



Release Notes for Cisco Secure ACS 4.1.4

Revised: June 10, 2008, OL-14207-03
CDC Date August 23, 2007

These release notes describe changes in Cisco Secure Access Control Server (ACS) release 4.1.4 for the Windows and Solution Engine platforms. Where necessary, the appropriate platform is clearly identified.

Cisco Secure ACS 4.1.4 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 4.1.4.

Contents

- [Introduction, page 1](#)
- [New and Changed Information, page 2](#)
- [Installation Notes, page 4](#)
- [Known Caveats, page 6](#)
- [Resolved Caveats, page 15](#)
- [Documentation Updates, page 16](#)
- [Product Documentation, page 18](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 20](#)

Introduction

ACS 4.1.4 is a maintenance release for ACS 4.1 that resolves customer and internally found defects, and includes the FIPS module. You can upgrade from ACS 4.1, ACS 4.1.2 or 4.1.3 to ACS 4.1.4.

This release includes the:

- ACS 4.1.4 software image
- Appliance upgrade CD for Solution Engines 1111, 1112, 1113



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

© 2007 Cisco Systems, Inc. All rights reserved.

New and Changed Information

New and changed information in release 4.1.4 includes:

- [Using ACS 4.1.4 in a FIPS 140-2-Compliant Mode](#), page 2
- [RADIUS Key Wrap Extended to All EAP Protocols](#), page 3
- [Temporary Elevated User Privileges](#), page 3
- [Object Identifier Check for EAP-TLS Authentication](#), page 3
- [Layer 2 Audit for Network Access Control](#), page 3
- [CSSupport Utility Added](#), page 4
- [UTF-8 Support](#), page 4
- [Add and Edit Devices Using the CSUtil Utility](#), page 4
- [Support for Microsoft Windows Server 2003 R2 with SP2](#), page 4

Using ACS 4.1.4 in a FIPS 140-2-Compliant Mode

This section describes how to use Cisco Secure ACS 4.1.4 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 4.1* 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 4.1.4 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

For ACS 4.1.4 patch releases, ACS FIPS module v 1.1 is available up to version 4.1.4.13.8. From patch 9 onwards, ACS 4.1.4 is 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 4.1.4 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.

Temporary Elevated User Privileges

In previous releases, ACS restricted administrator privilege. The ACS User Setup page now supports granting administrator privileges to another user for a defined number of days, hours, and minutes. The process automatically grants and revokes privileges according to the administrator's configuration. This option is available on the User Setup page in the web interface.

Object Identifier Check for EAP-TLS Authentication

The Authentication page in Network Access Profiles (NAPs) now includes an object identifier (OID) check. An administrator can enter the OID in the NAP policy configuration. ACS checks the OID against the Enhanced Key Usage (EKU) field in the user's certificate. ACS denies access if the OID and EKU do not match.



Note

To use this feature you must enable a protocol that uses client-side certificates within Network Access Profiles. See the *User Guide for Cisco Secure ACS 4.1* for information.

Layer 2 Audit for Network Access Control

ACS 4.1.4 adds support for the audit of agentless hosts connected to a Layer 2 (L2) Network Access Device (NAD). ACS first admits the device to a quarantined network, where the device can receive an IP address. The audit cannot begin until the device has received the IP address. When the audit begins, the audit is the same as an audit of a Layer 3 (L3) host. You can access this feature on the External Posture Validation Audit Setup page in the web interface.

The NAD must be preconfigured to learn the host's IP address. Then ACS responds to an initial access-request with a notification to the NAD to issue another access-request when the NAD has learned the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition, and policy flow follows the audit fail-open policy. Using the audit fail-open policy, administrators can choose to reject the user, or assign a posture token and an optional user-group.

Audit policy can serve as a backup verification when MAC Authentication Bypass (MAB) fails. The audit policy tests whether MAB failed by applying policy conditions that test the ACS user group assigned to the current session. For example, you can test whether the user-group is equal to the user-group that MAB assigns to failed authentications, and, if so, only then continue the audit.

For configuration information, see Chapter 14, Network Access Profiles, in the *User Guide for Cisco Secure Access Control Server*.

