



Release Notes for Cisco Secure ACS Solution Engine 4.0

March 2007

Full Build Numbers:

- 4.0.1.44 (1113-Quanta)
- 4.0.1.42 (1112-Quanta)
- 4.0.1.43 (1111-HP)

These release notes pertain to Cisco Secure Access Control Server Solution Engine release 4.0, hereafter referred to as ACS SE.

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 4.0.1.44 for Quanta (1113)
- 4.0.1.42 for Quanta (1112)
- ACS 4.0.1.43 for HP (1111)

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:

- [New and Changed Information, page 2](#)
- [Product Documentation, page 6](#)
- [Supported Databases, page 7](#)
- [Installation Notes, page 8](#)
- [Security Advisory, page 13](#)
- [Known Problems, page 13](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Resolved Problems, page 29](#)
- [Documentation Updates, page 31](#)
- [Obtaining Documentation, page 32](#)
- [Documentation Feedback, page 33](#)
- [Cisco Product Security Overview, page 34](#)
- [Obtaining Technical Assistance, page 35](#)
- [Obtaining Additional Publications and Information, page 36](#)

New and Changed Information

This section contains new and changed information for ACS SE 4.0:

- [New Quanta 1113 Platform, page 2](#)
- [New Hotfixes in ACS SE 4.0, page 2](#)
- [ACS Remote Agent for Windows, page 3](#)
- [SNMP Support and CSA Integration, page 3](#)
- [ACS New Features, page 3](#)

New Quanta 1113 Platform

The ACS SE 1113 release consists of a new hardware device that replaces the previous ACS SE 1112 device. The ACS SE 1113 device conforms to Reduction in Hazardous Substances (RoHS) directives of the European Economic Community (EEC)—Directive 73/23/EEC and Directive 89/336/EEC as amended by Directive 93/68/EEC.

New Hotfixes in ACS SE 4.0

The ACS SE base image contains the following Microsoft hotfixes:

- KB822831—BUG: Driver installation program does not install device drivers.
- KB823980—MS03-026: Buffer overrun in RPC may allow code execution.
- KB824105—MS03-034: Flaw in NetBIOS could lead to information disclosure.
- KB824146—MS03-039: A buffer overrun in RPCSS could allow an attacker to run malicious programs.
- KB828028—MS04-007: An ASN.1 vulnerability could allow code execution.
- KB828741—MS04-012: Cumulative Update for Microsoft RPC/DCOM.
- KB835732—MS04-011: Security Update for Microsoft Windows.
- KB893066—MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service.

For more information about these hotfixes, see the Microsoft website.

ACS Remote Agent for Windows

ACS Remote Agent for Windows is now supported on Japanese Windows 2000 and Japanese Windows 2003.

SNMP Support and CSA Integration

The following features were introduced in ACS SE 3.3:

- Support for Simple Network Management Protocol (SNMP).
- Integration of Cisco Security Agent in the ACS SE base image.

These features are described in the *User Guide for Cisco Secure ACS Solution Engine*.

ACS New Features

ACS contains the following new and changed features:

- **New RoHS Solution Engine platform.** The ACS SE 1113 release consists of a new hardware device that replaces the previous appliance hardware device (the ACS SE 1112 device). The ACS SE 1113 device conforms to Reduction in Hazardous Substances (RoHS) directives of the European Economic Community (EEC)—Directive 73/23/EEC and Directive 89/336/EEC as amended by Directive 93/68/EEC.
- **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 third-party audit vendors to audit hosts without the appropriate agent technology 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 5](#).
- **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 Virtual Private Network (VPN) access.
- **New storage infrastructure**—ACS now uses an 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 by using a hash of customer-provided password and an internal password. You can use the ACS SE CLI to change the password.

- **LDAP improvements**—ACS caches successful external authentications (by using LDAP), allowing it to immediately look up a user during reauthentication. ACS provides improved SSL support. See [LDAP Improvements, page 5](#), 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, which is installed on Japanese Windows Operating System (JOS). This feature is 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.
- **NTLM support**—ACS can now operate with Windows NT LAN Manager (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.
- **Online documentation**—The online documentation for ACS Solution Engine opens in a separate window, and contains all the information in the *User Guide for Cisco Secure ACS Solution Engine*. You can search the online documentation by using the Search button, and you can open a PDF version of the user guide.

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
 - 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 called 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.
 - Cisco:Host:Package:Version-String.

For additional details, see [Support for Linux Packages in Posture Validation, page 6](#).

- **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. The three options from which to choose for validation are:
 - internal policies located in ACS
 - policies defined on external servers
 - 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.
 - This product release includes changes 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 Secure Sockets Layer (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 the 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;ethtool;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;telnet;tetex;utempter;vim;xchat;xemacs;xfree86;xloadimage;xpdf;zip

You can add or remove attribute packages in the NAC Attributes Management Page in the ACS SE web interface.

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

Product Documentation

Table 1 describes the product documentation for ACS SE 4.0.

Table 1 Product Documentation Details

Document Title and Description	Available Formats
<i>Documentation Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> • Printed document with the product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html • Orderable; see Ordering Documentation, page 33.
<i>Release Notes for Cisco Secure ACS Solution Engine</i> New features, documentation updates, known problems, and resolved problems.	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html

Table 1 Product Documentation Details (continued)

Document Title and Description	Available Formats
<p><i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i></p> <p>Details on ACS SE 1112 and ACS SE 1113 hardware and hardware installation, and initial software configuration.</p>	<ul style="list-style-type: none"> Orderable; see Ordering Documentation, page 33. PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
<p>Product online help.</p> <p>Help topics for all pages in the ACS HTML interface.</p>	Select an option from the ACS menu; the help appears in the right pane.
<p><i>User Guide for the Cisco Secure ACS Solution Engine</i></p> <p>ACS functionality and procedures for using the ACS features.</p>	<ul style="list-style-type: none"> Orderable; see Ordering Documentation, page 33. On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_list.html
<p><i>Supported Devices Table for the Cisco Secure ACS Solution Engine</i></p> <p>Supported devices and firmware versions for all ACS features.</p>	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_device_support_tables_list.html
<p><i>Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine</i></p> <p>Translated safety warnings and compliance information.</p>	<ul style="list-style-type: none"> Orderable; see Ordering Documentation, page 33. PDF on the ACS Recovery CD-ROM. Online: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
<p><i>Installation Guide for User-Changeable Passwords</i></p> <p>Installation and user guide for the user-changeable password add-on.</p>	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
<p><i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents</i></p> <p>Installation and configuration guide for ACS remote agents for remote logging.</p>	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html

Supported Databases

The various databases that ACS supports provide uneven support for the various password protocols that ACS SE supports for authentication.



