



# Release Notes for Cisco Secure ACS for Windows 4.0

---

February 2006  
Full Build Number: 4.0.1.27

These release notes pertain to Cisco Secure Access Control Server for Windows, hereafter referred to as ACS version 4.0.



**Note**

---

The ACS release numbering system for software includes major release, minor release, maintenance build, and interim build number in the MMM.mmm.###.BBB format. For this release, the versioning information is Cisco Secure ACS 4.0.1.27. Elsewhere in this document where 4.0 is used, we are referring to 4.0.1. ACS major release numbering starts at 4.0.1, not 4.0.0. Use this information when working with your customer service representative.

---

## Contents

These release notes provide:

- [System Requirements, page 2](#)
- [ACS New Features, page 2](#)
- [Product Documentation, page 5](#)
- [Installation Notes, page 6](#)
- [Limitations and Restrictions, page 8](#)
- [Security Advisory, page 10](#)
- [Known Problems, page 10](#)
- [Resolved Problems, page 21](#)
- [Documentation Updates, page 22](#)
- [Obtaining Documentation, page 24](#)
- [Documentation Feedback, page 25](#)



---

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

© 2005 Cisco Systems, Inc. All rights reserved.

- [Cisco Product Security Overview, page 25](#)
- [Obtaining Technical Assistance, page 27](#)
- [Obtaining Additional Publications and Information, page 28](#)

## System Requirements

System requirements are documented in the *Installation Guide for Cisco Secure ACS for Windows*. For documentation updates after publication, see [Documentation Updates, page 22](#).

## Software Compatibility

See the *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows* on [Cisco.com](#).

## Upgrading to a New Software Release

For detailed instructions see *Installation Guide for Cisco Secure ACS for Windows* on [Cisco.com](#). For upgrade paths and known problems, see [Upgrade Paths, page 6](#) and [Known Problems, page 10](#).

## ACS New Features

ACS contains the following new and changed features:

- **Network Admission Control (NAC) Release 2.0 support**—ACS acts as a policy-decision point in NAC deployments. Using configurable policies, it evaluates the credentials received from the Cisco Trust Agent, determines the state of the host, and sends a per-user authorization to the network access device: access control lists (ACLs), a policy-based ACL, or a private VLAN assignment. Evaluation of the host credentials can enforce many specific policies, such as OS patch level and antivirus DAT file version. ACS records the policy evaluation results for use with your monitoring system. ACS also allows hosts without the appropriate agent technology to be audited by third-party audit vendors before granting network access. ACS policies can be extended with external policy servers to which ACS forwards credentials. For example, credentials specific to an antivirus vendor can be forwarded to the vendor's antivirus policy server, and audit policy requests can be forwarded to audit vendors. For more information about the new ACS features to support NAC 2.0, see [Support for NAC 2.0, page 4](#)
- **Increased number of supported devices**—ACS can now support up to 35,000 devices.
- **Profile-based authentication and authorization**—A new feature called network access profiles allows administrators to classify access requests according to network location, membership in a network device group, protocol type, or other specific RADIUS attribute values sent by the network device through which the user connects. Authentication, access control, posture validation and authorization policies can be mapped to specific profiles. An example of a profile-based policy is the ability to apply a different access policy for wireless access versus remote (VPN) access.
- **New storage infrastructure**—ACS now uses a SQL database to store all the user and configuration information. The new ACS internal database improves scaling and performance and is less reliant on the Windows Registry. The Windows Registry will be used only for application information. A

new database password is required during installation. The password is stored in the Windows registry using Microsoft Crypto API. The database is encrypted using a hash of customer-provided password and an internal password. You can use **CSUtil** to change the password.

- **LDAP improvements**—ACS caches successful external authentications (using LDAP), allowing it to immediately look up a user during re-authentication. ACS provides improved SSL support. See [LDAP Improvements, page 4](#), for more information.
- **Japanese browser support**—Supports administration of ACS by using MS Internet Explorer 6.0 SP1 and Netscape Communicator 8.0.4 with Sun Java JRE 1.5.0, or MS Internet Explorer 6.0 SP1 with Microsoft Java Virtual Machine, installed on Japanese Windows Operating System (JOS). This feature will be supported for entering data in English (not Japanese).
- **TACACS+ and RADIUS key support at group level**—Ability to set a shared secret at the group level (Network Device Group).
- **Purging capability for cached users in ACS**—Ability to remove dynamically saved users from the ACS database via User Setup.
- **Authentication improvements:**
  - Support for the Microsoft Windows Callback feature.
  - Ability for external users to authenticate via an enable password.
  - Certificate revocation list checking during EAP-TLS authentication.
- **Online Help** - The online documentation, *Cisco Secure ACS for Windows User Guide*, opens in a separate window. The online help contains a search button and capability to open a PDF version of the user guide.
- **NTLM Support** - ACS can now operate with NTLM v1, NTLM v2 (with appropriate Microsoft patches), and LAN Manager (if you require it).
- **External Novell NDS Database Support** - Support for group mappings for external Novell NDS databases is now done by using generic LDAP group set mappings.
- **Extended replication support**—Administrators can now replicate network access profiles and all related configuration, including:
  - Posture validation settings
  - AAA clients and hosts
  - External database configuration
  - Global authentication configuration
  - Network device groups
  - Dictionaries
  - Shared profile components
  - Additional logging attributes
- **Machine Access Restrictions (MAR) Exemption Lists**—You can specify which groups are allowed access to the network; regardless of whether they pass machine authentication. A MAR exemption list can be configured for specific user groups (for example, managers and administrators).
- **RADIUS Authorization Component (RAC) support**—Includes RADIUS authorization components as a new type of shared profile component. Shared RACs contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy.

- **Support of additional Cisco hardware devices**—ACS 4.0 includes support for Cisco wireless LAN controllers and Cisco adaptive security appliances.

