



Release Notes for Cisco Secure ACS

Release 3.3.4

Revised: December 28, 2006

These release notes pertain to Cisco Secure Access Control Server (ACS), release 3.3.4. These release notes contain information for the Windows and Solution Engine (SE) platforms. Where necessary, the appropriate platform is clearly identified.



Note

The release numbering system that ACS software uses includes major release, minor release, maintenance build, and interim build number in the MMM.mmm.###.BBB format. For this release, the versioning information is ACS 3.3.4.12. Elsewhere in this document where 3.3.4 is used, it refers to 3.3.4.12. ACS major release numbering starts at 3.3.1, not 3.3.0. Use this information when working with your customer service representative.

Contents

- [Introduction, page 2](#)
- [New and Changed Information, page 4](#)
- [Installation Notes, page 6](#)
- [Documentation Updates, page 9](#)
- [Caveats, page 11](#)
- [Product Documentation, page 17](#)
- [Obtaining Documentation, page 18](#)
- [Documentation Feedback, page 19](#)
- [Cisco Product Security Overview, page 19](#)
- [Product Alerts and Field Notices, page 20](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 22](#)



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

Introduction

ACS 3.3.4 is a maintenance release for ACS 3.3 that consolidates ACS 3.3 customer patches and resolves other customer and internally found defects. ACS 3.3.4 is available through the Cisco Technical Assistance Center (TAC) only for upgrading existing ACS software deployments.


Note

Cisco Secure ACS 3.3 is the final ACS 3.x platform release. Cisco service and support for ACS 3.3 ends August 28, 2009. Cisco recommends that you migrate to the current ACS 4.x platform. For detailed information on new capabilities and upgrades, refer to the Cisco Secure ACS for Windows data sheet at <http://www.cisco.com/go/acs>.

Table 1 describes the packages that ACS SE 3.3.4 includes.

Table 1 ACS SE 3.3.4 packages

File Name	Description
ACSse-v3.3.4.12-1111-recovery-K9.iso	Full Recovery CD image for the 1111 appliance (HP)
ACSse-v3.3.4.12-1112-recovery-K9.iso	Full Recovery CD image for the 1112 appliance (Quanta S20)
ACSse-v3.3.4.12-1113-recovery-K9.iso	Full Recovery CD image for the 1113 appliance (Quanta S27)
ACSse-Upgrade-Full-v3.3.4.12-K9.zip	Full Upgrade CD image for the 1111 appliance and 1112 appliance
ACSse-Upgrade-Pkg-acsv3.3.4.12-K9.zip	ACS 3.3.4 software package for the appliance. The full Upgrade CD image also includes this file.
ACSse-Upgrade-Pkg-appl-mng-v3.3.4.12-K9.zip	ACS 3.3.4 management software package for the appliance. The full Upgrade CD image also includes this file.
Remote-Agent-ACSse-solaris.5.8-v3.3.4.12-K9.tar	ACS SE 3.3.4 Remote Agent for Solaris.
Remote-Agent-ACSse-win-v3.3.4.12-K9.zip	ACS SE 3.3.4 Remote Agent for Windows.
UCPv3.3.4.12.zip	User Changeable Passwords (UCP) for ACS 3.3.4.
README_ACSSE33412.txt	Readme file for ACS SE 3.3.4

Table 2 describes the packages that ACS for Windows 3.3.4 includes.

Table 2 ACS for Windows 3.3.4 packages

File Name	Description
ACSv3.3.4.12-FULL-K9.zip	Full ACS 3.3.4 for Windows installation CD image including documentation, UCP, and Clean utility.
ACSv3.3.4.12-BIN-K9.zip	Installation files for ACS for Windows 3.3.4.
UCPv3.3.4.12.zip	User Changeable Passwords (UCP) for ACS 3.3.4.
README_ACSwin33412.txt	Readme file for ACS for Windows 3.3.4.

For information about installing and upgrading to ACS 3.3.4, see [Installation Notes, page 6](#).

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

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

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

1. ADDITIONAL LICENSE RESTRICTIONS.

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

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

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

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.

