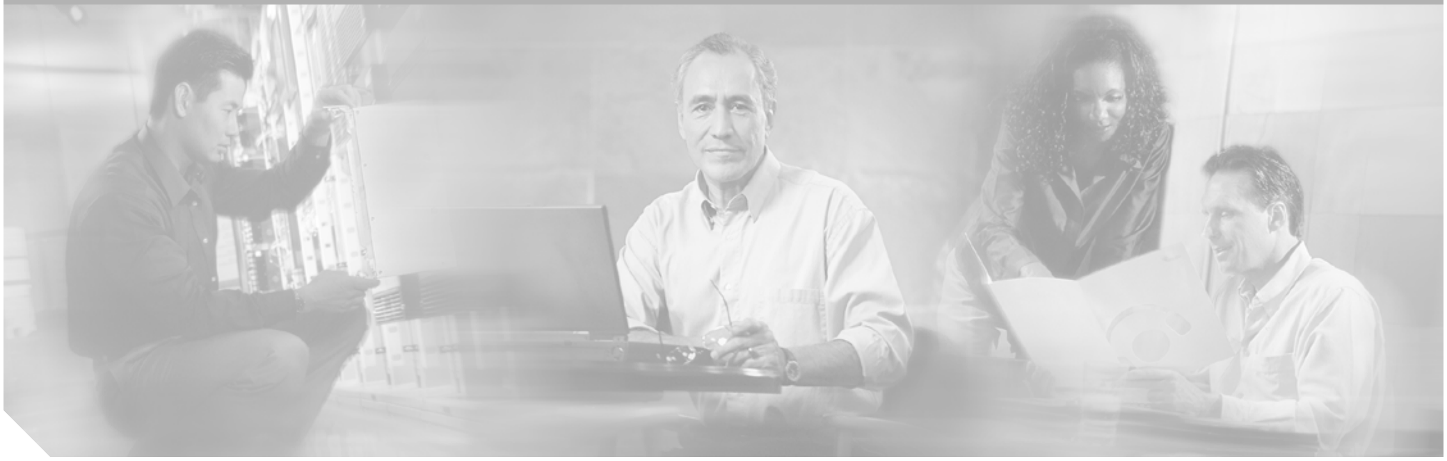

Installation Guide for Cisco Secure ACS for Windows

Version 4.0
July 2007

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-14105-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Installation Guide for Cisco Secure ACS for Windows, 4.0

CONTENTS

CHAPTER 2

Preface

This document will help you install and initially configure the Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

Audience

This guide is for system administrators who use install and configure internetworking software and are familiar with Cisco IOS software.

Organization

This document contains the following chapters:

- Chapter 1, "Installing Cisco Secure ACS"—Instructions on installing, reinstalling, and upgrading ACS.
- Chapter 2, "Post-Installation Tasks"—Details on initial configuration and post-installation tasks.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Indicates menu items to select, in the order you select them.	**Option > Network Preferences**

Tip Identifies information to help you get the most benefit from your product.

Note Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

Warning **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

Product Documentation

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

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Documentation Guide for Cisco Secure ACS for Windows	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com.
Release Notes for Cisco Secure ACS for Windows	On Cisco.com.
Installation Guide for Cisco Secure ACS for Windows	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816991=).[1]
User Guide for Cisco Secure ACS for Windows	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816992=).[1]
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	• PDF on the product CD-ROM. • On Cisco.com.

Table 1 Product Documentation (continued)

Document Title	Available Formats
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows	On Cisco.com.
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help	In the ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

Installing Cisco Secure ACS

This chapter provides information about installing, reinstalling, and upgrading to Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains:

- Preparation for Installing or Upgrading ACS, page 1-1
- What You Can Do, page 1-6
- Creating an ACS Installation, page 1-7
- Reinstalling or Upgrading ACS, page 1-11

Preparation for Installing or Upgrading ACS

Before performing an installation or upgrade procedure, read this section and perform the recommended actions.

This section contains:

- Understanding your ACS System, page 1-1
- System Requirements, page 1-2
- Network and Port Requirements, page 1-4
- Back Up Data, page 1-5
- Gathering Answers for the Installation Questions, page 1-6

Note ACS will not install properly if Sybase server is installed on the same machine.

Understanding your ACS System

You can use ACS network security software to help you authenticate users by controlling access to a AAA client—any one of many network devices that can be configured to defer authentication and authorization of network users to a AAA server. ACS operates as a set of Windows services that control the authentication, authorization, and accounting of user access to networks.

ACS operates on Windows 2000 Server and Windows Server 2003. ACS can run on a domain controller or a member server. For information about supported operating systems, see Server, Web Client, and Agent Requirements, page 1-2 or the latest version of the Release Notes, which are accessible from:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html

Note If you want to authenticate users with a Windows Security Account Manager user database or an Active Directory user database, additional Windows configuration is required after you have installed ACS. For more information, see Windows Authentication Configuration, page 2-1.

For additional information about ACS, refer to the *User Guide for Cisco Secure ACS for Windows 4.0*.

System Requirements

Your ACS server must meet certain minimum hardware, operating system, and third-party software requirements. Additionally, if you are upgrading from a previous version of ACS, refer to ACS Upgrade Requirements, page 1-2.

This section contains:

- ACS Upgrade Requirements, page 1-2
- Server, Web Client, and Agent Requirements, page 1-2

ACS Upgrade Requirements

The setup program supports upgrades from previous versions of ACS. For information about the versions of ACS that we used to test the upgrade process, see the Release Notes. The latest version of the Release Notes are on Cisco.com, accessible from:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html

Server, Web Client, and Agent Requirements

This section contains details on server, web client, and agent requirements:

- ACS for Windows Server Requirements, Table 1-1 on page 1-3
- ACS for Windows Web Client Requirements, Table 1-2 on page 1-3
- ACS for Windows Server UCP Requirements, Table 1-3 on page 1-4

Note ACS for Windows is not designed to use the multiprocessor feature of any supported operating system; however, we did test ACS by using dual-processor computers.

The Windows 2000 Datacenter Server is not a supported operating system.

Windows service packs can be applied before or after installing ACS. If you do not install a required service pack before installing ACS, the ACS installation program may warn you that the required service pack is not present. If you receive a service pack error message, continue the installation, and then install the required service pack before starting user authentication with ACS.

Table 1-1 ACS for Windows Server Requirements

Component	Minimum Requirement
Hardware	• IBM PC-compatible with Pentium IV processor, 1.8 GHz or faster • Color monitor with minimum graphics resolution of 256 colors at 800 x 600 resolution • CD-ROM drive • 100BaseT or faster connection
Operating System	• Windows 2000 Server • Windows 2000 Advanced Server (Service Pack 4) without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed • Windows Server 2003, Enterprise Edition or Standard Edition (Service Pack 1)
File System	NTFS
Memory	1 Gigabyte, minimum
Virtual Memory	1 Gigabyte, minimum
Hard Drive Space	At least 1 GB of free hard drive space, minimum **Note** The actual amount of hard drive space required depends on several factors, including log file growth, and replication or backup purposes.

