Release Notes for Cisco Trust Agent, Release 2.1, With Bundled Supplicant

Released for Use with Network Admission Control Framework 2.1

Revised: May 23, 2008

Contents

These release notes are for use with Cisco Trust Agent (CTA), Release 2.1, With Bundled Supplicant. The following information is provided:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Trust Agent 2.1 Release

The goals of Cisco Trust Agent, Release 2.1.103.0 (CTA 2.1) are to improve on the CTA 2.1.18.0 selective availability release by resolving outstanding product defects and to provide new functionality from that offered in the CTA 2.0.0.30 release. Cisco Trust Agent release 2.1 is an integral component of the Network Admission Control Framework 2.1 solution.

The CTA 802.1x Wired Client supplicant is bundled with this offering of CTA 2.1.103.0. The CTA 802.1x Wired Client is available for use on Windows operating systems.

Qualified Deployments of CTA 2.1

Cisco Trust Agent 2.1.103.0 will be distributed to existing customers of CTA and those customers evaluating the NAC Framework 2.1 programs.

CTA 2.1 is not intended for distribution to new customers of CTA nor new customers of the NAC 2.1 Framework solution. New customers to CTA and NAC should work with their Cisco Account Team representative to evaluate their NAC Framework-qualified infrastructure and use-case scenarios.

We are making an extra effort to qualify our customers' infrastructure and goals to ensure that the components in their network are compatible with the NAC Framework, that their goals will be met by the NAC Framework, and that the deployment of the NAC Framework will be successful.

Obtaining the CTA 2.1 Release

CTA 2.1.103.0 is available for download in this location:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

You must agree to the following terms before downloading Cisco Trust Agent Software Update (the "Software"):

In as much as this release of Cisco Trust Agent is intended for existing deployments, by clicking "Accept" below, in addition to any other license terms provided by Cisco with this Software, you on behalf of yourself and the organization you represent (collectively "You") agree to each of the following:

- That You on behalf of yourself and the entity You represent already have Cisco Trust Agent installed and You will use this Cisco Trust Agent download (the "Software") only for the purpose of upgrading Your previously installed version of Cisco Trust Agent (which You are using in accordance with the Cisco license terms governing the previously installed version of Cisco Trust Agent).
- You will keep this Software image confidential and will not provide it to any third party.
- If you are unable to agree to the above terms of use do not download the Software. Please contact your Cisco account team for further assistance.

Product Versioning

The full version number of this release is CTA 2.1.103.0. The full release number is used in installation files names and in the text of the *Administrator Guide for Cisco Trust Agent, Release 2.1* and the *Release Notes for Cisco Trust Agent, Release 2.1* when it is important to distinguish the version of CTA being discussed. Any references in the documentation to CTA 2.1 are referring to CTA 2.1.103.0 unless otherwise noted.

CTA 2.1 Product Limitations

Review these limitations of CTA 2.1 before installing or upgrading to the new release.

CTA 802.1x Wired Client Service Fails to Start Following Upgrade from CTA 2.0 to CTA 2.1

The CTA 802.1x Wired Client fails to start after an upgrade attempt from CTA 2.0.0.30 (CTA 2.0) to CTA 2.1.103.0 (CTA 2.1). In order to upgrade from CTA 2.0 with the CTA 802.1x Wired Client to CTA 2.1 with the CTA 802.1x Wired Client, you will need to uninstall CTA 2.0, delete leftover directories, and then install CTA 2.1 from scratch. See the "Upgrading CTA 2.0 to CTA 2.1" section on page 26 for this upgrade procedure.

New Authentication Profiles Required with Upgrade from CTA 2.0 to CTA 2.1

The user and machine authentication profiles that were created for use with CTA 2.0 are not compatible with CTA 2.1. During an upgrade from CTA 2.0 to CTA 2.1, the authentication profile files are deleted. New authentication profile files will need to be created after upgrading to CTA 2.1 to perform 802.1x authentication with CTA 2.1.

Configuring Machine Authentication

Cisco Trust Agent 2.1 supports machine authentication. However, you should be aware of these caveats when planning the deployment of machine authentication in your NAC environment:

- Some applications may not be appropriate choices to provide posture credentials during machine authentication. Such applications may be slow to start, for example, and they will not be ready to provide posture credentials immediately for machine authentication.

In this case, machine authentication could fail, not because of a security problem but because the application was not available to provide its posture credentials in time.

- In order to perform machine authentication, the EAP-FAST Configuration in ACS must allow machine authentication.
- Machine authentication can be performed on networks where Windows Active Directory is in use.

Windows NT is Not Supported

CTA 2.1 does not support Windows NT 4.0 Server or Windows NT 4.0 Workstation.

CTA is No Longer Bundled with CSA

In the past, CTA installation files have been distributed along with Cisco Security Agent (CSA). This allowed CTA to be distributed in Agent Kits produced and managed by the Cisco Security Agent Management Center. Though CTA may still be incorporated in an Agent Kit and distributed through CSA MC, the CTA installation files are no longer included in CSA distributions.

The CSA 5.1.0.88 and 5.0.0.205 hotfixes have removed all CTA installation files.

Customers who want to distribute CTA through an Agent Kit may do so by downloading the CTA software separately and following the instructions in Appendix B of the *Administrator's Guide for Cisco Trust Agent, Release 2.1*.

New Features Introduced in CTA 2.1

The following sections describe the new features available in Cisco Trust Agent, Release 2.1.

New Product Versioning Methodology

In previous releases of CTA, including the beta delivery of CTA 2.1, CTA product versions were expressed using a four field number; for example, CTA 2.1.0.10 was the product version of a beta release of CTA 2.1. The fields in the version number represent this information:

[Major Version].[Minor Version].[Maintenance Version].[Build Version].

Microsoft Installer (.msi) files are now used to install CTA on Windows operating systems. The Microsoft Installer expects a three field product version number and ignores the fourth field. This would prevent an upgrade of CTA from a release numbered CTA 2.1.0.10 to CTA 2.1.0.103. Microsoft Installer would see these two product builds as identical.

To accommodate the Microsoft Installer files, the product's version number is now represented by a four field number where the first three fields are significant and the last is populated with a zero.

[Major Version].[Minor Version].[Build Version].[0]

Using this new system, CTA can be upgraded from releases CTA 2.1.0.10, CTA 2.1.18.0, or CTA 2.1.100.0, to CTA 2.1.103.0 without uninstalling the previous release.

This number is used in the file naming conventions for the installation files of CTA on all operating systems.

Documentation Title Changes

This release note document, with part number, OL-11311-01, were previously entitled, *Release Notes for Cisco Trust Agent, Release 2.1*. It is now entitled *Release Notes for Cisco Trust Agent, Release 2.1, With Bundled Supplicant*.

