



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 <p>Note ACS 4.2 for Windows does not support 64-bit operating systems.</p>
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"> • Windows 2000 Server, or Advanced Server, Service Pack 4 • Windows 2000, Service Pack 4 • Windows XP, Service Pack 2 • 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 • Windows Vista, Service Pack 1
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"> 1. ACS SW 3.3.x to ACS SW 3.3.4 <ol style="list-style-type: none"> a. Back up your ACS SW 3.3.x configuration. b. Use the ACS for Windows Overall Upgrade CD. c. From the CD use the ACS 3.3.4 Upgrade for Windows. ACS SW 3.3.4 is installed. <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> 2. ACS SW 3.3.4 to ACS SW 4.1.1.24 <ol style="list-style-type: none"> a. Back up your ACS SW 3.3.4 configuration. b. Use the ACS for Windows Overall Upgrade CD. c. From the CD use the 4.1.1.24 Upgrade for Windows. ACS SW 4.1.1.24 is installed. <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> 3. 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"> a. Back up your ACS SW 4.1.1.24 configuration. b. 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.) ACS SW 4.2 is installed and includes the upgraded 4.1.1.24 configuration. • Do a fresh install of ACS 4.2 and restore the ACS 4.1 configuration. <ol style="list-style-type: none"> a. Back up the 4.1.1.24 configuration. b. Use the ACS 4.2 installation CD to do a fresh install of ACS 4.2. ACS 4.2 is installed. c. 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>

Table 1-6 Upgrade Use Cases

Upgrade Path	Results
<p>Full Upgrade from versions 3.3.3 or 3.3.4 to 4.2</p> <p>To perform a full upgrade with data restore from:</p> <ol style="list-style-type: none"> 1. ACS SW 3.3.3 or 3.3.4 to ACS SW 4.2 <ol style="list-style-type: none"> a. Back up your ACS SW 3.3.3 or 3.3.4 configuration. b. Use the ACS SW 4.2 Installation CD. c. From the CD use the ACS 4.1.1.24 Upgrade for Windows. ACS SW 4.1.1.24 is installed. <p>For instructions on upgrading to ACS 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> 2. 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"> a. Back up your ACS SW 4.1.1.24 configuration. b. 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.) ACS SW 4.2 is installed and includes the upgraded 4.1.1.24 configuration. • Do a fresh install of ACS 4.2 and restore the ACS 4.1 configuration. <ol style="list-style-type: none"> a. Back up the 4.1.1.24 configuration. b. Use the ACS 4.2 installation CD to do a fresh install of ACS 4.2. ACS 4.2 is installed. c. 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 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>

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"> 1. ACS SW 4.0 to ACS SW 4.1.1.24 <ol style="list-style-type: none"> a. 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"> b. Back up your ACS SW 4.0 configuration. c. Use the ACS for Windows Overall Upgrade CD. d. 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>	<p>ACS SW 4.1.1.24 is installed.</p>
<ol style="list-style-type: none"> 2. 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"> a. Back up your ACS SW 4.1.1.24 configuration. b. 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"> a. Back up the 4.1.1.24 configuration. b. 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"> c. 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 4.2 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 4.0 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.