Table 1-2 ACS for Windows Web Client Requirements

Component	Minimum Requirement
Hardware/Software	IBM PC-compatible computer with Pentium IV processor running: • Microsoft Windows 2000 Server, or Advanced Server (Service Pack 4) • Microsoft Windows 2000 (Service Pack 4) • Microsoft Windows XP (Service Pack 2) • Microsoft Windows 2003 (Service Pack 1) (Enterprise or Standard Edition)
Hard Drive Space	400 MB virtual memory
Memory	256 MB minimum

Table 1-2 ACS for Windows Web Client Requirements

Browser	You must also install one of the following HTML browsers: • Microsoft Internet Explorer 6 Service Pack 1 and 5.5 for Windows–English and Japanese version • Netscape Web Browser 7.0, 7.1, and 7.2 for Windows–English and Japanese version[1]
Java Run-time Environment (JRE)	Sun JRE 1.4.2_04 or Microsoft Java Virtual Machine (JVM) **Note** Microsoft does not include JVM in Windows Server 2003. Instead, use the Sun Java Plug-in which is previously listed. For more information about Microsoft plans regarding its JVM, see http://www.microsoft.com/mscorp/java/.

[1] Several known problems are related to using Netscape Communicator with ACS. For more information, see the *Release Notes for Cisco Secure ACS for Windows* on Cisco.com.

Table 1-3 ACS for Windows Server UCP Requirements

Component	Minimum Requirement
User Changeable Password (UCP) Web Server	• Microsoft IIS 6.0 • Apache 1.3 web server

Third-Party Software Requirements

The Release Notes provide information about third-party software products that we tested with ACS and support, including applications such as:

- Web browsers and Java virtual machines
- Novell Directory Server (NDS) clients
- Token-card clients

Other than the software products described in the Release Notes, we have not tested the interoperability of ACS and other software products on the same computer. We only support the interoperability issues of software products that are mentioned in the Release Notes.

The most recent version of the Release Notes is posted on Cisco.com, accessible from:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html

Network and Port Requirements

Your network should meet the following requirements before you begin deploying ACS:

- For full TACACS+ and RADIUS support on Cisco IOS devices, AAA clients must run Cisco IOS Release 11.1 or later.
- Non-Cisco IOS AAA clients must be configured with TACACS+, RADIUS, or both.
- Dial-in, VPN, or wireless clients must be able to connect to the applicable AAA clients.

- The computer that is running ACS must be able to ping all AAA clients.
- Gateway devices between ACS and other network devices must permit communication over the ports needed to support the applicable feature or protocol. For information about ports to which ACS listens, see Table 1-4.
- A supported web browser must be installed on the computer that is running ACS. For the most recent information about tested browsers, see the Release Notes, available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html
- All network cards in the computer that is running ACS must be enabled. If a disabled network card is present on the computer that is running ACS, installing ACS may proceed slowly, due to delays caused by Microsoft CryptoAPI.

Note We tested ACS on computers that have only one network interface card.

- If you want ACS to use the Grant Dial-in Permission to User feature in Windows when authorizing network users, you must select this option in the Windows User Manager or Active Directory Users and Computers for the applicable user accounts.

Table 1-4 lists the ports to which ACS listens for communications with AAA clients, other ACS machines and applications, and web browsers. ACS uses other ports to communicate with external user databases; however, it initiates those communications rather than listening to specific ports. For example, if ACS initiates communications with LDAP or RADIUS token server databases, you can configure these destination ports in ACS. For more information about ports to which a particular external user database listens, see the documentation for that database.

Table 1-4 Ports that ACS Listens To

Feature/Protocol	UDP or TCP	Ports
RADIUS authentication and authorization	UDP	1645, 1812
RADIUS accounting	UDP	1646, 1813
TACACS+	TCP	49
Cisco Secure Database Replication	TCP	2000
RDBMS Synchronization with synchronization partners	TCP	2000
User-Changeable Password web application	TCP	2000
Logging	TCP	2001
Administrative HTTP port for new sessions	TCP	2002
Administrative HTTP port range	TCP	Configurable; default 1024 through 65535

Back Up Data

Before you install or upgrade ACS, we strongly recommend that you back up the computer on which you install ACS by using a Windows backup utility of your choice. Include the Windows Registry in the backup.

If you are upgrading or reinstalling ACS, use the ACS Backup feature to back up the ACS configuration and database, and then copy the backup file to a drive that is not local to the computer running ACS.

Caution If you are upgrading ACS rather than reinstalling, the backups that you create cannot be used after the upgrade is successful. The backups provide for recovery if you need to restore your previous installation of ACS.

For information about backing up ACS, see the *User Guide for Cisco Secure ACS for Windows*.

Gathering Answers for the Installation Questions

During new installations, or upgrades and reinstallations that do not preserve the existing configuration, the installation requires specific information about the computer on which you want to install ACS. To facilitate the installation, collect the applicable information before you begin the installation.

Note If you are upgrading or reinstalling ACS and intend to keep the existing configuration and database, you do not need to perform the following procedure, which requires information that is already recorded in your ACS installation.

To collect information that is required during the installation of ACS:

Step 1 Determine whether the computer on which you will install ACS is a domain controller or a member server. If you want ACS to authenticate users with a Windows domain user database, after you install ACS, you must perform the additional Windows configuration, which is discussed in Windows Authentication Configuration, page 2-1.

Step 2 Confirm that these items are completed:

- End user clients can successfully connect to AAA clients.
- This Windows Server can ping the AAA clients.
- Any Cisco IOS clients are running Cisco IOS release 11.1 or later.
- Microsoft Internet Explorer 6.0 Service Pack 1 or Netscape 7.02 is installed.

Step 3 Create a password for your database access. You will need this password to manage your database information. Keep this password in a safe, accessible place so that technical support can gain access to the database.

What You Can Do

This document provides detailed procedures for installing, reinstalling, and upgrading ACS. You must select the right procedure for your situation.

Table 1-5 lists the five possible installation and upgrade scenarios. See Table 1-5 to determine which procedure applies to your situation.

Note Before you perform any installation or upgrade procedure, we strongly recommend that you read Preparation for Installing or Upgrading ACS, page 1-1, and perform the applicable tasks in that section.

Table 1-5 Installation and Upgrade Scenarios

If your installation scenario is a:	Refer to. . .
First-time installation	Creating an ACS Installation, page 1-7
Reinstallation, *preserving* the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration, page 1-11
Reinstallation, *overwriting* the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation, page 1-14
Upgrade, *preserving* the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration, page 1-11
Upgrade, *overwriting* the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation, page 1-14

Creating an ACS Installation

This section contains information on how to install ACS for the first time.

Note For information about upgrading or reinstalling an existing ACS installation, see Table 1-5.

Before You Begin

For information about what must be completed before installing ACS, see Preparation for Installing or Upgrading ACS, page 1-1.

If you want ACS to authenticate users with a Windows domain user database, after you install ACS you must perform additional Windows configuration, which is discussed in Windows Authentication Configuration, page 2-1.

To install ACS:

Step 1 Using a local administrator account, log in to the computer on which you want to install ACS.

Note Remote installations performed by using Windows Terminal Services are not tested and are not supported. We recommend that you disable Terminal Services while performing any installation or upgrade. Virtual Network Computing (VNC) has been tested successfully.

Step 2 Insert the ACS CD into a CD-ROM drive on the computer.

If the CD-ROM drive supports the Windows **autorun** feature, the ACS for Windows dialog box appears.

Note If the computer does not have the minimum system requirements, a dialog box appears. You can apply these requirements before or after installing ACS. You can continue with the installation, but you must apply the minimum requirements after the installation is complete; otherwise, ACS may not function reliably.

