



Release Notes for Cisco Secure ACS Solution Engine 3.3.3

October 2005

Full Build Number: 3.3.3.11

These release notes pertain to Cisco Secure Access Control Server Solution Engine (Cisco Secure ACS) version 3.3.3



Note

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 3.3.3.11, Appliance Management Software 3.3.3.5, and Appliance Base Image (1111 - 3.3.1.4 and 1112 - 3.3.1.8). Elsewhere in this document where 3.3.3 is used, it refers to 3.3.3.11. 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](#), includes new features from 3.3.1 to 3.3.3
- [Supplemental License Agreement for Cisco Systems Network Management Software Running on the Cisco 11XX Hardware Platform, page 5](#)

CISCO SYSTEMS



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Product Documentation](#), page 6
- [Related Documentation](#), page 7
- [Installation Notes](#), page 8
- [Upgrading to Cisco Secure ACS 3.3.3 from 3.2](#), page 15
- [Recovering Cisco Secure ACS 3.3](#), page 22
- [Security Patch Process](#), page 22
- [Limitations and Restrictions](#), page 23
 - [Important Known Problems with Network Admission Control](#), page 23
 - [Supported Migration Versions](#), page 23
 - [Supported Web Browsers](#), page 24
 - [Supported Operating Systems for Remote Agent](#), page 25
 - [Supported Platforms for CiscoSecure Authentication Agent](#), page 28
 - [Other Supported Devices and Software](#), page 29
- [Documentation Updates](#), page 29
- [Known Problems](#), page 30
- [Resolved Problems](#), page 49
- [Obtaining Documentation](#), page 61
- [Documentation Feedback](#), page 62
- [Obtaining Technical Assistance](#), page 62
- [Obtaining Additional Publications and Information](#), page 64

New Features

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

- **SNMP Support**—Cisco Secure ACS provides Simple Network Management Protocol (SNMP) support for the appliance only. The SNMP agent provides read-only SNMP v1 and SNMP v2c support. The supported MIBs include:
 - Structure and Identification of Management Information for TCP/IP-based Internets (1155)

- SNMP (1157)
- Management Information Base for Network Management of TCP/IP-based internets: MIB-II (1213)
- MIB-II and LAN Manager MIB-II for Windows
- Host Resources MIB (RFC 1514/2790)

The SNMP agent is configurable on the appliance configuration page.

- **Network admission control (NAC)**—Cisco Secure ACS acts as a policy decision point in NAC deployments. Using policies that you configure, it evaluates the credentials sent to it by the Cisco Trust Agent, determines the state of the host, and sends the AAA client ACLs that are appropriate to the host state. By evaluating the host credentials many specific policies can be enforced, such as operating system patch level and antivirus DAT file version. Cisco Secure ACS records the results of policy evaluation for use with your monitoring system. You can evaluate policies locally by the Cisco Secure ACS or by an external policy server to which Cisco Secure ACS forwards credentials. For example, credentials that are specific to an antivirus vendor can be forwarded to the vendor antivirus policy server.
- **Cisco Security Agent integration (CSA)**—Cisco Secure ACS Solution Engine ships with a preinstalled, standalone CSA. This integration in the base appliance image helps to protect Cisco Secure ACS Solution Engine from day-zero attacks. The new behavior-based technology available with CSA protects Cisco Secure ACS Solution Engine against the constantly changing threats that viruses and worms pose.
- **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 the 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
 - support a variety of user and password database types
 - support password expiration and change
 - is flexible, easy to deploy, and easy to manage

For example, a customer who uses Cisco LEAP can migrate to EAP-FAST for protection from dictionary attacks. Cisco Secure ACS supports EAP-FAST supplicants that are 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 that you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.
- **Network Access Filters (NAFs)**—Cisco Secure ACS includes NAFs as a new type of Shared Profile Component. NAFs 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 version 3.3 extends per-user ACL support to any layer-three network device that supports this feature. This support 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.
- **Configurable replication timeout**—An enhancement to CiscoSecure Database Replication which allows you to specify how long a replication event is permitted to continue before Cisco Secure ACS ends the replication attempt and restarts the affected services. This feature improves your ability to configure replication when network connections between replication partners are slow.

Supplemental License Agreement for Cisco Systems Network Management Software Running on the Cisco 11XX Hardware Platform

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 Cisco Secure Access Control Server Software component of the Cisco 11XX Hardware Platform is preinstalled. CD's containing tools to restore this Software to the 11XX hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported Cisco Secure Access Control Server Software on the Cisco 11XX Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 11XX Hardware Platform.
- **Software Upgrades, Major and Minor Releases.** Cisco may provide Cisco Secure Access Control Server Software updates and new version releases for the 11XX Hardware Platform. If the Software update and new version releases can be purchased through Cisco or a recognized partner or reseller, the Customer should purchase one Software update for each Cisco 11XX Hardware Platform. If the Customer is eligible to receive the Software update or new version release through a Cisco extended service program, the Customer should request to receive only one Software update or new version release per valid service contract.
- **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

Cisco sometimes updates 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 Solution Engine</i>	On Cisco.com .
<i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816532).¹
<i>User Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816534=).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>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • PDF on the product CD-ROM. • On Cisco.com.
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine</i>	On Cisco.com .

Table 1 *Product Documentation (continued)*

Document Title	Available Formats
<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.

1. See [Obtaining Documentation](#), page 61.

Related Documentation



Note

Cisco sometimes updates 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 for Windows Server; however, much of the information contained in these papers is applicable to Cisco Secure ACS Solution Engine. 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 for constructing a scalable network device-management system by using familiar and efficient TCP/IP protocols and utilities that Cisco devices support.
<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 the capabilities of Cisco Secure ACS.

Table 2 *Related Documentation (continued)*

Document Title	Description and Available Formats
<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.
<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.

Installation Notes

For information about installing Cisco Secure ACS, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

Upgrading to Cisco Secure ACS

[Table 3](#) describes the upgrade procedures for the Cisco Secure ACS software based on the device that you are using, the upgrade path, and whether you want to install the SNMP support feature. [Table 4](#) describes various installation use cases that may assist you in deciding the appropriate procedure to follow.



Caution

Backup and restore are supported and tested only when done on the *same* version. For example, back up on 3.3.3 and restore on 3.3.3 is supported; not backup on 3.3.2 and restore on 3.3.3.

Table 3 *Cisco Secure ACS Upgrade Paths*

Cisco Device	From Version	Upgrade Procedure
Cisco 1111	3.3.x	Upgrading to Cisco Secure ACS 3.3.3 from 3.3, page 10
Cisco 1112	3.3.x	Upgrading to Cisco Secure ACS 3.3.3 from 3.3, page 10
Cisco 1111	3.2.x	Upgrading to Cisco Secure ACS 3.3.3 from 3.2, page 15

**Tip**

If you failed to install Cisco Secure ACS on a previous upgrade to 3.3.1, you should do so now. Refer to the installation processes that are documented in the user guide and the installation guide.

