



Release Notes for Cisco Secure ACS 4.1.4

Revised: April 17, 2008, OL-14207-02

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.

Contents

- [Introduction, page 1](#)
- [New and Changed Information, page 2](#)
- [Installation Notes, page 5](#)
- [Known Caveats, page 6](#)
- [Resolved Caveats, page 20](#)
- [Documentation Updates, page 25](#)
- [Product Documentation, page 33](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 35](#)

Introduction

ACS 4.1.4 is a maintenance release for ACS 4.1 that resolves customer and internally found defects. 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:

- [Temporary Elevated User Privileges, page 2](#)
- [Object Identifier Check for EAP-TLS Authentication, page 2](#)
- [Layer 2 Audit for Network Access Control, page 2](#)
- [CSSupport Utility Added, page 3](#)
- [UTF-8 Support, page 3](#)
- [Add and Edit Devices Using the CSUtil Utility, page 3](#)
- [Support for Microsoft Windows, page 4](#)
- [Japanese Operating System Support, page 4](#)
- [Multiprocessor Support, page 4](#)
- [VMware ESX Server Support, page 4](#)

Temporary Elevated User Privileges

In previous releases, ACS restricted administrator privilege. The ACS User Setup page now supports the granting of 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 ECU 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

ACS 4.1.4.13 supports the following versions of Microsoft Windows and Microsoft Windows Server:

- Microsoft Windows 2003 (Service Pack 2).
- Microsoft Windows Server:
 - Microsoft Windows 2000 Server (English version only).
 - Microsoft Windows 2000 Advanced Server (Service Pack 4) without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed (English version only).
 - Microsoft Windows Server 2003, Enterprise Edition or Standard Edition (Service Pack 1).
 - Microsoft Windows Server 2003 R2 (Service Pack 2), which is new support in this release.

Japanese Operating System Support

ACS 4.1.4.13 supports the following versions of Japanese Windows 2003 Server:

- Japanese Windows 2003 Server, Service Pack 1.
- Japanese Windows 2003 Server, Service Pack 2, Enterprise Edition (or higher).
- Japanese Windows 2003 Server, Service Pack 2, R2, Enterprise Edition (or higher).
- Japanese Windows 2003 Server, Service Pack 2, Standard Edition (or higher).
- Japanese Windows 2003 Server, Service Pack 2, R2, Standard Edition (or higher).

Multiprocessor Support

ACS 4.1.4.13 adds multiprocessor support.

VMware ESX Server Support

ACS 4.1.4 has been tested on the VMware ESX server with the following configuration:

- VMWare ESX Server 3.0.0
- 16 GB of RAM
- AMD Opteron Dual Core processor
- 300 GB hard drive
- Four virtual machines
- Windows 2003 Standard Edition
- 3 GB of RAM for the guest operating system

The following versions of VMware ESX are supported:

- ESX 3.0.x (tested)
- ESX 3.5.x (not tested)
- ESX 3.5i (not tested)

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 with 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
CSCeb16956	Domain stripping fails if the username attribute is sent twice in RADIUS.	<p>Symptom If username attribute is present twice (with same username) in a radius request going to ACS windows 3.1, then domain stripping of username found in the attribute will not occur.</p> <p>Workaround Fix the NAS to send the username attribute only once as the second one is redundant.</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>

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

Bug ID	Summary	Explanation
CSCsb70717	Change Dr. Watson's log directory for CSSupport.	<p>Symptom drwtsn32.log not getting added to Package.cab.</p> <p>Conditions When C:\WINNT is not present drwtsn32.log will not get added to package.cab.</p> <p>Workaround Create C:\WINNT if not present in C: drive.</p>
CSCsb74346	Authorization of disabled user succeeds.	<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 correctly display a long list of disabled accounts.	<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>

