



Release Notes for Cisco Secure ACS 4.2

Revised: October 8, 2009, OL-14490-04

These release notes pertain to the Cisco Secure Access Control Server, hereafter referred to as ACS version 4.2. These release notes contain information for the Windows, Solution Engine(SE), and Cisco Secure Access Control Server 1120(CSACS 1120) platforms. Where necessary, the appropriate platform is clearly identified.

Cisco Secure ACS 4.2 is Federal Information Processing Standards (FIPS) 140-2-certified for Cisco Secure ACS FIPS module version 1.1—a software cryptographic library that provides cryptographic services to Cisco Secure ACS release 4.2.



Note

The ACS release numbering system for software includes major release, minor release, maintenance build, and interim build number in the MMM.mmm.###.BBB format. For this release, the versioning information is Cisco Secure ACS 4.2.0.xxx. Elsewhere in this document where 4.2 is used, we are referring to 4.2.0. ACS major release numbering starts at 4.2.0. Please use this information when working with your customer service representative.

Contents

This document contains:

- [Introduction](#)
- [New and Changed Information](#)
- [Installation Notes](#)
- [Known Caveats](#)
- [Resolved Caveats](#)
- [Documentation Updates](#)
- [Product Documentation](#)
- [Notices](#)
- [Obtaining Documentation and Submitting a Service Request](#)



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

Introduction

ACS is the policy-control and integration point for access to or through Cisco devices or solutions. ACS is the dominant enterprise network-access control platform, and it is the administrative access-control system for Cisco devices and applications.

ACS 4.2 is a minor release for the ACS 4.x versions that addresses customer enhancements, bug fixes, and includes the FIPS module. ACS 4.2 includes new functionality and features described in the document and in the User Guide for ACS 4.2.

New and Changed Information

ACS 4.2 contains the following new and changed information:

- [New Features](#)
- [Using ACS 4.2 in a FIPS 140-2-Compliant Mode](#)
- [RADIUS Key Wrap Extended to All EAP Protocols](#)

New Features

ACS 4.2 provides the following new features that protect networked business systems:

- **Transition to the Windows 2003 Operating System for the ACS SE**
- **Turning ICMP ping on/off (ACS SE)**—On the ACS SE, you can turn the ICMP ping response on or off. In some cases, another network device must receive a valid ICMP ping response before sending an authentication request.
- **Native RSA (ACS SE)**—Support of RSA proprietary interface on the ACS SE.
- **Programmatic interface enhancements for RDBMS Synchronization**— RDBMS synchronization has added capabilities for dACLs. You can create, update, and delete user-level and group-level downloadable ACLs through RDBMS synchronization.
- **Enabling Secure Shell (SSH) client remote invocation for RDBMS Synchronization for the ACS SE**— A command line interface where you can change the ACS configuration through remote systems. An SSH server now offers a service in the ACS SE. You can connect from any SSH client to the ACS SE and use the CSDBSync command to perform database synchronization.
- **Enabling CLI RDBMS Synchronization invocation for ACS for Windows.**
- **NetBIOS disabling**—In ACS for Windows, you can now disable NetBIOS on the server on which it is running.
- **Logging enhancements**—Enhanced Comma Separated Values (CSV)-generated log messages. Passed and failed authentication reports now include Response Time, Session-ID, and Framed-IP-Address attributes.
- **Upgrade features**—You use these features to preserve and restore ACS 4.1 backup configuration to ACS 4.2. This feature eliminates the problem of upgrading existing ACS 4.1 configuration to ACS 4.2.
- **Group filtering at NAP level when using LDAP**—When using LDAP to query an external user database, you can perform group filtering at the Network Access Profile level. Depending on the user's external database group membership, ACS can reject or accept access to the network, based on the group filtering settings.

- **RSA authentication with LDAP group mapping**—ACS can authenticate with RSA and simultaneously perform group mapping with LDAP. Administrators can now use this option to control authorization based on a user's LDAP group membership.
- **EAP_FAST options:**
 - **EAP-FAST enhancement for anonymous TLS renegotiation**—An anonymous TLS handshake occurs between the end-user client and ACS. EAP-MSCHAP is the only inner method in Phase 0 of EAP-FAST.
 - **EAP-FAST enhancement for an invalid PAC**—You can now run EAP-FAST without issuing or accepting any tunnel or machine PACs when it receives an invalid PAC. All requests for PACs are ignored. ACS takes no action with PAC requests; but, instead, responds with a `Success-TLV`; even though no valid PAC is present. All the relevant PAC options are disabled when you choose this option.
 - **EAP-TLS - PAC less and no Active Directory processing EAP-TLS**—ACS supports EAP-FAST tunnel establishment without PACs or client certificate lookup.
- **Option of disabling caching of dynamic users**—Administrators can determine whether they want to disable the creation of dynamic users while using an external database for authentication. Minimal performance disruption occurs when disabling caching of dynamic users.
- **Active Directory multi forest support**—ACS supports authentication in a multi-forest environment. Active Directory authentication succeeds as long as an appropriate trust relationship exists between the primary ACS forest and the requested domain's forest.
- **Time configuration**—You can set the ACS SE to the local or GMT time zone. Log viewing and syslog can receive local or GMT time zone stamps.
- **Temporary Elevated User Privileges**—ACS supports the granting of administrator privileges temporarily to another user.
- **Object Identifier (OID) Check for EAP-TLS Authentication**—ACS checks the OID against the Enhanced Key Usage (EKU) field in the user's certificate.
- **Layer 2 Audit for Network Access Control**—ACS supports auditing of agentless hosts connected to a Layer 2 Network Access Device (NAD).
- **ACS for Windows now includes the GUI based CSSupport utility.**
- **UTF-8 Support**—ACS supports the use of UTF-8 (the 8-bit Universal Coded Character Set (UCS)/Unicode Transformation Format) for the username and password only when authenticating with Active Directory.
- **Adding devices through CSUtil**—ACS now supports using the CSUtil *import.txt* file for adding and editing authentication, authorization, and accounting (AAA) devices.
- **ACS now supports 3COMUSR VSAs.**
- **User-defined vendors extended VSA ID**— You can use CSUtil or RDBMS synchronization to install dictionary components for vendors that require extended VSA ID length.
- **Customizing a Workstation Name for Windows Authentication**—ACS now supports multiple ACS deployments by using a single Active Directory tree.
- **Configuring the ACS RADIUS Server to reject or discard requests to an external ODBC Database.**
- **Improved Diagnostic Logs** —Diagnostic log files contain the line number of the source code that generated the error. The CSAuth diagnostic log now includes Session IDs.
- **Improved EAP Code Debug Messages**—All EAP debug messages are now reported to the CSAuth diagnostic log.

- **RADIUS Key Wrap is now extended to all EAP protocols.**
- **NAC-NAP IA**—ACS 4.2 supports NAC-NAP interoperable architecture (IA) which allows Cisco NAC and Microsoft NAP technology to interoperate. If you want to evaluate or deploy NAC-NAP IA, contact your Cisco account representative for assistance.

Using ACS 4.2 in a FIPS 140-2-Compliant Mode

This section describes how to use Cisco Secure ACS 4.2 in a FIPS 140-2-compliant mode:

- Follow the guidelines described in FIPS 140-2 Level 1 Security Policy for Cisco Secure ACS FIPS Module Version 1.1, at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp948.pdf> to operate your ACS in a FIPS-compliant mode.
- Use only FIPS 140-2 AAA clients in approved FIPS mode of operation. Refer to the client FIPS 140-2 Security Policy configuration guidelines found at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp948.pdf> for more information.
- Enable ACS logging; the default setting (Low) is acceptable. Refer to the *User Guide for Cisco Secure ACS 4.2* for more information.
- Enable RADIUS Key Wrap in ACS; refer to [RADIUS Key Wrap Extended to All EAP Protocols](#).
- AAA clients must use only EAP-TLS, EAP-FAST, or PEAP protocols for authentication, with key wrap.



