



# Installation Guide for Cisco Secure ACS for Windows Server

---

This chapter provides information about installing, reinstalling, and upgrading to Cisco Secure Access Control Server (ACS) for Windows Server, version 3.3.

This chapter contains the following topics:

- [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#)
  - [Cisco Secure ACS System Description, page 2](#)
  - [System Requirements, page 3](#)
  - [Network and Port Requirements, page 5](#)
  - [Back Up Data, page 7](#)
  - [Gathering Answers for the Installation Questions, page 7](#)
- [What You Can Do, page 9](#)
- [Creating a Cisco Secure ACS Installation, page 10](#)
- [Reinstalling or Upgrading Cisco Secure ACS and Preserving Existing Configuration, page 18](#)
- [Reinstalling or Upgrading Cisco Secure ACS without Preserving Existing Configuration, page 23](#)
- [Windows Authentication Configuration, page 32](#)
  - [Configuring for Domain Controller Authentication, page 32](#)
  - [Configuring for Member Server Authentication, page 37](#)
- [Migrating to Cisco Secure ACS Solution Engine, page 48](#)

- [Uninstalling Cisco Secure ACS, page 51](#)
- [Obtaining Documentation, page 53](#)
- [Documentation Feedback, page 54](#)
- [Obtaining Technical Assistance, page 54](#)
- [Obtaining Additional Publications and Information, page 56](#)

## Preparation for Installing or Upgrading Cisco Secure ACS

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

This section contains the following topics:

- [Cisco Secure ACS System Description, page 2](#)
- [System Requirements, page 3](#)
- [Network and Port Requirements, page 5](#)
- [Back Up Data, page 7](#)
- [Gathering Answers for the Installation Questions, page 7](#)

## Cisco Secure ACS System Description

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

Cisco Secure ACS operates on Windows 2000 Server and Windows Server 2003. Cisco Secure ACS can run on a domain controller or a member server. For full information about supported operating systems, see the latest version of the Release Notes, accessible from the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm)

**Note**

If you want to authenticate users with a Windows Security Account Manager user database or an Active Directory user database, there is additional Windows configuration required after you have installed Cisco Secure ACS. For more information, see [Windows Authentication Configuration, page 32](#).

For additional information about Cisco Secure ACS, refer to the *User Guide for Cisco Secure ACS for Windows Server*, version 3.3.

## System Requirements

Your Cisco Secure ACS server must meet the minimum hardware, operating system, and third-party software requirements detailed in the following sections. Additionally, if you are upgrading from a previous version of Cisco Secure ACS, refer to [Cisco Secure ACS Upgrade Requirements, page 3](#).

### Cisco Secure ACS Upgrade Requirements

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

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm).

### Hardware Requirements

The computer running Cisco Secure ACS must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space. If you are running your database on the same computer, more disk space is required.
- Minimum graphics resolution of 256 colors at 800 x 600 lines.

## Operating System Requirements

Cisco Secure ACS for Windows Servers 3.3 supports the Windows operating systems listed below. Both the operating system and the service pack must be English-language versions.

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
  - with Service Pack 4 installed
  - without Microsoft clustering service installed
  - without other features specific to Windows 2000 Advanced Server enabled



---

**Note** We have not tested and cannot support the multi-processor feature of Windows 2000 Advanced Server. Windows 2000 Datacenter Server is not a supported operating system.

---

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition

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

For the most recent information about tested operating systems and service packs, see the Release Notes. The current version of the Release Notes are on Cisco.com, accessible from the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm).

## Third-Party Software Requirements

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

- Web browsers and Java virtual machines
- Novell NDS clients
- Token-card clients

Other than the software products described in the Release Notes, we have not tested the interoperability of Cisco Secure ACS and other software products on the same computer. We only support interoperability issues of software products that are mentioned in the Release Notes. The most recent version of the Release Notes are posted on Cisco.com, accessible from the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm).

## Network and Port Requirements

Your network should meet the following requirements before you begin deploying Cisco Secure ACS.

- For full TACACS+ and RADIUS support on Cisco IOS devices, AAA clients must run Cisco IOS Release 11.2 or later.
- Non-Cisco IOS AAA clients must be configured with TACACS+ and/or RADIUS.
- Dialin, VPN, or wireless clients must be able to connect to the applicable AAA clients.
- The computer running Cisco Secure ACS must be able to ping all AAA clients.
- Gateway devices between Cisco Secure ACS and other network devices must permit communication over the ports needed to support the applicable feature or protocol. For information about ports that Cisco Secure ACS listens to, see [Table 1](#).

- A supported web browser must be installed on the computer running Cisco Secure ACS. For the most recent information about tested browsers, see the Release Notes. The most recent version of the Release Notes are posted on Cisco.com, accessible from the following URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm).
- All network cards in the computer running Cisco Secure ACS must be enabled. If there is a disabled network card on the computer running Cisco Secure ACS, installing Cisco Secure ACS may proceed slowly due to delays caused by Microsoft CryptoAPI.




---

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

---

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

**Table 1** lists the ports that Cisco Secure ACS listens to for communications with AAA clients, other Cisco Secure ACSes and applications, and web browsers. Cisco Secure ACS uses other ports to communicate with external user databases; however, it initiates those communications rather than listening to specific ports. In some cases, these ports are configurable, such as with LDAP and RADIUS token server databases. For more information about ports that a particular external user database listens to, see the documentation for that database.

**Table 1** *Ports that Cisco Secure ACS Listens To*

Feature/Protocol	UDP or TCP?	Ports
RADIUS authentication and authorization	UDP	1645, 1812
RADIUS accounting	UDP	1646, 1813
TACACS+	TCP	49
CiscoSecure Database Replication	TCP	2000
RDBMS Synchronization with synchronization partners	TCP	2000

**Table 1** *Ports that Cisco Secure ACS Listens To (continued)*

Feature/Protocol	UDP or TCP?	Ports
User-Changeable Password web application	TCP	2000
Logging	TCP	2001
Administrative HTTP port for new sessions	TCP	2002
Administrative HTTP port range	TCP	Configurable; default 1024 through 65535

## Back Up Data

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

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



### Caution

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

For information about backing up Cisco Secure ACS, see the *User Guide for Cisco Secure ACS for Windows Server*, version 3.3.

