



CHAPTER 1

Installing Cisco Secure ACS for Windows

This chapter provides information about installing, reinstalling, and upgrading to Cisco Secure Access Control Server Release 4.1 for Windows, hereafter referred to as ACS.

This chapter contains:

- [Understanding Your ACS System, page 1-1](#)
- [Preparing to Install or Upgrade ACS, page 1-1](#)
- [Installation and Upgrade Scenarios, page 1-7](#)
- [Installing ACS for the First Time, page 1-7](#)
- [Reinstalling or Upgrading ACS, page 1-11](#)

Understanding Your ACS System

You can use ACS network security software to authenticate users by controlling access to a 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 services that control the authentication, authorization, and accounting of user access to networks.

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

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



Note

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

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

Preparing to Install or Upgrade ACS

These topics provide recommended actions that you should perform before you install or upgrade ACS:

- [System Requirements, page 1-2](#)
- [ACS Upgrade Requirements, page 1-4](#)

- [Third-Party Software Requirements, page 1-4](#)
- [Network and Port Requirements, page 1-5](#)
- [Backing Up Data Before Installation, page 1-6](#)
- [Gathering Answers for the Installation Questions, page 1-6](#)

**Note**

ACS will not install properly if 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 the details of these requirements:

- [ACS for Windows Server Requirements, Table 1-1 on page 1-3](#)
- [ACS for Windows Web Client Requirements, Table 1-2 on page 1-4](#)
- [ACS for Windows Server UCP Requirements, Table 1-3 on page 1-4](#)



**Note**

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

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

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

Table 1-1 ACS for Windows Server Requirements

Component	Minimum Requirement
Hardware	<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 2000 Server (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, Enterprise Edition or Standard Edition (Service Pack 1) • Japanese Windows Server 2003 (Service Pack 1) <p> Note ACS 4.1 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	At least 1 GB of free hard drive space, minimum <p> Note The actual amount of hard drive space required depends on several factors, including log file growth, and replication or backup purposes.</p>

ACS 4.1 was also tested on the following VMWare platform:

- VMWare ESX server 3.0.0
- RAM—16.0 GB
- Processor—AMD Opteron Dual core
- HDD—300 GB
- # 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)
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 version • Netscape Web Browser 7.0, 7.1, and 7.2 for Windows–English and Japanese version¹
Java Run-time Environment (JRE)	Sun JRE 1.4.2_04

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

Table 1-3 ACS for Windows Server UCP Requirements

Component	Minimum Requirement
User Changeable Password (UCP) Web Server	<ul style="list-style-type: none"> • Microsoft IIS 5.0 • Apache 1.3 web server

ACS Upgrade Requirements

ACS supports the following upgrade paths. These paths have been tested and are supported:

- Cisco Secure ACS for Windows, release 3.3.3 to ACS 4.1
- Cisco Secure ACS for Windows, release 4.0 to ACS 4.1
- For releases of ACS prior to ACS 3.3.3, you must first upgrade to ACS 3.3.3, then upgrade to ACS 4.1.

For information about upgrading from previous versions of ACS, see [Reinstalling or Upgrading ACS](#), page 1-11.

Third-Party Software Requirements

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

- Web browsers and Java virtual machines

- Novell Directory Server (NDS) clients
- Token-card clients

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

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

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

Network and Port Requirements

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

- For full TACACS+ and RADIUS support on Cisco IOS devices, AAA clients must run Cisco IOS Release 11.1 or later.
- Non-Cisco IOS AAA clients must be configured with TACACS+, RADIUS, or both.
- Dial-in, VPN, or wireless clients must be able to connect to the applicable AAA clients.
- The computer that is running ACS must be able to ping all AAA clients.
- Gateway devices between ACS and other network devices must permit communication over the ports needed to support the applicable feature or protocol. For information about ports to which ACS listens, see [Table 1-4](#).
- A supported web browser must be installed on the computer that is running ACS. For the most recent information about tested browsers, see the Release Notes, available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html
- All network cards in the computer that is running ACS must be enabled. If a network card is disabled, the wrong IP might be selected, and installing ACS may proceed slowly, due to delays caused by Microsoft CryptoAPI.



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

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

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

Table 1-4 Ports that ACS Listens To

Feature/Protocol	UDP or TCP	Ports
RADIUS authentication and authorization	UDP	1645, 1812
RADIUS accounting	UDP	1646, 1813
TACACS+	TCP	49

Table 1-4 Ports that ACS Listens To (continued)

Feature/Protocol	UDP or TCP	Ports
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*.