Step 3 If:

a. The Cisco Secure ACS for Windows dialog box appears, click **Install**.

b. The Cisco Secure ACS for Windows dialog box does not appear, run *setup.exe*, located in the root directory of the ACS CD.

Note If the computer does not have a required service pack installed, a dialog box appears. You can apply Windows service packs before or after installing ACS. You can continue with the installation, but the required service pack must be installed after the installation is complete; otherwise, ACS may not function reliably.

The Cisco Secure ACS Setup dialog box displays the software license agreement.

Step 4 Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.

The Welcome dialog box displays basic information about the setup program.

Step 5 After you have read the information in the Welcome dialog box, click **Next**.

The Before You Begin dialog box lists items that you must complete before continuing with the installation. The same items are discussed in Gathering Answers for the Installation Questions, page 1-6.

Step 6 If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**.

Note If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see Preparation for Installing or Upgrading ACS, page 1-1.

The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. This is the drive and path where the setup program installs ACS.

Step 7 If you want to change the installation location:

a. Click **Browse**.

The Choose Folder dialog box appears. The Path box contains the installation location.

b. Change the installation location. You can type the new location in the **Path** box, or use the Drives and Directories lists to select a new drive and directory. The installation location must be on a drive local to the computer.

Note Do not specify a path that contains a percent symbol (%). If you do so, installation may appear to continue properly but will fail before it ends.

c. Click **OK**.

Note If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. To continue, click **Yes**.

In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.

Step 8 Click **Next**.

The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the ACS internal database only, or with a Windows user database.

Note After you have installed ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

Step 9 If you want to authenticate users with the ACS internal database only, click **Check the Cisco Secure ACS database only**.

Step 10 If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the ACS internal database:

a. Click **Also check the Windows User Database**.

The **Yes, refer to "Grant dial-in permission to user" setting** check box becomes available.

Note The **Yes, refer to "Grant dial-in permission to user" setting** check box applies to all forms of access that ACS controls; not just dial-in access. For example, a user accessing your network through a VPN tunnel is not dialing in to a network access server; however, if the **Yes, refer to "Grant dial-in permission to user" setting** check box is selected, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

b. If you want to allow access by users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, click **Yes, refer to "Grant dial-in permission to user" setting**.

Step 11 Click **Next**.

The setup program installs ACS and updates its configuration.

The Advanced Options dialog box displays several features of ACS that are not enabled by default. For more information about these features, see the *User Guide for Cisco Secure ACS for Windows 4.0*.

Note The features appear in the ACS HTML interface only if you enable them. After installation, you can enable or disable them on **Interface Configuration > Advanced Options**.

Step 12 For each feature that you want to enable, check the corresponding check box.

Step 13 Click **Next**.

The Active Service Monitoring dialog box appears.

Note After installation, you can configure active service monitoring features on the Active Service Management page in the System Configuration section.

Step 14 If you want ACS to monitor user authentication services, click **Enable Log-in Monitoring**. From the **Script to execute** list, select the option that you want applied in the event of authentication service failure:

- **No Remedial Action**—ACS does not run a script.

  Note This option is useful if you enable event e-mail notifications.

- **Reboot**—ACS runs a script that reboots the computer that runs ACS.
- **Restart All**—ACS restarts all ACS services.
- **Restart RADIUS/TACACS+**—ACS restarts only the RADIUS and TACACS+ services.

Step 15 If you want ACS to send an e-mail message when service monitoring detects an event, click **Mail Notification**.

Step 16 Click **Next**.

The Database Encryption Password dialog box appears.

Note The Database Encryption Password is encrypted and stored in the ACS registry. You might have to reuse this password when critical problems arise and the database needs to be accessed manually. Keep this password in a safe, accessible place so that technical support can gain access to the database.

Step 17 Enter a password for database encryption. The password should be at least 8 characters long and should contain characters and digits. There are no invalid characters. Click **Next**.

The setup program ends and the Cisco Secure ACS Service Initiation dialog box appears.

Step 18 For each option that you require, check the corresponding check box. The actions that are associated with the options occur after the setup program ends:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not select this option, the ACS HTML interface is not available; unless you reboot the computer or start the CSAdmin service.
- **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation**—Opens the ACS HTML interface in the default web browser for the current Windows user account.
- **Yes, I want to view the Readme file**—Opens *README.TXT* in Windows Notepad.

Step 19 Click **Next**.

If you so chose, the ACS services start. The Setup Complete dialog box displays information about the ACS HTML interface.

Step 20 Click **Finish**.

The setup program exits. If, in Step 18, you chose the options to view the HTML interface or *README.TXT* file, those options occur now.

On the computer that is running ACS, you can access the ACS HTML interface by using the ACS Admin desktop icon; or you can use this URL in a supported web browser:

```
http://127.0.0.1:2002
```

Note The ACS HTML interface is available only if you chose to start ACS services in Step 18. If you did not, to make the HTML interface available, you can reboot the computer or type **net start csadmin** at a DOS prompt.

Step 21 If you want ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For procedures, see Windows Authentication Configuration, page 2-1.

Reinstalling or Upgrading ACS

The two choices for upgrading or reinstalling ACS software are:

- Reinstalling or Upgrading an Existing Configuration, page 1-11
- Reinstalling or Upgrading ACS without Data Preservation, page 1-14

If you are installing ACS for the first time, see Creating an ACS Installation, page 1-7.

Reinstalling or Upgrading an Existing Configuration

Use this procedure to reinstall or upgrade ACS if you want to preserve all existing configuration and database information.

Note For information about installing ACS the first time, see Table 1-5.

Before You Begin

For information about what you must complete before reinstalling or upgrading ACS, see Preparation for Installing or Upgrading ACS, page 1-1.

Close all applications or command windows that are accessing any directory in the ACS directory. The installation cannot succeed if another process is using the ACS directory or any of its subdirectories. For example, if Windows Explorer is displaying the contents of a ACS directory, installation fails.

If you want ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For the appropriate procedures, see Windows Authentication Configuration, page 2-1.

To reinstall or upgrade ACS, and preserve the existing configuration and ACS internal database:

Step 1 Using a local administrator account, log in to the computer on which you want to install ACS.

Note Remote installations that you perform by using Windows Terminal Services are not tested and are not supported. We recommend that you disable Terminal Services while performing any installation or upgrade. Virtual Network Computing (VNC) has been tested successfully.

Step 2 Insert the ACS CD into a CD-ROM drive on the computer.

If the CD-ROM drive supports the Windows **autorun** feature, the Cisco Secure ACS for Windows dialog box appears.

Note If the computer does not have the minimum system requirements, a dialog box appears. You can apply these requirements before or after installing ACS. You can continue with the installation, but you must apply the minimum requirements after the installation is complete; otherwise, ACS may not function reliably.

Step 3 If:

a. The Cisco Secure ACS for Windows Server dialog box appears, click **Install**.

b. The Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the ACS CD.

Note If the computer does not have a required service pack installed, a dialog box appears. You can apply Windows service packs before or after installing ACS. You can continue with the installation, but the required service pack must be applied after the installation is complete; otherwise, ACS may not function reliably.

An information dialog box displays some details about Windows authentication. Click **OK**.

The Cisco Secure ACS Setup dialog box displays the software license agreement.

Step 4 Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.

The Welcome dialog box displays basic information about the setup program.

Step 5 After you have read the information in the Welcome dialog box, click **Next**.

