5.x is vulnerable to CVE-2015-0235.
CSCun84823	Non-authenticated users can see the input validation code in ACS.
CSCuo89864	In ACS 5.5, there are issues in cross frame scripting and session tokens in the URL.
CSCup10509	A security administrator can change his role to be a super administrator in ACS 5.5.
CSCur30345	SSLv3 Poodle vulnerability evaluation is found in ACS.
CSCuo78625	ACS 5.5 does not allow the special characters in the shared secret of TACACS+ and RADIUS authentications.
CSCuq79027	Injection Vulnerability is found in ACS.
CSCur42721	Improvement is required in ACS 5.x TACACS+ threading.
CSCur98716	ACS 5.4 displays "GC overhead limit exceeded" exception and the Monitoring and Reports web interface fails to load.
CSCus17482	The primary instance sends an incorrect reference to the secondary instances after deleting an object from the primary instance.

Table 11 Resolved Issues in Cumulative Patch ACS 5.4.0.46.8

Bug ID	Description
CSCur59417	ACS 5.x web interface fields does not allow the single quotes, apostrophe, and plus symbols
CSCup22665	Multiple Vulnerabilities are found in OpenSSL.
CSCuq79019	Multiple cross-site scripting vulnerability is found in ACS.
CSCur44131	ACS 5.5 does not display the installed patch version after installing patch 6.
CSCuq61347	ACS web interface logs the user out when you use special characters for device types, OCSP services, login banner, and so on.
CSCuq65102	ACS web interface logs the user out when you click submit from the TACACS+ global settings page.
CSCut01441	Runtime crashes if ACS receives a SIGPIPE (broken pipe) signal.
CSCus43434	Context limit is reached if ACS receives a reset request during packet processing.
CSCut61663	ACS needs to update “tzdata” for 2015 leap second.

Note It is highly recommended to execute the Reboot operation when the patch installation process prompts for it.

Resolved Issues in Cumulative Patch ACS 5.4.0.46.9

Table 12 lists the issues that are resolved in the ACS 5.4.0.46.9 cumulative patch.

You can download the ACS 5.4.0.46.9 cumulative patch from the following location:

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

Refer to “Applying Cumulative Patches” section on page 16 for instructions on how to apply the patch to your system.

Table 12 Resolved Issues in Cumulative Patch ACS 5.4.0.46.9

Bug ID	Description
CSCuu82493	OpenSSL Vulnerabilities were found in ACS during June 2015.
CSCus42781	OpenSSL Vulnerabilities were found in ACS during January 2015.
CSCut46073	OpenSSL Vulnerabilities were found in ACS during March 2015.
CSCux34781	Apache Common Collections Java library vulnerability was found in ACS during December 2015.

Limitations in ACS Deployments

Table 13 describes the limitations in ACS deployments.

Table 13 Limitations in ACS Deployments

Object Type	Medium	ACS System Limits
ACS Instances	13	21
Users	10,000	300,000
Hosts	1,000	150,000
Identity Groups	200	1,000
Network Devices	5,000	100,000
Network Device Groups	2	12
Device Hierarchies	3	6
All Locations	10	10,000
All Device Types	10	350
External Repositories	1 AD 1 LDAP	1 AD 1 LDAP 1 RSA
Services	5	25
Authorization Rules	25	320
Conditions	5	8
Authorization Profile	--	600
Service Selection Policy (SSP)	25	50
Network Conditions (NARs)	500	3,000
ACS Admins	15	50
	5 static roles	9 static roles
dACLs	2k size	600 dACL with 100 ACEs each

Known ACS Issues

Table 14 lists the known issues in ACS 5.4. You can also use the Bug Toolkit on Cisco.com to find any open bugs that do not appear here.

