Post-Installation Tasks

This section provides the post-installation tasks for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

- Windows Authentication Configuration, page 2-1
  - Configuring for Domain Controller Authentication, page 2-2
  - Configuring for Member Server Authentication, page 2-5
- ACS 3.x to 4.0 ODBC Logging Updates, page 2-12
- Migrating to ACS Solution Engine, page 2-13
- Uninstalling ACS, page 2-15
- What To Do Next, page 2-16

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.

This section contains:

- Configuring for Domain Controller Authentication, page 2-2
- Configuring for Member Server Authentication, page 2-5
  - Configuring Local Security Policies, page 2-9
  - Configuring ACS Services, page 2-11

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:

Step 1 Add CISCO workstation.

To satisfy 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 server service status.

The ACS authentication service depends on the Server service, which is a standard service in Microsoft Windows. 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 3 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 LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but need to ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager 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 involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

  or

- Domain controller involved in user authentication has the Windows 2003 Service Pack 1. This version does not require any patch.

Step 4 Create a user account.

Tip If you have upgraded or reinstalled ACS and you created a user account for the previous installation, complete this step only if you want to use a different user account to run ACS services.

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 explained in subsequent steps in this procedure).

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 are related to failed ACS authentication attempts.

To the domain administrator account that you create, grant **Read all properties** permission for all Active Directory (AD) folders containing users who require ACS authentication. To grant permission for AD folders, access AD by using 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 have upgraded or reinstalled 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 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, page 2-9.

Step 6 Configure 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 that you added to the security policies in the preceding step.

For more information, see Configuring ACS Services, page 2-11.

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 containing 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:

- Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server.
- Microsoft.com: Install WINS in Windows Server 2003.

Step 8 Ensure DNS operation.

Especially for authentication of users in AD, ACS needs DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event notification e-mail. 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 that are sent to AD.

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

Step 9 Specify DNS suffixes.

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

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

a. Access the advanced TCP/IP properties of the network connection.

b. Choose the DNS tab.

c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see:

- Microsoft.com: Configure TCP/IP to use DNS (Windows 2000).
- Microsoft.com: Configure TCP/IP to use DNS (Windows 2003).

Step 10 Configure WINS.

You must enable WINS on your network if ACS must authenticate users belonging 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 *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 that is running ACS, configure a *LMHOSTS* file to include entries for each domain controller of a trusted or child domain containing 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. Microsoft.com: LMHOSTS File.
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:

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 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 CISCO workstation.

To satisfy 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 server service, which is a standard service in Microsoft Windows. 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 LAN Manager (LM), NTLM version 1, or NTLM version 2 protocols. LAN Manager is considered the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but need to ensure that:

a. Regardless of the version of NTLM that you use, you must configure the LAN Manager Authentication level settings. In the applicable Windows security policy editor, choose **Local Policies > Security Options**; locate the **LAN Manager 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 setting the above, if you wish to use NTLM version 2 you must also ensure that each:

   – Windows 2000 domain controller involved in user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318 found on the Microsoft website.

     or

   – Domain controller involved in user authentication has Windows 2003 Service Pack 1. This version does not require any patch.

Step 5 Create a user account.

Tip If you have upgraded or reinstalled ACS and you completed this item previously, it 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 a domain administrator account that you can use to run ACS services (as explained in subsequent steps of this procedure).

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 are related to failed ACS authentication attempts.

b. To the domain administrator account that you create, grant **Read all properties** permission for all AD folders containing users who require ACS authentication. To grant permission for AD folders, access AD by using 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 clicking 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, page 2-9.

Step 7 Configure services.

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

For more information, see Configuring ACS Services, page 2-11.

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.
- The domain controller of the domain containing ACS.
- Domain controllers of trusted domains containing users that ACS must authenticate.
- Domain controllers of child domains containing users whom ACS must authenticate.

To enable **NetBIOS**:

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

For more information, see:

- Microsoft.com: Install WINS in Windows 2000 Server or Windows 2000 Advanced Server.
- Microsoft.com: Install WINS in Windows Server 2003.

Step 9 Ensure DNS operation.

Especially for authentication of users in Active Directory (AD), ACS needs DNS to operate correctly on your network. Other ACS features might also use DNS, such as RADIUS-based token server authentication or an ACS Service Management event-notification e-mail. 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 that are sent 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. Choose the DNS tab.

c. Configure the **Append these DNS suffixes** list, as applicable.

For more information, see:

- Microsoft.com: Configure TCP/IP to use DNS (Windows 2000).
- Microsoft.com: Configure TCP/IP to use DNS (Windows 2003).

Step 11 Configure WINS.

If ACS must authenticate users belonging to a trusted or child domain, and if 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 *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 a *LMHOSTS* file to include entries for each domain controller containing users that ACS must authenticate. This includes 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:

- Microsoft.com: LMHOSTS File
- 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.
- ACS runs on a domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run ACS. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-5, or Configuring for Domain Controller Authentication, page 2-2.