## Support for NAC 2.0

The following features support NAC 2.0:

- **EAP-FAST Version 1a support for NAC phase 2**—Supports an authenticated tunnel (by using the server certificate) inside of which the provisioning of PACs will occur. EAP types supported inside the tunnel include: EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.
- **Agentless host support**— Support for Cisco and third-party Audit Servers that determine posture information about a client, without relying on the presence of a NAC-compliant Posture Agent (PA). These types of clients are also referred to as NAC Agentless Hosts (NAH).
- **Linux packages support in posture validation**—Supports Linux packages for the Cisco:Host plugin. The following extended attributes are available for Linux packages: Cisco:Host:Package:Version and Cisco:Host:Package:Version-String. For additional details, see [Support for Linux Packages in Posture Validation, page 5](#).
- **Posture Validation:**
  - Support for an external audit server which determines posture information about a host without relying on the presence of a Posture Agent (PA).
  - Posture validation no longer requires NAC databases to verify compliance. You can choose from three options for validation: internal policies located in ACS, policies defined on external servers, and policies defined on audit servers for NAC agentless hosts.
  - Authorization for posture validation is now configured within the Network Access Profiles feature. Posture validation no longer requires special authorization rules.
  - Changes have been made to optimize posture validation. In previous versions, ACS requested all the credentials by using the type-length-value (TLV) protocol. ACS has been optimized to request only the attributes that are required to evaluate posture validation.

## LDAP Improvements

The ACS authentication and authorization service **CSAuth** supports multithreading to authenticate with the LDAP external database. Multiple users can simultaneously be searched and authenticated against the LDAP server(s).

LDAP over SSL now includes the option to authenticate by using certificate database files other than the *Netscape cert7.db* file. This new option uses the same mechanism as other SSL installations in the ACS environment.

When ACS checks authentication and authorization of a user on the LDAP server, it uses a connection with LDAP administrator account permissions to search for the user and for the users groups on the directory subtree. ACS keeps those administrator connections open for successive use. It is possible to limit the maximum number of concurrent administrator connections per generic LDAP external database configuration (primary and secondary).

After an LDAP user is successfully authenticated to the LDAP external database, its distinguished name (DN) on the LDAP server is cached in ACS. The cached DN is used during next authentication request of the user to save search time.

## Support for Linux Packages in Posture Validation

ACS 4.0 supports Linux packages for the Cisco:Host plugin. The following extended attributes are available for Linux packages:

- Cisco:Host:Package:Version
- Cisco:Host:Package:Version-String

The following Linux packages are supported:

- acrobat;cpio;cups;curl;cvs;cyrus-sasl;emacs;enscript;etherreal;evolution;gaim;gd;gdk-pixbuf;glibc;
- gnome-vfs2;gnupg;gtk2;httpd;ia32el;imagemagick;imap;imlib;iproute;ipsec-tools;kdegraphics;
- kdelibs;kdenetwork;kdepim;kernel;krb5;less;lftp;lha;libpng;libtiff;libxml;libxml2;mailman;mod\_python;
- mozilla;mutt;mysql;mysql-server;nasm;net-snmp;netpbm;nfs-utils;openmotif;openoffice.org;
- openssh;openssl;perl;perl-dbi;php;postgresql;pwlib;python;qt;realplayer;redhat-config-nfs;
- rh-postgresql;rsh;rsync;ruby;samba;sharutils;slocate;sox;spamassassin;squid;squirrelmail;sysstat;
- tcpdump;telnnet;tetex;utempter;vim;xchat;xemacs;xfree86;xloadimage;xpdf;zip

You can add or remove packages by using the **CSUtil** tool.

### Extended attributes

Extended attributes are only supported as descendants of the Cisco:Host application.

## Product Documentation

The following product documentation is available on ACS:

**Table 1** Product Documentation

Document Title	Description
<i>Release Notes for Cisco Secure ACS for Windows</i>	New features, documentation updates, known problems, and resolved problems. Available on Cisco.com: <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>Installation Guide for Cisco Secure ACS for 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>• Orderable; see <a href="#">Obtaining Documentation</a>, page 24.</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>
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 1 Product Documentation (continued)

Document Title	Description
<i>User Guide for Cisco Secure ACS for Windows</i>	ACS functionality and procedures for using the ACS features. Available in the following formats: <ul style="list-style-type: none"> <li>You can also access the user guide 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>Orderable; see <a href="#">Obtaining Documentation, page 24</a>.</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>
<i>Supported Devices and Interoperable Software Tables for Cisco Secure ACS for Windows</i>	Supported devices and firmware versions for all ACS features. Available on Cisco.com: <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 Cisco Secure ACS for User-Changeable Passwords</i>	Installation and user guide for the user-changeable password add-on. Available 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>

## Installation Notes

The following installation notes are of importance:

- ACS will not install properly if a Sybase server is installed on the same machine.
- Remote installations performed by using Windows Terminal Services are not tested and are not supported. We recommend that you disable Terminal Services while performing any installation or upgrade. Virtual Network Computing (VNC) has been tested successfully.

See the *Installation Guide for Cisco Secure ACS for Windows* for installation, upgrade, and uninstall instructions, as well as post-installation tasks. For post-installation tasks, see [Post-Upgrade Configuration, page 7](#).

## Upgrade Paths

ACS 4.0 supports these upgrade and migration paths:

- [Supported Upgrade Path, page 7](#)
- [Supported Migration Path, page 7](#)
- [Unsupported Migration Path, page 7](#)



### Note

To upgrade to version 4.0 from a version earlier than 3.2.3, upgrade to one of the supported upgrade versions, which are listed in this section, and then upgrade to ACS 4.0.

## Supported Upgrade Path

ACS supports the following upgrade paths. These paths have been tested and are supported:

- Cisco Secure ACS for Windows, release 3.3.3 to ACS 4.0
- Cisco Secure ACS for Windows, release 3.3.2 to ACS 4.0
- Cisco Secure ACS for Windows, release 3.3.1 to ACS 3.3.3, then to ACS 4.0
- Cisco Secure ACS for Windows, release 3.2.3 to ACS 4.0
- Cisco Secure ACS for Windows, release 3.2.2 to ACS 3.3, then to ACS 4.0
- Cisco Secure ACS for Windows, release 3.2.1 to ACS 3.3, then to ACS 4.0
- Cisco Secure ACS for Windows, release 3.1.2 to ACS 3.3, then to ACS 4.0
- Cisco Secure ACS for Windows, release 3.0.4 to ACS 3.3, then to ACS 4.0

**Note**

---

If you are upgrading to ACS 3.3.3 and do not have access to that software, review the README text for details on the upgrade procedure.

