



Installation Guide for Cisco Secure ACS for Windows 4.2

February 2008

Americas 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: 408 527-0883

Text Part Number: OL-14388-01

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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)



CONTENTS

Preface v

Audience	v
Organization	v
Conventions	v
Product Documentation	vi
Open Source License Acknowledgements	viii
OpenSSL/Open SSL Project	viii
License Issues	viii
Obtaining Documentation and Submitting a Service Request	x

Installing Cisco Secure ACS for Windows 1-1

Understanding Your ACS System	1-1
Preparing to Install or Upgrade ACS	1-2
System Requirements	1-2
Third Party Software Requirements	1-5
Network and Port Requirements	1-5
Backing Up Data Before Installation	1-6
Gathering Answers for the Installation Questions	1-6
Disabling NetBIOS	1-7
Installation and Upgrade Scenarios	1-7
Installing ACS for the First Time	1-11
Reinstalling or Upgrading ACS	1-15
Reinstalling or Upgrading an Existing Configuration	1-16
Reinstalling or Upgrading ACS without Data Preservation	1-18

Post-Installation Tasks 2-1

Windows Authentication Configuration	2-1
Configuring for Domain Controller Authentication	2-1
Configuring for Member Server Authentication	2-5
Configuring Local Security Policies	2-8
Configuring ACS Services	2-10
Disabling NetBIOS	2-12
ACS 3.x to 4.2 ODBC Logging Updates	2-12
Migrating to ACS Solution Engine	2-13

Uninstalling ACS	2-14
What To Do Next	2-16
Logging In and Out of the System	2-17
Viewing Software Version Information	2-17



Preface

This document will help you install and initially configure the Cisco Secure Access Control Server for Windows 4.2, hereafter referred to as ACS.

Audience

This guide describes how to install and initially configure the Cisco Secure ACS, hereafter referred to as ACS, for Windows and includes upgrade and migration information.

Organization

This document contains:

- [Chapter 1, “Installing Cisco Secure ACS for Windows”](#)—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	<i>italic</i> font
Displayed session and system information, paths and file names	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> 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
<i>Documentation Guide for Cisco Secure ACS Release 4.2</i>	<ul style="list-style-type: none"> Printed document with the product. PDF on the product CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
<i>User Guide for Cisco Secure Access Control Server 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. You can also access the user guide by clicking Online Documentation in the ACS navigation menu. The user guide PDF is available on this page by clicking View PDF. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Configuration Guide for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html
<i>Installation Guide for Cisco Secure ACS for Windows 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html
<i>Installation and User Guide for Cisco Secure ACS User Changeable Passwords 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucp42.html
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/rmag42.html
<i>Cisco Secure Access Control Server Troubleshooting Guide</i>	<p>On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACS_Troubleshooting.html</p>
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.2</i>	<ul style="list-style-type: none"> Shipped with product. PDF on the product CD-ROM. Printed document available by order (part number DOC-7817259). On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html
<i>Release Notes for Cisco Secure ACS 4.2</i>	On Cisco.com : http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help Help topics for all pages in the ACS HTML interface.	In the ACS HTML interface, online help appears in the right pane when you are configuring a feature.
Short help. Provides help topics for all pages in the ACS web interface.	Select an option from the ACS web interface; the help appears in the right pane.

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.
 The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Installing Cisco Secure ACS for Windows

This chapter provides information about installing, reinstalling, and upgrading to Cisco Secure Access Control Server Release 4.2 for Windows, hereafter referred to as ACS.

This chapter contains:

- [Understanding Your ACS System](#)
- [Preparing to Install or Upgrade ACS](#)
- [Installation and Upgrade Scenarios](#)
- [Installing ACS for the First Time](#)
- [Reinstalling or Upgrading ACS](#)

Understanding Your ACS System

You can use ACS network security software to authenticate users by controlling access to an Authentication, Authorization, and Accounting (AAA) client—any one of many network devices that you can configure to defer authentication and authorization of network users to a AAA server. ACS operates as a set of Windows-based services that controls the authentication, authorization, and accounting of user access to networks.

ACS operates on Windows 2000 server and Windows 2003 server. ACS can run on a domain controller or a member server. For information about supported operating systems, see [System Requirements](#), or the latest version of the Release Notes at:

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

ACS can also run on a Windows Server with Network Basic Input/Output System (NetBIOS) disabled.



Note

If you want to authenticate users with a Windows Security Account Manager user database or an Active Directory (AD) user database, additional Windows configuration is required after you install ACS. For more information, see [Windows Authentication Configuration](#).

For additional information about ACS, refer to the *User Guide for Cisco Secure Access Control Server 4.2*.

Preparing to Install or Upgrade ACS

The following sections describe actions to take before you install or upgrade ACS:

- [System Requirements](#)
- [Third Party Software Requirements](#)
- [Network and Port Requirements](#)
- [Backing Up Data Before Installation](#)
- [Gathering Answers for the Installation Questions](#)
- [Disabling NetBIOS](#)

**Note**

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

System Requirements

Your ACS server must meet certain minimum hardware and operating system requirements.

The following tables list these requirements:

- [ACS for Windows Server Requirements, Table 1-1](#)
- [ACS for Windows Web Client Requirements, Table 1-2](#)
- [ACS for Windows Server UCP Requirements, Table 1-3](#)

**Note**

ACS for Windows supports the multiprocessor feature on dual processor computers.

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

You can apply windows service packs 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.

