

Release Notes for Cisco Secure ACS for Windows Server 3.3.2

July 2005

Full Build Number: 3.3.2.2

These release notes pertain to Cisco Secure Access Control Server for Windows Server (Cisco Secure ACS) version 3.3.2.



The release numbering system used by Cisco Secure ACS 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 3.3.2.2. Elsewhere in this document where 3.3.2 is used, we are referring to 3.3.2.2. Cisco Secure ACS major release numbering starts at 3.3.1, not 3.3.0. Use this information when working with your customer service representative.

These release notes provide:

- [New Features, page 2](#)
- [Supplemental License Agreement for Cisco Systems Network Management: Cisco Secure Access Control Server Software, page 4](#)
- [Product Documentation, page 5](#)

CISCO SYSTEMS



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 6](#)
- [Installation Notes, page 8](#)
- [Evaluation Version, page 9](#)
- [Limitations and Restrictions, page 10](#)
 - [Important Known Problems with Network Admission Control, page 10](#)
 - [Interoperability Testing, page 10](#)
 - [Supported Upgrade Versions, page 11](#)
 - [Supported Operating System, page 11](#)
 - [Supported Web Browsers, page 14](#)
 - [Supported Platforms for CiscoSecure Authentication Agent, page 16](#)
 - [Other Supported Devices and Software, page 16](#)
- [Known Problems, page 16](#)
- [Resolved Problems, page 35](#)
- [Obtaining Documentation, page 42](#)
- [Documentation Feedback, page 43](#)
- [Obtaining Technical Assistance, page 43](#)
- [Obtaining Additional Publications and Information, page 45](#)

New Features

Cisco Secure ACS 3.3 contains the following new features and enhancements:

- **Network admission control (NAC)**—Cisco Secure ACS acts as a policy decision point in NAC deployments. Using policies you configure, it evaluates the credentials sent to it by Cisco Trust Agent, determines the state of the host, and sends the AAA client ACLs that are appropriate to the host state. Evaluation of the host credentials can enforce many specific policies, such as operating system patch level and anti-virus DAT file version. Cisco Secure ACS records the results of policy evaluation for use with your monitoring system. Policies can be evaluated locally by Cisco Secure ACS or

can be the result returned from an external policy server that Cisco Secure ACS forwards credentials to. For example, credentials specific to an anti-virus vendor can be forwarded to the vendor anti-virus policy server.

- **EAP Flexible Authentication via Secured Tunnel (EAP-FAST) support**—Cisco Secure ACS supports the EAP-FAST protocol, a new publicly accessible IEEE 802.1X EAP type developed by Cisco Systems that protects authentication in a TLS tunnel but does not require use of certificates, unlike PEAP. Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP can migrate to EAP-FAST for protection from dictionary attacks. Cisco Secure ACS supports EAP-FAST supplicants available on Cisco Compatible client devices and Cisco Aironet 802.11a/b/g PCI and CardBus WLAN client adapters.
- **Machine Access Restrictions (MARs)**—Cisco Secure ACS includes MARs as an enhancement of Windows machine authentication. When Windows machine authentication is enabled, you can use MARs to control authorization of EAP-TLS and Microsoft PEAP users who authenticate with a Windows external user database. Users who access the network with a computer that has not passed machine authentication within a configurable length of time are given the authorizations of a user group that you specify and which you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.
- **Network Access Filters (NAFs)**—Cisco Secure ACS includes NAF as a new type of Shared Profile Component. NAF provides a flexible way of applying network access restrictions and downloadable ACLs on AAA client names, network device groups, or the IP addresses of AAA clients. NAFs applied by IP addresses can use IP address ranges and wildcards. This feature introduces granular application of network access restrictions and downloadable ACLs, both of which previously only supported the use of the same access restrictions or ACLs to all devices. NAFs allow much more flexible network device restriction policies to be defined, a requirement common in large environments.
- **Downloadable ACL enhancements**—Cisco Secure ACS 3.3 extends per-user ACL support to any layer three network device that supports this feature. This includes Cisco PIX Firewalls, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that can be applied per user or per

group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When used in conjunction with NAFs, downloadable ACLs can be applied differently per AAA client, enabling you to tailor ACLs uniquely per user, per access device.

- **Replication enhancements**—Cisco Secure ACS 3.3 includes two enhancements to the CiscoSecure Database Replication feature:
 - **Configurable replication timeout**—You can specify how long a replication event is permitted to continue before Cisco Secure ACS ends the replication attempt and restarts affected services. This feature improves your ability to configure replication when network connections between replication partners are slow.
 - **Separate replication of user database and group database**—You can replicate the user and group databases separately. Replicating changes to user accounts no longer requires replicating groups. Likewise, replicating groups no longer requires replicating users. This increase to replication component granularity can reduce the amount of data sent between Cisco Secure ACSes during a replication event.

Supplemental License Agreement for Cisco Systems Network Management: Cisco Secure Access Control Server Software

IMPORTANT—READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

1. ADDITIONAL LICENSE RESTRICTIONS.

- **Installation and Use.** The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use following Software component:
 - Access Control Server (ACS): May be installed on one (1) server in Customer’s network management environment.
- **Reproduction and Distribution.** Customer may not reproduce nor distribute software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. Software License Agreement.

Product Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • On Cisco.com.

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Installation Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816529=).¹
<i>User Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816592=).¹
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com.
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server</i>	On Cisco.com .
<i>Recommended Resources for the Cisco Secure ACS User</i>	On Cisco.com .
Online Documentation	In the Cisco Secure ACS HTML interface, click Online Documentation.
Online Help	In the Cisco Secure ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

1. See [Obtaining Documentation](#), page 42.

Related Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes a set of white papers about Cisco Secure ACS. All white papers are available on Cisco.com. To view them, go to the following URL:

<http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>

Table 2 **Related Documentation**

Document Title	Description and Available Formats
<i>Building a Scalable TACACS+ Device Management Framework</i>	This document discusses the key benefits of and how to deploy Cisco Secure ACS Shell Authorization Command sets, which provide the facilities constructing a scalable network device management system using familiar and efficient TCP/IP protocols and utilities supported by Cisco devices.
<i>Catalyst Switching and ACS Deployment Guide</i>	This document presents planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in support of Cisco Catalyst Switch networks. It discusses network topology regarding AAA, user database choices, password protocol choices, access requirements, and capabilities of Cisco Secure ACS.
<i>Cisco Secure ACS for Windows vs. Cisco Secure ACS for UNIX</i>	This bulletin compares the overall feature sets of Cisco Secure ACS for Windows and CiscoSecure ACS for UNIX. It also examines the advantages and disadvantages of both platforms and discusses issues related to migrating from the UNIX-based product to the Windows version.
<i>Configuring LDAP</i>	This document outlines deployment concepts for Cisco Secure ACS when authenticating users of a Lightweight Directory Access Protocol (LDAP) directory server, and describes how to use these concepts to configure Cisco Secure ACS.
<i>Deploying Cisco Secure ACS for Windows in a Cisco Aironet Environment</i>	This paper discusses guidelines for wireless network design and deployment with Cisco Secure ACS.
<i>EAP-TLS Deployment Guide for Wireless LAN Networks</i>	This document discusses the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication protocol deployment in wireless networks. It introduces the EAP-TLS architecture and then discusses deployment issues.

