CHAPTER 4

Installing the Cisco Trust Agent on Windows Operating Systems

This chapter provides system requirement and installation information for installing Cisco Trust Agent (CTA) on Windows operating systems. Read this entire chapter before beginning the installation. There are advanced installation options detailed later in this chapter that you may want to use. For example, before deploying CTA on your network, you can create a custom installation package which allows you to set CTA configuration parameters and provision certificates, and posture plug-ins. Proceeding in this manner could save you time during the CTA deployment process.

See these other chapters for installation instructions for different operating systems:

- Chapter 2, “Installing the Cisco Trust Agent on Linux Operating Systems.”
- Chapter 3, “Installing the Cisco Trust Agent on Macintosh Operating Systems.”

This chapter contains the following sections:

System Requirements for Installation

Before installing Cisco Trust Agent on a Windows operating system, verify that the target system meets the requirements in Table 4-1.

Note CTA 2.1 does not support Windows NT 4.0 Server or Windows NT 4.0 Workstation. CTA 2.0 was the last release to support Windows NT 4.0.

Table 4-1 CTA System Requirements

System Component	Requirement
System	• Pentium II class processor or better • Network connection
Windows Installer (MSI)	Version 2.0 or later.
Free Hard Disk Space	20 MB minimum
Memory	256 MB of RAM
Listening Port	By default, Cisco Trust Agent listens on UDP port 21862. You can configure this port number if necessary. See the "Configuring EAP over UDP Communication" section on page 5-12.
Recommended Supplicant	Cisco Secure Services Client, version 4.1.2 or later

System Component	Requirement
Windows Operating Systems on which CTA 2.1 runs.	• Windows 2000 Professional and Advanced Server, SP4 and Update Rollup 1 • Windows XP Professional, SP1, SP2, and SP3 • Windows XP Home, SP1, SP2,and SP3 • Windows 2003 Server, SP1 and R2
Windows Operating Systems on which CTA 2.1 and Cisco Secure Services Client run.	• Windows 2000 Professional and Advanced Server, SP4 • Windows XP Professional, SP1, SP2 and SP3 • Windows 2003 Server **Note** See the *Cisco Secure Services Client Administrator Guide* for a complete list of operating systems that support CSSC.
Language Support for localized operating systems	All available localized versions of these operating systems support this release of CTA. **Note** Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English. • Windows 2000 Professional and Advanced Server, SP4 and Update Rollup 1 • Windows XP Professional, SP1, SP2, and SP3 • Windows XP Home, SP1, SP2, and SP3 • Windows 2003 Server, SP1 and R2

CTA Scripting Interface

The Cisco Trust Agent Scripting Interface feature allows software developers to write their own scripts to relay posture information, collected on the system, to CTA. The scripts can be written to perform the equivalent functions of a posture plugin. End-users will not need this feature unless they intend to write posture validation scripts.

The Scripting Interface is an optional feature of CTA. See "Installing Optional Features During CTA Installation" section on page 4-8 or "Installing CTA Using an Installation Wizard" section on page 4-11 for information on installing this feature along with CTA.

Cisco Secure Services Client

We recommend the use of the Cisco Secure Services Client, version 4.1.2 (CSSC) with CTA 2.1.103.0 for those customers who perform 802.1x authentication. For customers who deployed the CTA 802.1x Wired Client, with the previous offering of CTA 2.1.103.0, we recommend that you migrate to the Cisco Secure Services Client, version 4.1.2.

CSSC sends posture and authentication information, collected by CTA, using the IEEE 802.1x transport protocol to 802.1x-enabled access devices, such as an Ethernet switch, to the Cisco Secure Access Control Server (ACS). After successful client-server authentication, the port access control on the Ethernet switch allows the end-user to connect to the network.

If the NAC deployment in your enterprise uses network routers, or if your network switches communicate with CTA using the EAPoverUDP protocol, you do not need to install CSSC on the same computer as CTA.

Note CSSC is only available for Windows installations. Its default configuration supports only wired network access but it may be upgraded to support wireless network access as well. Learn more about Cisco Secure Services Client at http://www.cisco.com/en/US/products/ps7034/index.html.

Installation File

The CtaAdminEx-win-2.1.103.0.exe installation file is available for download at http://www.cisco.com/cgi-bin/tablebuild.pl/cta by registered users of Cisco.com.

Note These files are not available for download with this release of CTA 2.1.103.0:

- ctasetup-win-2.0.x.y.exe

- ctasetup-supplicant-2.0.x.y.exe
- CtaAdminEx-supplicant-win-2.1.103.0.exe

CtaAdminEx-win-2.1.103.0.exe contains the CTA end-user license agreement (EULA) and the ctasetup-win-2.1.103.0.msi installation file. By running the CtaAdminEx-win-2.1.103.0.exe file, you accept the EULA for all users and extract the ctasetup-win-2.1.103.0.msi installation file. You can use standard MSI commands or an installation wizard to install CTA 2.1.103.0 with or without the Scripting Interface.