New and Changed Information

ACS 3.3.4 includes the following new features:

- [ACS SE on the 1113 Appliance, page 4](#)
- [Configuring a Logging Queue, page 4](#)
- [Manual Group Mapping, page 5](#)
- [Matching Framed-IP-address with User IP, page 5](#)



Note

These new features are not described in the online user guide or online help in ACS 3.3.4.

ACS SE on the 1113 Appliance

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

The ACS SE 1113 comes equipped with ACS 4.0 installed. ACS 3.3 is not currently supported on the 1113 appliance. You can re-image the appliance with ACS 3.3.4 by using the Recovery CD for 1113. For more details, see [Installing ACS SE 3.3.4 on 1113, page 8](#).

Configuring a Logging Queue

The Logging Queue Configuration feature provides a solution for bug CSCeg40355. Remote logging delays due to network-related problems caused problems with authentication requests.

When you enable the logging queue, ACS maintains an internal queue for performing logging, which enables the processing of authentication and accounting requests to proceed without waiting for the logging operation to complete.

We recommend that you use this feature only if you have enabled remote logging, and remote logging targets are slow or non-responding, which might cause problems with authentication.



Note

The logging queue is not persistent; if the CSAuth process is restarted, all the queued logging information is lost.

To enable the Logging Queue:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
The Logging Configuration page appears.
 - Step 3** Check the **Logging Queue** check box.
 - Step 4** Click **Submit + Restart** to enable the logging queue.
-

Manual Group Mapping

The manual group mapping feature provides a solution for bug CSCef95887.

On the ACS appliance, ACS group mapping failed to enumerate groups in Active Directory when the Active Directory server had a large number of groups; for example, more than 500 groups. Use the Add Manual Mapping feature to add groups manually when you have too many groups to enumerate.

To map manually to an ACS group:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database name for which you want to configure a group mapping.
 - Step 4** Click the domain name for which you want to configure a group set mapping.
The Group Mappings for Domain: *domainname* table appears.
 - Step 5** To add groups manually:
 - a.** Click **Add Manual Mapping**. The Manual Mapping page opens.
 - b.** Enter the list of Windows groups separated by a comma (,).
 - c.** In the ACS group list, select the name of the ACS group to which you want to map users who belong to all the external user database groups in the Selected list.
 - Step 6** Click **Submit**.



Note ACS does not validate whether the group names exist in Active Directory.

Matching Framed-IP-address with User IP

This feature provides a solution for bug CSCse33323.

When the AAA client uses Cisco SSL WebVPN, the VPN concentrator sends two accounting packet pairs for each user session, which causes ACS to drop the session along with the IP address that was assigned to the user. On the next successful request processing, ACS gives out the dropped IP address, even though it is still assigned.

Use the Match Framed-IP-Address with user IP address for accounting packets from this AAA Client feature in the AAA Client page when the AAA client uses Cisco SSL WebVPN. This action ensures that ACS assigns different IP addresses to two different users when they log in through a Cisco SSL WebVPN client. By default, this check box is unchecked.

To access the AAA Client page:

-
- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** To add an AAA client, do one of the following:
- If you are using network device groups (NDGs), click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
 - To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.
- The Add AAA Client page appears.
- Step 3** To edit an AAA client, do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.
 - To edit AAA clients when you have not enabled NDGs, click the name of the AAA client in the AAA Client Hostname column of the AAA Clients table.
- The AAA Client Setup For *Name* page appears.
- Step 4** Click the **Match Framed-IP-Address with user IP address for accounting packets from this AAA Client** check box.
-

Installation Notes

This section contains installation information for ACS 3.3.4:

- [Upgrade Paths, page 6](#)
- [System Requirements for ACS 3.3.4, page 7](#)
- [Installing ACS 3.3.4 for Windows, page 7](#)
- [Upgrading to ACS 3.3.4 for Windows, page 7](#)
- [Upgrading to ACS 3.3.4 on 1111 and 1112 Appliances, page 7](#)
- [Installing ACS SE 3.3.4 on 1113, page 8](#)

Upgrade Paths

ACS Software

We support upgrading to ACS 3.3.4 from the following versions:

- ACS 3.3.3
- ACS 3.3.2

- ACS 3.3.1
- ACS 3.2.3
- ACS 3.2.2
- ACS 3.2.1
- ACS 3.1.2
- ACS 3.0.4

**Note**

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

ACS Solution Engine

We support upgrading ACS SE 1111 and 1112 appliances to ACS 3.3.4, and re-imaging ACS SE 1113 with ACS 3.3.4. (ACS 3.3 is not currently supported on the 1113 appliance.)