A dialog box displays any warnings if your machine will not run ACS without action on your part. Respond to the warning by performing any corrective action that is required. You may install the software without exiting the install; but you will see a reminder to fix any minimum system requirements that are not met after the setup program has run. Click **Next**.

If no warnings appear, the Before You Begin dialog box lists items that you must complete before continuing with the installation. The same items are discussed in Gathering Answers for the Installation Questions, page 1-6.

Step 6 If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item; then click **Next**.

Note If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see Preparation for Installing or Upgrading ACS, page 1-1.

The Previous Installation dialog box appears.

Step 7 Click **Yes, keep the existing configuration**.

Caution Ensure that you check the Yes, import the existing configuration check box; it should not be unchecked. If you proceed without checking the **Yes, keep the existing configuration** check box, the setup program deletes all existing AAA client, user, and group information.

If you are uncertain about keeping the configuration, click **Explain** to see details on keeping the existing configuration.

Step 8 Click **Next**.

The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. The setup program installs ACS on this drive and path.

Step 9 If you want to change the installation location:

a. Click **Browse**.

The Choose Folder dialog box appears. The Path box contains the installation location.

b. Change the installation location. You can type the new location in the **Path** box, or select a new drive and directory from the Drives and Directories lists.

Note The installation location must be on a drive that is local to the computer.

c. Click **OK**.

Note If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. To continue, click **Yes**.

In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.

Step 10 Click **Next**.

The setup program installs ACS and updates its configuration.

The Cisco Secure ACS Service Initiation dialog box appears.

Enter a password for database encryption, click **Next**.

Note The Database Encryption Password is encrypted and stored in the ACS configuration. You might have to reuse this password when critical problems arise and the database needs to be accessed manually. Keep this password in a safe, accessible place so that technical support can gain access to the database.

Step 11 The installation is finished. For each option that you require, check the corresponding check box. The actions that are associated with each option occur after the setup program ends:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not select this option, the HTML interface is not available; unless you reboot the computer or start the CSAdmin service.
- **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation**—Opens the ACS HTML interface in the default web browser for the current Windows user account.
- **Yes, I want to view the Readme file**—Opens *README.TXT* in Windows Notepad.

Step 12 Click **Next**.

If you so chose, the ACS services start. The Setup Complete dialog box displays information about the ACS HTML interface.

Step 13 Click **Finish**.

The setup program exits. If, in Step 11, you chose the options to view the HTML interface or *README.TXT* file, those options occur now.

Step 14 If minimum system requirements were not met, a message might appear warning you to remedy the problem. Click **OK** to continue and resolve the problem where possible.

On the computer that is running ACS, you can access the ACS HTML interface by using the ACS Admin desktop icon; or you can use this URL in a supported web browser:

```
http://127.0.0.1:2002
```

Note The ACS HTML interface is available only if you chose to start ACS services in Step 11. If you did not and you want to make the HTML interface available, you can reboot the computer or type **net start csadmin** at a DOS prompt.

Step 15 If you want ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For the appropriate procedures, see Windows Authentication Configuration, page 2-1.

Note If you previously configured ACS services to run by using a specific username, that configuration was lost during the reinstallation.

Reinstalling or Upgrading ACS without Data Preservation

Use this procedure to reinstall or upgrade ACS if you do not intend to preserve the existing configuration and database information.

Caution Performing this procedure deletes the existing configuration of ACS, including all AAA client, user, and group information. Unless you have backed up your ACS data and the Windows Registry, you cannot recover the previous configuration and database.

Before You Begin

For information about what must be completed before reinstalling or upgrading ACS, see Preparation for Installing or Upgrading ACS, page 1-1.

Close all applications or command windows that are accessing any directory in the ACS directory. The installation cannot succeed if another process is using the ACS directory or any of its subdirectories. For example, if Windows Explorer is displaying the contents of an ACS directory, installation fails.

If you want ACS to authenticate users with a Windows domain user database, after you install ACS you must perform additional Windows configuration, discussed in Windows Authentication Configuration, page 2-1.

To reinstall or upgrade ACS without preserving the existing configuration or ACS internal database:

Step 1 Using a local administrator account, log in to the computer on which you want to install ACS.

Note Remote installations that are performed by using Windows Terminal Services are not tested and are not supported. We recommend that you disable Terminal Services while performing any installation or upgrade. Virtual Network Computing (VNC) has been tested successfully.

Step 2 Insert the ACS CD into a CD-ROM drive on the computer.

If the CD-ROM drive supports the Windows **autorun** feature, the ACS for Windows dialog box appears.

Note If the computer does not have the minimum system requirements, a dialog box appears. You can apply these requirements before or after installing ACS. You can continue with the installation, but the minimum requirements must be applied after the installation is complete; otherwise, ACS may not function reliably.

Step 3 If:

a. The Cisco Secure ACS for Windows dialog box appears, click **Install**.

b. The Cisco Secure ACS for Windows dialog box does not appear, run `setup.exe`, located in the root directory of the ACS CD.

> **Note** If the computer does not have a required service pack installed, a dialog box appears. You can apply Windows service packs before or after installing ACS. You can continue with the installation, but the required service pack must be applied after the installation is complete; otherwise, ACS may not function reliably.

The Cisco Secure ACS Setup dialog box displays the software license agreement.

Step 4 Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.

The Welcome dialog box displays basic information about the setup program.

Step 5 After you have read the information in the Welcome dialog box, click **Next**.

The Before You Begin dialog box lists items that you must complete before continuing with the installation. The same items are discussed in Gathering Answers for the Installation Questions, page 1-6.

Step 6 If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**.

> **Note** If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see Preparation for Installing or Upgrading ACS, page 1-1.

The Existing Installation of Cisco Secure ACS v*x.x* dialog box appears.

Step 7 Click **Next**.

The setup program removes the previous installation of ACS.

If ACS services are running, the Cisco Secure ACS Uninstall dialog box appears.

Step 8 If the Cisco Secure ACS Uninstall dialog box appears. Click **Continue**.

The setup program ends, removing the previous installation of ACS.

The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. The setup program installs ACS on this drive and path.

Step 9 If you want to change the installation location:

a. Click **Browse**.

The Choose Folder dialog box appears. The Path box contains the installation location.

b. Change the installation location. You can type the new location in the **Path** box; or you can use the Drives and Directories lists to select a new drive and directory. The installation location must be on a drive that is local to the computer.

> **Note** Do not specify a path that contains a percent symbol (%). If you do, installation may appear to continue properly; but will fail before it ends.

c. Click **OK**.

Note If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. To continue, click **Yes**.

In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.

Step 10 During the installation ACS checks for previous instances of the application. If it detects a previous uninstallation, a dialog box appears with the message: `Setup has detected an existing ACS internal database. You may keep the existing ACS internal database if you wish.` Click **Yes** to install the existing dump file that was saved from your previous uninstall. If you click **No**, the database dump file will remain; but will not be installed.

If you clicked **Yes**, the previous database is installed. If you clicked **No**, the following installation continues without installing the database file.

The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the ACS internal database only; or with a Windows user database.

Note After you install ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

Step 11 If you want to authenticate users with the ACS internal database only, click **Check the Cisco Secure ACS database only**.

Step 12 If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the ACS internal database:

a. Click **Also check the Windows User Database**.

The **Yes, refer to "Grant dial-in permission to user" setting** check box becomes available.