If you intend to perform 802.1x authentication, we recommend you use the Cisco Secure Services Client (CSSC) as the supplicant. CSSC is downloaded and installed separately from CTA 2.1.103.0. Registered users of Cisco.com can download CSSC 4.1.2 by clicking this link and following the link to "Download Software" http://www.cisco.com/en/US/products/ps7034/index.html.

Installing Cisco Trust Agent

Cisco Trust Agent installation files are standard Microsoft Windows Installation (MSI) files. Once deployed to the end-point, you can use standard MSI commands to install CTA silently, without user-interaction, or allow users to perform the installation using an installation wizard.

General Installation Instructions

This is the outline of tasks required to install Cisco Trust Agent.

Step 1 Run the CtaAdminex-win-2.1.103.0.exe file and accept the EULA. The ctasetup-win-2.1.103.0.msi file is extracted. See the "Installation File" section on page 4-4 for an explanation of these files.

Step 2 (Optional) Create a custom installation package which could contain ACS root certificate, posture plugins, or a customized CTA configuration file. See the "Installing CTA Using a Custom Installation Package" section on page 4-19 for an explanation of these procedures.

Step 3 Install CTA by distributing the ctasetup-win-2.1.103.0.msi file to end-users alone or as part of a custom installation package. You can use standard MSI commands to specify the features installed with CTA and the level of user interaction.

See the "Installing CTA Using MSI Commands" section on page 4-6 and "Installing CTA Using an Installation Wizard" section on page 4-11 for descriptions of the different installation methods.

Step 4 Install Cisco Secure Access Control Server (ACS) root certificate on the end-point if not distributed as part of a custom installation package. See "About The ACS Server Root Certificate" section on page 8-3 for information about installing this certificate separately.

Step 5 Verify CTA installation.

Installing CTA Using MSI Commands

Standard MSI commands can be passed to the Microsoft Windows Installer through command-line options. These commands determine what features to install as well as the level of user interaction.

This section describes the most common MSI commands.

Note For more information on MSI installation commands see the Microsoft Windows Installer SDK at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_windows_installer.asp

- Installation Command
- Uninstallation Command
- Reinstalling or Repairing CTA
- Creating a Log File While Installing CTA
- Installing Optional Features During CTA Installation
- Specifying Installation Directory
- Specifying Reboot Options
- Setting User Interface Mode

Installation Command

To install CTA using MSI command line options, you must know the name and path of the ctasetup-win-2.1.103.0.msi installation file and use the "/I" option with the Msiexec.exe command. The command can be entered from any prompt. See the following example:

Msiexec.exe /I "*C:\Path_To_MSI\ctasetup-win-2.1.103.0.msi*"

This command installs CTA using an installation wizard. Users accept the EULA, choose what features to install, and the installation directory.

Uninstallation Command

To uninstall CTA using MSI command line options, you must know CTA's ProductCode or "GUID." To find the GUID, follow this procedure:

Step 1 Open the Windows Registry Editor.

Step 2 Navigate to **HKEY_LOCAL_MACHINE**\Software\Cisco Systems\Cisco Trust Agent.

The value of the **ProductCode** registry key, including the curly brackets, is the GUID.

To uninstall Cisco Trust Agent, use the /X option with Msiexec.exe command. The command can be entered from any prompt. See the following example:

```
Msiexec.exe /X {GUID}
```

Reinstalling or Repairing CTA

To reinstall or repair CTA from using MSI command line options, run the MSI installation file using the MSI "/F" option. The full command can be run from any prompt. See the following example:

```
Msiexec.exe /fmosu "C:\Path_To_MSI\ctasetup-win-2.1.103.0.msi"
```

The /fmosu argument performs these actions:

f – Reinstalls package

m - Rewrites all required computer-specific registry entries.

o - Reinstalls if file is missing or if an older version is installed.

s - Overwrites all existing shortcuts.

u - Rewrites all required user specific registry entries

Using this command users see messages asking them to wait while CTA is being configured.

Creating a Log File While Installing CTA

To create a log file during installation, run the MSI installation file using the MSI "/L" option. The full command can be entered from any prompt. This logging option requires that the log directory exist and is writable. The log file itself may not exist but the file name must be specified in the command. See the following example:

```
Msiexec.exe /I "C:\Path_To_MSI\ctasetup-win-2.1.103.0.msi" /L*V
"C:\ctalogfile.txt"
```

The `/L*V` option performs these actions:

L – Creates a log file

*V – Specifies verbose logging.