Table 4 *Installation Use Cases*

From Version	Upgrade Procedure	Results
3.3.x or 3.2.x	<p>Use upgrade packages: Upgrade Package Appliance Management Software ACS 3.3.3.X and Upgrade Package ACS Software 3.3.3.X for Appliance and backup your data. Then use the Recovery CD¹ to upgrade the appliance and restore the data.</p> <p>For 3.3.x, see Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 10. For 3.2.x, see Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 16.</p>	<ul style="list-style-type: none"> • SNMP supported • Cisco Security Agent (CSA) installed • Data restored

Table 4 *Installation Use Cases*

From Version	Upgrade Procedure	Results
3.3.x or 3.2.x	Use the Recovery CD ¹ from Cisco Secure ACS 3.3.3 to upgrade the appliance. For 3.3.x, see Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 10 . For 3.2.x, see Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 16 .	<ul style="list-style-type: none"> • SNMP supported • Cisco Security Agent (CSA) installed • Blank database
3.3.x or 3.2.x ²	Use the Upgrade Package Appliance Management Software ACS 3.3.3.X and Upgrade Package ACS Software 3.3.3.X for Appliance. For 3.3.x, see Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support, page 13 . For 3.2.x, see Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support, page 19 .	<ul style="list-style-type: none"> • No SNMP • No Cisco Security Agent (CSA) • Data restored

1. Ensure that you are using the proper recovery files for your specific hardware (Cisco 1111 or 1112).
2. If required, you can install the CSA patch available on Cisco.com.

Upgrading to Cisco Secure ACS 3.3.3 from 3.3

The two options to choose from when upgrading are:

- [Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 10](#)
- [Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support, page 13](#)

Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support

To upgrade to 3.3.3 with the SNMP support feature, you will need to upgrade your software to 3.3.3 by using the upgrade packages, back up your configuration, reinstall ACS 3.3.3, and then restore your data.

This procedure upgrades the Cisco Secure ACS software to version 3.3.3 on a Cisco 1111 or a Cisco 1112 device.

To reinstall a Cisco 1111 or 1112 device from Cisco Secure ACS Solution Engine 3.3.1 or 3.3.2 follow these steps:

-
- Step 1** If the Cisco Secure ACS Solution Engine is running Cisco Security Agent, you must disable the CSAgent service before upgrading. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is not selected. If it is selected, clear the **CSA Enabled** check box and click **Submit**.

- Step 2** Apply the Upgrade Package Appliance Management Software, which is available on the Cisco Secure ACS 3.3. upgrade CD.

- Step 3** Apply the Upgrade Package ACS Software 3.3.3.11 for Appliance, which is available on the Cisco Secure ACS 3.3 upgrade CD.

For details on using the HTML interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For details on using the command line to upgrade, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 4** To save and restore your existing data, you must perform the following steps. If you do not want to save your data, go to [Step 4b](#).
- a. Back up Cisco Secure ACS data and configuration. To do so, use one of the two following features:
 - ACS Backup, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - The **backup** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
 - b. Use the Recovery CD from Cisco Secure ACS 3.3 to upgrade the appliance to 3.3.3. The upgrade destroys all data and installs a new image. Ensure that you have the correct version for your hardware.

For more information about reimaging the hard drive, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- c. Perform an initial configuration of the Cisco Secure ACS Appliance. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
- d. To save and restore the appliance data and configuration, use one of the two following feature. If you do not want to save your data, go to [Step 5](#).
 - ACS Restore, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - The **restore** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

You can apply upgrades by using the HTML interface or the console. For assistance with applying the upgrade by using the HTML interface, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For assistance with applying the upgrade by using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

For assistance with applying the upgrade, use the upgrade procedure in *User Guide for Cisco Secure ACS Solution Engine*.

Step 5 Verify that Cisco Security Agent is enabled. You can do so at the console or in the HTML interface:

- Using the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
- Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is selected. If not, select it and click **Submit**.

Step 6 To see the results of this upgrade procedure, view the Appliance Upgrade page. To do so, log in to the HTML interface and select **System Configuration > Appliance Upgrade Status**.

When you complete this procedure, the Application Versions table on the Appliance Upgrade page will appear:

Application Versions	
Cisco Secure ACS	3.3.3.11

Application Versions (continued)

Appliance Management Software	3.3.3.5
Appliance Base Image	Cisco 1111 - 3.3.1.4; Cisco 1112 - 3.3.1.8

Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support

If you do not want SNMP support, you will need to upgrade your Appliance Management Software and Cisco Secure ACS upgrade packages on top of the existing image as specified in the procedure below.

This procedure upgrades the Cisco Secure ACS software to version 3.3.3 on either a Cisco 1111 device or a Cisco 1112 device.

To upgrade from Cisco Secure ACS Solution Engine from 3.3.2 or 3.3.1 without SNMP support, follow these steps:

-
- Step 1** If Cisco Secure ACS Solution Engine is running Cisco Security Agent, you must disable the CSAgent service before upgrading. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is not selected. If it is selected, clear the **CSA Enabled** check box and click **Submit**.
- Step 2** Apply the Upgrade Package Appliance Management Software ACS 3.3.3.11, which is available on the Cisco Secure ACS 3.3 upgrade CD.
- Step 3** Apply the Upgrade Package ACS Software for Appliance, which is available on the Cisco Secure ACS 3.3 upgrade CD.

For details on using the HTML interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For details on using the command line to upgrade, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 4** To save and restore your existing data, you must perform the following steps. If you do not want to save your data, go to [Step 5](#).
- a. Back up Cisco Secure ACS data and configuration. To do so, use one of the two following features:
 - ACS Backup, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - **backup** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
 - b. To save and restore the appliance data and configuration, use one of the two following features. If you do not want to save your data, go to [Step 5](#).
 - ACS Restore, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - **restore** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

You can apply upgrades by using the HTML interface or the console. For assistance with applying the upgrade using the HTML interface, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For assistance with applying the upgrade using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 5** Verify that Cisco Security Agent is enabled. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is selected. If not, select it and click **Submit**.
- Step 6** To see the results of this upgrade procedure, view the Appliance Upgrade page. To do so, log in to the HTML interface and select **System Configuration > Appliance Upgrade Status**.

When you complete this procedure, the Application Versions table on the Appliance Upgrade page will appear:

Application Versions	
Cisco Secure ACS	3.3.3.11
Appliance Management Software	3.3.3.5
Appliance Base Image	Cisco 1111 - 3.3.1.4; Cisco 1112 - 3.3.1.8

Upgrading to Cisco Secure ACS 3.3.3 from 3.2

This procedure upgrades the Cisco Secure ACS software on a Cisco 1111 device to Cisco Secure ACS Solution Engine 3.3.3 from any of the following versions:

- Cisco Secure ACS Solution Engine 3.2.3
- Cisco Secure ACS Solution Engine 3.2.2
- Cisco Secure ACS Solution Engine 3.2.1



Note

Cisco 1112 devices do not support versions of Cisco Secure ACS before version 3.3; therefore, this section does not apply to Cisco 1112 devices.