Table 14 Known Issues in ACS 5.4

Bug ID	Description
CSCua88450 Importing the .csv file with key-wrap enabled fails.	When you import a .csv file into ACS with key-wrap enabled, it fails. This problem occurs when you import a .csv file with key-wrap enabled into ACS. Workaround: 1. Export the .csv file with key-wrap enabled. 2. Open the file with notepad, edit the key-wrap values, and save the notepad file. 3. Now, import the .csv file. The import operation is completed successfully.
CSCua99537 Network Time Protocol Daemon (NTPD) running with ACS sometimes does not synchronize its clock with the Windows Time Service.	NTPD, when running with ACS, sometimes does not synchronize its clock with the Windows Time Service This problem occurs often when ACS or AD is running as a virtual machine. Workaround: None.
CSCtx42811 An error message is displayed while importing a CA certificate into ACS.	An error message is displayed while importing a CA certificate into ACS. This problem occurs when you import a CA certificate with an empty naming constraint. Workaround: Recreate the certificate without the empty constraint value.
CSCtz22307 ACS displays a script error in the secondary instance when you view the “ACS Instance Settings” under RSA.	ACS displays a **RSAInstance_edit.jsp** error when you view the “ACS Instance Settings” under RSA. This problem occurs when you do the following: a. Configure RSA (RSA SecurID Token Servers) in the distributed deployment. b. In the Secondary instance, select RSA Configuration and go to ACS Instance Settings page. c. Then select any of the ACS nodes and click **View**. Workaround: None.
CSCtz69725 Unable to set a value for the date attribute in a compound condition.	Unable to set a value for the date attribute in a compound condition. This problem occurs when you do the following: a. Create a date attribute under **Dictionary > Internal Users**. b. Now, try to create a compound condition in **Internal Users > Date Attribute > Static**. Workaround: None.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCua30932 ACS displays an "ACS: Resource not found" error on editing the attribute type in the AD page.	ACS displays an "ACS: Resource not found or internal server error" message. This problem occurs when you do the following: a. Choose **Users and Identity Stores > External Identity Stores > Active Directory > Directory Attributes.** b. Perform the attribute retrieval operation for any Active Directory user. Choose the attribute with the type string. For example, choose the name attribute. c. Choose **Access Policies > Access Services > Default Network Access > Authorization** and create a rule with the condition as AD1:name with a value, and click **Submit**. d. Now, choose **Users and Identity Stores > External Identity Stores > Active Directory > Directory Attributes** and edit the datatype of the name attribute from string to IPv4 Address, and click **Submit**. Workaround: Refrain from modifying the Active Directory attributes type after is created and used in a policy.
CSCua91354 TACACS+ proxy accounting requests are not logged properly in the ACS view.	TACACS+ proxy accounting requests are not logged in the ACS logs that proxy the requests to a remote server. However, the requests are properly logged in the remote server. This problem occurs when you use TACACS+ proxy accounting. Workaround: None.
CSCub15472 The user update operation with the change password option enabled is not working properly when you import or export the internal users.	When you import or export internal users, only one user out of the group of internal users has the change password option enabled. This problem occurs when you do the following: a. Create a Network Device Group (NDG), for example, Migrated_NDG, under Network Device Groups. b. Import the users (for instance, from internal_user_import_template-add). c. Update the same users in ACS with the change password option enabled or disabled. The result is that the change password option is enabled for a single user alone. For all the other users, it is disabled. Workaround: Manually enable the change password option.
CSCtz82993 Unable to launch the ACS web interface using IPv6 addresses in Firefox version 4 or later.	You cannot launch the ACS web interface using IPv6 addresses in Firefox version 4 or later. This problem occurs when you use Firefox version 4 or later to launch the ACS web interface using an IPv6 address. Workaround: Use the Internet Explorer browser version 8.x and 9.x or Firefox version 3.x to launch the ACS web interface using an IPv6 address.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCub31167 ACS shows the wrong replication status during full replication over WAN.	The status of the secondary ACS instance is shown as update when full synchronization is running. This problem occurs when you run full synchronization over the ACS secondary instance. Workaround: None.
CSCtz40538 ACS 5.x rejects PAC-based EAP-FAST authentication.	ACS 5.x rejects the expired tunnel PAC if the user's identity has a different format. This problem occurs when the EAP-FAST client sends an expired tunnel PAC and the user identity in different forms. The PAC contains a plain user name, while the authentication request contains the user identity in UPN form - user@domain.com. Workaround: Clean the expired PAC and retry the authentication.
CSCtu26765 Machine authentication and User authentication fail in a one-way trust domain.	Machine and User authentications fail and show the following: • Account disabled error, when it is in NetBios format. • Subject not found error, when it is in UPN format. This problem occurs when you join ACS to domain A, which has a one-way trust with domain B, and you try to authenticate the user or the machine from domain B. Workaround: None.
CSCtq12058 Debug logs are not displayed in the Monitoring and Report Viewer log.	Debug logs are not displayed in the Monitoring and Reports log. The default warning logs are displayed even after the log level is set to Debug. This problem occurs when you set the log level to Debug and view the reports in the Monitoring and Reports log. It also occurs when the system performs Authentication. Workaround: Restart ACS.
CSCtx42758 ACS configuration changes using REST are not shown in the audit reports.	When you update the Identity Group, Network Device Group, or Network Device Group Type, using REST, the ACS configuration updates are not shown in the audit report. This problem occurs when you update Identity Groups, Network Device Groups, or the Network Device Groups Type using REST. Workaround: None.