Note

ACS 4.2 conforms to FIPS 140-2 only when you use the allowed FIPS 140-2 compliant protocols. It is the network Administrator's (FIPS 140-2 Crypto Officer) responsibility to enforce this policy; ACS does not block you from using any protocol.



Note

In EAP-FAST, do not use the out-of-band protected access credentials (PAC) provisioning.

AAA clients must support Authenticated Diffie-Hellman with SHA1 and AES, or RSA with SHA1 and AES for TLS negotiation.



Note

EAP-FAST enhancement for anonymous TLS renegotiation, EAP-FAST enhancement for an invalid PAC, and EAP-TLS - PAC less and no Active Directory processing EAP-TLS features, are not FIPS compliant.

RADIUS Key Wrap Extended to All EAP Protocols

RADIUS Key Wrap is extended to all EAP protocols; previously, RADIUS key wrap was available only for EAP-TLS.

In previous ACS releases the Allow RADIUS Key Wrap check box resides in the EAP-TLS section of the **Network Access Profiles > Protocols** page.

ACS 4.2 has moved the Allow RADIUS Key Wrap check box to the top of the EAP Configuration section, in the new Key-Wrap area. You must use this option for EAP-TLS, EAP-FAST, and PEAP protocols when operating your ACS in a FIPS 140-2-compliant mode for authentication.

Installation Notes

This section contains installation information for ACS 4.2.

Installation Notes for ACS 4.2 for Windows

This section contains:

- [Upgrade Path for ACS 4.2 for Windows](#)
- [System Requirements for ACS 4.2 for Windows](#)

Upgrade Path for ACS 4.2 for Windows

For more information on ACS 4.2 upgrade paths, see the *Installation Guide for Cisco Secure ACS for Windows 4.2*.

System Requirements for ACS 4.2 for Windows

For information on supported operating systems and web browsers, see the *Installation Guide for Cisco Secure ACS for Windows 4.2*.

Installation Notes for ACS 4.2 Solution Engine

This section contains:

- [Upgrade Path for ACS 4.2 Solution Engine](#)
- [System Requirements for ACS 4.2 Solution Engine](#)

Upgrade Path for ACS 4.2 Solution Engine

For ACS 4.2 upgrade paths, see the *Installation Guide for Cisco Secure ACS Solution Engine 4.2*.

System Requirements for ACS 4.2 Solution Engine

For information on the system requirements for the Solution Engine, see the *Installation Guide for Cisco Secure ACS Solution Engine 4.2*.

Miscellaneous Issues

This issue refers to bug CSCea91690 which explains about the event viewer errors that appear on startup and shutdown of the Windows .NET Server 2003.

When the Windows .Net Server 2003 boots up or is shutdown, false errors that indicate the Cisco Secure ACS service has failed, are generated. At startup, a dialog box appears indicating that a service, such as CSLog, encountered a problem and needs to close. The same error is logged to the Event Viewer as:

```
Reporting queued error: faulting application CSLog.exe, version 0.0.0.0, faulting
module unknown, version 0.0.0.0, fault address 0x00000000.
```

The problem occurs in Windows Server 2003 when the Service Manager queries the Cisco Secure ACS services status during startup and shutdown. But, ACS services may not have started or may have stopped. Even though this is normal behavior for ACS services, Windows perceives this as an error and logs it to the Event Viewer. When Windows Server 2003 boots up and the user logs into windows, the event viewer displays all errors from the previous log session.

This behavior occurs on Windows Server 2003. To solve this error, you must verify that the ACS services are running using the control panel.

Known Caveats

Table 1 contains known caveats in ACS for Windows and Solution Engine 4.2. You can also use the Bug Toolkit on Cisco.com to find any open bugs that might not appear here.