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

Bug ID	Summary	Explanation
CSCsc81075	A Shell Command Authorization Set added to the Group using ODBC is not sorted.	<p>Symptom Shell Command Authorization Set (SCAS) for Group is not sorted when added via ODBC</p> <p>Conditions Add a pre-existing SCAS to a pre-existing group via ODBC interface.</p> <p>Example: SequenceId, Priority, UserName, GroupName, Action, ValueName, Value1, Value2, Value3, DateTime, MessageNo, ComputerNames, AppId, Status 1, 0, , GroupName, 271, shell, NDGTest-1, "AllAccess", , , , , 0 2, 0, , GroupName, 271, shell, NDGTest-2, "AllAccess", , , , , 0 3, 0, , GroupName, 271, shell, NDGTest-3, "AllAccess", , , , , 0 4, 0, , GroupName, 271, shell, NDGTest-4, "AllAccess", , , , , 0 5, 0, , GroupName, 271, shell, NDGTest-5, "AllAccess", , , , , 0 6, 0, , GroupName, 271, shell, NDGTest-6, "AllAccess", , , , , 0 7, 0, , GroupName, 271, shell, NDGTest-7, "AllAccess", , , , , 0 8, 0, , GroupName, 271, shell, NDGTest-8, "AllAccess", , , , , 0 9, 0, , GroupName, 271, shell, NDGTest-9, "AllAccess", , , , , 0 10, 0, , GroupName, 271, shell, NDGTest-10, "AllAccess", , , , , 0 Output to Group in UI will appear as: NDGTest9 AllAccess NDGTest7 AllAccess NDGTest5 AllAccess NDGTest3 AllAccess NDGTest1 AllAccess NDGTest2 AllAccess NDGTest4 AllAccess NDGTest6 AllAccess NDGTest8 AllAccess NDGTest10 AllAccess This is a cosmetic sorting issue; the SCAS still work as expected.</p> <p>Workaround Manually add SCAS via UI.</p>
CSCsc93204	E-mail notifications are not sent when CSAuth restarts.	<p>Symptom Email notifications are sent when the CSAuth process is stopped or suspended during various events. However, there is no notice sent when CSAuth is restarted or resumed, necessitating the system administrator to manually check for CSAuth status.</p> <p>Conditions Email notifications are configured. This was observed on ACS 3.3.3(11).</p> <p>Workaround None.</p>

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

Bug ID	Summary	Explanation
CSCsd01768	Appliance CLI reports Appliance upgrade in progress after an upgrade has finished.	<p>Symptom Appliance shows upgrade in progress, after it has finished:</p> <pre>CSAdmin running CSAuth running CSDBSync running CSLog running CSMon running CSRADIUS running CSTacacs running CSAgent running Appliance upgrade in progress..</pre> <p>Conditions Upgrade using the CLI.</p> <p>Workaround Go to appliance upgrade page, and click submit, this would clear the upgrade flag.</p>
CSCse23653	The first three characters of LDAP groups are missing.	<p>Symptom All LDAP groups in any list boxes are displayed without the first three characters of the name. LDAP groups are ordered by the fourth and following characters.</p> <p>Conditions The problem occurs anywhere the LDAP group is displayed.</p> <p>Workaround The following steps might fix the problem:</p> <ol style="list-style-type: none"> 1) Verify the "GroupObjectType" contains the correct value as defined on the LDAP server. 2) Remove any leading and trailing spaces in the "GroupObjectType" configuration field.
CSCse26754	ACS/ACSE Administration can implement 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
CSCsf11087	Cisco:PA: attributes are not showing in the Passed Auth report for the Linux client.	<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>
CSCsf13603	Cisco-PEAP authentication against an RSA API server fails with an error message.	<p>Symptom Cisco-PEAP authentication against RSA API server provide and using FUNK as supplicant</p> <p>Conditions Working with RSA API as the external DB, and trying to Auth using funk, fails with an error message</p> <p>Workaround None.</p>
CSCsf13615	Authentication with RSA using expired password is not logged.	<p>Symptom Working with RSA as the external DB, login with user with old password - nothing is recorded.</p> <p>Conditions The Supplicant is using CISCO - PEAP authentication.</p> <p>Workaround None.</p>
CSCsf25057	ACS does not support TACACS single-connection.	<p>Symptom ACS does not support the TACACS single-connect flag.</p> <p>Workaround None.</p>
CSCsf27581	RAC, User Group Any problem.	<p>Symptom When the you select the User Group "ANY" in the authorization section of the NAP, and you tell it to use a particular RAC, it does not work.</p> <p>Workaround User must be prevented from configuring this rule in the UI.</p>