Installing Optional Features During CTA Installation

The ADDLOCAL option allows you to install the Scripting Interface feature along with CTA. This example shows using the ADDLOCAL option to install the Scripting Interface feature:

```
Msiexec.exe /I "C:\Path_To_MSI\ctasetup-win-2.1.103.0.msi"
ADDLOCAL=Scripting_Interface
```

Note The ADDLOCAL command can be used with an interactive installation or a silent installation. (See the "Setting User Interface Mode" section on page 4-10 for information about "silent" and "interactive" installations.)

Specifying Installation Directory

By default, the ctasetup-win-2.1.103.0.msi installation file installs CTA in the "\ProgramFiles\Cisco Systems" directory of the local drive. You can use the "INSTALLDIR" MSI command to specify a different directory. The directory does not have to exist before you issue the command. See the following example:

```
Msiexec.exe /I "C:\Path_To_MSI\ctasetup-win-2.1.103.0.msi"
INSTALLDIR="D:\NewDirectory"
```

This command shows users the installation wizard. During the installation, users will still have an opportunity to change the destination directory.

Specifying Reboot Options

By default the Microsoft Windows Installer determines when a reboot of the system is necessary and automatically prompts the user to reboot at the end of the installation. You can customize this action by using the Microsoft Windows Installer property called "REBOOT." This property forces or suppresses certain system prompts for a reboot. The behavior of the REBOOT option also depends on whether the end-user is following an installation wizard or the installation is being performed silently.

The REBOOT property has three options:

- **Force** - If end-users perform the installation using an installation wizard, they will be prompted to reboot the system after the installation. If the installation is silent, the system reboots automatically without prompting the user.
- **Suppress** - If end-users perform the installation using an installation wizard, they will not be prompted to reboot the system at the end of the installation. If a reboot is required in the middle of an installation, end-users will be prompted to reboot system. If the installation is silent, end-users will not be prompted to reboot at the end of the installation. If a reboot is required in the middle of an installation, the system will be rebooted automatically without prompting the user.
- **ReallySuppress** - All prompts to reboot the system at the end or during an installation, whether the installation is being performed with an installation wizard or is silent, are suppressed.

This is an example of using the REBOOT option with the Force value:

```
Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" REBOOT=Force
```

Setting User Interface Mode

By default, CTA's MSI files provide users with an installation wizard. Using various MSI commands, you can control how much the user is involved in CTA's installation.

For a full description of how the installation wizard works, see the "Installing CTA Using an Installation Wizard" section on page 4-11.

The command options in the following table specify the amount of end-user interaction with the CTA installation:

Table 4-2 User Interface MSI Command Line Options

Command Option	Description
/q, /qn	There is no user interaction. This provides a silent installation. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /q`
/qb	Users see messages alerting them that CTA is being configured, however, users are not prompted perform any action. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /qb`
/qr	Users see some of the installation wizard windows including a progress bar showing installation, however, users are not prompted perform any action. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /qr`
/qf	Users are fully involved in the installation of CTA. They install CTA using the installation wizard. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /qf`

Command Option	Description
/qn+	Users receive a pop-up message at the end of the installation specifying the success or failure of the installation. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /qn+`
/qb+	Users see messages alerting them that CTA is being configured, however, users are not prompted perform any action during the installation. At the end of the installation users receive a pop-up message that specifies the success or failure of the installation. Example: `Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi" /qb+`

Tip When combining MSI options, specify the user interface command at the end of the entire command. For example, the following command installs CTA with the Scripting Interface, logging is turned on, and users experience basic user interaction with a final pop-up message.

```
Msiexec.exe /I "C:\ctasetup-win-2.1.103.0.msi"
ADDLOCAL=Scripting_Interface /L*V "C:\logfile.txt" /qb+
```

Installing CTA Using an Installation Wizard

This section describes installing CTA and the Scripting Interface by following an installation wizard. You must have administrator privileges on the client to install CTA.

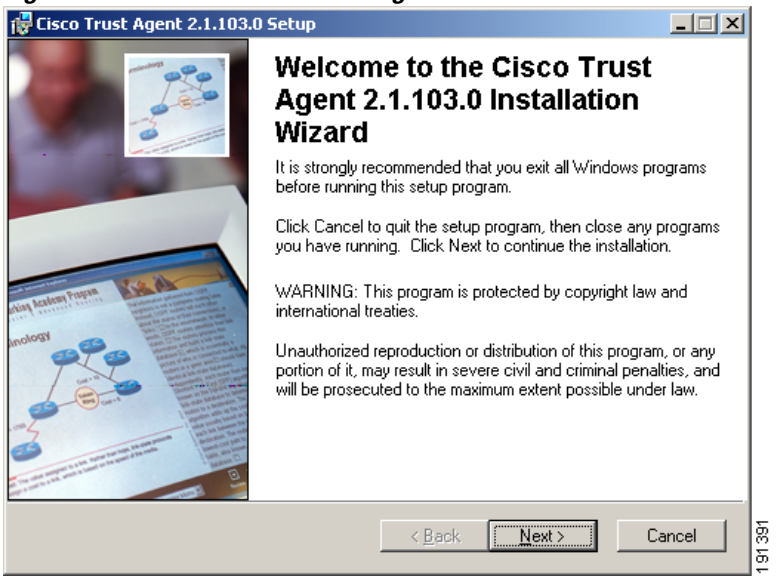
Note If the group policy for the target system allows for elevated privileges for the MSI, then users with Standard or Restricted privileges can install CTA. To use the elevated privileges, MSI 2.0 must be installed before you begin the CTA installation. You cannot use a custom installation package to install the MSI unless you have administrator privileges.

