



CHAPTER 2

Installing Cisco Secure ACS Remote Agent for Windows

This chapter provides information about installing Cisco Secure Access Control Server (ACS) Remote Agent for Windows.

This chapter contains:

- [System Requirements](#)
- [Network Requirements](#)
- [Installing a Remote Agent for Windows](#)
- [Uninstalling ACS Remote Agent for Windows](#)
- [Upgrading ACS Remote Agent for Windows](#)
- [Windows Authentication Configuration](#)

System Requirements

The computer on which ACS Remote Agent for windows is running must contain:

- [ACS Requirements](#)
- [Hardware Requirements](#)
- [Operating System Requirements](#)

ACS Requirements

You must use ACS Remote Agent for Windows, version 4.2, with ACS SE, version 4.2. We do not support other Cisco Secure ACS releases.



Note

ACS Remote Agent 4.2 for Windows does not support 64-bit operating systems.

Hardware Requirements

The computer running ACS Remote Agent for Windows must contain:

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space.

Operating System Requirements

The computer on which ACS Remote Agent for windows is running must use one of the following operating systems:

- Windows 2000 Server, with Service Pack 3 or Service Pack 4 installed.
- Windows 2003 Server, with Service Pack 1 or Service Pack 2 installed.
- Windows 2000 Advanced Server:
 - With Service Pack 3 or 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 multiprocessor feature of Windows 2000 Advanced Server. Windows 2000 Datacenter Server is not a supported operating system.

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

The Japanese Operating System (JOS), Windows 2000 and Windows 2003 also supports ACS Remote Agent for Windows 4.2.

Tested Windows Security Patches

We have tested ACS Remote Agent for Windows 4.2 with the Windows Server 2003 patches documented in the following Microsoft Knowledge Base articles:

- 819696
- 823182
- 823559
- 824105
- 824141
- 824146
- 825119
- 828028
- 828035
- 828741

- 832894
- 835732
- 837001
- 837009
- 839643
- 840374

ACS Remote Agent for Windows has been tested with the Windows 2000 Server patches documented in the following Microsoft Knowledge Base Articles:

- 329115
- 823182
- 823559
- 823980
- 824105
- 824141
- 824146
- 825119
- 826232
- 828035
- 828741
- 828749
- 835732
- 837001
- 839643

**Note**

Cisco Systems officially supports and encourages the installation of all Microsoft security patches for Windows Server 2000 and Windows Server 2003 when they are used with ACS. Our experience has shown that these patches do not cause problems with the operation of ACS. If the installation of security patches does cause a problem with ACS, contact TAC and we will work on resolving the issue.

Network Requirements

Before you install ACS Remote Agent, ensure that the:

- Computer running ACS Remote Agent for Windows must be able to ping the ACS SEs that it supports.
- Gateway devices must permit traffic between the computer running ACS Remote Agent for Windows and the ACS SE. Specifically, the remote agent must receive TCP communication on the TCP ports that you configure in *CSAgent.ini*. If ACS uses all services, the default TCP ports are 2004, 2006, and 2007. The appliance must receive TCP communication on TCP port 2003.

**Note**

By using the *CSAgent.ini* file, you can configure the ports that the Remote Agent uses to communicate with ACS. If you change the communication ports, you must configure intervening gateway devices to permit TCP traffic on the ports that you configure the Remote Agent to use. For more information about changing the ports that a Remote Agent uses, see [Configuring a Remote Agent](#).

Installing a Remote Agent for Windows

Before You Begin

Determine the IP address of the Cisco Secure ACS for Windows that will be the configuration provider for this remote agent. For more information about configuration providers, see [Configuration Provider](#).

**Note**

If CSA (Cisco Security Agent) is enabled on the machine, you must disable it before installing ACS Remote Agent for Windows 4.2.

To install ACS Remote Agent for a Windows operating system:

Step 1 By using the local administrator account, log in to the Microsoft Windows server on which you want to install ACS Remote Agent.

Step 2 Insert the ACS Software Migration CD into a CD-ROM drive on the Microsoft Windows server. If the CD-ROM drive supports the Windows autorun feature, a dialog box might appear. Click **Cancel** to close the dialog box.

**Note**

If the computer does not have a required service pack installed, a dialog box may appear. You can apply Windows service packs before or after installing ACS Remote Agent. You can continue with the installation, but you must install the required service pack after the installation is complete; otherwise, ACS Remote Agent may not function reliably. For more information on Windows service packs, refer to the Microsoft website.