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

Bug ID	Summary	Explanation
CSCsg07008	Incorrect error code is sent when the certificate has expired.	<p>Symptom When ACS is configured for CRL checking and the CRL has expired but the certificate is fine, ACS will send back to the supplicant a TLS error code with a value of 45 (certificate_expired).</p> <p>Conditions ACS should be sending a certificate_unknown (46) error code.</p> <p>Workaround None.</p>
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>
CSCsg61729	ACS fails to find an issuer's certificate for a CRL list uploaded from a CDP.	<p>Symptom In multi-tier certificate structures, ACS will sometimes take the CRL pointer from the root certificate, even if the CRL URL is configured to point to a different system.</p> <p>Conditions This has been observed on ACS 3.3.3(11) and 4.0.1(27). Other versions may be affected as well.</p> <p>Workaround None.</p>

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

Bug ID	Summary	Explanation
CSCsg71976	Invalid LDAP/SSL authentications with referrals hangs 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>
CSCsh78523	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 reauthentication".</p> <p>Workaround None.</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
CSCsi05349	Columns of the failed attempts log are shifted and incorrect.	<p>Symptom Columns of failed attempts log are shifted/incorrect The authentication failure code show up under "Network Access Profile Name" in the failed attempts log.</p> <p>Workaround None.</p>
CSCsi50359	Enable authentications from CatOS are rejected with an <code>Internal Error</code> message.	<p>Symptom Users on CatOS switches are denied enable authentication, even though they're entering the correct password. Login authentications work correctly.</p> <p>Conditions This has been observed on ACS 4.1.1(23). Other versions may be affected as well. The problem occurs when the users have "TACACS Enable Control" set to "Use Group Level Setting".</p> <p>Workaround Configure the user to have a max privilege level setting under "Max Privilege for any AAA Client".</p>
CSCsi55085	ACS services do not start after replicate and reboot on a machine with 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>

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

Bug ID	Summary	Explanation
CSCsi62622	The system replication partners table is empty.	<p>Symptom ACS replication Master GUI is not visually populating the partner replication table with the slave hostname/IP address.</p> <p>Conditions Upon adding the host from the 'AAA server' left column to the 'replication' right column, then hitting submit, and subsequently returning to replication screen, the master ACS GUI does not visually save/keep-populated replication partner table -The replication data is successfully replicated to Slave, and cascaded to any subsequent slaves -Initial prognosis show this to be a cosmetic issue. DE does not see the issue rectified in v4.1.1b23 patch 4.</p> <p>Workaround 1. Add hostname, that is, Flprdasaaa01, to replication partner table (right pane), hit 'submit' or 'replicate now'. 2. Upon return to replication table page, the right pane window might be empty. Add a second hostname, that is, Flprdasaaa02, hit submit 3. Upon next return to replication table page, hostname Flprdasaaa02, might/should be visible via GUI, 4. At this point, one should be able Add/Remove hostnames to the replication table pane accordingly.</p>
CSCsi63656	Unknown Radius Token Server message after replication.	<p>Symptom After replication users show up with a Database of 'Unknown Radius Token Server'.</p> <p>Conditions Occurs when multiple Radius Token Servers were created on the primary but only one was created on the secondary.</p> <p>Workaround There are two known workarounds for this problem. 1. Delete all Radius token servers from both ACS's. The re-create the Radius token server on each ACS. Note: This will require you to re associate all users with this token server. 2. Produce a package.cab from the primary ACS. Extract the files and edit the ACS.reg. In that file find the following section: [CiscoACS\Authenticators\Libraries\30] Under that you will have another section that has the same information but includes another two numbers after the 30. That will be the number of the slot that server is in. It starts with slot 00 being the first server in the list. If that number is 02 then it is in slot 3. So on the secondary ACS delete all radius token servers, then create two dummy radius token servers then the actual token server. After you create all of them you can delete the first two. Now your secondary server will have the radius token server in slot 02 also and your users will show up correctly.</p>