System Requirements for ACS 3.3.4

The system requirements for ACS 3.3.4 are the same as for ACS 3.3.3. For information on supported operating systems and web browsers for ACS 3.3.3 for Windows, see *Release Notes for ACS for Windows 3.3.3* at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_note09186a0080451263.html.

In addition, ACS 3.3.4 is supported on Pentium dual-core processors.

**Note**

ACS is not currently supported on Windows Server 2003 R2.

Installing ACS 3.3.4 for Windows

The installation instructions for ACS 3.3.4 are the same as for ACS 3.3.3. For information about installing ACS, see *Installation Guide for Cisco Secure ACS for Windows 3.3* at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080238b18.html.

Upgrading to ACS 3.3.4 for Windows

The instructions for upgrading to ACS 3.3.4 are the same as for upgrading to ACS 3.3.3. For information about upgrading ACS, see *Installation Guide for Cisco Secure ACS for Windows 3.3* at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080238b18.html.

Upgrading to ACS 3.3.4 on 1111 and 1112 Appliances

The instructions for upgrading to ACS 3.3.4 on the 1111 and 1112 appliances are the same as for upgrading to ACS 3.3.3 on those appliances. For information about upgrading ACS SE, see *Release Notes for Cisco Secure ACS Solution Engine 3.3.3* at http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_note09186a0080451261.html.

Installing ACS SE 3.3.4 on 1113

The 1113 appliance has ACS 4.0 pre-installed. You must first install and set up the 1113 appliance and then re-image the 1113 appliance with ACS 3.3.4.

- [Installing the 1113 Appliance, page 8](#)
- [Re-imaging the 1113 Appliance, page 8](#)

Installing the 1113 Appliance

For instructions on installing the 1113 appliance, see *Installation Guide for Cisco Secure ACS Solution Engine 4.1* at http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_guide_book09186a00807072d2.html.

Re-imaging the 1113 Appliance



Caution

Re-imaging an appliance destroys all data stored on the ACS SE.

To re-image the 1113 appliance:

-
- Step 1** Connect a console to the appliance console port.
 - Step 2** Insert the Recovery CD for 1113 into the appliance CD-ROM drive.
 - Step 3** Power up the appliance. (Or, if ACS SE is already running, reboot it.)

Result: ACS SE displays the following message on the console:

```
ACS Appliance Recovery Options
[1] Reset administrator account
[2] Restore hard disk image from CD
[3] Exit and reboot
Enter menu item number: [ ]
```

- Step 4** Type **2**, then press **Enter**.

Result: ACS SE displays the following message on the console:

```
This operation will completely erase the hard drive. Press 'Y' to confirm, any other key
to cancel: __
```

- Step 5** Type **Y**.

Result: ACS SE processes the new image (this may take more than 2 minutes) while displaying odd characters and then displays the following message on the console:

```
The system has been reimaged successfully. Please remove this recovery CD from the drive,
then hit RETURN to restart the system:
```

- Step 6** Remove the Recovery CD from the CD-ROM drive.
- Step 7** Press **Enter** to restart ACS SE.

Result: The appliance reboots, performs some configurations, and reboots again. The configurations that occur after the first reboot take a significant amount of time, during which the screen displays no feedback; this is normal system behavior.

After re-imaging the solution engine hard drive, you must perform initial configuration of ACS SE. For detailed instructions, see the section “Configuring the Cisco Secure ACS Solution Engine” in *Installation Guide for Cisco Secure ACS for Windows 3.3* at http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080238b18.html.