Table 2 *Related Documentation (continued)*

Document Title	Description and Available Formats
<i>External ODBC Authentication</i>	This paper presents concepts and configuration issues in deploying Cisco Secure ACS for Windows Server to authenticate users against an external open database connectivity (ODBC) database. This paper also describes configuring, testing, and troubleshooting a relational database management system (RDBMS) with ODBC and Cisco Secure ACS, and provides sample Structured Query Language (SQL) procedures.
<i>Guidelines for Placing ACS in the Network</i>	This document discusses planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in an enterprise network. It discusses network topology, user database choices, access requirements, integration of external databases, and capabilities of Cisco Secure ACS.
<i>Initializing MC Authorization on ACS 3.1</i>	This application note explains how to initialize Management Center authorization on Cisco Secure ACS.
<i>Securing ACS Running on Microsoft Windows Platforms</i>	This paper describes how the Cisco Secure ACS can be protected against the vulnerabilities of the Windows 2000 operating system and explains how to improve security on the computer running Cisco Secure ACS. It discusses making the system dedicated to Cisco Secure ACS, removing all unnecessary services, and other measures. It also discusses how to improve administrative security for Cisco Secure ACS through such methods as stronger passwords and controlled administrative access. This paper concludes with considerations of physical security for Cisco Secure ACS and its host.

Installation Notes

For information about installing Cisco Secure ACS, see *Installation Guide for Cisco Secure ACS for Windows Server 3.3*. To see all Cisco Secure ACS documentation, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

Evaluation Version

The evaluation version of Cisco Secure ACS 3.3 provides full functionality for 90 days after the date of installation. This allows you to use all features of Cisco Secure ACS 3.3 while determining if it suits your needs. The evaluation version of Cisco Secure ACS 3.3 will be available within 30 days after the release of the commercial version of Cisco Secure ACS 3.3.

The evaluation version of Cisco Secure ACS 3.3 can be distinguished from the commercial version in the following ways:

- The word “trial” appears in the title of the installation routine.
- The Windows Control Panel Add/Remove applet indicates that the Cisco Secure ACS installation is a trial version.
- In the administrative interface of Cisco Secure ACS, the word “trial” appears on the title of the initial screen.

When the evaluation period has elapsed, the CSRADIUS and CSTACACS services fail to start. You will receive a message upon accessing the Cisco Secure ACS HTML interface notifying you that your evaluation period has elapsed.

Purchasing the Commercial Version

Please contact your Cisco Sales Representative(s) to inquire about purchasing the commercial version of Cisco Secure ACS. To purchase the commercial version of Cisco Secure ACS 3.3 online, use the following URL:

<http://www.cisco.com/pcgi-bin/cm/welcome.pl>

Upgrading to the Commercial Version

After purchasing a commercial version of Cisco Secure ACS 3.3, you can upgrade your Cisco Secure ACS server from the evaluation version to the commercial version by installing the commercial version over the evaluation version. For information on installing Cisco Secure ACS 3.3, follow the instructions in *Installation Guide for Cisco Secure ACS for Windows Server 3.3*.

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, 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

Limitations and Restrictions

The following limitations and restrictions apply to Cisco Secure ACS 3.3.

Important Known Problems with Network Admission Control

The following known problems are related to Network Admission Control. We recommend that you review them.

- [CSCee88908](#)—CSLog crash if a logged attribute is deleted due to replication, page 34
- [CSCee87826](#)—A deleted policy is being reassign when created with the same name, page 32
- [CSCee87899](#)—Replication of CNAC policies should be updated in the doc, page 33

Interoperability Testing

Cisco Secure ACS has not been interoperability tested with other Cisco software. Other than for the software and operating system versions listed in this document, we performed no interoperability testing. Using untested software with Cisco Secure ACS may cause undesired results. For the best performance of Cisco Secure ACS, we recommend that you use the versions of software and operating systems listed in this document.

Supported Upgrade Versions

We support upgrading to Cisco Secure ACS for Windows Server 3.3.2, from the following versions:

- Cisco Secure ACS for Windows Server 3.3.1
- Cisco Secure ACS for Windows Server 3.2.3
- Cisco Secure ACS for Windows Server 3.2.2
- Cisco Secure ACS for Windows Server 3.2.1
- Cisco Secure ACS for Windows Server 3.1.2
- Cisco Secure ACS for Windows Server 3.0.4

**Note**

To upgrade to version 3.3 from a version earlier than 3.0.4, upgrade to one of the supported upgrade versions, listed above, and then upgrade to Cisco Secure ACS 3.3.

Supported Operating System

Cisco Secure ACS for Windows Servers 3.3 supports the Windows operating systems listed below. Both the operating system and the service pack must be English-language versions.

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
 - with Service Pack 4 installed
 - without features specific to Windows 2000 Advanced Server enabled
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition



Note

The following restrictions apply to support for Microsoft Windows operating systems:

- Cisco Secure ACS for Windows Server is not designed to make use of the multi-processor feature of any supported operating system; however, we did test Cisco Secure ACS using dual-processor computers.
- We cannot support Microsoft clustering service on any supported operating system.
- Windows 2000 Datacenter Server is not a supported operating system.
- When running Cisco Secure ACS on Windows Server 2003, you may encounter event messages that falsely indicate that Cisco Secure ACS services have failed. This issue is documented in bug CSCea91690. For more information about CSCea91690, see [Table 3](#).

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 Cisco Secure ACS for Windows.

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

For information about our process for evaluating and releasing Microsoft security patches for Cisco Secure ACS Solution Engine, see the *Cisco Secure ACS Solution Engine Q & A* document, available in the Product Literature area for Cisco Secure ACS Solution Engine on Cisco.com.