Please read this procedure carefully before proceeding. Upgrading from Cisco Secure ACS 3.2.x requires additional steps that must be taken to preserve Cisco Secure ACS data and configuration.

The two options to choose from when upgrading from 3.2 are:

- [Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support, page 16](#)
- [Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support, page 19](#)

Upgrading to Cisco Secure ACS 3.3.3 with SNMP Support

To upgrade to 3.3.3 with the SNMP support features, you will need to upgrade your software to 3.3 using the upgrade packages, back up your configuration, and reinstall ACS 3.3.3. Keeping the DB requires a backup/restore.

To upgrade a Cisco 1111 device from Cisco Secure ACS Solution Engine 3.2.3, 3.2.2, or 3.2.1, follow these steps:

-
- Step 1** If the Cisco 1111 is running Cisco Security Agent, you must disable the CSAgent service before upgrading. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is not selected. If it is selected, clear the **CSA Enabled** check box and click **Submit**.

- Step 2** Determine what versions of the following software the Cisco 1111 is running:
- Cisco Secure ACS
 - Appliance Management Software
 - Patches

To do so, log in to the HTML interface, select **System Configuration > Appliance Upgrade Status**, and view the version information that appears.

- Step 3** Apply the Upgrade Package Appliance Management Software, which is available on the Cisco Secure ACS 3.3. upgrade CD.
- Step 4** Apply the Upgrade Package ACS Software 3.3.3.11 for Appliance, which is available on the Cisco Secure ACS 3.3 upgrade CD.

For details on using the HTML interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For details on using the command line to upgrade, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 5** If the Cisco 1111 that you are upgrading is running Cisco Secure ACS 3.2.1, 3.2.2, or 3.2.3 and you want to keep your database, you must perform the following steps. If you do not want to keep the database, perform the backup, but skip the restore steps ([Step 5d.](#)).
- a. Back up Cisco Secure ACS data and configuration. To do so, use one of the following features:
 - ACS Backup, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - The **backup** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
 - b. Use the Recovery CD from Cisco Secure ACS 3.3.3 to upgrade the appliance to 3.3.3. This upgrade will destroy all data and install a new image.

For more information about reimaging the hard drive, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

For assistance with applying the upgrade, use the upgrade procedure in *User Guide for Cisco Secure ACS Solution Engine*.
 - c. Perform the initial configuration of the Cisco Secure ACS Appliance. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
 - d. Restore the appliance data and configuration. To do so, use one of the following features:
 - ACS Restore, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - The **restore** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
- Step 6** If either of the following conditions is true:
- In Step 5 you reimaged the Cisco 1111 with Cisco Secure ACS 3.2.3.
 - The Cisco 1111 is running Appliance Management Software version 3.2.3.11

you must apply the “Upgrade Package Appliance Management Software ACS 3.2.3.12”, available on the Cisco Secure ACS 3.3 upgrade CD. You can apply upgrades by using the HTML interface or the console. For assistance with applying the upgrade by using the HTML interface, see the *User Guide for CiscoSecure ACS Solution Engine 3.3*. For assistance with applying the upgrade using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 7** If either of the following conditions is true:
- In Step 5 you reimaged the Cisco 1111 with Cisco Secure ACS version 3.2.3
 - The Cisco 1111 does not have the patch named “Microsoft Security Bulletin MS04-11 and MS04-012” applied

you must apply the “MS Security hotfix MS04-011 for ACS Appliance 3.2.3” patch, available on the Cisco Secure ACS 3.3 upgrade CD.

- Step 8** Verify that Cisco Security Agent is enabled. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is selected. If not, select it and click **Submit**.

- Step 9** To see the results of this upgrade procedure, view the Appliance Upgrade page. To do so, log in to the HTML interface and select **System Configuration > Appliance Upgrade Status**.

When you complete this procedure, the Application Versions table on the Appliance Upgrade page will appear:

Application Versions	
Cisco Secure ACS	3.3.3.11
Appliance Management Software	3.3.3.5
Appliance Base Image	Cisco 1111 - 3.3.1.3

Upgrading to Cisco Secure ACS 3.3.3 without SNMP Support

If you do not want SNMP support, you will need to use the management and ACS upgrade packages as specified in the procedure below.

To upgrade a Cisco 1111 device from Cisco Secure ACS Solution Engine 3.2.3, 3.2.2, or 3.2.1, follow these steps:

-
- Step 1** If the Cisco 1111 is running Cisco Security Agent, you must disable the CSAgent service before upgrading. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is not selected. If it is selected, clear the **CSA Enabled** check box and click **Submit**.

- Step 2** Determine what versions of the following software the Cisco 1111 is running:
- Cisco Secure ACS
 - Appliance Management Software

To do so, log in to the HTML interface, select **System Configuration > Appliance Upgrade Status**, and view the version information that appears.

- Step 3** Apply the Upgrade Package Appliance Management Software ACS 3.3.3.5, which is available on the Cisco Secure ACS version 3.3 upgrade CD.
- Step 4** Apply the Upgrade Package ACS Software 3.3.3.11 for Appliance, which is available on the Cisco Secure ACS 3.3.3 upgrade CD.

For assistance with applying the upgrade, use the upgrade procedure in the *User Guide for Cisco Secure ACS Solution Engine*.

- Step 5** To save and restore your existing data, you must perform the following steps. If you do not want to save your data, skip to [Step 6](#).
- a. Back up Cisco Secure ACS data and configuration. To do so, use one of the following features:
 - ACS Backup, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.

- The **backup** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.
- b. To save and restore the appliance data and configuration, use one of the following features. If you do not want to save your data, go to [Step 5](#).
 - ACS Restore, which is available in the System Configuration section of the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*.
 - **restore** command, which is available on the serial console. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

You can apply upgrades by using the HTML interface or the console. For assistance with applying the upgrade using the HTML interface, see the *User Guide for Cisco Secure ACS Solution Engine 3.3*. For assistance with applying the upgrade using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

Step 6 If you do not want to save your data, perform the following steps:

- a. Use the Recovery CD from Cisco Secure ACS 3.3 to upgrade the appliance to 3.3.3. This upgrade will destroy all data and install a new image.
For more information about reimaging the hard drive, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.2*.
- b. Perform the initial configuration of the Cisco Secure ACS Appliance. For more information, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

Step 7 If either of the following conditions is true:

- In Step 5 you reimaged the Cisco 1111 with Cisco Secure ACS 3.2.3.
- The Cisco 1111 is running Appliance Management Software version 3.2.3.11

you must apply the “Upgrade Package Appliance Management Software ACS 3.2.3.12”, available on the Cisco Secure ACS 3.3 upgrade CD. You can apply upgrades by using the HTML interface or the console. For assistance with applying the upgrade by using the HTML interface, see the *User Guide for CiscoSecure ACS Solution Engine 3.3*. For assistance with applying the upgrade using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.