Table 1-1 ACS for Windows Server Requirements

Component	Minimum Requirement
Hardware	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Windows Server 2000 (English version only) • Windows 2000 Advanced Server Service Pack 4 without features specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service installed (English version only) • Windows Server 2003 Service Pack 1, Enterprise Edition or Standard Edition (English version only) • Japanese Windows 2003 server, Service Pack 1 • Japanese Windows 2003 server, Service Pack 2, Enterprise Edition (or higher, if available 90 days prior to FCS). • Japanese Windows 2003 server, Service Pack 2, R2, Enterprise Edition (or higher, if available 90 days prior to FCS). • Japanese Windows 2003 server, Service Pack 2, Standard Edition (or higher, if available 90 days prior to FCS). • Japanese Windows 2003 server, Service Pack 2, R2, Standard Edition (or higher if available 90 days prior to FCS). • Windows Server 2003, R2, Standard Edition • Windows Server 2003, Service Pack 2 • Windows Server 2003, R2, Service Pack 2
File System	New Technology File System (NTFS)
Memory	1 Gigabyte, minimum
Virtual Memory	1 Gigabyte, minimum
Hard Drive Space	<p>At least 1 GB of free hard drive space, minimum</p> <p>Note The actual amount of hard drive space required depends on several factors, including log file growth, and replication or back up purposes.</p>

We also tested ACS 4.2 on the following VMWare platform:

- VMWare ESX server 3.0.0
- RAM—16.0 GB
- Processor—AMD Opteron Dual core
- HDD—300 GB

- Number of Virtual machines—4
- Guest operating system—Windows 2003 Standard Edition
- RAM for each guest operation system—3 GB

Table 1-2 ACS for Windows Web Client Requirements

Component	Minimum Requirement
Hardware/Software	IBM PC compatible computer with Pentium IV processor running: <ul style="list-style-type: none"> • 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 (English version only) • Windows Server 2003, R2, Standard Edition • Windows Server 2003, Service Pack 2 • Windows Server 2003, R2, Service Pack 2
Hard Drive Space	400 MB virtual memory
Memory	256 MB minimum
Browser	You must also install one of the following HTML browsers: <ul style="list-style-type: none"> • Microsoft Internet Explorer 6 Service Pack 1 and 5.5 for Windows—English and Japanese versions • Microsoft Internet Explorer 7 Service Pack 2 for Windows Server 2003 and Service Pack 2 for Windows XP • Mozilla Firefox 2.0 and 2.0.0.6 • Netscape Web Browser 7.0, 7.1, and 7.2 for Windows—English and Japanese versions¹
Java Run-time Environment (JRE)	<ul style="list-style-type: none"> • Sun JRE 1.4.2_04 • Sun JRE 1.4.2_16 • Sun JRE 5.0 Update 13 • Sun JRE 6.0 Update 3

1. Several known problems result from using Netscape Communicator with ACS. For more information, see the *Release Notes for Cisco Secure ACS for Windows 4.2* on Cisco.com.

Table 1-3 ACS for Windows Server UCP Requirements

Component	Minimum Requirement
User Changeable Password (UCP) Web Server	<ul style="list-style-type: none"> • Microsoft IIS 5.0 • 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 the Release Notes mention.

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 Terminal Access Controller Access Control System + (TACACS+) and Remote Access Dial-in User Service (RADIUS) support on Cisco IOS devices, AAA clients must run Cisco IOS Release 11.1 or later.
- You must configure non-Cisco IOS AAA clients with TACACS+, RADIUS, or both.
- Dial-in, Virtual Private Network (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](#).
- You must install a supported web browser 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
- You must enable all network cards in the computer that is running ACS. If you disable a network card, the wrong IP might be selected, and the installing of ACS may proceed slowly, due to delays caused by Microsoft CryptoAPI.

**Note**

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

- When authorizing network users, if you want ACS to use the Grant Dial-in Permission to User feature in Windows, you must check this check box in the Windows User Manager or AD Users and Computers for the applicable user accounts.

[Table 1-4](#) lists the ports on 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 Lightweight Directory Access Protocol (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 on*

Feature or 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

Backing Up Data Before Installation

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 on which ACS is running. For information about backing up ACS, see the *User Guide for Cisco Secure ACS 4.2*.

You can use a new back up and restore option in the ACS System Restore Setup page to back up and restore the ACS System Configuration and User and Group database, when upgrading from ACS version 4.1 to 4.2. This feature is applicable for both Windows and SE platforms of ACS.



Note

If you are upgrading ACS rather than reinstalling, the backups that you create cannot be used for the upgraded installation; they provide for recovery if you need to restore your previous installation of ACS. But, in ACS 4.2, you can restore the ACS 4.1.x configuration after installing ACS 4.2.

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

You do not need to perform the following procedure, if you are upgrading or reinstalling ACS and intend to keep the existing configuration and database. This procedure 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, in [Windows Authentication Configuration](#).
- Step 2** Confirm that:
- 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.
 - You installed Microsoft Internet Explorer 6.0 Service Pack 1 or Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0 or Netscape 7.02. or Netscape 8.x.
- 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.

Disabling NetBIOS

NetBIOS (NBT or NetBT) is an API that allows applications on different computers to communicate with each other over a LAN. NBT is a broadcast-based, non routable, insecure transport protocol and session-level interface that normally runs over TCP/IP. NetBT found its way into the early versions of Windows and still functions on many legacy machines like Windows 9x and Windows NT. These machines require NetBIOS to function properly on the network. However, since the evolution of Windows 2000, Domain Name Service (DNS) has become the default name-resolution method for windows-based networking. Although Windows 2000, Windows XP, and Windows Server 2003 provide the option of disabling NetBIOS over TCP/IP, many corporate networks are reluctant to do so because they still use legacy machines on their networks. ACS4.2 supports the Windows server with NetBIOS disabled. You must disable NetBT in Windows.

Installation and Upgrade Scenarios

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

ACS for Windows supports the following upgrade scenarios:

- **ACS 3.x to ACS 3.3.x**—You can upgrade ACS 3.2.x or 3.3.x (ACS 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2) to ACS 3.3.3 or 3.3.4 on Windows.
- **ACS 3.3.3 to 3.3.4**— You can upgrade ACS 3.3.3 to ACS 3.3.4 on Windows.
- **ACS 3.3.x to ACS 4.1.1.23 or ACS 4.1.1.24**— You can upgrade from ACS 3.3.x (ACS 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, or 3.3.4) to ACS 4.1.1.23 or ACS 4.1.1.24 on Windows.



