



# Release Notes for Cisco Secure ACS 4.1.2

---

**Revised: June 07, 2007, OL-13026-01**  
**CDC Date June 07, 2007**

These release notes describe Cisco Secure Access Control Server (ACS) version 4.1.2. These release notes contain information 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](#)

[Product Documentation, page 2](#)

[Known Caveats, page 4](#)

[Resolved Caveats, page 20](#)

[Installation Notes, page 21](#)

[Obtaining Documentation, Obtaining Support, and Security Guidelines, page 22](#)

## Introduction

ACS 4.1.2 is a maintenance release for ACS 4.1 that consolidates ACS 4.1 customer patches, and resolves other customer and internally found defects. ACS 4.1.2 is available through the Cisco Technical Assistance Center (TAC) only for existing ACS software deployments.

This release includes the 4.1.2 software image.



**Caution**

---

You cannot upgrade from ACS 4.1.3 to 4.1.2, or from 4.1.2 to 4.1.3, and you cannot downgrade from 4.1.2 to 4.1.1.

---



---

**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

ACS 4.1.2 contains information for the enhancement—[RADIUS Key Wrap Extended to All EAP Protocols](#), page 2.

## 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 4.1.2 has moved the Allow RADIUS Key Wrap check box to the top of the EAP Configuration section, in the new Key-Wrap area.

## Product Documentation

[Table 1](#) lists the product documentation for ACS 4.1.2.

**Table 1**      **Product Documentation**

| Document Title                                      | Description  |
|---|--|
| <i>Documentation Guide for Cisco Secure ACS 4.1</i> | <ul style="list-style-type: none"> <li>Printed document with the product.</li> <li>PDF on the product CD-ROM.</li> <li>Available on Cisco.com:<br/><a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html</a></li> </ul>  |
| <i>Release Notes for Cisco Secure ACS 4.1</i>       | ACS 4.1 features, documentation updates, and resolved problems. Available on Cisco.com:<br><a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</a>   |
| <i>Release Notes for Cisco Secure ACS 4.1.2</i>     | New features, documentation updates, and resolved problems. Available on Cisco.com:<br><a href="http://www.cisco.com">http://www.cisco.com</a>   |
| 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.  |
| <i>User Guide for Cisco Secure ACS 4.1</i>          | ACS functionality and procedures for using the ACS features. Available in the following formats: <ul style="list-style-type: none"> <li>By clicking <b>Online Documentation</b> in the ACS navigation menu. The user guide PDF is available on this page by clicking <b>View PDF</b>.</li> <li>PDF on the ACS Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html</a></li> </ul> |

**Table 1**      **Product Documentation (continued)**

| Document Title   | Description   |
|--|---|
| <i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.1</i>      | Supported devices and firmware versions for all ACS features. Available on Cisco.com:<br><a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html</a>  |
| <i>Installation and User Guide for User Changeable Passwords 4.1</i>                         | Installation and user guide for the user-changeable password add-on. Available on Cisco.com:<br><a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html</a>   |
| <i>Configuration Guide for Cisco Secure ACS 4.1.</i>   | Provides provide step-by-step instructions on how to configure and deploy ACS. Available on Cisco.com:<br><a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html</a>   |
| <i>Installation Guide for Cisco Secure ACS 4.1 Windows</i>                                   | Details on installation and upgrade of ACS software and post-installation tasks. Available in the following formats: <ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html</a></li> </ul>   |
| <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 in the following formats: <ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html</a></li> </ul>             |
| <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"> <li>• Printed document with the product.</li> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html</a>.</li> </ul>                      |
| <i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents</i>               | Installation and configuration guide for ACS remote agents for remote logging. Available in the following formats: <ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html</a></li> </ul> |

# Known Caveats

Table 2 contains known caveats in ACS for Windows and Solution Engine 4.1.2. You can also use the Bug Toolkit to find open bugs.