## 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 you want to install Cisco Secure ACS on and a AAA client on your network. To facilitate the installation, collect the applicable information before beginning the installation.

**Note**

---

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

---

To collect information that is required during the installation of Cisco Secure ACS, follow these steps:

- 
- Step 1** Determine whether the computer that you will install Cisco Secure ACS on is a domain controller or a member server. If you want Cisco Secure ACS to authenticate users with a Windows domain user database, be aware that after you install Cisco Secure ACS you must perform the additional Windows configuration, discussed in [Windows Authentication Configuration, page 32](#).
- Step 2** For the first AAA client that you want to configure to use AAA services provided by Cisco Secure ACS, determine which AAA protocol and vendor-specific attribute you want to implement:
- TACACS+ (Cisco IOS)
  - RADIUS (Cisco Aironet)
  - RADIUS (Cisco BBSM)
  - RADIUS (Cisco IOS/PIX)
  - RADIUS (Cisco VPN 3000)
  - RADIUS (Cisco VPN 5000)
  - RADIUS (IETF)
  - RADIUS (Ascend)

- RADIUS (Juniper)
  - RADIUS (Nortel)
  - RADIUS (iPass)
- Step 3** Record the name of the AAA client.
- Step 4** Record the IP address of the AAA client.
- Step 5** Record the IP address of the computer that you want to install Cisco Secure ACS on.
- Step 6** Record the TACACS+ or RADIUS key (shared secret).
- 

## What You Can Do

This document provides detailed procedures for installing, reinstalling, and upgrading Cisco Secure ACS. You must select the right procedure for your situation. [Table 2](#) lists the five possible installation and upgrade scenarios. See [Table 2](#) to determine which procedure applies to your situation.



### Note

Before you perform any installation or upgrade procedure, we strongly recommend that you read [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#), and perform the applicable tasks detailed in that section.

**Table 2** *Installation and Upgrade Scenarios*

If your installation scenario is a:	Refer to. . .
New installation	<a href="#">Creating a Cisco Secure ACS Installation, page 10</a>
Reinstallation, <i>preserving</i> the CiscoSecure user database and Cisco Secure ACS configuration	<a href="#">Reinstalling or Upgrading Cisco Secure ACS and Preserving Existing Configuration, page 18</a>
Reinstallation, <i>overwriting</i> the CiscoSecure user database and Cisco Secure ACS configuration	<a href="#">Reinstalling or Upgrading Cisco Secure ACS without Preserving Existing Configuration, page 23</a>

**Table 2** *Installation and Upgrade Scenarios (continued)*

If your installation scenario is a:	Refer to. . .
Upgrade, <i>preserving</i> the CiscoSecure user database and Cisco Secure ACS configuration	<a href="#">Reinstalling or Upgrading Cisco Secure ACS and Preserving Existing Configuration, page 18</a>
Upgrade, <i>overwriting</i> the CiscoSecure user database and Cisco Secure ACS configuration	<a href="#">Reinstalling or Upgrading Cisco Secure ACS without Preserving Existing Configuration, page 23</a>

## Creating a Cisco Secure ACS Installation

Use this procedure to install Cisco Secure ACS for the first time.



### Note

For information about upgrading or reinstalling an existing Cisco Secure ACS installation, see [Table 2](#).

### Before You Begin

For information about what must be completed before installing Cisco Secure ACS, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

If you want Cisco Secure ACS to authenticate users with a Windows domain user database, after you install Cisco Secure ACS you must perform additional Windows configuration, discussed in [Windows Authentication Configuration, page 32](#).

To install Cisco Secure ACS, follow these steps:

- Step 1** Using a local administrator account, log in to the computer you want to install Cisco Secure ACS on.



### Note

We only support installations performed at the computer you are installing Cisco Secure ACS on. Remote installations, performed using Windows Terminal Services or products such as Virtual Network Computing (VNC), are not tested and are not supported.

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

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



---

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

---

**Step 3** Do one of the following:

- a. If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- b. If the Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the Cisco Secure ACS CD.



---

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

---

The CiscoSecure ACS Setup dialog box displays the software license agreement.

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

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

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

The Before You Begin dialog box lists items that you must complete before continuing with the installation. These are the same items discussed in [Gathering Answers for the Installation Questions, page 7](#).

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



---

**Note** If you have not completed all items listed in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items listed in the Before You Begin dialog box, restart the installation. For more information, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

---

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

**Step 7** If you want to change the installation location, follow these steps:

a. Click **Browse**.

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

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



---

**Note** Do not specify a path that contains a percent character, “%”. If you do so, installation may appear to continue properly but will fail before it completes.

---

c. Click **OK**.



---

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

---

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

**Step 8** Click **Next >**.

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



---

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

---

**Step 9** If you want to authenticate users with the CiscoSecure user database only, select the **Check the CiscoSecure ACS database only** option.

**Step 10** If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the CiscoSecure user database, follow these steps:

- a. Select the **Also check the Windows User Database** option.

The **Yes, refer to “Grant dialin permission to user” setting** check box becomes available.



---

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

---

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

**Step 11** Click **Next >**.

The CiscoSecure ACS Network Access Server Details dialog box appears. The information you provide in this dialog box has two uses:

- The setup program creates the AAA client definition in the Network Configuration section of Cisco Secure ACS.
- If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) in the Authenticate Users Using list, the setup program uses this information in [Step 19](#), in which you can configure a Cisco IOS network device to use this Cisco Secure ACS for AAA services.



---

**Note** You are not limited to defining a network access server in this dialog box. You can define any network device that can act as a AAA client.