Note The Yes, refer to "Grant dial-in permission to user" setting check box applies to all forms of access that ACS controls; not just dial-in access. For example, a user accessing your network through a VPN tunnel is not dialing in to a network access server; however, if the **Yes, refer to "Grant dial-in permission to user" setting** check box is checked, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

b. If you want to allow access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, click **Yes, refer to "Grant dial-in permission to user" setting**.

Step 13 Click **Next**.

The setup program installs ACS and updates its configuration.

The Advanced Options dialog box lists several ACS features that are not enabled by default. For more information about these features, refer to the *User Guide for Cisco Secure ACS for Windows 4.0*.

Note The features appear in the ACS HTML interface only if you enable them. After installation, you can enable or disable them by choosing **Interface Configuration > Advanced Options**.

Step 14 For each feature that you want to enable, check the corresponding check box. Click **Next**.

The Active Service Monitoring dialog box appears.

Note After installation, you can configure active service-monitoring features on the Active Service Management page in the System Configuration section.

Step 15 If you want ACS to monitor user authentication services, click **Enable Log-in Monitoring**. From the **Script to execute** list, select the option that you want applied in the event of authentication service failure:

- **No Remedial Action**—ACS does not run a script.

  Note This option is useful if you enable event e-mail notifications.

- **Reboot**—ACS runs a script that reboots the computer that runs ACS.
- **Restart All**—ACS restarts all ACS services.
- **Restart RADIUS/TACACS+**—ACS restarts only the RADIUS and TACACS+ services.

Step 16 If you want ACS to send an e-mail message when service monitoring detects an event, click **Mail Notification**.

If you chose to save the previous instance of the database, the Cisco Secure ACS Service Initiation dialog box appears.

Step 17 Enter the password that you created during the uninstall procedure to save the database. Click **Next**.

Step 18 For each option that you require, check the corresponding check box. The actions that are associated with each option occur after the setup program ends:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not select this option, the ACS HTML interface is not available; unless you reboot the computer or start the CSAdmin service.
- **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation**—Opens the ACS HTML interface in the default web browser for the current Windows user account.
- **Yes, I want to view the Readme file**—Opens *README.TXT* in Windows Notepad.

Step 19 Click **Next**.

If you so chose, the ACS services start. The Setup Complete dialog box displays information about the ACS HTML interface.

Step 20 Click **Finish**.

The setup program exits. If, in Step 18, you chose the options to view the HTML interface or *README.TXT* file, those options occur now.

On the computer that is running ACS, you can access the ACS HTML interface by using the ACS Admin desktop icon or you can use this URL in a supported web browser:

```
http://127.0.0.1:2002
```

Note The ACS HTML interface is available only if you chose to start ACS services in Step 18. If you did not, to make the HTML interface available, you can reboot the computer or type **net start csadmin** at a DOS prompt.

Step 21 If you want ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For the appropriate procedures, see Windows Authentication Configuration, page 2-1.

Note If you previously configured ACS services to run by using a specific username, that configuration was lost during the reinstallation.

CHAPTER 2

Post-Installation Tasks

This section provides the post-installation tasks for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

Windows Authentication Configuration

If ACS uses Windows databases to authenticate users, additional configuration is required for reliable user authentication and group mapping. Requirements vary depending on whether you install ACS on a domain controller or member server.

This section contains:

Configuring for Domain Controller Authentication

When ACS runs on a domain controller and you need to authenticate users with a Windows user database, the additional configuration required varies, depending on your Windows networking configuration. Some of the following steps are always applicable when ACS runs on a domain controller; other steps are required only in certain conditions, as noted at the beginning of the step. Perform only those steps that always apply and that apply to your Windows networking configuration:

Step 1 Add CISCO workstation.

To satisfy Windows requirements for authentication requests, ACS must specify the Windows workstation in to which the user is attempting to log. Because ACS cannot determine this information from authentication requests that AAA clients send, it uses a generic workstation name for all requests. Use *CISCO* as the name of the workstation.

In the local domain, and in each trusted domain and child domain that ACS will use to authenticate users, ensure that:

- A computer account named *CISCO* exists.
- All users that Windows will authenticate have permission to log in to the computer named *CISCO*.

For more information, see the Microsoft documentation for your operating system.

Step 2 Verify the server service status.

The ACS authentication service depends on the Server service, which is a standard service in Microsoft Windows. On the computer that is running ACS, verify that the Server service is running and that its Startup Type is set to Automatic.

Tip To configure the Server service, use the local administrator account to log in to the computer that is running ACS and choose **Start > Programs Administrative Tools > Services**. The services appear alphabetically.

For more information, see the Microsoft documentation for your operating system.

Step 3 Verify the NTLM version.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains. No changes are required on ACS, only Windows.

ACS supports authentication of Windows credentials by using LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but need to ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager Authentication Level policy;** and set the policy. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication level documentation on the Microsoft website.

b. In addition to the previous setting, if you want to use NTLM version 2, you must also ensure that each:

   - Windows 2000 domain controller involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

     or

   - Domain controller involved in user authentication has the Windows 2003 Service Pack 1. This version does not require any patch.

Step 4 Create a user account.

Tip If you have upgraded or reinstalled ACS and you created a user account for the previous installation, complete this step only if you want to use a different user account to run ACS services.

If you are installing ACS on Windows 2003, then in the domain of the domain controller that is running ACS, you must create a Domain Administrator account that you can use to run ACS services (as explained in subsequent steps in this procedure).

a. Create a domain administrator account. Use this domain administrator account to run ACS services.

Tip Give the domain administrator account an easily recognizable name, such as *ACSuser*. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems that are related to failed ACS authentication attempts.

To the domain administrator account that you create, grant **Read all properties** permission for all Active Directory (AD) folders containing users who require ACS authentication. To grant permission for AD folders, access AD by using the Microsoft Management Console and configure the security properties for the folders that contain users whom ACS will authenticate.

Tip You can access the security properties of an AD folder of users by right-clicking the folder, selecting **Properties**, and choosing the Security tab. Click **Add** to include the username.

For more information, see Windows 2000 Server AD.

Step 5 Configure Local Security policies.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains.

Tip If you have upgraded or reinstalled ACS and you completed this step for the previous installation, it is required only if you want to use a different user account to run ACS services.

For the domain administrator account that you created in the preceding step, add the user to the following local security policies:

- **Act as part of the operating system**.
- **Log on as a service**.
- **Log on a batched job**.

For more information, see Configuring Local Security Policies, page 2-9.

Step 6 Configure services.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains.

Configure all ACS services to run as the user that you added to the security policies in the preceding step.

For more information, see Configuring ACS Services, page 2-11.

Step 7 Enable NetBIOS.

ACS requires NetBIOS for communications with domain controllers of trusted or child domains. Therefore, you must enable NetBIOS on:

- The domain controller that is running ACS.
- Trusted domain controllers for domains containing users that ACS must authenticate.
- Domain controllers for child domains containing users whom ACS must authenticate.

To enable **NetBIOS**:

a. Access the advanced TCP/IP properties of the network connections on each domain controller.

b. Click the **WINS** tab.

c. Configure NetBIOS as applicable.

For more information, see:

- Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server.
- Microsoft.com: Install WINS in Windows Server 2003.

Step 8 Ensure DNS operation.

Especially for authentication of users in AD, ACS needs DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event notification e-mail. If you configure such features by using hostnames, rather than IP addresses, and DNS does not operate correctly, those features might fail, as would authentication requests that are sent to AD.

For more information, see the Microsoft documentation for your operating system.