Note

For information about support for Microsoft patches issued after the release of Cisco Secure ACS for Windows Server 3.3, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server 3.3*.

We tested Cisco Secure ACS for Windows Server 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](#)

We tested Cisco Secure ACS for Windows Server 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](#)

Upgrading from Windows NT 4.0

If you are upgrading from a previous version of Cisco Secure ACS that is running on Windows NT 4.0, you cannot upgrade the operating system to Windows 2000 Server. This is because the setup program for previous versions of Cisco Secure ACS detected which Windows operating system the computer used and customized Cisco Secure ACS for that operating system. As a result, upgrading the operating system to Windows 2000 Server without taking the necessary steps causes Cisco Secure ACS to fail.

We last published information about how to upgrade the operating system of the computer running Cisco Secure ACS to Windows 2000 in the documentation for Cisco Secure ACS 3.1. For more information, see *Installation Guide for Cisco Secure ACS for Windows Server 3.1*, available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs31/acsinst

Supported Web Browsers

To administer all features included in the HTML interface of Cisco Secure ACS 3.3, use an English-language version of one of the following tested and supported web browsers:

- Microsoft Internet Explorer for Microsoft Windows
 - Version 6.0
 - Service Pack 1
 - Sun Java Plug-in 1.4.2_04 or Microsoft Java Virtual Machine (JVM)



Note Microsoft does not include its JVM in Windows Server 2003. Instead, use the Sun Java Plug-in listed above. For more information about Microsoft plans regarding its JVM, see <http://www.microsoft.com/mscorp/java/>.

- Netscape Communicator for Microsoft Windows
 - Version 7.1
 - Sun Java Plug-in 1.4.2_04

**Note**

-
- Several known problems are related to using Netscape Communicator with Cisco Secure ACS. For more information, please review [Table 3](#).
 - We do not recommend using a slow network connection for remote access to the Cisco Secure ACS HTML interface. Some features that use Java applets do not operate optimally, such as the HTML pages for configuring Network Access Restrictions and Network Admission Control.
-

We do not support other versions of these browsers or other Java virtual machines with these browsers, nor do we test web browsers by other manufacturers.

**Note**

To use a web browser to access the Cisco Secure ACS HTML interface, configure your web browser as follows:

- Use an English-language version of a supported browser.
 - Enable Java (see the supported browser list above for JVM details).
 - Enable JavaScript.
 - Disable HTTP proxy.
-

Supported Platforms for CiscoSecure Authentication Agent

For use with Cisco Secure ACS 3.3, we tested CiscoSecure Authentication Agent on Windows XP with Service Pack 1. We support the use of CiscoSecure Authentication Agent with Cisco Secure ACS 3.3 when CiscoSecure Authentication Agent runs on one of the following client platform operating systems:

- Windows XP
- Windows 2000 Professional
- Windows 98
- Windows 95
- Windows NT 4.0

Other Supported Devices and Software

For information about supported Cisco devices, external user databases, and other software, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server Version 3.3*. To see all Cisco Secure ACS documentation, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

Known Problems

This section contains information about the following topics:

- [Cisco AAA Client Problems, page 17](#)
- [Known Microsoft Problems, page 17](#)
- [Known Problems in Cisco Secure ACS 3.3, page 18](#)

Cisco AAA Client Problems

Refer to the appropriate release notes for information about Cisco AAA client problems that might affect the operation of Cisco Secure ACS. You can access these release notes online at the following URLs.

Cisco Aironet Access Point

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/>

Cisco BBSM

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/>

Cisco Catalyst Switches

<http://www.cisco.com/univercd/cc/td/doc/product/lan/>

Cisco IOS

<http://www.cisco.com/univercd/cc/td/doc/product/software/>

Cisco Secure PIX Firewall

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/>

Cisco VPN 3000 Concentrator

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/>

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/>

Cisco VPN 5000 Concentrator

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/>

Known Microsoft Problems

Due to a defect in the Microsoft PEAP supplicant provided in Windows XP Service Pack 2, the PEAP supplicant cannot reauthenticate successfully with Cisco Secure ACS. Microsoft case SRX040922603052 has been opened on this issue. Customers 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 in Cisco Secure ACS 3.3

Table 3 describes problems known to exist in version 3.3.



Note

- A “—” in the Explanation column indicates that no information was available at the time of publication. You should check the Cisco Software Bug Toolkit for current information. To access the Cisco Software Bug Toolkit, go to <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log in to Cisco.com.)
- Bug summaries and explanations in Table 3 are printed word-for-word as they appear in our bug tracking system.

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3

Bug ID	Summary	Explanation
CSCdv35872	Insufficient length for NDS context entry	When a Novell NDS database configuration in Cisco Secure ACS has a context list greater than 4095 characters long, editing the NDS configuration page results in incorrect HTML in the browser interface. <i>Workaround/Solution:</i> Use a context list no longer than 4096 characters.
CSCdv86708	HTTP Port Allocation is not replicated	Changes to HTTP Port Allocation settings do not appear to replicate. After the HTTP Port Allocation settings are changed on the Access Policy Setup page in the Administration Control section on the primary Cisco Secure ACS server and replication succeeds, the secondary Cisco Secure ACS server does not display the changes to the HTTP Port Allocation settings in the HTML interface. <i>Workaround/Solution:</i> The changes to the HTTP Port Allocation settings do replicate successfully; however, to see the changes on the secondary Cisco Secure ACS server, restart the CSAdmin service.