CSSupport Utility Added

ACS for Windows now includes the CSSupport utility. To access the utility, choose System Configuration > Support in the web interface. The utility includes the same options that are currently available on the Solution Engine. Similarly, CSSupport on ACS for Windows can collect a user-configurable set of options and generate a package.cab file. The information in the file is collected from the machine that is running the web interface.

The options include collection of:

- User database
- Logs for a configurable number of days
- Diagnostic logs

**Note**

If you choose diagnostic logs, the package.cab generation process restarts the ACS services. If you do not select diagnostic logs, ACS services do not restart.

UTF-8 Support

ACS now 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 (AD). The UTF-8 format can preserve the full US-ASCII range, providing compatibility with the existing ASCII handling software. See RFC 3629 for more information.

Add and Edit Devices Using the CSUtil Utility

ACS now supports use of the CSUtil Import.txt file for adding and editing authentication, authorization, and accounting (AAA) devices. You can edit all attributes of the AAA devices, including the:

- IP address
- Shared secret
- Vendor
- Network device group
- Single connection
- Keepalive settings

Support for Microsoft Windows Server 2003 R2 with SP2

ACS release 4.1.4 adds support for the Microsoft Windows Server 2003 R2 Service Pack (SP) 2.

Installation Notes

This section contains:

- [Installation Notes for ACS 4.1.4 for Windows, page 5](#)

- [Installation Notes for ACS 4.1.4 Solution Engine, page 5](#)

Installation Notes for ACS 4.1.4 for Windows

This section contains information on system requirements and upgrades.

System Requirements for ACS 4.1.4 for Windows

The system requirements for ACS 4.1.4 are the same as the system requirements for ACS 4.1. For information on supported operating systems and web browsers, see the *Installation Guide for Cisco Secure ACS for Windows 4.1*.



Note

ACS 4.1.4 adds support for Microsoft Windows Server 2003 R2 SP 2.

Upgrade Paths to ACS 4.1.4 for Windows

Cisco supports the upgrade paths of versions:

- 4.1 to 4.1.4
- 4.1.2 to 4.1.4
- 4.1.3 to 4.1.4



Note

If you are running ACS 4.1.2, you should upgrade directly from 4.1.2 to 4.1.4. The upgrade from 4.1.2 to 4.1.3 is not supported.

For more information on ACS 4.1 upgrades, see the *Installation Guide for Cisco Secure ACS for Windows 4.1*.

Installing ACS 4.1.4 for Windows

You must have ACS 4.1 installed before you install ACS 4.1.4. ACS 4.1.4 is available through the Cisco Technical Assistance Center (TAC) only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.4 are the same as for ACS 4.1. For information about installing ACS, refer to the *Installation Guide for Cisco Secure ACS 4.1 Windows*.

Installation Notes for ACS 4.1.4 Solution Engine

This section contains installation information for the ACS 4.1.4 Solution Engine (SE).

Upgrade Paths to the ACS 4.1.4 Solution Engine

Cisco supports the upgrade paths of versions:

- 4.1 to 4.1.4
- 4.1.2 to 4.1.4

- 4.1.3 to 4.1.4

**Note**

If you are running ACS 4.1.2, you should upgrade directly from 4.1.2 to 4.1.4. The upgrade from 4.1.2 to 4.1.3 is not supported.

For more information on ACS 4.1 upgrades, see the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

Installing the ACS Solution Engine 4.1.4

ACS 4.1 is pre-installed on the 1113 appliance. The ACS 4.1.4 Solution Engine upgrade package is available through the TAC only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.4 Solution Engine are the same as ACS 4.1. For information about installing ACS, refer to the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

Known Caveats

[Table 1](#) contains known caveats in ACS for Windows and Solution Engine 4.1.4. You can also use the Bug Toolkit to find open bugs.