Step 3 On the ACS Software Migration CD, locate the Windows remote agent subdirectory.

Step 4 From the Windows remote agent subdirectory, run *Setup.exe*.

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

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

The Choose Destination Location dialog box appears.

Step 6 The installation location appears under Destination folder. You can change the installation location. Click **Next**.

Step 7 The Agent Services dialog box appears with a list of options that ACS Remote Agent for Windows supports.

Step 8 Choose the agent services that you want to use:

- Logging Service
- Windows Authentication Service

Click **Next**. The Configuration Provider dialog box appears.

- Step 9** In the **Hostname** box, enter the hostname or IP address of the ACS SE that should control the configuration of this remote agent.



Note If you enter a hostname, be sure that DNS is operating correctly or that the appliance hostname is in the local hosts file.
You can add the IP address or hostname at a later time, before using Remote Agent, by editing the configuration file, *CSAgent.ini*.

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

The setup program installs ACS Remote Agent for Windows.

The Setup Complete dialog box lists options for restarting the computer.

- Step 11** Select the reboot option that you want.



Note To complete the installation successfully you must reboot. If you chose not to reboot now, do so before you use remote agent services.

- Step 12** Click **Finish**.

The setup program exits. If you chose to reboot the computer automatically, Windows restarts.

Where to go next:

If you want to:

- Authenticate users with a Windows domain user database, you must perform the additional Windows configuration which [Windows Authentication Configuration](#) describes.



Note If you are reinstalling the remote agent after uninstalling it, the previous configuration of the remote agent service was lost during the uninstallation. For more information, see [Windows Authentication Configuration](#).

- Use the Logging Service, you must perform additional configuration in ACS SE. See *User Guide for ACS Solution Engine 4.2* for more information.

Uninstalling ACS Remote Agent for Windows

Use the Windows Control Panel to uninstall ACS Remote Agent for Windows. No special steps are required.



Note If you do not intend to reinstall ACS Remote Agent for Windows on this computer, remove the applicable remote agent configurations from all ACS SEs.

Upgrading ACS Remote Agent for Windows

The upgrade process entails uninstalling the old version of the remote agent and installing the new version.

To upgrade ACS Remote Agent for Windows software:

-
- Step 1** Remove the old version of the remote agent by performing the steps in [Uninstalling ACS Remote Agent for Windows](#).
- Step 2** By using the version of ACS Remote Agent for Windows to which you want to upgrade, perform the steps in [Installing a Remote Agent for Windows](#).
-

Windows Authentication Configuration

If ACS uses Windows databases to authenticate users, you must perform additional configuration for reliable user authentication and group mapping. Requirements vary depending on whether you installed the remote agent on a domain controller or member server.

This section contains:

- [Configuring for Domain Controller Authentication](#)
- [Configuring for Member Server Authentication](#)

Configuring for Domain Controller Authentication

When ACS Remote Agent for Windows 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 subsequent steps are always applicable when the remote agent 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 those that apply to your Windows networking configuration:

-
- Step 1** Add CISCO workstation.
- To meet Windows requirements for authentication requests, ACS must specify the Windows workstation in to which the user tries 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 remote agent depends on the Server service, which is a standard service in Microsoft Windows. On the computer that is running the remote agent, 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. 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.

ACS supports authentication of Windows credentials by using LAN Manager (LM), NTLM version 1, or NTLM version 2, protocols. LAN Manager is the weakest protocol and NTLM version 2, is the strongest. You can support one or more protocols, but must 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 that performs user authentication has the Windows 2000 Service Pack 2 or the Microsoft hot fix KB893318. Refer to 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.

**Tip**

If you upgraded or reinstalled the remote agent, 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 the remote agent service.

In the domain of the domain controller that is running the remote agent, you must have a domain user account that you can use to run the remote agent service (as explained in subsequent steps in this procedure).

- a. Create a domain user account. Use this user account to run the remote agent service. The user account does not require any particular group membership in the domain.

**Tip**

Give the user 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 user account that you create, grant **Read all properties** permission for all Active Directory (AD) folders containing users that ACS must be able to authenticate. To grant permission for AD folders, access AD from the Microsoft Management Console (MMC) 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 Active Directory](#).

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 the remote agent, and you completed this step for the previous installation, it is required only if you want to use a different user account to run the remote agent service.

For the user 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.