Note

In the *User Guide for Cisco Secure ACS Solution Engine 4.0*, the tables that summarize database compatibility for the protocols that ACS supports state incorrectly that ACS SE supports ODBC databases. [Table 2](#) and [Table 3](#) correct this error.

[Table 2](#) specifies non-EAP authentication protocol support.

Table 2 *Non-EAP Authentication Protocol and User Database Compatibility*

Database	ASCII/PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2
ACS	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes
Windows AD	Yes	No	No	Yes	Yes
LDAP	Yes	No	No	No	No
ODBC	No	No	No	No	No
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes
All Token Servers	Yes	No	No	No	No

Table 3 specifies EAP authentication protocol support.

Table 3 *EAP Authentication Protocol and User Database Compatibility*

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	No	Yes
ODBC	No	No	No	No	No	No	No
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No

Installation Notes

This section provides information about installing and upgrading ACS SE and ACS Remote Agents:

- [Installing from the ACS SE 1111 \(HP\) Recovery CD, page 9](#)
- [Software Compatibility, page 9](#)
- [Upgrading and Migrating to ACS SE 4.0, page 9](#)
- [Tested Windows Security Patches for ACS Remote Agent, page 11](#)



Note

You should view ACS SE only via a console by using a serial port. We do not recommend using a monitor via the VGA port. If you use a monitor via the VGA port, you will see Windows error messages when starting ACS SE. You can ignore these messages and there is no need to reboot.

Installing from the ACS SE 1111 (HP) Recovery CD

When installing from the Recovery CD for ACS SE 1111 (HP), you might encounter the following issues:

- 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. If, after about an hour, the CLI Initial Configuration screen does not appear, switch off the appliance, and switch it on again. Refer to [CSCsc90467](#).
- After initial configuration ends, if you cannot access the web interface, use the CLI command, `reboot`, to restart the appliance. Refer to [CSCsd20149](#).



Note

These problems occur only on ACS SE 1111 (HP), after installing from the Recovery CD, when performing a full upgrade, including the appliance base image. If you are not upgrading the appliance base image, you do not need to install from the Recovery CD.

Software Compatibility

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

Upgrading and Migrating to ACS SE 4.0

You can upgrade your existing ACS SE appliance with the latest ACS software, appliance management software, and appliance base image. For detailed instructions see *Installation Guide for Cisco Secure ACS Solution Engine* on [Cisco.com](#).

You can migrate from an existing ACS SE appliance (ACS SE 1111 or 1112) to the ACS SE 1113 by making a backup of the installation on the existing hardware device (SE 1111 or 1112) and then performing a restore of the installation on the new hardware device (SE 1113).



Note

ACS Release 3.x is not supported on the SE 1113 platform.

If the existing ACS SE appliance has a previous software version, you must first upgrade the existing appliance to software version 4.0.

For detailed information, see Chapter 5 of the *Installation and Setup Guide for the Cisco Secure ACS Solution Engine*, “Upgrading and Migrating to Cisco Secure ACS Solution Engine.”

Upgrade Paths

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

- ACS SE release 3.3.3 to ACS SE release 4.0.
- ACS SE, release 3.3.2 to ACS SE 4.0.
- ACS SE, release 3.3.1 to ACS SE 4.0.

- ACS SE, release 3.2.3 to ACS SE 4.0.
- ACS SE versions before ACS SE 3.2.3, first upgrade to ACS SE 3.3.3, then to ACS SE 4.0. For information about upgrading to ACS SE 3.3.3, see *Release Notes for Cisco Secure ACS Solution Engine 3.3.3* on Cisco.com.

Migration Paths

ACS supports the migration path from ACS for Windows 4.0 to ACS SE 4.0. Before performing migration, you must first upgrade ACS for Windows to version 4.0.

The following migration paths have been tested and are supported:

- Upgrade ACS for Windows, release 3.0.4, via 3.3.3, to ACS for Windows, release 4.0. Migrate to ACS SE 4.0.
- Upgrade ACS for Windows, release 3.2.3, to ACS for Windows, release 4.0. Migrate to ACS SE 4.0.
- Upgrade ACS for Windows, release 3.3.1, to ACS for Windows, release 4.0. Migrate to ACS SE 4.0.
- Upgrade ACS for Windows, release 3.3.2, to ACS for Windows, release 4.0. Migrate to ACS SE 4.0.
- Upgrade ACS for Windows, release 3.3.3, to ACS for Windows, release 4.0. Migrate to ACS SE 4.0.

For ACS SE versions before ACS SE 3.2.3, first upgrade to ACS SE 3.3.3, then to ACS SE 4.0. For information about upgrading to ACS SE 3.3.3, see *Release Notes for Cisco Secure ACS Solution Engine 3.3.3* on Cisco.com.

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.

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 NAP, (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 ACS dynamically updates the posture-token Cisco-av-pair attribute at runtime, there is not need to configure it manually.
5. If you manually added posture validation attributes in ACS 3.3, they will be added to the ACS version 4.0 posture dictionary during the upgrade.

Tested Windows Security Patches for ACS Remote Agent

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 Remote Agent for Windows.