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2

Bug ID	Summary	Explanation
CSCsb74346	Authorization of disabled user succeeded.	<p>Symptom When you disable a user account in the ACS Internal Database, it does not influence TACACS+ authorization requests to the user. TACACS+ authorization requests succeed, if they match the user's TACACS+ settings, although the user's account is disabled. TACACS+ authentication requests fail for such users.</p> <p>Workaround None.</p>
CSCsb95897	ACS cannot display a long list of disabled accounts correctly.	<p>Symptom The ACS web interface cannot display several pages of disabled accounts list as the Previous button can be clicked only once.</p> <p>Workaround None.</p>
CSCse26754	ACS/ACSE Administration performs limited session validation.	<p>Symptom After successful login, ACS performs only limited session validation by matching the IP alone. This is due to a weakness in the default configuration of ACS. Cisco is investigating this issue and further details will be added to the Cisco Security Response as it becomes available.</p> <p>Workaround For details, see Cisco.com.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCse93831	In 4.0, the number of IP addresses per AAA client is limited.	<p>Symptom Data is missing from certain Network Device Groups even after the ACS upgrade process completes normally.</p> <p>Conditions This was observed while upgrading from ACS 3.3.3(11) to 4.0(1). After the upgrade process, two Network Device Groups containing AAA clients with a large number of subnets (over 240), of subnets had been truncated at 94.</p> <p>Workaround No workaround available this time.</p>
CSCsf11087	Cisco PA attributes not being displayed in the Passed Authentication Report for a Linux client.	<p>Symptom Cisco:PA attributes are not being displayed in the Passed Authentication Report for a Linux client with CTA 2.1.0.10 installed. The attributes are being displayed in the auth.log file and on a Win XP client on the same network.</p> <p>Workaround In System Configuration > Logging > Passed Authentication, select Cisco:PA attributes and click on Submit. This performs the authentication using the Linux client with CTA 2.1.0.10 4. After this process is complete, check the passed authentication log on the Reports and Activity page.</p>
CSCsg24486	Two New Tacacs Services with similar names have issues with data.	<p>Symptom In Interface Configuration > TACACS (Cisco IOS), create two new services with similar names. When you enter data in one service and save the changes, the same data will be copied to both services.</p> <p>Conditions The new service names contain spaces.</p> <p>Workaround Do not use spaces in service names.</p>
CSCsg37180	ACS LDAP query size limit is 50000.	<p>Symptom When you use LDAP as an external user database and try to edit the ACS group to LDAP group mapping; for example, when you click Add Group, the web interface will display the error message "LDAP disconnected".</p> <p>Conditions Your LDAP group list query response contains more than 50000 results.</p> <p>Workaround Keep the number of groups under control.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsg71976	ACS hangs with invalid LDAP/SSL authentications with referrals.	<p>Symptom When you use ACS, with LDAP/SSL configured as an external user database, if one login attempt fails due to an invalid username or password, then all subsequent login attempts will fail, even if login details are valid. You must reboot to refresh the authentications, but if an invalid username or password is entered again, then all further authentication attempts will fail.</p> <p>Conditions The Use Secure Authentication checkbox must be checked to enable LDAP/SSL in the LDAP external user database. The LDAP server must respond with referrals to other servers.</p> <p>Workaround Unencrypted LDAP works. If you use LDAP/SSL, then you must configure the LDAP database to reply without referrals. You must reboot to refresh the authentications, until the next invalid username or password is issued.</p>
CSCsh89581	ACS Administration does not respond under heavy load.	<p>Symptom When the ACS Administration GUI does not respond after a period of time, the service has to be restarted to allow administration access to ACS. However, this does not affect user authentication to the ACS.</p> <p>Conditions When LMS 2.6 is authenticating to an ACS appliance on 4.0.1.44 code, a patch is applied to the LMS server to ensure that sessions created by auto-refresh are also logged out. When this issue occurred, the CSAdmin logs stopped sending any further information until the services are restarted. In the environment in which this issue occurred, within 5 minutes the LMS servers established over 6000 administrative connections to CSAdmin (and logged out again). There is a high probability that this issue is related to load.</p> <p>Workaround Restart the ACS (for an ACS Solution Engine) or the CSAdmin process (for ACS installed on Windows) to allow administration access to ACS GUI.</p>
CSCsi55085	ACS services do not start on a dual CPU machine after it is replicated or rebooted.	<p>Symptom ACS services do not start when the Secondary ACS machine is rebooted within 30 minutes after database replication.</p> <p>Conditions After the database replication between a primary ACS and a secondary ACS machine with dual processors, this issue occurs when the secondary ACS machine is rebooted within 30 minutes.</p> <p>Workaround Do not reboot the secondary ACS machine within 30 minutes of database replication.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsj14508	Some special characters in the FTP password are wrong.	<p>Symptom When an incorrect password is used, backup attempts fail with the FTP server.</p> <p>Conditions This occurs when a password contains special characters such as #, %, @, etc. This may be present in ACS 4.1.3 and other ACS versions.</p> <p>Workaround Use a password with only text or number characters.</p>
CSCsj60407	ACS Backup filename is changed to uppercase letters.	<p>Symptom The FTP filename created for backups must contain the hostname of the appliance but, the hostname randomly changes to uppercase or lowercase letters.</p> <p>Conditions ACS for Windows and ACS Solution Engine on 4.1(1) Build 23.</p> <p>Workaround None.</p>
CSCsk25159	ACS Upgrade: Dictionary Corruption CiscoACS\Dictionaries\005	<p>Symptom After upgrading to 4.1.1.23 or 4.1.1.24 from 4.0.1.27, service does not start. The RDS.log displays the error: RDS 28/08/2007 09:29:33 P 0202 0700 Dictionary Config Error: Ignoring unrecognized value 'Type' in key CiscoACS\Dictionaries\005 RDS 28/08/2007 09:29:33 P 0202 0700 Dictionary Memory Error: dict_DictionaryInitCallback cannot parse dictionary configuration</p> <p>Conditions Run ACS 4.0.1.27 and then upgrade to 4.1.1.23 or 4.1.1.24. This occurs in rare cases.</p> <p>Workaround Call TAC and send in your database backup. The dictionary can be repaired.</p>
CSCsk27193	Can't use <cr> when entering multiple MAC addresses.	<p>Symptom When defining authentication configuration for NetworkAccess Profiles Access Policies, if you press "return" after each MAC address and submit the changes, error messages are displayed.</p> <p>Conditions This occurs in ACS 4.1.1(23) when using Internet Explorer 6.0 and JRE 1.5</p> <p>Workaround Separate MAC addresses with a comma (,), and do not press "return" after the last MAC address has been entered.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsk93795	ACS 4.1 sends invalid MS-CHAP-MPPE-Keys to PPTP client.	<p>Symptom A PPTP client that connects to an IOS router with Radius authentication, fails if "Require encryption" is selected. Radius attributes are configured at the user level.</p> <p>Conditions ACS returns "Invalid MPPE key length (11)" this should be (34) bytes. 11 bytes are: 0c (vendor-type 12) 0b (vendor-length = 11) and 41 75 74 6f 6d 61 74 6963 (the word "Automatic"). ACS sends the wrong key length as IOS accepts a vendor-length of 34.</p> <p>Workaround Use local authentication or optional encryption.</p>
CSCsk94878	Cannot change the windows password when the PDC Emulator is down.	<p>Symptom The user cannot change the windows password when the PDC Emulator is down.</p> <p>Conditions This symptom occurs even if the other Domain Controller is up for the same domain, and all of DCs are running in Native mode (W2K3 mode or W2K mode). User authentication can be successful with the other DC even if the PDC Emulator is down.</p> <p>Workaround Do not attempt to change the windows password when the PDC Emulator is down.</p>
CSCsl46350	Authentication complete message not displayed.	<p>Symptom When an invalid username is entered, ACS does not reply.</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. Use EOU with EAP-FAST. 2. Select "Prompt automatically for username and Password" in the EAP-FAST "User Credentials" setup, and enter an invalid username. <p>Workaround None.</p>
CSCsl50122	ACS SE needs configurable RA timeout value.	<p>Symptom This is a request to add a timer to the ACS Appliance. This timer can be configured to monitor how long the ACS SE waits before timing out the Remote Agent during group mapping.</p> <p>Conditions ACS SE running 4.1.1.23 or higher.</p> <p>Workaround If group mapping times out, manual mappings can be used.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCs170457	Some ACS 1113 Appliances ship with BIOS password.	<p>Symptom Some ACS 1113 appliances that ship from RMA depots, come with a bootup password of 'acs1113'.</p> <p>Conditions Appliance comes with a BIOS Password.</p> <p>Workaround On boot, enter the BIOS password of 'acs1113'.</p>
CSCs188008	ACS GUI does not prevent the dynamic allocation of port 2002.	<p>Symptom ACS does not prevent the dynamic allocation of port 2002 when a users logs in or when LMS is used.</p> <p>Workaround Login to ACS, change the Administration Control, Access Policy, and HTTP Port Allocation to:</p> <p>Restrict Administration Sessions to the following port range From Port 2003 to Port 65535.</p>
CSCs199170	Logged in Users not functional in Proxy Scenario.	<p>Symptom Logged in users are not being updated in the proxy ACS. This error occurs only real time and does not occur in simulators (Used Switch with dot1x config).</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. Configure two ACS servers as ACS 2 & ACS 3. 2. Configure ACS 2 as the Primary ACS server. 3. When a request is received in UPN format (user@nmtg.com), ACS 2 directs the request to ACS 3 (@nmtg.com, suffix, strip) (Acct - local/remot) 4. ACS 3 processes the request and authenticates the user. 5. Logged in users are not updated in ACS 3. <p>Workaround None.</p>
CSCsm36747	Increasing memory consumption in the CSAdmin during import process.	<p>Symptom CSAdmin consumes memory and does not get released.</p> <p>Conditions During the import process of AAA clients from the CLI, using the CSUtil tool.</p> <p>Workaround Restart all services.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsm45861	Windows Database Group Mapping fails when the username is in UPN format.	<p>Symptom Unable to find user name even though it is present in the local group.</p> <p>Conditions When ACS is configured to use the old API.</p> <p>Workaround You must use a plain username without the UPN format (without domain suffix).</p>
CSCsm60215	ACS Appliance has authorization issues with extended attributes.	<p>Symptom After upgrading to 4.1.1, third party devices using extended attributes, fail to authorize ACS and sends an RST to the authorization session.</p> <p>Conditions Using 4.x code on an appliance that uses extended attributes.</p> <p>Workaround None.</p>