Note

You cannot directly upgrade ACS 3.2.x or 3.3.x or 4.x to ACS 4.2. You must upgrade to ACS 4.1, backup the ACS 4.1 configuration and then upgrade to ACS 4.2.

- **ACS 4.0 to ACS 4.1.1.23 or ACS 4.1.1.24**— You can upgrade from ACS 4.0 to ACS 4.1.1.23 or ACS 4.1.1.24 on Windows.

**Note**

If you are upgrading from ACS 4.0 to ACS 4.1, you must install the CSCsh32888 patch on the 4.0 installation before upgrading to ACS 4.1.

- **ACS 4.1.1.23 or ACS 4.1.1.24 to ACS 4.1.3 or ACS 4.1.4**— You can upgrade from ACS 4.1.1.23, 4.1.1.24, to ACS 4.1.3 or 4.1.4 on Windows.
- **ACS 4.1 to ACS 4.2**— You can upgrade from ACS 4.1.1.23, 4.1.1.24, 4.1.2, 4.1.3 or 4.1.4 to ACS 4.2 on Windows.

[Table 1-5](#) lists the possible installation and upgrade scenarios. Determine which procedure applies to your situation.

**Note**

Before you perform any installation or upgrade procedure, we strongly recommend that you read [Preparing to Install or Upgrade ACS](#), 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	Installing ACS for the First Time
Reinstallation, <i>preserving</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration
Reinstallation, <i>overwriting</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation
Upgrade, <i>preserving</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration
Upgrade, <i>overwriting</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation

Depending on the ACS version you are upgrading from, there are different paths for upgrading to ACS 4.2. [Table 1-6](#) describes the various upgrade use cases that you can use to decide the appropriate upgrade path to follow.

Table 1-6 Upgrade Use Cases

Upgrade Path	Results
<p>Full Upgrade from versions Prior to 3.3.3 to 4.2</p> <p>To perform a full upgrade with data restore from:</p> <ol style="list-style-type: none"> ACS SW 3.3.x to ACS SW 3.3.4 <ol style="list-style-type: none"> Back up your ACS SW 3.3.x configuration. Use the ACS for Windows Overall Upgrade CD. From the CD use the ACS 3.3.4 Upgrade for Windows. <p>ACS SW 3.3.4 is installed.</p> <p>For detailed instructions on upgrading to ACS SW 3.3.3, refer <i>Release Notes for Cisco Secure Access Control Server for Windows 3.3</i> at: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p> ACS SW 3.3.4 to ACS SW 4.1.1.24 <ol style="list-style-type: none"> Back up your ACS SW 3.3.4 configuration. Use the ACS for Windows Overall Upgrade CD. From the CD use the 4.1.1.24 Upgrade for Windows. <p>ACS SW 4.1.1.24 is installed.</p> <p>For instructions on upgrading to ACS 3.3.3, refer <i>Release Notes for Cisco Secure Access Control Server for Windows 3.3</i> at: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p> ACS SW 4.1.1.24 to ACS SW 4.2 <p>There are two options to upgrade to ACS 4.2:</p> <ul style="list-style-type: none"> Do an upgrade to ACS 4.2. <ol style="list-style-type: none"> Back up your ACS SW 4.1.1.24 configuration. Use the ACS SW 4.2 Installation CD to upgrade to ACS SW 4.2. (To keep the 4.1 configuration, check the Backup Database option.) <p>ACS SW 4.2 is installed and includes the upgraded 4.1.1.24 configuration.</p> Do a fresh install of ACS 4.2 and restore the ACS 4.1 configuration. <ol style="list-style-type: none"> Back up the 4.1.1.24 configuration. Use the ACS 4.2 installation CD to do a fresh install of ACS 4.2. <p>ACS 4.2 is installed.</p> <ol style="list-style-type: none"> Restore the 4.1.1.24 configuration. <p>For instructions on upgrading to ACS SW 4.1.1.24, refer <i>Release Notes for Cisco Secure Access Control Server for Windows 4.1.1.24</i> at: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html.</p> 	<p>ACS SW 3.3.4 is installed.</p> <p>ACS SW 4.1.1.24 is installed.</p> <p>ACS SW 4.2 is installed.</p> <p>ACS SW 4.1.1.24 configuration is upgraded to ACS SW 4.2 configuration.</p>

[illegible]

Table 1-6 Upgrade Use Cases

Upgrade Path	Results
<p>Full Upgrade from version 4.0 to 4.2</p> <p>To perform a full upgrade with data restore from:</p> <ol style="list-style-type: none"> ACS SW 4.0 to ACS SW 4.1.1.24 <ol style="list-style-type: none"> Install the CSCsh32888 patch on the 4.0 installation. <p>Note If you are upgrading from ACS 4.0 to ACS 4.1, you must install the CSCsh32888 patch on the 4.0 installation before upgrading to ACS 4.1.</p> <ol style="list-style-type: none"> Back up your ACS SW 4.0 configuration. Use the ACS for Windows Overall Upgrade CD. From the CD use the ACS 4.1.1.24 Upgrade for Windows. <p>ACS SW 4.1.1.24 is installed.</p> <p>For instructions on upgrading to ACS SW 4.1.1.24, refer <i>Release Notes for Cisco Secure Access Control Server for Windows 4.1.1.24</i> at:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p> <ol style="list-style-type: none"> ACS SW 4.1.1.24 to ACS SW 4.2 <p>There are two options to upgrade to ACS 4.2:</p> <ul style="list-style-type: none"> Do an upgrade to ACS 4.2. <ol style="list-style-type: none"> Back up your ACS SW 4.1.1.24 configuration. Use the ACS SW 4.2 Installation CD to upgrade to ACS SW 4.2. (To keep the 4.1 configuration, check the Backup Database option.) <p>ACS SW 4.2 is installed and includes the upgraded 4.1.1.24 configuration.</p> Do a fresh install of ACS 4.2 and restore the ACS 4.1 configuration. <ol style="list-style-type: none"> Back up the 4.1.1.24 configuration. Use the ACS 4.2 installation CD to do a fresh install of ACS 4.2. <p>ACS 4.2 is installed.</p> <ol style="list-style-type: none"> Restore the 4.1.1.24 configuration. <p>For instructions on upgrading to ACS SW 4.1.1.24, refer <i>Release Notes for Cisco Secure Access Control Server for Windows 4.1.1.24</i> at:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html</p> 	<p>ACS SW 4.1.1.24 is installed.</p> <p>ACS SW 4.2 is installed.</p> <p>ACS SW 4.1.1.24 configuration is upgraded to ACS SW 4.2 configuration.</p>

Installing ACS for the First Time

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 [Preparing to Install or Upgrade ACS](#).