Documentation Updates

This section provides updates for errors and omissions in the ACS user documentation:

- [Specifying Private Key File Name on ACS SE, page 9](#)
- [Replication with Different Send and Receive Configurations, page 9](#)
- [Preventing Folder Locking During Upgrade, page 10](#)
- [RDBMS Synchronization Failure Codes, page 10](#)



Note

Refer to [Table 6](#) for the product documentation that you should use with ACS 3.3.4.

Errors

This section provides updates for errors in the ACS user documentation.

Specifying Private Key File Name on ACS SE

The user guide for the ACS appliance states that you should provide the full directory path for the private key file, for example, *c:\privateKeyFile.pem*.

This information is incorrect and causes the certificate generation to fail with an error (bug CSCed95260).

On ACS SE, you must specify only the file name; otherwise the certificate generation fails with an error.

Replication with Different Send and Receive Configurations

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

This information is incorrect (bug CSCsg93907).

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

Omissions

This section provides updates for omissions in the ACS user documentation.

Preventing Folder Locking During Upgrade

The following troubleshooting information was omitted in the ACS user guide (bug CSCeg16365).

Condition

When upgrading ACS, **setup.exe** hangs and displays an error message:

```
The CiscoSecure ACS folder appears to be locked by another application... . Please close
any applications that are using any files or directories and re-run Uninstall.
```

Action

Remove excess log files. ACS stores log files in `\CiscoSecure ACS v.3.3\Logs`. If you cannot upgrade because a log file folder is too large, you must first delete all but the last three log files from the folder. When ACS starts up, choose **System Configuration > Service Control**. In the Services Log File Configuration, check **Manage Directory**, and choose **Keep only the last <n> files**. Set <n> to 3.

If PNLogAgent is running, stop that service to release any locks that it might have on the folder.

RDBMS Synchronization Failure Codes

The following information was omitted in the ACS user guide (bug CSCsd41474).

Fatal as well as nonfatal RDBMS synchronization errors can occur during a single transaction. When a nonfatal error message is written to the RDBMS synchronization audit log, and processing continues as if it is a successful transaction, the record is deleted from the action table. When a fatal error message is written to the RDBMS synchronization audit log, synchronization stops.

Although the expected behavior for ACS is to send the error code 2 to the database, ACS RDBMS synchronization does not send the error code 2, nor does it delete the database records if a failure occurs.

You can add new devices and NDGs when performing RDBMS synchronization from the database to ACS. The new devices are appended to the end.

If the device already exists in ACS, ACS reports an error in the log `Failed to create new NAS/AAA record- Host database failure. Host already exists`. Although the expected behavior for ACS is to delete the database records if a failure occurs, ACS remove the entries from the database and does not send an error code to the database.

[Table 3](#) lists RDBMS Synchronization fatal errors.

Table 3 *List of Fatal Errors*

Error Code
Attempt to create account with user name that already exists.
Password supplied for user was not valid.
An internal error in packet format has occurred.
The file or directory could not be opened - no free handles.
File write in the user file space failed.
File read in the user file space failed.

Table 3 *List of Fatal Errors*

Error Code
An invalid directory name was supplied.
An invalid file name was supplied.
Server could not allocate memory.
File set pointer in the user file space failed.
CSAuth client tried to send a message greater than 31K.
Attempt to create account with user name that already exists.
A value in the registry was not found.
Database file cannot be made bigger.
Proxy database failure.
UDB_PROXY_DB_FAILURE
Invalid counter type.
UDB_USER_REMOVED
UDB_UDV_CONFIG_ERROR

Caveats

These release notes include:

- [Open Caveats, page 11](#)
- [Resolved Caveats, page 12](#)

Open Caveats

[Table 4](#) describes the known bugs in ACS 3.3.4.



Note

Bug summaries and descriptions appear here word-for-word as they appear in our bug-tracking system.