CSCsm64286	Request from NAS fails when default NAS is defined under NDG.	<p>Symptom Authentication fails, when a request is sent from the "other" NAS.</p> <p>Conditions NAR is configured to deny the request from the defined NAS. While the "others" default TACACS+ NAS is defined under NDG.</p> <p>Workaround None.</p>
CSCsm64931	NAR does not filter users when "Apply password change rule" is selected.	<p>Symptom All the devices are TACACS+ devices.</p> <ol style="list-style-type: none"> 1. Define per group NAR with two NDGs (GA, GB) and configure it to permit access (Permit). 2. Define the device named 'others' with IP address *.*.*.*. 3. Do not include 'others' in the NAR. 4. In the group setting, check the checkbox "Apply password change rule". 5. Change the password for one of the users in that group. 6. Authenticate (telnet) to a TACACS+ device which is not explicitly defined in any group. <p>Result: You are prompted to change the password and subsequently access the device. But in the next authentication, you are denied access to the device.</p> <p>Conditions This error occurs when NAR is applied.</p> <p>Workaround None.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsm66268	If there is no NAP, Group Mapping fails with Ext DB when service type is 10.	<p>Symptom Group mapping fails when service type is 10 and when no Network Access Profile is configured in ACS.</p> <p>Conditions Perform MAC authentication with service type as 10 against the LDAP database. Do not configure NAP in ACS if Group mapping fails.</p> <p>Workaround Configure NAP and enable "Allow Agentless Request Processing" or do not send the request with service-type as 10.</p>
CSCsm68921	No console access during System Recovery.	<p>Symptom When performing system recovery with the recovery CD, the console output freezes after the "Press <SpaceBar> to update BIOS" message appears.</p> <p>Conditions The problem can occur with any version of the recovery CD.</p> <p>Workaround None.</p>
CSCsm69491	Disabled users accounts and groups still check external databases.	<p>Symptom ACS checks the external database for password verification before checking if the user account is disabled.</p> <p>Conditions ACS checks the external database for password verification before checking if the user account is disabled. This was present in the RADIUS database but may also be present in other external databases.</p> <p>Workaround This is an enhancement request. This is a request to change the flow, so that ACS first checks if the account is disabled before checking the external database for password verification.</p>
CSCsm70790	Default BIOS configuration are changed.	<p>Symptom In some of the new appliances the BIOS settings are different from the existing one. Due to this image the appliance cannot be imaged with the recovery CD.</p> <p>Conditions This error occurs in some of the new appliances.</p> <p>Workaround None.</p>
CSCsi82254	FAST1a When Posture PA is large - Auth is failed.	<p>Symptom Authorization using FAST1a with big PA message fails.</p> <p>Conditions It occurs in ACS 4.1.2.11 on Windows 2003.</p> <p>Workaround Provide a short PA.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsj23646	Performing a stress test on GAME during audit server outage, causes an internal error.	<p>Symptom An internal error occurs, when testing GAME on an audit server that is down.</p> <p>Conditions When performing a stress test using GAME.</p> <p>Workaround The Audit server must be up and running.</p>
CSCsj87562	Remote Logging Reports shows wrong information.	<p>Symptom The remote logging report displays wrong information for the column "Logged Remotely".</p> <p>Conditions Configure Remote Logging and do an authentication check for the Remote Logging Reports (passed Authentication or Failed Attempts). The Column "Logged Remotely" displays "No" when it should be "Yes". This occurs in ACS 4.1.</p> <p>Workaround None.</p>
CSCsj99992	RDS logs show Merge Control attribute missing from PDE policy output.	<p>Symptom RDS logs show the Merge Control attribute missing from the policy agent. This is a warning message as a result of the client packet and can be ignored.</p> <p>Conditions It occurs in ACS 4.2.</p> <p>Workaround None.</p>
CSCsk09761	Called Station ID value is not logged in passed or failed attempts reports.	<p>Symptom Called-Station-ID is not logged in the Passed or Failed attempts report.</p> <p>Conditions While performing any authentication with Called-Station-ID attribute.</p> <p>Workaround None.</p>
CSCsk17182	Extend maximum allowed characters for absolute filepath - DBSync via CSV.	<p>Symptom [Microsoft][ODBC Text Driver]String data right truncated on column number 6 (ValueName). Warning message appears in RDBMS Synchronization reports.</p> <p>Conditions Absolute file path specified for account action codes (ex 385 ..), is more than 49 characters.</p> <p>Workaround Specify absolute filepath that is less than 49 characters.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsk29412	ACS fails to use correct credentials to authenticate users.	<p>Symptom Failure to authenticate user in anonymous in-band PAC provisioning.</p> <p>Conditions In ACS EAP-FAST when anonymous in-band PAC provisioning is configured and the clients user identity is an outer identity, PAC provisioning fails to authenticate the user when incorrect credentials are provided. This authentication fails even when the correct credentials are provided as ACS continues to use the invalid credentials when attempting to authenticate the user. This condition occurs in all versions of ACS 4.x</p> <p>Workaround Use an anonymous identity as the outer identity.</p>
CSCsk32262	Count increases in group when the same user is authenticated by PKI auth Bypass.	<p>Symptom The function "List All Users" under "User Setup" increases for the same user.</p> <p>Conditions This occurs when you configure EAP-FAST with PAC-less when the Client Certificate Lookup and Comparison is disabled.</p> <p>Workaround None.</p>
CSCsk53325	Windows Authentication must fail when duplicate NetBIOS names exist in forest.	<p>Symptom Creates ambiguity when searching for a user in AD.</p> <p>Conditions This occurs when more than one domain is configured and the NETBIOS name of two domains are identical.</p> <p>Workaround Windows does not allow you to create two domains with identical NETBIOS names.</p>
CSCsk53454	ACS should allow you to retry in case of password change failure.	<p>Symptom ACS does not allow password retry for the error code 709 - "Password Change failed".</p> <p>Conditions Change the password through EAP-FAST/GTC (or any other methods that support password change) with the new password which does not meet password complexity.</p> <p>Workaround Enter a new password that meets the password complexity rule.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsk59988	EAP-FAST [TLS] does not work for Cross forest user authentication.	<p>Symptom Occurs when doing EAP-FAST authentication with the CSSC client.</p> <p>Conditions Client is sends inner-identity without domain markup.</p> <p>Workaround This is not a bug since CSSC can be customized to send inner-identity in UPN format.</p>
CSCsk60007	Inconsistent message when deleting the CA certificate in CTL.	<p>Symptom Message when you delete CA certificate in CTL.</p> <p>Conditions When you delete the CA certificate in CTL it fails but does not explain the reason for failure. This condition occurs in ACS 4.2.</p> <p>Workaround None.</p>
CSCsk62859	EAP-FAST: Second phase represented as None during machine authentications.	<p>Symptom EAP-FAST Inner methods appear as None in machine authentication. This error occurs for all inner methods for EAP-FAST.</p> <p>Conditions Occurs in ACS 4.2 for all EAP-FAST inner methods.</p> <p>Workaround None.</p>
CSCsk68870	Work Station Restriction not functioning with EAP-TLS authentication.	<p>Symptom While doing EAP-TLS authentication, the workstation does not allow the user to be present.</p> <p>Conditions While doing EAP-TLS authentication</p> <p>Workaround This is not a bug as TLS authentication searches for the user in a respective domain. The workstation attribute is acceded only if the user is authenticated using a password.</p>
CSCsk92498	CS-Log fails to start after Replicating the Secondary machine.	<p>Symptom CS-Log fails to start after Replication in the secondary machine.</p> <p>Conditions This error occurs when you replicate a huge database from Primary Windows 2000 ACS to Secondary Windows 2003 Standard Edition ACS.</p> <p>Workaround None.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCs102590	CS-Auth restarts & authentication fails during EAP-TLS.	<p>Symptom CSAuth restarts and the authentication fails during EAP-TLS.</p> <p>Conditions When a stress test is run from one machine with 1000 user X 100 cycle 1 workers per client for the build ACS 4.2.0 build 111 in windows 2003 machines.</p> <p>Workaround None.</p>
CSCs110248	Log files become unusable after downloading using firefox and netscape.	<p>Symptom Log files downloaded using Firefox or Netscape browsers are not usable.</p> <p>Conditions This occurs when the download is done using Firefox or Netscape.</p> <p>Workaround Use Internet Explorer.</p>
CSCs116871	CSUtil strips username while creating PAC.	<p>Symptom While creating PAC, CSUtil strips domain information from the username.</p> <p>Conditions When the manual cPAC provisioning is used.</p> <p>Workaround Automatic PAC provisioning will solve the issue or a username without domain markup.</p>
CSCs179863	ACS Certificate Installation	<p>Symptom When installing a new certificate in ACS Windows, from the System Configuration > Install ACS Certification page, the old certificate is deleted even before the new certificate is uploaded.</p> <p>Conditions Occurs in all 4.x releases of ACS.</p> <p>Workaround None.</p>
CSCs196222	Appliance RDBMS Sync: Failed to connect to FTP server.	<p>Symptom While syncing, FTP connection is failed.</p> <p>Conditions While downloading files from FTP, connection is not established.</p> <p>Workaround By setting FTP password without '/' can solve this issue.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsm07762	Drop Down Menu not functioning for posture token - do not audit groups.	<p>Symptom The drop down menu for selecting the Posture Token for the host that will not be audited, is not functioning.</p> <p>Conditions The user does not want to audit the members of some ACS user groups. He needs to select a Posture Token for the hosts that will not be audited.</p> <p>Workaround There is an option to audit, based on the Host IP Addresses and Ranges or Host MAC Addresses. Select the option, do not audit these hosts. This option will enable the functioning of the Drop down menu for selecting the Posture Token for the host that will not be audited. You can select the required posture token.</p>
CSCsm36481	PEAP TLS MachineAuthentication with account disabled generates internal error.	<p>Symptom PEAP TLS MachineAuthentication with account disabled displays the following error message:</p> <p style="padding-left: 40px;">Authentication fails with Internal error in the Auth log, instead of:</p> <p style="padding-left: 40px;">Authentication fails with External DB account disabled.</p> <p>Conditions This error message appears if you:</p> <ul style="list-style-type: none"> • Configure PEAP TLS machine authentication. • Disable the machine account in AD. • Perform Authentication. <p>Workaround None.</p>
CSCsm36518	Machine Authentication with groupmapping configuration set to <No Access> is not logged in Failed.	<p>Symptom Machine Authentication with group mapping configuration to <No Access> is not logged in the Failed attempts log.</p> <p>Conditions Occurs in ACS 4.1 and 4.2 with the following ACS configuration:</p> <ul style="list-style-type: none"> • Configure PEAP TLS Machine Authentication. • Configure External DB group mapping to be <No Access>. • Perform Machine Authentication. <p>Workaround None.</p>