---

## Supported Migration Path

ACS supports the migration path from ACS 3.1.2 to ACS 3.3.3 to ACS 4.0. This path has been tested and is supported.

## Unsupported Migration Path

ACS does not support the following migration paths. These paths have not been tested and are not supported. See the tested and supported paths for migration at [Supported Migration Path, page 7](#).

- ACS 3.2.3 to ACS 3.3.3 to ACS 4.0
- Prior to ACS 3.2.3 to ACS 3.3.x to ACS 4.0

## Post-Upgrade Configuration

The following section contains information about post-upgrade configuration:

- After upgrading to ACS 4.0, you may need to perform additional configuration steps to successfully use ACS and Network Access Profiles (NAP). If you used NAC in ACS 3.3, ACS will not operate in an identical manner in ACS 4.0. For example, you must create a new set of authorization rules for Network Access Profiles that are created during the upgrade process.
- If you used ACS 3.xODBC logging and upgraded to ACS 4.0, preserving your data, you must update the ODBC tables so that the SQL tables continue to work.

For details on how to complete post-installation tasks, see the *Installation Guide for Cisco Secure ACS for Windows*.

## Upgrading From Version 3.3

The following actions are performed automatically when you upgrade from ACS 3.3 to ACS 4.0:

1. Local and external posture policies are automatically transformed.
2. A single Network Access Profile, (configured for NAC only) is created as a process of the upgrade.
3. Each instance of the selected ACS 3.3 Network Posture Validation Database will automatically be transformed into a posture validation rule. All the rules will be associated with the NAP that was created (in step 2). All PA message and URL redirects are mapped correspondingly.
4. A RADIUS Authorization Component will be created for each mapped group. ACS populates the RAC with all attributes that were configured in the user or group setup menus, except for the posture-token Cisco-av-pair. Since the posture-token Cisco-av-pair attribute is generated dynamically at runtime, by ACS, there is not need to configure it manually.
5. If you manually added posture validation attributes in ACS 3.3, they will added to the ACS version 4.0 posture dictionary during the upgrade.

## Limitations and Restrictions

The following limitations and restrictions apply to ACS 4.0.

- User/Machine Out-of-Band PAC Provisioning for EAP-FAST v1a has not been tested. The Out-of-band provisioning feature was not tested since the MDC (meetinghouse) supplicant does not support it. (CSCsb46242)
- The TACACs+ and LEAP protocols for Network Access Profiles are not supported in ACS version 4.0.
- Network device limitation will support up to 35,000 devices.
- Installation on Japanese Windows 2000 SP4 or Japanese Windows 2003 SP1 is not supported.

## Interoperability Testing

ACS has not been tested for interoperability with other Cisco software. Other than for the software and operating system versions listed in this document, Cisco performed no interoperability testing. Using untested software with ACS may cause problems. For the best performance of ACS, Cisco recommends that you use the versions of software and operating systems in the *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows* on [Cisco.com](http://Cisco.com).

## Tested Windows Security Patches

Cisco Systems officially supports and encourages the installation of all Microsoft security patches for Windows 2000 Server and Windows Server 2003 as used for ACS for Windows.

Cisco experience has shown that these patches do not cause any problems with the operation of ACS for Windows. If the installation of one of these security patches does cause a problem with ACS, please contact Cisco TAC and Cisco will resolve the problem as quickly as possible.

ACS for Windows has been tested with the Windows Server 2003 patches documented in the following Microsoft Knowledge Base Articles:

- 819696
- 823182
- 823559
- 824105
- 824141
- 824146
- 825119
- 828028
- 828035
- 828741
- 832894
- 835732
- 837001
- 837009
- 839643
- 840374

ACS has been tested with the Windows 2000 Server patches documented in the following Microsoft Knowledge Base Articles:

- 329115
- 823182
- 823559
- 823980
- 824105
- 824141
- 824146
- 825119
- 826232
- 828035
- 828741
- 828749
- 835732
- 837001
- 839643

## Security Advisory

Cisco issues a security advisory when security issues directly impact its products and require action to repair. For the list of security advisories for Cisco Secure on [Cisco.com](http://www.cisco.com), see the *Cisco Security Advisory: Multiple Vulnerabilities in Cisco Secure Access Control Server* at:

[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

## Known Problems

The following problems are known to exist in this release:

- [Cisco AAA Client Problems, page 10](#)
- [Known Microsoft Problems, page 10](#)
- [Known Problems with ACS 4.0, page 10](#)

## Cisco AAA Client Problems

Refer to the appropriate release notes for information about Cisco AAA client problems that might affect the operation of ACS. You can access these release notes online at [Cisco.com](http://www.cisco.com). For NAC-specific client problems, go to <http://www.cisco.com/go/NAC>.

## Known Microsoft Problems

Due to a defect in the Microsoft PEAP supplicant provided in the Windows XP Service Pack 2, the PEAP supplicant cannot reauthenticate successfully with ACS. Cisco has opened case SRX040922603052 with Microsoft on this issue. Customers who are affected by this problem should open a case with Microsoft and reference this case ID. Microsoft has prepared hotfix KB885453, which resolves the issue.

When ACS runs on a domain controller and you need to authenticate users with a Windows user database, you must take additional configuration steps; see the *Installation Guide for Cisco Secure ACS for Windows, 4.0* for post-installation steps regarding NTLM. A Microsoft hotfix may be required, depending on your configuration.

## Known Problems with ACS 4.0

[Table 2](#) contains problems known to exist in ACS 4.0.