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCea91690 | Event Viewer errors on startup/shutdown in .NET | <p><b>Symptom</b> On Windows .Net Server 2003 shutdown and startup you may see errors that falsely indicate that Cisco Secure ACS service have failed. At startup, you may see a dialog box indicating that a service, such as CSLog, encountered a problem and needs to close. The same error logged to Event Viewer, as in the following example:</p> <p>"Reporting queued error: faulting application CSLog.exe, version 0.0.0.0, faulting module unknown, version 0.0.0.0, fault address 0x00000000."</p> <p>The problem is that in Windows Server 2003, the Service Manager queries the Cisco Secure ACS services status during startup and shutdown, but Cisco Secure ACS services may not have started yet or may have stopped already. Even though this is normal behavior for Cisco Secure ACS services, Windows perceives this as an error and logs it to the Event Viewer.</p> <p>On startup, all errors from event viewer displayed to user, which is why, when users logs into Windows right after startup, they see errors from the previous login session.</p> <p>This behaviour observed on Windows Server 2003 only.</p> <p><b>Workaround</b> You can verify that Cisco Secure ACS services are running by using Control Panel.</p> |
| CSCec72911 | Win2003-password aging page display issue       | <p><b>Symptom</b> ACS is installed on Windows 2003 Server and Password Aging feature is enabled. Only the option "Generate greetings for successful logins" in Password Aging settings is checked. After pressing Submit or Submit + Restart ACS for the first time displays the valid error message: "Error: Generation of greetings on successful logins requires at least one password aging rule to be configured". But on the second press to one of these buttons page bwrong error "active canceled" or "the page cannot be displayed" is shown.</p> <p><b>Conditions</b> Occurs on after install and as long as no changes are performed. Occurs when managing ACS only on the local machine using IE 6.0.</p> <p><b>Workaround</b> Restart ACS.</p>   |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation  |
|------------|--|--|
| CSCee89510 | dates are logged in local time instead of GMT                      | <p><b>Symptom</b> NAC attributes that are in date format are in GMT timezone. When ACS logs these attributes, it converts them to ACS local timezone (the timezone of the ACS server).</p> <p><b>Workaround</b> Configure ACS to use the GMT timezone.</p>   |
| CSCef85310 | Group dACL is downloaded if Users dACL content is empty            | <p><b>Symptom</b> It is possible to define an ACL with an empty content. Following this defect, if a user with an empty ACL, belongs to a group on which a non-empty ACL is defined, authenticates, the ACL of the group is downloaded to the device, instead of the user's one. (While the user's dACL content is not empty, it is downloaded to the device, as it should).</p> <p><b>Workaround</b> The workaround would be not to define an empty downloadable ACL.</p> |
| CSCef96208 | ACS reports incorrect privilege level                              | <p><b>Symptom</b> ACS may report users with the incorrect authorized privilege level. In particular, when using TACACS+ user who are correctly being authenticated with a privilege level of 15 are being reported with a level of 1.</p> <p><b>Workaround</b> The error is cosmetic, and there is no workaround</p>   |
| CSCeh13105 | WinDB maps all other combinations instead of selected groups       | <p><b>Symptom</b> Mapping an AD group to an ACS group may fail. After configuring a map, the result may be that the AD group which was selected is now mapped to the "all other combinations" group instead of the intended group.</p> <p><b>Workaround</b> Workaround is to delete the erroneous map and try the mapping again.</p>   |
| CSCeh52700 | AD expired-user passed EAP-TLS authentication; should be rejected! | <p><b>Symptom</b> EAP-TLS authentication will still pass for users in Active Directory even if their account has expired - no error is given from ACS.</p> <p><b>Conditions</b> EAP-TLS authentication of users in Active Directory running in Windows 2000 environment.</p> <p><b>Conditions</b> None. Windows 2003 has introduced some new attributes that should help resolve this issue in future.</p>   |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation   |
|------------|---|---|
| CSCeh60564 | AD locked-out User passed EAP-TLS authentication, should be rejected! | <p><b>Symptom</b> EAP-TLS authentication will still pass for users in Active Directory even if their account is locked-out. There is no error indication from ACS.</p> <p><b>Conditions</b> EAP-TLS authentication of users in Active Directory running in Windows 2000 environment.</p> <p><b>Workaround</b> None. Windows 2003 has introduced some new attributes that should help resolve this issue in future.</p>                                |
| CSCeh79954 | EAP-TLS time of day restriction in AD doesn't fail user - authen succ | <p><b>Symptom</b> EAP-TLS authentication of users in Windows Active Directory will still pass when a users time-of-day setting (located in AD) is outside the hours they are allowed - no error is given from ACS.</p> <p><b>Conditions</b> EAP-TLS authentication of users in Active Directory running in Windows 2000 or 2003 environment.</p> <p><b>Workaround</b> None.</p>   |
| CSCeh86479 | CSUtil import -85 errors to be changed to info msg-not error          | <p><b>Symptom</b> The csutil utility with the options -n, -g, and -u may print an ODBC error message similar to the following:</p> <pre>ODBC Error. Message=[Sybase][ODBC Driver][Adaptive Server Anywhere]Communication error, SqlState=08S01, NativeError=-85</pre> <p><b>Conditions</b> This would only happen when running csutil from Remote Services.</p> <p><b>Workaround</b> This is really an informational message, and can be ignored.</p> |