- Step 8** If either of the following conditions is true:
- In Step 5 you reimaged the Cisco 1111 with Cisco Secure ACS version 3.2.3
 - The Cisco 1111 does not have the patch named “Microsoft Security Bulletin MS04-11 and MS04-012” applied

you must apply the “MS Security hotfix MS04-011 for ACS Appliance 3.2.3” patch, available on the Cisco Secure ACS 3.3 upgrade CD.

- Step 9** Verify that Cisco Security Agent is enabled. You can do so at the console or in the HTML interface:
- Using the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
 - Using the HTML interface, select **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is selected. If not, select it and click **Submit**.

- Step 10** To see the results of this upgrade procedure, view the Appliance Upgrade page. To do so, log in to the HTML interface and select **System Configuration > Appliance Upgrade Status**.

When you complete this procedure, the Application Versions table on the Appliance Upgrade page will appear:

Application Versions	
Cisco Secure ACS	3.3.3.11
Appliance Management Software	3.3.3.5
Appliance Base Image	Cisco 1111 - 3.3.1.3

Recovering Cisco Secure ACS 3.3

You can recover Cisco Secure ACS 3.3 on a Cisco 1111 or Cisco 1112 device. The recovery process for Cisco Secure ACS Solution Engine 3.3 is documented in the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*.



Caution

Be sure you use the correct recovery CD for your Cisco Secure ACS Solution Engine device. Do not use the recovery CD for Cisco 1111 devices on a Cisco 1112 device; likewise, do not use the recovery CD for Cisco 1112 devices on a Cisco 1111 device.

Security Patch Process

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.

Past 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 resolve 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, which is available in the Product Literature area for Cisco Secure ACS Solution Engine on Cisco.com.

For information on tested security patches, see [Tested Windows Security Patches, page 26](#).

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. Cisco recommends that you review them.

- [CSCee88908](#)—CSLog crash if a logged attribute is deleted due to replication, page 44
- [CSCee87826](#)—A deleted policy is being reassign when created with the same name, page 42
- [CSCee87899](#)—Replication of NAC policies should be updated in the doc, page 43

Supported Migration Versions

Cisco supports migrating to Cisco Secure ACS Solution Engine version 3.3.3 from many versions of Cisco Secure ACS for Windows Server; however, migration requires upgrading Cisco Secure ACS for Windows Server to version 3.3.3.

For detailed steps for performing a migration from Cisco Secure ACS for Windows Server to Cisco Secure ACS Solution Engine, see one of the following documents:

- *Installation Guide for Cisco Secure ACS for Windows Server 3.3*
- *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3*

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 which are 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
- Netscape Communicator for Solaris 2.8
 - Version 7.0
 - Mozilla 5.0
 - Sun Java Plug-in 1.4.0_01

**Note**

-
- Several known problems are related to using Netscape Communicator with Cisco Secure ACS. For more information, see [Table 5](#).
 - Cisco does 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.
-

Cisco does not support other versions of the previous 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 Operating Systems for Remote Agent

Cisco Secure ACS 3.3 supports Cisco Secure ACS Remote Agent on Microsoft Windows 2000 and Solaris operating systems, as specified in the following two sections.

- [Windows Support for Remote Agent, page 26](#)
- [Solaris Support for Remote Agent, page 28](#)

Windows Support for Remote Agent

The computer that runs Cisco Secure ACS Remote Agent for Windows must use an English-language version of one of the following operating systems:

- 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 with Service Pack 1 installed
- Windows Server 2003, Standard Edition with Service Pack 1 installed

**Note**

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

- Cisco Secure ACS Remote Agent for Windows is not designed to use the multiprocessor feature of any supported operating system; however, we did test the remote agent on dual-processor computers.
 - Cisco cannot support Microsoft clustering service on any supported operating system.
 - Windows 2000 Datacenter Server is not a supported operating system.
-

Tested Windows Security Patches

Cisco Secure 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](#)

Cisco Secure ACS Remote Agent for Windows 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](#)

Solaris Support for Remote Agent

The computer that runs Cisco Secure ACS Remote Agent for Solaris must use Solaris 2.8 or 2.9.

You cannot back up, restore, replicate information, or log in remotely using different versions of Cisco Secure ACS. For example:

- You cannot restore from dump files produced by using the backup process on different versions numbers of Cisco Secure ACS.
- You must not perform replication between different versions numbers of Cisco Secure ACS.
- You must not use remote logging between different versions numbers of Cisco Secure ACS.
- You must not use remote logging on Cisco Secure ACS for Windows Server software between different versions numbers of Cisco Secure ACS.

The following Cisco Secure ACS components that have identical versions and build numbers are supported and have been tested:

- Replication
- Backup/restore processes
- Remote logging software to remote ACS
- Remote logging of Windows authentication to the Cisco Secure Solution Engine.

Other combinations of authentication and remote logging agents may work together; however, they have not been tested and are not supported.

Supported Platforms for CiscoSecure Authentication Agent

For use with Cisco Secure ACS 3.3, Cisco tested CiscoSecure Authentication Agent on Windows XP with Service Pack 1. Cisco supports 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

Other Supported Devices and Software

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

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

Documentation Updates

This section describes new or changed documentation for this release.

Configuring SNMP Support

To configure the SNMP Agent, select **System Configuration > Appliance Configuration** from the navigation bar. For more details, see the online help.

Using the CRL Issuer Page

The CRL Issuers Page has been revised. You can no longer add a CRL by using this page. A CRL is automatically added to the CRL Issuers page after you select a CA in the Certificate Trust List. The CRL Issuers list contains an entry for every trusted CA in the Certificate Trust List.

Installation Guide Chassis Figures Updated

The front and back panel figures in the *Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3* have been updated.

LDAP Multi-Threading

Cisco Secure ACS 3.3.3 now processes multiple LDAP authentication requests in parallel as opposed to the sequential processing mechanism in versions earlier than 3.2.

Unknown NAS Authentication Failure

Documentation on unknown NAS authentication failure can be found in the Troubleshooting section of the *User Guide for Cisco Secure ACS Solution Engine*.

Known Problems

This section contains information about the following topics:

- [Cisco AAA Client Problems, page 30](#)
- [Known Microsoft Problems, page 31](#)
- [Known Problems in Cisco Secure ACS 3.3, page 31](#)

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. You can download the hotfix at <http://www.microsoft.com>. A workaround is to disable Fast Reconnect.