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.

Gathering Answers for the Installation Questions

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


Note

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

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

- Step 1** Determine whether the computer on which you will install ACS is a domain controller or a member server. If you want ACS to authenticate users with a Windows domain user database, after you install ACS, you must perform the additional Windows configuration, which is discussed in [Windows Authentication Configuration, page 2-1](#).
- Step 2** Confirm that these items are completed:
- End user clients can successfully connect to AAA clients.
 - This Windows Server can ping the AAA clients.

- Any Cisco IOS clients are running Cisco IOS release 11.1 or later.
- Microsoft Internet Explorer 6.0 Service Pack 1 or Netscape 7.02 is installed.

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

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.

[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, page 1-1](#), and perform the applicable tasks in that section.

Table 1-5 Installation and Upgrade Scenarios

If your installation scenario is a:	Refer to...
First-time installation	Installing ACS for the First Time, page 1-7
Reinstallation, <i>preserving</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration, page 1-11
Reinstallation, <i>overwriting</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation, page 1-13
Upgrade, <i>preserving</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading an Existing Configuration, page 1-11
Upgrade, <i>overwriting</i> the ACS internal database and ACS configuration	Reinstalling or Upgrading ACS without Data Preservation, page 1-13

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, page 1-1](#).

**Note**

Remote installations performed by using Windows Terminal Services or Remote Desktop (RDP) are not tested and are not supported. 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. Virtual Network Computing (VNC) has been tested 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*, located 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 the required service pack must be installed after the installation is complete; otherwise, ACS may not function reliably.
- The Cisco Secure ACS Setup dialog box displays the software license agreement.
- Step 4** Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.
- The Welcome dialog box displays basic information about the setup program.
- Step 5** After you have read the information in the Welcome dialog box, click **Next**.
- The Before You Begin dialog box appears.
- Step 6** If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions, page 1-6](#).
- If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see [Preparing to Install or Upgrade ACS, page 1-1](#).
- After you click **Next**, the Choose Destination Location dialog box appears.
- Step 7** To change the installation location, enter the new path name or click the **Browse** button to select the drive and path where the setup program installs ACS.
- The installation location must be 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 so, installation may appear to continue properly but will fail before it ends.
-
- Step 8** Click **Next**.
- The Authentication Database Configuration dialog box appears.
- Step 9** Choose an option for authentication users:

- To authenticate users with the ACS internal database only, check **Check the Cisco Secure ACS database only**.
- To authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory 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” setting** check box becomes available. This option applies to all forms of access that ACS controls; not just dial-in access. For example, a user accessing your network through a VPN tunnel is not dialing in to a network access server; however, if you check **Yes, refer to “Grant dial-in permission to user” setting**, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

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



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

Step 10 Click **Next**.

The setup program installs ACS and updates its configuration.

The Advanced Options dialog box appears.

Step 11 Choose the features that you want to enable.

These features are not enabled by default; they appear in the ACS HTML interface only if you enable them. For more information about these features, see the *User Guide for Cisco Secure ACS*.



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

Step 12 Click **Next**.

The Active Service Monitoring dialog box appears.

Step 13 Choose service monitoring features:

- If you want ACS to monitor user authentication services, check **Enable Log-in Monitoring**. From the **Script to execute** list, select the option that you want applied in the event of authentication service failure:
 - **No Remedial Action**—ACS does not run a script. 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 **Mail Notification**.



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

Step 14 Click **Next**.

The Database Encryption Password dialog box appears.

Step 15 Enter a password 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 the database needs to be accessed manually. Keep this password in a safe, accessible place so that technical support can gain access to the database.

Step 16 Click **Next**.

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

Step 17 For each option that you require, check the corresponding check box. The actions that are associated with the options occur after the setup program ends:

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

Step 18 Click **Next**.

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

Step 19 Click **Finish**.

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

Step 20 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.
- To access the ACS HTML interface, use the ACS Admin desktop icon, or use this URL in a supported web browser:

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

**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 additional Windows configuration, which is discussed in [Windows Authentication Configuration, page 2-1](#).

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 4.1 from previous versions of ACS. For information about upgrade paths, see [ACS Upgrade Requirements, page 1-4](#).

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

The upgrade process to ACS 4.1 transforms the data from ACS 4.0 to conform to the data structures and values in ACS 4.1. The new ACS 4.1 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 are stored 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 created by the conversion will be removed.