**Table 2**      **Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)**

| Bug ID     | Summary   | Explanation   |
|------------|---|---|
| CSCsb19051 | TCP checksum error from CiscoSecure ACS Solution Engine 1111      | <p>A Cisco Secure Access Control Server Solution Engine (ACS SE) 1111 (CSACSE-1111-UP-K9) may generate transient TCP Checksum errors which may cause error logging on other devices in the network. In particular, Cisco switches would generate the following error message:</p> <pre>%IP-3-TCP_BADCKSUM:TCP bad checksum.</pre> <p>The cause of the error is the NIC Software Driver. Not every packet being transmitted will be affected. Given that TCP will retransmit any unacknowledged packet, the system will recover. Excessive logging of the error message within the network might occur. The problem only affects TCP packets; therefore, TACACS may be affected, while RADIUS will not. This problem might also occur on an ACS SE 1112 (Quanta).</p> <p><b>Workaround</b> A temporary workaround is to reload the server; but, because the problem is transient, it will likely return within days or weeks. A patch is available from TAC, which will help to reduce the amount of errors; however, since this is a network configuration problem, it cannot resolve the problem completely. Contact your TAC representative for the appropriate TCP_checksum patch for your platform.</p> |
| CSCsb27597 | Limitation on the custom attributes (of 31k as CSAdmin indicates) | <p><b>Symptom</b> In the T+ Settings per User/group Configuration page, which is accessed from the Interface Configuration page, if you add 1201st entry in the custom attribute field, the browser crashes. The custom attribute field is currently limited to 31KB (which is around 1200 attributes).</p> <p><b>Workaround</b> None.</p>  |
| CSCsb93223 | Policy created when template profile not added upon error         | <p><b>Symptom</b> If for any reason, when using the NAC 802.1x template, you cannot create a profile (for example, Global Authentication Setup is not configured properly), an internal posture validation policy is created in any case.</p> <p><b>Workaround</b> None.</p>  |
| CSCsb95897 | ACS cant display long list of Disabled accounts correctly         | <p><b>Symptom</b> The ACS web interface has problems in displaying disabled accounts lists if they contain several pages. Next is working as needed, but Previous is available only once.</p> <p><b>Workaround</b> None.</p>  |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation   |
|------------|--|---|
| CSCsc41638 | ACS doesn't check if the CA certificate that issued to user exist in CTL | <p><b>Symptom</b> A user who presents a certificate in EAP-TLS or EAP-FAST/EAP-TLS may be authenticated; even though the ACS machine no longer trusts the certificate issuer.</p> <p><b>Workaround</b> Uncheck the CA certificate in question from the ACS web interface before removing the CA certificate from the machine storage.</p>   |
| CSCsc63854 | ODBC Mapping exists after restoring image created on software            | <p><b>Symptom</b> After restoring the appliance image from the software version of ACS 4.0.1, there is still ODBC configuration in Unknown User Policy and in NAP/Authentication.</p> <p><b>Workaround</b> None.</p>  |
| CSCsc77154 | Proxy authentications fail when no DHCP is present at installation       | <p><b>Symptom</b> 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 proxy the authentication packets to an incorrect ip address, while the proxy configuration still presents the default appliance name of deliverance1.</p> <p><b>Workaround</b></p> <ol style="list-style-type: none"> <li>1. Verify that 'Distributed System Settings' is checked under Interface Configuration --&gt; Advanced Options.</li> <li>2. Remove DELIVERANCE1 from "Forward To" list box in "Network Configuration -&gt; "Edit Default Proxy Distribution Entry"</li> <li>3. Remove dummy server from "Network Configuration -&gt; AAA Servers"</li> <li>4. Reboot.</li> </ol> |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation  |
|------------|--|--|
| CSCsc90467 | After Install from Recovery CD, no CLI access.                           | <p><b>Symptom</b> This problem occurs on ACS SE 1111 (HP), when performing a full upgrade including appliance base image. When installing from the ACS SE 1111 (HP) Recovery CD, after 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, 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><b>Conditions</b> 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><b>Workaround</b> Switch off the appliance, and switch it on again.</p> |
| CSCsd18172 | After Installing Appliance the default windows IP remains in the AAA ser | <p><b>Symptom</b> If the user does re-image from the ACS SE CD (quanta model 1112), they should NOT connect the device on the network during the installation. During installation, the configuration (such as hostname, IP) can be some bogus information. After the reboot, using console port to reset the hostname and IP address.</p> <p><b>Workaround</b> Not connecting to the network will avoid this duplicate entries problem.</p>   |
| CSCsd88833 | Manual setup of ip configuration failed, cli is not foolproof enough     | <p><b>Symptom</b> An ACS Appliance may not operate correctly after installation, if there were any problems or changes with the IP addressing. In particular, if there is no DHCP server, or the DHCP server is configured incorrectly, or if the installation occurs with the NIC disconnected.</p> <p><b>Workaround</b> 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>   |
| CSCsd91218 | Appliance filter may not work if during initiate config set invalid ip   | —  |
| CSCsd93779 | Backup every X minutes is not functioning for specific configuration     | —  |
| CSCsd94022 | Shifting system clock forward disrupting scheduled backup process        | —  |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCsd98589 | authentications fail when NIC reconnected after reboot                  | <p><b>Symptom</b> Authentications on an ACS Appliance may fail after the following sequence of events:</p> <ol style="list-style-type: none"> <li>1. Disconnect the NIC cable from</li> <li>2. reboot</li> <li>3. reattach the NIC cable</li> </ol> <p><b>Workaround</b> restart the services after the cable has been reconnected</p>   |
| CSCse01363 | Appliance Configuration page is not replicated from Quanta 4.0.1.42     | —  |
| CSCse04125 | SNMP ports in Appliance S27 can get wrong values                        | —  |
| CSCse69819 | Custom UDV, Replication don't replicate. Failure to create on secondary | <p><b>Symptom</b> When try to create a custom UDV on a secondary ACS server, you get the message of: Vsa attribute [UDV-Vendor-Attribute] already defined by vsa vendor [UDV-Vendor]. Must be unique</p> <p><b>Conditions</b> UDV was defined on primary and replication took place before the UDV was defined on the secondary.</p> <p><b>Workaround</b> Un-install and Re-install ACS on the secondary add the UDV to the secondary and then start replication to the secondary.</p>   |