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4

Bug ID	Summary	Explanation
CSCef61785	ACS Appliance fails to recognize an installed certificate.	<p>Symptom ACS appliance does not recognize the installed certificate.</p> <p>Conditions Cisco Security Agent is running.</p> <ol style="list-style-type: none"> 1. Install a certificate. The web interface will report the certificate as installed and validated. 2. Enable PEAP. 3. An error appears: Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is not installed. Install the CA certificate using ACS Certification Authority Setup page. <p>Workaround Disable the Cisco Security Agent and repeat the installation procedure. Re-enable the Cisco Security Agent.</p>
CSCef96208	ACS reports an incorrect privilege level.	<p>Symptom ACS may report users with an incorrect authorized privilege level. In particular, when using TACACS+, users who are correctly being authenticated with a privilege level of 15 are being reported with a level of 1.</p> <p>Workaround The error is cosmetic, and there is no workaround.</p>
CSCsa79327	Authentications fail for usernames that contain the Euro symbol (non-ASCII) in their passwords.	<p>Symptom Authentication fails for users that contain the Euro symbol (non-ASCII) in their passwords.</p> <p>Workaround Remove the Euro symbol (non-ASCII) from the user password.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsb74346	Authorization of a disabled user succeeded.	<p>Symptom Disabling a user account in the ACS Internal Database does not influence TACACS+ authorization requests related to the user. In other words, TACACS+ authorization requests succeed if they match user's TACACS+ settings, although the user's account is disabled. TACACS+ authentication requests fail for such users as expected.</p> <p>Workaround None.</p>
CSCsb95897	ACS cannot display a long list of disabled accounts correctly.	<p>Symptom The ACS web interface has problems in displaying disabled accounts lists if the lists contain several pages. The Next button is working, but the Previous button is available only once.</p> <p>Workaround None.</p>
CSCsc77154	Proxy authentications fail when no DHCP server is present at installation.	<p>Symptom When an ACS appliance is installed where the IP configuration is manual (for example, no DHCP server), subsequent proxy authentications may fail.</p> <p>The ACS Appliance will send the authentication packets to an incorrect proxy IP address, while the proxy configuration still presents the default appliance name of DELIVERANCE1.</p> <p>Workaround</p> <ol style="list-style-type: none"> 1. Verify that Distributed System Settings is checked under Interface Configuration > Advanced Options. 2. Remove DELIVERANCE1 from the Forward To list box in Network Configuration > Edit Default Proxy Distribution Entry. 3. Remove dummy server from Network Configuration > AAA Servers. 4. Reboot.
CSCsc90467	After install from Recovery CD, no CLI access is available.	<p>Symptom This problem occurs on the ACS SE 1111 (HP), when performing a full upgrade that includes the appliance base image. When installing from the ACS SE 1111 (HP) Recovery CD, installation completes, the ACS SE reboots, performs some configurations, and reboots again. The configurations that occur after the first reboot take a significant amount of time to load, during which there is no feedback, which is normal system behavior. After this time, the CLI Initial Configuration screen should appear, but does not.</p> <p>Conditions On ACS SE 1111 (HP), when installing from the Recovery CD, when performing a full upgrade, including the appliance base image. Note: If you are not upgrading the appliance base image, you do not need to install from the Recovery CD.</p> <p>Workaround Switch off the appliance, and switch it on again.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsd18172	After installing the appliance, the default windows IP remains in the AAA server.	<p>Symptom If the user does re-image from the ACS SE CD (quanta model 1112), they should <i>not</i> connect the device on the network during the installation. During installation, the configuration (such as hostname and IP) can contain incorrect information. After the reboot, use console port to reset the hostname and IP address.</p> <p>Workaround Do not connect to the network to avoid the duplicate entries problem.</p>
CSCsd42955	ACS SE requires reboot after a new User Defined Vendor (UDV) is added using RDBMS synchronization.	<p>Symptom RDBMS Synchronization succeeds, but you cannot see the added UDVs.</p> <p>Conditions On the ACS Appliance, use the RDBMS Sync feature to add new UDV.</p> <p>Workaround Physically reboot the appliance.</p>
CSCsd46457	ACS exhibits problems limiting authentications to 40, with 20 second load intervals.	<p>Symptom Internal architecture of ACS limit the number of authentication per second that ACS can handle.</p> <p>Conditions Tests done with Dual processor, XEON machines (HP DL38T G4s with two ACSs, two AD, two clients) show that ACS can not scale above 40 EAP authentications per second. If ACS is pushed harder, authentications will go up, and after 120 seconds will drop to approximately 10 per second. Testing used the stress employer.</p> <p>Workaround None.</p>