Step 1 Read the "General Installation Instructions" section on page 4-5.

Step 2 Exit all Windows programs.

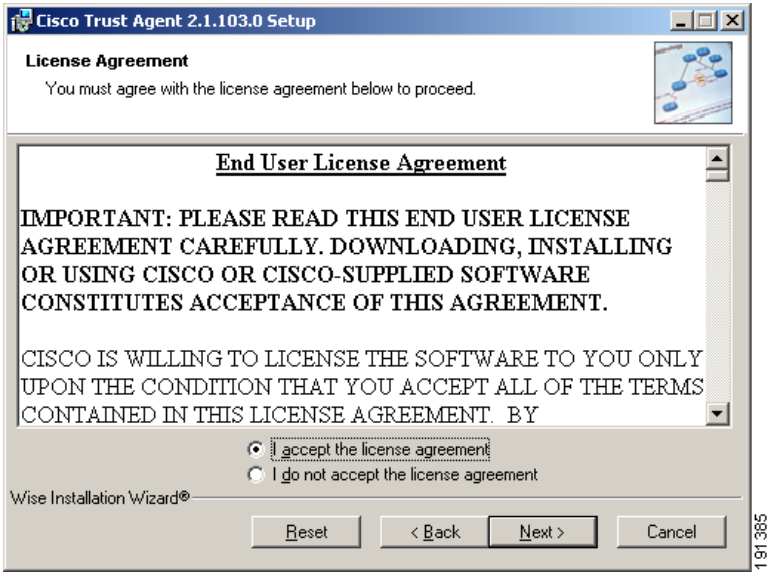
Step 3 Launch the appropriate ctasetup-win-2.1.103.0.msi file by issuing the proper MSI command line option or by double-clicking the file. The Cisco Trust Agent **Installation Wizard** opens as shown in Figure 4-1.

Figure 4-1 The Cisco Trust Agent Installation Wizard



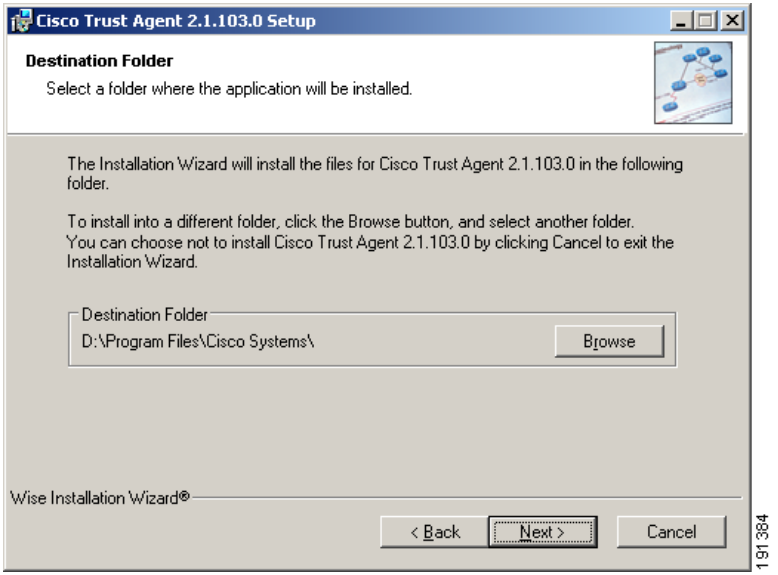
Step 4 Click **Next.** The **License Agreement** window opens as shown in Figure 4-2.

Figure 4-2 The License Agreement on Windows



Step 5 Accept the license agreement by selecting the **I accept the license agreement** radio button and by clicking **Next**. The Destination Folder window opens as shown in Figure 4-3.