| CSCsf13603 | Cisco-PEAP authentication against RSA API server provide an error msg   | <p><b>Symptom</b> Working with RSA API as the external DB, and trying to Auth using funk. The Supplicant is using CISCO - PEAP authentication. in the log the following lines appears:</p> <pre> AUTH 10/03/2006 16:20:00 I 0396 3396 External DB [SecurID.dll]: Response from user [rsauser] with state [0] AUTH 10/03/2006 16:20:00 I 0396 3396 External DB [SecurID.dll]: NULL response supplied AUTH 10/03/2006 16:20:00 I 0396 3396 External DB [SecurID.dll]: SecurID_AbortSession state [0] AUTH 10/03/2006 16:20:00 E 0396 3396 External DB [SecurID.dll]: Invalid session state detected [0] </pre> |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation   |
|------------|---|---|
| CSCsf16737 | CSAuth/CSAdmin/CSRADIUS/CSTacacs are not started up after reboot        | <p><b>Symptom</b> After system reboot, the following Services are not started up when Windows service, "Windows Firewall/Internet Connection Sharing (ICS)" is started:</p> <ul style="list-style-type: none"> <li>• CSAuth</li> <li>• CSRADIUS</li> <li>• CSTacacs</li> <li>• CSAdmin</li> </ul> <p><b>Workaround</b> Disable Windows Service "Windows Firewall/Internet Connection Sharing (ICS)" -&gt; services.msc -&gt; Right click and select properties of "Windows Firewall/Internet Connection Sharing (ICS)" -&gt; Change "Startup type" to "Disbaled".</p> <p>or</p> <p><b>Workaround</b> Start them manually.</p> |
| CSCsf25057 | ACS support for TACACS single-connection                                | <p><b>Symptom</b> ACS does not support the TACACS single-connect flag.</p> <p><b>Workaround</b> None.</p>   |
| CSCsg19044 | Acs syslog/ODBC configuration missing listing for trend, mcafee, qualys | <p><b>Symptom</b> Under system configuration, logging configuration, configure failed attempts or passed attempts for syslog and ODBC. The attributes for trend, qualys and mcafee are not listed in either column but are listed under the CSV configuration.</p> <p><b>Conditions</b> when adding 3rd vendors credentials using csutil -addAVP command, these credentials won't appear in syslog or odbc.</p> <p><b>Workaround</b> None.</p>  |
| CSCsg24408 | ACS Syslog facility needs to be configurable for localX, not fixed AUTH | <p><b>Symptom</b> Currently ACS doesn't state what facility is used in the system specifications as far I as I have read into them. I had to trace the traffic coming from ACS that was destined for my syslog server on port 514 to determine what facility was being used.</p> <p><b>Workaround</b> Setup syslog to except with AUTH and not a localX facility. Example: auth.debug /var/log/ACS1.txt.</p>  |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation  |
|------------|--|--|
| CSCsg40727 | ACS 4.0: RDMS fails account action 220 250 with Synchronization Partners | <p><b>Symptom</b> - NDG is not getting added to "Synchronization Partners", but an additional (duplicated) entry is getting added to "primary" - AAA-Client may can't be deleted anymore afterwards</p> <p><b>Conditions</b> Account-Action-File:<br/>                     SequenceId,Priority,UserName,GroupName,Action,ValueName,Value1,Value2,Value3,DateTime,MessageNo,ComputerNames,AppId,Status 1,0,testUser01,foobar,100,,foobar,,26/08/1998 00:00,0,,0<br/>                     9,0,testUser09,foobar,100,,foobar,,26/08/1998 00:00,0,,0<br/>                     10,0,testUser10,foobar,100,,foobar,,26/08/1998 00:00,0,,0<br/>                     11,0,,foobar,170,,exec,,,,,0 12,0,,foobar,172,priv-lvl,exec,,15,,,,,0<br/>                     13,0,,220,chimpanzee070707,9.9.9.9,cisco,VENDOR_ID_CISCO_RADIUS,,,,,0 14,0,,250,monkeycage,,,,,0<br/>                     15,0,,252,chimpanzee070707,monkeycage,,,,,0</p> <p><b>Workaround</b> None.</p> |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation   |
|------------|--|---|
| CSCsg56677 | After upgrade re-authenticate EAP-FAST user with UPN or SAM format fails | <p><b>Symptom</b> When authenticating user with SAM/UPN format (Domain\username or username@domain) on ACS 4.0.1.49 or ACS 4.1, it succeeds at the first time and also after trying to re-authenticate with the same PAC. However, if we try to upgrade ACS 4.0 (i.e. 4.0.1.27, 4.0.1.42/43/44) to build 4.0.1.49 or to ACS 4.1, we will see that the re-authentication (i.e. stateless session resume) will fail with the error - "Access denied:fast-reconnect was successful but user was not found in cache". This bug has the same behavior as describe in CSCsd82223, but after performing the above upgrade.</p> <p><b>Workaround</b></p> <p>Case #1: Customers using Manual PAC provisioning. Advise a customer to reprovision PACs with correct usernames (i.e. usernames containing domains).</p> <p>Case #2: Customers using Automatic PAC provisioning. Advise a customer to do the next workaround: 1. Set the next values for the EAP-FAST settings (see EAP-FAST Configuration page) : Active master key TTL = 1 hours Retired master key TTL = 2 hours Tunnel PAC TTL = 30 minutes Authorization PAC TTL = 10 minutes</p> <p><b>Note</b></p> <ol style="list-style-type: none"> <li>Active master and Retired master key TTLs are changed to force invalidation of PACs issued by ACS 4.0 (i.e. 4.0.1.27, 4.0.1.42/43/44).</li> <li>Tunnel PAC and Authorization PAC TTLs are changed due to limitation that their values must be less then Active master and Retired master key TTLs.</li> <li><b>IMPORTANT:</b> When customer's environment contains several ACS servers, this change must be applied on ALL ACS servers configured as EAP-FAST master server and then this change should be replicated to corresponding slave ACS Servers. This change will lead to reprovisioning of ALL PACs. 2. It is safe to change these EAP-FAST settings back a day after this change was applied/replicated to ALL ACS servers in the customer's environment. The default values for them are: Active master key TTL = 1 months Retired master key TTL = 3 months Tunnel PAC TTL = 1 weeks Authorization PAC TTL = 1 hours.</li> </ol> |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCsg96534 | ACS support for Windows 2003 R2 needs clarification.              | <p><b>Symptom</b> ACS 4.1 and previous releases have not been tested on Windows 2003 server R2. Authentication to ACS on this platform might have unpredictable results. The release notes and documentation might not make it clear that there is a distinction between Windows 2003 and Windows 2003 R2.</p> <p><b>Conditions</b> Installation of ACS on Windows 2003 R2</p> <p><b>Workaround</b> Use ACS on a supported platform that is specified in the release notes.</p>  |
| CSCsh42920 | Online help has old Key Wrap functionality description.           | <p><b>Symptom</b> RADIUS Key Wrap was extended to all EAP protocols instead of only EAP-TLS.</p> <p><b>Workaround</b> Refer to <a href="#">RADIUS Key Wrap Extended to All EAP Protocols, page 2</a> for more information.</p>   |