**Note**

We did not test, nor do we support, remote installations that you perform by using Windows Terminal Services or Remote Desktop (RDP). Do not install or upgrade over a remote connection using Terminal Services or RDP. We recommend that you disable Terminal Services and RDP while performing any installation or upgrade. We have tested Virtual Network Computing (VNC) successfully.

To install ACS:

-
- Step 1** Using a local administrator account, log in to the computer on which you want to install ACS.
- Step 2** Insert the ACS CD into a CD-ROM drive on the computer.
- 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.
- If the CD-ROM drive supports the Windows **autorun** feature, the ACS for Windows dialog box appears; otherwise, run *Setup.exe*, which resides in the root directory of the ACS CD.
- Step 3** In the Cisco Secure ACS for Windows dialog box, click **Install**.
- 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 you must install the required service pack after the installation is complete; otherwise, ACS may not function reliably.
- The Cisco Secure ACS v4.2 Setup dialog box displays the software license agreement.
- Step 4** If you read and accept the software license agreement, click **ACCEPT**.
- The Welcome dialog box displays information about the setup program.
- Step 5** Read the information in the Welcome dialog box and click **Next**.
- The IMPORTANT NOTICE dialog box displays information about the processes running on your computer which may affect some ACS operations.
- Step 6** Read the information in the IMPORTANT NOTICE dialog box and click **Next**.
- The Before You Begin dialog box appears.
- Step 7** Once you complete the items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions](#).
- If you did not complete 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 [Preparing to Install or Upgrade ACS](#).
- After you click **Next**, the Choose Destination Location dialog box appears.
- Step 8** To change the installation location, enter the new path name or click the **Browse** button to choose the drive and path where the setup program installs ACS.
- The installation must reside on a drive that is local to the computer. If you specified a folder that does not exist, click **Yes** to confirm the creation of the folder.

**Note**

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

Step 9 Click **Next**.

The Authentication Database Configuration dialog box appears.

Step 10 Choose an option. To authenticate users with:

- The ACS internal database only, check **Check the ACS Internal database only**.
- A Windows Security Access Manager (SAM) user database or AD user database in addition to the ACS internal database, check **Also check the Windows User Database**.

The **Yes, refer to “Grant dial-in permission to user”** check box is enabled when you select the **Also check the Windows User Database** option. This option applies to all forms of access that ACS controls; not just dial-in access. For example, a user who accesses your network through a VPN tunnel is not dialing in to a network access server; however, if you check **Yes, refer to “Grant dial-in permission to user”** check box, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

If you want to grant access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check **Yes, refer to “Grant dial-in permission to user”** check box.

**Note**

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

Step 11 Click **Next**.

The setup program installs ACS and updates its configuration.

The Advanced Options dialog box appears.

Step 12 Choose the features that you want to enable.

These features are not enabled by default; they appear in the ACS web interface only if you enable them. To view the web interface:

- In the navigation bar, click **Interface Configuration**.
- Click **Advanced Options**.

The web interface appears.

For more information about these features, see the *User Guide for Cisco Secure ACS 4.2*.

**Note**

After installation, you can enable or disable advanced features on the Advanced Options page in the Interface Configuration section.

Step 13 Click **Next**.

The Active Service Monitoring dialog box appears.

Step 14 Choose service monitoring features:

- If you want ACS to monitor user authentication services, check **Enable Login Monitoring**. From the **Script to execute** list, choose the option that you want applied in the event of authentication service failure. The options are:

- **No Remedial Action**—ACS does not run a script. 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.
- If you want ACS to send an e-mail message when service monitoring detects an event, check the **Enable Mail Notifications** checkbox. The SMTP mail server and Mail account to notify fields are enabled. You must enter the following information:
 - **SMTP mail server** - Name and domain of the mail server that is sending the notification.
 - **Mail account to notify**- The e-mail address of the intended recipient.

**Note**

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

Step 15 Click **Next**.

The Cisco Secure ACS Service Initiation dialog box appears.

Step 16 You must enter a password and for database encryption. The password should be at least 8 characters long and should contain characters and numbers. There are no invalid characters.

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

Step 17 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. The check boxes are:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not check this check box, the ACS web 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 web 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**.

The ACS service installation starts. The Setup Complete dialog box displays information about the ACS web interface.

Step 20 Click **Finish**.

The setup program exits. If, in [Step 17](#), you chose the options to view the web interface or *README.TXT* file, those options become effective now.

Step 21 If you did not choose the options in [Step 17](#). To:

- Start ACS services, reboot the computer, or type **net start csadmin** at a DOS prompt.
- Access the ACS web interface, use the ACS Admin desktop icon, or use this URL in a supported web browser:

http://127.0.0.1:2002

http://localhost:2002



Note For more information on supported web browsers see [Browser](#)



Note During installation a setup log text file, *acssetup.log*, is created in the C: drive. This log records each stage of the installation process that is completed, and can be used for troubleshooting.

What to Do Next

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 [Windows Authentication Configuration](#).

You can also disable NetBIOS on Windows Server since ACS can support Windows Server with NetBIOS disabled.

Reinstalling or Upgrading ACS

You can reinstall ACS over the same version that is already installed. This procedure is also known as overinstalling ACS. You can also upgrade to ACS 4.2 from previous versions of ACS.