---

- Step 12** Complete the following items in the CiscoSecure ACS Network Access Server Details dialog box:
- **Authenticate Users Using**—Select the AAA protocol used by the AAA client you are defining. If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), in [Step 19](#) you can configure the network device specified in this dialog box.
  - **Access Server Name**—Type the name of the AAA client that will use Cisco Secure ACS for AAA services.
  - **Access Server IP Address**—Type the IP address of the AAA client that will use Cisco Secure ACS for AAA services.
  - **Windows Server IP Address**—Type the IP address of the computer that you are installing Cisco Secure ACS on.
  - **TACACS+ or RADIUS Key**—Type the shared secret of the AAA client and Cisco Secure ACS. To ensure proper function and communication between the AAA client and Cisco Secure ACS, the key must be identical to the AAA client key. Shared secrets are case sensitive.

**Step 13** Click **Next >**.

The setup program installs Cisco Secure ACS and updates the Windows Registry. The Advanced Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, see the *User Guide for Cisco Secure ACS for Windows Server*, version 3.3.



---

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

---

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

**Step 15** Click **Next >**.

The Active Service Monitoring dialog box appears.



---

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

---

**Step 16** If you want Cisco Secure ACS to monitor user authentication services, select the **Enable Log-in Monitoring** check box. From the **Script to execute** list, select the option you want applied in the event of authentication service failure:

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



---

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

---

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

**Step 17** If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, select the **Mail Notification** check box.

**Step 18** Click **Next >**.

If, in [Step 12](#), you specified TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) as the AAA protocol for your first AAA client, the Network Access Server Configuration dialog box appears.

If, in [Step 12](#), you specified a AAA protocol other than TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), the CiscoSecure ACS Service Initiation dialog box appears.

**Step 19** If the Network Access Server Configuration dialog box appears and you want to configure AAA functionality on a Cisco IOS network device, follow these steps:

- a. Select the **Yes, I want to configure Cisco IOS software now** check box and click **Next >**.

The Enable Secret Password dialog box appears.

- b. In the Enable Secret Password box, type an enable secret password for the Cisco IOS network device.



---

**Note** You must type the shared secret exactly the same as it is configured on the Cisco IOS device, including whether the characters are uppercase or lowercase.

---

- c. Click **Next >**.

The Access Server Configuration dialog box displays information about configuring a Cisco IOS network device.

- d. After reading the text in the Access Server Configuration dialog box, click **Next >**.

The NAS Configuration dialog box displays the minimum Cisco IOS configuration needed for the network device you specified in [Step 12](#). The minimum configuration includes information you have provided during installation, including the IP address of the computer you are installing Cisco Secure ACS on, the TACACS+ or RADIUS key, and the enable secret password.



---

**Note** When using the Cisco IOS **aaa new-model** command, always provide for a local login method. This guards against the slight risk of being locked out of a Cisco IOS device should the administrative Telnet session fail while you are in the process of enabling a new AAA paradigm. For more information about the Cisco IOS **aaa** command, refer to Cisco IOS documentation.

---

- e. If you want to print the minimum Cisco IOS configuration, click **Print**.



---

**Note** Especially if you intend to implement the minimum configuration provided by the setup program, we recommend that you print the configuration now.

---

The setup program prints the configuration using the server's default printer.

- f. To telnet to the network device you specified in [Step 12](#), click **Telnet Now**.

The setup program opens a Telnet window. You can log in to the Cisco IOS device and update the device configuration, as applicable. The setup program copies the minimum configuration it provides to the Windows clipboard. If you want to use the minimum configuration, you can paste it in the Telnet window after you have entered the applicable configuration mode.

- g. After you finish with the options in the NAS Configuration dialog box, click **Next >**.

The CiscoSecure ACS Service Initiation dialog box appears.

- h. Proceed to [Step 21](#).

**Step 20** If the Network Access Server Configuration dialog box appears and you want to skip configuring a Cisco IOS network device, clear the **Yes, I want to configure Cisco IOS software now** check box, and then click **Next >**.

The CiscoSecure ACS Service Initiation dialog box appears.

**Step 21** For each option you want, select the corresponding check box. The actions associated with the options occur after the setup program finishes.

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

**Step 22** Click **Next >**.

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

**Step 23** Click **Finish**.

The setup program exits. If, in [Step 21](#), you chose the options to view the HTML interface or `README.TXT` file, those options occur now.

On the computer running Cisco Secure ACS, you can access the Cisco Secure ACS HTML interface using the ACS Admin desktop icon or you can use the following URL in a supported web browser:

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



---

**Note** The Cisco Secure ACS HTML interface is available only if you chose to start Cisco Secure ACS services in [Step 21](#). If you did not, to make the HTML interface available, you can either reboot the computer or type **net start csadmin** at a DOS prompt.

---

**Step 24** If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For procedures, see [Windows Authentication Configuration, page 32](#).

---

## Reinstalling or Upgrading Cisco Secure ACS and Preserving Existing Configuration

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



**Note**

---

For information about installing Cisco Secure ACS the first time, see [Table 2](#).

---

### Before You Begin

For information about what must be completed before reinstalling or upgrading Cisco Secure ACS, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

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

If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For procedures, see [Windows Authentication Configuration, page 32](#).

To reinstall or upgrade Cisco Secure ACS and preserve the existing configuration and CiscoSecure user database, follow these steps:

---

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



---

**Note** We only support installations performed at the computer you are installing Cisco Secure ACS on. Remote installations, performed using Windows Terminal Services or products such as Virtual Network Computing (VNC), are not tested and are not supported.

---

**Step 2** Insert the Cisco Secure ACS CD into a CD-ROM drive on the computer. If the CD-ROM drive supports the Windows autorun feature, the Cisco Secure ACS for Windows Server dialog box appears.



---

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

---

**Step 3** Do one of the following:

- a. If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- b. If the Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the Cisco Secure ACS CD.




---

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

---

The CiscoSecure ACS Setup dialog box displays the software license agreement.