Step 9 Specify DNS suffixes.

Note This step is required only if ACS authenticates users with the AD of more than one domain.

On the domain controller that is running ACS, configure the network connection that ACS uses so that the network connection lists each trusted and child domain as a DNS suffix:

a. Access the advanced TCP/IP properties of the network connection.

b. Choose the DNS tab.

c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see:

- Microsoft.com: Configure TCP/IP to use DNS (Windows 2000).
- Microsoft.com: Configure TCP/IP to use DNS (Windows 2003).

Step 10 Configure WINS.

You must enable WINS on your network if ACS must authenticate users belonging to a trusted or child domain, and if ACS cannot rely on DNS to contact the domain controllers in those domains.

For more information, see the Microsoft documentation for your operating system.

Step 11 Configure *LMHOSTS* file.

Note Only perform this step if, after performing the preceding steps, Windows authentication and group mapping for users who belong to trusted domains or child domains are unreliable.

As a final means of ensuring communication with other domain controllers, on the domain controller that is running ACS, configure a *LMHOSTS* file to include entries for each domain controller of a trusted or child domain containing users whom ACS must authenticate.

Tip The format of an *LMHOSTS* file is very particular. You must understand the requirements of configuring the *LMHOSTS* file.

For more information, see:

1. Microsoft.com: LMHOSTS File.
2. The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is *<systemroot>\system32\drivers\etc\lmhosts.sam*.

Configuring for Member Server Authentication

When ACS runs on a member server and you must authenticate users with a Windows user database, the additional configuration that is required varies, depending on your Windows networking configuration. Most of the following steps are always applicable when ACS runs on a member server; other steps are required only in certain conditions, as noted at the beginning of the step. Perform only those steps that always apply and that apply to your Windows networking configuration:

Step 1 Verify domain membership.

One common configuration error that prevents Windows authentication is the erroneous assignment of the member server to a workgroup with the same name as the Windows domain that you want to use to authenticate users. While this error might seem obvious, we recommend that you verify that the computer running ACS is a member server of the correct domain.

Tip To determine domain membership of a computer, on the Windows desktop, right-click **My Computer**, select **Properties**, click the **Network Identification** tab, and read the information on that tab.

If the computer that is running ACS is not a member of the domain that your deployment plans require, correct this situation before continuing the procedure.

For more information, see the Microsoft documentation for your operating system.

Step 2 Add CISCO workstation.

To satisfy Windows requirements for authentication requests, ACS must specify the Windows workstation in to which the user is attempting to log. Because ACS cannot determine this information from authentication requests that AAA clients send, it uses a generic workstation name for all requests. Use *CISCO* as the name of the workstation.

In the local domain, and in each trusted domain and child domain that ACS will use to authenticate users, ensure that:

- A computer account named *CISCO* exists.
- All users that Windows will authenticate have permission to log in to the computer named *CISCO*.

For more information, see the Microsoft documentation for your operating system.

Step 3 Verify the server service status.

The ACS authentication service depends on the server service, which is a standard service in Microsoft Windows. On the computer that is running ACS, verify that the server service is running and that its Startup Type is set to **Automatic**.

Tip To configure the Server service, use the local administrator account to log in to the computer that is running ACS and choose **Start > Programs Administrative Tools > Services**. The services appear alphabetically.

For more information, see the Microsoft documentation for your operating system.

Step 4 Verify the NTLM version.

Note This step is required only if ACS authenticates users who belong to trusted domains or child domains. No changes are required on ACS, only Windows.

ACS supports authentication of Windows credentials by using LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but need to ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager Authentication Level policy;** and set the policy. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication level documentation on the Microsoft website.

b. In addition to setting the above, if you wish to use NTLM version 2 you must also ensure that each:

  – Windows 2000 domain controller involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

  or

  – Domain controller involved in user authentication has Windows 2003 Service Pack 1. This version does not require any patch.

Step 5 Create a user account.

Tip If you have upgraded or reinstalled ACS and you completed this item previously, it is required only if you want to use a different user account to run ACS services.

If you are running ACS on Windows 2003, then the domain of the domain controller that is running ACS must contain a domain administrator account that you can use to run ACS services (as explained in subsequent steps of this procedure).

a. Create a domain administrator account. Use this domain administrator account to run ACS services.

Tip Give the domain administrator account an easily recognizable name, such as *ACSuser*. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems that are related to failed ACS authentication attempts.

---

b. To the domain administrator account that you create, grant **Read all properties** permission for all AD folders containing users who require ACS authentication. To grant permission for AD folders, access AD by using the Microsoft Management Console and configure the security properties for the folders that contain users whom ACS will authenticate.

Tip You can access the security properties of an AD folder of users by right-clicking the folder, selecting **Properties**, and clicking the **Security** tab. Click **Add** to include the username.

For more information, see Windows 2000 Server AD.

Step 6 Configure local security policies.

To the domain administrator account that you created in the preceding step, add the user to the following local security policies:

- **Act as part of the operating system**.
- **Log on as a service**.
- **Log on a batched job**.

For more information, see Configuring Local Security Policies, page 2-9.

Step 7 Configure services.

Configure all ACS services to run as the user that you added to the security policies in the preceding step.

For more information, see Configuring ACS Services, page 2-11.

Step 8 Enable NetBIOS.

ACS requires NetBIOS for communications with all domain controllers to which it submits user authentication requests. Therefore, you must enable NetBIOS on:

- The member server that is running ACS.
- The domain controller of the domain containing ACS.
- Domain controllers of trusted domains containing users that ACS must authenticate.
- Domain controllers of child domains containing users whom ACS must authenticate.

To enable **NetBIOS**:

- Access the advanced TCP/IP properties of the network connections on each domain controller.
- Click the **WINS** tab.
- Configure NetBIOS as applicable.

For more information, see:

- Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server.
- Microsoft.com: Install WINS in Windows Server 2003.

Step 9 Ensure DNS operation.

Especially for authentication of users in Active Directory (AD), ACS needs DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event-notification e-mail. If you configure such features by using hostnames, rather than IP addresses, and DNS does not operate correctly, those features might fail, as would authentication requests that are sent to AD.

For more information, see the Microsoft documentation for your operating system.

Step 10 Specify DNS suffixes.

Note This step is required only if ACS authenticates users with the AD of more than one domain.

On the member server that is running ACS, configure the network connection that ACS uses so that the network connection lists each domain as a DNS suffix:

a. Access the advanced TCP/IP properties of the network connection.

b. Choose the DNS tab.

c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see:

- Microsoft.com: Configure TCP/IP to use DNS (Windows 2000).
- Microsoft.com: Configure TCP/IP to use DNS (Windows 2003).

Step 11 Configure WINS.

If ACS must authenticate users belonging to a trusted or child domain, and if ACS cannot rely on DNS to contact the domain controllers in those domains, you must enable WINS on your network.

For more information, see the Microsoft documentation for your operating system.

Step 12 Configure *LMHOSTS* file.

Note Only perform this step if, after performing the preceding steps, Windows authentication and group mapping are unreliable.

As a final means of ensuring communication with domain controllers, on the member server that is running ACS, configure a *LMHOSTS* file to include entries for each domain controller containing users that ACS must authenticate. This includes domain controllers of child domains.

Tip The format of an *LMHOSTS* file is very particular. Ensure that you understand the requirements of configuring the *LMHOSTS* file.