CSCtx42763 Unable to edit the parent Network Device Group name after creating it.	After creating the parent Network Device Group name, you cannot edit it. This problem occurs when you try to edit a newly created parent Network Device Group. Workaround: None.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCtx83716 Unable to launch the interactive viewer for reports from the dashboard in the Internet Explorer 8.x and 9.x browser.	The interactive viewer for reports cannot be launched from the dashboard when you use Internet Explorer versions 8.x and 9.x. This problem occurs when you try to open the interactive viewer for reports using Internet Explorer versions 8.x and 9.x. Workaround: Enable the compatibility view from the Tools menu in Internet Explorer versions 8.x and 9.x.
CSCtx95500 Opening certain view pages in a large deployment setup takes a long time.	Opening the following view pages in a large deployment that consists of 20 or more secondaries takes a long time to load the page. • Dash Board ACS authentication trend: 4 minutes. • Dashboard Health status: 3 minutes. • Log collection page: 4 minutes • AAA RADIUS authentication report page: 2 minutes • Catalog > AAA Protocol > Authentication Trend: 3 minutes. The above specified time may vary depending on the load and network latency. This problem occurs when you open the above-mentioned pages in a large deployment setup. Workaround: None.
CSCty35640 The timestamps in the ACS Monitoring and Reports Viewer web interface and the ACS Monitoring and Reports viewer reports are different.	There is a big difference observed in the timestamp shown in the ACS view reports and the timestamp in the ACS view web interface. This occurs only when log recovery is enabled. This problem occurs when there are active session database transaction log files opened that are large in size. Workaround: Restart ACS and remove all the large active session database transaction log files that were created.
CSCty40513 The ACS Application upgrade fails, showing a file transfer error.	The ACS application upgrade fails, showing a file transfer error. This problem occurs in the following scenarios: • When there is a problem in the network connectivity between ACS and the remote repository. • When the file transfer server has problems sending a large amount of data. Workaround: • Make sure that the network connectivity is working fine before executing the application upgrade procedure. • Make sure that the remote repository is capable of sending a large amount of data. If the problem still exists, then try using a different remote repository.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCty53666 The Network Device Group location filter is not working properly.	The Network Device Group location filter does not work properly when you execute a query where the name "Equals" a value and the condition "Starts With" a value. This problem occurs when you try to filter a list with a network device group location. Workaround: Refresh the page once.
CSCtz79960 The administrator authentication settings page displays an error.	In ACS, the administrator authentication settings page displays the "Unexpected error has occurred" error message. This problem occurs when you access the **System Administration > Administrators > Settings > Authentication** page soon after accessing the **System Administration > Administrators > Settings > Access** page. Workaround: None.
CSCua13802 The system status and the AAA status are shown as not available and zero in the dashboard.	The system status and the AAA status of all the other secondary instances shown in the ACS log collector web interface dashboard does not display correctly. This problem occurs when you process the status of each secondary instance from the ACS log collector using the path **Monitoring and Reports > Dashboard > ACS Health Status**. Workaround: None.
CSCua20683 Unable to reset the admin password using the CLI.	The application password is not reset when you try to reset it using the **application reset-passwd acs acsadmin** command in the CLI. This problem occurs when you execute the **application reset-passwd acs acsadmin** command in the CLI. Workaround: Use the **acs reset-password** command in acs-config mode.
CSCua95069 Need to reduce the time taken to export the ACS view logs to a .csv file.	The time that is takes to export the ACS view logs to a .csv file should be reduced. This problem occurs when you export the ACS view logs to a .csv file from the ACS web interface. Workaround: None. However, you can export a smaller amount of data.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCub67627 The **show ad-agent-configuration-changes** command does not retrieve the latest changes made in the AD agent configuration.	The command **show ad-agent-configuration-changes** does not retrieve the latest changes that were in the AD agent configuration parameters. This problem occurs when you do the following: **a.** Configure the ad-agent parameter. **b.** Execute the **show ad-agent-configuration-changes** command. This shows the configured parameters with the current values. **c.** Now, execute the **ad-agent reset-config** command. This resets the value of the ad-agent configuration parameters. **d.** Now, execute the **show ad-agent-configuration-changes** command. This does not show the parameter value after reset. Instead, it shows the old value. Workaround: None.
CSCub71249 An incomplete command error is displayed when you execute the **ad-agent** command partially in CLI.	An incomplete command error is displayed when you only partially execute the **ad-agent** command in CLI. This problem occurs when you only partially execute the **ad-agent** command. Workaround: Execute the full command.
CSCub74889 There is a mount issue when upgrading to ACS 5.4 with the customer database.	The system does not reboot after the application upgrade and displays the following error in CLI: `Error 17: cannot mount selected partition` This problem occurs when you change the hard disk order in the CAM server. In the CAM server, you have a configuration in BIOS to change the hard disk order. HD0 should be selected first, and HD1 should be selected next. You should not change this order. Workaround: You can correct the hard disk order and reimage the CAM server with ACS 5.3, and then upgrade to ACS 5.4. Cisco does not provide support if the customer manually changes the BIOS configuration.
CSCuc13466 Unable to select the identity source in Firefox version 15.x.	You are unable to select the identity source when you use Firefox version 15.x. This problem occurs when you edit the identity source in Firefox version 15.x using **Access Policies > Access Services > Default Device Admin > Identity**. Workaround: Use a previous version of the Firefox browser.
CSCuc16427 Exporting records to a .csv file using the timestamp option does not work properly.	The export of records to a .csv file using the timestamp option does not work properly. ACS exports all the records instead of exporting the records for the selected timestamp. This problem occurs when you export records to a .csv file using the timestamp option. Workaround: None.