Table 1 **Known Caveats in ACS Windows and Solution Engine 4.2 (continued)**

Bug ID	Summary	Explanation
CSCsm37778	ACS needs to normalize MAC addresses for Attribute [1].	<p>Symptom ACS does not normalize the MAC addresses for Attribute [1].</p> <p>Conditions MAB from a switch sends the following attributes:</p> <ul style="list-style-type: none"> • Attribute [1] (Username) - MAC address of the client that requires network access for MAB. • Attribute [30] (Called-Station-ID) - MAC address of the ingress interfaces of the switch or authenticator. • Attribute [31] (Calling-Station-ID) - MAC address of the client that requires network access for MAB. <p>Attributes [30] and [31] are sent in the format of XX-XX-XX-XX-XX-XX for all switches. This has recently been updated in the switch code base to ensure compatibility with legacy switch code and also compliance with RFC 3580. 802.1X requests operate the same way. Neither of these attributes, are expected to provide the authentication service provided by MAB.</p> <p>Authentication and authorization are provided from RADIUS Attribute [1] (username) and RADIUS Attribute [2] (password). For IOS-based switches and recent versions of CatOS, the format for the username and password attributes is simply hhhhhhhhhhhh. This is an all lower-case version of hhhh.hhhh.hhhh with the punctuation stripped out.</p> <p>ACS normalizes a MAC address for Attribute [31] only. When an LDAP query is performed when a NAP is matched, 3 separate queries are generated in the form of:</p> <ul style="list-style-type: none"> • macAddress=00-11-22-33-44-55 • macAddress=00:11:22:33:44:55 • macAddress=0011.2233.4455- <p>ACS must be able to do this for Attribute [1] and support legacy MAB environments, whose back end databases may not store the MAC address in the "hhhhhhhhhhh" format.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsm37851	RADIUS Accounting logs are false.	<p>Symptom RADIUS Accounting logs are false.</p> <p>Conditions When MAB authenticates on a port and sets the following on a RADIUS Access-Accept:</p> <ul style="list-style-type: none"> • Attribute[27] = 60 • Attribute[29] = RADIUS-Request--> <p>Every 60 seconds the device should re-authenticate and an interim update should also be logged in RADIUS-Accounting.</p> <p>However, before the Accounting entry for any interim update occurs, a false entry appears in the accounting, which displays "NAS-Port re-used". It reports an incorrect session time.</p> <p>Workaround None.</p>
CSCsm43674	Fields edited for an upgraded user, displays wrong information in Administration Audit.	<p>Symptom Fields edited for an upgraded user, gives wrong information in Administration audit.</p> <p>Conditions It occurs in ACS 4.2 with the following configuration:</p> <ul style="list-style-type: none"> • In ACS4.1 add users with Network Access restriction. • Take a back up of ACS 4.1. • Restore the dump in ACS 4.2 using "Restore from 4.1 backup file to ACS 4.2". • Edit the ACS 4.1 user, and check the logs in Administration Audit. The administration audit contains information for the file that is not edited. <p>Workaround None.</p>
CSCsm52514	ACS Java causes Firefox and JRE 1.6.0_04 to hang on Japanese Windows.	<p>Symptom Sun Java hangs and prevents login when accessing ACS.</p> <p>Conditions</p> <ul style="list-style-type: none"> • Japanese Windows XP/2003: Japanese Firefox 2.0.0.11 + JRE 1.6.0_04 • Japanese Windows XP/2003: Japanese Firefox 2.0.0.11 + JRE 1.6.0_03 => OK • Japanese Windows XP/2003: Japanese internet Explorer 6.0 SP2 + JRE 1.6.0_04 is OK • US-English Windows XP/2003: US-English Firefox 2.0.0.11 + JRE 1.6.0_03 => OK <p>Workaround Use IE or Open Java Console first <firefox menu -> tools -> Java Console>, and then access ACS.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.2 (continued)

Bug ID	Summary	Explanation
CSCsm57518	ODBC Configuration fails after upgrading from 4.1.	<p>Symptom Occurs when upgrading from 4.1 to 4.2.</p> <p>Conditions ODBC configuration is missing after upgrading to 4.2.</p> <p>Workaround After upgrading, configure once more to solve the issue.</p>
CSCsm57566	Windows user fails when ODBC is placed above in Unknown User Policy.	<p>Symptom When performing authentication with Windows database and ODBC, if the ODBC is placed at the top in an unknown user policy, then authentication fails.</p> <p>Conditions While doing authentication with windows database and ODBC.</p> <p>Place the windows database at the top of the unknown user policy when the user is authenticating to a windows database.</p>

Table 2 contains known caveats in ACS that are specific to CSACS 1120. You can also use the Bug Toolkit on Cisco.com to find any open bugs that might not appear here.



Note The following known caveats will not impact the functionality and performance of ACS.

Table 2 Known Caveats for CSACS 1120

Bug ID	Summary	Explanation
CSCsy06360	CSACS 1120 console not available during appliance reboot.	<p>Symptom During the appliance reboot, BIOS-POST processing messages are not displayed in the terminal emulation which is connected to the CSACS 1120 appliance.</p> <p>Conditions This occurs during the CSACS 1120 appliance reboot.</p> <p>Workaround None.</p>
CSCsy06738	USB port are enabled by default in the CSACS 1120 appliance.	<p>Symptom USB ports are enabled by default in the CSACS 1120 appliance.</p> <p>Conditions BIOS settings</p> <p>Workaround These ports are disabled in the base image (MSFT win2k3 OS) of the appliance.</p>

Table 2 Known Caveats for CSACS 1120

Bug ID	Summary	Explanation
CSCsy39711	Recovery/Restore options not displayed in CSACS 1120 monitor.	<p>Symptom After the CSACS 1120 appliance is rebooted from the DVD-ROM, the recovery options are not displayed if the monitor is connected. Previous versions of appliances supported the display of recovery options on the monitor.</p> <p>Conditions This occurs after the CSACS 1120 appliance is rebooted from the DVD-ROM.</p> <p>Workaround None.</p>
CSCsy89476	CSACS-1120 appliances are not protected with BIOS password.	<p>Symptom CSACS-1120 appliances are not protected with BIOS password.</p> <p>Conditions When entering into CSACS 1120 appliance BIOS.</p> <p>Workaround None.</p>

Resolved Caveats

Table 3 contains the resolved caveats for ACS 4.2. Check the Bug Toolkit on Cisco.com for any resolved bugs that might not appear here.