The administrator guide, with part number, OL-11310-01, was previous entitled *Administrator Guide for Cisco Trust Agent, Release 2.1*. It is now entitled *Administrator Guide for Cisco Trust Agent, Release 2.1, With Bundled Supplicant*.

These changes are made to distinguish this CTA 2.1.103.0 product offering which includes the CTA 802.1x Wired Supplicant, from the latest CTA 2.1.103.0 product offering which does not include the CTA 802.1x Wired Client. The latest offering of CTA 2.1.103.0 removes the bundled supplicant and recommends the use of Cisco Secure Services Client as the supplicant to be used in a NAC environment.

Single RPM Installation File for Linux Installations

The installation files for CTA for Linux are contained in the **ctaadminex-linux-2.1.103-0.tar.gz** file which can be downloaded from Cisco.com. After downloading the **ctaadminex-linux-2.1.103-0.tar.gz** file, the administrator uncompress the file and runs the **ctaadminex-linux-2.1.103-0.sh** file to accept the license agreement and extract the **cta-linux-2.1.103-0.i386.rpm**. The cta-linux-2.1.103-0.i386.rpm file is then used to install CTA for Linux using standard RPM commands.

The CTA Scripting Interface feature is now installed by default on Linux platforms. There is no CTA 802.1x Wired Client for use with Linux platforms.

Support for CTA on Mac OS X Operating Systems

Cisco Trust Agent, with its standard features and the optional Scripting Interface feature, is now available for installation on Mac OS X operating systems. There is no CTA 802.1x Wired Client for use with Mac OS X platforms.

Microsoft Windows Installer (MSI) Installation Files

There are now two files which you can download and use to install CTA on Windows operating systems:

- CtaAdminEx-win-2.1.103.0.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.

After running the CtaAdminEx-win-2.1.103.0.exe file, the administrator accepts the EULA for all users and the ctasetup-win-2.1.103.0.msi is extracted to the same directory as the CtaAdminEx-win-2.1.103.0.exe file. You use the ctasetup-win-2.1.103.0.msi file to install CTA using standard MSI commands.

You can use the ctasetup-win-2.1.103.0.msi file to install the CTA Scripting Interface feature, however, you can not use the file to install the 802.1x Wired Client feature.

CtaAdminex-supplicant-win-2.1.103.0.exe contains the EULA and the ctasetup-supplicant-win-2.1.103.0.msi installation file. By running the CtaAdminEx-supplicant-win-2.1.103.0.exe file, you accept the EULA for all users and extract the ctasetup-supplicant-win-2.1.103.0.msi installation file. By default, the ctasetup-supplicant-win-2.1.103.0.msi file installs Cisco Trust Agent with the CTA 802.1x Wired Client and provides an option to install Scripting Interface feature. If you do not intend to install the CTA 802.1x Wired Client on some end-points, that feature may also be suppressed using standard MSI commands.

Note Previously the CTA features could be enabled using the "/si" argument to install the scripting interface, and the "/ls" argument for CTA 802.1x Wired Client. Now that the installation files uses standard MSI commands, the /si and /ls arguments are no longer used. See, the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 4, "Installing Optional Features During CTA Installation" for the new commands used to install these features.

New Configuration Options in CTA

Standardized Naming Convention for ctad.ini Template Files

The names of the template files used to create ctad.ini files have been standardized across all platforms. The new name for the file is ctad-temp.ini on all operating systems.

Table 1 ctad-temp.ini Naming Convention and File Location

New Template Name is Standard for All Operating Systems	Old Template Names Used for Different Operating Systems	Location of New Template File
ctad-temp.ini	ctad.ini.windows	\Program Files\Cisco Systems\CiscoTrustAgent\
ctad-temp.ini	ctad.ini.linux	/etc/opt/CiscoTrustAgent/
ctad-temp.ini	ctad.inin.macosx	/etc/opt/CiscoTrustAgent/

New Naming Convention for ctalogd.ini Template File

The names of the template file one could use to create the ctalogd.ini file has been changed to reflect a new file-naming convention in configuration files. The new name of the template file used to create the ctalogd.ini is ctalogd-temp.ini.

Table 2 ctalogd-temp.ini Naming Convention and File Location

New Template Name for All Operating Systems	Old Template Names Used for all Operating Systems	Location of New Template File
ctalogd-temp.ini	ctalogd.tmp	Location on Windows: \Program Files\Cisco Systems\CiscoTrustAgent\Logging\
ctalogd-temp.ini	ctalogd.tmp	Location on Linux: /etc/opt/CiscoTrustAgent/
ctalogd-temp.ini	ctalogd.tmp	Location on Mac OS X: /etc/opt/CiscoTrustAgent/

Configuring User Notifications

The user notification parameters are configured in the ctad.ini file. See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 5, "Configuring User Notifications" for more information about these and other notification parameters.

UserActionDelayTimeout. The **UserActionDelayTimeout** parameter allows you to delay the launch of the browser window so that the host has more time to obtain an IP address. This parameter was added to the ctad.ini file because if the browser that displays the posture message is launched before the host obtains an IP address, the browser will fail to open the URL contained in the posture message This feature is available on Linux, Mac OS X, and Windows operating systems.

EnableLogonNotifies. The behavior of the **EnableLogonNotifies** parameter is now the same on all operating systems. The parameter enables or disables user notification received before the user is logged on. User notifications received before the user is logged on can be saved or discarded.

LogonMsgTimeout. The behavior of the **LogonMsgTimeout** parameter is now the same on all operating systems. The default value of the parameter on all operating systems is 86,400 seconds. The parameter specifies how long, in seconds, a message is saved when no user is logged on and when EnableLogonNotifies enabled.

Configuring CTA and Posture Plugin Interaction

CTA and the posture plugins interact for the transfer of posture data, posture notifications, and status updates. Two new parameters, **PPInterfaceType** and **PPWaitTimeout**, are used together to determine how CTA interacts with the plugins and how long the interaction with all plugins lasts.

See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 5, "Configuring CTA and Posture Plugin Interaction." for a complete explanation of these parameters and how to configure them.

This feature is available for Linux, Mac OS X, and Windows operating systems.

Configuring Posture Plugin Message Size

By default, plugins are permitted to provide 1024 bytes (1KB) of information to CTA. This number can be increased to allow all plug-ins to provide up to 6KB of information. **PPMsgSize** is the parameter in the ctad.ini file which you use to configure the plugin message size.

You can also create an application-specific posture plugin message size by adding the ***PluginName*_PPMsgSize** parameter to the ctad.ini file. This parameter allows you to define a posture message size for a specific plugin.

Note If there is a Symantec posture plugin installed on the client, the ctad.ini file must be configured in one of two ways:

- PPMsgSize must be set to 1024 bytes.
- The Symantec posture plugin must use an application-specific posture plugin set to 1024 bytes.

See, the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 5, "Configuring the Posture Plugin Message Size" for a complete explanation of this parameter and how to configure it.