For more information, see:

- Microsoft.com: LMHOSTS File
- The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is <*systemroot*>*\system32\drivers\etc\lmhosts.sam*

Configuring Local Security Policies

Before You Begin

This procedure is required only if one of the following conditions is true:

- ACS runs on a member server and must authenticate users with a Windows user database.
- ACS runs on a domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run ACS. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-5, or Configuring for Domain Controller Authentication, page 2-2.

To configure local security policies:

Step 1 Using the local administrator account, log in to the computer that is running ACS.

Step 2 Choose **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

Tip If Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**. Double-click **Administrative Tools**. and then double-click **Local Security Policy**.

The Local Security Settings window appears.

Step 3 In the Name column, double-click **Local Policies**, and then double-click **User Rights Assignment**.

The Local Security Settings window displays a list of policies with associated settings. The two policies that you must configure are:

- Act as part of the operating system.
- Log on as a service.

Step 4 For the **Act as part of the operating system** policy and **Log on as a service** policy:

a. Double-click the policy name.

The Local Policy Setting dialog box appears.

b. Click **Add**.

The Select Users or Groups dialog box appears.

c. In the box below the Add button, type the username for the user account.

Note The username must be in domain-qualified format. For example, if you created a user named *ACSuser* in the *CORPORATE* domain, type *CORPORATE\ACSuser*.

d. Click **Check Names**.

The Enter Network Password dialog box appears.

e. Complete the following:

- **Connect as**—Type a domain-qualified username. The username must exist in the domain specified in c. For example, if the domain specified is *CORPORATE* and *echamberlain* is a valid user in that domain, type *CORPORATE\echamberlain*.
- **Password**—Type the password for the user account that you specified. Click **OK**.

Windows verifies the existence of the username in c. The Enter Network Password dialog box closes.

f. In the Select Users or Groups dialog box, click **OK**.

The Select Users or Groups dialog box closes.

Windows adds the username to the Assign To list in the Local Policy Setting dialog box.

g. Click **OK**.

The Local Policy Setting dialog box closes. The domain-qualified username specified in c. appears in the settings associated with the policy that you configured.

h. Verify that the username that is specified in c. appears in the Local Setting column for the policy that you modified. If it does not, repeat these steps.

Tip To see the username that you added, you might have to widen the Local Setting column.

Note The Effective Setting column does not dynamically update. This procedure includes subsequent verification steps for ensuring that the Effective Setting column contains the required information.

After you have configured the **Act as part of the operating system** policy and the **Log on as a service** policy, the user account appears in the Local Setting column for the policy that you configured.

Step 5 Verify that the security policy settings that you changed are in effect on the computer that is running ACS:

a. Close the Local Security Settings window.

To refresh the information in the Effective Setting column, close the window.

b. Open the Local Security Settings window again. Choose **Start > Programs > Administrative Tools > Local Security Policy**.

c. In the Name column, double-click **Local Policies** and double-click **User Rights Assignment**.

The Local Security Settings window displays an updated list of policies with their associated settings.

d. For the **Act as part of the operating system** policy and again for the **Log on as a service** policy, verify that the username that you added to the policy appears in the Effective Setting column.

Note If the username that you configured the policies to include does not appear in the Effective Setting column for both policies, the security policy settings on the domain controller might conflict with the local setting. Resolve the conflict by configuring security policies on the domain controller to allow the local settings to be the effective settings for these two policies. For more information about configuring security policies on the domain controller, see the Microsoft documentation for your operating system.

The user account has the required privileges to run ACS services and support Windows authentication.

Step 6 Close the Local Security Settings window.

The specified user account has the permissions necessary to run ACS services successfully.

Configuring ACS Services

Before You Begin

This procedure is required only if one of the following conditions is true:

- ACS runs on a member server and must authenticate users with a Windows user database.
- ACS runs on a domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run ACS and assigned it the permissions necessary to run ACS services. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-5, or Configuring for Domain Controller Authentication, page 2-2.

To configure ACS services:

Step 1 Using the local administrator account, log in to the computer that is running ACS.

Step 2 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Tip If the Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**. Double-click **Administrative Tools** and then double-click **Services**.

The Services window displays a list of service groups and a list of all registered services for the current group. The list of service groups is labeled Tree. The registered services for the current group appear in the list to the right of the Tree list.

Step 3 In the Tree list, click **Services (local)**.

The Windows services that ACS installs are:

- CSAdmin
- CSAuth
- CSDbSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

Step 4 For each ACS service:

a. In the list of services, right-click a ACS service and, from the shortcut menu, choose **Properties**.

The Computer Browser Properties (Local Computer) dialog box appears.

b. Choose the **Log On** tab.

c. Select the **This account** option.

d. In the box next to the **This account** option, type the username for the account.

Note The username must be in domain-qualified format. For example, if you created a user named *ACSuser* in the *CORPORATE* domain, type **CORPORATE\ACSuser**.

e. In the **Password** box and in the **Confirm Password** box, type the password for the user account.

f. Click **OK**.

All ACS services are configured to run by using the privileges of the user account.

Step 5 To restart all ACS services:

a. Log in to the ACS HTML interface.

b. Click **System Configuration**, click **Service Control**, and then, at the bottom of the browser window, click **Restart**.

With the exception of CSAdmin, ACS services restart.

c. Wait until ACS finishes restarting services. This usually takes a minute or two.

d. Continuing as the local administrator on the computer that is running ACS, choose **Start > Programs Administrative Tools > Services**.

e. In the Name column, double-click **CSAdmin**.

The CSAdmin Properties dialog box appears.

f. Click **Stop** and wait for the Service Control dialog box to close.

g. Click **Start** and wait for the Service Control dialog box to close.

h. In the CSAdmin Properties dialog box, click **OK**.

The CSAdmin Properties dialog box closes.

i. Close the Services window.

The ACS services run by using the privileges of the user account that you specified.

ACS 3.x to 4.0 ODBC Logging Updates

If you used ACS 3.x ODBC logging and upgraded to ACS 4.0 preserving your data, you must update the ODBC tables so that the SQL tables continue to work.

Changes to the SQL database now present all the ODBC fields as strings rather than numbers. Field types have been changed from INTEGER to VARCHAR. For example, `Message_Type VARCHAR(255) NULL`.

To recreate the tables:

Step 1 Choose **System Configuration > Logging.**

The Logging Configuration page appears.

Step 2 Click the name of the ODBC log to enable.

The ODBC log Configuration page appears, where *log* is the name of the ODBC log that you selected.

Step 3 To create the table, click **Show Create Table.**

The right side of the browser displays an SQL create table statement for Microsoft SQL Server. The table name is the name that are specified in the Table Name box. The column names are the attributes that are specified in the Logged Attributes list.

Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

Step 4 Using the information in the generated SQL, create a table in your relational database for this ODBC log.

Note For ODBC logging to work, the table name and the column names must match exactly the names in the generated SQL.

Step 5 Check the **Log to ODBC accounting report** check box, where *log* is the name of the ODBC log that you selected.

Step 6 Click **Submit**.

ACS begins sending logging data to the relational database table that is specified by using the system DSN that you configured.

Step 7 Repeat the previous steps for each ODBC log.

For additional information on configuring logs, see Logs and Reports chapter of the *User Guide for Cisco Secure ACS for Windows 4.0*.

Migrating to ACS Solution Engine

Migrating from ACS for Windows to ACS Solution Engine uses the backup and restore features. ACS for Windows produces backup files that are compatible with ACS Solution Engine, provided that both use the same version of ACS software.