You can upgrade and reinstall ACS with the existing configuration and database information, or without preserving the data from the existing installation.

You can back up and restore the ACS system configuration and user and group database, when upgrading from ACS version 4.1 to 4.2. This feature is applicable for the Windows and SE platforms of ACS.

The upgrade process to ACS 4.2 transforms the data from ACS 4.1 to conform to the data structures and values in ACS 4.2.



Note You cannot directly upgrade from ACS 4.1 to ACS 4.2, you must first upgrade to ACS 4.1, and then upgrade to ACS 4.2. Before upgrading from ACS 4.0 to ACS 4.1, you must install the CSCsh32888 patch on the 4.0 installation and then upgrade to ACS 4.1.

The new ACS 4.2 attributes are set to the default values, which do not affect the existing configuration, except for:

- The timestamps for Administrator passwords are reset to the time of the upgrade.
- MAC addresses that reside in the ACS internal database are converted to a single hexadecimal format. If the database contained multiple representations of the same MAC address, the redundant MAC addresses that the conversion creates are removed.

**Note**

We did not test, nor do we support remote installations that you perform by using Windows Terminal Services or RDP. Do not install or upgrade over a remote connection using Terminal Services or RDP. We recommend that you disable Terminal Services and RDP while performing any installation or upgrade. VNC has been tested successfully.

For upgrading or reinstalling ACS, see:

- [Reinstalling or Upgrading an Existing Configuration](#)
- [Reinstalling or Upgrading ACS without Data Preservation](#)

If you are installing ACS for the first time, see [Installing ACS for the First Time](#).

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.

Before You Begin

For information about what you must complete before reinstalling or upgrading ACS, see [Preparing to Install or Upgrade ACS](#).

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.

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.
- Step 2** Insert the ACS CD into a CD-ROM drive on the computer.
- 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.
- If the CD-ROM drive supports the Windows **autorun** feature, the Cisco Secure ACS for Windows dialog box appears; otherwise, run *setup.exe*, which resides in the root directory of the ACS CD.
- Step 3** In the Cisco Secure ACS for Windows Server dialog box, click **Install**.
- 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 you must apply the required service pack after the installation is complete; otherwise, ACS may not function reliably.
- An informational dialog box displays some details about Windows authentication.
- Step 4** Click **OK**.
- The Cisco Secure ACS Setup dialog box displays the software license agreement.
- Step 5** If you read and accept the software license agreement, click **ACCEPT**.
- The Welcome dialog box displays basic information about the setup program.
- Step 6** Read the information in the Welcome dialog box, click **Next**.

The IMPORTANT NOTICE dialog box displays information about the processes running on your computer which may affect some ACS operations.

Step 7 Read the information in the IMPORTANT NOTICE dialog box and click **Next**.

The Before You Begin dialog box appears.

Step 8 Once you complete the items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions](#).

If you did not complete 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 [Preparing to Install or Upgrade ACS](#).

After you click **Next**, the Previous Installation Location dialog box appears.

Check **Yes, keep the existing configuration**.



Note

You can back up and restore the ACS system configuration and database by checking this option. This is applicable to the Windows and SE platforms of ACS.



Caution

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 9 Click **Next**.

The Choose Destination Location dialog box appears.

Step 10 To change the installation location, enter the new path name or click the **Browse** button to choose the drive and path where the setup program installs ACS.

The installation location must reside on a drive that is local to the computer. If you specified a folder that does not exist, click **Yes** to confirm the creation of the folder.



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.

Step 11 Click **Next**.

The Cisco Secure ACS Service Initiation dialog box appears.

Step 12 You must enter a password and for database encryption. The password should be at least 8 characters long and should contain characters and numbers. There are no invalid characters.

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

Step 13 Click **Next**.

The Cisco Secure ACS Service Initiation dialog box appears.

Step 14 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. The check boxes are:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not check this check box, the web interface is not available. You can start the ACS service later.
- **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation**—Opens the ACS web 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 15 Click **Next**.

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

Step 16 Click **Finish**.

The setup program exits. If, in [Step 14](#), you chose the options to view the web interface or *README.TXT* file, those options become effective now.

If you failed to meet the minimum system requirements, a message might appear warning you to address the problem. Click **OK** to continue and resolve the problem where possible.

Step 17 If you did not choose the options in [Step 14](#), to:

- Start ACS services, reboot the computer, or type **net start csadmin** at a DOS prompt.
- Access the ACS web interface, use the ACS Admin desktop icon, or use this URL in a supported web browser:

http://127.0.0.1:2002

http://localhost:2002



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

What to Do Next

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 [Windows Authentication Configuration](#) describes.

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.



Caution

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

Before You Begin

For information about what you must complete before reinstalling or upgrading ACS, see [Preparing to Install or Upgrade ACS](#).

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 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.
- 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.
- 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.
- If the CD-ROM drive supports the Windows **autorun** feature, the Cisco Secure ACS for Windows dialog box appears; otherwise, run *setup.exe*, which resides in the root directory of the ACS CD.
- Step 3** In the Cisco Secure ACS for Windows Server dialog box, click **Install**.
- 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 informational dialog box displays some details about Windows authentication.
- Step 4** Click **OK**.
- The Cisco Secure ACS Setup dialog box displays the software license agreement.
- Step 5** If you read and accept the software license agreement, click **ACCEPT**.
- The Welcome dialog box displays basic information about the setup program.
- Step 6** Read the information in the Welcome dialog box and click **Next**.
- The IMPORTANT NOTICE dialog box displays information about the processes running on your computer which may affect some ACS operations.
- Step 7** Read the information in the IMPORTANT NOTICE dialog box and click **Next**.
- The Before You Begin dialog box appears.
- Step 8** Once you complete the items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions](#).
- If you did not complete 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 [Preparing to Install or Upgrade ACS](#).
- After you click **Next**, the Previous Installation Location dialog box appears.
- Step 9** Leave the check box unchecked and click **Next**.
- If ACS services are running, the Cisco Secure ACS Uninstall dialog box appears. Click **Continue**.
- The setup program removes the previous installation of ACS.