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

ACS Remote Agent 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

Documentation Updates

This section corrects errors and omissions in the ACS user documentation:

- [Supported Databases, page 12](#)
- [Replication with Different Send and Receive Configurations, page 12](#)
- [Submit and Apply Button Changed to Apply Button, page 12](#)

Supported Databases

In the *User Guide for Cisco Secure ACS Solution Engine 4.0*, the tables that summarize database compatibility for the protocols that ACS supports state incorrectly that ACS SE supports ODBC databases. [Table 2](#) and [Table 3](#) in [Supported Databases, page 7](#) correct this error.

Replication with Different Send and Receive Configurations

The user guide states that the primary ACS compares the list of database components that it is configured to send with the list of database components that the secondary ACS is configured to receive. If the secondary ACS is not configured to receive any of the components that the primary ACS is configured to send, the database replication fails.

The previous information is incorrect (bug CSCsg93907).

The primary ACS first synchronizes with the secondary ACS, and sends only the components that the secondary ACS is configured to receive. The primary ACS does not send components that the secondary ACS is not configured to receive, even if you configure the primary ACS to send those components. Thus, database replication does not fail when different send and receive configurations exist on the primary and secondary ACS.

Submit and Apply Button Changed to Apply Button

In several parts of the *User Guide for Cisco Secure ACS Solution Engine 4.0*, the documentation instructs the reader to click **Submit + Apply** to save and apply configuration changes. In release 4.0, the **Apply** button replaces the **Submit + Apply** button.

Click the **Apply** button to save and apply configuration changes.

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

Known Problems

The following problems exist in this release:

- [Cisco AAA Client Problems, page 13](#)
- [Known Microsoft Problems, page 13](#)
- [Known Problems with ACS 4.0, page 14](#)

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.

Known Problems with ACS 4.0

Table 4 contains problems known to exist in ACS SE 4.0.