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

Bug ID	Summary	Explanation
CSCsi82393	CiscoAAA Event ID 5 error in the Windows Event Viewer Application 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>
CSCsi90613	Error messages in the event log regarding the perfmon and ACS.	<p>Symptom ACS 4.1.1.23 installed on Windows 2003 leaves consistent error messages in the Event Log of the host OS.</p> <p>Conditions The following error messages are seen in event logs: App: E 'Thu May 03 06:58:25 2007': LoadPerf - " Installing the performance counter strings for service WmiApRpl (WmiApRpl) failed. The Error code is the first DWORD in Data section. " App: E 'Thu May 03 06:58:25 2007': LoadPerf - " Unable to update the performance counter strings of the 009 language ID. The Win32 status returned by the call is the first DWORD in Data section. " App: E 'Thu May 03 06:58:22 2007': LoadPerf - " Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The Error code is the first DWORD in Data section. " App: E 'Thu May 03 06:58:22 2007': LoadPerf - " Unable to update the performance counter strings of the 009 language ID. The Win32 status returned by the call is the first DWORD in Data section. "</p> <p>Workaround This does not hamper the functionality of ACS, so no work around needed.</p>
CSCsj03348	Pattern matching in shell command authorization sets.	<p>Symptom Command authorization for commands without arguments fails.</p> <p>Conditions The permit statement is specified as "permit ^\$" This has been observed on ACS 4.1.1, other versions may be affected as well.</p> <p>Workaround Specify the permit statement as "permit <cr>".</p>
CSCsj12604	When trying to bulk import, the ODBC operation fails.	<p>Symptom We receive the following error messages failed to add/update NAS [4].</p> <p>Conditions When trying to bulk import ODBC using csutil, Operation failed.</p> <p>Workaround Bring up the ODBC connection for the Sybase Adaptive Server Anywhere.</p>

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

Bug ID	Summary	Explanation
CSCsj14508	Some special characters in the FTP password are not accepted.	<p>Symptom Backups attempts fail with the FTP server reporting an incorrect password.</p> <p>Conditions This has been observed when the password contains @ characters on ACS 4.1.3. Other versions may be affected as well.</p> <p>Workaround Use a password without @ characters.</p>
CSCsj27387	Aire-WLAN-ID attribute should be changed back to IN OUT.	<p>Symptom Aire-WLAN-ID variable not available for return.</p> <p>Workaround Use NAR to limit access to WLAN by profile names / groups.</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>
CSCsk06231	Renaming a NDG with the same name while changing case can cause devices to disappear.	<p>Symptom If you rename a Network Device Group (NDG) to the same name but different case, for example ABCDE to abcde then the group and all of the devices within appear 'lost' in Network Configuration page. If you do a device search they show up in the search with the old upper-case NDG name. However, when you click to view the device the NDG appears to be the previous NDG in the list shown under Network Configuration.</p> <p>Conditions Rename a Network Device Group (NDG) to the same name but use a different case, for example ABCDE to abcde.</p> <p>Workaround None.</p>

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

Bug ID	Summary	Explanation
CSCsk25159	On ACS Upgrade, ACS returns a Dictionary Corruption CiscoACS\Dictionaries\005 error.	<p>Symptom Service do not start after upgrade to 4.1.1.23 or 4.1.1.24 from 4.0.1.27. Error in the RDS.log shows: RDS 28/08/2007 09:29:33 P 0202 0700 Dictionary Config Error: Ignoring unrecognised 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 Running ACS 4.0.1.27 and upgrading to 4.1.1.23 or 4.1.1.24. This happens in rare cases.</p> <p>Workaround Call TAC and snd in your database backup, the dictionary can be repaired.</p>
CSCsk27193	Cannot use <cr> while entering multiple MAC addresses.	<p>Symptom Pressing "return" after each MAC address yields error messages when clicking on the "Submit" button while defining authentication configuration for Network Access Profiles Access Policies.</p> <p>Conditions This has been observed on ACS 4.1.1(23) using Internet Explorer 6.0 and JRE 1.5.</p> <p>Workaround Separate MAC addresses with a comma (,), do not press "return" after the last MAC address has been entered.</p>
CSCsk77632	cert7.db causes issues with TACACS+ services using LDAP.	<p>Symptom The server has a problem with Tacacs authentications to the back-end LDAP database. This will cause the Tacacs services to shut down and authentications to stop.</p> <p>Conditions Doing secure LDAP using cert7.db.</p> <p>Workaround Change to SSL LDAP using CA cert instead of cert7.d.b</p>
CSCsk89270	Extra certificates copied into ACS backup file.	<p>Symptom Restoring a dump in a different machine than where it was backed up and backing up it once again after modifying it may cause the increase in size of the dump file.</p> <p>Workaround None.</p>