Table 4 *Known Bugs in ACS 3.3.4*

Bug ID	Summary	Description
CSCsh12148	Cannot reinstall CSA after removing it.	<p>This problem occurs only on the Quanta S27 appliance (1113) when trying to reinstall the CSA after removing it using the rollback function.</p> <p>The CSA rollback succeeds; but before the appliance reboots the following error appears:</p> <pre>The process cannot access the file because it is being used by another process.</pre> <p>Then, after the appliance reboots, an error message appears when trying to reinstall CSA.</p>

Resolved Caveats

[Table 5](#) describes the bugs that have been fixed in ACS 3.3.4.



Note Bug summaries appear here word-for-word as they appear in our bug-tracking system.

Table 5 *Resolved Bugs in ACS 3.3.4*

Bug ID	Summary	Explanation
CSCdu43103	ACS Perflib cosmetic error message 8-byte boundary alignment.	The problem has been fixed and the warning message no longer appears.
CSCea74289	Cascade replication due to user pass change-doesn't work.	Cascade replication with password changes now replicates successfully.
CSCeb43948	Could not generate valid Password with password length => 9.	The problem has been fixed. No errors are issued.
CSCec54223	ENH: Need ability to add more than 30 LDAP servers to ACS.	You can now add more than 30 LDAP servers to ACS.
CSCed83628	Replication displays error when nothing to be replicated.	The problem has been fixed. No errors are issued.
CSCee14756	ACS with Open LDAP server - Secure LDAP does not work.	ACS supports Secure LDAP, but only for server-side authentication. Some LDAP servers may request that ACS (as the LDAP client) send a certificate to identify itself. ACS will fail to open connections over SSL to servers with such a configuration. To use communication over SSL between ACS and LDAP server, configure the LDAP server to use SSL without client certificate authentication.
CSCee65661	Need the NoCacheUser feature for unknown user policy.	The problem has been fixed.
CSCee83680	Transport service failed to go up after using Automation CLI-Shutdown.	The problem has been fixed.
CSCee88908	CSLog crash if a logged attribute is deleted due to replication.	The CSLog works as expected after replication.
CSCee94357	Illegal characters are not checked when config set admin or recovery.	Input characters are now validated.
CSCef05950	Access to ACS Admin without Authentication.	The problem has been fixed.
CSCef27403	Email sender stays as default, even when ACS appliance gets renamed.	The problem has been fixed.
CSCef95887	ACS Appliance should support more than 500 Windows groups.	The problem has been fixed. For details, see Manual Group Mapping, page 5 .
CSCeg04666	CSRADIUS service stops with junk attributes.	The problem has been fixed.
CSCeg04788	CSRADIUS services stops with long length tunnel attributes.	The problem has been fixed.

Table 5 **Resolved Bugs in ACS 3.3.4 (continued)**

Bug ID	Summary	Explanation
CSCeg24513	Cannot import large route table via RDBMS.	The exception caused by the profile exceeding its allocated buffer has been fixed. When the profile is too large, an error message appears in the RDBMS Sync report: Failed to add TACACS+ attribute - Profile is larger than maximum allowed size.
CSCeg40355	Authentication failures when remote logging fails.	The problem has been fixed. For details, see Configuring a Logging Queue, page 4 .
CSCeg51873	ACS chooses wrong NDG for NAR with TACACS/RADIUS NAS on same IP.	ACS no longer chooses the wrong NDG for NAR matching if both a TACACS+ and RADIUS NAS are defined with the same IP, and placed in separate NDGs and the authentication is performed via RADIUS.
CSCeh17104	ACS Appliance: Certain Hostname/Admin name cause loss of access	ACS will not allow you to use the same name for hostname and administrator name.
CSCeh24688	CSAuth mem leak after EAP-TLS authentications to LDAP.	The problem has been fixed.
CSCeh37849	TACACS performance limited to 14 sessions/s, winsock-1 causes TCP RSTs.	The problem has been fixed.
CSCeh37907	Duplicate IP assignment due to accounting packets reordering.	Duplicate IP address are no longer assigned.
CSCeh42116	EAP-TLS Machine Authentication fails when AD PDC emulator down.	The problem has been fixed.
CSCeh54670	ACS couldn't find user in AD if sent w/out domain name.	The Windows EAP Setting, EAP-TLS Strip Domain Name check box, has been removed from the user interface, and the Active Directory (AD) search functionality enables you to authenticate a username.
CSCeh55725	Failed to get NIC config FFFFFFFF.	The problem has been fixed. No errors are issued.
CSCeh69359	CSLog/ODBC exception after timeout of log update.	The problem has been fixed.
CSCeh91809	VoIP messages cause CSRADIUS service unexpected termination.	CSRADIUS no longer terminates unexpectedly.
CSCeh96024	LDAP Failback Retry Delay parameter ignored in failover scenario.	The problem has been fixed.
CSCei07191	Logged Remotely Attribute is not present in Solaris Remote-Agent.	Logged Remotely attributes are now present in the Solaris remote agent logs.
CSCsa86272	ACS discards EAP-FAST reauthentication requests from 350 wireless cards.	The problem has been fixed.
CSCsb06387	ACS: Authentication fails, while CSRADIUS is up.	The problem has been fixed.
CSCsb25098	ACS SE upgraded to 3.3.3 generates a Backup and Restore failure.	The problem has been fixed.
CSCsb25151	When AAA client has multiple/range of IP addresses, NAF for DACLS fails.	NAF for downloadable ACLs no longer fails for AAA clients.