**Note**

To run the Remote Agent, the user account must be a member of the local or domain admin. For more information, see [Configuring Local Security Policies](#).

Step 6 Configure services.

**Note**

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

Configure the remote agent service to run as the user that you added to the security policies in the preceding step.

For more information, see [Configuring the Remote Agent Service](#).

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 the remote agent.
- 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 Windows Internet Name Service (**WINS**) tab.
- c. Configure NetBIOS as applicable.

For more information, see the appropriate Microsoft documentation.

Step 8 Ensure DNS operation.

Especially for authentication of users in AD, the remote agent requires 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 the remote agent, configure the network connection that the remote agent 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. 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 or 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 the remote agent 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 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 the appropriate Microsoft documentation.

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 the remote agent 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 the remote agent 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 member server authentication:

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, ensure that you verify that the computer on which the remote agent runs belongs to the correct domain.



Tip

To determine domain membership of a computer, on the Windows desktop, choose **My Computer > Properties > Network Identification**, and read the information under that tab.

If the computer that is running the remote agent 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, child and in each trusted domain through which ACS authenticates 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 the remote agent, 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 belonging 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 the weakest protocol and NTLM version 2 is the strongest. You can support one or more protocols, but must 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; 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 setting in step a, if you 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. Refer to 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 the remote agent, and you completed this item previously, this step is required only if you want to use a different user account to run the remote agent service.

The domain of the domain controller that is running the remote agent must contain a domain user account that you can use to run the remote agent service (as explained in subsequent steps of this procedure).

- a. Create a domain user account. Use this user account to run the remote agent service. The user account does not require any particular group membership in the domain.

For more information on creating a domain user account, see the Microsoft website.



Tip

Give the user 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 with failed ACS authentication attempts.

- b. To the user account that you create, grant **Read all properties** permission for all AD folders containing users that ACS must authenticate. To grant permission for AD folders, access AD by using the MMC 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 Active Directory](#).

Step 6 Configure local security policies.

To the user 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.

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

Step 7 Configure services.

Configure the remote agent service to run as the user that you added to the security policies in the preceding step.

For more information, see [Configuring the Remote Agent Service](#).

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 the remote agent computer.
- 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:

- 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 appropriate Microsoft documentation.

Step 9 Ensure DNS operation.

Especially for authentication of users in AD, the remote agent 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. Moreover 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 the remote agent, configure the network connection that the remote agent 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 appropriate Microsoft documentation.

Step 11 Configure WINS.

If ACS must authenticate users belonging to a trusted or child domain, and if the remote agent 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 the remote agent, configure an *LMHOSTS* file to include entries for each domain controller containing users that ACS must authenticate. You should also include domain controllers of child domains.

**Tip**

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

For more information, see the appropriate Microsoft documentation.

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. The remote agent 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 that you intend to use to run the remote agent. For full configuration requirements, see the applicable procedure:

- [Configuring for Member Server Authentication](#)
- [Configuring for Domain Controller Authentication](#)

To configure local security policies:

Step 1 By 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 click **User Rights Assignment**.

The Local Security Settings window displays a list of policies with associated settings. You must configure these two policies:

- 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, enter 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:

- **Connect as**—Enter 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, enter *CORPORATE\echamberlain*.
- **Password**—Enter 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 configure 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 in the policies 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 now has the required privileges to run the remote agent service and support Windows authentication.

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

Configuring the Remote Agent Service

Before You Begin

This procedure is required only if one of the following conditions is true. The remote agent 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 that you intend to use to run the remote agent and assigned it the permissions necessary to run the remote agent service. 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 the remote agent.

- 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 service installed to support the remote agent appears in the lists of services as Cisco Secure ACS Agent. The service name is **CSAgent**.

Step 4 For the remote agent service:

- a. In the list of services, right-click the CiscoSecure ACS Agent service and, from the shortcut menu, choose **Properties**.

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

- b. Click the **Log On** tab.
- c. Click the **This account** option.
- d. In the box next to the **This account** option, enter 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, enter *CORPORATEACSuser*.

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

You must configure the **CSAgent** service to run by using the privileges of the user account.

Step 5 To restart the **CSAgent** service:

- a. On the Computer Browser Properties (Local Computer) dialog box, click the **General** tab.
- b. Click **Stop**.

The Service Control dialog box appears while the service is stopping.

- c. Click **Start**.

The Service Control dialog box appears while the service is starting.

The remote agent service runs by using the privileges of the user account specified.
