



CHAPTER 2

Post-Installation Tasks

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

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

Windows Authentication Configuration

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

These topics describe configuration required for Windows authentication:

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

Configuring for Domain Controller Authentication

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

Step 1 Add the *CISCO* workstation.

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

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

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

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

Step 2 Verify the status of the Server and Net Logon services.

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



Tip

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

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

Step 3 Verify the NT LAN Manager (NTLM) version.



Note

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

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

- a. Regardless of the version of NTLM that you use, you must configure the LM Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LM Authentication Level policy**; and set the policy. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication level documentation on the Microsoft website.
- b. In addition to the previous setting, if you want to use NTLM version 2, you must also ensure that each:
 - Windows 2000 domain controller that performs user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 on the Microsoft website.
 - or
 - Domain controller that performs user authentication has the Windows 2003 Service Pack 1. This version does not require any patch.

Step 4 Create a user account.

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

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

**Tip**

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

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

**Tip**

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

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

Step 5 Configure Local Security policies.

**Note**

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

**Tip**

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

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

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

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

Step 6 Configure the services.

**Note**

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

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

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

Step 7 Enable NetBIOS.

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

- Domain controller that is running ACS.

- Trusted domain controllers for domains containing users that ACS must authenticate.
- Domain controllers for child domains that contains users whom ACS must authenticate.

To enable **NetBIOS**:

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

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



Note

ACS can also support Windows Server with NetBIOS disabled.

Step 8 Ensure DNS operation.

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

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

Step 9 Specify DNS suffixes.



Note

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

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

- Access the advanced TCP/IP properties of the network connection.
- Click the DNS tab.
- Configure the **Append these DNS suffixes** list, as applicable.

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

Step 10 Configure WINS.

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

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

Step 11 Configure the *LMHOSTS* file.



Note

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

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

**Tip**

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

For more information, see:

1. The appropriate [LMHOSTS File](#) on the Microsoft website.
2. The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is `<systemroot>\system32\drivers\etc\lmhosts.sam`.

Configuring for Member Server Authentication

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

To configure for member server authentication:

Step 1 Verify domain membership.

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

**Tip**

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

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

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

Step 2 Add the *CISCO* workstation.

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

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

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

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

Step 3 Verify the server service status.

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

**Tip**

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

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

Step 4

Verify the NTLM version.

**Note**

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

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

- a. Regardless of the version of NTLM that you use, you must configure the LM Authentication level settings. In the applicable Windows security policy editor:
 1. Choose **Local Policies > Security Options**
 2. Locate the **LM Authentication Level policy** and set the policy.
 3. For example, if you are using LM or NTLM version 1, set it to **Send LM & NTLM responses**. For information on the various options and NTLM version 2 settings, see the appropriate NTLM authentication level documentation on the Microsoft website.
- b. In addition to the previous setting, if you wish to use NTLM version 2 you must also ensure that each:
 - Windows 2000 domain controller that performs user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 on the Microsoft website.
 - or
 - Domain controller that performs user authentication has Windows 2003 Service Pack 1. This version does not require any patch.

Step 5

Create a user account.

**Tip**

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

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

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

**Tip**

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

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

**Tip**

To access the security properties of an AD folder of users, right-click the folder, select **Properties**, and choose the Security tab. Click **Add** to include the username.

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

Step 6 Configure local security policies.

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

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

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

Step 7 Configure the services.

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

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

Step 8 Enable NetBIOS.

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

- Member server that is running ACS.
- Domain controller of the domain that contains ACS.
- Domain controllers of trusted domains that contain users that ACS must authenticate.
- Domain controllers of child domains that contain users whom ACS must authenticate.

To enable **NetBIOS**:

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

For more information, see the Microsoft website for appropriate documentation about installing WINS on Windows Server 2000 and Windows Server 2003.

Step 9 Ensure DNS operation.

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

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

Step 10 Specify DNS suffixes.

**Note**

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

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

- a. Access the advanced TCP/IP properties of the network connection.
- b. Click the DNS tab.
- c. Configure the **Append these DNS suffixes** list, as applicable.

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

Step 11 Configure WINS.