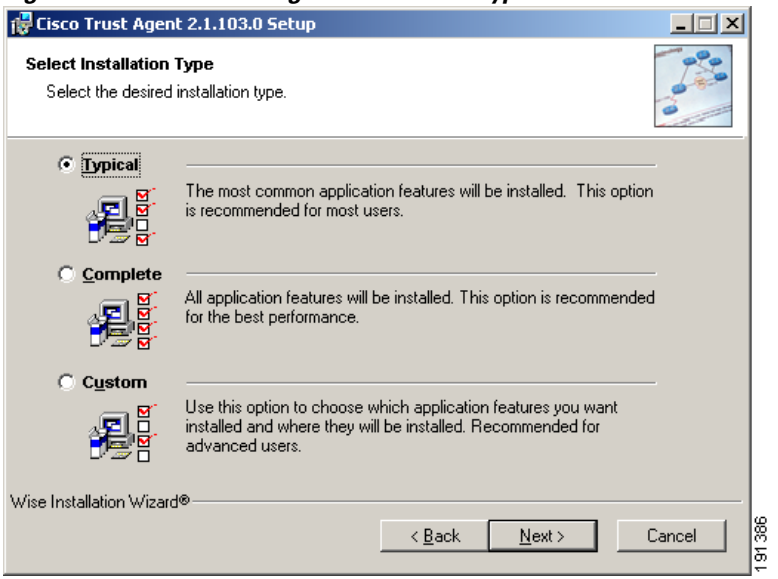
Figure 4-3 The Destination Window



Step 6 Click **Next** to accept the default destination folder or click **Browse** and navigate to the desired drive and folder and then click **OK**. The new install location appears in the **Destination Folder** pane. Click **Next** to install CTA in the folder you specified.

Step 7 The **Select Installation Type** dialog box opens (Figure 4-4).

Figure 4-4 Selecting an Installation Type

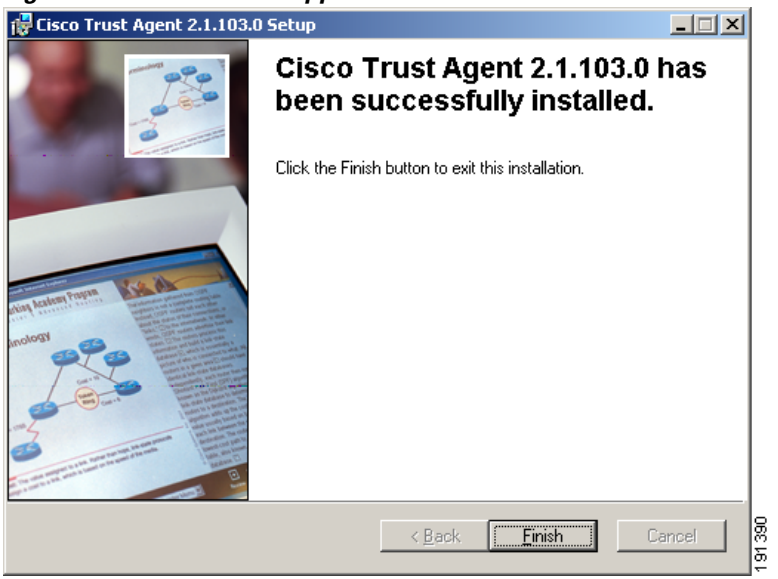


Selecting **Typical** will install CTA. The Scripting Interface is an optional feature and it is not installed during a **Typical** installation.

Selecting **Complete** installation will install the Scripting Interface feature along with CTA.

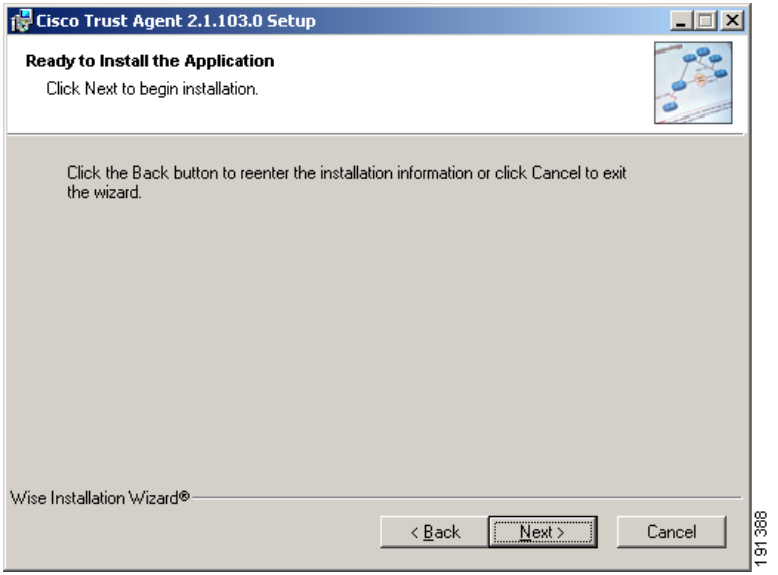
Selecting **Custom** installation will allow you to include or exclude any features available with the installation file. Figure 4-5 shows how you can select the Scripting Interface feature during a **Custom** installation.