CSCsd88833	Manual setup of IP configuration failed, CLI improvement needed.	<p>Symptom An ACS Appliance may not operate correctly after installation if there were problems with or changes to the IP addressing.</p> <p>Conditions In particular, no DHCP server is found, or the DHCP server is configured incorrectly, or the installation occurs with the NIC disconnected.</p> <p>Workaround The only workaround may be to install the Appliance again, with the Ethernet0 NIC attached, and with a valid DHCP setting or (if there is no DHCP server) the correct IP address configured.</p>
CSCse26754	ACS/ACSE administration may do limited session validation.	<p>Symptom The attacks described in the report take advantage of a weakness in the default configuration of the Cisco ACS. Cisco is investigating this issue and further detail 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 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCse69819	For custom UDV, replication does not replicate. Failure to create on secondary.	<p>Symptom When trying to create a custom UDV on a secondary ACS server, you get the message: VSA attribute [UDV-Vendor-Attribute] already defined by VSA vendor [UDV-Vendor]. Must be unique</p> <p>Conditions UDV was defined on the primary, and replication took place before the UDV was defined on the secondary.</p> <p>Workaround Uninstall and reinstall ACS on the secondary add the UDV to the secondary and then start replication to the secondary.</p>
CSCsf11087	Cisco:PA: Attributes do not show in the Passed Authentications report for Linux clients.	<p>Symptom Cisco:PA attributes are not showing up in the Passed Authentication Report for a Linux client with CTA 2.1.0.10 installed. The attributes are showing up in the auth.log file and are showing up for a Win XP client on the same network.</p> <p>Workaround In System Configuration > Logging > Passed Authentication, select Cisco:PA attributes click on Submit, which performs authentication using the Linux client with CTA 2.1.0.10 4. Then check the passed authentication log on Reports and Activity page.</p>
CSCsf15057	Cannot ping the ACS appliance if the CSA agent is turned on.	<p>Symptom The ACS SE appliance cannot be pinged from network devices.</p> <p>Conditions By default, the CSA is turned on, which in turn prevents the ACS SE appliance from responding to ping requests from other network devices.</p> <p>Workaround The only way to have the ACS SE appliance reply to pings is to disable the CSA. Given the security implications of doing so, this practice is not recommended.</p>
CSCsf17112	SSL Handshake error message too general.	—
CSCsf29684	CSLog should include a port number on all relevant entries.	<p>Symptom The CSLog component does not always include the port number used to communicate with the remote agent.</p> <p>Conditions Observed on ACS 3.3.3(11) and 4.01(27). Other versions may be affected as well.</p> <p>Workaround None.</p>
CSCsg14788	Active Directory machine authentication may fail.	<p>Symptom Active directory machine authentication may fail if AD tried to locate a machine in the child domain which is not a true physical child domain of the top level domain.</p> <p>Conditions Active Directory machine authentication may fail if Active Directory when trying to authenticate/locate a machine in a child domain which is not a true physical child domain of the top level domain, that is, it is a naming context of the parent domain.</p> <p>Workaround None.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsg24486	Two TACACS new services with similar names have issues with data.	<p>Symptom In Interface Configuration > TACACS (Cisco IOS), create two new services with similar names. Entering data in one service and saving the change will copy the same data 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 You use LDAP as an external user database and attempt to edit the ACS group to LDAP group mapping. For example, when you click Add Group, the web interface will respond with “LDAP disconnected”.</p> <p>Conditions Your LDAP group list query response is larger than 50000 results.</p> <p>Workaround Keep the number of groups under control.</p>
CSCsg40727	ACS 4.0: RDBMS fails account action 220 250 with Synchronization Partners.	<p>Symptom A Network Device Group (NDG) is not getting added to Synchronization Partners, but an additional (duplicated) entry is getting added to primary, then the AAA-Client cannot be deleted.</p> <p>Workaround None.</p>