Table 2 Known Problems in ACS 4.0

Bug ID	Summary	Explanation
CSCsc49673	UPGRADE:Add Filter aaa:service=ip_admission to Upgrade-Profile NAP	<p><b>Symptom</b> After upgrading from ACS 3.3 that included a NAC database, a profile is created with an authorization method: PEAP - posture only. This profile does not have a filter, which will cause failure of all incoming authentications except from PEAP-POSTURE.</p> <p><b>Workaround</b> Add a filter of Cisco-av-pair <code>aaa:service = ip_admission</code> to the Upgrade-Profile. The no-posture requests will be authenticated against the global settings configuration (if you ensure the <b>Grant access using global configuration, when no profile matches</b> option is selected in the created profile).</p>
CSCsc43287	Replication: Admin Control > Access Policy. Port allocation not replicated.	<p><b>Symptom</b> After replication of interface security settings, the HTTP port allocation settings in Admin Control &gt; Access Policy were not replicated (remained default - allow any).</p> <p><b>Workaround</b> Ensure that the HTTP access policy is set correctly on the slave GUI.</p>
CSCsc41860	<b>CSAuth</b> fails when you use <b>CSUtil</b> to delete over 10,000 AAA clients concurrently.	<p><b>Symptom</b> A large amount of AAA clients were imported to an ACS server. Then <b>CSUtil</b> import was used to delete 35,000 devices. After deleting the AAA clients, <b>CSAuth</b> failed.</p> <p><b>Conditions</b> This defect can occur on a clean installation.</p> <p><b>Workaround</b> When deleting a large number of AAA clients, you can use <b>CSUtil</b> to delete them in batches of up to 10,000 AAA clients concurrently.</p>
CSCsc41673	<b>CSAuth</b> fails after importing an Airespace NAS.	<p><b>Symptom</b> The <b>CSAuth</b> service occasionally fails after being restarted if <b>CSUtil</b> was running immediately beforehand; for example when running <b>csutil -i</b>.</p> <p><b>Conditions</b> Starting <b>CSAuth</b> immediately after <b>CSUtil</b> has run an import causes an exception in <b>CSAuth</b> due to a race condition in the <b>CSAuth</b> internal initialization sequence. This problem is particularly noticeable if using <b>CSUtil</b> to stop <b>CSAuth</b>, perform some action, then automatically restart <b>CSAuth</b>.</p> <p><b>Workaround</b> Restart <b>CSAuth</b> manually from the Control Panel, or wait for CSMon to detect the scenario and automatically restart <b>CSAuth</b>.</p>
CSCsc41638	ACS does not check if the CA certificate that was issued to a user exists in the CTL.	<p><b>Symptom</b> A user that 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>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc41623	Configuring Logs - Reset Columns erroneously populates selection lists.	<p><b>Symptom</b> For several report types, <b>Reset Columns</b> on the ACS web interface Logging configuration page sets the selected attributes to log (columns) to a different set of <b>Logged Attributes</b> than the actual default attributes, initially set on a fresh ACS installation.</p> <p><b>Conditions</b> In ACS, when you configure the logged information through the ACS web interface by clicking on System Configuration &gt; Logging and choosing one of the listed reports, the Reset Columns sets the selected attributes in the Selected Attributes list box to an incorrect set of attributes.</p> <p>This action occurs on the following reports:</p> <ul style="list-style-type: none"> <li>• CSV Failed Attempts</li> <li>• CSV Passed Authentications</li> <li>• CSV VoIP Accounting</li> </ul> <p><b>Workaround</b> Select and deselect attributes in the <b>Logged Attributes</b> list manually from the provided Attributes list.</p> <ul style="list-style-type: none"> <li>• <b>CSV Failed Attempts</b>—Remove the <b>Filter Information</b></li> <li>• <b>CSV Passed Authentications</b> —Add the <b>Cisco-av-pair</b> attribute</li> <li>• <b>CSV VoIP Accounting:</b> <ul style="list-style-type: none"> <li>– Add the <b>Call Leg Setup Time</b> attribute</li> <li>– Add the <b>Gateway Identifier</b> attribute</li> <li>– Add the <b>Connection Id</b> attribute</li> <li>– Add the <b>Call Leg Direction</b> attribute</li> <li>– Add the <b>Call Leg Type</b> attribute</li> <li>– Add the <b>Call Leg Connect Time</b> attribute</li> <li>– Add the <b>Call Leg Disconnected Time</b> attribute</li> <li>– Add the <b>Call Leg Disconnected Cause</b> attribute</li> <li>– Add the <b>Remote Gateway IP Address</b> attribute</li> </ul> </li> </ul>
CSCsc41129	<b>CSAuth</b> exceptions during EAP-TLS stress versus LDAP external database with SSL connections.	<p><b>Symptom</b> After a heavy load for a few hours of EAP-TLS authentications with an LDAP external database and LDAP connections over SSL (Trusted Root CA option), <b>CSAuth</b> may experience exceptions and fail.</p> <p><b>Workaround</b> Restart ACS services.</p>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc40001	Session resume in EAP-FAST-TLS does not work.	<p><b>Symptom</b> EAP-TLS inside EAP-FAST always assumes that the user is trying to authenticate for the first time, resulting in going to the external DB (if valid) to get the user credentials, instead of permitting the user to resume a previously used TLS session.</p> <p><b>Conditions</b> EAP-TLS as the inner method in EAP-FAST.</p> <p><b>Workaround</b> None.</p>
CSCsc39979	When a Network Access Profile (NAP) is being updated, all dynamic users related to the NAP are deleted from the logged in user list. The internally defined users are not deleted.	<p><b>Workaround</b> None</p>
CSCsc32154	Upgrading from 3.3 removed APT, SPT, and Reason from Logged Attributes.	If one or more of the APT, SPT, and Reason attributes were selected to be logged in the Failed or Passed reports in ACS 3.3, they will not appear in the Logged Attributes column after upgrading to 4.0.
CSCsc27168	User authentication succeeds even though a database is not selected.	<p><b>Symptom</b> If the external database list in NAP authentication settings is empty, access requests that match the NAP are authenticated in the ACS internal database.</p> <p><b>Workaround</b> Before deleting the external database configuration be sure that it is not used in any NAP.</p>
CSCsc27158	There is a memory leak during LDAP stress - PAP authentication with legacy LDAP SSL connections.	<p><b>Symptom</b> A memory leak was found during stress tests of PAP authentications with LDAP server (OpenLDAP) and legacy SSL enabled (<i>cert7.db</i> file). For example, memory usage reached 100MB after ~1.5 million authentications.</p> <p>Memory was freed after ACS services were restarted.</p> <p>No memory leak was found when the configuration was changed to use the new SSL mechanism (select Trusted Root CA).</p> <p><b>Workaround</b> In the Generic LDAP configuration in ACS, use the new SSL option (Trusted Root CA), instead of the old option (<i>cert7.db</i> file).</p>
CSCsc06942	Script interface fails the 1K limit at the layer 2 level.	<p><b>Symptom</b> Script interface fails the 1K limit at layer 2 level.</p> <p><b>Conditions</b> This issue is relevant only for non fragmented messages in tunneled protocols (MS-PEAP, CISCO-PEAP, and EAP-FAST). Unfragmented tunneled EAP messages should not exceed the total length of 1002 bytes.</p> <p><b>Workaround</b> Set the supplicant size fragmentation threshold to be lower than 1002 bytes. If it cannot be configured, another option is to set the MTU size that affects this value.</p>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc00788	Password change is not supported in GTC against Windows DB.	<p><b>Symptom</b> Password change is not supported in EAP-GTC against Windows database.</p> <p><b>Conditions</b> EAP-GTC authentication of user in Windows database whose account has expired or needs changed.</p> <p><b>Workaround</b> None.</p>
CSCsb95897	ACS cannot display a long list of disabled accounts correctly.	The ACS web interface has problems in displaying disabled accounts lists if they contain several pages. <b>Next</b> is working as needed, but <b>Previous</b> is available only once.
CSCsb72286	ACS RADIUS proxy uses RADIUS 1645, not current 1812.	<p><b>Symptom</b> ACS for Windows uses port 1645 for RADIUS authentication and authorization proxy to another RADIUS server. Some AAA servers may only accept connections to port 1812.</p> <p><b>Workaround</b> None</p>
CSCsb48683	Log and accounting file locking causes problems with backup software.	<p><b>Symptom</b> ACS diagnostic and accounting log file locking results in service problems when the directories are backed up by certain software applications (in reported case, Veritas software was used).</p> <p><b>Workaround</b> Upgrade your backup software.</p>
CSCsb25151	When a AAA client has multiple IP addresses, NAF for downloadable ACLs fail.	<p><b>Symptom</b> When a single AAA client configured with a range or list of IP address in ACS solution engine, the Network Access Filter (NAF) under Shared Profile Components cannot correctly determine the IP address of either the Network Device Group (NDG) or the correct IP address of the AAA client.</p> <p><b>Conditions</b> Must have Network Access Filtering defined and must have multiple IP addresses listed under the AAA client configuration section (under Network Setup) for the AAA client that is supposed to receive the downloadable ACL.</p> <p><b>Workaround</b> Perform one of the following:</p> <ul style="list-style-type: none"> <li>Remove all but the correct IP address from the AAA client configuration component for the NAS/NAD.</li> <li>Configure <code>ip radius source interface</code> to point to the correct IP address.</li> </ul>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCsb15116	The Apply and Restart button in NAP page does not release the NAF policy.	<p><b>Symptom</b> When deleting a Network Access Filter, which is used in a Network Access Profile setup page, an unexpected behavior occurs and authentications fail.</p> <p><b>Workaround</b> Perform one of the following:</p> <ol style="list-style-type: none"> <li>1. Before deleting a Network Access Filter, remove it from the relevant Network Access Profiles.</li> </ol> <p>or</p> <ol style="list-style-type: none"> <li>2. After deleting a Network Access Filter for each relevant Network Access Profile, click <b>Submit</b> (without performing changes) in the profile setup page.</li> </ol>
CSCsa79327	Authentications fail for users that contain the euro symbol in their password.	<p><b>Symptom</b> Authentication fails for users that contain the euro symbol in their password.</p> <p><b>Workaround</b> Remove the euro symbol from the user password.</p>
CSCeh79954	EAP-TLS time of day restriction in AD does not fail user; authentication succeeds.	<p><b>Symptom</b> EAP-TLS authentication of users in Windows Active Directory will still pass when a user's time-of-day setting (located in AD) is outside the hours they are allowed. ACS does not generate an error.</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>
CSCeh68821	LDAP authentication passes after modifying the subtree node due to DN caching.	<p><b>Symptom</b> If you change the User Directory Subtree in the Common LDAP Configuration, users that already authenticated by using this Generic LDAP instance (External User Database) are not affected and will continue to pass authentication; even if users are no longer under the new User Directory Subtree. ACS does not perform a new search for the users because of the user-cached Distinguished Name.</p> <p><b>Workaround</b> If you want to enforce a new search on the User Directory Subtree, delete the users from the ACS internal database.</p>
CSCeh64162	Supplicant attempts to authenticate by using UPN format and failure results.	<p><b>Symptom</b> If a supplicant attempts to authenticate by using EAP-FAST and supplies the username in UPN format (<i>user@domain.com</i>) and the username before the at sign (@) is different to the pre-Windows 2000 name, then ACS may not be able to locate the user in Active Directory.</p> <p><b>Conditions</b> ACS installed in Windows 2000/2003 Active Directory environment. Authentication with EAP-FAST and UPN usernames.</p> <p><b>Workaround</b> Rename the user to have the same username as pre-Windows 2000 one.</p>