Figure 4-5 Choose Application Features



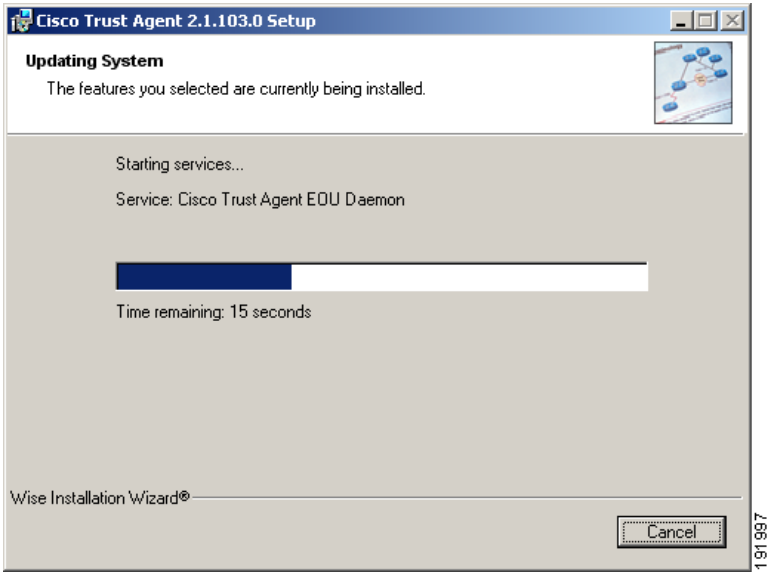
After choosing an installation type and selecting a CTA feature, click **Next**. The **Installing the Application** window opens as shown in Figure 4-6.

Figure 4-6 Installing the Application



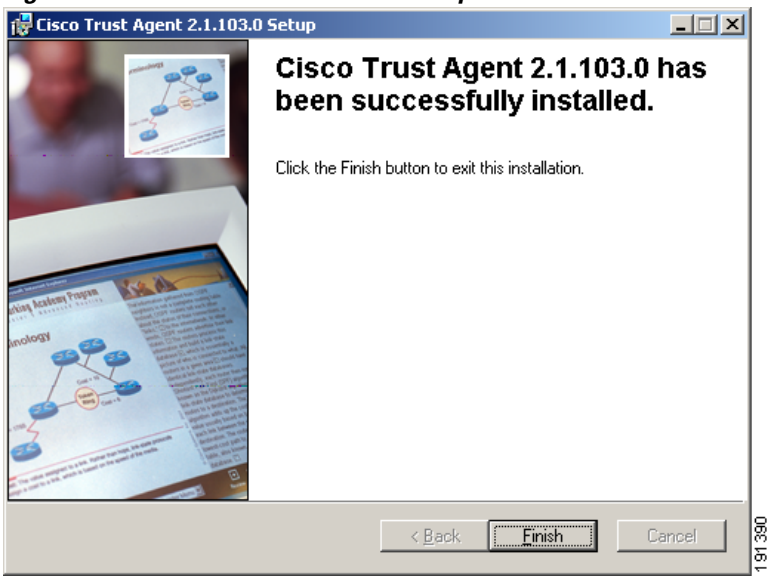
Step 8 Click **Next.** The application installs in the selected directory. Figure 4-7 illustrates the window that shows the progress of the installation.

Figure 4-7 The System is Being Updated



When the installation has completed, the installer displays the **Installation Completed** window as shown in Figure 4-8.

Figure 4-8 The Installation is Complete



Step 9 Click **Finish**. You do not need to restart your machine after installation.

Note For CTA to establish a secure form of communication with the Cisco Secure ACS server, you must have either a CA certificate or a matching root certificate from the Cisco Secure ACS server installed on the system. Refer to "About The ACS Server Root Certificate" section on page 8-3 for information.

Installing CTA Using a Custom Installation Package

Use this section as an example of how to create a customized CTA installation.

The CTA install application is a single executable file. To create a custom installation package, you create a directory structure which includes the desired CTA installation file, .ini files, plugin subdirectories and certificate subdirectories. This directory structure can then be distributed by a software deployment mechanism, such as a script or a software deployment tool.

After the software deployment mechanism distributes the directory structure to the remote network clients, it runs the CTA installation file with the desired MSI command line options. The CTA installation file copies the contents of the directory structure to the proper locations on the remote network client. The software deployment mechanism does not recompile the CTA installation file to create a custom installation.

Please read this entire procedure before beginning. There are options detailed later in the instructions that you should be aware of before beginning.