Known Problems in Cisco Secure ACS 3.3

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

•

Table 5 **Known Problems in Cisco Secure ACS Solution Engine 3.3**

Bug ID	Summary	Explanation
CSCdv86708	HTTP Port Allocation is not replicated	<p>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.</p> <p><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, restart the CSAdmin service.</p>
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. See Supported Web Browsers, page 24.</p>

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
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>
CSCea62226	CSAgent (Solaris) - appliance present the RA as running while is not	<p>The HTML interface of a Cisco Secure ACS Appliance indicates that the logging service of a Solaris remote agent is available even though it is not. For Solaris remote agents, the service status displayed for the remote agent in Network Configuration is not reliable.</p> <p><i>Workaround/Solution:</i> Log into the computer running the Solaris remote agent to determine if the CSLogAgent process is running.</p>

Table 5 *Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)*

Bug ID	Summary	Explanation
CSCea74289	cascade replication due to user pass change-does not work	<p>Cascading replication does not occur when the replication trigger in the user password changes 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>
CSCea87748	Downloadable ACLs deleted and downsized after backup via CLI	<p>If your Cisco Secure ACS Appliance has downloadable ACLs that have more than approximately 31 kilobytes of text, and you use the system console to back up and restore the database; the downloadable ACLs are truncated to approximately 31 kilobytes or are deleted entirely.</p> <p><i>Workaround/Solution:</i> Do not create downloadable ACLs that contain more than 30 kilobytes of data. If your DACLs exceed 30 kilobytes, keep text file records of the ACLs. Then if a restoration performed from the system console is necessary, you can recreate the downloadable ACLs.</p>

Table 5 Known Problems in Cisco Secure ACS Solution Engine 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 reregister 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 reregister all MCs.</p> <p>Log out of CiscoWorks.</p>
CSCeb21037	Windows Remote Agent uninstall issue	<p>Uninstalling Cisco Secure Remote Agent for Windows does not remove some subdirectories, such as those that contain log files.</p> <p><i>Workaround/Solution:</i> Manually delete the directories left by the uninstallation process.</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 they are working on the downloadable ACLs.</p>

Table 5 Known Problems in Cisco Secure ACS Solution Engine 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 environments where primary and secondary Cisco Secure ACS servers are kept in synch by using the replication feature, authentication may fail for users defined in an external database s. 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 are 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>

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCec64143	Uninstalling Win Remote Agent when uninstall terminates unexpected	<p>When Windows Remote Agent uninstallation process terminates unexpectedly and the uninstallation process could not be completed, registry keys remain for the remote agent. Further attempts to install the remote agent will fail due to these registry keys.</p> <p><i>Workaround:</i> Use regedit to delete all Cisco Remote Agent entries. In the registry, search for csagent and acs agent. Delete all matching entries. If they cannot be deleted, ignore them.</p>
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 by using an administrator account that doesn't have access to all groups.</p> <p>If a page of the Disabled Accounts report has users who belong 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>
CSCed42437	RADIUS Proxy with Cisco PEAP operates only with RADIUS Aironet	—
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	—

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCed77992	Action Code 211 does not 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>
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>
CSCee38482	Admin account can see all users who 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>

Table 5 *Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)*

Bug ID	Summary	Explanation
CSCee58593	CSAdmin restart during Replication between two ACS SW in slow link	<p>When replication occurs between two Cisco Secure ACSs in slow link (128k), the services of the primary ACS are restarted 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 • CSAAuth • CSTacacs • CSRradius
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 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 appears</p> <p>If name is more then 34 chars - “Name is invalid or contains illegal characters” message appears</p> <p>The maximum length of the name should be limited in UI</p>
CSCee73004	CSLog handles reach more than 11,000 after failed ODBC connections	<p>The message queue was added to CSAAuth for message storage and dedicated thread which actually log the messages from the queue. The default message number in queue is 20K, but it can be managed by registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AAAv3.3\CSAuth\MaxMsgInLogQueue</p>

Table 5 Known Problems in Cisco Secure ACS Solution Engine 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>
CSCee78472	Netscape prevents pressing links inside the Logging configuration	<p>Using Netscape Communicator 7.1 on Windows 2000 Server to access the HTML interface of Cisco Secure ACS can result in a “The document contains no data” error message from Netscape.</p> <p><i>Workaround:</i> Use a different supported browser. See Supported Web Browsers, page 24.</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 on which you later attempt to install Cisco Secure ACS for Windows Server, 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>

Table 5 *Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)*

Bug ID	Summary	Explanation
CSCee83687	Wrong application name appears	<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 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCee83977	Change in NAF is not valid until the services are restarted	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. <i>Workaround:</i> Restart ACS services.
CSCee84044	Restore form SW to APPL delete all NAC attributes from remote agent	—
CSCee84048	New attributes do not replicate to remote agent	—
CSCee87826	A deleted policy is being reassign when created with the same name	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: <ol style="list-style-type: none"> 1. Local policy 'policy1' is assigned to NAC database 'NAC-DB1'. 2. 'policy1' is also assigned to NAC database 'NAC-DB2'. 3. Customer edits 'NAC-DB2' and deletes 'policy1'. 4. 'policy1' disappears from 'NAC-DB1' as well. 5. Customer creates a new policy named 'policy1'. 6. ACS assigns the new policy named 'policy1' to 'NAC-DB1'. 7. <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.

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCee87899	Replication of NAC 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 ACSs. 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 ACSs, 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 5 Known Problems in Cisco Secure ACS Solution Engine 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 ACSs (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 ACSs 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>
CSCef61117	ACS on 2003 huge performance impact when writing to registry	<p>Cisco Secure ACS 3.2.3 or 3.3 running on Windows 2003 Standard and Enterprise edition may cause a huge delay when writing to the registry.</p> <p>Therefore when more than six operations write to the Microsoft registry, a failure may occur. Refer to the field notices on Cisco.com for more details.</p>
CSCef64318	CSTacacs process exhibits high CPU consumption	<p>There was a problem with regexp code used by TACACS code. The regexp code was not multi-thread safe. The problem has been fixed. It is hard to reproduce the problem. However, probability of its occurrence grows with number of concurrent TACACS authorization requests for commands which arguments defined using regular expression syntax.</p>

Table 5 **Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)**

Bug ID	Summary	Explanation
CSCeg20307	Unable to authenticate user, found in unknown external DB after upgrade	Users that upgraded to version 3.3.1 or 3.3.2 and were previously authenticated with a Token Server database no longer see an "Unknown DB type 0d00" error in the Authenticate With field.
CSCeg40355	Authentication breaks when lost connectivity to remote log server	<p><i>Symptom:</i> An ACS server may fail an authentication attempt but log the attempt as successful.</p> <p><i>Conditions:</i> If one ACS server is configured to log remotely the passed authentications to another acs server AND that remote acs server is available, everything functions as expected.</p> <p>If the remote acs server is not avail (link down) the user will be notified authentication failed (i.e. via telnet) however, the acs server will log this as a successful authentication.</p> <p><i>Workaround:</i> To restore service you need to do one of the following: bring the link back up on remote ACS or turn off remote logging on local ACS. This will be fixed in the next release.</p>
CSCeg51873	ACS chooses wrong NDG for NAR with TACACS/RADIUS NAS on same IP	ACS chooses the wrong NDG for NAR matching if both a TACACS+ and RADIUS NAS are defined with the same IP and placed in separate NDGs and the authentication is performed via RADIUS. The NDG containing the TACACS+ NAS will always be used.
CSCeh00074	GUI/ LDAP group mapping submission failure	This behavior sometimes occurs sometimes of various browsers and java plug-in configurations.
CSCeh04327	SNMP get and get-next requests for host.hrSystemNumUsers return error	SNMP 'get' and 'get-next' requests for host.hrSystemNumUsers return 'Generic error'.