Table 5 *Resolved Bugs in ACS 3.3.4 (continued)*

Bug ID	Summary	Explanation
CSCsb26537	PAC Invalid isn't responded by TLS_Alert, hence no auto provisioning.	The problem has been fixed.
CSCsb26676	Console unavailable after upgrade.	The problem has been fixed.
CSCsb36764	ACLs from ACS can not be downloaded to the PIX.	The problem has been fixed.
CSCsb47726	WLSE - AP/WDS fails to fully authenticate.	The problem has been fixed.
CSCsb47755	Upgrading appliance leaves the SNMP port open.	The problem has been fixed.
CSCsb71359	Hostname limited to 15 characters.	The hostname limit is 15 characters; you can no longer enter more than 15 characters.
CSCsb74859	Click on Next in Radius Accounting, TACACS +Accounting & Admin error 500.	The problem has been fixed. No errors are issued.
CSCsb81671	CSTacacs and CSRadius services fail to start with Windows 2003.	The problem has been fixed.
CSCsb83399	ACS SE should save the FTP settings during software upgrade.	ACS SE saves the FTP settings during a software upgrade.
CSCsb94681	ACU 6.5 Shows Garbage Characters with Manual Login in EAP-FAST.	The problem has been fixed.
CSCsb99213	CSAuth fails intermittently on ACS Windows 3.3.3 build 11.	The problem has been fixed.
CSCsc12154	Logging tables aren't reset after restore.	The problem has been fixed.
CSCsc12614	RSA ext. DB stop working after failure with wrong password.	The problem has been fixed.
CSCsc33346	ACS Appliance remote logging missing system-posture-token attribute.	The problem has been fixed.
CSCsc49596	Enhancement Request: Print EAP requests in Radius Logging.	The EAP value is now displayed in hexadecimal format in the logs.
CSCsc50048	ACS 3.3.3 may fail to reconnect to ODBC for logging.	The problem has been fixed.
CSCsc54772	NTLM Version 2, Win2k Domain, ACS 3.3.3.11, Patch CSCea91947 doesn't work.	The problem has been fixed.
CSCsc62488	ACS: AAA client with overlapping IP address can be configured.	The problem has been fixed. An error message appears when there are overlapping IP addresses.
CSCsc66978	ACS RA will crash for user belonging to many AD groups.	The problem has been fixed.
CSCsc69608	Deleting RSA database unchecks PEAP,EAP-TLS options in Windows database.	The problem has been fixed.
CSCsc74808	CSRadius.exe memory leak.	The problem has been fixed.
CSCsc80481	Proxy distribution table prevents SNMP from working.	The problem has been fixed.
CSCsc84951	RDBMS synchronization fails after some time.	The problem has been fixed.
CSCsc87874	Shared profile can causes IE to display Action Cancelled, Shared Profile.	The problem has been fixed.