Table 2 Known Problems in ACS 4.0 (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. ACS does not generate an error message.</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>
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. ACS does not generate an error message.</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>
CSCeh37907	Duplicate IP assignment due to accounting packets reordering.	<p><b>Symptom</b> Address assignment from IP pools is based on Accounting Start/Stop records. A duplicate IP address might be assigned to a user if an Accounting Stop packet is received out of order following a new access request by the same user. If ACS receives a late Stop packet, it might erroneously mark an IP address as free even though it has just been assigned. That might lead to a duplicate address assignment during the next connection.</p> <p>Such situations can happen in DSL environments where a router starts new PPP connections in less than 1 second after a previous disconnection.</p> <p><b>Workaround</b> There is no work around.</p>
CSCeh35121	Local logging stopped working after ODBC logging removed.	<p><b>Symptom</b> ODBC logging is enabled for passed and failed attempts. The ODBC data source is incorrect. After removing ODBC logging, only local logging remained; but no local logging is written.</p> <p><b>Conditions</b> ODBC data source must be incorrect.</p> <p><b>Workaround</b> Specify the correct ODBC data source for logging and restart ACS.</p>
CSCeh24979	Users fail to authenticate when upgrading and attempting to access an obsolete (no longer used) database.	<p><b>Symptom</b> When upgrading from ACS V.3.1 or later to ACS V.4.0 (these are 2 step upgrades), if a user is trying to authenticate to a database which was in use before the upgrade but not in use after the upgrade, the user will fail to authenticate. This information will be reported in the Failed Attempts log.</p> <p><b>Workaround</b> Select <b>User Setup</b> and then select <b>Remove Dynamic Users</b> after upgrading.</p>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCeh10491	Authentication errors on timeout waiting for local logging.	<p><b>Symptom</b> Authentication takes a lot of time when ACS is configured to log on remote ACS or to ODBC and the remote server, the ODBC data source is unreachable. When all worker threads are used; ACS provides no more authentications.</p> <p><b>Conditions</b> The remote ACS or ODBC data source is unreachable.</p> <p><b>Workaround</b> Make the remote server and ODBC data source available for logging or disable logging to it in the ACS configuration</p>
CSCeh00074	GUI LDAP group mapping submission failure.	<p><b>Symptom</b> When adding LDAP groups to be mapped to ACS groups, the Submit operation sometimes fails and an empty list error message appears.</p> <p><b>Conditions</b> This might occur when working on the ACS web interface from a remote machine (for example, with Terminal Services) or from other group mapping pages.</p> <p><b>Workaround</b> Move to another window from the Group Mapping page, before you click <b>Submit</b>, or click on another frame in the ACS web interface.</p>
CSCeg50237	Overinstall causes the added AVP Attributes to disappear.	<p><b>Symptom</b> Adding AVP attributes and then performing an overinstall causes those attributes to disappear from the Log Attribute field.</p>
CSCeg47441	CRL is not preserved when upgrading from ACS 3.3.2 or below to ACS 3.3.3 or higher.	<p><b>Symptom</b> When upgrading from ACS 3.3.1.16 to ACS 3.3.3.2, the CRL entries are not transferred.</p> <p><b>Workaround</b> Create the CRL entries manually.</p>
CSCeg40355	Authentication failures occur when remote logging fails.	<p><b>Symptom</b> If an ACS server that is configured for remote logging fails to successfully transmit an accounting log to the remote server, authentication attempts to this ACS server during this time may fail. The authentication failure may not be reported at all; or, it may be reported incorrectly (as being successful).</p> <p>The <i>auth.log</i> file may have output similar to this during an authentication failure:</p> <pre>AUTH 10/13/2005 10:29:55 E 0552 19568 Timeout waiting for ack from CSlog [logger name] AUTH 10/13/2005 10:29:55 E 0559 19568 Closing CSlog connection to [logger name] AUTH 10/13/2005 10:29:55 E 0574 19568 Re-sending packet to CSLog [logger name] AUTH 10/13/2005 10:29:55 E 0546 19568 -ve ack from CSLog [logger name] AUTH 10/13/2005 10:29:55 E 0499 19568 Failed to log accounting packet to logger [logger name]</pre> <p><b>Workaround</b> Disable the remote logging functionality or correct the cause of the logging failure.</p>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
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; there is no workaround.</p>
CSCef85314	Group DACL is downloaded if users content NAF is not suitable.	<p><b>Symptom</b> If a user attempts authentication to the device that is not part of the NAF specified on the user's DACL content, the ACL of the group to which the user belongs is downloaded to the device; instead of rejecting the download.</p>
CSCef85310	Group DACL is downloaded if users DACL content is empty.	<p><b>Symptom</b> It is possible to define an ACL with 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, then the ACL of the group is downloaded to the device instead of the user's. (While the user's DACL content is not empty, it is downloaded to the device, as it should).</p> <p><b>Workaround</b> Do not define an empty downloadable ACL.</p>
CSCef55730	ACS authorization passes even for a disabled user.	<p><b>Symptom</b> The default administrative user account defined within the CiscoWorks local (user) database (and replicated within ACS TACACS+ user database) is granted access to all installed Management Center applications, even if the user account is disabled within ACS.</p>
CSCef12461	Restoration on Windows 2000 with many administrators does not restore them.	<p><b>Symptom</b> When ACS contains a big database with 500 or more administrators, after restoring the dump file on Windows 2000, the ACS administrators are not restored.</p> <p><b>Workaround</b> Manually create administrators after restore.</p>
CSCee64596	During stress tests, ACS does not reduce the size of the CSAdmin file based on the Service Control settings.	<p><b>Symptom</b> Intensive use of the Logged-In Users report may lead to significant memory utilization by the CSAdmin service.</p> <p><b>Workaround</b> Restart the CSAdmin service.</p>
CSCec72911	Windows 2003 password aging page display issue.	<p><b>Symptom</b> ACS is installed on Windows 2003 Server and the password-aging feature is enabled. Only the <b>generate greetings for successful logins</b> option in Password Aging settings is checked. After pressing <b>Submit</b> or <b>Submit + Restart</b>, 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, the errors active canceled or the page cannot be displayed appear.</p> <p><b>Conditions</b> Occurs after installing 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 Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCeb78551	When handling an LEAP RADIUS proxy between a front-end ACS server and a back-end ACS server, problems arise if the configuration is not correct.	<p>The LEAP Server (back-end ACS Server) must contain an AAA Client entry of the LEAP Proxy Server (front-end ACS Server) and it must be set to use <b>RADIUS (Cisco IOS/PIX 6.0)</b>.</p> <p>The LEAP Server (back-end ACS Server) must be set to use the RADIUS (Microsoft) [026/311/012] MS-CHAP-MPPE-Keys attribute in <b>Interface Configuration</b> and in Group or User Settings (depending on the profile used).</p> <p>This setting is required to communicate MS MPPE keys, which LEAP uses, between the Proxy LEAP Server (front end ACS Server) and the Proxy Server (back end ACS Server).</p> <p>This sort of communication is encapsulated in Cisco VSA and this is the reason why the AAA Client must be RADIUS (Cisco IOS/PIX 6.0).</p>
CSCea91690	Event Viewer errors on startup and shutdown in .NET	<p><b>Symptom</b> On Windows .NET Server 2003 or Windows 2003 Enterprise Edition shutdown and startup, you may see errors that falsely indicate that ACS service have failed. At startup, you may see a dialog box that indicates that a service, such as CSLog, encountered a problem and will close. The same error logged to Event Viewer, as in the following example:</p> <pre>Reporting queued error: faulting application CSLog.exe, version 0.0.0.0, faulting module unknown, version 0.0.0.0, fault address 0x00000000.</pre> <p>The problem is that, in Windows Server 2003, the Service Manager queries the ACS services status during startup and shutdown; but ACS services may not have started yet or may have stopped already. Even though this is normal behavior for ACS services, Windows perceives this as an error and logs it to the Event Viewer.</p> <p>On startup, the user sees all errors from the Event Viewer, which is why, when users logs into Windows right after startup, they see errors from the previous login session.</p> <p>This behavior observed on Windows Server 2003 only.</p> <p><b>Workaround</b> Verify that ACS services are running by using the Control Panel.</p>
CSCsc69976	Local logging file size and days are not displayed correctly after performing an additional action in the graphic user interface.	<p><b>Symptom</b> While changes are applied and in use correctly, default values are displayed after selecting Submit instead of the new values.</p> <p><b>Workaround</b> There is no workaround.</p>
CSCsc43577	CSAdmin stalls and has a memory leak.	<p><b>Symptom</b> CSAdmin consumes memory when updating EAP-FAST inner method GTC to MSCHAPv2, using the Network Access Profile page.</p> <p><b>Workaround</b> Restart the CSAdmin service.</p>