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

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

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

The Before You Begin dialog box lists items that you must complete before continuing with the installation. These are the same items discussed in [Gathering Answers for the Installation Questions, page 7](#).

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




---

**Note** If you have not completed all items listed in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items listed in the Before You Begin dialog box, restart the installation. For more information, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

---

The Existing Installation of CiscoSecure ACS vx.x dialog box appears.

**Step 7** Select the **Yes, import the existing configuration** check box.



**Caution**

---

Be sure that the Yes, import the existing configuration check box is selected, not cleared. If you proceed without selecting the Yes, import the existing configuration check box, the setup program deletes all existing AAA client, user, and group information.

---

**Step 8** Click **Next** >.

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

**Step 9** If you want to change the installation location, follow these steps:**a.** Click **Browse**.

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

**b.** Change the installation location. You can either type the new location in the Path box or you can use the Drives and Directories lists to select a new drive and directory.

---

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

---

**c.** Click **OK**.

---

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

---

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

**Step 10** Click **Next** >.

The setup program installs Cisco Secure ACS and updates the Windows Registry.

The CiscoSecure ACS Service Initiation dialog box appears.

**Step 11** For each option you want, select the corresponding check box. The actions associated with each option occur after the setup program finishes.

- **Yes, I want to start the CiscoSecure ACS Service now**—Starts the Windows services that compose Cisco Secure ACS. If you do not select this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.

- **Yes, I want Setup to launch the CiscoSecure ACS Administrator from my browser following installation**—Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.
- **Yes, I want to view the Readme file**—Opens the `README.TXT` file in Windows Notepad.

**Step 12** Click **Next** >.

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

**Step 13** Click **Finish**.

The setup program exits. If, in [Step 11](#), you chose the options to view the HTML interface or `README.TXT` file, those options occur now.

On the computer running Cisco Secure ACS, you can access the Cisco Secure ACS HTML interface using the ACS Admin desktop icon or you can use the following URL in a supported web browser:

`http://127.0.0.1:2002`



---

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

---

**Step 14** If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For procedures, see [Windows Authentication Configuration, page 32](#).



---

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

---

# Reinstalling or Upgrading Cisco Secure ACS without Preserving Existing Configuration

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

**Caution**

Performing this procedure deletes the existing configuration of Cisco Secure ACS, including all AAA client, user, and group information. Unless you have backed up your Cisco Secure ACS data and the Windows Registry, there is no recovery of the previous configuration and database.

**Before You Begin**

For information about what must be completed before reinstalling or upgrading Cisco Secure ACS, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

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

If you want Cisco Secure ACS to authenticate users with a Windows domain user database, after you install Cisco Secure ACS you must perform additional Windows configuration, discussed in [Windows Authentication Configuration, page 32](#).

To reinstall or upgrade Cisco Secure ACS without preserving the existing configuration or CiscoSecure user database, follow these steps:

**Step 1**

Using a local administrator account, log in to the computer you want to install Cisco Secure ACS on.

**Note**

We only support installations performed at the computer you are installing Cisco Secure ACS on. Remote installations, performed using Windows Terminal Services or products such as Virtual Network Computing (VNC), are not tested and are not supported.

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

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




---

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

---

**Step 3** Do one of the following:

- a. If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- b. If the Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the Cisco Secure ACS CD.




---

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

---

The CiscoSecure ACS Setup dialog box displays the software license agreement.

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

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

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

The Before You Begin dialog box lists items that you must complete before continuing with the installation. These are the same items discussed in [Gathering Answers for the Installation Questions, page 7](#).

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



---

**Note** If you have not completed all items listed in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items listed in the Before You Begin dialog box, restart the installation. For more information, see [Preparation for Installing or Upgrading Cisco Secure ACS, page 2](#).

---

The Existing Installation of CiscoSecure ACS vx.x dialog box appears.

**Step 7** Clear the **Yes, import the existing configuration** check box.



---

**Note** Be sure that the Yes, import the existing configuration check box is cleared, not checked; otherwise, the existing configuration and CiscoSecure user database are preserved.

---

**Step 8** Click **Next >**.

The setup program removes the previous installation of Cisco Secure ACS.

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

**Step 9** If the CiscoSecure ACS Uninstall dialog box appears, click **Continue**.

The setup program finishes removing the previous installation of Cisco Secure ACS.

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

**Step 10** If you want to change the installation location, follow these steps:

a. Click **Browse**.

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

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



---

**Note** Do not specify a path that contains a percent character, “%”. If you do so, installation may appear to continue properly but will fail before it completes.

---

c. Click **OK**.



---

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

---

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

**Step 11** Click **Next >**.

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



---

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

---

**Step 12** If you want to authenticate users with the CiscoSecure user database only, select the **Check the CiscoSecure ACS database only** option.

**Step 13** If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the CiscoSecure user database, follow these steps:

a. Select the **Also check the Windows User Database** option.

The **Yes, refer to “Grant dialin permission to user” setting** check box becomes available.



---

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

---

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

**Step 14** Click **Next >**.

The CiscoSecure ACS Network Access Server Details dialog box appears. The information you provide in this dialog box has two uses:

- The setup program creates the AAA client definition in the Network Configuration section of Cisco Secure ACS.
- If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) in the Authenticate Users Using list, the setup program uses this information in [Step 22](#), in which you can configure a Cisco IOS network device to use this Cisco Secure ACS for AAA services.



---

**Note** You are not limited to defining a network access server in this dialog box. You can define any network device that can act as a AAA client.

---

**Step 15** Complete the following items in the CiscoSecure ACS Network Access Server Details dialog box:

- **Authenticate Users Using**—Select the AAA protocol used by the AAA client you are defining. If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), in [Step 22](#) you can configure the network device specified in this dialog box.
- **Access Server Name**—Type the name of the AAA client that will use Cisco Secure ACS for AAA services.