| CSCsh77806 | EAP-TLS will fail authentication if name contains forward slash / | <p><b>Symptom</b> EAP-TLS users authenticating to ACS (and in turn to Active Directory) fail authentication if the Distinguished Name returned from the LDAP server contains a forward slash. Logs from the ACS will cite this as a permissions issue and do not make it clear that it's the format of the username at fault.</p> <p><b>Conditions</b> Issue is seen in Distinguished names defined in the following format:</p> <p>Distinguished Name: CN=Lastname\, Firstname<br/>Department1/Department2,OU=...</p> <p>but presumably will be seen in any instance in which the Distinguished Name contains a forward slash. Windows Domain controllers will allow the forward slash as a part of the username and do not appear to use an escape character prior to the forward slash (the above example does include an escape character prior to the comma).</p> <p><b>Workaround</b> Avoid use of forward slashes in user names authentication via EAP-TLS.</p> <p>Further Problem Description:</p> <p>Issue is possibly a bug in Microsoft's handling of the forward slash character. Since this character is used as a separator in LDAP, the LDAP replies back should be padded with a backslash prior to the forward slash.</p> |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation   |
|------------|---|---|
| CSCsh90602 | MAB no more functional after installing accumulative patch 4.1.1.23.3 | <p><b>Symptom</b> After installing the Accumulative Patch 4.1.1.23.3 on ACS 4.1.1.23 the Mac Authentication Bypaas feature is no longer functional. The Failed Attempts.csv file shows the following error - Authentication protocol is not allowed for this network access profile.</p> <p><b>Workaround</b> Cisco recommends that you apply patch 4.1.3.12.1 to ensure the correct MAB and MAC functionality.</p> <p><b>Note</b> This patch includes a fix for CSCsh62641: MAC authentication causes internal errors.</p> <p>After you apply the patch, if:</p> <ul style="list-style-type: none"> <li>• Type(6) = 10 and NAP is present, MAB is invoked.</li> <li>• Service-Type(6) = 10 and NAP is non-existent, MAC authentication is invoked.</li> </ul> <p>This correction retains the ACS 4.1 functionality for MAB and the ACS 4.0 functionality for MAC authentication.</p> |
| CSCsh95071 | Database replication does not propagate certain log settings          | <p><b>Symptom</b> After customizing the columns to log configuration on the primary, the corresponding settings are not replicated to the secondary servers.</p> <p><b>Conditions</b> This has been observed on ACS SW version 4.1(1.23).</p> <p><b>Workaround</b> Manually configure the columns to log information on the secondary servers.</p>  |
| CSCsi04187 | ACS: MS-PEAP Machine authentication fails with host/<dns name> format | <p><b>Symptom</b> PEAP MS-CHAP machine authentication will fail with machine not found if host/&lt;dns name&gt; format is sent from client. This only happens if the machine is authenticating to a domain forest that the ACS is not a member of.</p> <p><b>Conditions</b> The Machine authenticating to ACS is in a different domain forest then the ACS and the supplicant is using host/&lt;dns name&gt; as the machine name format. You also have to be using PEAP MS-CHAPv2.</p> <p><b>Workaround</b> If the supplicant has the option you can send the machine name in hos/&lt;netbios&gt; format. Many supplicants do not have this option.</p>   |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCsi10581 | CSLogagent application error/crashes                            | <p><b>Symptom</b> ACS Remote Agent 4.1.1.23.<br/>MS is faulting cslogagent.exe because of module msvcr7.dll.</p> <p><b>Workaround</b> None</p>   |
| CSCsi13785 | ACS won't replicate users previously set for dynamic mapping    | <p><b>Symptom</b> ACS Database replication may inappropriately flag users as "learned dynamically" and fail to replicate them in certain cases.</p> <p><b>Conditions</b> This issue has been observed under the following circumstances:</p> <ul style="list-style-type: none"> <li>• Database for user points to external database (windows) and</li> <li>• Group for the user is set as dynamic, assigned by external authenticator</li> <li>• Database was upgraded from previous code in which we did replicate dynamic users (prior to ACS 4.0)</li> </ul> <p><b>Conditions</b> Delete and recreate the affected users or Set the unknown user database to allow unknown users to authenticate to external databases.</p> |
| CSCsi17499 | Remote password change setting isn't replicated                 | <p><b>Symptom</b> The setting of the remote password management feature, found under Local Password Management in the System Configuration tab, is not replicated from the primary ACS server to any of the secondaries.</p> <p><b>Conditions</b> This has been observed on ACS 4.1(1.23) on both Windows and ACS SE appliances. Other versions may be affected also.</p> <p><b>Workaround</b> Manually enable/disable the remote password management feature on the secondary server(s).</p>  |
| CSCsi50359 | Enable authentications are rejected with Internal Error message | <p><b>Symptom</b> Users on CatOS switches are denied enable authentication, even though they're entering the correct password. Login authentications work correctly.</p> <p><b>Conditions</b> 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><b>Workaround</b> Configure the user to have a max privilege level setting under "Max Privilege for any AAA Client"</p>  |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary  | Explanation  |
|------------|--|--|
| CSCsi55085 | ACS services not started after replicate/reboot on machine with dual cpu | <p><b>Symptom</b> ACS services are not started when rebooting Secondary ACS machine within 30 minutes after the DB replication.</p> <p><b>Conditions</b> After the DB replication between the Primary ACS and the Secondary ACS machines with dual processor, this issue is only seen when rebooting the Secondary ACS machine within 30 minutes.</p> <p><b>Workaround</b> Not to reboot the Secondary ACS within 30 minutes after the DB replication.</p> |
| CSCsi56892 | 'Logged Remotely' Radius Attribute not available for Remote Agent Log    | <p><b>Symptom</b> 'Logged Remotely' Radius attribute is not available to be chosen in the Remote Logging section of Radius Accounting.</p> <p><b>Conditions</b> This problem exists on appliances that are running 3.3.4.12 or 4.1.1.23.</p> <p><b>Workaround</b> None at this time.</p>   |
| CSCsi60213 | Last character of RADIUS IETF attr 81 is truncated                       | <p><b>Symptom</b> Accounting reports show that the last character on VLAN id for 802.1x supplicants is truncated. The clients are placed on the correct VLAN, however.</p> <p><b>Conditions</b> This has been observed on ACS 4.1.1(23), other versions may be affected as well.</p> <p><b>Workaround</b> No workarounds are known at this time.</p>   |