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

Bug ID	Summary	Explanation
CSCsk93795	ACS 4.1 is sending invalid MS-CHAP-MPPE-Keys to PPTP client.	<p>Symptom PPTP client connecting to a IOS router with Radius authentication fails if "Required 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. Those 11 bytes are: 0c (vendor-type 12) 0b (vendor-length = 11) and 41 75 74 6f 6d 61 74 69 63 (the word "Automatic"). Vendor-length must be 34 which is what IOS is looking for. So the ACS sending the wrong key length.</p> <p>Workaround Use local authentication or "Optional encryption".</p>
CSCsk94878	Windows password change does not work when the PDC Emulator is down.	<p>Symptom Windows user fails to change Windows password when 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 as Native mode (W2K3 mode or W2K mode). User authentication can be successful with other DC even if PDC Emulator is down.</p> <p>Workaround Not attempting the Windows password change when PDC Emulator is down.</p>
CSCsl12657	Disabling password aging still retains Your password will expire in message.	<p>Symptom If an administrator first enables password aging, then disables it, the following text may be seen when users authenticate against ACS: "Your password will expire in" (with no value).</p> <p>Conditions Issue has been observed in the following ACS builds 4.0.1.27, 4.1.1.23, 4.1.3.12. It is possible it affects other versions as well.</p> <p>Workaround Create a new group that doesn't have password aging configured and migrate users from the problematic group to the newly configured group.</p>
CSCsl50122	ACS SE needs configurable RA timeout value.	<p>Symptom This is a request to have a configurable timer added to the ACS Appliance for how long it waits before timing out the Remote Agent during group mapping. By default there is a 60 second timer that the appliance will wait for the RA to return the group information for mapping. If there are a large number of groups in the AD environment (around 12,000) this timer is not high enough.</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 4.1.4 (continued)

Bug ID	Summary	Explanation
CSCsl62845	ACS Remote Agent logging date format is not identical to the date specified on the Appliance.	<p>Symptom ACS Remote agent for windows logs with timestamps in the format mm/dd/yyyy instead of dd/mm/yyyy unlike what is configured on the Solution Engine ACS.</p> <p>The remote agent should get the configuration from the configuration provider (ACS SE) and this is not happening. The date format is always mm/dd/yyyy instead of dd/mm/yyyy as specified on the Solution Engine.</p> <p>Workaround None.</p>
CSCsl70457	Some ACS SE 1113 Appliances ship with BIOS password.	<p>Symptom Some ACS 1113 appliances that are shipping from RMA depots are coming with a bootup password of 'acs1113' Appliance comes with BIOS Password.</p> <p>Workaround Enter the BIOS password of 'acs1113' on bootup.</p>

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

Bug ID	Summary	Explanation
CSCs188008	The ACS web interface does not prevent the dynamic allocation of port 2002.	<p>Symptom ACS doesn't prevent the dynamic allocation of port 2002 when a users logs in or LMS is used.</p> <p>Workaround Login to ACS change the Administration Control, Access Policy, HTTP Port Allocation to: Restrict Administration Sessions to the following port range From Port 2003 to Port 65535.</p>
CSCs198198	Password replication fails with users imported from ACS Unix.	<p>Symptom Password replication may intermittently fail from Master to Slave. This deviation is seen in cases where users were imported from ACS Unix using the import tool and RDBMS to migrate from ACS UNIX. When this import is done it sets the user password authentication type to "Imported Unix". There is a problem with the way the password replication works for Unix Type passwords. The password type can be seen in the GUI by looking at the User Screen and then User Setup > Password Authentication. Users set to ACS Internal Database, Windows Database or Generic LDAP should not see this issue.</p> <p>Conditions This issue was seen in ACS Appliance version: Release 4.1(1) Build 23 Patch 5.</p> <p>Workaround Restart the replication partners. Further Problem Description: Customer has ACS configured to require password change every 30 days (approx). The customer engineer changes the passwords manually on the Master and then replicates the change to the other 4 ACS devices. Found that one user would only work in one Server. We think the replication worked, but it's almost like the change did not "take". The customer engineer has never seen evidence that the replication fails. He always does manual replications and the behavior or the result of that process never changes. No error messages are seen.</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.
CSCef85310	Group DACL is downloaded if Users dACL content is empty.
CSCeg52536	Failed PEAP authentication not shown up in ACS logs.