Table 3 Resolved Caveats in ACS Windows and Solution Engine 4.2

Bug ID	Description
CSCee89510	Syslog: dates are logged in GMT always, need to be configurable.
CSCsb24849	ACS does not purge the AAA Client user information after Accounting On.
CSCsc77154	Proxy authentications fail when no DHCP is present at installation.
CSCsc84543	CSMon doesn't restart services when CSTacacs hangs.
CSCsc90467	After Install from Recovery CD, no CLI access.
CSCsd18172	After Installing Appliance the default windows IP remains in the AAA server.
CSCsd25239	ACS does not detect a change to its IP address.
CSCsd40204	Document that dynamic ACL is not applicable for DDR/aggregation.
CSCsd52663	Cross forest user/machine authentication does not work.
CSCsd88833	Manual setup of ip configuration failed, CLI is not foolproof enough.
CSCse69819	Custom UDV, Replication don't replicate. Failure to create on secondary.
CSCsf15057	Can't ping the ACS appliance if the CSA agent is turned on.
CSCsf17112	SSL Handshake error message too general.
CSCsg40727	ACS 4.0: RDMS fails account action 220 250 with Synchronization Partners.
CSCsi39730	ACS Solution Engine 4.1 Rec CD Install Wrong Device Name and IP address.

Table 3 *Resolved Caveats in ACS Windows and Solution Engine 4.2 (continued)*

Bug ID	Description
CSCsi53074	ACS Account permissions sometimes needs Logon as a Batched Job.
CSCsi77061	The called-station-id attr is not included in passed/failed reports.
CSCsj01813	BIOS settings on the ACS SE for action on power up.
CSCsj08738	Optional Posture Validation in ACS not functional.
CSCsj09748	csmon logs filled with Message:Could not generate valid Password.
CSCsj32256	Permit/Denied for others TACACS+ default NAS is inverse in NARs.
CSCsj36562	Replication fails under condition of stress between WAN Geography.
CSCsj58199	CSAuth crashes Exception trapped on UDB_SEND_RESPONSE
CSCsj61652	ACS does not update the version number in registry after upgrade.
CSCsj70952	ASA 8.0: ACS 3076/11 attribute needs new enumeration for SVC protocol.
CSCsj71204	Need to post ACS 4.1.x and 4.0.x patches for ASA 8.0 attributes deltas.
CSCsj86746	Unable to add attributes for logging.
CSCsj87434	ACS does not bind ACS group and Domain after config replication.
CSCsk02317	Misleading Error messages in Auth.log after replication.
CSCsk12033	Replication might take long time to finish due to EventNotifier deadlock.
CSCsk15339	To allow no AD processing when PACLESS is enabled.
CSCsk15412	Action code 224 and 225 for Update and Read AAA client.
CSCsk20823	CSTacacs memory leak.
CSCsk23467	Remote agent installation guide doesn't contain updated info.
CSCsk44072	MS-PEAP authentication failed not shown up in ACS logs.
CSCsk44292	After ACSE and switch re all authentications are failing.
CSCsk50267	CSAuth crashes when EAP-FAST user and initiator IDs are different.
CSCsk53707	Exception trapped and CSAuth restarts with NAR configured.
CSCsk62604	CAA fails to prompt for password change in ACS 4.1.3 code.
CSCsk64715	Group mapping (NAP) replication fails with a timed replication.
CSCsk67139	ACS SE patch certificate expired. Throwing warning message.
CSCsk71372	Make 4.1.4 replication updates configurable.
CSCsk76343	'others' NAS is processed inversely by NAR when in an NDG.
CSCsk76533	ACS will not restart by CSMon, when caughting exception.
CSCsk88667	Provide option for both implicit AND and implicit OR for OID comparison.
CSCsl09917	CSAuth restarts when machine auth user name is without domain info.
CSCsl11777	dbserv9 start up parameters and command line should be hidden.
CSCsl41548	ACS using EAP-FAST-Authentication(inner EAP type GTC) reprompts 3 times.
CSCsl49180	Cisco Secure ACS User-Changeable Password Buffer Overflows.
CSCsl49205	Cisco Secure ACS User-Changeable Password XSS Vulnerability.

Table 3 *Resolved Caveats in ACS Windows and Solution Engine 4.2 (continued)*

Bug ID	Description
CSCsl51500	Failed to get GC Server for trust - when DC & GC are different machines.
CSCsl62845	ACS Remote Agent logging date format is not as specified on Appliance.
CSCsm23558	Problem while logging TACACS+ command accounting.
CSCsm52554	Doc:EAP TLS machine authentication not allowed for SAN & CN outer identity.
CSCsm55253	Others TACACS+ adopt permit/denied from defined NAR.
CSCsm71037	CSAgent doesn't start after bootup.

Table 4 contains the resolved caveats for ACS Windows and Solution Engine 4.1.3. Check the Bug Toolkit on Cisco.com for any resolved bugs that might not appear here.

Table 4 *Resolved Caveats in ACS Windows and Solution Engine 4.1.3*

Bug ID	Description
CSCeb43948	Could not generate valid Password with password length => 9.
CSCed45731	ACS logs should indicate level of logging.
CSCee65661	CSCeh42116
CSCeg52536	Failed PEAP authentication not shown up in ACS logs.
CSCeh42116	EAP-TLS Machine Authentication fails when AD PDC emulator down.
CSCsd12551	IP pools disappear occasionally from Group Setup/Edit Settings.
CSCsd20149	After initial config from Recovery CD, no GUI access.
CSCsd63894	ACS does not respond with the same IP address for RADIUS.
CSCsd95346	VSA definition for Total Control HiperARC card accounting attributes.
CSCsd98589	Authentications fail when NIC reconnected after reboot.
CSCse49827	ACS Remote Agent fails users with too many groups.
CSCsf28775	Expired accounts are incorrectly reported.
CSCsf98129	Client host name in ACS cannot be deleted.
CSCsg24465	Update OS to support Daylight Saving Time for the 2007 energy bill.
CSCsg32883	Feature: Authentications from ACS not hardcoded to workstation CISCO.
CSCsg37381	ACS authentication stops intermittently with - Unknown error code: -1018.
CSCsg62459	Unable to delete CA Cert from CA list.
CSCsg87232	Enhancement: Add Cisco-AvPair to VOIP accounting records.
CSCsg89656	CSAuth does not shutdown cleanly in some ACS 4.0 installs.
CSCsg96534	ACS support for Windows 2003 R2 needs clarification.
CSCsg97429	TACACS+ Command Accounting does not work in ACS 4.1(1) Build 23.
CSCsh05964	ACS 4.1: Separate enable password fails when unix password type used.
CSCsh18742	ACS should silently discard packet when external ODBC DB not available.
CSCsh24710	Shell Commands Authorization Set part of commands are effective
CSCsh32888	Separate enable password does not work after ACS upgrade to 4.1

Table 4 *Resolved Caveats in ACS Windows and Solution Engine 4.1.3 (continued)*

Bug ID	Description
CSCsh39305	Administrative access policy does not take effect after replication.
CSCsh42893	ACS GUI hangs and times out when service is restarted during stress.
CSCsh43814	No users at IP x.x.x.x.
CSCsh62641	MAC authentication causes internal errors.
CSCsh65197	CSAuth crashes when username has a comma.
CSCsh69160	EAP FFAST1: ACS does not provide the supplicant with reason of rejection.
CSCsh74140	Loss of ext. database breaks NAD AAA redundancy concept.
CSCsh77651	Anti Virus is locking DB file.
CSCsh77806	EAP-TLS will fail authentication if name contains forwardslash /
CSCsh84447	Limited administrator sees first page empty if trying to list all users.
CSCsh87466	Authentication failure on first login after remote agent restart.
CSCsh89335	ACS EAP-FAST Replication fails generating server not responding error.
CSCsh90602	MAB no more functional after installing accumulative patch 4.1.1.23.3
CSCsh91209	ACS 4.X will fail to upgrade if DASL is greater than 32K.
CSCsh91761	ACS: XSS vulnerability via search facility in online help.
CSCsh99260	Feature: need to support Solaris 9 & 10 for ACS remote logging agent.
CSCsi03015	EAP-FAST(GTC) may grant access to AD user with empty username.
CSCsi97490	DOC: Missing format of CSUtil .ini file for setting VSA ID Length.
CSCsj84279	ACS 4.1.3 Accounting Proxy doesn't work properly.
CSCsm71037	CSAgent doesn't start after bootup.