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

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

Step 12 Configure the *LMHOSTS* file.**Note**

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

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

**Tip**

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

For more information, see:

- The appropriate [LMHOSTS File](#) on the Microsoft website.
 - The example *LMHOSTS* file is included with the Windows operating system. The default location and filename for the sample file is `<systemroot>\system32\drivers\etc\lmhosts.sam`
-

Configuring Local Security Policies

Before You Begin

This procedure is required only if one of the following conditions is true. ACS runs on a:

- Member server and must authenticate users with a Windows user database.
- Domain controller and must authenticate users in trusted domains or child domains.

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

To configure local security policies:

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



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

The Local Security Settings window appears.

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

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

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

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

- a. Double-click the policy name.

The Local Policy Setting dialog box appears.

- b. Click **Add**.

The Select Users or Groups dialog box appears.

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



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

- d. Click **Check Names**.

The Enter Network Password dialog box appears.

- e. In:

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

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

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

The Select Users or Groups dialog box closes.

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

- g. Click **OK**.

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

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



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



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

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

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

- a. Close the Local Security Settings window.
To refresh the information in the Effective Setting column, close the window.
- b. Open the Local Security Settings window again. Choose **Start > Programs > Administrative Tools > Local Security Policy**.
- c. In the Name column, double-click **Local Policies** and double-click **User Rights Assignment**.
The Local Security Settings window displays an updated list of policies with their associated settings.
- d. For the **Act as part of the operating system** policy and again for the **Log on as a service** policy, verify that the username that you added to the policy appears in the Effective Setting column.



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

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

Step 6 Close the Local Security Settings window.

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

Configuring ACS Services

Before You Begin

This procedure is required only if one of the following conditions is true. ACS runs on a:

- Member server and must authenticate users with a Windows user database.
- Domain controller and must authenticate users in trusted domains or child domains.

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

To configure ACS services:

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

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



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

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

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

The Windows services that ACS installs are:

- **CSAdmin**
- **CSAuth**
- **CSDBSync**
- **CSLog**
- **CSMon**
- **CSRADIUS**
- **CSTacacs**

Step 4 For each ACS service:

- a. In the list of services, right-click an ACS service and, from the shortcut menu, choose **Properties**. The Computer Browser Properties (Local Computer) dialog box appears.
- b. Click the **Log On** tab.
- c. Select the **This account** option.
- d. In the box next to the **This account** option, type the username for the account.



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

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

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

Step 5 To restart all ACS services:

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

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

- c. Wait until ACS finishes restarting all services.; this usually takes a minute or two.
- d. Continuing as the local administrator on the computer that is running ACS, choose **Start > Programs Administrative Tools > Services**.
- e. In the Name column, double-click **CSAdmin**.
The **CSAdmin** Properties dialog box appears.
- f. Click **Stop** and wait for the Service Control dialog box to close.
- g. Click **Start** and wait for the Service Control dialog box to close.
- h. In the **CSAdmin** Properties dialog box, click **OK**.
The **CSAdmin** Properties dialog box closes.
- i. Close the Services window.

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

Disabling NetBIOS

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

ACS 3.x to 4.2 ODBC Logging Updates

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

From ACS 4.0 and later versions, changes to the SQL database present all the ODBC fields as strings rather than numbers. Field types have changed from INTEGER to VARCHAR; for example:

```
Message_Type VARCHAR(255) NULL.
```

To recreate the tables:

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

The Logging Configuration page appears.

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

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

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

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



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

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



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

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

Step 6 Click **Submit**.

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

Step 7 Repeat the previous steps for each ODBC log.

For additional information on configuring logs, see Logs and Reports chapter of the *User Guide for Cisco Secure ACS 4.2*.

Migrating to ACS Solution Engine

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

Before You Begin

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

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

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

Step 2 Upgrade ACS for Windows to version 4.2. If you do not have a license for version 4.2, you can use the trial version, which is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des>.



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

Step 3 In the web interface of ACS for Windows, use the ACS Backup feature to back up the database. For more information about the ACS Backup feature, see the *User Guide for Cisco Secure Access Control Server 4.2*.