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCdz61464	Solaris Netscape 7.0 - Minor Features Failure	<p>When the administrative browser is Netscape 7.0 on Solaris 8.0, some menus in the HTML interface for Cisco Secure ACS do not work properly.</p> <p><i>Workaround/Solution:</i> Use a supported Windows browser.</p>
CSCea25090	Logged In User not showing after going into enable mode on router	<p>With AAA Accounting for exec sessions configured on a NAS, a user shows up in the Logged-In User report on Cisco Secure ACS. With Accounting also configured for going into enable mode, the user no longer appears in the Logged-In User report after authenticating successfully.</p> <p>Cisco Secure ACS tracks user sessions by IP address and port number. When enable authentication succeeds, Cisco Secure ACS sees that the IP address and port number combination for the existing session have been reused and assumes that the accounting stop packet was not sent or was lost; therefore, the user session is removed from the Logged-In User report even though the session continues in enable mode.</p> <p>Because the NAS cannot be configured to send new accounting start packets when the enable mode is entered, the Logged-In User report cannot correctly report the user session as ongoing.</p> <p><i>Workaround:</i> None.</p>
CSCea55457	Radius Attributes do not appear in user/group profile page	<p>After you enable RADIUS attributes in the Interface Configuration section of the Cisco Secure ACS HTML interface, they do not appear or appear only partially in Group Setup or User Setup, as applicable.</p> <p><i>Workaround/Solution:</i> Restart the CSAdmin service.</p>
CSCea74289	cascade replication due to user pass change-dont work	<p>Cascading replication does not occur when the replication trigger is user password change and the primary Cisco Secure ACS is configured to perform replication manually.</p> <p><i>Workaround/Solution:</i> Use scheduled replication on the primary Cisco Secure ACS.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCea91690	Event Viewer errors on startup/shutdown in .NET	<p>On Windows .Net Server 2003 shutdown and startup you may see errors that falsely indicate that Cisco Secure ACS service have failed. At startup, you may see a dialog box indicating that a service, such as CSLog, encountered a problem and needs to close. The same error logged to Event Viewer, as in the following example:</p> <pre data-bbox="610 496 1177 597">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 Cisco Secure ACS services status during startup and shutdown, but Cisco Secure ACS services may not have started yet or may have stopped already. Even though this is normal behavior for Cisco Secure ACS services, Windows perceives this as an error and logs it to the Event Viewer.</p> <p>On startup, all errors from event viewer displayed to user, which is why, when users logs into Windows right after startup, they see errors from the previous login session.</p> <p>This behaviour observed on Windows Server 2003 only.</p> <p><i>Workaround:</i> You can verify that Cisco Secure ACS services are running by using Control Panel.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCeb16968	ACS shared profile components disappear with XML error messages	<p>After you upgrade Cisco Secure ACS, authorization support for Management Center (MC) applications, such as Management Center for Firewalls, fails. In the Shared Profile Components section of the Cisco Secure ACS HTML interface, each MC that has registered with Cisco Secure ACS has a set of pages for configuring authorization components. If you access a page for editing or adding authorization components, you see an error message about a missing XML file.</p> <p><i>Workaround/Solution:</i> You must use CiscoWorks to re-register all MCs with Cisco Secure ACS.</p> <p>Log into the CiscoWorks desktop with admin privileges.</p> <p>Go to Server Configuration > Setup > Security > Select Login Module. Configure CiscoWorks to use the CiscoWorks Local module, and then configure CiscoWorks to use the TACACS+ module.</p> <p>Go to VPN Security Management Solution > Administration > Common Services > Configuration > AAA Servers. Unregister all MCs and then re-register all MCs.</p> <p>Log out of CiscoWorks.</p>
CSCeb51393	multi-admin needs to be able to add/edit/delete downloadable ACLs	<p>With multi-administrator tries to add/edit/delete downloadable acl under the shared profile components, after the first admin submitted any changes, the other administrator's ACS session got locked up.</p> <p><i>Workaround:</i> There is no workaround. Administrators must inform each other when he/she is working on the downloadable ACLs.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCeb62898	Group mapping ordering applet is not properly ordered	<p>In a newly created Windows group mapping configuration, group mappings list in the wrong order.</p> <p><i>Workaround:</i> On the page for ordering group mappings, order the group mappings and click Submit. As additional mappings are added, they appear properly at the end of the list of mappings.</p>
CSCec61110	authentications on secondary acs may fail after replication	<p><i>Symptom:</i> In environment where primary and secondary Cisco Secure ACS primary and secondary servers are kept in synch using the replication feature, user authentication may fail for users defined in an external database users and the Failed Attempts log will contain an “external DB not configured” error.</p> <p><i>Conditions:</i> This happens with certain external database types such as LDAP, NDS, and the various token server types. It can't happen with the Windows external DB. By configuring external databases in a different order on the primary and secondary Cisco Secure ACS servers, authentication fails on the secondary server for users defined in the databases configured in a different order. If external databases are configured in same order on primary and secondary servers, this does not happen. For example, if you configure two instances of LDAP external user databases on primary and secondary servers but configure them in different orders, after users are replicated, LDAP authentication attempts fail on the secondary server.</p> <p><i>Workaround:</i> For each database type involved in the problem, delete the external databases on all secondary servers and reconfigure them in the same order that they are defined on the primary server. If this fails, delete the affected external databases on the primary and secondary servers and reconfigure them.</p>
CSCec72911	2003-password aging page display issue	—