Table 2 Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary                                 | Explanation   |
|------------|---|---|
| CSCsi62622 | system replication partners table empty | <p><b>Symptom</b> -ACS replication Master GUI is not visually populating the partner replication table with the slave hostname/IP address</p> <p><b>Conditions</b> -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</p> <p><b>Workaround</b></p> <ol style="list-style-type: none"> <li>1. Add hostname, ie. Flprdasaaa01, to replication partner table (right pane), hit 'submit' or 'replicate now'.</li> <li>2. Upon return to replication table page, the right pane window might be empty. Add a second hostname, ie. Flprdasaaa02, hit submit</li> <li>3. Upon next return to replication table page, hostname Flprdasaaa02, might/should be visible via GUI,</li> <li>4. At this point, one should be able Add/Remove hostnames to the replication table pane accordingly</li> </ol> <p>FURTHER PROBLEM DESCRIPTION:<br/>-DE does not see the issue rectified in v4.1.1b23 patch 4.</p> |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCsi63656 | Unknown Radius Token Server after replication.                    | <p><b>Symptom</b> After replication users show up with a Database of 'Unknown Radius Token Server'.</p> <p><b>Conditions</b> Occurs when multiple Radius Token Servers were created on the primary but only one was created on the secondary.</p> <p><b>Workaround</b> There are two known workarounds for this problem.</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol> |
| CSCsi65427 | ACS SE: Hostname greater than 15 characters locks out GUI and CLI | <p><b>Symptom</b> After initial setup of the ACS Appliance the user is prompted to reboot the SE. After the reboot CLI and GUI access is lost and can not be regained with out reinstalling the SE.</p> <p><b>Conditions</b> If a hostname is entered in the CLI initial setup greater than 15 characters, after the reboot the SE will not have GUI or CLI access.</p> <p><b>Workaround</b> None, re-install the Appliance and enter a hostname that includes 15 characters or less.</p>  |