This feature is available for Linux, Mac OS X, and Windows operating systems.

Configuring CTA for Use with the Windows XP Firewall

The BootTimeUDPExemptions parameter alters the Windows XP Firewall policy and enables CTA to receive packets when the Windows XP SP2 or SP3-based computer is booting.

By enabling BootTimeUDPExemptions you alter the Windows XP Firewall setting by adding CTA's local EAPoUDP port to the Windows XP Firewall boot time UDP exemptions policy. This enables CTA to communicate with ACS over the network.

Note Use of the BootTimeUDPexemptions parameter is relevant only when used in conjunction with Microsoft's hot fix for Windows XP (KB17730)

See *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 5, "ctad.ini Configuration Parameters" for more information about this parameter and how to configure it.

Configuring Logging for Large Deployments

A procedure has been added to the *Administrator Guide for Cisco Trust Agent, Release 2.1* that describes how to configure CTA logging for a large deployment. A sample ctalogd-temp.ini file has also been provided.

See the Administrator *Guide for Cisco Trust Agent, Release 2.1*, Chapter 6, "Configuring CTA Logging for Large Deployments for the procedure.

New Posture Plugin Features

The features in this section are described in the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 7, "Posture Plugins."

Host Posture Plugin Now Returns MAC Address

The Host Posture Plugin reports basic information about the client running CTA to the ACS. With the release of CTA 2.1, the Host Posture Plugin can now return the MAC address of the client running CTA, provided that the MacAddress attribute has been added to the Posture-Validation Attribute Definition File employed by the ACS CSUtil database utility. (For more information about the ACS CSUtil database utility and the Posture-Validation Attribute Definition File, see the *User Guide for Cisco Secure ACS for Windows Server.*)

The attribute information for MacAddress is below.

```
[attr#n]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00009
attribute-name=MacAdress
attribute-profile=in
attribute-type=string
```

The plugin will return all the MAC addresses available on the client running CTA and combine them into one string; the MAC addresses will be separated by pipes (|). For example, a wireless network card and a wired network card will each return a MAC address.

If you are defining a posture validation rule in ACS based on only one of these MAC addresses, the posture attribute should “contain” the MAC address you are verifying rather than “equal” or “start with” the MAC address you are verifying.

This feature is available for Linux, Mac OS X, and Windows operating systems.

Package Information Returned by Host Posture Plugin For Mac OS X

For Mac OS X, there are two types of applications that are of concern to CTA: system applications which have receipts in /Library/Receipts/ and user applications which are installed in /Applications directory.

System applications are identified by the first level folder name under /Library/Receipts, like “Danish.pkg”, “X11SDK.pkg”. User applications are identified by the application name under /Applications directory as displayed in Finder. For example, “Firefox”, “DVD\ Player”.

The applications located in the subfolders of /Applications directory can also be queried, in these cases the package name looks like the relative path to /Applications. For example, “Utilities/Disk\ Utility”, “Zinio/Zinio\ Reader”.

Note White spaces in package names must be escaped with backslash (“\”).

The version information of system applications is parsed out of the Contents/version.plist file under the package's directory under the /Library/Receipts directory. Version information is in the form of “a.b.c.d”. The first three fields of version are from the CFBundleShortVersionString key, and the fourth field is from SourceVersion key. For user application packages, the version information is retrieved from the Info.plist file under the Contents/ directory in the application’s directory. We first look for the value of CFBundleShortVersionString key. If this key is not present we will return the value of CFBundleVersion key. If both keys are missing no information will be returned for the package.

New Features Introduced in CTA 802.1x Wired Client

The user interface for the Cisco Trust Agent 802.1x Wired Client was changed significantly in between CTA 2.0 and CTA 2.0.1, and then revised further for the CTA 2.1 release. The procedures for configuring user and machine authentication have also changed to reflect the new user interface the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "Cisco Trust Agent 802.1x Wired Client."

Differentiating Connected States

In previous versions of the CTA 802.1x Wired Client, the connection state of "Connected" included both authenticated connections and unauthenticated connections. Unauthenticated connections were those where authentication was not required.

The client now differentiates between "connected and authenticated" and "connected and unauthenticated", both in the displayed status text and the coloring pattern of the network/access icons in the CTA 802.1x Wired Client main window and the system tray icon.

A green icon indicates that the network adapter is connected and authenticated. The new blue colored icon indicates that the network adapter is connected but unauthenticated or does not require authentication.

Realtime Information on Connection Process

The main window of the CTA 802.1x Wired Client main window now contains a hotspot labeled "Details." Clicking Details displays the Information window which provides real-time feedback of the individual steps of any (manual or automatic) connection or disconnection process. See, the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "802.1x Wired Client Window" for an illustration and explanation of the Details hot spot.

Connection Status Dialog Enhancements

Several new aspects to the Connection Status informational dialog were added.

- Client (network adapter) MAC address is now displayed.

- Dynamic parameters are now updated in real time.

See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "Viewing Access Device Status" for more information about the status window.

Authentication Retries Enhancement

This feature prevents the CTA 802.1x Wired Client from failing users' authentication attempts before they can be re-routed to a special vlan. This is also referred to as the "Auth-fail VLAN feature" in the NAC environment.

Some more intelligent access devices support special features that have, for example, the ability on a failed connection attempt to open the port but switch the user into a special vlan. In order to support these access devices, the client provides the administrator with the capability on a deployed end-user client of adjusting the number of connection retries before disconnecting, allowing the access device to make intelligent decisions based on multiple authentication failures.

This functionality is available to the user in the Station Policy window in the **Authentication Retries Wired /Ethernet Settings** area. See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "Authentication Retries Wired / Ethernet Settings" for an explanation of this new functionality and a description of the related GUI area.

New "User Identity Protection" Area on Station Policy Window

The Authentication Method area and associated radio buttons have been renamed to better describe the functions represented in the interface. The area is now named the **User Identity Protection** area. The area has these radio buttons:

- Send 'anonymous' in clear
- Send Username in clear.

Note The **Send Username in Clear** radio button choice is compatible with ACS 4.1 and later versions.

See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "User Credentials Area" for an explanation of the function of these radio buttons.

New "Allow Unprotected Client Cert" Area on Station Policy Window

The Use Client Certificate area and associated check boxes on the Station Policy window have been renamed to better describe the functions represented in the interface. The area is now named the **Allow Unprotected Client Cert** area and has these checkboxes:

- Machine Auth (Boot-time)
- User Auth (Logon-time)

See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9, "Allow Unprotected Client Cert Area" for an explanation of the function of these check boxes.

Global Enable Client Control Enhancements

In previous versions of the client, the global control for managing all the adapters was available on the popup menu off of the system tray icon and was labeled "Active" control.