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCeh01822	Radius-Proxy with MS-CHAPv2 authentication failed when using strip	When trying to authenticate dialup client using MS-CHAPv2 to the ACS proxy server which forwards the username without the suffix (i.e. with strip) to the second ACS, the authentication failed. When using prefix characters with ".", "/", "-" at the end, the authentication failed.
CSCeh09266	Errors occurs while installing ACS on directory with special chars	Do not install ACS in a directory which contains one of the following characters "~!@#%\$^&()". Microsoft Windows cannot understand the path later.
CSCeh09351	ACS Appliance shows constantly high CPU	<i>Symptom:</i> Appliance Status Page shows always high CPU, which is inconsistent with the output of the 'Status' page and the information within the 'package.cab'. <i>Workaround:</i> No workaround.
CSCeh17061	ACS Remote Agent uninstall program does not delete all files/folders	Not all files are deleted when an uninstall of RA is initiated. <i>Workaround:</i> Stop RA before performing an uninstall.
CSCeh19171	NAC Attributes on RA logging are not added after upgrading on HP	The NAC attributes disappear on the appliance after upgrading to 3.3.3. Workaround is to add them manually after the upgrade.
CSCeh20969	Fully Qualified Novell names are not authenticated	If the username contains a period (.) it may not authenticate against NDS.
CSCeh24688	CSAuth mem leak after EAP-TLS authentications to LDAP	CSAuth memory consumption increases after EAP-TLS authentications to LDAP. The memory problem was found in LDAP SDK library. No workaround.
CSCeh25025	Upgrade of CRL does not keep all CRL info	CRL upgrade doesn't keep the CRL description.
CSCeh25112	Network Access Filter (NAF) reedit requests restart.	After editing NAF data, no changes are updated on ACS. Workaround is to restart from the services control to update the changes.

Table 5 **Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)**

Bug ID	Summary	Explanation
CSCeh25166	Field src IP Address in NAR gets illegal values	An invalid src IP address value can be entered when editing the NAR. No workaround.
CSCeh38960	Restoring from SW removes the Appliance entry inside the proxy	When restoring the database from the software version to an appliance the restore removes the default proxy entry (appliance itself) from the proxy table. <i>Workaround:</i> Use the backup from the appliance version or add the default proxy entry manually.
CSCeh41690	Documentation does not include default TACACS+ NAS configuration	Documenting default TACACS+ NAS configuration to accommodate any non-configured NAS in ACS cannot be found in the User Guide. This feature is available, but is documented in the following location: http://www.cisco.com/en/US/partner/products/sw/securew/ps2086/products_user_guide_chapter09186a0080205a45.html
CSCeh44022	Replication errors in CSAAuth on CryptDecrypt	There are some errors in csauth.log files related to replication and Windows Crypto API on win 2003.
CSCeh50690	Install ACS certificate from storage is not supported if CA server is on Windows 2003	This is a Microsoft bug. Refer to Microsoft documentation in order to generate certificates with exportable private keys.
CSCeh52808	Admin session is timed out when configuring long list of permit addr	When configuring a long list of permitted IP addresses (Accept SNMP packets from selected hosts), the administration session times out after submitting the list. <i>Work around:</i> Do not enter more then 10 IPs. Worst case, if more are configured, the system will accept it but the user will have to start a new admin session.
CSCeh52846	EAP-TLS against LDAP is responding Too Busy to handle connection	After heavy load of EAP-TLS authentications against LDAP DB all handles are occupied and the log shows : "Too Busy to handle connection" error message." <i>Workaround :</i> Restart CSAAuth.

Table 5 Known Problems in Cisco Secure ACS Solution Engine 3.3 (continued)

Bug ID	Summary	Explanation
CSCeh54670	ACS could not find user in AD if sent w/out domain name	When using EAP-TLS AD authentication, the user name should contains domain name.
CSCeh81080	ACS does not record an error when retying same C-PEAP client Password	Cisco-PEAP client that has to change passwords at next logon and enters the same password, does not get any error from fail-attempts log in ACS.
CSCeh82247	ACS with Netscape on Solaris OS with JRE 1.5	Netscape on Solaris OS with JRE 1.5 does not work well with ACS. Various problems occur.
CSCeh84997	Replication fails to create backup dir RegValues	<p><i>Symptoms:</i> The following error may be generated by the ACS appliance or ACS Windows server after a database replication.</p> <p>Database Replication.csv file:</p> <pre>ERROR Outbound database replication failed - refer to CSAuth log file</pre> <p>CSAuth log file:</p> <pre>CSBackupRestore(OUT) Failed to create output directory C:\Program Files\CiscoSecure ACS v3.3\CSAuth\DbSyncScratch\\RegValues for DLL</pre> <p><i>Conditions:</i> The target folder on the replication slave machine already exists.</p> <p><i>Workaround:</i> Delete the target folder.</p>
CSCeh91809	VoIP messages cause CSRADIUS service unexpected termination	—
CSCeh91820	Inserting malformed description under CRL Issuer closes the session	Use of a javascript tokens in the CRL description causes the current admin session to close.

Resolved Problems

[Table 6](#) describes problems resolved in Cisco Secure ACS Solution Engine 3.3.3.
[Table 7](#) describes problems resolved in Cisco Secure ACS Solution Engine 3.3.2.
[Table 8](#) describes problems resolved in Cisco Secure ACS Solution Engine 3.3.1.



Note Bug summaries in [Table 6](#) through [Table 8](#) are printed word-for-word as they appear in our bug tracking system.