**Table 2** Known Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Summary   | Explanation  |
|------------|---|--|
| CSCsi71613 | Cannot login to UCP when password contains an '&' symbol                  | <p><b>Symptom</b> If a user wants to change their password in UCP, but their current password contains an '&amp;' in it, then the user will be unable to login to the UCP application to begin the password change process.</p> <p>The error in the ACS logs shows:</p> <pre>AUTH 11/04/2007 11:27:52 E 2489 1180 Plain DB pass check for 30419 failed</pre> <p><b>Conditions</b> This has been seen in the ACS 3.3 line, and the ACS 4.1 line of code. It only happens when the user's password contains an '&amp;' in it.</p> <p><b>Workaround</b> The only workaround is to change the users password manually in the ACS Admin GUI, which users will not have access to, so it would fall to an administrator to change the users password instead of the end user themselves.</p> |
| CSCsi78265 | CSRadius mem leak when some MS RADIUS Attributes are selected in group    | —  |
| CSCsi82393 | CiscoAAA Event ID 5 error in Windows Event Viewer\Applcaition log         | <p><b>Symptom</b> Event ID (5) in Source (CiscoAAA) error generated in MS Windows Application Event log on the primary ACS every time when ACSs is replicating its database.</p> <p><b>Conditions</b> Primary/secondary ACSs for Windows configured for database replication.</p> <p><b>Workaround</b> none.</p>   |
| CSCsi84005 | During stresses of EAP-FAST(TLS/GTC inner)+LDAP on Dual CPU CSAAuth crash | —  |