- **Access Server IP Address**—Type the IP address of the AAA client that will use Cisco Secure ACS for AAA services.
- **Windows Server IP Address**—Type the IP address of the computer you are installing Cisco Secure ACS on.
- **TACACS+ or RADIUS Key**—Type the shared secret of the AAA client and Cisco Secure ACS. These passwords must be identical to ensure proper function and communication between the AAA client and Cisco Secure ACS. Shared secrets are case sensitive.

**Step 16** Click **Next >**.

The setup program installs Cisco Secure ACS and updates the Windows Registry. The Advanced Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, refer to the *User Guide for Cisco Secure ACS for Windows Server*, version 3.3.




---

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

---

**Step 17** For each feature you want to enable, select the corresponding check box.

**Step 18** Click **Next >**.

The Active Service Monitoring dialog box appears.




---

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

---

**Step 19** If you want Cisco Secure ACS to monitor user authentication services, select the **Enable Log-in Monitoring** check box. From the **Script to execute** list, select the option you want applied in the event of authentication service failure:

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




---

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

---

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

**Step 20** If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, select the **Mail Notification** check box.

**Step 21** Click **Next >**.

If, in [Step 15](#), you specified TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) as the AAA protocol for your first AAA client, the Network Access Server Configuration dialog box appears.

If, in [Step 15](#), you specified a AAA protocol other than TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), the CiscoSecure ACS Service Initiation dialog box appears.

**Step 22** If the Network Access Server Configuration dialog box appears and you want to configure AAA functionality on a Cisco IOS network device, follow these steps:

- a. Select the **Yes, I want to configure Cisco IOS software now** check box and click **Next >**.

The Enable Secret Password dialog box appears.

- b. In the Enable Secret Password box, type an enable secret password for the Cisco IOS network device.



---

**Note** You must type the shared secret exactly the same as it is configured on the Cisco IOS device, including whether the characters are uppercase or lowercase.

---

- c. Click **Next >**.

The Access Server Configuration dialog box displays information about configuring a Cisco IOS network device.

- d. After reading the text in the Access Server Configuration dialog box, click **Next >**.

The NAS Configuration dialog box displays the minimum Cisco IOS configuration needed for the network device you specified in [Step 15](#). The minimum configuration includes information you provided during the installation, including the IP address of the computer running Cisco Secure ACS, the TACACS+ or RADIUS key, and the enable secret password.




---

**Note** When using the Cisco IOS **aaa new-model** command, always provide for a local login method. This guards against the slight risk of being locked out of a Cisco IOS device should the administrative Telnet session fail while you are in the process of enabling a new AAA paradigm. For more information about the Cisco IOS **aaa** command, refer to Cisco IOS documentation.

---

- e. To print the minimum Cisco IOS configuration, click **Print**.




---

**Note** Especially if you intend to implement the minimum configuration provided by the setup program, we recommend that you print the configuration now.

---

The setup program uses the server's default printer to print the configuration.

- f. To telnet to the network device you specified in [Step 15](#), click **Telnet Now**.

The setup program opens a Telnet window. You can log in to the Cisco IOS device and update the device configuration, as applicable. The setup program copies the minimum configuration it provides to the Windows clipboard. If you want to use the minimum configuration, you can paste it in the Telnet window after you have entered the applicable configuration mode.

- g. After you finish with the options in the NAS Configuration dialog box, click **Next >**.

The CiscoSecure ACS Service Initiation dialog box appears.

- h. Proceed to [Step 24](#).

**Step 23** If the Network Access Server Configuration dialog box appears and you want to skip configuring a Cisco IOS network device, clear the **Yes, I want to configure Cisco IOS software now** check box, and then click **Next >**.

The CiscoSecure ACS Service Initiation dialog box appears.

- Step 24** For each option you want, select the corresponding check box. The actions associated with each option occur after the setup program finishes.
- **Yes, I want to start the CiscoSecure ACS Service now**—Starts the Windows services that compose Cisco Secure ACS. If you do not select this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.
  - **Yes, I want Setup to launch the CiscoSecure ACS Administrator from my browser following installation**—Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.
  - **Yes, I want to view the Readme file**—Opens the `README.TXT` file in Windows Notepad.

**Step 25** Click **Next >**.

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

**Step 26** Click **Finish**.

The setup program exits. If, in [Step 24](#), you chose the options to view the HTML interface or `README.TXT` file, those options occur now.

On the computer running Cisco Secure ACS, you can access the Cisco Secure ACS HTML interface using the ACS Admin desktop icon or you can use the following URL in a supported web browser:

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



---

**Note**

The Cisco Secure ACS HTML interface is available only if you chose to start Cisco Secure ACS services in [Step 24](#). If you did not, to make the HTML interface available, you can either reboot the computer or type **net start csadmin** at a DOS prompt.

---

**Step 27** If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. For procedures, see [Windows Authentication Configuration, page 32](#).



---

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

---

## Windows Authentication Configuration

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

This section contains the following topics:

- [Configuring for Domain Controller Authentication, page 32](#)
- [Configuring for Member Server Authentication, page 37](#)
  - [Configuring Local Security Policies, page 42](#)
  - [Configuring Cisco Secure ACS Services, page 46](#)

## Configuring for Domain Controller Authentication

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

---

**Step 1** Add CISCO Workstation.

To satisfy Windows requirements for authentication requests, Cisco Secure ACS must specify the Windows workstation that the user is attempting to log into. Because Cisco Secure ACS cannot determine this information from authentication requests sent by AAA clients, it uses a generic workstation name for all requests. The workstation name used is “CISCO”.

In the local domain and in each trusted domain and child domain that Cisco Secure ACS will use to authenticate users, ensure both of the following:

- A computer account named “CISCO” exists.
- All users to be authenticated by Windows have permission to log into the computer named “CISCO”.

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

**Step 2** Verify Server Service Status.

The Cisco Secure ACS authentication service depends upon the Server service, which is a standard service in Microsoft Windows. On the computer running Cisco Secure 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 into the computer running Cisco Secure ACS and choose **Start > Programs Administrative Tools > Services**. The services list alphabetically.