Table 4 Known Problems in ACS SE 4.0

Bug ID	Summary	Explanation
Appliance-specific bugs		
CSCse04125	SNMP ports on the ACS SE 1113 can be assigned incorrect values.	<p>Symptom On the ACS SE 1113, deleting the default SNMP port value, adding characters instead of numbers to the SNMP port value, adding a port number greater than 65536, or adding an SNMP port that is already in use by the device can be performed without the appearance of any error message. In the previous release (ACS 3.3.3), the error message “The port number is in use or invalid” appears.</p> <p>Workaround Enter a correct SNMP port number that is not already in use by the device.</p>
CSCse03681	Entering a community string that begins or ends with a space does not result in an error message.	<p>Symptom Entering a community string that begins or ends with a space does not result in an error message. Instead the ACS system deletes the space without informing the user about it.</p>
CSCse01363	The appliance configuration page is not replicated when the system is migrated from the ACS SE 1112 device to the ACS SE 1113 device.	<p>Symptom Under certain conditions, the appliance configuration is not replicated when the system is migrated from the ACS SE 1112 to the ACS SE 1113.</p> <p>Conditions This occurs when a user performs the following sequence of steps:</p> <ol style="list-style-type: none"> 1. On the Master ACS (Quanta 4.0.1.42) accesses the Appliance Configuration page from System Configuration. 2. Enables NTP Synchronization and adds an IP address to the NTP Server. 3. Enables Cisco Security Agent. 4. Enables the SNMP Agent and changes the SNMP default Community and port, and then adds SNMP Agent Contact and Location. 5. Selects Accept SNMP packets from selected hosts and adds a host address. 6. Submits the changes. 7. The ACS SE 1112 is replicated to the ACS SE 1113.
CSCse01194	After system migration from ACS for Windows to the Solution Engine version on the ACS SE 1113, the existing HTTP configuration is not retained.	<p>Symptom If the Master ACS system (ACS for Windows 4.0.1.27) is configured for certain HTTP settings (the port ranges are changed to 60000-60005) and the system is replicated to the ACS SE 1113 version (4.0.1.44), the specified HTTP configuration settings are not retained on the ACS SE 1113 installation.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsd98589	When the Network Interface Card (NIC) is disconnected, authentication cannot be performed.	<p>Symptom If the NIC is disconnected from a previously configured and functioning appliance, the system is rebooted and then restarted, and the NIC is reconnected, authentications fail.</p> <p>Error messages similar to the following appear:</p> <pre>04/17/2006 22:01:52 Unknown NAS .. .10.56.60.115 quanta-new-5 .. No (Unknown)</pre> <p>Workaround Restart CSAuth. Then select System Configuration > Service Control and click the Restart button. This restarts CSLog, RADIUS, and TACACS+.</p>
CSCsd94022	Setting the system clock forward disrupts a scheduled backup process.	<p>Symptom If the system clock is set forward, for example, from 16:00 to 16:58, and a scheduled backup is configured to run during a later time period, for example, from 17:00 to 18:00, the scheduled backup might take a long time to complete or might not occur. This condition can occur when the system time is changed because of a switchover to Daylight Savings Time.</p>
CSCsd93818	When the ACS SE 1113 appliance is restarted, the CSAdmin service does not restart.	<p>Symptom If the CSAdmin service is stopped and the ACS SE 1113 device is rebooted, the CSAdmin service remains in the “stopping” state and does not restart. The GUI is not accessible.</p> <p>Workaround Reboot the appliance, and then restart the CSAdmin service. Then reboot again.</p>
CSCsd93779	When backup is set to run after a specified period, the backup does not run.	<p>Symptom When a large database is loaded from the SE 1111 release and system backup is configured to run after a specified period, for example, every 15 minutes, the backup process does not run.</p>
CSC92719	The NTP configuration is not restored after a system backup.	<p>Symptom When the ACS SE 1113 appliance is backed up, the NTP configuration is not retained.</p>
CSCsd91218	Under certain conditions when IP filtering is set during initial configuration, the specified IP filtering does not work.	<p>Symptom If during an initial configuration, IP filtering is set and the specified IP addresses are incorrect or are used by another ACS SE 1113 device, and the ACS SE 1113 is rebooted, the specified devices do not work; even if they are set manually by using the set ip command.</p>
CSCsd88833	Manual setup of IP configuration on the ACS SE 1113 appears to fail.	<p>Symptom On a newly installed ACS SE 1113 device, if IP configuration is performed manually by using the set ip command, the output from the command does not show the specified configuration. However, entering a show ip command shows the correct configuration. For example, if a valid IP address is entered by using the set ip command, a message similar to the following appears:</p> <pre>Use Static IP Address [Yes]: IP Address [0.0.0.0]: 10.56.60.114</pre> <p>However, entering a show ip command displays the correct IP address.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCse05502	The online documentation for the ACS SE 1113 states that the name of a downloadable IP ACL can contain up to 27 characters and cannot contain a backslash (\).	Symptom The name specified for a downloadable IP ACL can contain up to 32 characters and can contain backslashes (\). Entering a backslash (\) causes an error on the page. (See the description of CSCse05420.)
CSCse05463	The online documentation for the ACS SE 1113 states that the description field for a downloadable IP ACL can contain up to 30,000 characters.	Symptom The description can contain only 1,006 characters.
CSCse05420	Adding an illegal backslash (\) to the downloadable Access Control List (DACL) causes an <code>Error on page</code> message to appear.	Symptom The online documentation correctly states that the downloadable IP ACL name cannot contain a backslash character. However, the system allows you to enter a backslash (\) in the DACL name. No specific error message appears; however, an <code>Error on page</code> message appears at the lower left of the web page. This condition also occurs in the ACS for Windows 4.0 (4.0.1.27) release.
CSCse04244	CSAdmin crashes when fewer than 255 characters are added to an SNMP host address.	Symptom The CSAdmin utility should allow entering up to 255 characters in the SNMP host address field. However, CSAdmin sometimes terminates abnormally if a user enters a number of characters within this range.
CSCse08310	System performance is degraded when no dynamic users exist.	Symptom If the ACS internal database does not contain any users (is empty) and the system is configured to use Remote Agent for AD authentication, it takes a long time for the system to stabilize. This system instability is more prevalent when more complicated authentication protocols are used, for example, MS-PEAP, EAP-TLS, or PAP.
CSCsd20149	After installing from the ACS SE 1111 (HP) Recovery CD, you cannot access the web interface.	<p>Symptom This problem occurs on the ACS SE 1111 (HP), when performing a full upgrade including the appliance base image. When you log in to the CLI, the appliance status indicates:</p> <pre>pfpipmon not running.</pre> <p>Conditions This occurs on the ACS SE 1111 (HP), after installing from the Recovery CD, when performing a full upgrade, including the appliance base image.</p> <p>Note If you are not upgrading the appliance base image, you do not need to install from the Recovery CD.</p> <p>Workaround Use the <code>reboot</code> CLI command to restart the appliance.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc90467	After installing from the ACS SE 1111 (HP) Recovery CD, the CLI initial configuration screen does not appear.	<p>Symptom This problem occurs on the 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>Conditions On ACS SE 1111 (HP), when installing from the Recovery CD, when performing a full upgrade, including the appliance base image.</p> <p>Note If you are not upgrading the appliance base image, you do not need to install from the Recovery CD.</p> <p>Workaround Switch off the appliance, and switch it on again.</p>
CSCsc81981	CSAdmin crashed when editing the Remote Agent field after replication.	<p>Symptom After replication, if you edit the Remote Agent field in the Network Configuration page in the slave machine, the ACS displays the error message <code>Action canceled</code>.</p> <p>Workaround None.</p>
CSCsc80481	Proxy distribution table prevents SNMP from working.	<p>If you configure ACS SE for SNMP and check the Accept SNMP packets from selected hosts check box, and then add an entry to Proxy Distribution Table like: <code>@cisco.com -> local ACS -> strip -> local (Default) -> local ACS -> no strip -> local</code>, SNMP stops working and there are no more responses from ACS.</p> <p>Workaround Uncheck the Accept SNMP packets from selected hosts check box.</p>