**Note**

Remote installations performed by using Windows Terminal Services or Remote Desktop (RDP) are not tested and are not supported. 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. Virtual Network Computing (VNC) has been tested successfully.

For upgrading or reinstalling ACS, see:

- [Reinstalling or Upgrading an Existing Configuration, page 1-11](#)
- [Reinstalling or Upgrading ACS without Data Preservation, page 1-13](#)

If you are installing ACS for the first time, see [Installing ACS for the First Time, page 1-7](#).

Reinstalling or Upgrading an Existing Configuration

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

Before You Begin

For information about what you must complete before reinstalling or upgrading ACS, see [Preparing to Install or Upgrade ACS, page 1-1](#).

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

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*, located 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 information 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 Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.

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

Step 6 After you have read the information in the Welcome dialog box, click **Next**.

The Before You Begin dialog box appears.

Step 7 If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions, page 1-6](#).

If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see [Preparing to Install or Upgrade ACS, page 1-1](#).

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

Step 8 Check **Yes, keep the existing configuration**.



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 select the drive and path where the setup program installs ACS.

The installation location must be 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 so, installation may appear to continue properly but will fail before it ends.

Step 11 Click **Next**.

The Database Encryption Password dialog box appears.

Step 12 Enter a password for database encryption.

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

Step 13 Click **Next**.

The setup program installs ACS and updates its configuration.

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:

- **Yes, I want to start the Cisco Secure ACS Service now**—Starts the Windows services that ACS comprises. If you do not check this option, the HTML 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 HTML interface in the default web browser for the current Windows user account.
- **Yes, I want to view the Readme file**—Opens *README.TXT* in Windows Notepad.

Step 15 Click **Next**.

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

Step 16 Click **Finish**.

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

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

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.
- To access the ACS HTML interface, use the ACS Admin desktop icon, or use this URL in a supported web browser:

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



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 additional Windows configuration, which is discussed in [Windows Authentication Configuration, page 2-1](#).

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 have backed up your ACS data and the Windows Registry, you cannot recover the previous configuration and database.

Before You Begin

For information about what must be completed before reinstalling or upgrading ACS, see [Preparing to Install or Upgrade ACS, page 1-1](#).

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

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 the minimum requirements must be applied 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*, located 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 information 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** Read the software license agreement. If you accept the software license agreement, click **ACCEPT**.
- The Welcome dialog box displays basic information about the setup program.
- Step 6** After you have read the information in the Welcome dialog box, click **Next**.
- The Before You Begin dialog box appears.
- Step 7** If you have completed all items in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**. For more information about these items, see [Gathering Answers for the Installation Questions, page 1-6](#).
- If you have not completed all items in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items in the Before You Begin dialog box, restart the installation. For more information, see [Preparing to Install or Upgrade ACS, page 1-1](#).
- After you click **Next**, the Previous Installation Location dialog box appears.
- Step 8** 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 9** To change the installation location, enter the new path name or use the Browse button to select the drive and path where the setup program installs ACS.

The installation location must be on a drive 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 so, installation may appear to continue properly but will fail before it ends.

- Step 10** Click **Next**.

The Authentication Database Configuration dialog box appears.

- Step 11** Choose an option for authentication users:

- To authenticate users with the ACS internal database only, check **Check the Cisco Secure ACS database only**.
- To authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory 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” setting** check box becomes unchecked. This option applies to all forms of access that ACS controls; not just dial-in access. For example, a user accessing your network through a VPN tunnel is not dialing in to a network access server; however, if you check **Yes, refer to “Grant dial-in permission to user” setting**, ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

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



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

- Step 12** 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*.



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

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

- 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, click **Enable Log-in Monitoring**. From the **Script to execute** list, select the option that you want applied in the event of authentication service failure:
 - **No Remedial Action**—ACS does not run a script. 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, click **Mail Notification**.



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

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

Step 17 Click **Next**.

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

Step 18 Click **Finish**.

The setup program exits. If, in [Step 16](#), you chose the options to view the HTML interface or *README.TXT* file, those options occur now.

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

`http://127.0.0.1:2002`



Note The ACS HTML interface is available only if you chose to start ACS services in [Step 16](#). If you did not, to make the HTML interface available, you can reboot the computer or type **net start csadmin** at a DOS prompt.

**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 additional Windows configuration, which is discussed in [Windows Authentication Configuration, page 2-1](#).