---

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

**Step 3** Verify NTLM Version.**Note**

---

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

---

Verify that the NT LAN Manager (NTLM) version used is version 1. In the applicable Windows security policy editor, access **Local Policies > Security Options**, and locate the **LAN Manager Authentication Level** policy and set the policy to **Send LM & NTLM responses**. Other settings involve the use of NTLM v2, which Cisco Secure ACS does not support.

For more information, see [Microsoft.com: LAN Manager authentication level](https://www.microsoft.com/lan-manager-authentication-level).

**Step 4** Create User Account.**Note**

---

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

---

**Tip**

---

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

---

In the domain of the domain controller running Cisco Secure ACS, you must have a domain user account that can be used to run Cisco Secure ACS services (as explained in later steps of this procedure). Do both of the following:

1. Create a domain user account. This is the user account that you will use to run Cisco Secure ACS services. The user account does not require any particular group membership in the domain.

**Tip**

---

Give the user account an easily recognizable name, such as “CSACS”. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems related to failed Cisco Secure ACS authentication attempts.

---

2. To the user account you create, grant “Read all properties” permission for all Active Directory folders containing users that Cisco Secure ACS must be able to authenticate. Granting permissions for Active Directory folders is done by accessing Active Directory using the Microsoft Management Console and configuring the security properties for the folders containing users who are to be authenticated by Cisco Secure ACS.

**Tip**

---

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

---

For more information, see [Windows 2000 Server Active Directory](#).

**Step 5** Configure Local Security Policies.

**Note**

---

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

---

**Tip**

---

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

---

For the user account 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.

For more information, see [Configuring Local Security Policies, page 42](#)

**Step 6**

Configure Services.

**Note**

---

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

---

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

For more information, see [Configuring Cisco Secure ACS Services, page 46](#).

**Step 7**

Enable NetBIOS.

Cisco Secure ACS requires NetBIOS for communications with domain controllers of trusted or child domains. This means that you must enable NetBIOS on the following computers:

- The domain controller running Cisco Secure ACS.
- Trusted domain controllers for domains containing users who Cisco Secure ACS needs to authenticate.
- Domain controllers for child domains containing users who Cisco Secure ACS needs to authenticate.

To enable NetBIOS, access the advanced TCP/IP properties of the network connections on each domain controller, go to the WINS tab, and configure NetBIOS as applicable.

For more information, see the following references:

1. [Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server](#)
2. [Microsoft.com: Install WINS in Windows Server 2003](#)

**Step 8** Ensure DNS Operation.

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

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

**Step 9** Specify DNS Suffixes.



**Note**

---

This step is required only if Cisco Secure ACS authenticates users with the Active Directory of more than one domain.

---

On the domain controller running Cisco Secure ACS, configure the network connection that Cisco Secure ACS uses so that the network connection lists each trusted and child domain as a DNS suffix. To do so, access the advanced TCP/IP properties of the network connection, select the DNS tab, and configure the **Append these DNS suffixes** list, as applicable.

For more information, see the following references:

1. [Microsoft.com: Configure TCP/IP to use DNS \(Windows 2000\)](#)
2. [Microsoft.com: Configure TCP/IP to use DNS \(Windows 2003\)](#)

**Step 10** Configure WINS.

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

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

**Step 11** Configure LMHOSTS File.**Note**

---

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

---

As a final means of ensuring communication with other domain controllers, on the domain controller running Cisco Secure ACS, configure a LMHOSTS file to include entries for each domain controller of a trusted or child domain containing users who Cisco Secure ACS needs to authenticate.

**Tip**

---

The format of an LMHOSTS file is very particular. Be sure you understand the requirements of configuring the LMHOSTS file.

---

For more information, see the following references:

1. [Microsoft.com: LMHOSTS File](#).
  2. The example LMHOSTS file 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 Cisco Secure ACS runs on a member server and you need to authenticate users with a Windows user database, the additional configuration required varies, depending upon your Windows networking configuration. Most of the steps below are always applicable when Cisco Secure ACS runs on a member server; other steps are required only in certain conditions, as noted at the beginning of the step. Perform only those steps that always apply and that apply to your Windows networking configuration.

---

**Step 1** Verify Domain Membership.

One common configuration error that prevents Windows authentication is the erroneous assignment of the member server to a workgroup with the same name as the Windows domain that you want to use to authenticate users. While this may seem obvious, we recommend that you verify that the computer running Cisco Secure 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**, select the **Network Identification** tab, and read the information provided on that tab.

---

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

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

**Step 2** Add CISCO Workstation.

To satisfy Windows requirements for authentication requests, Cisco Secure ACS must specify the Windows workstation that the user is attempting to log into. Because Cisco Secure ACS cannot determine this information from authentication requests sent by AAA clients, it uses a generic workstation name for all requests. The workstation name used is “CISCO”.

In the local domain and in each trusted domain and child domain that Cisco Secure ACS will use to authenticate users, ensure both of the following:

- A computer account named “CISCO” exists.
- All users to be authenticated by Windows have permission to log into the computer named “CISCO”.

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

**Step 3** Verify Server Service Status.

The Cisco Secure ACS authentication service depends upon the Server service, which is a standard service in Microsoft Windows. On the computer running Cisco Secure 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 into the computer running Cisco Secure ACS and choose **Start > Programs Administrative Tools > Services**. The services list alphabetically.

---

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

**Step 4** Verify NTLM Version.

Verify that the NT LAN Manager (NTLM) version used is version 1. In the applicable Windows security policy editor, access **Local Policies > Security Options**, and locate the **LAN Manager Authentication Level** policy and set the policy to **Send LM & NTLM responses**. Other settings involve the use of NTLM v2, which Cisco Secure ACS does not support.

For more information, see [Microsoft.com: LAN Manager authentication level](#).