This control has been relabeled as "Enable Client", which is the equivalent to the previous checked Active control, or unchecked "Enable Client", which is the equivalent to the previous unchecked Active control. The new control is also available from an associated drop-down menu. Additionally, this control has been added to the main screen menu bar as part of the 802.1x Wired Client drop-down choices. Otherwise there are no functional changes.

See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 9 "802.1x Wired Client System Tray Shortcut Menu" for more information about this control.

Popup Notifications

The system tray icon autonomous popup "bubble" notification messages have been removed to reduce impact on the user. All useful information is still available via the icon status color and the icon mouse rollover statuses.

New Features Introduced in CTA 2.0.1

The following sections describe the new features that were introduced in Cisco Trust Agent, Release 2.0.1.

CTA 2.0.1 was released only for Windows XP operating systems. The changes and features delivered in CTA 2.0.1 are available in Cisco Trust Agent 2.1.

CTA 802.1x Wired Client System Report Tool

The System Report utility provides end users a simple way to automatically gather data needed by support personnel to troubleshoot any problems. It captures the following information:

- Current end-user technical log contents.
- Current internal application activity log.
- Information on the machine's hardware and software environment.

The System Report utility is packaged with the CTA 802.1x Wired Client and automatically installed with the CTA 802.1x Wired Client, however, it is a separate utility and it operates whether the CTA 802.1x Wired Client is active or not.

The System Report utility creates a single compressed file, the System Report, that contains information about the end station's hardware and software environment, the CTA 802.1x Wired Client, as well as the gathered technical and developer logs.

You can launch the System Report Tool by navigating Start > Programs > Cisco Systems, Inc. > Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client System Report.

CTA 802.1x Wired Client Technical Log

The technical log file is a time-stamped, Unicode text file that is the destination for log messages capable of being viewed with Microsoft Notepad (or equivalent) on Windows 2000 and Windows XP. See the *Administrator Guide for Cisco Trust Agent, Release 2.1*, Chapter 10, “Cisco Trust Agent Wired Client Logging” for more information.

Machine Authentication Methods

Authentication Using Machine Password

Starting in Cisco Trust Agent Release 2.0.1, machine authentication can occur during the boot up process. This is controlled by whether the "use machine credentials" button in the Station Policy dialog box is checked or unchecked. If the "use machine credentials" button is checked, then machine authentication is performed in place of user context authentication and one of the three machine credential types is passed.

There are different types of machine credentials:

- Machine certificate (This is an existing feature.)
- Machine PAC (This is an existing feature.)
- Machine Password (This is a **new** feature.)

CTA 2.1 supports using the machine password whenever machine context authentication is done. A benefit of this method is that a certificate infrastructure is not needed.

See "Deploying End User 802.1x Wired Clients" in Chapter 11 of the *Administrator Guide for Cisco Trust Agent, Release 2.1* for more information.

Machine Authentication Only

Either of these machine credentials can be used for machine authentication only:

- Machine certificate
- Machine password

See "Deploying End User 802.1x Wired Clients" in Chapter 11 of the *Administrator Guide for Cisco Trust Agent, Release 2.1* for more information.

Configurable Outer Tunnel Identity for EAP-FAST

The construction of the encrypted tunnel through which the 802.1x Wired Client passes authentication credentials to the Cisco Secure Access Control Server (ACS) is initiated in the case of machine or user authentication.

During user authentication, *UserName@FullyQualifiedDomainName*, *anonymous@FullyQualifiedDomainName*, or *UserName* are the credentials passed to ACS.

During machine authentication, *HostName/FullyQualifiedDomainName* is the credential passed to ACS.

System Requirements

CTA may be installed on Linux, Mac OS X, and Windows operating systems. The following sections describe the system requirements for each type of operating system.

System Requirements for Installations on Linux

Before installing Cisco Trust Agent on a Linux operating system, verify that the target system meets the requirements in the following table.

Table 3 CTA System Requirements for Linux

System Component	Requirement
System	• Pentium class processor or better • Network connection
Operating System and Language Support	All available internationalized versions of these Linux operating systems support CTA 2.1.: • Red Hat Linux 9 • Red Hat Enterprise Linux v3 (Enterprise, Advanced Server, and Workstation) • Red Hat Enterprise Linux v4 (Enterprise, Advanced Server, and Workstation) **Note Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English.**
Linux Installers	Red Hat Package Management (RPM) v4.2 or greater.
Hard Disk Space	20 MB

Table 3 CTA System Requirements for Linux

System Component	Requirement
Memory	256 MB Red Hat Enterprise Linux v3 (Enterprise, Advanced, Workstation) 256 MB Red Hat Enterprise Linux v4 (Enterprise, Advanced, Workstation)
Listening Port	By default, Cisco Trust Agent listens on UDP port 21862.

System Requirements for Installations on Mac OS X

Before installing Cisco Trust Agent on a Mac OS X operating system, verify that the target system meets the requirements in the following table.

Table 4 CTA System Requirements for Mac OS X

System Component	Requirement
System	• G3 processor and later • Network connection
Free Hard Disk Space	20 MB minimum
Memory	256 MB RAM
Listening Port	By default, Cisco Trust Agent listens on UDP port 21862.
Operating System and Language Support	All available internationalized versions of Mac OS X 10.3.9 and 10.4 operating systems support CTA 2.1. **Note** Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English.

System Requirements for Installation on Windows

Before installing Cisco Trust Agent on a Windows operating system, verify that the target system meets the requirements in the following table.

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 5 CTA System Requirements for Windows

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.
Windows Operating Systems on which CTA 2.1 and the CTA 802.1x Wired Client Run	• Windows 2000 Professional and Advanced Server, SP4 and Update Rollup 1 • Windows XP Professional, SP1, SP2, and SP3 • Windows 2003 Standard, SP1 and R2

Table 5 CTA System Requirements for Windows (continued)

System Component	Requirement
Additional Windows operating systems on which CTA 2.1 runs but that do not support CTA 802.1x Wired Client	Windows XP Home, SP1, SP2, and SP3
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 Standard, SP1 and R2

Installation Notes

Chapter 2, Chapter 3, and Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release Version 2.1* discuss installing Cisco Trust Agent on Linux, Mac OS X, and Windows platforms. These chapters refer to installation files such as cta-linux-2.1.x-0.i386.rpm, cta-darwin-2.1.x.0.dmg, and ctasetup-supplicant-win-2.1.x.0.msi. Any installation file in this format is referring to CTA release 2.1.103.0 installation files.

Obtaining the Latest Release of CTA

The latest release of Cisco Trust Agent 2.1 is version 2.1.103.0.

Table 6 lists the files used to install CTA 2.1 on the supported operating systems. See the *Administrator Guide for Cisco Trust Agent, Release 2.1* for a complete description of content of the files and how they can be used in a CTA installation.