Table 5 Resolved Bugs in ACS 3.3.4 (continued)

Bug ID	Summary	Explanation
CSCsd11868	CSRadius doesn't forward IPADDR VSAs for accounting.	The problem has been fixed.
CSCsd12551	IP pools disappear occasionally from Group Setup/Edit Settings.	The problem has been fixed.
CSCsd14562	Incorrect string size check for IETF Attribute 22 (Framed-route).	The problem has been fixed.
CSCsd18735	ODBC logging to Oracle DB fails if embedded quote marks in data.	The problem has been fixed.
CSCsd21392	CSMon fails to restart CSAAuth after varsdb check failure.	The problem has been fixed.
CSCsd40764	ACS SE on 3.3.3 build 11 cannot allocate CSAAuth threads.	The problem has been fixed.
CSCsd41569	CSAAuth crashed during MS-PEAP authen using wired environment.	The problem has been fixed.
CSCsd52574	MachineSPNToSAM: __DsCrackNames failed message in auth.log.	The problem has been fixed, and the failed messages no longer appear.
CSCsd63894	ACS does not respond with the same IP address for RADIUS.	ACS now responds with the correct IP address.
CSCsd83232	Unicode on Full name in AD breaks EAP-TLS.	The problem has been fixed.
CSCsd84485	ACS Appliance memory leak.	The problem has been fixed.
CSCsd94968	ACS SE:AAA server IP for UCP changes to SE IP after reboot.	The problem has been fixed.
CSCsd96132	Same value (16) on registry key for two different error message on ACS.	Value 16 appears now only for External DB Password Invalid error message.
CSCsd96293	Crash when using special string in HTTP get (CSAdmin).	The problem has been fixed.
CSCse06667	Problem in the RADIUS Token Servers failover logic.	When the primary server is not available all requests are now forwarded to a secondary server.
CSCse18250	CSRadius crashes on a specific Access-Request message.	The problem has been fixed.
CSCse18278	CSRadius crashes on specific Accounting-Request packet.	The problem has been fixed.
CSCse26719	Cisco Secure Port Redirect may be predictable.	The problem has been fixed.
CSCse33323	ACS assigns duplicate IPs from address pool.	The problem has been fixed. For details, see Matching Framed-IP-address with User IP, page 5 .
CSCse57094	MachineSPNToSAM: __DsCrackNames failed errors in auth.log.	The problem has been fixed, and the failed messages no longer appear.
CSCse74158	ACS SE 4.01 does not accept machine authentication.	The problem has been fixed.
CSCse75718	ACS reports External DB account Restriction error for Internal Error.	The problem has been fixed.

Table 5 *Resolved Bugs in ACS 3.3.4 (continued)*

Bug ID	Summary	Explanation
CSCse80031	CSAuth fails in PPTP environment with roaming 3rd-party supplicant.	The problem has been fixed.
CSCse81436	Incorrect user reported when EAP-TLS SSL handshake failure.	This problem occurred if another user was concurrently negotiating EAP-TLS. The username field of the Failed Attempts report now displays only Framed-IP address when the EAP-TLS or PEAP authentication fails during SSL handshake.
CSCse87913	Memory leak in CSRadius when VSA attrs are present in proxied requests.	The problem has been fixed.
CSCse94583	ACS EAP processing can inadvertently create new sessions.	ACS now maintains the original session.
CSCse94593	CTA client and ACS can get stuck in PEAP start/NAK loop.	The problem has been fixed.
CSCse94684	Starting and ending spaces are allowed in password field.	A message now appears stating that starting and ending spaces will be ignored.
CSCsf06306	ACS not replicating all clients in NDG.	The information was replicated, but did not appear in the ACS web interface. An error message now appears when this happens.
CSCsf07405	Admin log entries are truncated and bleed to a second line.	The problem has been fixed.
CSCsf23731	Invalid message while connecting to a non-existing server from upgrade g.	The message has been changed to <code>Error due to Invalid Host Name, or Upgrade image is not for this hardware platform.</code>
CSCsf96289	ACS Logs are not available for initial authentication requests.	The problem has been fixed.
CSCsg02249	Restore fails in appliance when SNMP is already running in same port.	The problem has been fixed.
CSCsg18312	LDAP group mapping can not be created for the 2nd connection.	The problem has been fixed.
CSCsg37835	MS-CHAP authentication failed when username in UPN format.	The problem has been fixed.
CSCsg56177	EAP-TLS may fail for AD user if username has NetBIOS domain prefix.	The problem has been fixed.
CSCsg63983	Message for large accounting packets in RDS should be modified in 3.3.4.	The following message now appears: <code>Error in logging packet: the incoming RADIUS packet is too large 4221 bytes.</code>
CSCsg81524	CSAuth Crashed at time of EAP-FASTv1a stress against Active Directory.	The problem has been fixed.