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

Bug ID	Description
CSCeh00074	GUI/ LDAP group mapping submission failure.
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 doesnt succeeded.
CSCsb24849	ACS does not purge the AAA Client user information after Accounting On.
CSCsc71828	No space error and can't add inverted commas to the string fields ofSNMP.
CSCsd52663	Cross forest user/machine authentication does not work.
CSCsf07915	Memory leak while running CiscoPEAP with Active Directory.
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.
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.
CSCsg32655	MAB Request hangs when username attribute contains valid user in ACS DB.
CSCsg42483	No Access-Rejected is being sent by ACS when Cisco Peap TLS fails.
CSCsg50297	Session timeout with eap-fast.
CSCsg81886	CSACS is subject to multiple XSS vulnerabilities.
CSCsg83134	CSLog timeouts and performance degradation during RADIUS Accounting reqs.
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.

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

Bug ID	Description
CSCsh62641	MAC authentication causes internal errors.
CSCsh68129	No documentation for CSUpdate utility which is available in ACS 4.1.
CSCsh74704	Keep only the last ... files option for backup does not work.
CSCsh77806	EAP-TLS will fail authentication if name contains forwardslash /.
CSCsh79488	ACS logging configuration is not replicated.
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.
CSCsi05807	Some services are stopped but not restarted when restart button pushed.
CSCsi06922	Replication log message says CSRADIUS and CSTacacs failed to start.
CSCsi08214	Wrong message when trying to upgrade not from ACS 4.1.1.
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.
CSCsi20185	Incorrect message in CSAuth.log when binary comparison failed.
CSCsi20298	Free disk space in appliance incorrectly reported.
CSCsi24169	AAA Client IP Address field has no length checking.
CSCsi29212	For limitedAdministrator-List all users didnt work in case of more users.
CSCsi30860	CSAuth shows garbage characters while sending change password request.
CSCsi30990	Info messages are shown are errors for PEAP-TLS authentications.
CSCsi35892	Layer 2 Audit Feature for NAC.
CSCsi42315	CSRADIUS failed to release memory after stress stopped.
CSCsi43436	CSAuth takes max 5 seconds to auth when CSLog is slow or going down.

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

Bug ID	Description
CSCsi46668	User auth succeeds if <No Access> is defined for failed Machine Auth.
CSCsi56204	ACS Fails on wired connection with a Fast Re-Connect error.
CSCsi56892	'Logged Remotely' Radius Attribute not available for Remote Agent Log.
CSCsi57134	QoS values incorrect for WLC.
CSCsi57155	Need to add cisco-av-pair 009\001 to WLC.
CSCsi57310	Disk Space reported incorrectly in appliance cli.
CSCsi59931	ACS error when mapping groups to Microsoft database.
CSCsi59997	Syslog/ODBC configuration missing for NetworkAccessProfile name.
CSCsi60213	Last character of RADIUS IETF attr 81 is truncated.
CSCsi62373	update ASA attribute IETF code 3076.
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.
CSCsi73324	add support for Tmp. elevated user_privilege.
CSCsi73330	CSUtil - for updating device.
CSCsi73334	OID check at the NAP level in the User Certificate for user authen.
CSCsi73372	support for PEAP-GTC machine auth with utf8 username & password.
CSCsi73392	CSSupport for SW GUI.
CSCsi73447	Support for Microsoft Windows Server 2003 R2 with SP2.
CSCsi78265	CSRadius mem leak when some MS RADIUS Attributes are selected in group.
CSCsi80174	When challenge is not provided-it should be logged to failed attemps.
CSCsi82620	Acs GUI displays Incorrect copyright.
CSCsi86114	Cslog restarts intermittently during stress test with remote logging.
CSCsi86304	ACS does not allow for a 64-character shared secret with AP.
CSCsi97449	RDBMS Sync needs to support VSA Type Length above 2 bytes.
CSCsi97551	Machine authentications fail with errors: 1213,20498 with AD API.
CSCsi97644	Support for utf-8 uname & password in EAP-FAST (GTC&MS-CHAPV2) with AD.
CSCsi99644	Custom role is not deleted when CiscoView is re-registered with ACS.