Table 6 CTA 2.1.103.0 Files

Downloadable File and Description of	Content of the File and Description
cta21ag.pdf	Administrator Guide for Cisco Trust Agent, Release 2.1.
cta21rn.pdf	Release Notes for Cisco Trust Agent, Release 2.1.
ctaadminex-linux-2.1.103-0.tar.gz	This is the installation package for Linux operating system. It contains the **ctaadminex-linux-2.1.103-0.sh** script which allows administrators to accept the end user license agreement and extract the **cta-linux-2.1.103-0.i386.rpm** file used to install CTA.
ctaadminex-darwin-2.1.103.0.tar.gz	This is the installation package for Mac OS X operating systems. It contains the **ctaadminex.sh** script which allows administrators to accept the end user license agreement and extract the **cta-darwin-2.1.103.0.dmg** file used to install CTA.

Table 6 CTA 2.1.103.0 Files (continued)

Downloadable File and Description of	Content of the File and Description
CtaAdminEx-win-2.1.103.0.exe	This is an installation package for Windows operating systems. It contains the **ctasetup-win-2.1.103.0.msi** file which allows administrators to accept the end user license agreement and install CTA. The file does not contain the CTA 802.1X Wired Client.
CtaAdminex-supplicant-win-2.1.103.0.exe	This is an installation package for Windows operating systems. It contains the **ctasetup-supplicant-win-2.1.103.0.msi** file which allows administrators to accept the end user license agreement and install CTA. The file does contain the CTA 802.1X Wired Client.

Upgrade Support

Cisco Trust Agent supports upgrade installations from versions 1.0, 2.0, 2.0.1, 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.

Note When upgrading a version of CTA along with the CTA 802.1x Wired Client, to CTA 2.1 with the CTA 802.1x Wired Client, the computer is disconnected from the network at the end of the software upgrade process. The final step of the upgrade procedure is to reboot the computer; rebooting restores the network connection and it is a required step in the upgrade process.

In the case of a silent upgrade, administrators should use MSI commands which limit interruptions to users but still prompt users to reboot their computers at the end of the software upgrade.

There are different methods of upgrading CTA from version 1.0, 2.0, 2.0.1, and selective availability and beta versions to CTA 2.1.103.0. See Chapter 2 and Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1*, for information about upgrading previous versions of CTA for Linux and Windows to CTA 2.1.

Upgrading CTA 2.0 to CTA 2.1

This section describes upgrading CTA 2.0.0.30 to CTA 2.1.103.0.

Upgrading CTA without the CTA 802.1x Wired Client

Both Linux and Windows versions of CTA 2.0 without the CTA 802.1x Wired Client can be upgraded to CTA 2.1.

Upgrading CTA with the CTA 802.1x Wired Client

In order to upgrade from CTA 2.0 with the CTA 802.1x Wired Client to CTA 2.1 with the CTA 802.1x Wired Client, you need to uninstall CTA 2.0, delete the CTA 802.1x Wired Client directory, and then install CTA 2.1 from scratch.

If you attempt to directly upgrade CTA 2.0 with the CTA 802.1x Wired Client to CTA 2.1 with the CTA 802.1x Wired Client the CTA 802.1x Wired Client service fails to start and you will not be able to start the service manually.

To upgrade from CTA 2.0 with the CTA 802.1x Wired Client to CTA 2.1 with the CTA 802.1x Wired Client, follow this procedure:

Step 1 Uninstall CTA 2.0 using the procedure in "Uninstalling Cisco Trust Agent on Windows" in Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1*.

Step 2 Reboot the PC when prompted.

Step 3 Delete this directory and its contents:

\Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client

Step 4 Install CTA 2.1 from scratch using the methodology described in Chapter 4, "Installing the Cisco Trust Agent on Windows" in the *Administrator Guide for Cisco Trust Agent, Release 2.1.*

Step 5 Reboot the computer when prompted.

Note The computer remains disconnected from the network until the computer is rebooted.

Upgrading from Selective Availability and Beta Releases to CTA 2.1

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

CTA 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 without being uninstalled first. The certificates, third-party posture plugins, ctad.ini, ctalogd.ini, log files, and the deployment profile files remain in the directories in which they were installed and they are used by CTA 2.1.103.0.

Upgrading CTA without the CTA 802.1x Wired Client

You can upgrade from any of the CTA 2.1 selective availability or beta releases without the CTA 802.1x Wired Client to CTA 2.1.103.0 without the 802.1x Wired Client without having to uninstall CTA 2.1.x. Use the upgrade procedures in Chapter 2 or Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1*, to upgrade a Linux or Windows installation.

Upgrading CTA with the CTA 802.1x Wired Client

You can upgrade from any of the CTA 2.1 selective availability or beta releases with the CTA 802.1x Wired Client to CTA 2.1.103.0 with the 802.1x Wired Client, you can run the installation for the new version of CTA while the old version is still installed. At the end of the upgrade process, you must reboot the computer.

If you are upgrading from CTA 2.1.x with the CTA 802.1x Wired Client to CTA 2.1.103.0 with the CTA 802.1x Wired Client, the authentication profiles installed on the client used in CTA 2.1.x are compatible with CTA 2.1.103.0 and will remain in their directories through the upgrade process.

Note At the end of the upgrade process the computer is disconnected from the network until the computer is rebooted.

Use any of the installation procedures in Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1*, to upgrade a Windows installation.

Known Defects in CTA 2.1 Posture Agent

This section describes problems known to exist in the posture agent of Cisco Trust Agent, Release 2.1. This section excludes defects of the 802.1x Wired Client component of CTA 2.1.

Note A "—" in the Explanation column indicates that no information was available at the time of publication. You should check the Cisco Software Bug Toolkit for current information. To access the Cisco Software Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. (You will be prompted to log in to Cisco.com.)