The Choose Destination Location dialog box appears.

- Step 10** To change the installation location, enter the new path name or click the **Browse** button to choose the drive and path where the setup program installs ACS.

The installation location must reside on a drive that is local to the computer. If you specified a folder that does not exist, click **Yes** to confirm the creation of the folder.



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.

- Step 11** Click **Next**.

The Authentication Database Configuration dialog box appears.

- Step 12** Choose an option. To authenticate users with:

- The ACS internal database only, check **Check the Cisco Secure ACS database only**.
- A Windows SAM user database or AD user database in addition to the ACS internal database, click **Also check the Windows User Database**.

The **Yes, refer to “Grant dial-in permission to user” check box** is enabled when you select the **Also check the Windows User Database** option. This option applies to all forms of access that ACS controls; not just dial-in access. For example, a user who accesses your network through a VPN tunnel is not dialing in to a network access server; however, if you check **Yes, refer to “Grant dial-in permission to user” check box**, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

If you want to grant access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check **Yes, refer to “Grant dial-in permission to user” check box**.



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

- 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 4.2*.



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

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

- Step 14** Click **Next**.

The Active Service Monitoring dialog box appears.

- Step 15** Choose service monitoring features:

- If you want ACS to monitor user authentication services, check **Enable Login Monitoring**. From the **Script to execute** list, choose the option that you want applied in the event of authentication service failure. The options are:

- **No Remedial Action**—ACS does not run a script. 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.
- If you want ACS to send an e-mail message when service monitoring detects an event, check the **Enable Mail Notifications** checkbox. The SMTP mail server and Mail account to notify fields are enabled. You must enter the following information:
 - **SMTP mail server** - Name and domain of the mail server that is sending the notification.
 - **Mail account to notify**- The e-mail address of the intended recipient.

**Note**

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

Step 16 Click **Next**.

The Cisco Secure ACS Service Initiation dialog box appears.

Step 17 You must enter a password and for database encryption. The password should be at least 8 characters long and should contain characters and numbers. There are no invalid characters.

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

Step 18 Click **Next**.

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

Step 19 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. The check boxes are:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not check this check box, the ACS web 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 web 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 20 Click **Next**.

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

Step 21 Click **Finish**.

The setup program exits. If, in [Step 19](#), you chose the options to view the web interface or *README.TXT* file, those options become effective now.

On the computer that is running ACS, to access the ACS web interface click the **ACS Admin** desktop icon or enter this URL in a supported web browser:

http://127.0.0.1:2002

http://localhost:2002

**Note**

The ACS web interface is available only if you chose to start ACS services in [Step 19](#). If you did not, to make the web interface available, you can reboot the computer; or, at a DOS prompt type **net start csadmin**.

**Note**

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

What to Do Next

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 [Windows Authentication Configuration](#) describes.



CHAPTER 2

Post-Installation Tasks

This section provides the post-installation tasks for Cisco Secure Access Control Server Release 4.2 for Windows, hereafter referred to as ACS.

- [Windows Authentication Configuration](#)
- [Disabling NetBIOS](#)
- [ACS 3.x to 4.2 ODBC Logging Updates](#)
- [Migrating to ACS Solution Engine](#)
- [Uninstalling ACS](#)
- [What To Do Next](#)

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.

These topics describe configuration required for Windows authentication:

- [Configuring for Domain Controller Authentication](#)
- [Configuring for Member Server Authentication](#)
- [Configuring Local Security Policies](#)
- [Configuring ACS Services](#)

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. To configure domain controller authentication:

Step 1 Add the *CISCO* workstation.

To meet 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 status of the Server and Net Logon services.

The ACS authentication service depends on the Server and Net Logon services, which are standard services in Microsoft Windows. On the computer that is running ACS, verify that these services are running and that the Startup Type is set to *Automatic*.



Tip

To configure the server service and the Net Logon 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 NT LAN Manager (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 LM, NTLM version 1 or NTLM version 2 protocols. LM is the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but should ensure that:

- Regardless of the version of NTLM that you use, you must configure the LM Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LM 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.
- In addition to the previous setting, if you want to use NTLM version 2, you must also ensure that each:
 - Windows 2000 domain controller that performs user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 on the Microsoft website.
 - or
 - Domain controller that performs user authentication has the Windows 2003 Service Pack 1. This version does not require any patch.

Step 4 Create a user account.

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 subsequent steps in this procedure explain).

- 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 result from failed ACS authentication attempts.

To the domain administrator account that you create, grant Read all properties permission for all AD folders that contain users who require ACS authentication. To grant permission for AD folders, access AD through 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 upgraded or reinstalled ACS and you completed this step for the previous installation, this step 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](#).

Step 6

Configure the 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 whom you added to the security policies in the preceding step.

For more information, see [Configuring ACS Services](#).

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 that contains 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 Windows Internet Name Service (**WINS**) tab.
- c. Configure NetBIOS as applicable.

For more information, see the Microsoft website for appropriate documentation about installing WINS on Windows.

**Note**

ACS can also support Windows Server with NetBIOS disabled.

Step 8 Ensure DNS operation.

Especially for authentication of users in AD, ACS requires DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an event-notification e-mail for Service Management. 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 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. Click the DNS tab.
- c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see the Microsoft website for appropriate documentation about configuring TCP/IP to use DNS on Windows 2000 and Windows 2003.

Step 10 Configure WINS.

You must enable WINS on your network if ACS must authenticate users who belong 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 the *LMHOSTS* file.**Note**

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

As a final means of ensuring communication with other domain controllers, on the domain controller that is running ACS, configure an *LMHOSTS* file to include entries for each domain controller of a trusted or child domain that contains 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. The appropriate [LMHOSTS File](#) on the Microsoft website.
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.

To configure for member server authentication:

Step 1 Verify domain membership.

One common configuration error that prevents Windows authentication is the 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 the *CISCO* workstation.