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCec89440	Unable to edit some of the disabled accounts	<p>The Disabled Accounts report in the Reports and Activity section of the Cisco Secure ACS HTML interface can behave oddly when you access it using an administrator account that doesn't have access to all groups.</p> <p>If a page of the Disabled Accounts report has users belonging to groups that the administrator cannot access, the report doesn't allow the administrator to move to the next page of the report.</p> <p>If a user account is configured to be assigned a group by the group mapping feature, the user account appears on the Disabled Accounts report even though the administrator only has access to specific groups.</p> <p><i>Workaround:</i> Access the Disabled Accounts report with an administrative account that has permission to access all groups.</p>
CSCed42439	Active Directory via LDAP - Group Mappings skip first group	When Active Directory is configured as Generic LDAP and group mappings are configured, the first group in the LDAP directory is skipped.
CSCed59826	CSAdmin stops responding when editing java using netscape	—
CSCed62260	Remote Agents entries are being deleted after restore	<p>When restoring a dump file created on Cisco Secure ACS software version on Appliance, Remote Agent entries (Inside Network Configuration) will be deleted.</p> <p>This behaviour should be taken into consideration since ACS on Appliance behaves similarly as it behaves on the software version and runs over the existing data and settings.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCed77992	Action Code 211 doesn't return group settings to factory defaults	<p>Action Code 211 doesn't work as documented.</p> <p>Document states, this code “Resets a Group User record back to its original factory defaults”. However some settings are not reset to factory defaults like Shell (exec) and No escape check boxes.</p>
CSCed83628	Replication displays error when nothing to be replicated	<p>In a scheduled replication scheme, a secondary server incorrectly records an error in the replication log when scheduled replication does not occur because no changes have occurred on the primary server. For example, this can occur when the primary and secondary servers are only configured to replicate the user database and network configuration, and then a change is made to Network Configuration on the primary server but no change is made in the user database. At the next scheduled replication, the primary server correctly sends only the network configuration, but the secondary logs an error message that the user database was not received. This is not an error and the message should not be logged.</p> <p><i>Workaround:</i> None.</p>
CSCed83648	Renaming of NDG removes it from Selected Items of NAF UI	Once some NDG, which is in the Selected Items window of the NAF UI, changes its name on Network Devices page, it's being removed from the Selected Items of NAF back to the source NDG window, where its known by its new name.
CSCed93251	Fail to locate ACL for updating when ACL uses the same name as NAF	<p>Procedure to reproduce the problem:</p> <ol style="list-style-type: none"> 1. Configure one Network Access Filtering (e.g. Healthy) 2. Configure one Downloadable IP ACL with the same name as that of NAF (e.g. Healthy) <p>Then the following error message shows up: “Failed to locate the ACL for updating”.</p> <p><i>Workaround:</i> Create a different name for ACL other than those used by NAF.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCed90144	When deleting a NAF it should be deleted from the assigned dACLs	<p>Deleting a NAF removes it from Cisco Secure ACS; however, the NAF is still referenced by any downloadable ACLs that referenced it before the NAF was deleted. This causes the downloadable ACLs to fail to download and, as a result, the user to whom the ACLs were to be applied fails to authenticate.</p> <p><i>Workaround:</i> When you delete a NAF, examine all downloadable ACL configurations and ensure that the NAF is not referenced by any of them.</p>
CSCee13658	Failed attempts report statement is not clear enough	<p>When user validation fails for any reason (external server down, wrong SSL certificate, or key mismatch with NAS), the csv failed attempts report states that the authentication failure code is 'external db account restriction' or 'CS password invalid'.</p> <p><i>Workaround:</i> This is cosmetic. No workaround.</p>
CSCee29758	very low performance/CSAuth hangs when connection to SQL fails-logg	—
CSCee38482	Admin account can see all users that are dynamically mapped	<p>Local admin can see dynamic mapped users.</p> <p><i>Workaround:</i> It's a read only. No other workaround at this time until bug is fixed.</p>
CSCee58593	CSAdmin restart during Replication between two ACS SW in slow link	<p>Replication between two Cisco Secure ACSes in slow link (128k), the services of the primary ACS are restart after the time out that is configured on the CiscoSecure Database Replication page is expired and replication was not completed. The services that restart are:</p> <ul style="list-style-type: none"> • CSAdmin • CSAuth • CSTacacs • CSRADIUS