Table 2 Known Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCsb93223	An internal posture validation policy is created even though a template profile cannot be configured.	<b>Symptom</b> If for any reason you cannot create a profile (for example, Global Authentication Setup is not configured properly) using the NAC 802.1x template, an internal posture validation policy is created in any case.
CSCsc57975	The database order inside a Network Access Profile may cause authentication to fail and provide an erroneous error.	<b>Symptom</b> When a user account in the Windows AD has expired, the user may be authenticated in another external database, which is configured sequentially after the Windows database in the authentication settings in the matched NAP. If the user exists in another database, authentication is successful. If the user does not exist in another database, an erroneous failure code "CS user unknown" (instead of "Database account expired") is displayed.
CSCsc95237	ACS Services do not start after upgrading from 3.x to 4.0.1	<b>Symptom</b> During an upgrade to 4.0 attempt, the services would not start post-upgrade. This is due to trailing spaces in the ACS 3.x host IP configuration. ACS 4.0 does not allow trailing spaces in the host IP configuration.  <b>Workaround</b> After upgrading and installing 4.0, if the services do not start ,please call TAC to request a Post-Upgrade Utility to fix the problem.
CSCsc72958	ACS documentation does not indicate that IP NAR requires attribute 31.	IP-based NAR filters work only if ACS receives the Radius Calling-Station-Id (31) attribute. The Calling-Station-Id (31) must contain a valid IP address. If it does not, it will fall over to DNIS rules. This requirement was not specified in the documentation.
CSCsc69976	Local logging file size and days are incorrectly displayed after change.	<b>Symptom</b> When selecting <b>System Configuration &gt; Logging</b> , after you select one of the local logging configurations, in the <b>Log File Management</b> section, there is a check box marked " <b>Manage Directory</b> ". If checked, you can select to " <b>Keep only the last N files</b> " or " <b>Delete files older that N days</b> ". If either of these numbers are changed, the actual underlying value is correctly modified, however, when you return to this page the original value of 7 will still be displayed.  <b>Conditions</b> This happens whenever the number of files or number of days is modified.  <b>Workaround</b> After you change or enter a new value for the number of files, or the file age and press <b>Submit</b> , perform the following steps to see the correct value:  a. Navigate back to the page. b. Enter an invalid value (such as -1). c. Press Submit. This should produce a validation error . d. Press Cancel and navigate back to the page.  The correct value should appear."