Table 7 Known Defects in the CTA 2.1 Posture Agent Client

Defect ID	Headline	Explanation
CSCsc18885	Erroneous log entry, claiming "Failed to read Registry Key" in CTA log.	**Symptom** When a user performs a fresh installation, upgrade, or reinstallation of Cisco Trust Agent with logging enabled, an **erroneous** log message is generated. This message is similar to this message: `2 12:00:00.000 11/11/2005 Sev=Critical/1 PSDaemon/0xE3C0001A Failed to Read Registry Key, error code 2` **Conditions** This erroneous log message is generated when the Cisco Trust Agent Version 2.0.0.30 is Installed, Reinstalled, or Upgraded with logging enabled. This **erroneous** log message was observed on the following platforms: Windows NT 4.0, Window 2000 and Windows XP. **Workaround** No workarounds are available. Note that this log message is erroneous and does not affect the running of Cisco Trust Agent.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCse27741	CTA uses wrong root certificate when an expired certificate exists along with working certificate.	**Symptom** Existing customer certificates work with some authentication protocols but not EAP over UDP (NAC-L3-IP or NAC-L2-IP). The certificates are valid and are stored in the correct locations. This message is in the ACS Failed Attempts log: "EAP-TLS or PEAP authentication failed during SSL handshake." **Conditions** The existing certificate is part of a certificate chain in which the root certificate is expired. The expired root certificate has the same subject name as the valid certificate and both certificates coexist in CTA client's certificate store. **Workaround** Remove this expired root certificate from the user certificate store.
CSCsg08764	CTAstat incorrectly reports operational status for plugin	**Symptom** ctastat reports that a posture plugin is working correctly when some other system behavior, such as a failed authentication, indicates that a plugin might not be working correctly. **Conditions** Any condition where the plugin is not working correctly or it is missing; for example, corrupted or missing .dll or .so file, missing .inf file, the plugin was installed in the wrong directory, or the plugin is corrupted etc. **Workaround** Enable logging on the client in order to capture information about the failed plugin.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsg15684	ctapsd crash after 5 hours with SAV PP and 1K buffer	**Symptom** Cisco Trust Agent Posture Server Daemon crashes after running approximately 5 hours with a Symantec posture plugin installed on the client machine and when PPMsgSize is set to 1024. **Conditions** Running CTA 2.1.14.0 and PPMsgSize is set to 1024 in ctad.ini and occurs on Windows operating systems. **Workaround** There is no workaround. **Note** This problem is NOT reproducible with CTA 2.1.18.0 or later versions.
CSCsg26209	CTA does not support downgrade of posture plugins	**Symptom** A posture plugin for a third-party application does not respond at all or does not respond with values for all posture attributes. In the CTA log files you may see these messages like "client not installed," "client is running the wrong version," or "client communication error." **Conditions** The third-party client application has been downgraded, and though the corresponding downgraded plugin has been dropped into the Cisco Trust Agent plugins/install directory, CTA has not installed it because the previous plugin has a higher version number. **Workaround** Uninstall the higher revision of the plugin then install the version of the plugin that corresponds to the downgraded application's version. **Note** You can verify the version numbers of the plugin and application by viewing their properties.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsi49862	CTA should set BootTimeUDPExemptions as String Value	**Symptom** In default status, CTA creates windows registry key "BootTimeUDPExemptions" as DWORD, and set it to 0x00005566. However the value is incompatible with Windows specification. CTA should set BootTimeUDPExemptions as String Value. **Conditions** BootTimeUDPExemptions is set to 1 in ctad.ini. This is the default setting. **Workaround** Set BootTimeUDPExemptions in ctad.ini to 0, and set BootTimeUDPExemptions in registry by hand. This is documented by Microsoft at this location: http://support.microsoft.com/kb/917730/en-us
CSCsi91317	HostPP truncates MAC addresses if there are 2 or more	**Symptom** If the MAC OS X host being postured has more than two active IPV4 interfaces (not including loopback interfaces), and the host is postured of the HostPP MacAddress, the Mac address of the 2nd interface will be incomplete, and the Mac addresses of 3+ interfaces will be missing. **Conditions** Host machine has more than one active IPV4 interfaces, and the host is postured of the HostPP MacAddress. **Workaround** None.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsi91358	Linux-Truncated addresses with 2 MAC address requested thorough HostPP	**Symptom** If the Linux host being postured has more than two active IPV4 interfaces (not including loopback interfaces), and the host is postured of the HostPP MacAddress, the Mac address of the 2nd interface will be incomplete, and the Mac addresses of 3+ interfaces will be missing. **Conditions** Host machine has more than one active IPV4 interfaces, and the host is postured of the HostPP MacAddress. **Workaround** None.
CSCsi98520	Creating a Custom Installation Package procedure for Mac OS X is incorrect.	**Symptom** The "Creating a Custom Installation Package" procedure in Chapter 3 of the "Administrator Guide for Cisco Trust Agent, Release 2.1, with Bundled Supplicant" and the "Creating a Custom Installation Package" procedure in Chapter 3 of the "Administrator Guide for Cisco Trust Agent, Release 2.1 Without Bundled Supplicant" requires that you rename the disk image before customizing the CiscoTrustAgent volume. This is unnecessary. **Conditions** All. **Workaround** Do not perform step 3, 4, or 5 of the procedure. Step 6 should be written, "Double-click the CiscoTrustAgent volume on the desktop." the rest of the step should be deleted.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsj76891	CTACERT.exe throws application exception	**Symptom** Running CTACERT.EXE to import a certificate into the root store in windows XP results in an error, Dr. Watson log (if enabled) and minidump file. The CTACERT.EXE program crashes. **Conditions** This error was observed on Windows XP SP2 and using CTA 2.1.103. The command used when the error occurred was: "C:\Program Files\Cisco Systems\CiscoTrustAgent\ctacert.exe" /ui 2 /add "C:\Program Files\Cisco Systems\CiscoTrustAgent\rocselfcert.cer" /store "root" **Workaround** The certificate should be installed in the root store, even though the error occurs. The certificate can also be manually imported using the certificate MMC, Group policy, etc.

Table 7 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsk70794	Parameters in the User Notifies section of the ctad.ini file do not parse correctly. This occurs only in Danish versions of Windows operating systems.	**Symptom** Two symptoms present themselves as a result of this defect. The parameters named in the symptoms are in the [User Notifies] section of the ctad.ini file. • After the user receives a posture notification message, the user has to click **OK** in the message box before launching another program from the start menu even when SysModal=0 in the ctad.ini file. • The default value of UserActionDelayTimeout is 25 seconds. When the value of this parameter is decreased dramatically, it still takes 25 seconds for the browser to open the URL contained in the posture message. **Conditions** This occurs in all versions of Danish Windows operating systems. **Workaround** None

Known Defects in CTA 802.1x Wired Client

These are the defects in the CTA 802.1x Wired Client that was released with CTA 2.1.103.0. The CTA 802.1x Wired Client may also be referred to as the "light supplicant" or "supplicant."