**Step 5** Create User Account.



**Tip**

---

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

---

In the domain of the domain controller running Cisco Secure ACS, you must have a domain user account that can be used to run Cisco Secure ACS services (as explained in later steps of this procedure). Do both of the following:

1. Create a domain user account. This is the user account that you will use to run Cisco Secure ACS services. The user account does not require any particular group membership in the domain.



**Tip**

---

Give the user account an easily recognizable name, such as “CSACS”. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems related to failed Cisco Secure ACS authentication attempts.

---

2. To the user account you create, grant “Read all properties” permission for all Active Directory folders containing users that Cisco Secure ACS must be able to authenticate. Granting permissions for Active Directory folders is done by accessing Active Directory using the Microsoft Management Console and configuring the security properties for the folders containing users who are to be authenticated by Cisco Secure ACS.

**Tip**

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

For more information, see [Windows 2000 Server Active Directory](#).

**Step 6** Configure Local Security Policies.

To the user account 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.

For more information, see [Configuring Local Security Policies, page 42](#).

**Step 7** Configure Services.

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

For more information, see [Configuring Cisco Secure ACS Services, page 46](#).

**Step 8** Enable NetBIOS.

Cisco Secure ACS requires NetBIOS for communications with all domain controllers to which it submits user authentication requests. This means that you must enable NetBIOS on the following computers:

- The member server running Cisco Secure ACS.
- The domain controller of the domain containing Cisco Secure ACS.
- Domain controllers of trusted domains containing users that Cisco Secure ACS needs to authenticate.
- Domain controllers of child domains containing users that Cisco Secure ACS needs to authenticate.

To enable NetBIOS, access the advanced TCP/IP properties of the network connections on each computer listed above, go to the WINS tab, and configure NetBIOS as applicable.

For more information, see the following references:

1. [Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server](#)
2. [Microsoft.com: Install WINS in Windows Server 2003](#)

**Step 9** Ensure DNS Operation.

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

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

**Step 10** Specify DNS Suffixes.



**Note**

---

This step is required only if Cisco Secure ACS authenticates users with the Active Directory of more than one domain.

---

On the member server running Cisco Secure ACS, configure the network connection that Cisco Secure ACS uses so that the network connection lists each domain as a DNS suffix. To do so, access the advanced TCP/IP properties of the network connection, select the DNS tab, and configure the **Append these DNS suffixes** list, as applicable.

For more information, see the following references:

1. [Microsoft.com: Configure TCP/IP to use DNS \(Windows 2000\)](#)
2. [Microsoft.com: Configure TCP/IP to use DNS \(Windows 2003\)](#)

**Step 11** Configure WINS.

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

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

**Step 12** Configure LMHOSTS File.**Note**

---

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

---

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

**Tip**

---

The format of an LMHOSTS file is very particular. Be sure to you understand the requirements of configuring the LMHOSTS file.

---

For more information, see the following references:

1. [Microsoft.com: LMHOSTS File](#)
2. The example LMHOSTS file 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:

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

You should have already created a user account that you intend to use to run Cisco Secure ACS. For full configuration requirements, see the applicable procedure: [Configuring for Member Server Authentication, page 37](#), or [Configuring for Domain Controller Authentication, page 32](#).

To configure local security policies, follow these steps:

- 
- Step 1** Using the local administrator account, log in to the computer running Cisco Secure ACS.
- Step 2** Choose **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.



---

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

---

The Local Security Settings window appears.

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

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

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

- Step 4** For the **Act as part of the operating system** policy and again for the **Log on as a service** policy, follow these steps:

- 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 “CSACS” in the “CORPORATE” domain, type “CORPORATE\CSACS”.

---

- d. Click **Check Names**.

The Enter Network Password dialog box appears.

- e. If the Enter Network Password dialog box appears, complete the following fields:
- **Connect as**—Type a domain-qualified username. The username provided must exist in the domain specified in **c.**. For example, if the domain specified is “CORPORATE” and “echamberlain” is a valid user in that domain, type “CORPORATE\echamberlain”.
  - **Password**—Type the password for the user account specified.

Then, click **OK**.

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

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

The Select Users or Groups dialog box closes.

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

- g. Click **OK**.

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

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



---

**Tip** To see the username you added, you may have to widen the Local Setting column.

---



---

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

---

After you have configured both 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 you configured.

- Step 5** Verify that the security policy settings you changed are in effect on the computer running Cisco Secure ACS. To do so, follow these steps:
- a. Close the Local Security Settings window.  
The window closes. This is the only way to refresh the information in the Effective Setting column.
  - b. Open the Local Security Settings window again. To do so, choose **Start > Programs > Administrative Tools > Local Security Policy**.
  - c. In the Name column, double-click **Local Policies**, and then 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 you added to the policy appears in the Effective Setting column.

**Note**

---

If the username you configured the policies to include does not appear in the Effective Setting column for both policies, there may be security policy settings on the domain controller that 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 Microsoft documentation for your operating system.

---

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

- Step 6** Close the Local Security Settings window.

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

---

## Configuring Cisco Secure ACS Services

### Before You Begin

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

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

You should have already created a user account that you intend to use to run Cisco Secure ACS and assigned it the permissions necessary to run Cisco Secure ACS services. For full configuration requirements, see the applicable procedure: [Configuring for Member Server Authentication, page 37](#), or [Configuring for Domain Controller Authentication, page 32](#).

To configure Cisco Secure ACS services, follow these steps:

- 
- Step 1** Using the local administrator account, log in to the computer running Cisco Secure ACS.
- Step 2** Choose **Start > Settings > Control Panel > Administrative Tools > Services**.




---

**Tip** If 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)**.
- Step 4** The Windows services installed by Cisco Secure ACS are the following:
- CSAdmin
  - CSAuth
  - CSDbSync
  - CSLog

- CSMon
- CSRADIUS
- CSTacacs

For each Cisco Secure ACS service, follow these steps:

- In the list of services, right-click a Cisco Secure ACS service, and from the shortcut menu, choose **Properties**.  
The Computer Browser Properties (Local Computer) dialog box appears.
- Select the **Log On** tab.
- Select the **This account** option.
- 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 “CSACS” in the “CORPORATE” domain, type “CORPORATE\CSACS”.