# Resolved Problems

Table 3 contains the problems from the ACS 4.0 release that are resolved. Check the Bug Navigator on Cisco.com for any resolved bugs that may not appear here.

**Table 3** Resolved Problems in ACS 4.0

Bug ID	Summary	Explanation
CSCeh91809	VoIP messages cause the <b>CSRADIUS</b> service to unexpectedly terminate	<b>CSRADIUS</b> no longer terminates unexpectedly.
CSCeh46130	Replication timeout causes <b>CSAuth</b> restart without any error in ACS reports	Replication on Windows 2003 works without <b>CSAuth</b> problems and logs are correct.
CSCeh25112	Network Access Filter (NAF) reedit requests restart	After editing NAF data, ACS web interface now displays a message after you click <b>Submit</b> and Restart to restart the services.
CSCeh09266	Errors occurs while installing ACS on a directory with special characters	The percent sign (%) that caused the problem with ACS installing correctly is fixed in ACS 4.0.
CSCeg51873	ACS chooses wrong NDG for NAR with TACACS or RADIUS NAS on same IP	ACS no longer chooses the wrong NDG for NAR matching if both a TACACS+ and RADIUS NAS are defined with the same IP, and placed in separate NDGs and the authentication is performed via RADIUS.
CSCef67002	Documentation of multiprocessor and dual processor support inaccurate	Text has been updated in the ACS 4.0 installation guide.
CSCee88908	CSLog fails if a logged attribute is deleted due to replication	The CSLog works as expected after replication.
CSCee88831	days-since-last-update operator should compare to GMT	ACS displays date and time correctly in logs and reports.
CSCee85046	ODBC logger cannot log attribute with name > 32 chars	ODBC logging can be an imported NAC attribute that has more than 30 characters (vendor name + application name + attribute name). Maximum log name of the attribute is now set to 128 characters.
CSCed83648	Renaming an NDG removes it from the Selected Items of NAF HTML page	A pop-up window has been added to confirm deletion.
CSCee83977	A change in the NAF is not valid until the services are restarted	Changes in the NAF configuration take affect without restarting ACS services.
CSCee83677	NAC attribute type change can cause NAC GUI error	NAC errors no longer occur after an administrator changes the type of an existing NAC attribute by using the <b>CSUtil</b> (or because of backup and restore).
CSCee81203	In SQL, the DataType of integer is different than the integer that ACS displays.	There are no datatype errors in ACS or SQL.
CSCee81070	ACS install fails if installing on machine with running Remote Agent	The ACS 4.0 installation no longer fails if the ACS Remote Agent is already installed.
CSCee77099	The navigation bar (buttons) disappears after exiting from the Global Authentication Setup page	The navigation bar (button bar on the left) in the ACS web interface appears successfully after exiting from the Global Authentication page.