Product Documentation

Table 6 describes the product documentation that you should use with ACS 3.3.4.

Table 6 Product Documentation on Cisco.com

Document Title and Description	Available on Cisco.com at:
<p><i>Release Notes for Cisco Secure ACS 3.3.4</i></p> <p>Lists new features, documentation updates, known problems, and resolved problems.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/release/notes/ACS334rn.html</p>
<p><i>Release Notes for Cisco Secure ACS 3.3.3</i></p> <p>Use to upgrade to ACS 3.3.4 on the 1111 and 1112 appliances. Use in conjunction with <i>Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3</i></p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/release/notes/RNsol333.html</p>
<p><i>Installation and Setup Guide for Cisco Secure ACS Solution Engine 3.3</i></p> <p>Use in conjunction with <i>Release Notes for Cisco Secure ACS 3.3.3</i> to upgrade to ACS 3.3.4 on the 1111 and 1112 appliances.</p> <p>Use to perform initial configuration after re-imaging the 1113 appliance.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/installation/guide/appliance/install.html</p>
<p><i>Installation and Setup Guide for Cisco Secure ACS Solution Engine 4.1</i></p> <p>Use to install the 1113 appliance.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/igse41.html</p>
<p><i>Installation Guide for Cisco Secure ACS for Windows 3.3</i></p> <p>Use to install ACS 3.3.4 for Windows and to upgrade to ACS 3.3.4 for Windows.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/installation/guide/windows/install.html</p>
<p><i>User Guide for Cisco Secure ACS Solution Engine 3.3</i></p> <p>Explains ACS SE functionality and procedures for using the ACS SE features.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/user/guide/user.html</p>
<p><i>User Guide for Cisco Secure ACS for Windows 3.3</i></p> <p>Explains ACS for Windows functionality and procedures for using the ACS for Windows features.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/user/guide/user.html</p>
<p><i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents</i></p> <p>Use to install and configure Remote Agents for ACS SE</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/installation/guide/remote_agent/ra.html</p>
<p><i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i></p> <p>Use to install and configure user-changeable passwords for ACS 3.3.4.</p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/installation/guide/passwords/ucp.html</p>
<p><i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows 3.3</i></p>	<p>http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/device/table/win33sdt.html</p>

Table 6 Product Documentation on Cisco.com (continued)

Document Title and Description	Available on Cisco.com at:
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine 3.3</i>	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/device/table/app33sdt.html
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 3.3</i> Provides translated safety warnings and compliance information for the 1111 and 1112 appliances.	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/3.3/regulatory/compliance/RCSI_33.html
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.1</i> Provides translated safety warnings and compliance information for the 1113 appliance.	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/regulatory/compliance/RCSI_41.html
Online Documentation	In the ACS web interface, click Online Documentation.
Online Help	In the ACS web interface, online help appears in the right pane when you are configuring a feature.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

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

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

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

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

- For emergencies only — security-alert@cisco.com

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

- For nonemergencies — psirt@cisco.com

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

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

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

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

Cisco Support Website

The Cisco 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 at this URL:

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

Access to all tools on the Cisco 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>



Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—An existing 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 operations 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 the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

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

Obtaining Additional Publications and Information

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

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- 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 “Product Documentation” section.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.