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client

Defect ID	Headline	Explanation
CSCsb47789	TLS alert bad_certificate(42) should be unknown_ca(48)	**Symptom** The CTA 802.1X Wired Client sends an incorrect error code to the ACS. The 802.1X Wired Client sends bad_certificate(42) when it should send unknown_ca(48). This error gets logged on the ACS and might mislead ACS administrators. The result is an incorrect log on the ACS, but it does not affect the functionality of the 802.1X Wired Client nor ACS. **Conditions** A valid certificate chain or a partial chain was received, but the certificate was not accepted because the CA certificate could not be located or could not be matched with a known, trusted CA **Workaround** There is no workaround.
CSCsb88110	The 802.1X Wired Client pop up box is hidden during bootup with multiple interfaces.	**Symptom** When booting up a PC with multiple interfaces (four), with the 802.1X Wired Client installed, a user enters his username on first popup box and then his password. However, the second popup box does not appear. The 802.1X Wired Client is waiting for the password to be entered for the second popup box. Then the third popup box appears. The forth popup box does not appear but the 802.1X Wired Client waits for the password to be entered. **Conditions** This occurs with multiple interfaces that are all getting authenticated. **Workaround** Set the EnableLogonNotifies attribute to 0 in the ctad.ini for CTA.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsc31219	User credentials dialog does not close upon failure to connect.	**Symptom** If the network client fails to provide a posture at Layer 2, and ACS fails to set a policy for the network client, and if the user enters incorrect credentials, the user credentials dialog box is not automatically removed from the screen. **Workaround** Users need to manually close the user credentials dialog box.
CSCsc39374	RSA 5.2 new pin mode does not work with CTA 802.1x Wired Client	**Symptom** User authentication fails. **Conditions** RSA 5.2 is used for authentication. This is the behavior the user experiences: 1. User is prompted for username. 2. User is prompted for password. User enters RSA tokencode here. 3. User responds with "y" at the prompt to create a new PIN. 4. The user is then prompted for username two times, until the connection fails. **Workaround** There is no workaround.
CSCsd60058	802.1x, EAP-GTC password change fails when password complexity requirement is enforced.	**Symptom** Password change fails with EAP-GTC. **Conditions** ACS is configured for EAP-GTC and password complexity rule enabled on Active Directory. **Workaround** Disable password complexity rule on Active Directory.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse35094	Password entered in supplicant Credentials popup is not used.	**Symptom** Password entered in supplicant Credentials popup is not used for authentication. **Conditions** With machine and user authentication enabled, the password entered in supplicant Credentials popup is not used for authentication. **Workaround** There is no workaround.
CSCse35113	CTA 802.1x Wired Client can indicate that the ethernet interface is authenticated and connected when it is not.	**Symptom** With IEEE 802.1x authentication configured, the CTA 802.1x Wired Client status shows that the client is authenticated and connected to the network when it is not. **Conditions** This error can happen when you try to reconnect after a failed authentication. **Workaround** The incorrect connection status will time out in about one minute.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse54397	CTA 802.1x Wired Client delays 802.1x authentication after returning from hibernation.	**Symptom** While client is coming out of hibernation state the supplicant needs to initiate a IEEE 802.1x connection for either machine or user authentication. The time it takes for supplicant to initiate for IEEE 802.1x authentication may vary form 15-to-80 seconds. **Conditions** The CTA 802.1x Wired client eventually initiates IEEE 802.1x authentication but the time it takes varies between 15-to-80 seconds after the network interface comes up. This delay depends on various factors like Operating system, PC hardware configuration, and the context of the machine, for example, is the user logged into desktop or not. **Workaround** Wait for the CTA 802.1x Wired Client to initiate IEEE 802.1x authentication after the interface comes up or open the CTA 802.1x Wired Client main window, select the network adapter you use to connect to the network, click Disconnect, and then click Connect.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse77264	CTA 802.1x Wired Client fails to launch after a reboot	**Symptom** This problem occurs intermittently. Reboot the client on which CTA and 802.1x Wired Client is installed. You see the following behaviors: • 802.1x Wired Client user interface does not prompt for password. • User does not see posture popup message after logging in. • CTA 802.1x Wired Client user interface cannot be seen, and its icon is not visible in the system tray. • Navigating Start > Program Files > Cisco Systems > Cisco Systems, Inc. Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client Open does not launch the 802.1x Wired Client. • The Windows Services control panel indicates that all the CTA related services are running. • Stopping the “Posture Server Daemon” takes an unusually long time, and fails. • Client needs to be rebooted to fix this. **Conditions** Behavior was detected on Windows 2000 Professional with Service Pack 4. 802.1x Wired Client is configured to prompt for user password. **Workaround** There is no workaround.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse93282	MSCHAP authentication uses system credentials with a specific profile	**Symptom** 1. Reboot client. 2. Login using Microsoft GINA. 3. CTA 802.1x Wired Client prompts for authentication credentials. 4. Provide a nonexistent username. 5. Client will posture and authenticate using the GINA/System user account. It works like an SSO scenario. **Conditions** ACS is configured to use EAP-MSCHAPv2 (ONLY) as inner authentication method. ACS uses Windows Active Directory as back-end user database. The client uses an authentication profile with these attributes: • Request password when needed. • Use client certificate during machine authentication and user authentication. • Never validate Trusted Servers. • Use anonymous as identity. • Automatically establish machine connection. **Workaround** There is no workaround.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsf24460	CTA 802.1x Wired Client EAP-FAST Inner identity in UPN format should include domain.	**Symptom** ACS initiates a domain controller lookup of a username in UPN format that either fails or takes a long time to complete. **Conditions** The CTA 802.1x wired client removed the domain from the username, and ACS does the lookup in a Windows multi-domain architecture where the domain portion of the UPN username is needed to clarify the username. **Workaround** None, other than re-architect the Windows network to avoid multi-domain lookups.
CSCsf29511	Under high CPU of PC situation, CTA cannot respond IEEE 802.1x packet	**Symptom** Under high CPU utilization on a PC, CTA cannot respond IEEE 802.1x packet. **Conditions** High CPU utilization on the PC because of resource depletion or other issues. This occurs on Windows PCs where the CTA 802.1x Wired Client has also been installed. **Workaround** Make sure all logging levels for CTA are set to the lowest value or even turned off. Try adding more memory or increase CPU on machine. Try eliminating applications that are using the device's resources.
CSCsf29547	CTA 802.1x Wired Client remains in connecting state when certificate is revoked.	**Symptom** When the machine certificate has been revoked, the connection does fail, but the CTA 802.1x Wired Client continues to try to re-connect. This results in the supplicant staying in a constant "yellow" state. **Conditions** CTA 802.1x Wired Client is configured for machine authentication only and it uses a revoked machine certificate. **Workaround** There is no workaround.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsf32767	CTA 802.1x Wired Client sends wrong password after Active Directory password change.	**Symptom** IEEE 802.1x user authentication may fail if user has to change Active Directory password. **Conditions** Using single sign-on with CTA 802.1x Wired Client, the user is prompted to change their Active Directory password. CTA 802.1x Wired Client sends the old password and User authentication fails. **Workaround** Reboot or logoff the user and attempt a login with the new/correct Active Directory credentials.
CSCsg14487	Password is cached even when GTC is configured	**Symptom** OTP passwords are cached after a successful connection attempt until the subsequent connections (3 attempts) have failed authentication. **Conditions** GTC is enabled on ACS. **Workaround** Click “clear credentials” button in Network Configuration Summary window prior to making a connection attempt.
CSCsg23722	User not allowed to change incorrect username right away.	**Symptom** When an invalid username is entered in the supplicant popup the user is not given the opportunity to change it for about 30 seconds. The popup's that appear for about 30 seconds only allow you to enter the password. **Conditions** This only occurs when the host is configured for machine and user authentication without single sign on and EAP-GTC is user for an inner authentication method. **Workaround** After about 30 seconds, the user receives another popup dialog box where they can enter the correct username.