**Note**

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

**Note**

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

- Step 4** Copy the backup file from the computer that is running ACS for Windows to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS SE must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.
- Step 5** In the web interface of ACS SE, use the ACS Restore feature to restore the database. For more information about restoring databases, see the *User Guide for Cisco Secure Access Control Server 4.2*. The ACS SE contains the original configuration of the Windows version of ACS from which you migrated.
- Step 6** Continuing in the web interface of the ACS SE:
- a. Verify the settings for **(Default)** entry in the Proxy Distribution Table are correct.
 - b. Choose **Network Configuration > (Default)**, and ensure that the Forward To list contains the entry for the appliance.
- Step 7** If you want to replace the computer that is running ACS for Windows with ACS SE, you must change the appliance's IP address to that of the computer that is running ACS for Windows.

**Note**

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

To change the IP address of the ACS SE:

- a. Record the IP address of the computer that is running ACS for Windows.
- b. Change the IP address of the computer that is running ACS with Windows to a different IP address.
- c. Change the IP address of the ACS SE to the IP address previously used by the computer that is running ACS for Windows. This is the IP address that you recorded in **a**. For detailed steps, see *Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine 4.2*.

Uninstalling ACS

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

Before You Begin

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

To uninstall ACS:

-
- Step 1** Using the local administrator account, log in to the computer from which you want to uninstall ACS.
- Step 2** Choose **Start > Settings > Control Panel > Add/Remove Programs**.
The Add/Remove Programs window appears.
- Step 3** From the **Currently installed programs** list, choose **Cisco Secure ACS v $x.x$** , where $x.x$ is the version of ACS that is installed on the computer.
- Step 4** Click **Change/Remove**.
The Confirm File Deletion dialog box appears.



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

- Step 5** Click **Yes**.
The process of uninstallation begins.
- Step 6** A dialog box displays the message:
The Cisco Secure ACS Service is currently running.
If you still want to continue the uninstall, it will be stopped for you.

Click **Continue**.



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

The uninstallation process continues. ACS services stop.

- Step 7** A dialog box displays the following message:
You might choose to keep the existing ACS internal database, which will save time if you reinstall the software at a later date.

To preserve the ACS internal database user and group data, click **Keep Database**. This action saves the user-group configuration in the directory where ACS was installed.



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



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

You are asked to enter a password. Use this password during the installation import step. Make a note of this password for any future installation import phase or if technical support needs access to the database.

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

**Caution**

If you choose **Delete Database** and you have not backed up the database, you will lose user and group data.

The uninstallation process ends.

Step 8

Click **OK**.

Troubleshooting Uninstallation Problems

Cannot use the Add/Remove Programs Feature or Uninstallation Fails

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

Solution You can uninstall ACS using the ACS Clean Utility. Locate the *clean.exe* program on the ACS CD and run it on the computer on which the damaged installation of ACS resides. The *clean.exe* program thoroughly removes ACS.

To remove ACS using the Clean Utility:

Step 1

Run the *clean.exe*.

The setup program shows a welcome screen.

Step 2

Click **Next**.

Step 3

ACS Clean Utility will automatically detect the ACS installation and prompt for confirmation. Check the **Yes Uninstall ACS** check box.

Step 4

Click **Next**.

A dialog box displays the following message:

The Cisco Secure ACS Service is currently running.

If you want to continue the uninstallation process, Click **Continue**. This will stop the ACS services and begin the uninstallation process.

**Note**

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

After the uninstallation process is complete, Uninstall Complete is displayed on the setup screen.

**Note**

You cannot preserve the ACS internal database like in case of normal installation procedure.

ACS Uninstallation Fails to Delete the Files

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

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

What To Do Next

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

Refer to the *Configuration Guide for Cisco Secure ACS 4.2* for suggested deployment sequences. Refer to the *User Guide for Cisco Secure ACS 4.2* for details about all administrative functions, such as Backup and Restore; Certificate Setup; and other important tasks.

Refer to the release notes for up-to-date information on Cisco.com.

Logging In and Out of the System

To access ACS:

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

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

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

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

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

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

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

For detailed information on logging in and accessing the web interface, see the *User Guide for Cisco Secure ACS 4.2*.

Viewing Software Version Information

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

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