Table 14 Known Issues in ACS 5.4 (continued)

Bug ID	Description
CSCud58337 In Small UCS and IBM machines, sometimes the NICs are not in proper order.	In ACS 5.4, after the initial setup is completed, the gateway ping failed error occurs when you connect the ethernet cables in to the NICs which are not in proper order. This problem occurs when you assume the NICs are in proper order and connect the ethernet cables in to it. But, sometimes, in small UCS and IBM machines, the NICs may not be in proper order. Workaround: • Connect the ethernet cables from slot 1 to slot 3 in a proper order. • Reimage.
CSCud75015 RADIUS port is disabled if multiple NICs are configured one after another without restarting the ACS server	This issue occurs when you configure two network interfaces and assign IP addresses consecutively without waiting for the ACS services to restart after the first IP change. As a result, RADIUS communication is not working on the second interface that was configured. Other interfaces are not affected. Workaround: Restart ACS services.

Documentation Updates

Table 15 lists the updates to Release Notes for Cisco Secure Access Control System 5.4.

Table 15 Updates to Release Notes for Cisco Secure Access Control System 5.4

Date	Description
01/06/2016	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.9.
06/08/2015	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.8.
10/06/2014	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.7.
01/03/2014	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.6.
10/08/2013	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.5.
06/25/2013	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.4.
05/17/2013	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.3.
02/21/2013	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.2.
01/08/2012	Updated the document with Resolved Issues in Cumulative Patch ACS 5.4.0.46.1.
10/30/2012	Updated the guide with Cisco 3415 Secure Access Control System information.
10/23/2012	Cisco Secure Access Control System, Release 5.4.

Product Documentation

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

Table 16 lists the product documentation that is available for ACS 5.4. To find end-user documentation for all the products on Cisco.com, go to: http://www.cisco.com/go/techdocs

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

Table 16 Product Documentation

Document Title	Available Formats
Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
Migration Guide for Cisco Secure Access Control System 5.4	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 5.4	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 5.4	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 5.4	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 5.4	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
Release Notes for Cisco Secure Access Control System 5.4	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-release-notes-list.html
Software Developer's Guide for Cisco Secure Access Control System 5.4	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:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

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 1121 Hardware Platform is preinstalled. CDs containing tools to restore this Software to the 1121 hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported Cisco Secure Access Control System Software Products on the Cisco 1121 Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 1121 Hardware Platform.
- Software Upgrades, Major and Minor Releases. Cisco may provide Cisco Secure Access Control System Software upgrades for the 1121 Hardware Platform 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 1121 Hardware Platform. If the Customer is eligible to receive the Software release through a Cisco extended service program, the Customer should request to receive only one Software upgrade or new version release per valid service contract.
- Reproduction and Distribution. Customer may not reproduce nor distribute software.

3. DEFINITIONS

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

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

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Release Notes for Cisco Secure Access Control System 5.4