These are the procedures you need to follow to create a custom installation package:

Step 1 Install CTA on the Administrator's Client

Step 2 Create the Custom Installation Directory Structure

Step 3 Customize the Installation Directory

Step 4 Run the CTA Installation File to Install the Custom Package

Install CTA on the Administrator's Client

Before you create the custom installation package, install CTA on the client you will use to create the custom installation package. This will install the template ctad.ini file and familiarize you with CTA's installation process. Use the "Installing CTA Using an Installation Wizard" section on page 4-11 to install CTA.

Create the Custom Installation Directory Structure

Step 1 Create an empty directory on your network client. For example, D:\CTA\Custom_Package

Step 2 Open a command prompt.

Step 3 CD to the directory which contains the **CtaAdminEx-win-2.1.103.0.exe** file. (See the "Installation File" section on page 4-4 for a description of this file.)

Step 4 After the prompt, on one line, type the name of the CtaAdminEx-win-2.1.103.0.exe file followed by a -p switch and the path to the directory you created in Step 1 of this procedure. This will extract the ctasetup-win-2.1.103.0.msi file to the new directory. For example:

```
D:\CTA>CtaAdminEx-win-2.1.103.0.exe -p D:\CTA\Custom_Package
```

Note If you do not use the -p switch in the command, the ctasetup-win-2.1.103.0.msi is extracted to the same directory that contains the CtaAdminEx-win-2.1.103.0.exe file.

Note If you want to create a custom installation package for a wizard-driven installation, copy the ctasetup-win-2.1.103.0.msi to the Custom_Package directory.

Step 5 When prompted, read and accept the End User License Agreement (EULA) on behalf of all users by typing **Y** and pressing **<Enter>**. After the CTA installation file has been extracted, a message is returned showing the path to which the installation file was extracted. In our example, you should now have a D:\CTA\Custom_Package directory with one file in it: ctasetup-win-2.1.103.0.msi

Step 6 Proceed to "Customize the Installation Directory."

Customize the Installation Directory

The customization choices in this procedure are optional. However, you will find that including some of these customizations is worthwhile. CTA is not a centrally managed product. If you do not plan to use the product defaults, it is to your benefit to pre-configure all available product settings before deploying CTA.

Step 1 Create a **certs** subdirectory. For example: D:\CTA\Custom_Package**certs**

Copy the root certificate for your Cisco Secure ACS server to this directory. During installation, any certificates in this directory are added to the systems root certificate store.

If your Cisco Secure ACS server uses self-signed certificates, see the Cisco Secure ACS documentation for information about obtaining the certificate; if you use a CA server, refer to your CA server documentation.

Note This step is not required if a CA certificate or ACS root certificate have already been distributed to the network clients receiving this customized CTA installation. If these certificates have not been distributed, this step is required.

Step 2 Create a **plugins** subdirectory. For example: D:\CTA\Custom_Package**plugins**

Copy any third-party plugins that you want to provision at installation time into this directory.

Step 3 Create a new **ctad.ini** file and store it in the D:\CTA\Custom_Package directory. This file is used to configure CTA communication settings, user notifications, and certificate validation rules. Refer to Chapter 5, "Configuring Cisco Trust Agent" for instructions on how you should create and format this file.

Step 4 Create a new ctalogd.ini file and store it in the D:\CTA\Custom_Package directory. This file is used to enable and disable CTA logging. Refer to Chapter 6, "Cisco Trust Agent Event Logging"for instructions on how you should create and format this file.

Step 5 Proceed to "Run the CTA Installation File to Install the Custom Package."

Run the CTA Installation File to Install the Custom Package

For the sake of this procedure, we assume that the custom package is deployed to the appropriate network clients by a software deployment mechanism such as a software deployment tool or script.

Note The custom package consists of the customized installation directories and the CTA installation .msi file. The installation .msi does not recompile the customized files into a new installation .msi file, it installs CTA and the customized files you created in the "Customize the Installation Directory" section on page 4-21.

Step 1 The software deployment mechanism deploys the custom package to the appropriate network clients and saves it to a local directory. For the sake of this example, we assume that the custom installation package is saved to the C:\Temp directory. There would now be a C:\Temp\Custom_Package directory on the client.

Step 2 The software deployment mechanism can then run the CTA installation file and employ whatever MSI command line options you choose. (See the "Installing CTA Using MSI Commands" section on page 4-6 for a summary of common MSI commands and examples of how they are used with the CTA installation files.)