CSCsg71976	Invalid LDAP/SSL authentications with referrals hang ACS.	<p>Symptom Using ACS with LDAP/SSL configured as an external user database, after one failed login attempt due to an invalid username or password, ACS will then fail all subsequent login attempts, valid or not. A reboot is required to get authentications working again, but then the next invalid username or password will again fail all further authentication attempts.</p> <p>Conditions LDAP is the external user database, with the Use Secure Authentication checkbox checked to enable LDAP/SSL. The LDAP server must respond with referrals to other servers.</p> <p>Workaround Unencrypted LDAP works. If LDAP/SSL must be used, configure the LDAP database to not reply with referrals. A reboot will get the authentications working again, until the next invalid username or password is issued.</p>
CSCsh71482	Unable to get a wireless client authenticated with EAP-TLS and Keywrap.	<p>Symptom EAP-TLS authentication getting failed when Keywrap was configured on the ACS server.</p> <p>Conditions The KEK were 16 bytes in length and MACK 20 bytes length, configured in ASCII.</p> <p>Workaround Keywrap should be configured with same wireless LAN controller.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsh77461	Assigned IP field is not populated in the Logged-In Users report.	<p>Symptom The assigned IP field is not populated after receiving access-request and an accounting-start.</p> <p>Conditions The IP field does not get populated after receiving access-request and accounting-start.</p> <p>Workaround None.</p>
CSCsh78523	The Logged-In User entry disappears before the user has logged off.	<p>Symptom Logged-In users disappear from Logged-In Users report.</p> <p>Conditions The symptom occurs when authenticating users using "dot1x re-authentication".</p> <p>Workaround None.</p>
CSCsh81281	No error message when the accountactions.csv file is missing the required values.	<p>Symptom When required values for the accountactions table are missing, ACS displays a generic error ("Sync complete with no transactions performed") in ACS 4.x or no error message on ACS 3.x. The ACS appliance under 3.x will proceed to download and rename a .csv file as usual and will not log any error message.</p> <p>Conditions The ACS RDBMS import utility is being used.</p> <p>Workaround Check and double check your data against the standards defined in the documentation in the User Guide for the Cisco Secure Access Control Server Solution Engine version 3.3.</p>
CSCsh89581	ACS Admin can become unresponsive under heavy load.	<p>Symptom The ACS Administration web interface becomes unresponsive after a period of time, requiring the service to be restarted in order to allow administration of the ACS. This does not affect user authentication to the ACS itself, which appears to continue.</p> <p>Conditions Seen in an environment in which LMS 2.6 is authenticating to an ACS appliance on 4.0.1.44 code. A patch was applied to the LMS server to insure sessions created by auto-refresh are also logged out, but issues with the CSAdmin service stopping continue. When the issue occurs, the CSAdmin logs appear not to be sending any further information until restart of the services. There is a high probability that the issue is related to load. In the environment in which the issue was seen, over 6000 administrative connections were made to CSAdmin (and logged out again) within 5 minutes by the LMS servers.</p> <p>Workaround Restarting the ACS (for an ACS Solution Engine) or restarting the CSAdmin process (for ACS installed on Windows) allows access back into the ACS web interface for administration.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsi39730	ACS Solution Engine 4.1 Recovery CD installation, wrong device name and IP address.	<p>Symptom Two local AAA client entries are created when running the ACS 4.1 recovery CD (1111, 1112 and 1113) without upgrade.</p> <p>Conditions Standard configuration.</p> <p>Workaround Requires the deletion of the AAA client correctly named for the system.</p>
CSCsi55085	ACS services not started after replication and reboot on a machine that contains dual CPUs.	<p>Symptom ACS services are not started when rebooting Secondary ACS machine within 30 minutes after the database replication.</p> <p>Conditions After the database replication between the primary ACS and the secondary ACS machines with dual processors, this issue is only seen when rebooting the secondary ACS machine within 30 minutes.</p> <p>Workaround Do not reboot the secondary ACS within 30 minutes after the database replication.</p>
CSCsi82393	CiscoAAA Event ID 5 error in Windows Event Viewer\Applcaition log.	<p>Symptom Event ID (5) in source (CiscoAAA) error generated in Microsoft Windows Application Event log on the primary ACS every time when ACS is replicating its database.</p> <p>Conditions Primary/secondary ACSs for Windows configured for database replication.</p> <p>Workaround None.</p>
CSCsi99414	ACS stops logging after upgrade from 3.3.3 to 4.1.23.	<p>Symptom CSLog fails to log CSV reports.</p> <p>Conditions Upgrade ACS from 3.3.3 to 4.1.1.23.</p> <p>Workaround In the web interface, choose System Configuration > Logging, and choose the appropriate Report Name. Move the Unknown attribute in the Logged Attribute list from right to left. Click Submit, and then restart the CSLog service.</p>