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee62147	when create CRL with CTL contains two or more CA they change uncheck	<p>When you configure a CRL, you associate it with a specific CA that you have enabled on the certificate trust list (CTL). Once the CRL is associated with the CA, the checkbox for enabling the CA on the CTL is not shown. This is intentional; however, if any other CA certificate in local storage has the exact same CN as the CA associated with the CRL, the checkboxes for those other CAs also are not shown. This is unintentional.</p> <p><i>Workaround:</i> To make the checkboxes accessible on the CTL, temporarily select a different CA for the CRL, make the configuration changes needed in the CTL, and then reselect the original CA for the CRL.</p>
CSCee65671	Need to be able to roll back previously installed older patches	Using the CLI on the Appliance, there is no ability to go back to a previously installed older patch version.
CSCee68644	SPC type created by EMBU DLL returns errors in Name field	<p>In case of SPC component that was created by MC-based applications, the “Name” field is not limited to desired 31 chars, and allows entering many more, also returning an error message to the user. The following pattern of errors is received:</p> <p>If name is less then 28chars - The name is accepted</p> <p>If name is between 28 and 34 chars - “Internal Error, Failed to locate or create record for update” message is displayed</p> <p>If name is more then 34 chars - “Name is invalid or contains illegal characters” message is displayed</p> <p>The maximum length of the name should be limited in UI</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee77099	navigation bar(buttons) disappear after exit from Global Auth page	<p>The navigation bar (button bar on the left) in the HTML interface may disappear after the following sequence:</p> <ol style="list-style-type: none"> 1. Click System Configuration > ACS Certificate Setup > Certificate Revocation Lists. 2. Click an “Issuer Friendly Name”. 3. Click Cancel three times, which returns you to the System Configuration page. 4. Click Global Authenticate Setup. 5. Click Cancel. 6. The navigation bar disappears. <p><i>Workaround:</i> Log out of the HTML interface and log in again.</p>
CSCee81070	ACS install fails if installing on machine with running Remote Agent	<p>If Cisco Secure ACS Remote Agent is already installed on a computer that you later attempt install Cisco Secure ACS for Windows Server on, the installation of Cisco Secure ACS for Windows Server fails.</p> <p><i>Workaround:</i> Stop the remote agent service (CSAgent) before beginning the installation of Cisco Secure ACS for Windows Server.</p>
CSCee81203	DataType in SQL of int is different than int displayed in ACS	<p>AcS shows the example of SQL query to create table. The integer field in that example might be not enough depending on particular SQL server, because of different integer interpretation (like unsigned int or signed)</p> <p>So, before use the table creation example need to check how this particular SQL server interpret the integer field and modify query accordingly.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee83677	CNAC attrs type change can cause CNAC GUI error	<p>When administrator changes the type of an existing CNAC attribute using the CSUtil (or because of backup/restore) and this attribute is used in CNAC policies, the “Local Policy Configuration” page cannot be displayed and error message “An error has occurred while processing the Authen DLL Configure Page because an error occurred in the DLL processing this request” is being shown.</p> <p>For example, the attribute Trend:Software-Name is used in one of the rules and then its type was changed to integer. The bug can occur in the following situations:</p> <ol style="list-style-type: none"> 1. Attribute was deleted and then added with different type using the CSUtil. 2. Due to policies are stored in VarsDB (user database) and dictionaries in registry, administrator can get the different attrs types in dictionary and in policy doing the restore only on one of the components: user database or configuration. 3. Attribute type was modified do to CSCee83667 <p><i>Workaround:</i> On the CNAC GUI page of supplier configuration, administrator can remove the problematic policy from local policies list and thus the policy page can be displayed without any problems. Go to supplier config page, press “Local policies” button, remove problematic policy from the selected list and submit this change.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee83687	Wrong application name is being displayed	<p>When more than one network admission control (NAC) attribute (also known as a credential) has the same application type ID but the application names are different, Cisco Secure ACS always displays the application name associated with the lowest vendor ID.</p> <p>For example, if there are two credential types, VENDOR:AV (3000:03) and Cisco:Example (9:3), on the mandatory credentials list for configuring a NAC database, where “VENDOR:AV” should appear, Cisco Secure ACS will display “VENDOR:Example”.</p> <p>This problem is not obvious at first because the default attributes in Cisco Secure ACS that have the same application ID but different vendor IDs coincidentally do use the same application name. The problem arises when you add attributes that use a different application name but an application ID that is used by other attributes.</p> <p><i>Workaround:</i> Avoid adding NAC attributes whose application name is different than the application name used by other NAC attributes with the same application ID.</p>
CSCee83875	Restoring to ACS Win from ACS Sol. Engine lost Interface Cfg. data	<p>When backing up from a Cisco 1112 appliance to Cisco Secure ACS for Windows Server, all Interface Configuration attributes including TACACS+ and RADIUS Attributes were not the same as they were on the appliance.</p> <p>Also when HTTPS was enabled on the appliance, HTTPS wasn't enabled after restoring the backup to Cisco Secure ACS for Windows Server. Instead, only HTTP was used.</p> <p>These problems did not occur when a backup from Cisco Secure ACS for Windows Server was restored in Cisco Secure ACS Solution Engine.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee83977	Change in NAF is not valid until the services are restarted	<p>Given an IP-based NAR with NAF as its AAA client, if a change occurs in the NAF configuration, such as selection of a different NDG or a change to an IP range, the NAF change does not affect the NAR using the NAF until the ACS services are restarted.</p> <p><i>Workaround:</i> Restart ACS services.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee85046	odbc logger can not log attribute with name > 32 chars	<p>An imported CNAC attribute that have more then total (vendor name + application name + attribute name) of 30 characters can not be logged with ODBC logging.</p> <p>When trying to logging this attribute the “show create table” generate an SQL statement with a column name <vendor name>_< application name>_<attribute name>.</p> <p>The SQL has no problem this column. But when acs is trying to write to SQL it will not succeed. When checking the CSlog.log the column name was found but only first 32 characters where there the rest was cut. After renaming the column in the SQL to fit length of 32 characters it was successfully logged.</p> <p>For example the flowing attribute was add:</p> <pre>[attr#0] vendor-id=666 vendor-name=Automation application-id=1 application-name=AutoTest attribute-id=00003 attribute-name=Attr-3-Version attribute-profile=in out attribute-type=version</pre> <p>the show create table generate the following SQL statement:</p> <pre>CREATE TABLE failedAttempts (LoggedAt DATE NULL, Automation_ AutoTest_ Attr_3_Version VARCHAR(255) NULL)</pre> <p>in the CSlog.log the following error was found :</p> <pre>CSLog 06/15/2004 11:09:59 E 9001 4404 [odbcDLL] ODBC error 207: [Microsoft] [ODBC SQL Server Driver][SQL Server]Invalid column name 'Automation_AutoTest_Attr_3_Versi'.</pre>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee86310	Csutil -n delete all shared components and CNAC policies	<p>Using the -n option with CSUtil.exe deletes all shared profile components (shared NARs, downloadable ACLs, shared command authorization sets, and NAFs) and NAC policies (both local and external), in addition to users. References to the deleted SPCs remain in group profiles.</p> <p>Backups of the user database, including dump file created with the -d option of CSUtil.exe do preserve SPCs and NAC policies in addition to users; therefore, if you use CSUtil.exe to perform database compaction, the SPCs and policies are not lost, since database compaction depends upon the -d option to dump the database and the -l option to load it again after -n has been used to initialize the database.</p> <p><i>Workaround:</i> None at this time. We strongly recommend routine backups of ACS data and using the -d option to dump the database prior to using the -n option to initialize the database.</p>
CSCee87826	A deleted policy is being reassign when created with the same name	<p>If you delete a NAC policy while it was assigned to NAC databases and then create a new policy with the same name, ACS automatically assigns the newly created policy to the databases that the deleted policy was assigned to. An example scenario:</p> <ol style="list-style-type: none"> 1. Local policy 'policy1' is assigned to NAC database 'CNAC-DB1'. 2. 'policy1' is also assigned to NAC database 'CNAC-DB2'. 3. Customer edits 'CNAC-DB2' and deletes 'policy1'. 4. 'policy1' disappears from 'CNAC-DB1' as well. 5. Customer creates a new policy named 'policy1'. 6. ACS assigns the new policy named 'policy1' to 'CNAC-DB1'. <p><i>Workaround:</i> Use unique names for policies and never reuse them. Also, before you delete a policy, remove it from all NAC databases except the one database you use to access the policy when you delete it.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee87899	Replication of CNAC policies should be updated in the doc	<p>Documentation incorrectly states that replication of NAC policies is affected by the order in which the NAC databases are created on the primary and secondary ACSes. This is wrong.</p> <p>Also, the following information is missing from the user guide and online documentation:</p> <p>NAC databases are not replicated, just as any external user database configurations are not replicated, but local and external NAC policies are replicated; therefore, to ensure that replicated policies are associated with the correct NAC databases on secondary ACSes, you must take the following steps on each secondary ACS that receives replicated NAC policies:</p> <ol style="list-style-type: none"> 1. For each NAC database on the primary ACS, create a NAC DB of the same name on the secondary ACS. 2. In each NAC database, define same mandatory credentials. 3. For each policy on the primary ACS, create policies with the same names on the secondary ACS. 4. Assign the policies to the NAC databases in the secondary ACS in the same way they assigned on the primary ACS. <p>When replication occurs, the NAC database configurations on the secondary are not affected, including how policies are assigned to them, but the contents of the policies are updated to reflect any changes on the primary ACS.</p>
CSCee88831	days-since-last-update operator should compare to GMT	<p>Whenever ACS uses the operator days-since-last-update to evaluate a network admission control attribute, ACS compares the time that it got from the NAC client to ACS local time instead of comparing to Greenwich Mean Time (GMT).</p> <p><i>Workaround:</i> Set local time on the ACS server to GMT.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCee88908	CSLog crash if a logged attribute is deleted due to replication	<p>The CSLog service on a secondary ACS will not stop or start for the following reason:</p> <ol style="list-style-type: none"> 1. Primary and secondary ACSes (either Windows or Solution Engine) have custom NAC attributes 2. Custom NAC attributes on the primary ACS have been deleted 3. The NAC attributes deleted on the primary ACS are selected to be logged on the secondary ACS 4. Replication succeeded <p>If you encounter this problem, please call TAC for assistance.</p> <p><i>Workaround:</i> If you delete NAC attributes on a primary ACS, be sure that the NAC attributes are deleted on secondary ACSes BEFORE the next replication event.</p>
CSCee89510	dates are logged in local time instead of GMT	<p>NAC attributes that are in date format are in GMT timezone. When ACS logs these attributes, it converts them to ACS local timezone (the timezone of the ACS server).</p> <p><i>Workaround:</i> Configure ACS to use the GMT timezone.</p>
CSCef16320	Upgrading to 3.3 causes Attributes not to be seen in the R.Agent CSV	<p>When Upgrading Appliance 323 to 3.3, all the CNAC Attributes (Cisco:PA, Cisco:HIP, Symantec:AV, NAI:AV, Trend:AV, Application-Posture-Token, System-Posture-Token, Reason) didn't moved to the "CSV Failed Attempts" and to the "CSV Passed Authentications" in the Remote Agent Logging Configuration.</p> <p>Same Problem occurred when upgrading software to 3.3, Backup it and Restore it on Appliance 3.3.</p>