Table 6 *Resolved Problems in Cisco Secure ACS 3.3.3*

Bug ID	Summary	Explanation
Resolved Problems Common to All Cisco Secure ACS Version 3.3 Platforms		
CSCeh54669	CSAuth crashed when supplicant sent UPN without domain	When a username is different from a pre-Windows name and the supplicant sends the user name without a domain name, the CSAuth service does not break.
CSCeh32487	TCP checksum on hardware	<p>Problem A Cisco Secure Access Control Server Solution Engine (ACS SE) 1111 (CSACSE-1111-UP-K9) and 1112 (CSACSE-1112-K9) Hardware may generate transient TCP Checksum errors which may cause error logging on other devices in the network. In particular, Cisco switches would generate the following error message: IP-3-TCP_BADCKSUM:TCP bad checksum</p> <p>The cause of the error is the NIC Software Driver. Not every packet being transmitted will be affected. Given that TCP will retransmit any unacknowledged packet, the system will recover. There may be excessive logging of the error message within the network. The problem only affects TCP packets; therefore TACACS may be affected, while RADIUS will not.</p> <p>(continued)</p>

Table 6 *Resolved Problems in Cisco Secure ACS 3.3.3*

Bug ID	Summary	Explanation
CSCeh32487	TCP checksum on hardware	<p>Workaround A temporary workaround is to reload the server; while the problem is transient, it will likely return within days or weeks. To resolve the problem, install a patch (appl_All_Versions_HP_TCP_checksum_Patch.zip for the Cisco 1111 and appl_Quanta_TCP_checksum_MTU_Patch.zip for the Cisco 1112) from:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/solution_engine</p> <p>The fix is integrated into the 1111 Base Image version 3.3.1.4-HP and later and resolves the TCP checksum issue. The fix is integrated into the 1112 Base Image version 3.3.1.8-Quanta and later and resolves the TCP checksum issue and sets the MTU value to 1500. Use the CLI show command output command or the Appliance Upgrade status page to confirm the current version in use.</p>
CSCeg88336/ CSCeg82632	ACS server allows for remote file retrieval	Authorized users can no longer retrieve arbitrary files via the web interface.
CSCeg82170	ACS admin with no ACS Certificate Setup privileges can generate CSR & Self-Signed Certificates	Generate Self-Signed Certificate and Generate Certificate Signing Request are denied for administrator with no 'ACS Certificate Setup' privilege.
CSCeg81851	ACS exception in RDS.log if quota is configured	When usage quota is turned on for default group radius service exception no longer appears.

Table 6 Resolved Problems in Cisco Secure ACS 3.3.3

Bug ID	Summary	Explanation
CSCeg76049	When a replication is > 5 minutes, a second replication starts	<p><i>Symptom:</i> If a replication process takes more than 5 minutes to complete, another replication process begins immediately before the first one ends. The outbound (source) machine sends another replication to the inbound (destination) machine; but, since the first replication hasn't finished yet, the second one is aborted. An error message appears in the replication log, saying: "Inbound database replication from ACS 'host-name' aborted - outbound replication in progress."</p> <p>Additionally, by the time the second replication is aborted, the first replication has also finished (successfully). This means that both the failed and the successful replications try to start the services. Some error messages might appear regarding services which cannot be started, for instance: "Service CSLog failed to start.". These messages do not take into account a situation where the service is not running, but is actually being started.</p> <p><i>Conditions:</i> This happens when the inbound machine is running on a 2003 Server or Advanced Server, which might cause replication to take more than 5 minutes. The outbound machine's OS is irrelevant.</p> <p><i>Workaround:</i> This problem is related to the error messages that appears while the second replication is (rightfully) aborted. No real error condition was found, and since there is no known workaround for this, the only thing to do is ignore the error messages themselves.</p>
CSCeg72353	CSMon timeout period on replication destination does not apply	The timeout now works on the destination machine.

Table 6 *Resolved Problems in Cisco Secure ACS 3.3.3*

Bug ID	Summary	Explanation
CSCeg71157	MAX Session setting of 2 allows more than 2 sessions	When configuring MAX Sessions for User settings or Group settings to a value of '2' on the CSACS server, using local database, it now works properly.
CSCeg70175	ACS: PEAP-GTC SDI - User properties changing suddenly during auth.	When PEAP-Session Resume is enabled (value NOT zero) and PEAP fast reconnect is disabled, user properties do not change during authorization.
CSCeg66630	ACS: Failed to retrieve CRL	CRL download no longer fails in certain CA environments. ACS now retrieves CRL.
CSCeg62666	Clarify cross-version remote logging isnt supported	Information has been added to the release notes to clarify that you cannot back up, restore, replicate information, or log in remotely when using different versions of Cisco Secure ACS.
CSCeg60140	ACS LDAP search query ascii character non-rfc-compliant	RFC2254 (http://www.ietf.org/rfc/rfc2254.txt) states that search strings using certain special characters must be encoded as the backslash '\' character followed by the two hexadecimal digits representing the ASCII value of the encoded character. So a '\' would be '\5c' and a '(' would be '\28'. ACS is doing these as the actual character instead of the ascii. This is resolved. If for any reason you would like one of the LDAP configurations, to work with the old format (not comply to RFC 2254), go to the registry entry of the specific configuration and change the variable EncodeFilter to zero.
CSCeg55534	LDAP authentication continues past success until fails More than 1 instance of LDAP is defined in the external user database.	Failures are no longer occurring for users not already in the ACS database.

Table 6 **Resolved Problems in Cisco Secure ACS 3.3.3**

Bug ID	Summary	Explanation
CSCeg52536	Failed PEAP authentication not shown up in ACS logs	During machine authentication, supplicant doesn't expect the retrieable errors, so when machine authentication fails, ACS immediately rejects the attempt and updates the log.
CSCeg41917	LDAP Group mapping fails due to a comma (,)	ACS/LDAP group-mapping fails if DisplayName contains a comma (,).
CSCeg38123	EAP-TLS auth fails if SAN doesnt match netbios	This is resolved.
CSCeg20752	Cannot revoke certificate for intermediate CA	ACS no longer passes authentication for EAP-TLS users, even though their certificate has been revoked.
CSCef92064	Value PASS_TYPE_SDI for action code 108 missing though supported	<p>Symptom: The value PASS_TYPE_SDI (corresponding to password type RSA SecurID Token Server) of action 108 in a CSV file for RDBMS synchronization is not recognized and gives a parser error.</p> <p>Conditions: This only shows with ACS version 3.3 when doing RDBMS Synchronization.</p> <p>Workaround: The password type "RSA SecurID Token Server" can be configured in the graphical interface.</p>
CSCef35343	LDAP Multithreading does not work	Cisco Secure ACS 3.3 can process multiple LDAP authentication requests in parallel as opposed to the sequential processing mechanism employed in versions earlier than 3.2.
CSCee87726	CSA installation could be initiated although CSA is already installed	—