## Resolved Caveats

Table 3 contains the resolved caveats for ACS 4.1.2. Check the Bug Toolkit on Cisco.com for any resolved bugs that might not appear here.

**Table 3** Resolved Caveats in ACS Windows and Solution Engine 4.1.2

| Bug ID     | Description   |
|------------|---|
| CSCse67259 | Typo in "ACS has been tested on release 6.5" but the Rel is just 6.3.5. |
| CSCsg44419 | CSAuth service does not start -if DNS is unavailable.                   |
| CSCsg97429 | TACACS+ Command Accounting does not work in ACS 4.1(1) Build 23.        |

**Table 3** Resolved Caveats in ACS Windows and Solution Engine 4.1.2 (continued)

| Bug ID     | Description  |
|------------|--|
| CSCsh32888 | Separate enable password does not work after ACS upgrade to 4.1.       |
| CSCsh39771 | ACS is unable to exit from restore process.                            |
| CSCsh42893 | ACS GUI hangs and times out when service is restarted during stress.   |
| CSCsh48625 | ACS radius error 2162 - switch isn't sent RAC/DACL client recvs token. |
| CSCsh62641 | MAC authentication causes internal errors.                             |
| CSCsh74140 | Loss of ext. database breaks NAD AAA redundancy concept.               |
| CSCsh77651 | Anti Virus is locking DB file.   |
| CSCsh87466 | Authentication failure on first login after remote agent restart.      |
| CSCsi03015 | EAP-FAST(GTC) may grant access to AD user with empty username.         |
| CSCsi25108 | submit CRL with wrong URL causes CSAdmin become "IDLE" state.          |
| CSCsi42315 | CSRadius failed to release memory after stress stopped                 |
| CSCsi46668 | User auth succeeds if <No Access> is defined for failed Machine Auth.  |
| CSCsi47515 | Multiple Testcases Cause CSLog Failures.                               |

## Installation Notes

This section contains installation information for ACS 4.1.2.

### Installation Notes for ACS 4.1.2 for Windows

This section contains:

- [Upgrade Path for ACS 4.1.2 for Windows, page 21](#)
- [System Requirements for ACS 4.1.2 for Windows, page 21](#)
- [Installing ACS 4.1.2 for Windows, page 22](#)

### Upgrade Path for ACS 4.1.2 for Windows

Cisco tested the upgrade to ACS for Windows Server 4.1.2 from release 4.1. For ACS 4.1 upgrade paths, see the *Installation Guide for Cisco Secure ACS for Windows 4.1*.



**Note**

Cisco does not support upgrade from 4.1.3 to 4.1.2 or upgrade from 4.1.2 to 4.1.3.

### System Requirements for ACS 4.1.2 for Windows

The system requirements for ACS 4.1.2 are the same as 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*.

## Installing ACS 4.1.2 for Windows

You must have ACS 4.1 installed before you install ACS 4.1.2. ACS 4.1.2 is available through the Cisco Technical Assistance Center (TAC) only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.2 are the same as for ACS 4.1. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS for Windows 4.1*.

## Installation Notes for ACS 4.1.2 Solution Engine

This section contains:

- [Upgrade Path for ACS 4.1.2 Solution Engine, page 22](#)
- [Installing ACS 4.1.2 Solution Engine, page 22](#)

## Upgrade Path for ACS 4.1.2 Solution Engine

Cisco tested the upgrade to ACS Solution Engine 4.1.2 from release 4.1. For ACS 4.1 upgrade paths, see the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

## Installing ACS 4.1.2 Solution Engine

ACS 4.1 is pre-installed on the 1113 appliance. The ACS 4.1.2 Solution Engine upgrade package is available through the Cisco Technical Assistance Center (TAC) only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.2 Solution Engine are the same as ACS 4.1. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

# 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.