To meet 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 Microsoft Windows server service. 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 LM, NTLM version 1, or NTLM version 2 protocols. LM is the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but should ensure that:

- a. Regardless of the version of NTLM that you use, you must configure the LM Authentication level settings. In the applicable Windows security policy editor:
 - i. Choose **Local Policies > Security Options**
 - ii. Locate the **LM Authentication Level policy** and set the policy.
 - iii. 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 wish to use NTLM version 2 you must also ensure that each:
 - Windows 2000 domain controller that performs user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 on the Microsoft website.
 - or
 - Domain controller that performs user authentication has Windows 2003 Service Pack 1. This version does not require any patch.

Step 5

Create a user account.

**Tip**

If you upgraded or reinstalled ACS and you completed this previous step, this step 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 an administrator account that you can use to run ACS services (as subsequent steps in this procedure explain).

- 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 result from failed ACS authentication attempts.

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

**Tip**

To access the security properties of an AD folder of users, right-click the folder, select **Properties**, and choose 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](#).

Step 7 Configure the services.

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

For more information, see [Configuring ACS Services](#).

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.
- Domain controller of the domain that contains ACS.
- Domain controllers of trusted domains that contain users that ACS must authenticate.
- Domain controllers of child domains that contain 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 the Microsoft website for appropriate documentation about installing WINS on Windows Server 2000 and Windows Server 2003.

Step 9 Ensure DNS operation.

Especially for authentication of users in AD, ACS requires DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an event-notification e-mail for Service Management. 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 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. Click the DNS tab.
- c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see the Microsoft website for appropriate documentation about configuring TCP/IP to use DNS on Windows 2000 and Windows 2003.

Step 11 Configure WINS.

If ACS must authenticate users who belong to a trusted or child domain and 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 the *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 an *LMHOSTS* file to include entries for each domain controller that contains users that ACS must authenticate. This entry should also include 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:

- The appropriate [LMHOSTS File](#) on the Microsoft website.
- 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.
- Domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account through which you run ACS. For full configuration requirements, see the applicable procedure: [Configuring for Member Server Authentication](#), or [Configuring for Domain Controller Authentication](#).

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 the 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 *CORPORATEACSuser*.

- d. Click **Check Names**.

The Enter Network Password dialog box appears.

- e. In:

- **Connect as**—Type a domain-qualified username. The username must exist in the domain in **c**. For example, if the domain 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 in **c** appears in the settings associated with the policy that you configured.

- h. Verify that the username that is 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 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 user account that you specified 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.
- Domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account through which you 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](#), or [Configuring for Domain Controller Authentication](#).

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 an ACS service and, from the shortcut menu, choose **Properties**. The Computer Browser Properties (Local Computer) dialog box appears.
- b. Click 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 run by using the privileges of the user account.

Step 5 To restart all ACS services:

- a. Log in to the ACS web interface.
- b. Click **System Configuration, Service Control**, and **Restart**.

With the exception of **CSAdmin**, ACS services restart.

- c. Wait until ACS finishes restarting all 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.

Disabling NetBIOS

NetBIOS (NBT or NetBT) is an API that allows applications on different computers to communicate with each other over a LAN. NBT is a broadcast-based, non routable, insecure transport protocol and session-level interface that normally runs over TCP/IP. NetBT found its way into the early versions of Windows and still functions on many legacy machines like Windows 9x and Windows NT. These machines require NetBIOS to function properly on the network. However, since the evolution of Windows 2000, Domain Name Service (DNS) has become the default name-resolution method for windows-based networking. Although Windows 2000, Windows XP, and Windows Server 2003 provide the option of disabling NetBIOS over TCP/IP, many corporate networks are reluctant to do so because they still use legacy machines on their networks. ACS4.2 supports the Windows server with NetBIOS disabled. You must disable NetBT in Windows.

ACS 3.x to 4.2 ODBC Logging Updates

If you used ACS 3.x ODBC logging and upgraded to ACS 4.2 while preserving your data, you must update the ODBC tables so that the Structured Query Language (SQL) tables continue to work.

From ACS 4.0 and later versions, changes to the SQL database present all the ODBC fields as strings rather than numbers. Field types have 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 chose.

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

The right side of the browser displays a SQL create table statement for Microsoft SQL Server. The table name is the name in the Table Name box. The column names are the attributes 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 exactly match 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 chose.

Step 6 Click **Submit**.

Through the system DSN that you configured, ACS begins sending logging data to the relational database table.

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 4.2*.

Migrating to ACS Solution Engine

When you migrate from ACS for Windows to ACS Solution Engine (ACS SE), you must use the Backup and Restore features in ACS. ACS for Windows produces backup files that are compatible with ACS SE, if use the same version of ACS software.

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 on which ACS is running.

To migrate from ACS Windows version of ACS to ACS SE:

Step 1 Set up the appliance, following the steps in the *Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine 4.2*.

Step 2 Upgrade ACS for Windows to version 4.2. If you do not have a license for version 4.2, you can use the trial version, which is available 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 web interface of ACS for Windows, 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 Access Control Server 4.2*.

**Note**

You can perform a Backup and Restore of the ACS system configuration and user and group database when upgrading from ACS version 4.1 to 4.2. This feature is applicable for the Windows and SE platforms of ACS. Refer to the *User Guide for Cisco Secure Access Control Server Release 4.2* for more information.

**Note**

The *cert7.db* file is not backed up. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery. When you migrate from an ACS server to ACS appliance, move the *cert7.db* to an FTP server and download according to the normal provisioning instructions.

- Step 4** Copy the backup file from the computer that is running ACS for Windows to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS SE 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 web interface of ACS SE, 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 4.2*. The ACS SE contains the original configuration of the Windows version of ACS from which you migrated.
- Step 6** Continuing in the web interface of the ACS SE:
- 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 SE, you must change the appliance's IP address to that of the computer that is running ACS for Windows.

**Note**

If you do not change the IP address of the ACS SE 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 SE.