---

- In the Password box and in the Confirm Password box, type the password for the user account.
- Click **OK**.

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

**Step 5** Restart all Cisco Secure ACS services. To do so, follow these steps:

- Log in to the Cisco Secure ACS HTML interface.
- Click **System Configuration**, click **Service Control**, and then, at the bottom of the browser window, click **Restart**.

With the exception of CSAdmin, Cisco Secure ACS services restart.

- Wait until Cisco Secure ACS finishes restarting services. This usually takes a minute or two.
- Continuing as the local administrator on the computer running Cisco Secure ACS, choose **Start > Programs Administrative Tools > Services**.
- 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 Cisco Secure ACS services run using the privileges of the user account specified.

---

## Migrating to Cisco Secure ACS Solution Engine

Migrating from Cisco Secure ACS for Windows Server to Cisco Secure ACS Solution Engine uses the backup and restore features of Cisco Secure ACS. Backup files produced by Cisco Secure ACS for Windows Server are compatible with Cisco Secure ACS Solution Engine, provided that both are using the same version of Cisco Secure ACS software.

Depending upon what version of Cisco Secure ACS for Windows Server is used and the operating system that it runs on, the migration process varies. For example, if Cisco Secure ACS runs on Windows NT 4.0, the procedure below will advise you when it is necessary to upgrade to Windows 2000 Server. Because the use of the backup and restore features is only supported between Cisco Secure ACSes of the same version, you must use Cisco Secure ACS for Windows Server, version 3.3, to transfer data from Cisco Secure ACS for Windows Server to Cisco Secure ACS Solution Engine. Cisco Secure ACS for Windows Server, version 3.3, supports Windows 2000 Server and Windows Server 2003, not Windows NT 4.0. See the following procedure for more details.

### Before You Begin

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

To migrate from a Windows version of Cisco Secure ACS to Cisco Secure ACS Solution Engine, follow these steps:

---

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

**Step 2** Upgrade Cisco Secure ACS for Windows Server to version 3.3. If you do not have a license for version 3.3, you can use the trial version, available at <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des>.

If you run Cisco Secure ACS on Windows NT 4.0, upgrade to Cisco Secure ACS version 3.0, then migrate to Windows 2000 Server before upgrading to Cisco Secure ACS version 3.3. Cisco Secure ACS version 3.3 does not support Windows NT 4.0 and Cisco Secure ACS version 3.0 is the most recent version of Cisco Secure ACS that supports Windows NT 4.0. For information about upgrading to Cisco Secure ACS version 3.0 or about migrating to Windows 2000 Server, see *Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*. You can acquire the trial version of Cisco Secure ACS version 3.0 at <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des>.



---

**Note** For information about the versions of Cisco Secure ACS that we used to test the upgrade process, see the Release Notes. The most recent version of the Release Notes are on Cisco.com, accessible from the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm)

---

**Step 3** In the HTML interface of Cisco Secure ACS for Windows Server, version 3.3, use the Cisco Secure ACS Backup feature to back up the database. For more information about the Cisco Secure ACS Backup feature, see the *User Guide for Cisco Secure ACS for Windows Server*, version 3.3.

**Step 4** Copy the backup file from the computer running Cisco Secure ACS for Windows Server, version 3.3, to a directory on an FTP server. The directory must be accessible from the FTP root directory. Cisco Secure ACS Solution Engine must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.

- Step 5** In the HTML interface of Cisco Secure ACS Solution Engine, use the Cisco Secure ACS Restore feature to restore the database. For more information about restoring databases, see the *User Guide for Cisco Secure ACS Solution Engine*, version 3.3.
- The Cisco Secure ACS Solution Engine contains the original configuration of the Windows version Cisco Secure ACS that you migrated from.
- Step 6** Continuing in the HTML interface of the Cisco Secure ACS Solution Engine, verify the settings for “(Default)” entry in the Proxy Distribution Table are correct. To do so, select **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 running Cisco Secure ACS for Windows Server with Cisco Secure ACS Solution Engine, you must change the IP address of the appliance to that of the computer running Cisco Secure ACS for Windows Server.



---

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

---

To change the IP address of the Cisco Secure ACS Solution Engine, follow these steps:

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

# Uninstalling Cisco Secure ACS

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

**Note**

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

**Before You Begin**

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

To uninstall Cisco Secure ACS, follow these steps:

- Step 1** Using the local administrator account, log in to the computer that you want to uninstall Cisco Secure ACS from.
- Step 2** Choose **Start > Settings > Control Panel > Add/Remove Programs**.

**Tip**

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

The Add/Remove Programs window appears.

- Step 3** From the **Currently installed programs** list, select **CiscoSecure ACS v.x.x**, where *x.x* is the version of Cisco Secure ACS installed on the computer.
- Step 4** Click **Change/Remove**.

The Confirm File Deletion dialog box appears.

**Step 5** Click **Yes**.

The uninstallation begins. A dialog box appears.

**Step 6** If a dialog box with the following message appears:

The CiscoSecure 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 Cisco Secure ACS remains installed on the computer.

---

The uninstallation continues. Cisco Secure ACS services stop. A dialog box appears.

**Step 7** When a dialog box with the following message appears:

You may choose to keep the existing CiscoSecure ACS User Database which will save time if you re-install the software at a later date.

do one of the following:

- If you want to preserve the CiscoSecure user database, including all group data, click **Keep Database**.
- If you do not want to preserve the CiscoSecure user database, click **Delete Database**.



**Caution**

---

If you delete the database and you have not backed up the database, user and group data is lost.

---

Uninstallation completes.

**Step 8** Click **OK**.

---

# Obtaining Documentation

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

## Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

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

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

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

## Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:  
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication

identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

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

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

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

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

■ **Obtaining Additional Publications and Information**