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

Bug ID	Description
CSCsi99902	Administrators don't have privileges for Support page.
CSCsj03185	CSUtil is not importing UDV/VSA if the ID LENGTH=4.
CSCsj03359	Feature: machine authentication GTC inner method.
CSCsj06122	ACS only log first instance of VSA under RADIUS attribute 26.
CSCsj07019	3Com/USR attr missing in the ODBC RADIUS acc config logged attr.
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.
CSCsj12651	Info message shown as error while doing eap-tls with OID enabled.
CSCsj12715	Time bound alternate Group does not take alternate group settings.
CSCsj12729	certOID in AUTHEN_EAP_STATE should be changed to array of pointers.
CSCsj12730	ACS checks for alternate group settings even though its disabled.
CSCsj12767	Time bound alternate Group does not store time(hours) correctly.
CSCsj12791	ACS accepts wrong formatted OID.
CSCsj14075	GTC authentication failed with chinese password.
CSCsj14407	Admin Privilege is not given to selected user even during vocation time.
CSCsj15002	Reset current failed attempts count on submit is not working.
CSCsj16264	No proper validation check for EAP-TLS - OID.
CSCsj16936	RDBMS Synchronization accepts the UDV VSA ID greater than 4 byte.
CSCsj17742	elevated user privilege check moved to more appropriate place.
CSCsj25306	Evenafter disabling timebound alternate group-user has admin privilege.
CSCsj25552	Build 5 does not check user credentials for user authentications.
CSCsj26695	utf-8: machine authentication option to lsa is not passed properly.
CSCsj27202	ACS crashes when irrelevant url is given for Ext Post validation server.
CSCsj27212	Seconds to wait for L 2 audit shows -1 seconds as default.
CSCsj27331	Delete files older than x days options for Back Up does not work proper.
CSCsj32256	Permit/Denied for others TACACS+ default NAS is inverse in NARs.

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

Bug ID	Description
CSCsj54389	Group mapping fails for domain local users.
CSCsj63992	CRL Issuer table is not displayed properly.
CSCsj70507	Few Services Logs Do Not Display ACS Version and Build Number.
CSCsj71737	ACS Appliance memory leak in CSMon.
CSCsj84279	ACS 4.1.3 Accounting Proxy doesn't work properly.
CSCsj85656	Regarding with CSCsh42915 RDBMS issue.
CSCsj87733	CRL page hangs when trying to auto enable link for ACSserver cert issuer.
CSCsj87749	Minor GUI Misalignment for the Temporary Elevated User Privilege Feature.
CSCsk02186	OIDs not replicated when OIDs are defined in NAP on ACS.
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.
CSCsk53606	CSDbsync and CSlog shows unwanted log messages on Event Notifier.
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.
CSCsk77023	MAB fails when MAC is in AD.
CSCsk88667	Provide option for both implicit AND and implicit OR for OID comparison.
CSCsl05805	Windows DB Group Mapping API need to be Configurable.
CSCsl09917	CSAuth restarts when machine auth user name is without domain info.
CSCsl13137	Upgradation of patch version failed in appliance.
CSCsl26045	Support for the New Venezuela Standard Time.

Documentation Updates

This section provides documentation updates, including:

- [Changes, page 26](#)
- [Cisco Secure Authentication Agent, page 27](#)
- [Omissions, page 29](#)

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.

CSUtil Example Returns Error Message

The `csutil.exe -d -n -l` example on page 8 in the *User Guide for Cisco Secure ACS 4.1*, Appendix D, “CSUtil Database Utility” returns an error message.

Modification to RADIUS Access Request/Reject Online Help

The information in the ACS online help at **External User Database > Database Configuration > External ODBC Database > Configure**, choose **RADIUS behavior in the event of database failure**. The second option should be "Discard the access request".

Remote Agent for Windows 4.1.4 Does Not Require Reboot

The *Installation Guide for Cisco Secure ACS Solution Engine 4.1*, steps 10 and 11 state that the you must reboot in order to complete the installation. However, the services restart automatically and you do not need to reboot the remote agent.

Terminal Services and Remote Desktop Not Supported on the Remote Agent

The *Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.1* should include this information. Remote installations performed by using Windows Terminal Services or Remote Desktop (RDP) are not tested and are not supported. Do not install or upgrade over a remote connection using Terminal Services or RDP. We recommend that you disable Terminal Services and RDP while performing any installation or upgrade. Virtual Network Computing (VNC) has been successfully tested.