CSCsc77508	Stress tests with EAP-TLS cause CSAuth to fail.	<p>During overnight EAP-TLS stress tests against CSDB with NAP and RAC, and a Certificate Revocation List (CRL) (30% of all certificates revoked), CSAuth failed a number of times.</p> <p>Workaround None.</p>
CSCsc77228	RSA token appears in the external User DB after upgrade from 3.2.3.	<p>Symptom If, in a previous version of ACS, you added RSA SecurID Token Server to the external user database, mapped it to a group, and selected this database in the Unknown User Policy section; then, after upgrading to ACS 4.0, the RSA SecurID Token Server still appears, even though all instances of it should be deleted in the external user database, not just from the database configuration.</p> <p>Moreover, the configuration in the RSA SecurID Token Server should be replicated in the RADIUS Token Server after the upgrade to 4.0.</p> <p>Workaround None.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc69997	Machine authentication fails on 2003 DC with binary comparison on.	<p>Symptom EAP-TLS machine authentication fails if only binary comparison is selected, and 2003 DC is used as the external database. There are no problems with user authentication.</p> <p>Workaround None.</p>
CSCsc52381	ACS SE console access may not work if NTP synchronization is enabled.	<p>Symptom The login prompt might not appear on the CLI console after rebooting through the CLI or through the GUI; even if NTP synchronization is enabled and the NTP server address is set correctly.</p> <p>Workaround Disable NTP synchronization.</p>
CSCsc03778	Access Policy changes made in Administration Control and replicated to another SE are not enforced unless the receiving SE is rebooted.	<p>Symptom If you make a change in the access policy under Administration Control and then replicate the change to another appliance, the changes are not enforced on the receiving appliance.</p> <p>Workaround On the receiving (secondary) appliance, do one of the following:</p> <ul style="list-style-type: none"> • Click Submit on the Access Policy page. • Reboot the secondary appliance.
CSCsc02553	GUI logging change does not affect CSadmin until server restarted.	<p>Symptom When a user changes the logging level for an ACS appliance by using the GUI, and clicks the Restart button, the CSadmin service is not restarted; therefore, the CSadmin logging level does not change until the CSadmin service is manually restarted.</p> <p>Workaround Restart the CSadmin service manually.</p>
CSCsb83399	ACS SE should save the FTP settings during software upgrade.	<p>Symptom The ACS appliance does not save the defined FTP settings during software upgrade; but, the defined backup scheduling is saved. This behavior causes a backup problem after software upgrade.</p> <p>Workaround Reenter the FTP information manually after an upgrade.</p>
CSCsb27597	Limitation on the custom attributes (of 31 KB as CSAdmin indicates).	<p>Symptom In the T+ Settings per User/Group Configuration page, which is accessed from the Interface Configuration page, if you add over 1,200 entries in the custom attribute field, the browser crashes.</p> <p>The custom attribute field is currently limited to 31 KB (which is around 1,200 attributes).</p> <p>Workaround None.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsb19051	TCP checksum error from Cisco Secure ACS Solution Engine 1111.	<p>Symptom An 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 may generate the following error message: <pre>%IP-3-TCP_BADCKSUM:TCP bad checksum.</pre></p> <p>This error is caused by the network interface card (NIC) software driver. Not every packet being transmitted is affected. Because TCP retransmits 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 be affected.</p> <p>This problem might also occur on an ACS SE 1112 (Quanta).</p> <p>Workaround A temporary workaround is to reload the server; but, because the problem is transient, it will likely recur within days or weeks.</p> <p>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 <i>TCP_checksum</i> patch for your platform.</p>
CSCsb13998	ACS dial-in authorization fails against Win2K active directory.	<p>Symptom When ACS is configured to obtain dial-in authorization from a Microsoft Active Directory user database, user authorization sometimes fails with the error: <i>User does not have dial-in permission (needed)</i>.</p> <p>This defect was found in an environment where Active Directory was being replicated from an NT domain. The same errors occurred when the remote agent was installed on a Member Server or a Domain Controller.</p> <p>Workaround The problem occurs because replication does not synchronize the <i>userParameters</i> and <i>msNPAllowDialin</i> attributes. See Microsoft KB article 252398 for a possible workaround (run a script to synchronize the attributes).</p>
CSCeh17104	Certain Hostname/Admin names cause loss of access.	<p>Symptom If the administrator name is same as the hostname, there is no GUI access or CLI access.</p> <p>Workaround Ensure that the administrator name is different from the hostname.</p>
CSCeh04327	SNMP <code>get</code> and <code>get-next</code> requests for <code>host.hrSystemNumUsers</code> return error.	<p>Symptom SNMP <code>get</code> and <code>get-next</code> requests for <code>host.hrSystemNumUsers</code> return <code>Generic error</code>.</p> <p>Workaround None.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCee89510	Dates are logged in local time instead of GMT.	<p>Symptom NAC attributes that are in date format are in GMT time. When ACS logs these attributes, it converts them to the ACS local time zone (the time zone of the ACS server).</p> <p>Workaround Configure ACS to use the GMT time zone.</p>
General ACS bugs		
CSCsc69976	Local logging file size and days do not appear after change in GUI.	<p>Symptom For local logging files, changes to the following fields are not saved:</p> <ul style="list-style-type: none"> • Keep only the last 7 files • Delete files older than 7 days <p>When you change the number of files or days from 7 to another number, the setting is not saved.</p> <p>Workaround None.</p>
CSCsc57975	The database order inside a Network Access Profile may cause authentication to fail and an error message appears.	<p>Symptom 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 the other database, authentication is successful. If the user does not exist in the other database, the error message <code>cs user unknown</code> (instead of <code>Database account expired</code>) is displayed.</p>
CSCsc49673	UPGRADE:Add Filter <code>aaa:service=ip_admission</code> to Upgrade-Profile NAP.	<p>Symptom 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 all incoming authentications to fail: except from PEAP-POSTURE.</p> <p>Workaround Add a filter of <code>Cisco-av-pair aaa:service = ip_admission</code> to the Upgrade-Profile. The no-posture requests will be authenticated against the global settings configuration (check the Grant access using global configuration, when no profile matches option in the created profile).</p>
CSCsc43577	CSAdmin stalls and has a memory leak.	<p>Symptom CSAdmin uses a large amount of memory when users change the EAP-FAST inner method from GTC to MSCHAPv2 on the Network Access Profile page.</p> <p>Workaround Restart the CSAdmin service.</p>
CSCsc43287	Replication: Administration Control > Access Policy. Port allocation not replicated.	<p>Symptom After replication of the interface security settings, the HTTP port allocation settings in Administration Control > Access Policy were not replicated (remained set to the default - Allow any TCP ports to be used for Administration HTTP Access).</p> <p>Workaround Ensure that the HTTP access policy is set correctly on the remote GUI.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc41638	ACS does not check if the CA certificate that was issued to a user exists in CTL.	<p>Symptom 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>Workaround Uncheck the CA certificate in question from the ACS web interface before removing the CA certificate from the machine storage.</p>
CSCsc41623	Configuring Logs - Reset Columns erroneously populates selection lists.	<p>Symptom For several report types, Reset Columns on the ACS web interface Logging configuration page sets the selected attributes to log (columns) to a different set of Logged Attributes than the actual default attributes, initially set on a fresh ACS installation.</p> <p>Conditions In ACS, when you configure the logged information through the ACS web interface by choosing System Configuration > Logging and selecting one of the listed reports, the Reset Columns selection 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"> • CSV Failed Attempts • CSV Passed Authentications • CSV VoIP Accounting <p>Workaround Use the right (->) and left (<-) arrow buttons to add and remove attributes in the Logged Attributes list, shown below.</p> <ul style="list-style-type: none"> • CSV Failed Attempts—Remove the Filter Information. • CSV Passed Authentications —Add the Cisco-av-pair attribute. • CSV VoIP Accounting. Add the following attributes: <ul style="list-style-type: none"> – Call Leg Setup Time. – Gateway Identifier. – Connection Id. – Call Leg Direction. – Call Leg Type. – Call Leg Connect Time. – Call Leg Disconnected Time. – Call Leg Disconnected Cause. – Remote Gateway IP Address.