CSCsj18497	ACS Appliance documentation does not list supported SNMP MIBs.	<p>Cisco Secure ACS provides Simple Network Management Protocol (SNMP) support for the appliance only. The SNMP agent provides read-only SNMP v1 and SNMP v2c support. The supported MIBs include:</p> <ul style="list-style-type: none"> • Structure and Identification of Management Information for TCP/IP-based Internets (1155). • SNMP (1157). • Management Information Base for Network Management of TCP/IP-based internets: MIB-II (1213). • MIB-II and LAN Manager MIB-II for Windows. • Host Resources MIB (RFC 1514/2790). <p>The SNMP agent is configurable on the appliance configuration page.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsj32256	Permit/Denied for others TACACS+ Network Access Service (NAS) is inverse in Network Access Restrictions (NARs).	<p>Symptom When configuring a NAR, the NAR results are opposite to the configuration for the default TACACS+ NAS. If the default TACACS+ NAS is used as a permitted point of calling access will be filtered. If the default TACACS+ NAS is used as a denied point of calling, access will be permitted.</p> <p>Conditions Use of the “others” default TACACS+ NAS with any kind of NAR.</p> <p>Workaround Configure the NAS using a wildcard range or individually and configure NARs accordingly.</p>
CSCsj36562	Replication fails under condition of stress between WAN geographies.	<p>Symptom Replication fails under condition of stress between WAN geographies.</p> <p>Workaround None.</p>
CSCsj54389	Group mapping fails for domain local users.	<p>Symptom Dynamic group mapping with Active Directory does not work well for windows domain local group.</p> <p>Conditions ACS: 3.3.4, 4.0.1 or above Active Directory: Mixed mode User: belonging to domain local group.</p> <p>Workaround Use Native mode on Active Directory.</p>
CSCsj58199	CSAuth crashes, exception trapped on UDB_SEND_RESPONSE.	<p>Symptom Under load ACS 4.1.x may experience CSAuth Exception crashes when authenticating to SecureID and mediating extended authentications.</p> <p>Conditions The SecureID.dll is returning an invalid code to ACS. The load issue might apply to the ACS or the backend SecureID.</p> <p>Workaround CSAuth crash is caught and the module restarts automatically. Service interruption is very short.</p>
CSCsj60407	The ACS backup filename is changed to uppercase letters.	<p>Symptom The FTP filename created for backups should also contain the hostname of the appliance. The part of the hostname with the filename randomly changed 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>
CSCsj70952	ASA 8.0: ACS 3076/11 attribute needs new enumeration for svc protocol.	<p>Symptom ASA 8.0: ACS 3076/11 attribute needs new enumeration for svc protocol.</p> <p>Workaround Update to the VPN3000/PIX/ASA7.x+ ACS attribute [3076/11] Tunneling-Protocols for new enumerations to include the svc protocol for ASA 8.0.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsj71204	Need to post ACS 4.1.x and 4.0.x patches for ASA 8.0 attribute deltas.	<p>Symptom Need to post ACS 4.1.x and 4.0.x patches for ASA 8.0 attribute deltas.</p> <p>Workaround None.</p>
CSCsj86746	Unable to add attributes for logging.	<p>Symptom Unable to configure logging for newly added attribute. In the system configuration logging, see a new attribute added named unknown. When moving it to the right 'selected' and submitted, the CSLog service stops.</p> <p>Conditions Import the .ini file using CSUtil -addavp, to add external vendor AVPs.</p> <p>Workaround Roll back to ACS 4.0 or earlier.</p>
CSCsj87434	ACS does not bind the ACS group and domain after configuration replication.	<p>Symptom AAA client is not authenticated as correct Group mapped NT groups which config is replicated from the other ACS.</p> <p>Conditions ACS group is mapping for domain -Config replication is successful.</p> <p>Workaround Restart ACS services (CSAuth service).</p>
CSCsk02790	UCP fails to install correctly on Windows 2000.	<p>Symptom UCP reports problems contacting the ACS server during the installation process. Inspection of the Windows registry reveals that none of the required keys have been generated.</p> <p>Conditions Observed while installing UCP 4.1 on Windows 2000 systems. UCP 4.1 correctly installs on Windows 2003 systems.</p> <p>Workaround Install UCP on a Windows 2003 system.</p>
CSCsk08299	ACS 4.0.1.27 using TACACS gets authentication/authorization delay.	<p>Symptom ACS 4.0.1.27 with TACACS+ intermittently gets an authentication and authorization sequence delay of about 8 seconds, which makes ACS less productive.</p> <p>Conditions ACS 4.0.1.27.</p> <p>Workaround None.</p>
CSCsk08313	ACS Group Mapping fails with Foreign Domains.	<p>Symptom Group mapping between a Foreign Domain group and the ACS Default group, but users are being mapped to Group ID -1, which is the No Access Group. Changing the All Other Combinations from No Access To Default Group maps the Foreign Domain users to the Default group.</p> <p>Conditions ACS 4.1.3 and a Foreign Domain or a Domain that is not the same as the machine on which ACS is installed.</p> <p>Workaround None.</p>