Table 3 Known Problems in Cisco Secure ACS for Windows Server 3.3 (continued)

Bug ID	Summary	Explanation
CSCef28686	CSUtil password parsing errors when using marks	CSUtil parses tokens (strings) either delimited by spaces, tabs and newlines OR set between a pair of quotation marks (") if a user's password starts with " and includes another " within it (e.g "user1\$"3) parsing is incorrect and potentially results in undesired error. The parsed password is different than the intended (user1\$ rather than "user1\$"3). <i>Workaround:</i> None.
CSCef76208	CSAuth Thread not closed, blocks NDS authentication until timeout	CSAuth thread may not close connection, blocking subsequent authentication attempts until the thread timeouts.

Resolved Problems

[Table 4](#) describes problems resolved in Cisco Secure ACS 3.3.2. [Table 5](#) describes problems resolved in Cisco Secure ACS 3.3.1.



Note

Bug summaries in [Table 4](#) and [Table 5](#) are printed word-for-word as they appear in our bug tracking system.

Table 4 Resolved Problems in Cisco Secure ACS 3.3.2

Bug ID	Summary	Explanation
CSCef81506	ACS generates CSR with wrong version number.	ACS now generates CSR with the correct version.
CSCef62937	RA connection timeout required	When connection to RA is broken, the authentication now works properly.
CSCef61828	MSCHAPv2 Password change problems in special conditions	If username does not includes domain name and AD initiated password change procedure by it's policy, user now receives password change dialog.

Table 4 *Resolved Problems in Cisco Secure ACS 3.3.2 (continued)*

Bug ID	Summary	Explanation
CSCef61749	EndPoint leaks memory when an encrypted connection is closed	The end point no longer leaks memory. Resolved but not verified.
CSCef47975	Integer and IP radius attributes corrupted on RADIUS proxy	When ACS Windows is configured as RADIUS proxy for another Radius server, fields are no longer corrupted in the radius proxy message sent by ACS.
CSCef47917	ACS Appliance intermittently cannot talk with remote agent	Duplicate of CSCef00468. Fixed.
CSCef46527	Error in MAC list in Generic EAP causes CSRadius 100% CPU time	The MAC address list algorithm has been fixed.
CSCef46478	Supplier selection for CSDB users does not work	The supplier selection for CSDB users now works. Ensure that all Windows AD appears after all other configured external DBs.
CSCef46186	ODBC logging error 1830 says date format set by ACS 3.3 does not match the default format of Oracle	The ODBC is now logging all attributes successfully.
CSCef34765	Upgrades from ACS 3.1 to 3.3 will stop RSA Secure ID Authentication	Upgrades no longer stop RSA Secure ID authentication. Although, some Windows behavior problems may still occur. Since Windows AD returns code 1326L either if user not present or password not valid - it is very difficult to distinguish between them. Hence, if Window AD is present in the list of external DBs and occupies first place, it will fail all authentication. The most appropriate workaround of this issue is to keep Windows AD <code>_AFTER_</code> all other configured external DBs.
CSCef30310	Only last line of an Access Filters list applied during RDBMS import	RDBMS Synchronization is no longer broken for Action Codes 120/122 and 121/123.
CSCef29903	ACS truncates password longer than 16 bytes when token server is used	When ACS is configured to use a "RADIUS Token Server" external database, the password is no longer truncated.

Table 4 *Resolved Problems in Cisco Secure ACS 3.3.2 (continued)*

Bug ID	Summary	Explanation
CSCef25874	If log file browsed, web session might crash	The CSAdmin process no longer crashes when trying to access reports where their csv files were in size of 4096, 8192, and so on.
CSCef18815	HTTP parsing error results in a failed HCAP validation in CNAC	The parsing error no longer occurs when the HTTP headers are broken into separate TCP packets.
CSCef05950	Access to ACS Admin without Authentication	User can access the ACS Admin Gui with the same port of the ACS admin as long as the browser of the ACS Admin is still open and ACS Admin Access policy is the default one (HTTP), otherwise the user will be declined.
CSCef00468	Appliance cannot open new connection to RA after several connection failures	After a limit of connection failures occur between ACS Appliance and Remote Agent, new connections can be initiated.
CSCee86457	MS PEAP pwd change not work for unknown user with CNAC	When using the external Windows database together with a different type of external user database, if a user is not cached in the internal database and user must change password on first login, the change password will no longer fail.
CSCec60586	No Action id available to set Per User Cmd authorization	For enabling the per-user command authorization, an additional value “per user” was added for V1 field in action code 270.

Table 5 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
CSCdy51214	fail to delete aaa server when its in sync table/aaa server side	Deletion of AAA server entries occurs without error.
CSCdy59706	CAA messaging wont work with ppp callback and callin authentication	Documentation is updated to explain CiscoSecure Authentication Agent limitations with respect to PPP.
CSCdz61875	Configured Default Proxy Distribution Entry is not restored	The “(Default)” entry in the Proxy Distribution Table is restored correctly.