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc41129	CSAuth exceptions occur during EAP-TLS stress tests using an LDAP external database with SSL connections.	<p>Symptom After a few hours of EAP-TLS authentications with an LDAP external database and LDAP connections over SSL (Trusted Root CA option), CSAuth may experience exceptions and fail.</p> <p>Workaround Restart the ACS services.</p>
CSCsc40001	Session resume in EAP-FAST-TLS does not work.	<p>Symptom 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>Conditions EAP-TLS as the inner method in EAP-FAST.</p> <p>Workaround None.</p>
CSCsc39979	When a NAP is updated, internal users are not deleted from the logged-in users list.	<p>Symptom 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> <p>Workaround None</p>
CSCsc32154	Upgrading from ACS 3.3 removed APT, SPT, and Reason from Logged Attributes.	<p>Symptom 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.</p> <p>Workaround None.</p>
CSCsc27168	User authentication succeeds even though a database is not selected.	<p>Symptom 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>Workaround Before deleting the external database configuration, ensure that it is not used in any NAP.</p>
CSCsc27158	There is a memory leak during LDAP stress - PAP authentication with legacy LDAP secure socket layer (SSL) connections.	<p>Symptom A memory leak occurred during stress tests of PAP authentications with LDAP server (OpenLDAP) and legacy SSL enabled (<i>cert7.db</i>). For example, memory usage reached 100 MB after ~1.5 million authentications.</p> <p>Memory was freed after ACS services were restarted.</p> <p>No memory leak occurred when the configuration was changed to use the new SSL mechanism. (Check Trusted Root CA.)</p> <p>Workaround In the LDAP Configuration Options page in ACS, use the new SSL option (Trusted Root CA), instead of the old option (<i>cert7.db</i>).</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsc06942	Script interface fails the 1 KB limit at Layer 2 level.	<p>Symptom Script interface fails the 1,000 byte limit at Layer 2 level.</p> <p>Conditions This issue is relevant only for nonfragmented messages in tunneled protocols (MS-PEAP, CISCO-PEAP, and EAP-FAST). Unfragmented tunneled EAP messages should not exceed the total length of 1,002 bytes.</p> <p>Workaround Set the supplicant size fragmentation threshold to be lower than 1,002 bytes. If it cannot be configured, another option is to set the maximum transmission unit (MTU) size that affects this value.</p>
CSCsc00788	Password change is not supported in Generic Token Card (GTC) against Windows database.	<p>Symptom Password change is not supported in EAP-GTC against Windows database.</p> <p>Conditions EAP-GTC authentication of user in Windows database whose account has expired or needs changed.</p> <p>Workaround None.</p>
CSCsb95897	ACS cannot display a long list of disabled accounts correctly.	<p>Symptom The ACS web interface has problems displaying disabled accounts lists if they contain several pages. Next is working as needed; but, Previous is available only once.</p> <p>Workaround None</p>
CSCsb93223	ACS creates a policy when a template profile is added and an error occurs.	<p>Symptom When using the NAC 802.1x template, if you cannot create a profile (for example, Global Authentication Setup is not configured properly), ACS still creates an internal posture validation policy.</p> <p>Workaround None.</p>
CSCsb72286	ACS RADIUS proxy uses RADIUS port 1645.	<p>Symptom 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>Workaround None</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsb25151	When a AAA client has multiple IP addresses, NAF for downloadable ACLs fails.	<p>Symptom When a single AAA client is configured with a range or list of IP address in ACS SE, the Network Access Filter (NAF) under Shared Profile Components cannot correctly determine the IP address of the Network Device Group (NDG) or the correct IP address of the AAA client.</p> <p>Conditions NAF must be 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>Workaround Perform one of the following:</p> <ul style="list-style-type: none"> Remove all but the correct IP address from the AAA client configuration component for the network access server (NAS) and NAD. Configure <code>ip radius source interface</code> to point to the correct IP address.
CSCsb15116	Apply and Restart button in NAP page does not release the NAF policy.	<p>Symptom 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>Workaround Perform one of the following:</p> <ul style="list-style-type: none"> Before deleting a Network Access Filter, remove it from the relevant Network Access Profiles. After deleting a Network Access Filter for each relevant Network Access Profile, click Submit (without performing changes) in the profile setup page.
CSCsh04536	When generating a report, entering a regular expression enclosed in brackets and including text preceded by a caret (^) does not exclude a user.	<p>Symptom <i>The User Guide for Cisco Secure ACS Solution Engine 4.0</i> states that entering a caret (^) in a regular expression immediately following a left bracket ([]) excludes the remaining characters from a search action:</p> <p>“When a caret (^) is positioned to immediately follow a left bracket ([], it excludes the remaining characters within brackets from matching the target string. For example, [^0-9] indicates that the target character is alpha rather than numeric.”</p> <p>This syntax does not work. When a filter is set up to exclude a user from a report by using this method, the user is not excluded from the report output.</p> <p>Workaround None.</p>
CSCsa79327	Authentications fail for users whose password includes the Euro symbol.	<p>Symptom Authentication fails for users whose password includes the Euro (€) symbol.</p> <p>Workaround Remove the Euro symbol from the user password.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCeh79954	EAP-TLS time of day restriction in Active Directory (AD) does not fail user; authentication succeeds.	<p>Symptom 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>Conditions EAP-TLS authentication of users in AD running in Windows 2000 or 2003 environment.</p> <p>Workaround None.</p>
CSCeh68821	LDAP authentication passes after modification of a subtree node due to DN caching.	<p>Symptom 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>Workaround 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>Symptom 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 from the pre-Windows 2000 name, then ACS may not be able to locate the user in Active Directory.</p> <p>Conditions ACS installed in Windows 2000/2003 Active Directory environment. Authentication with EAP-FAST and UPN usernames.</p> <p>Workaround Rename the user to have the same username as the pre-Windows 2000 username.</p>
CSCeh60564	An Active Directory locked-out user passed EAP-TLS authentication; should be rejected.	<p>Symptom 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>Conditions EAP-TLS authentication of users in Active Directory running in Windows 2000 environment.</p> <p>Workaround None. Windows 2003 has introduced some new attributes that should help resolve this issue in future.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCeh52700	Users who are expired in AD pass EAP-TLS authentication, but should be rejected.	<p>Symptom 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>Conditions EAP-TLS authentication of users in Active Directory running in Windows 2000 environment.</p> <p>Workaround 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>Symptom Address assignment from IP pools is based on Accounting Start and 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.</p> <p>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>Workaround None.</p>
CSCeh24979	Users fail to authenticate when upgrading and attempting to access an obsolete (no longer used) database.	<p>Symptom When upgrading from ACS release 3.1 or later to ACS release 4.0 (these are two-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>Workaround Select User Setup > Remove Dynamic Users after upgrading.</p>
CSCeh00074	GUI LDAP group mapping submission failure.	<p>Symptom When adding LDAP groups to be mapped to ACS groups, the Submit operation sometimes fails and an <code>Empty list</code> error message appears.</p> <p>Conditions This problem 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>Workaround Move to another window from the Group Mapping page, before you click Submit, or click on another frame in the ACS web interface.</p>
CSCeg50237	Overinstall causes the added AVP Attributes to disappear.	<p>Symptom Adding AVP attributes and then performing an overinstall causes those attributes to disappear from the Log Attribute field.</p> <p>Workaround None.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCeg47441	The CRL is not preserved when upgrading from ACS 3.3.2 or below to ACS 3.3.3 or higher.	<p>Symptom When upgrading from ACS 3.3.1.16 to ACS 3.3.3.2, the CRL entries are not transferred.</p> <p>Workaround Create the CRL entries manually.</p>
CSCeg40355	Authentication failures occur when remote logging fails.	<p>Symptom 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>Workaround Disable the remote logging functionality or correct the cause of the logging failure.</p>
CSCef96208	ACS reports incorrect privilege level.	<p>Symptom ACS may report users with the incorrect authorized privilege level. In particular, when using TACACS+, users who are correctly being authenticated with a privilege level of 15 are being reported with a level of 1.</p> <p>Workaround None.</p>
CSCef85314	Group DACL is downloaded if user's content NAF is not suitable.	<p>Symptom 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> <p>Workaround None.</p>
CSCef85310	Group DACL is downloaded if users DACL content is empty.	<p>Symptom It is possible to define an ACL with empty content. If this error is made, if a user with an empty ACL belongs to a group on which a non-empty ACL is defined, and the user 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 be.).</p> <p>Workaround Do not define an empty downloadable ACL.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCef55730	ACS authorization passes even for a disabled user.	<p>Symptom 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> <p>Workaround None.</p>
CSCef12461	Symptom ACS administrators are not restored, when on a large database, you restore a dump file on Windows 2000.	<p>Symptom When ACS contains a large database with 500 or more administrators, after restoring the dump file on Windows 2000, the ACS administrators are not restored.</p> <p>Workaround 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>Symptom Intensive use of the Logged-In Users report may lead to significant memory utilization by the CSAdmin service.</p> <p>Workaround Restart the CSAdmin service.</p>
CSCeb78551	When handling a LEAP RADIUS proxy between a front-end ACS server and a back-end ACS server, problems arise if the configuration is not correct.	<p>Symptom When handling a LEAP RADIUS proxy between a front-end ACS server and a back-end ACS server, problems arise if the configuration is not correct.</p> <p>Conditions 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 RADIUS (Cisco IOS/PIX 6.0).</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 Interface Configuration 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, which is the reason why the AAA Client must be RADIUS (Cisco IOS/PIX 6.0).</p> <p>Workaround None.</p>
CSCse38771	The ACS SE automatically creates a <i>Self</i> entry in the AAA Servers Table.	<p>Symptom The ACS Solution Engine automatically creates an entry called <i>Self</i> in the AAA Servers Table. This entry identifies the Solution Engine machine.</p> <p>However, in the Proxy Distribution Table and the AAA Server Table for RDMS synchronization, the ACS Solution Engine creates an entry for the hostname of the device that is running the ACS Solution Engine.</p> <p>Workaround None.</p>