Table 6 *Resolved Problems in Cisco Secure ACS 3.3.3*

Bug ID	Summary	Explanation
CSCee62147	when create CRL with CTL contains two or more CA they change uncheck	This problem has been resolved by updates to the CRL graphical user interface. You can no longer add CRLs to the Certificate Trust List. The CRL Issuer list contains an entry for every trusted CA found in the Certificate Trust List. After selecting a CA in the Certificate Trust List, it automatically appears in the CRL Issuer's list. The default status is Not in Use.
CSCee56978	ACS generates EAP packet flood if LEAP and EAP-X is enabled	The problem resolved by fixing the EAP id handling in LEAP protocol handler. Now ACS correctly generates the EAP id for new LEAP conversations and EAP resends are handled right.
CSCeb21231	Failure code not logged when wrong password provided	This problem has been resolved.
Resolved Problems Specific to Cisco Secure ACS Solution Engine		
CSCeg46059	Telnet 23 port open	Cisco Secure ACS appliance (Cisco 1111) does not close telnet(23) port and additional ports. Reimaging with 3.2.3, 3.3.2 software does not fix this problem. Workaround: To resolve the issue, install the patch appl_All_Versions_HP_NIC_driver_7.80_fixPatch.zip from Cisco.com. Patch has new NIC drivers for HP appliance (Cisco 1111).
CSCsa85575	Lack of information on an ACS 1111 model	The Cisco 1111 stopped shipping in January 2005. For illustrations found in the Overview chapter, refer to the Installation and Setup Guide for Cisco Secure ACS Appliance 3.2 on Cisco.com. Those illustrations are of the Cisco 1111. The Cisco 1112 started to ship exclusively in January 2005, so the current Installation and Setup Guide for Cisco Secure ACS Appliance 3.3 includes illustrations of that chassis front and back panel.

Table 7 *Resolved Problems in Cisco Secure ACS 3.3.2*

Bug ID	Summary	Explanation
Resolved Problems Common to All Cisco Secure ACS Version 3.3 Platforms		
CSCef81506	ACS generates CSR with wrong version number.	ACS now generates CSR with the correct version.
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.
CSCef61749	EndPoint leaksmemory when an encrypted connection is closed	The end point no longer leaks memory.
CSCef47917	ACS Appliance intermittently cannot talk with remote agent	Duplicate of CSCef00468. Fixed.
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 occurs between ACS Appliance and Remote Agent, new connections can be initiated.
CSCee86457	MS PEAP pwd change not work for unknown user with NAC	When using the external Windows and other type of external database, the changed password will no longer fail.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1*

Bug ID	Summary	Explanation
Resolved Problems Specific to Cisco Secure ACS Solution Engine		
CSCdz06719	Support cmd allows illegal values	The support command allows only valid values.
CSCdz61454	FTP Restore button is not working on Solaris	The Restore button works correctly when you use the supported Netscape browser and Solaris operating system.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
CSCdz73781	Netscape browser on WinNT pointing ACSAppliance is not stable	The supported Netscape browser operates stably while accessing the HTML interface of a Cisco Secure ACS Solution Engine.
CSCdz74860	Cannot delete if Radius and AAA have same self IP	Management of network device entries works correctly.
CSCea00431	Appliance AAA Server entry does not exist after install	The AAA Server table entry for the appliance is created appropriately during installation and initial configuration of the appliance.
CSCea28562	Restore deleted Self AAA Server	The self-referential AAA Servers table entry is not deleted during a database restoration.
CSCea66355	Login prompt displayed too early when upgrade via CLI	The Login prompt no longer appears when it should not during appliance upgrade using the console.
CSCea74269	CSAdmin issue when downloading upgrade via GUI and https is in use	The CSAdmin service operates correctly while downloading an upgrade package and HTTPS is enabled.
CSCeb00443	ODBC logging settings appear after restore/replication from SW	ODBC logging settings no longer appear after restoring a database using a database backup file from a Windows release of Cisco Secure ACS.
CSCeb11207	rdbms sync dont get the first line in action file	RDBMS Synchronization handles all lines of the accountActions.csv file appropriately.
CSCeb14972	appliance ip is 0.0.0.0 after recovery & upgrade	After recovery and upgrade, the appliance IP address is correct.
CSCeb15110	appliance name does not appear in dist table, rdbms sync table	The appliance host name appears in the Proxy Distribution Table and the Synchronization Partners table.
CSCeb16877	free system disk space looks incorrect for ACS in separate disk	The CSMon service checks the correct partition for disk free space.
CSCeb21358	CSLogAgent could not be started when certain acct attr is selected	CSLogAgent starts without difficulty.
CSCeb64219	NTP sync problem	NTP synchronization works properly.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
CSCec86357	Upgrade via GUI is effected when using CLI for certain operations	Upgrade via the HTML interface operates correctly when the console is in use.
CSCed08009	Directory / file management does not enforce exact number of files	File management enforces file restrictions properly.
CSCed14948	Pls add logging for NTP status	NTP status is logged in ApplianceLog, which is available in System Configuration > View Diagnostic Logs. The results of the new console command ntpsync are also logged here.
CSCee33563	ACS 3.2.3 fails https management	Use of SSL for securing access to the HTML interface works properly.
CSCee45135	TWO NTP servers cannot be defined	You can configure Cisco Secure ACS to use multiple NTP servers in a simple failover mode.
Resolved Problems Common to All Cisco Secure ACS Version 3.3 Platforms		
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 will not work with PPP callback and call-in 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.
CSCea67901	UCP has trouble with dots in usernames	HTML pages show whole usernames including the dot (.).
CSCea71759	Headline of UCP application stating Cisco Secure ACS	The headline of the User-Changeable Passwords application reads correctly.
CSCeb15219	Could not add NAS filter by CSDdsync	Action code 122 works appropriately.
CSCeb23766	Inconsistency with ACS response if username contains invalid chars	Cisco Secure ACS now responds consistently to RADIUS requests containing invalid usernames.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
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 close 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	Cisco Secure ACS only permits 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 rekeying type not logged to Failed log	PEAP rekeying is logged accurately.
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.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
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	The description of the Calling-Station-ID attribute has been corrected.
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 uppercase letters to lowercase in username RADIUS att	Username case is preserved in RADIUS proxying.
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.
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 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
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.
CSCed01640	Memory leak in CSAuth caused with Leap-Proxy scenario	The memory leak has been fixed.
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.
CSCed43307	Administrator access to report User Change Password	Administrator permissions correctly grant or deny administrators access to the User Password Changes report.
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.

Table 8 *Resolved Problems in Cisco Secure ACS 3.3.1 (continued)*

Bug ID	Summary	Explanation
CSCee41393	Action Code 163 example is wrong in user guide	The documentation has been corrected.
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 dial-in authentication.
CSCee58096	Cisco Generic EAP not associated with vendor RADIUS (Cisco VPN 3000)	Generic EAP is associated with the Cisco VPN 3000 RADIUS vendor.
CSCeg01497	Management Software build number is incorrect in Appliance	The build number of Appliance Management software is build 1 and not 2.
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>

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.

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 by 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, call 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>

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. 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* is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, *Packet* delivers coverage of the latest industry trends, technological 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* at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems that is 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 publication published by Cisco Systems for engineering professionals who are 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.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCN, Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeDrive, HomeLink, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Bandwidth, and WebEx 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 trademarks in this document does not constitute a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

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