Table 5 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
CSCea67901	UCP has trouble with dots in usernames	HTML pages show whole usernames including the dot character.
CSCea71759	Headline of UCP application stating Cisco Secure ACS	The headline of the User-Changeable Passwords application reads correctly.
CSCeb15219	Couldnt add NAS filter by CSDdsync	Action code 122 works appropriately.
CSCeb23766	Inconsistency with ACS response if username contains invalid chars	Cisco Secure ACS responds consistently to RADIUS requests containing invalid usernames.
CSCeb32885	schedule backup don't work properly	Scheduled backups operate correctly.
CSCeb47081	Using VOIP accounting with CID as user names cause to problem	Cisco Secure ACS properly handles VoIP accounting with CID used for usernames.
CSCeb58021	Server Hello packet of TLS from ACS Server has garbage.	TLS packets contain valid data.
CSCeb58107	cisco-nas-port attribute should be included in VoIP accounting log	The cisco-nas-port attribute is available for VoIP accounting logs.
CSCeb62893	T+ does not closes registry key, causes windows error 1450	Cisco Secure ACS handles use of registry keys correctly when performing TACACS+ operations.
CSCeb63032	SPC names are limited to 31 characters in size	Names of shared profile components allow the correct number of valid characters.
CSCeb63188	database define with special chars permitted but unusable later	We only permit databases to be named with valid characters.
CSCeb77357	ACS strips off CN from DN for GroupObjectType	Cisco Secure ACS displays LDAP group names correctly.
CSCeb78279	ACS 3.2 is unable to authenticate users in external database	Authentication works correctly.
CSCeb82133	PEAP re-keying type not logged to Failed log	PEAP rekeying is logged accurately.

Table 5 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
CSCeb82136	ACL size 35K cannot be edited - The page cannot be displayed	The HTML interface handles large ACL content correctly.
CSCeb82554	External User database group mapping not works with NDS	NDS group mapping operates correctly.
CSCeb84811	ACS strips off CN from DN for GroupObjectType	Cisco Secure ACS displays LDAP group names correctly.
CSCec00119	SQL accounting causes cslog crash for Ascend acct packet >=529&<=535	ODBC logging of Ascend RADIUS packets does not cause the CSLog service to crash.
CSCec00299	SQL accounting causes cslog crash for Ascend acct packet >=529&<=535	ODBC logging of Ascend RADIUS packets does not cause the CSLog service to crash.
CSCec00789	Calling-Station-ID attribute description inaccurate	We corrected the description of the Calling-Station-ID attribute.
CSCec05303	VPN3000 downloadable ACL not working on upgraded ACS	Downloadable ACLs that existed prior to upgrades work correctly.
CSCec06340	acs is miscalculating the user-password when proxying	Cisco Secure ACS proxies user passwords correctly.
CSCec09349	Replication over slow link fails - CSAUTH restarted	Replication timeout is configurable, allowing you to account for replication over slow connections.
CSCec18522	PIX downloadable ACLs do not allow -; no pix object groups	Hyphens are no longer allowed in downloadable ACL content.
CSCec18573	Replication of VMS configurations requires restart of CSAdmin	VMS configuration replication no longer requires restart of CSAdmin.
CSCec19050	acs might crash due to misbehaviour under stress of endpoint.dll	Cisco Secure ACS operates correctly under stress of the endpoint.dll file.
CSCec39523	Proxy ACS changes upper case letters to lower in username RADIUS att	Usernames case is preserved in RADIUS proxying.

Table 5 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
CSCec46370	Group mapping misbehavior	Group specification by the cisco-av-pair RADIUS VSA behaves correctly when the group number returned from the external RADIUS server is 500.
CSCec54370	DOC - Cross-domain group memberships cannot be used in mappings	Documentation reflects the limitations of group mapping for users authenticated by Windows user databases.
CSCec55657	doc wrongly says CSUtil imports SENDAUTH passwords	Documentation reflects the lack of CSUtil support for importing SENDAUTH passwords
CSCec57161	wrong ODBC logging causes major CSLog mem leak & stop local logging	Incorrect ODBD logging configuration is handled more gracefully.
CSCec61799	Eventhough the RDBMS synchronization succeeds, error says it did not.	RDBMS Synchronization no longer produces an incorrect error message.
CSCec63624	ACS 3.2 admin gui locks and displays action canceled message	The HTML interface operates correctly.
CSCec73065	csutil messup NAR if CR/LF in description field	Newly submitted shared profile components, such as network access restrictions, downloadable ACLs, and network access filters, are scanned when you submit them and any carriage returns in the description are changed to blanks, preventing a formatting error during database restoration.
CSCed01640	Memory leak in CSAuth caused with Leap-Proxy scenario	We fixed the memory leak.
CSCed33624	CSRADIUS fails to start if RDS.log is longer than 4GB	CSRADIUS can handle files much larger than 4 GB.
CSCed39969	PIX Command Authorization Sets assignment feature does not work.	Documentation explains the limitations inherent in the PIX Shell Command Authorization feature.
CSCed42094	RADIUS proxy fails due to small timeout value	Timeout for RADIUS proxy has been increased to 10 seconds.

Table 5 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
CSCed43307	Administrator access to report User Change Password	Administrator permissions correctly grant or deny administrators access to the User Password Changes report.
CSCed43496	acs 3.2 odbc fields limited to 50 characters	ODBC logging no longer inappropriately truncates attribute length.
CSCed61135	DOC - Certificate Signing Request for public CA	Documentation explains all valid values for certificate signing requests.
CSCed65806	no logging/wrong ODBC attr logging causes major performance issues	Cisco Secure ACS gracefully handles ODBC logging errors when the attributes in the packet received do not match the columns in the ODBC table.
CSCed71133	All Other Combinations mapping ignored when group fetch fails	The All Other Combinations group mapping is honored correctly.
CSCed82937	Password attribute malformed to external RADIUS token database	Password attributes sent to external RADIUS token servers are formed correctly.
CSCed95272	Document ACS Group Mapping Feature only supports up to 500 WinGroups	Documentation includes an explanation of the 400 group limit.
CSCee41393	Action Code 163 example is wrong in user guide	We corrected the documentation.
CSCee49269	ACS server ignore EAP id of LEAP client challenge	Cisco Secure ACS handles the EAP ID of a LEAP client challenge correctly.
CSCee50132	Windows Callback does not work with EAP-TLS over dial-in	The callback feature operates with EAP-TLS dialin authentication.
CSCee58096	Cisco Generic EAP not associated with vendor RADIUS (Cisco VPN 3000)	Generic EAP is associated with the Cisco VPN 3000 RADIUS vendor.
CSCin45582	VMS2.2-BT:Shared Profile components are not overwritten	Unregistering and reregistering a management center application with Cisco Secure ACS causes the role-based settings for that application to be reset to default settings in Cisco Secure ACS.

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/univercd/home/home.htm>

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

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

Access to all tools on the Cisco Technical Support 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>

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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>

- *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>

- 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 “[Related Documentation](#)” section.



Copyright © 2003–2004 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.