Table 1 Known Caveats in ACS Windows and Solution Engine 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCso78089	Rollback of csupdate patch is not functional	<p>Symptom CSUpdate patch cannot be rolled back.</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. Re-image the appliance with ACS 4.1.4.13. 2. Upgrade the appliance and install patch 7 or 8. 3. Check the Appliance Upgrade Status page for the applied patches. 4. In the CLI, enter <code>rollback+caupdate</code> patch. 5. The Failed to roll back ACS-4.1.4.13.8-CSUpdate error appears. <p>Workaround None.</p>
CSCso78098	Additional restart required for NAP attribute to reflect in Syslog	<p>Symptom NAP attribute is missing in Syslog for Radius Accounting for Patch 7 & 8.</p> <p>Workaround Restart the CSAdmin service in the CLI.</p>

Resolved Caveats

Table 2 contains the resolved caveats for ACS 4.1.4. Check the Bug Toolkit on Cisco.com for any resolved caveats that might not appear here.

Table 2 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 message, not error message.
CSCei01730	EAP-TLS authentication to the trusted DC does not succeed.
CSCsa95381	ACS requires Domain Administrator privileges for Win 2003 authentication.
CSCsf22420	ACS 3.3(3) CSR sent to TrustWise returns an error 0x3110.
CSCsf25881	Does not clear the certificate trust list when a new certificate is installed.
CSCsg00942	UCP does not support special characters.
CSCsg12989	Cannot enable CRL checking unless certificate is checked in CTL.
CSCsg14022	PPTP clients authenticating 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 previous set.

Table 2 *Resolved Caveats in ACS Windows and Solution Engine 4.1.4 (continued)*

Bug ID	Description
CSCsg89042	Appliance upgrade using the web interface 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 does not work for Group level.
CSCsh62641	MAC authentication causes internal errors.
CSCsh77806	EAP-TLS will fail authentication if name contains forward slash (/).
CSCsh88934	Issue in authentication when Ciscoworks is not added as AAA client.
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 maximum 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 attribute 81 is truncated.
CSCsi65427	ACS SE: Hostname greater than 15 characters locks out web interface and CLI.
CSCsi68322	ACS Release 3.3(4) Build 12 cannot sort distribution entries in the proxy.
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.
CSCsj12509	NTlib should use IDirectorySearch handle in thread-safe manner.
CSCsj42058	JRE version in install guide needs update.
CSCsj42080	Misleading information about supported Microsoft security patches.
CSCsj84279	ACS 4.1.3 Accounting Proxy does not work properly.

Documentation Updates

This section provides documentation updates.

Changes

This section provides changes to the ACS user documentation.

Domain Privileges for Windows 2003 Authentication

ACS requires Domain Administrator privileges for the service account when authenticating against Windows 2003. Explanations now appear in the:

- *Installation Guide for Cisco Secure ACS for Windows 4.0*
- *Installation Guide for Cisco Secure ACS for Windows 4.1*

Supported ODBC Data Sources

In the *User Guide for Cisco Secure ACS 4.1*, Appendix F, “RDBMS Synchronization Import Definitions”, in the section “Supported Versions for ODBC Data Sources (ACS for Windows)”, the opening statement needs to be revised.

ACS supports any database that has been tested with ACS, and any database that is compliant with ODBC. The current information appears to restrict support to only certain versions of ODBC and MS-SQL.

Java Runtime Environment (JRE) Version

In Table 1-2, ACS for Windows Web Client Requirements, in the *Installation Guide for Cisco Secure ACS for Windows 4.1*, the minimum requirement for the JRE needs to change to the current minimum requirement, which is Sun JRE 1.5.x.