Table 4 Known Problems in ACS SE 4.0 (continued)

Bug ID	Summary	Explanation
CSCsd90369	Table 9 in the RDBMS Synchronization Import Definitions appendix of the <i>User Guide for Cisco Secure ACS Solution Engine 4.0</i> incorrectly lists RADIUS/TACACS+ attributes.	<p>Symptom The listing for TACACS+ Attributes: 160, 162, RADIUS Attributes 170, 17 is incorrect. The values should be reversed:</p> <p>RADIUS Attributes: 160, 162</p> <p>TACACS+ Attributes 170, 173</p>
CSCsd92659	The description of the Shutdown button in the short help for the Solution Engine is incorrect.	<p>Symptom The short help states that the user can shut down the Solution engine by clicking the Shutdown button. The appliance is not powered down when the following steps are taken as stated in the documentation.</p> <ol style="list-style-type: none"> 1. The user chooses System Configuration > Appliance Configuration. 2. The user clicks the Shutdown button at the bottom of the page. <p>The Solution Engine does not power down as indicated in the short help. Instead, the message <code>It is now safe to turn off the computer</code> appears.</p> <p>Workaround After the message <code>It is now safe to turn off the computer</code> appears, press the power switch on the ACS SE to turn off the appliance.</p>

Resolved Problems

Table 5 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 5 Resolved Problems in ACS 4.0

Bug ID	Summary	Explanation
CSCsc52660	UCP 4.0 on Windows 2000 or Windows 2003 may cause a Common Gateway Interface (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: http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des
CSCeh93481	NAF is selected automatically after deleting and creating with the same name.	This problem has been solved.
CSCeh91809	VoIP messages cause the CSRADIUS service to unexpectedly terminate.	CSRADIUS no longer terminates unexpectedly.
CSCeh55725	ACS 3.3.2.2 on the HP 1111 platform fails to get NIC configuration.	This problem has been fixed in the most recent version of ACS.
CSCeh46130	Replication timeout causes CSAuth restart without any error in ACS reports	Replication on Windows 2003 works without CSAuth problems, and logs are correct.