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 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. Complete the following:

- **Connect as**—Type a domain-qualified username. The username 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 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 specified in c. appears in the settings associated with the policy that you configured.

h. Verify that the username that is specified 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 have 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 specified user account 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.
- ACS runs on a domain controller and must authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to 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, page 2-5, or Configuring for Domain Controller Authentication, page 2-2.

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 a ACS service and, from the shortcut menu, choose **Properties**.

The Computer Browser Properties (Local Computer) dialog box appears.

b. Choose the **Log On** tab.

c. Select the **This account** option.

d. In the box next to the **This account** option, type the username for the account.

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

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

f. Click **OK**.

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

Step 5 To restart all ACS services:

a. Log in to the ACS HTML interface.

b. Click **System Configuration**, click **Service Control**, and then, at the bottom of the browser window, click **Restart**.

With the exception of CSAdmin, ACS services restart.

c. Wait until ACS finishes restarting 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.

ACS 3.x to 4.0 ODBC Logging Updates

If you used ACS 3.x ODBC logging and upgraded to ACS 4.0 preserving your data, you must update the ODBC tables so that the SQL tables continue to work.

Changes to the SQL database now present all the ODBC fields as strings rather than numbers. Field types have been 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 selected.

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

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

Step 6 Click **Submit**.

ACS begins sending logging data to the relational database table that is specified by using the system DSN that you configured.

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 for Windows 4.0*.

Migrating to ACS Solution Engine

Migrating from ACS for Windows to ACS Solution Engine uses the backup and restore features. ACS for Windows produces backup files that are compatible with ACS Solution Engine, provided that both use the same version of ACS software.

Depending on what version of ACS for Windows you use and the operating system on which it runs, the migration process varies. For example, if ACS runs on Windows NT 4.0, the following procedure 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 ACSs of the same version, you must use ACS for Windows, version 4.0, to transfer data from ACS for Windows to ACS Solution Engine. ACS for Windows, version 4.0, 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 ACS and save the backup file in a location on a drive that is not local to the computer that is running ACS.

To migrate from a Windows version of ACS to ACS Solution Engine:

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

Step 2 Upgrade ACS for Windows to version 4.0. If you do not have a license for version 4.0, you can use the trial version, which is available at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

If you run ACS on Windows NT 4.0, upgrade to ACS version 3.0; then migrate to Windows 2000 Server before upgrading to ACS version 4.0. ACS version 4.0 does not support Windows NT 4.0 and ACS version 3.0 is the most recent version of ACS that supports Windows NT 4.0. For information about upgrading to 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 download the trial version of ACS version 3.0 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 HTML interface of ACS for Windows, version 4.0, 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 ACS for Windows* 4.0.

Step 4 Copy the backup file from the computer that is running ACS for Windows, version 4.0, to a directory on an FTP server. The directory must be accessible from the FTP root directory. 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 ACS Solution Engine, 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 Solution Engine*, version 4.0.

The ACS Solution Engine contains the original configuration of the Windows version ACS from which you migrated.

Step 6 Continuing in the HTML interface of the ACS Solution Engine, verify the settings for **(Default)** entry in the Proxy Distribution Table are correct. Choose **Network Configuration** > **(Default)**, and ensure that the Forward To list contains the entry for the appliance.

Step 7 If you want to replace the computer that is running ACS for Windows with ACS Solution Engine, you must change the IP address of the appliance to that of the computer that is running ACS for Windows.

Note If you do not change the IP address of the ACS Solution Engine 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 Solution Engine.

To change the IP address of the ACS Solution Engine:

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 Solution Engine 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*.

Uninstalling ACS

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

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

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**.

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

The Add/Remove Programs window appears.

Step 3 From the Currently installed programs list, select **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.

Step 5 Click **Yes**.

The 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 CD and run it on the computer that has the damaged installation of ACS.

The uninstallation 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**. The user-group configuration is saved in the directory where ACS was installed.

Caution No other configuration is saved (only user and group data). Perform a backup first if you want to save other configuration data. See Back Up Data, page 1-5 or the backing up instructions in the *User Guide for Cisco Secure ACS for Windows 4.0*.

You are asked to enter a password. Use this password during the installation import step. Keep this password in a safe location 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, user and group data is lost.

Uninstallation ends.

Step 8 Click **OK**.

What To Do Next

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

Refer to the *User Guide for Cisco Secure ACS for Windows 4.0* for the suggested deployment sequence and how to take advantage of the features of your ACS product in Deployment Considerations. You can also see the *User Guide for Cisco Secure ACS for Windows 4.0* 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 HTML 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 HTML interface, see the *User Guide for Cisco Secure ACS or Windows 4.0*.

Viewing Software Version Information

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

```
Cisco Secure ACS
Release 4.0(1) Build xx
Copyright ©2005 Cisco Systems, Inc.
```