Update for LD_LIBRARY_PATH Environment Variable

In the section “Environment Variable Settings”, in *Installing Cisco Secure ACS Remote Agent for Solaris*, the information on libstdc++.so is obsolete since Release 4.1.3. You no longer need to place libstdc++.so in the LD_LIBRARY_PATH environment variable.

Omissions

This section provides information that was omitted from the ACS user documentation.

Password Aging

In the *User Guide for Cisco Secure ACS 3.1*, in the section “Enabling Password Aging for the CiscoSecure User Database”, the sequence of steps for changing a password for now includes further supplemental information.

To change your password for IOS:

-
- Step 1** Open a Telnet window to the router that is running IOS.
 - Step 2** Enter your user name.

Step 3 When prompted, enter the old password and then enter the new password.

DBSync Process Keeps Restarting

ACS Troubleshooting needs to include a workaround for this problem.

Condition

When the CSAdmin service is started with a different Windows user than the CSDBSync service, the CSDBSync service keeps restarting and floods the log with the message “CSDbSync 08/31/2006 16:58:34 E 0000 5408 WaitForMultipleObjects returned [-1], error [6]”.

Action

Run the CSAdmin and CSDBSync services as the same user.

For ACS Replication, Server Information Must Match

In the *User Guide for Cisco Secure ACS 4.1*, in the section “Replication Options”, the information needs to include a note about matching server configurations. You must set the sending and receiving servers to replicate the Network Access Profile (NAP) information.

Because the network configuration and NAP configuration can overlap, both servers should be set to replicate only NAP information. For example, if the receiving server is set to receive both network configuration and NAP information, but the sending server is set to send only NAP information, then ACS replication will fail.

Logging Configuration Update Restarts CSLog

The “Logging and Reports” chapter in the *User Guide for Cisco Secure ACS 4.1* needs additional information about logging configuration updates. When ACS updates the logging configuration, the CSLog process restarts.

Support for Microsoft Windows Server Security Patches

In the *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Release 4.1*, in the section “Tested Windows Security Patches”, the initial note needs additional information. Patches that Microsoft released after the release of ACS 4.1 may not be supported. For information on recent patches, contact the TAC.

Product Documentation

[Table 3](#) lists the product documentation that is associated with ACS 4.1.4.

Table 3 **Product Documentation**

Document Title	Description
<i>Documentation Guide for Cisco Secure ACS 4.1</i>	<p>Describes product documentation:</p> <ul style="list-style-type: none"> • Printed document with the product. • PDF on the product CD-ROM. <p>Available on Cisco.com:</p> <ul style="list-style-type: none"> • Windows—http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_documentation_roadmaps_list.html • Solution Engine—http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_documentation_roadmaps_list.html
<i>Release Notes for Cisco Secure ACS 4.1</i>	<p>ACS 4.1 features, documentation updates, and resolved problems. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p>
<i>Release Notes for Cisco Secure ACS 4.1.2</i> <i>Release Notes for Cisco Secure ACS 4.1.3</i> <i>Release Notes for Cisco Secure ACS 4.1.4</i>	<p>New features, documentation updates, and resolved problems since ACS 4.1. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p>
Product online help	<p>Help topics for all pages in the ACS web interface. Select an option from the ACS menu; the help appears in the right pane.</p>
<i>User Guide for Cisco Secure ACS 4.1</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. <p>Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_list.html</p>
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.1</i>	<p>Supported devices and firmware versions for all ACS features. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html</p>
<i>Installation and User Guide for User Changeable Passwords 4.1</i>	<p>Installation and user guide for the user-changeable password add-on. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html</p>
<i>Configuration Guide for Cisco Secure ACS 4.1.</i>	<p>Provides provide step-by-step instructions on how to configure and deploy ACS. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html</p>

Table 3 *Product Documentation (continued)*

Document Title	Description
<i>Installation Guide for Cisco Secure ACS 4.1 Windows</i>	Details on installation and upgrade of ACS software and post-installation tasks. Available as PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.1</i>	Details on ACS SE 1112 and ACS SE 1113 hardware and hardware installation, and initial software configuration. Available as PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.1</i>	Translated safety warnings and compliance information. Available in the following formats: <ul style="list-style-type: none"> • Printed document with the product. • PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents</i>	Installation and configuration guide for ACS remote agents for remote logging. Available as PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.

