Installation of Cisco Secure ACS Remote Agent for Windows

This chapter provides information about installing Cisco Secure ACS Remote Agent for Windows.

This chapter contains the following topics:

System Requirements

The computer running Cisco Secure ACS Remote Agent for Windows must meet the minimum requirements detailed in the sections that follow.

Cisco Secure ACS Requirements

You must use Cisco Secure ACS Remote Agent for Windows, version 3.3, with Cisco Secure ACS Solution Engine, version 3.3. Other releases of Cisco Secure ACS are not supported.

Hardware Requirements

The computer running Cisco Secure ACS Remote Agent for Windows must meet the following minimum hardware requirements:

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

Operating System Requirements

The computer running Cisco Secure ACS Remote Agent for Windows must use one of the following operating systems:

- Windows 2000 Server, with Service Pack 3 or Service Pack 4 installed.
- Windows 2000 Advanced Server, with the following conditions:
  - 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 multi-processor 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

For the most recent information about tested operating systems, see the *Release Notes for Cisco Secure ACS Solution Engine*. The current version of the Release Notes are posted on Cisco.com (http://www.cisco.com).

Network Requirements

Your network must meet the following requirements before you begin installing Cisco Secure ACS.

- The computer running Cisco Secure ACS Remote Agent for Windows must be able to ping the Cisco Secure ACS Solution Engines that it supports.
- Gateway devices must permit traffic between the computer running Cisco Secure ACS Remote Agent for Windows and the Cisco Secure ACS Solution Engine. Specifically, the remote agent must receive TCP communication on TCP ports you configure in CSAgent.ini. The default TCP ports, if all services are used, are 2004, 2005, 2006, and 2007. The appliance must receive TCP communication on TCP port 2003.

Note Using the CSAgent.ini file, you can configure the ports used by the remote agent to communicate with Cisco Secure ACS. If you change the ports used, 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, page 4-1.

Installing a Remote Agent for Windows

Use this procedure to install Cisco Secure ACS Remote Agent for Windows.

Before You Begin

Determine the IP address of the Cisco Secure ACS Solution Engine that is to be the configuration provider for this remote agent. For more information about configuration providers, see Configuration Provider, page 1-3.

If you want Cisco Secure ACS to authenticate users with a Windows domain user database, after you install the remote agent you must perform additional Windows configuration, discussed in Windows Authentication Configuration, page 2-7.

To install Cisco Secure ACS Remote Agent for Windows, follow these steps:

Step 1 Using the local administrator account, log in to the Microsoft Windows server on which you want to install Cisco Secure ACS.

Step 2 Insert the Cisco Secure ACS CD into a CD-ROM drive on the Microsoft Windows server.

If the CD-ROM drive supports the Windows autorun feature, a dialog box may appear.

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

Step 3 If a dialog box appears, click **Cancel**.

Step 4 On the Cisco Secure ACS Solution Engine CD, locate the Windows remote agent subdirectory.

Step 5 From the Windows remote agent subdirectory, run `Setup.exe`.

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

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

The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. This is the drive and path to which the setup program installs Cisco Secure ACS Remote Agent for Windows.

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

a. Click **Browse**.

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

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

Note The installation location must be on a drive local to the Windows server.

c. Click **OK**.

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

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

Step 8 Click **Next >**.

The Agent Services dialog box lists options supported by Cisco Secure ACS Remote Agent for Windows:

- Logging Service
- Windows Authentication Service

Step 9 Select the agent services you want to use, and then click **Next >**.

The Configuration Provider dialog box appears.

Step 10 In the Hostname box, type the hostname or IP address of the Cisco Secure ACS Solution Engine that should control the configuration of this remote agent.

Note If you type a hostname, be sure either that DNS is operating correctly or that the appliance hostname is in the local hosts file.

Step 11 Click **Next >**.

The setup program installs Cisco Secure ACS Remote Agent for Windows.

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

Step 12 Select the reboot option you want.

Note Rebooting is required to complete installation successfully. If you chose not to reboot now, do so before attempting to use remote agent services.

Step 13 Click **Finish**.

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

Step 14 If want to authenticate users with a Windows domain user database, you must perform the additional Windows configuration discussed in Windows Authentication Configuration, page 2-7.

Note If you are reinstalling the remote agent after uninstalling it, previous configuration of the remote agent service was lost during the uninstallation. For more information, see Windows Authentication Configuration, page 2-7.

Uninstalling Cisco Secure ACS Remote Agent for Windows

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

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

Upgrading Cisco Secure ACS Remote Agent for Windows

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

To upgrade Cisco Secure ACS Remote Agent for Windows software, follow these steps:

Step 1 Remove the old version of the remote agent by performing the steps in Uninstalling Cisco Secure ACS Remote Agent for Windows, page 2-6.

Step 2 Using the version of Cisco Secure ACS Remote Agent for Windows that you want to upgrade to, perform the steps in Installing a Remote Agent for Windows, page 2-3.

Windows Authentication Configuration

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

This section contains the following topics:

Configuring for Domain Controller Authentication

When Cisco Secure 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 upon your Windows networking configuration. Some of the steps below 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 that apply to your Windows networking configuration.

Step 1 Add CISCO Workstation.

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

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

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

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

Step 2 Verify Server Service Status.

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

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

Step 3 Verify NTLM Version.

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

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

For more information, see Microsoft.com: LAN Manager authentication level.

Step 4 Create User Account.

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

Tip If you have uninstalled and 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.

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

1. Create a domain user account. This is the user account that you will use to run 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 "CSACS". If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems related to failed Cisco Secure ACS authentication attempts.

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

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

For more information, see Windows 2000 Server Active Directory.