[Table 5](#) contains the resolved caveats for ACS Windows and Solution Engine 4.1.4. Check the Bug Toolkit on Cisco.com for any resolved bugs that might not appear here.

Table 5 *Resolved Caveats in ACS Windows and Solution Engine 4.1.4*

Bug ID	Description
CSCeb43302	WaitForMultipleObjects returned [-1] feeds up HDD, then system down.
CSCeg52536	Failed PEAP authentication not shown up in ACS logs.
CSCeh13105	WinDB maps all other combinations instead of selected groups.
CSCeh86479	CSUtil import -85 errors to be changed to info msg-not error.
CSCei01730	EAP-TLS authentication to the trusted DC doesn't succeeded.
CSCsa95381	ACS requires Domain Administrator privileges for Win 2003 authentication.
CSCsb24849	ACS does not purge the AAA Client user information after Accounting On.
CSCsd52663	Cross forest user/machine authentication does not work.
CSCsf22420	ACS 3.3(3) CSR sent to TrustWise returns an error 0x3110.
CSCsf25881	Don't clear the certificate trust list when a new certificate is install.
CSCsg00942	UCP does not support special chars.

Table 5 *Resolved Caveats in ACS Windows and Solution Engine 4.1.4 (continued)*

Bug ID	Description
CSCsg12989	Cannot enable CRL checking unless certificate is checked in CTL.
CSCsg14022	PPTP clients auth. using MSCHAP v2 stops passing traffic sporadically.
CSCsg14329	ACS 4.0 and semi-colon separator in cisco-av-pair RADIUS attributes.
CSCsg81886	CSACS is subject to multiple XSS vulnerabilities.
CSCsg84315	CSACS admin users can get access to unprivileged web pages.
CSCsg88641	ACS SW/SE: Delete AAA server and Replication denied when rep to prev set.
CSCsg89042	Appliance upgrade via GUI requires additional step to release CLI.
CSCsh29345	ACS 4.0 - Unable to delete server under Network Configuration.
CSCsh42915	RDBMS synchronization using SQL MS intermittently fails.
CSCsh58091	Voice-over-Ip-Group sends password prompt when it should not.
CSCsh58656	ACS 4.0 - IETF attribute 006 Administrative doesn't work for Group level.
CSCsh62641	MAC authentication causes internal errors.
CSCsh77806	EAP-TLS will fail authentication if name contains forwardslash /
CSCsh88934	Unknown NAS errors not reported in failed attempts in ACS 4.1.
CSCsh91209	ACS 4.X will fail to upgrade if DASL is greater than 32K.
CSCsh95071	Database replication does not propagate certain log settings.
CSCsh97121	NDG shared secret display issue.
CSCsi13785	ACS won't replicate users previously set for dynamic mapping.
CSCsi16980	Tunnel-Server-Endpoint attribute field is truncated during logging.
CSCsi17499	Remote password change setting isn't replicated.
CSCsi24169	AAA Client IP Address field has no length checking.
CSCsi43436	CSAuth takes max 5 seconds to auth when CSLog is slow or going down.
CSCsi56892	'Logged Remotely' Radius Attribute not available for Remote Agent Log.
CSCsi57134	QoS values incorrect for WLC.
CSCsi59931	ACS error when mapping groups to Microsoft database.
CSCsi60213	Last character of RADIUS IETF attr 81 is truncated.
CSCsi65427	ACS SE: Hostname greater then 15 characters locks out GUI and CLI.
CSCsi68322	ACS Release 3.3(4) Build 12 cannot sort distribution entries in the prox.
CSCsi73447	Support for Microsoft Windows Server 2003 R2 with SP2.
CSCsi97449	RDBMS Sync needs to support VSA Type Length above 2 bytes.
CSCsi97551	Machine authentications fail with errors: 1213,20498 with AD API.
CSCsj06122	ACS only log first instance of VSA under RADIUS attribute 26.
CSCsj07046	EAP-TLS authentications fail when user name is in DOMAIN\user format.
CSCsj12121	Expression matching for command authorization does not fully work in ACS.
CSCsj18497	ACS Appliance documentation does not list supported SNMP MIBs.
CSCsj32256	Permit/Denied for others TACACS+ default NAS is inverse in NARs.

Table 5 *Resolved Caveats in ACS Windows and Solution Engine 4.1.4 (continued)*

Bug ID	Description
CSCsj42058	JRE version in install guide needs update.
CSCsj42080	Misleading information about supported Microsoft security patches.
CSCsj54389	Group mapping fails for domain local users.
CSCsj71737	ACS Appliance memory leak in CSMon.
CSCsj84279	ACS 4.1.3 Accounting Proxy doesn't work properly.
CSCsk12033	Replication might take long time to finish due to EventNotifier deadlock.
CSCsk20823	CSTacacs memory leak.
CSCsk50267	CSAuth crashes when EAP-FAST user and initiator IDs are different.
CSCsk64715	Group mapping (NAP) replication fails with a timed replication.
CSCsk71372	Make 4.1.4 replication updates configurable.
CSCsk76343	'others' NAS is processed inversely by NAR when in an NDG.
CSCsk88667	Provide option for both implicit AND and implicit OR for OID comparison.
CSCsl09917	CSAuth restarts when machine auth user name is without domain info.

Documentation Updates

This section provides the following documentation updates:

- [Updates](#)
- [Errors](#)
- [Omissions](#)

Updates

Cisco Secure Authentication Agent

This section provides information about installing the CiscoSecure Authentication Agent, hereafter referred to as CAA.

Installing the Cisco Secure Authentication Agent

This section provides information about installing the CiscoSecure Authentication Agent Configurator Software in Microsoft Windows 95 or Windows NT 4.0, hereafter referred to as CAA.



Note

This information is intended for the system administrator.

Extracting the CAA Configurator File

To launch the CAA Configurationself-extracting file:

Step 1 Download of the *caaadmin.exe* file (the self-extracting zip file).

Step 2 Locate the downloaded *caaadmin.exe* file and double-click it.

The WinZip self-extractor program launches automatically.

Step 3 Unzip the *caa* zip folder.

Once the unzip process is complete, the prompt displays:

```
Files have unzipped successfully.
```

Click **Close**, to exit the WinZip program.

Step 4 When the extraction process is complete; new installation files are created in the specified directory.



Note

Be sure to read the *readme.txt* file for the most recent information on this product.

Installing the CAA Configurator

The administrator must install the CAA Configurator software for Windows 95 or Windows NT and, optionally install the CAA.

To install the CAA Configurator software:

Step 1 Locate the *setup.exe* file in the CAA directory.

To run the *setup.exe* file, double-click it.

Step 2 You are prompted to choose the destination location for the installation.



Note

The default destination directory is *C:\Program Files\CiscoSecureAACfg*.

Step 3 To change the installation location, click the **Browse** button to choose the directory where the setup program installs the CAA Configurator and click **Yes**.

The CAA Configurator files are copied and you are prompted to launch the Configurator. If you are only using the Messaging Service feature (for example, to use the Password Aging feature), you do not have to run the CAA Configurator.