Bidirectional Logging

The *User Guide for Cisco Secure ACS 4.1* should state that bi-directional remote logging should not be configured with ACS. For example, do not configure ACS_SERVER_1 to refer to ACS_SERVER_2 as remote logger and ACS_SERVER_2 to refer to ACS_SERVER_1 as remote logger.

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 Configuration self-extracting file:

-
- Step 1** Download of the *caadmin.exe* file (the self-extracting zip file).
 - Step 2** Locate the downloaded *caadmin.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.

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.

Error Code Definitions

The *Online Troubleshooting Guide* needs to provide error code definitions. These definitions can be found on Microsoft.com.

Incomplete accountActions Table

In the *User Guide for Cisco Secure ACS 4.1, Appendix F*, the note preceding Table F-10 does not mention the Status (S) field. Although omitted in Table F-10, the accountActions table normally contains the Status field, which shows one of these values:

- 0—Not Processed
- 1—Done
- 2—Failed

The Status value is normally zero (0).

Machine Authentication Support in a Multi-Forest Environment

ACS supports machine authentication in a multi-forest environment. Machine authentications succeed as long as an appropriate trust relationship exists between the primary ACS forest and the requested domain's forest. When a requested user's or machine's domain is part of trusted forest, machine authentication will succeed.

Installation of the Remote Agent

Remote installations performed by using Windows Terminal Services or Remote Desktop (RDP) are not tested and are not supported. Do not install or upgrade over a remote connection using Terminal Services or RDP. We recommend that you disable Terminal Services and RDP while performing any installation or upgrade. We have successfully tested Virtual Network Computing (VNC).

Agentless Host for L2 and L3



Note

The Help link for in the online help for Agentless Host for L2 and L3 does not resolve.

This template is used for access requests from agentless hosts connected to an L2 Network Access Device (NAD). ACS first admits the device to a quarantine network where it can receive an IP address. Audit begins when the device has received an IP address. At this point, the audit is the same as an audit for an L3 host. The NAD must be configured to learn the host's IP address ahead of time. ACS responds to an initial Access-Request with a notification to the device to issue another request when it learns the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition and policy flow falls over to Audit Fail-Open policy. The administrator can then choose to reject the user, or assign a posture token and an optional user group.

[Table 3](#) describes the Profile Sample in the Agentless Host for L2 and L3 Sample Profile Template.

Table 3 *Agentless Host for L2 and L3 Sample Profile Template*

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(([006]Service-Type = 10) AND (not exist [26/9/1]cisco-av-pair aaa:service) AND (audit-session-id=^)
	Credential Validation Database	N/A
Posture Validation	N/A	

Table 3 *Agentless Host for L2 and L3 Sample Profile Template (continued)*

Section	Property	Value			
Authorization	Rules	User-group	System Posture Token	RAC	DAACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked				

Table 4 describes the Shared Profile Components in the Agentless Host for L2 and L3 Sample Profile Template.

Table 4 *Shared Profile Components for Agentless Host for L3 and L3 Sample*

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)

Table 4 Shared Profile Components for Agentless Host for L3 and L3 Sample (continued)

Type	Object	Value		
Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Product Documentation

Table 5 lists the product documentation that is associated with ACS 4.1.4.

Table 5 Product Documentation

Document Title	Description
<i>Documentation Guide for Cisco Secure ACS 4.1</i>	Describes product documentation: <ul style="list-style-type: none"> Printed document with the product. PDF on the product CD-ROM. Available on Cisco.com: <ul style="list-style-type: none"> Windows—http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.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>	ACS 4.1 features, documentation updates, and resolved problems. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html
<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>	New features, documentation updates, and resolved problems since ACS 4.1. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.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.

Table 5 *Product Documentation (continued)*

Document Title	Description
<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: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/user.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: 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: 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: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html</p>
<i>Installation Guide for Cisco Secure ACS 4.1 Windows</i>	<p>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</p>
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.1</i>	<p>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</p>

Table 5 **Product Documentation (continued)**

Document Title	Description
<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/products_installation_and_configuration_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>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, 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, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, 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, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, 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. (0801R)

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.