Here are two different examples of the CTA installation:

Run the CTA installation file as it is, this installs CTA and your customizations. To do so, the software deployment mechanism would run the following commands:

a. CD to the C:\Temp\Custom_Package directory.

b. From the prompt, run the **ctasetup-win-2.1.103.0.msi** file. For example:

C:\Temp\Custom_Package>**ctasetup-win-2.1.103.0.msi**

Run the CTA installation file with MSI command line options. The command in the procedure installs CTA with your customizations, the Scripting Interface, it logs the installation, and stores the log file in "C:\Custom_Package\logfile.txt, and it is a silent installation.

a. CD to the C:\Temp\Custom_Package directory.

b. From the prompt, run the **ctasetup-win-2.1.103.0.msi** file with the MSI command line options. For example:

```
C:\Temp\Custom_Package>Msiexec.exe /I ctasetup-win-2.1.103.0.msi
ADDLOCAL=Scripting_Interface /L*V "C:\Custom_Package\logfile.txt" /qn
```

Upgrading to Cisco Trust Agent, Release 2.1

Cisco Trust Agent supports upgrade installations from versions 1.0, 2.0, 2.0.1, and Selective Availability and Beta 2.1 releases to CTA 2.1.103.0.

The behavior of an upgrade reflects the kind of installation being used. If the upgrade is performed using an installation wizard, CTA 2.1.103.0 recognizes the previous installation of CTA and prompts users to upgrade. In the case of a silent installation, it is assumed that the user intends to perform an upgrade and the installation proceeds without prompting the user.

Upgrade procedures are the same as the installation procedures described in "Installing CTA Using MSI Commands" section on page 4-6, "Installing CTA Using an Installation Wizard" section on page 4-11, and "Installing CTA Using a Custom Installation Package" section on page 4-19.

Upgrading from Cisco Trust Agent, Release 1.0

During an upgrade installation of CTA from 1.0 to CTA 2.1, existing certificates remain in the certificate store in which they were installed during the CTA 1.0 installation. Posture plugins and the ctalogd.ini file are moved to their new location in the CTA 2.1.103.0 directory structure. The ctad.ini file used in CTA 1.0 remains in the directory in which it was originally installed and CTA 2.1.103.0 recognizes the file in its original location.

Upgrading from Cisco Trust Agent, Release 2.0.0.30

During an upgrade installation of CTA from 2.0.0.30 to CTA 2.1.103.0, certificates, third-party posture plugins, ctad.ini, ctalogd.ini, and log files remain in the directories in which they were installed and they are used by CTA 2.1.103.0.

Upgrading from Cisco Trust Agent, Release 2.0.1

Cisco Trust Agent 2.0.1 was a release supported on Windows XP platforms only. During an upgrade installation of CTA from 2.0.1 to CTA 2.1, certificates, third-party posture plugins, ctad.ini, ctalogd.ini, and log files remain in the directories in which they were installed and they are used by CTA 2.1.103.0.

Upgrading from CTA 2.1 Selective Availability and Beta Releases to CTA 2.1.103.0

Some customers of Cisco's Network Admission Control program participated in testing "selective availability" or "limited availability" releases and Beta releases of CTA 2.1 to test its functionality in their NAC environments.

These builds, numbered 2.1.18.0, 2.1.100.0, 2.1.101.0, and 2.1.102.0 may be upgraded to CTA 2.1.103.0. The certificates, third-party posture plugins, ctad.ini, ctalogd.ini, and log files remain in the directories in which they were installed and they are used by CTA 2.1.103.0.

Upgrading Cisco Trust Agent with the CTA 802.1x Wired Client to Cisco Secure Services Client

The *Migrating from CTA 802.1x Wired Client to Cisco Secure Servics Client* document describes how to upgrade 802.1x supplicant used with CTA from the CTA 802.1x Wired Client to Cisco Secure Services Client.

Verifying the Cisco Trust Agent Installation

After Cisco Trust Agent has been installed you will find the following directory structures containing CTA's executable files:

- \Program Files\Cisco Systems\CiscoTrustAgent
- \Program Files\Common Files\PostureAgent

After installing CTA, to verify that CTA is running, follow this procedure:

Step 1 Open a command prompt window on the target system.

Step 2 Type **net start** and then click **Enter**.

Step 3 Verify that the following services are running:

Current Service Names:

- Cisco Posture Server Daemon

- Cisco Systems Inc. CTA Posture State Daemon
- Cisco Trust Agent EoU Daemon
- Cisco Trust Agent Logger Daemon

If these services are not running, reboot the computer and check again. If the services still do not run, reinstall the application.

Uninstalling Cisco Trust Agent on Windows

To uninstall Cisco Trust agent, follow these steps:

Step 1 Choose **Start > Settings > Control Panel > Add/Remove Programs**.

Step 2 Choose **Cisco Trust Agent** from the list of installed applications.

Step 3 Click **Remove**.

A confirmation dialog box appears.

Step 4 Click **Yes** to continue the removal.

Note Certificates and plugin files are not deleted when CTA is uninstalled; they remain on the client.