Depending on what version of ACS for Windows you use and the operating system on which it runs, the migration process varies. For example, if ACS runs on Windows NT 4.0, the following procedure will advise you when it is necessary to upgrade to Windows 2000 Server. Because the use of the backup and restore features is only supported between ACSs of the same version, you must use ACS for Windows, version 4.0, to transfer data from ACS for Windows to ACS Solution Engine. ACS for Windows, version 4.0, supports Windows 2000 Server and Windows Server 2003; not Windows NT 4.0.

See the following procedure for more details.

Before You Begin

Before upgrading or transferring data, back up your original ACS and save the backup file in a location on a drive that is not local to the computer that is running ACS.

To migrate from a Windows version of ACS to ACS Solution Engine:

Step 1 Set up the appliance, following the steps in the *Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine*.

Step 2 Upgrade ACS for Windows to version 4.0. If you do not have a license for version 4.0, you can use the trial version, which is available at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

If you run ACS on Windows NT 4.0, upgrade to ACS version 3.0; then migrate to Windows 2000 Server before upgrading to ACS version 4.0. ACS version 4.0 does not support Windows NT 4.0 and ACS version 3.0 is the most recent version of ACS that supports Windows NT 4.0. For information about upgrading to ACS version 3.0 or about migrating to Windows 2000 Server, see *Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*. You can download the trial version of ACS version 3.0 at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

Note For information about the versions of ACS that we used to test the upgrade process, see the Release Notes. The most recent version of the Release Notes is on Cisco.com, at: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html

Step 3 In the HTML interface of ACS for Windows, version 4.0, use the ACS Backup feature to back up the database. For more information about the ACS Backup feature, see the *User Guide for Cisco Secure ACS for Windows* 4.0.

Step 4 Copy the backup file from the computer that is running ACS for Windows, version 4.0, to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS Solution Engine must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.

Step 5 In the HTML interface of ACS Solution Engine, use the ACS Restore feature to restore the database. For more information about restoring databases, see the *User Guide for Cisco Secure Access Control Server Solution Engine*, version 4.0.

The ACS Solution Engine contains the original configuration of the Windows version ACS from which you migrated.

Step 6 Continuing in the HTML interface of the ACS Solution Engine, verify the settings for **(Default)** entry in the Proxy Distribution Table are correct. Choose **Network Configuration** > **(Default)**, and ensure that the Forward To list contains the entry for the appliance.

Step 7 If you want to replace the computer that is running ACS for Windows with ACS Solution Engine, you must change the IP address of the appliance to that of the computer that is running ACS for Windows.

Note If you do not change the IP address of the ACS Solution Engine to the address of the computer that is running ACS for Windows, you must reconfigure all AAA clients to use the IP address of the ACS Solution Engine.

To change the IP address of the ACS Solution Engine:

a. Record the IP address of the computer that is running ACS for Windows.

b. Change the IP address of the computer that is running ACS with Windows to a different IP address.

c. Change the IP address of the ACS Solution Engine to the IP address previously used by the computer that is running ACS for Windows. This is the IP address that you recorded in a. For detailed steps, see *Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine*.

Uninstalling ACS

You can remove ACS software from the computer on which it is installed by using the Windows Control Panel feature, Add/Remove Programs. Of course, when you remove ACS, the AAA services that it provided are no longer available from the computer that ran it.

Note If you cannot use the Add/Remove Programs feature (which can occur when ACS has been installed improperly, removed improperly, or otherwise damaged), locate the **clean.exe** program on the ACS CD and run it on the computer that has the damaged installation of ACS. The **clean.exe** program thoroughly removes ACS.

Before You Begin

Close all applications or command windows that are accessing any directory in the ACS directory. The installation cannot succeed if another process is using the ACS directory or any of its subdirectories. For example, if Windows Explorer is displaying the contents of an ACS directory, installation fails.

To uninstall ACS:

Step 1 Using the local administrator account, log in to the computer from which you want to uninstall ACS.

Step 2 Choose **Start > Settings > Control Panel > Add/Remove Programs**.

Tip If the Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**. Then double-click **Add/Remove Programs**.

The Add/Remove Programs window appears.

Step 3 From the Currently installed programs list, select **Cisco Secure ACS v*x.x***, where *x.x* is the version of ACS that is installed on the computer.

Step 4 Click **Change/Remove**.

The Confirm File Deletion dialog box appears.

Step 5 Click **Yes**.

The uninstallation begins.

Step 6 A dialog box displays the message:

```
The Cisco Secure ACS Service is currently running.
If you still want to continue the uninstall, it will be
stopped for you.
```

Click **Continue**.

Note If you click **Abort Uninstall**, the uninstallation stops and ACS remains installed on the computer. If the uninstallation fails, locate the **clean.exe** program on the ACS CD and run it on the computer that has the damaged installation of ACS.

The uninstallation continues. ACS services stop.

Step 7 A dialog box displays the following message:

```
You might choose to keep the existing ACS internal database,
which will save time if you reinstall the software at a later date.
```

- To preserve the ACS internal database user and group data, click **Keep Database**. The user-group configuration is saved in the directory where ACS was installed.

Caution No other configuration is saved (only user and group data). Perform a backup first if you want to save other configuration data. See Back Up Data, page 1-5 or the backing up instructions in the *User Guide for Cisco Secure ACS for Windows 4.0*.

You are asked to enter a password. Use this password during the installation import step. Keep this password in a safe location for any future installation import phase or if technical support needs access to the database.

- If you do not want to preserve the ACS internal database, click **Delete Database**.

Caution If you choose **Delete Database** and you have not backed up the database, user and group data is lost.

Uninstallation ends.

Step 8 Click **OK**.

What To Do Next

After installation is complete, you have many options to deploy ACS in your network.

Refer to the *User Guide for Cisco Secure ACS for Windows 4.0* for the suggested deployment sequence and how to take advantage of the features of your ACS product in Deployment Considerations. You can also see the *User Guide for Cisco Secure ACS for Windows 4.0* for details about all administrative functions, such as backup and restore, certificate setup, and other important tasks.

Refer to the Release Notes for up-to-date information on Cisco.com.

Logging In and Out of the System

To access ACS:

Step 1 Open a web browser by using the uniform resource locator (URL) for the machine.

- http://*IP address*:2002
- http://*hostname*:2002

where *IP address* is the dotted decimal IP address of the computer that is running ACS and *hostname* is the hostname of the computer that is running ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer that is running the browser.

If ACS is configured to use SSL to protect administrative sessions, you can also access the HTML interface by specifying the HTTPS protocol in the URLs:

- https://*IP address*:2002
- https://*hostname*:2002

Step 2 In the ACS login page, enter a valid username and password in the login screen to log in, and click **Login**.

Step 3 To log off, click the **X** in the upper-right corner of the browser window. After the page refreshes, click **Logoff**.

For detailed information on logging in and accessing the HTML interface, see the *User Guide for Cisco Secure ACS or Windows 4.0*.

Viewing Software Version Information

ACS software version information appears on the initial login page in the lower half of the HTML interface. If you are using the HTML interface, you can return to the login page by clicking the **X** in the upper-right corner of the HTML interface. An example of the software version and a portion of the copyright information is:

```
Cisco Secure ACS
Release 4.0(1) Build xx
Copyright ©2005 Cisco Systems, Inc.
```

INDEX