**Table 3** *Resolved Problems in ACS 4.0 (continued)*

Bug ID	Summary	Explanation
CSCee73004	CSLog handles reach more than 11,000 after failed ODBC connections	The CSLog handles failed ODBC connections successfully.
CSCee68644	SPC type created by EMBU DLL returns errors in Name field	Name field limitation of 31 characters defined. Error messages no longer appear.
CSCed93251	Fail to locate ACL for updating when ACL uses the same name as NAF	NAFs with the same name no longer cause problems.
CSCee58593	CSAdmin restart during Replication between two ACS SW in slow link	Replication between two ACSs in a slow link (128k) works successfully.
CSCed42439	Active Directory via LDAP - Group Mappings skip first group	Database group mappings are now correct.
CSCec89440	Unable to edit some of the disabled accounts.	All Disabled Accounts report errors are fixed.
CSCec61110	Authentications on a secondary ACS may fail after replication.	In environments where primary and secondary ACS servers are kept in sync by using the replication feature, user authentications no longer fail for users who are defined in an external database and the Failed Attempts log no longer contains an external DB not configured error.
CSCeb16968	ACS shared profile components disappear with XML error messages.	Shared profile component errors no longer occur during upgrades from ACS 3.2.3 to ACS 4.0.
CSCeb51393	Multi-admin needs to be able to add, edit, and delete downloadable ACLs.	No conflicts exist when multiple administrators try to add, edit, and delete downloadable ACLs under the shared profile components.
CSCea74289	Cascade replication due to user password changes do not work.	Cascade replication with password changes replicates successfully.
CSCea91947	ACS does not authenticate Windows 2000 users when NTLMv2 is enabled on the network	ACS now supports NTLMv2.
CSCeh93481	NAF is selected automatically after deleting and creating with the same name	This problem has now been solved.
CSCsc52660	UCP 4.0 on Windows 2000 or Windows 2003 may cause a CGI error.	The problem with the ACS User Changeable Password feature that operates as a CGI in IIS, under Windows 2000 SP4 (IIS 5.0) or Windows 2003 SP1 (IIS 6.0) has been fixed. Use the latest version of UCP downloadable from CCO at: <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des">http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des</a>

## Documentation Updates

The following errors exist in the ACS online help:

- The ACS documentation and short help indicate that you can disable the dynamic user cache, which is incorrect.
- The information in the Accounting Logs in the ACS Online Help contains an error. It should read:

By default, these logs are available in CSV format, with the exception of the Passed Authentications log. You can also configure ACS to export the data for these logs to an ODBC-compliant relational database that you configure to store the log data.

The note for Passed Authentications in the Accounting Log Descriptions table is incorrect and should be disregarded.

The corresponding information in the ACS documentation on Cisco.com is correct.

- The information for the *url-redirect-acl* variable in the Cisco Secure ACS User Guide for Windows Network Access Profiles chapter is incorrect. The *url-redirect-acl* value can only be the switch ACL name. A number is not acceptable.
- The short help for the External Posture Validation Audit Server Setup incorrectly states:

You then configure posture validation credentials that a NAC Agentless Host (NAH) forwards to the primary audit server or, in a failover scenario, to the secondary audit server.

However, you cannot configure the posture validation credentials that a NAH forwards. The sentence is correct only for NAC external posture validation servers, and not for Audit Servers.

- The minimum Microsoft IIS version required for the User Changeable Password (UCP) Web Server for ACS for Windows Server is Microsoft IIS 5.0. The information is correct in the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords*; however, Table 1-3 of the *Installation Guide for Cisco Secure ACS for Windows* contains an error.

- In the section on ACS Attributes and Action Codes, it incorrectly states:

```
TACACS Attributes: 160, 162
RADIUS Attributes 170, 173
```

It should read the other way around:

```
RADIUS Attributes: 160, 162
TACACS Attributes 170, 173
```

- In the section on downloadable IP ACLs, it incorrectly states that the description of a new IP ACL can be up to 30000 characters. The maximum number of characters allowed in the Description field is 1006 characters.
- Omissions from ACS documentation include:
  - We do not support distributed ACS deployments in a NAT environment. If a primary or secondary address is in NAT format, the database replication file will indicate shared secret mismatch. The next release of the documentation will address this omission.
  - The Logged-In Users report takes up to 20 seconds to open. All other reports are opened instantly when selected. Specific user information takes several minutes to appear; see CSCsb74228.
  - LEAP is not supported when working with Network Access Profiles. You can use LEAP only if your system is operating in legacy ACS mode.
  - The ODBC Passed Authentications is not documented in the short help file in the **System Configuration > Logging Configuration** page. You can click this option to enable and configure ACS to generate an ODBC log of successful login attempts.
  - When creating a package.cab file that is larger than 2GB, additional .cab files are created due to the size limit of the packer. The sequence is as follows: the first package name is: package.cab, the second: package1.cab, and so on, until the N package: packageN.cab, where N is the number of packages minus one. The files are saved in the same location that is specified

before the packing begins. These files are not stand-alone and all of them must be sent to package. Problems with the packed file (package.cab) may arise if there is not enough hard-disk space.

- The backup procedure does not back up the cert7.db file. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery. When you migrate from an ACS server to ACS appliance, move the cert7.db to a ftp server and download according to the normal provisioning instructions. When you upgrade an ACS appliance, repeat the download procedure as originally used to provision the original appliance.

## Obtaining Documentation

Cisco documentation and additional literature are available on [Cisco.com](http://www.cisco.com). Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on [Cisco.com](http://www.cisco.com).

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- **Emergencies**—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- **Non-emergencies**—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the *Documentation Guide for Cisco Secure ACS for Windows* document.

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)