To change the IP address of the ACS SE:

- Record the IP address of the computer that is running ACS for Windows.
- Change the IP address of the computer that is running ACS with Windows to a different IP address.
- Change the IP address of the ACS SE 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 4.2*.

Uninstalling ACS

To remove ACS software from the computer on which it is installed, use the Add/Remove Programs feature from the Windows control panel. When you remove ACS, the AAA services that it provided are no longer available from the computer that ran it.

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**.
- The Add/Remove Programs window appears.
- Step 3** From the **Currently installed programs** list, choose **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.



Note You can also access this dialog box by choosing **Start > Programs > CiscoSecure ACS v4.2 > Uninstall**.

- Step 5** Click **Yes**.
- The process of 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 installation CD and run it on the computer that has the damaged installation of ACS.

The uninstallation process 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**. This action saves the user-group configuration in the directory where ACS was installed.



Note You can Backup and Restore the ACS system configuration and user and group database when upgrading from ACS version 4.1 to 4.2.



Caution No other configuration is saved (only user and group data). Perform a backup first if you want to save other configuration data. See the backup instructions [Backing Up Data Before Installation](#) in the *User Guide for Cisco Secure ACS 4.2*.

You are asked to enter a password. Use this password during the installation import step. Make a note of this password 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, you will lose user and group data.

The uninstallation process ends.

Step 8

Click **OK**.

Troubleshooting Uninstallation Problems

Problem You cannot use the Add/Remove Programs feature (which can occur when ACS has been installed improperly, removed improperly, or otherwise damaged); or, uninstallation fails.

Solution Locate the *clean.exe* program on the ACS CD and run it on the computer on which the damaged installation of ACS resides. The *clean.exe* program thoroughly removes ACS.

Problem The ACS uninstallation fails to delete the files *rad_mon.dll* and *tac_mon.dll* in */bin* because they are in use.

Solution Restart your machine and delete the files. (These two processes do not start up automatically.) If you do not remove these files and they remain locked, you will not be able to reinstall ACS.

What To Do Next

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

Refer to the *Configuration Guide for Cisco Secure ACS 4.2* for suggested deployment sequences. Refer to the *User Guide for Cisco Secure ACS 4.2* 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 web 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 web interface, see the *User Guide for Cisco Secure ACS 4.2*.

Viewing Software Version Information

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

```
Cisco Secure ACS
Release 4.2(1) Build xx
Copyright ©2006 Cisco Systems, Inc.
```




INDEX

A

AAA clients
 requirements [1-7](#)
Apache web server, for UCP [1-4](#)

B

backing up
 See also User Guide [1-6](#)
browser
 HTML supported [1-4](#)
 requirements
 See Web client requirements [1-4](#)

C

cautions
 significance of [1-vi](#)
Cisco IOS release [1-5, 1-7](#)
clean.exe [2-16](#)
conventions [1-v](#)

D

database password [1-7](#)
documentation
 conventions [1-v](#)
 objectives [1-v](#)
domain controller
 configuring Windows [2-1](#)
 installation option [1-7](#)

F

first time installation [1-11](#)

H

hard drive space [1-3](#)
 system [1-3](#)
 web client [1-4](#)
hardware requirements [1-3](#)

I

installation
 backing up before [1-6](#)
 new [1-11](#)
 questions to answer before [1-6](#)
Internet Explorer browser [1-4](#)

J

Java run-time environment [1-4](#)

L

local security setting, configuring in Windows [2-8](#)
logging, ODBC [2-12](#)
logging in or out [2-17](#)

M

member server
 configuring Windows [2-5](#)

- installation option [1-7](#)
- memory
 - system [1-3](#)
 - web client [1-4](#)
- Microsoft IIS, for UCP [1-4](#)
- migrating to solution engine [2-13](#)

N

- Netscape browser [1-4](#)
- net start admin [1-22](#)
- network card, requirements [1-5](#)
- network requirements [1-5](#)
- NTFS [1-3](#)
- NTLM [2-2, 2-6](#)

O

- ODBC logging updates [2-12](#)
- operating system
 - not supported DataCenter Server [1-2](#)
 - server [1-3](#)
 - web client requirements [1-4](#)

P

- password
 - database access [1-7](#)
- ports
 - ACS listens to [1-6](#)
 - network requirements [1-5](#)
- post-installation tasks [2-16](#)

R

- rebooting [1-22](#)
- reinstalling
 - and preserving configuration [1-16](#)

- backing up before [1-6](#)
 - without preserving configuration [1-18](#)
- removing ACS software
 - using Add/Remove Programs [2-14](#)
 - using clean.exe [2-15](#)
- requirements
 - network [1-5](#)
 - server [1-3](#)
 - web client [1-4](#)

S

- server requirements [1-3](#)
- services, configuring in Windows [2-10](#)
- software version information [2-17](#)
- solution engine, migrating to [2-13](#)
- SQL table changes [2-12](#)
- system requirements [1-2](#)
 - file system [1-3](#)
 - hard drive space [1-3](#)
 - hardware [1-3](#)
 - memory [1-3](#)
 - operating system, server [1-3](#)
 - server [1-3](#)
 - virtual memory [1-3](#)
 - see web client requirements

T

- third-party software, requirements [1-5](#)
 - see also Release Notes

U

- uninstalling ACS [2-14](#)
 - troubleshooting problems [2-16](#)
 - using clean.exe [2-16](#)
- upgrading

- and preserving configuration [1-16](#)
- backing up before [1-6](#)
- without preserving configuration [1-18](#)
- user changeable passwords, requirements [1-4](#)

V

- version information [2-17](#)
- virtual memory [1-3](#)
- VMWare [1-3](#)

W

- warnings
 - significance of [1-vi](#)
- web client requirements
 - hard drive space [1-4](#)
 - hardware [1-4](#)
 - memory [1-4](#)
 - software [1-4](#)
- what to do next [2-16](#)
- Windows authentication
 - additional steps [2-1](#)
 - domain controller [2-1](#)
 - member server [2-5](#)