Step 5 Configure Local Security Policies.

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

Tip If you have uninstalled and 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 created in the preceding step, add the user to the following local security policies:

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

For more information, see Configuring Local Security Policies, page 2-17

Step 6 Configure Services.

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

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

For more information, see Configuring the Remote Agent Service, page 2-21

Step 7 Enable NetBIOS.

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

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

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

For more information, see the following references:

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

Step 8 Ensure DNS Operation.

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

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

Step 9 Specify DNS Suffixes.

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

On the domain controller running 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. To do so, access the advanced TCP/IP properties of the network connection, select the DNS tab, and configure the **Append these DNS suffixes** list, as applicable.

For more information, see the following references:

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

Step 10 Configure WINS.

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

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

Step 11 Configure LMHOSTS File.

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

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

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

For more information, see the following references:

1. Microsoft.com: LMHOSTS File
2. The example LMHOSTS file included with the Windows operating system. The default location and filename for the sample file is *%systemroot%*\system32\drivers\etc\lmhosts.sam

Configuring for Member Server Authentication

When the remote agent runs on a member server and you need to authenticate users with a Windows user database, the additional configuration required varies, depending upon your Windows networking configuration. Most of the steps below are always applicable when 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.

Step 1 Verify Domain Membership.

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

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

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

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

Step 2 Add CISCO Workstation.

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

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

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

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

Step 3 Verify Server Service Status.

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

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

Step 4 Verify NTLM Version.

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

For more information, see Microsoft.com: LAN Manager authentication level.

Step 5 Create User Account.

Tip If you have uninstalled and reinstalled the remote agent and you completed this item previously, it is required only if you want to use a different user account to run the remote agent service.

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

1. Create a domain user account. This is the user account that you will use to run 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 “CSACS”. If you enable audit policies, Event Viewer entries with this username will make it easier to diagnose permissions problems related to failed Cisco Secure ACS authentication attempts.

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

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

For more information, see Windows 2000 Server Active Directory.

Step 6 Configure Local Security Policies.

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

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

For more information, see Configuring Local Security Policies, page 2-17

Step 7 Configure Services.

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

For more information, see Configuring the Remote Agent Service, page 2-21

Step 8 Enable NetBIOS.

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

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

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

For more information, see the following references:

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

2. Microsoft.com: Install WINS in Windows Server 2003

Step 9 Ensure DNS Operation.

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

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

Step 10 Specify DNS Suffixes.

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

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

For more information, see the following references:

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

Step 11 Configure WINS.

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

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

Step 12 Configure LMHOSTS File.

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

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

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

For more information, see the following references:

1. Microsoft.com: LMHOSTS File
2. The example LMHOSTS file included with the Windows operating system. The default location and filename for the sample file is *%systemroot%*\system32\drivers\etc\lmhosts.sam

Configuring Local Security Policies

Before You Begin

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

- The remote agent runs on a member server and needs to authenticate users with a Windows user database.
- The remote agent runs on a domain controller and needs to authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run the remote agent service. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-12 or Configuring for Domain Controller Authentication, page 2-7.

To configure local security policies, follow these steps:

Step 1 Using the local administrator account, log in to the computer running the remote agent.

Step 2 Choose **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

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

The Local Security Settings window appears.

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

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

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

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

a. Double-click the policy name.

The Local Policy Setting dialog box appears.

b. Click **Add. . .**.

The Select Users or Groups dialog box appears.

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

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

d. Click **Check Names**.

The Enter Network Password dialog box appears.

e. If the Enter Network Password dialog box appears, complete the following fields:

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

Then, click **OK**.

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

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

The Select Users or Groups dialog box closes.

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

g. Click **OK**.

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

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

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

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

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

Step 5 Verify that the security policy settings you changed are in effect on the computer running Cisco Secure ACS. To do so, follow these steps:

a. Close the Local Security Settings window.

The window closes. This is the only way to refresh the information in the Effective Setting column.

b. Open the Local Security Settings window again. To do so, choose **Start > Programs > Administrative Tools > Local Security Policy**.

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

The Local Security Settings window displays an updated list of policies with their associated settings.

d. For the **Act as part of the operating system** policy and again for the **Log on as a service** policy, verify that the username you added to the policy appears in the Effective Setting column.

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

The user account has the required privileges to run the remote agent service and support Windows authentication.

Step 6 Close the Local Security Settings window.

The user account specified has the permissions necessary to run the remote agent service successfully.

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 needs to authenticate users with a Windows user database.
- The remote agent runs on a domain controller and needs to authenticate users in trusted domains or child domains.

You should have already created a user account that you intend to use to run the remote agent service and assigned it the permissions necessary to run the service. For full configuration requirements, see the applicable procedure: Configuring for Member Server Authentication, page 2-12, or Configuring for Domain Controller Authentication, page 2-7.

To configure the remote agent service, follow these steps:

Step 1 Using the local administrator account, log in to the computer running the remote agent.

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

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

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

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

The Windows service installed to support the remote agent appears in the lists of services as CiscoSecure ACS Agent. The service name is `CSAgent`.

Step 4 Configure the CiscoSecure ACS Agent service. To do so, follow these steps:

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. Select 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 "CSACS" in the "CORPORATE" domain, type "CORPORATE\CSACS".

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

f. Click **Apply**.

Note If a confirmation dialog box appears, click **OK**.

The CiscoSecure ACS Agent service is configured to run using the privileges of the user account specified.

Step 5 Restart the CiscoSecure ACS Agent service. To do so, follow these steps:

a. On the Computer Browser Properties (Local Computer) dialog box, select 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 using the privileges of the user account specified.