Table 5 Resolved Problems in ACS 4.0 (continued)

Bug ID	Summary	Explanation
CSCeh38960	Restoring from software removes the appliance entry inside the proxy.	The default proxy entry for the appliance is no longer removed from the proxy table when restoring the database from the software version to an appliance.
CSCeh25112	Network Access Filter (NAF) reedit requests restart.	After editing NAF data, ACS web interface now displays a message after you click Submit 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 network access restriction (NAR) with TACACS+ or RADIUS NAS on same IP.	ACS no longer chooses the wrong NDG for NAR matching if a TACACS+ and RADIUS NAS are defined with the same IP and placed in separate NDGs, and the authentication is performed via RADIUS.
CSCee88908	CSLog fails if a logged attribute is deleted due to replication.	The CSLog service 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.
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 CSUtil (or because of backup and restore).
CSCee77099	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.
CSCee68644	SPC type created by EMBU DLL returns errors in Name field.	Name field limitation of 31 characters defined. Error messages no longer appear.
CSCee58593	CSAdmin restart during replication between two ACS SW in slow link.	Replication between two ACSs in a slow link (128 KB) works successfully.
CSCed93251	Fail to locate ACL for updating when ACL uses the same name as NAF.	NAFs with the same name no longer cause problems.
CSCed83648	Renaming an NDG removes it from the Selected Items of NAF HTML page.	A pop-up window has been added to confirm deletion.
CSCed77992	Action Code 211 does not return group settings to factory defaults.	Action Code 211 now works as documented in the <i>User Guide for Cisco Secure ACS Solution Engine 4.0</i> .
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 synchronized 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.

Table 5 **Resolved Problems in ACS 4.0 (continued)**

Bug ID	Summary	Explanation
CSCeb51393	Multiple administrators need 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.
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.
CSCea91947	ACS does not authenticate Windows 2000 users when NTLMv2 is enabled on the network.	ACS now supports NTLMv2.
CSCea74289	Cascade replication due to user password changes do not work.	Cascade replication with password changes replicates successfully.
CSCea62226	CSAgent (Solaris)—The appliance indicates that the RA is running when it is not running.	The appliance no longer shows the Remote Agent as running when it is not.
CSCsd95649	Dbcompact has been removed from the console commands available in ACS SE 4.0 code.	This command was deliberately removed due to the different database structure.
CSCsd14750	The ACS documentation is not clear about how to power on the ACS 1112. The power switch is on the power LED. The documentation describes only three states for the LED, even though another state exists. The green blinking LED state indicates that the unit is plugged in and power is available, but power is off. Press the power LED to turn on the ACS 1112 or 1113.	The documentation on the front panel LEDs and components has been updated to correct this error. See the <i>Installation and Setup Guide for the Cisco Secure ACS Solution Engine</i> : http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_guide_chapter09186a008068f7f2.html

Documentation Updates

Updates for Online Help Documentation

The following errors exist in the ACS online help:

- The ACS documentation indicates that you can disable the dynamic user cache, which is incorrect.
- Support files are not matched to the number of selected days in the basic system configuration section. If you want the support information to be downloaded to include service log files that are older than the current log files, check the **Collect Previous X Days logs** check box and type the number of days of log files to be included. The “Current Log File” may not be today's date, rather it may be several days older than today's date.
- The online documentation for the ACS SE 1113 states that the description field for a downloadable IP ACL can contain up to 30,000 characters; however, the description can contain only 1006 characters.

- The online help for the Solution Engine states that clicking the **Shutdown** button powers down the appliance. Clicking the **Shutdown** button causes a message to appear, indicating that it is safe to power down the appliance. To power down the appliance, press the Power button on the front panel.

Omissions and errors in the ACS documentation include:

- The ACS documentation erroneously indicates that the ODBC database is supported for EAP and Non-EAP Authentication Protocol-Database Compatibility.
- 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 a shared secret mismatch. The next release of the documentation will address this omission.
- LEAP is not supported when working with Network Access Profiles. You can use LEAP only if your system is operating in legacy ACS mode.
- 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. See bug CSCsc72958.
- 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: the first package name is *package.cab*; the second is *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 standalone 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.
- Replication of the appliance configuration is not mentioned in the short help or in the *User Guide for the Cisco Secure ACS Solution Engine*.
- When you generate a certificate signing request or a self-signed certificate, you should enter only a file name for the private key file and certificate file, not the full directory path.
- The ACS Solution Engine automatically creates an entry called *Self* in the AAA Servers Table. This entry identifies the Solution Engine machine. However, in the Proxy Distribution Table and the AAA Server Table for RDMS synchronization, the ACS Solution Engine creates an entry for the hostname of the device that is running the ACS Solution Engine.
- In the **System Configuration > Support** page, the **Collect Previous X Days** logs check box applies to the number of days previous to the current service log files, which m.

Obtaining Documentation

Cisco documentation and additional literature are available on 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

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 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.

You can send comments about Cisco documentation to 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

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

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

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 nonemergencies.

- Nonemergencies—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

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 Solution Engine* 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)