Click **No**, to use the default configuration file (*default.caa*).

Step 4 To create a new configuration file, click **Yes**. If you click **No**, the *default.caa* configuration file is automatically loaded.

If you have additional configuration files, you can choose one file to modify, or you can click **Cancel** to create a new configuration.

Step 5 If you choose the Simplified ISDN Token Authentication option, you must choose the Single or Double Authentication method.



Note

The Messaging Service is a standalone feature at this time and is ignored if you use the Single or Double Authentication mode.

Step 6 Click **Exit**.

You are prompted to save the changes to the *default.caa* file.



Note We recommend you enter another name (for example, *lsmith.caa*, for the end user's username) for the *.caa* file.

Step 7 If you do not have a previous version of CAA installed on your PC, you are prompted to install it. Click **Yes**, to continue with the installation; click **No** to exit.

Step 8 If you click **No**, you can do a manual installation later. (See the next section for the manual installation steps.)

Step 9 To provide users with disks containing the CAA software, copy the contents of Disk1 and Disk2 onto separate disks. Copy each user's configuration file (for example, *lsmith.caa*), onto Disk1. You can also create a new zip file to include Disk1, Disk2, and the specific user's *.caa* file, and, then e-mail the files to individual users.

Installing the CAA Software

To manually install the CAA software:

Step 1 Locate the directory *Disk1* and run the *setup.exe* file.



Note The default location is *C:\ProgramFiles\CiscoSecureAACfg\Program\Disk1*.

You are prompted to choose the destination directory for the installation.



Note The default destination directory is *C:\ProgramFiles\CiscoSecureAA*.

Step 2 To change the installation location, click the **Browse** button to choose the directory where the setup program installs CAA.

Step 3 After you choose the directory, click **Next** to continue. You are prompted to choose the configuration file to use.



Note The default configuration file is *default.caa*. If more than one configuration file exists, no file name appears.

Step 4 To choose a configuration file, click the **Browse** button. You can choose to load the configuration file at startup. The CAA starts automatically when Windows 95 or Windows NT is boots. You are prompted to restart your computer.

Step 5 Click **Yes**, to restart your computer now. Click **No**, to restart your computer later.

Step 6 Click **Finish**.

The Installation process is completed.

Regulatory Compliance and Safety Information

In the printed and online version of the *Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.2*, Statement 191—VCCI Class A Warning for Japan has been updated.

Windows and Active Directory 2008 Supported Scenarios

In the online *Supported Interoperable Devices and Software Tables for Cisco Secure ACS Release 4.2* guide, the following information must be updated in:

- Supported Operating Systems section
 - Windows Server 2008, Standard Edition
 - Windows Server 2008, Enterprise Edition
 - Japanese Windows Server 2008, Standard Edition, Service Pack 2
 - Japanese Windows Server 2008, Enterprise Edition, Service Pack 2
- Table 2 Web Browsers

Program	Version	Notes
Microsoft Internet Explorer	Version 7 <ul style="list-style-type: none"> • Service Pack 2 for Microsoft Windows XP Professional (Japanese Language Version) <ul style="list-style-type: none"> – Sun Java Plug-in, v.1.6.0_16 • Service Pack 2 for Microsoft Windows Vista Business (Japanese Language Version) <ul style="list-style-type: none"> – Sun Java Plug-in, v.1.6.0_16 	Tested
Microsoft Internet Explorer	Version 6.0 <ul style="list-style-type: none"> • Service Pack 2 for Microsoft Windows XP Professional (Japanese Language Version) <ul style="list-style-type: none"> – Sun Java Plug-in, v.1.6.0_16 • Service Pack 2 for Microsoft Windows Vista Business (Japanese Language Version) <ul style="list-style-type: none"> – Sun Java Plug-in, v.1.6.0_16 	Tested with Service Pack 3
Mozilla Firefox	Version 3.5.2 <ul style="list-style-type: none"> • Japanese Language Version • Sun Java Plug-in, v.1.6.0_16 	Tested

- Table 16 User Databases

Platform	Version	Requirement
Win 2008 Active Directory Services	—	Tested with Service Pack 1
Remote Agent in Win 2008 Domain Controller / Windows 2008 Domain	—	Tested with Service Pack 1


Note

The support for Windows Server 2008 is applicable for ACS 4.2 Patch 4 onwards.

Types of SAN Supported

In the online *User Guide for Cisco Secure Access Control Server 4.2*, the following information must be updated in the EAP-TLS and ACS section, in Chapter 9.

ACS supports the following types of SANs:

- Machine authentication supports DNS Subject Alt Name.
- User authentication supports PRINCIPAL Subject Alt Name.

Errors

In the online *User Guide for Cisco Secure ACS 4.2*, in the New Features section, the Upgrade information pertains to ACS for Windows as well as the ACS SE.

Omissions

In the online *User Guide for Cisco Secure ACS 4.2*, the following note was omitted from the Global Authentication Setup Page in Chapter 9:

**Note**

Subjective Alternative Name (SAN) and Common Name (CN) outer identities cannot be used for EAP-TLS machine authentication.

This note pertains to the option: **Select one of the following options for setting username during authentication.**

In the online *User Guide for Cisco Secure ACS 4.2*, the following information was omitted from Table 8-1, Replication Component Descriptions:

Remote Agents configuration is replicated when the **Network Configuration Device tables** is chosen for the replication components.

Product Documentation

[Table 6](#) lists the product documentation for ACS 4.2.

Table 6 **Product Documentation**

Document Title	Description
<i>Documentation Guide for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> • Printed document with the product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
<i>User Guide for Cisco Secure Access Control Server 4.2</i>	<p>ACS functionality and procedures for using the ACS features. Available in the following formats:</p> <ul style="list-style-type: none"> • By clicking Online Documentation in the ACS navigation menu. The user guide PDF is available on this page by clicking View PDF. • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html
<i>Configuration Guide for Cisco Secure ACS 4.2.</i>	<p>Provides provide step-by-step instructions on how to configure and deploy ACS.</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html
<i>Installation Guide for Cisco Secure ACS for Windows 4.2</i>	<p>Details on installation and upgrade of ACS software and post-installation tasks. Available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.2</i>	<p>Details on ACS SE 1112 and ACS SE 1113 hardware and hardware installation, and initial software configuration. Available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html

Table 6 **Product Documentation (continued)**

Document Title	Description
<p><i>Installation and User Guide for Cisco Secure ACS User Changeable Passwords 4.2</i></p>	<p>Installation and user guide for the user-changeable password add-on.</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucpNW42.html
<p><i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.2</i></p>	<p>Installation and configuration guide for ACS remote agents for remote logging. Available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/RA42.html
<p><i>Installation Guide for the Cisco 1120 Secure Access Control Server 4.2</i></p> <p>Explains the installation process of ACS 4.2 on CSACS 1120.</p>	<p>On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/csacs_1120/csacs1120_4.2.html</p>
<p><i>Cisco Secure Access Control Server Troubleshooting Guide</i></p>	<p>On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACSTrbG42.html</p>
<p><i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.2</i></p>	<p>Translated safety warnings and compliance information. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document with the product. • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html
<p><i>Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control Server 4.2</i></p> <p>Provides translated safety warnings and compliance information for the CSACS 1120.</p>	<ul style="list-style-type: none"> • Shipped with the product. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/ACS1120_RCSI_42.html
<p><i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2</i></p>	<p>Supported devices and firmware versions for all ACS features.</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html

Table 6 *Product Documentation (continued)*

Document Title	Description
<i>Release Notes for Cisco Secure ACS 4.2</i>	ACS 4.2 features, documentation updates, and resolved problems. On Cisco.com : http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
Product online help	Help topics for all pages in the ACS web interface. Select an option from the ACS menu; the help appears in the right pane.

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 SSLey 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].

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.