Table 8 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsg34154	CTA 802.1x Wired Client does not re-start authentication after aborted CSA downgrade.	**Symptom** PC wired interface does not re-authenticate after an aborted CSA downgrade. **Conditions** Only observed during aborted CSA downgrade. **Workaround** Open wired client GUI and click Connect.
CSCsh17908	Windows CTA 802.1x Wired Client conflicts with some Smart Card software	**Symptom** Users receive the error message "The system cannot log you on due to the following error: The handle is invalid." when they attempt to connect with some smartcard software after installing CTA with the 802.1x Wired Client **Conditions** The issue has been observed in an environment using the CTA 802.1x Wired Client distributed with CTA 2.0.1.14 in conjunction with third-party smartcard software. Installation of CTA on this system interferred with Windows authentication using this software. **Workaround** Current version of Cisco SSC 802.1x client combined with the non-802.1x CTA client worked in this environment.
CSCsh39205	Cancelled shutdown causes supplicant icon to disappear	**Symptom** The Cisco Trust Agent 802.1x wired client icon no longer appears in the Windows system tray. **Conditions** User has cancelled a Windows shutdown sequence, logged off, and re-logged in to Windows with a different user account. **Workaround** There is no workaround.

Closed and Resolved Defects in CTA

These are the groups of closed and resolved defects reported in these release notes:

Following the release of CTA 2.0 was CTA 2.0.1, which was a product release sent to a small group of customers.

Defects Closed or Resolved in CTA 2.1 Posture Agent

This section describes defects that were resolved by the selective availability, beta, and CTA 2.1.103.0 releases.

Table 9 Defects Closed or Resolved in the CTA Posture Agent

Defect ID	Headline	Description
CSCsb09542	With EnableLogonNotifies=1, strange results during logon and logoff	**Symptom** During login on Windows XP machines, there are conditions where the network authentication will occur while the system is still initializing its screens. It will cause a failure to correctly “paint” the notification box. It will not affect the connectivity of the network. However, it will require the user to press Enter if this happens. **Conditions** EnableLogonNotifies must be enabled in the ctad.ini file. (ex: EnableLogonNotifies=1). You must have a notification message configured in the ACS. This error will occur at random (based on timing conditions). **Resolution** Resolved in CTA Release 2.1.100.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCsd43949	Posture notification not displaying after 802.1x authentication/posture	**Symptom** After entering the Windows domain and the supplicant user credentials, the user is authenticated. The "healthy" posture notification is never displayed on the user's desktop. **Conditions** The host machine has 802.1x Wired Client installed. While the machine is being rebooted, machine authentication occurs before the user logon processing completes. The "EnableLogonNotifies" setting is disabled. **Resolution** EnableLogonNotifies is now enabled by default. The notification received before logon will be displayed after the logon processing is complete. Resolved in CTA Release 2.1.100.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCse02440	Ctacert /add command needs better error codes	**Symptom** This is a feature request and not a direct report of a defect. CTACert /add needs more robust error handling / error reporting. Specifically, if the certificate being imported already exists in the user's Trusted Root Certificate Authority, it will state a generic error message that the certificate failed to import - and it will fail to import the certificate into any of the other stores. We need to be able to either: - Report that the certificate already exists in the store and (ideally) which store it is already present in or - In the case of the certificate already existing in the store bypass that store and move on to the next Trusted Root Certificate Authority store. **Conditions** Any error condition encountered produces the same error message. Note that using ctacert without any options at all produces the same error message. **Resolution** Resolved in CTA Release 2.1.100.0 • Enhanced the CTA Certificate utility to being more user-friendly by adding a new usage/help popup. • Added more robust error reporting into application. When the utility is complete we now display a detailed break down of files imported and import status with any potential error message/return codes. • In addition to the modification to display import status, a trace log is now created to log detailed information in regards to certificates and error returns. This log is stored in the %TEMP% and is called “CtaCertTrace.Log”

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCse23586	ctaeou stops responding to NAD	**Symptom** CTA EOU Daemon stops responding to a layer 3 network access device. **Conditions** Layer 3 posture is used and the collection of posture data takes unusually long which causes Cisco Trust Agent EOU Daemon server to timeout on the posture response. After many such failures, CTA EOU Daemon stops responding to the network access device. **Resolution** Resolved in CTA Release 2.1.100.0
CSCse27560	CTA should not remove 802.1x Wired Clients files during install/upgrade	**Symptom** When installing or upgrading to a new version of the Cisco 802.1x Wired Client feature, the CTA package took care to remove the contents of the following Cisco Trust Agent Wired 802.1x Clients directories \Program Files\Cisco Systems \Cisco Trust Agent 802_1x Wired Client\. This was done because the 802.1x Wired Client profiles for CTA 2.0 were not compatible with CTA 2.1. **Conditions** All. **Resolution** This issue has since been fixed in the 4.0.5 builds of the CTA 802.1x Wired Client. To resolve this bug the CTA package will no longer remove the wired CTA 802.1x Wired Client directories during an install. Resolved in CTA Release 2.1.100.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCse50876	Scripting interface not registering posture data file	**Symptom** Customer posture information is not being sent via the scripting interface to ACS. **Conditions** The "VendorIDName= Cisco Systems" field is missing in the scripting interface .inf file, and/or the .inf or posture data file is not a plaintext file. **Resolution** Added the "VendorIDName=Cisco Systems" field to the description of the Information file in Administrator Guide for Cisco Trust Agent, Release 2.1 and made clear that the information file must be a plain text file. Resolved in CTA Release 2.1.100.0
CSCse76333	EapHandlePacket Error	**Symptom** Although very rare, CTA Posture Server Daemon intermittently fails to return the posture data. **Conditions** No posture data is returned from CTA and an "EapHandlePacket Error" entry is logged in the CTA log. **Resolution** Resolved in CTA Release 2.1.100.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCse90646	ctacert.exe fails on some installations	**Symptom** Ctacert.exe fails to import a known good certificate on some CTA installs. **Conditions** This has been noticed most on Windows 2000 installations of CTA. **Workaround** Install the certificate directly into the the local certificate store using Internet Explorer, Microsoft Management Console, or the ctaCert utility. See the *Administrator Guide for Cisco Trust Agent, Release 2.1* for more information about the ctaCert utility. **Closure comment** This defect was closed because it was unreproducable. Closed in CTA Release 2.1.100.0
CSCsf16515	hostpp on XP spk1 installed causes ctad.exe to take 100% CPU	**Symptom** ctad.exe for CTA 1.0.55 spikes to 100% **Conditions** One must have XP spk1, cta 1.0.55 with the hostpp, and the CSA (since the CSA actually installs the hostpp). The spike only occurs when one connects via VPN (thus causing a posture request. **Resolution** ctad.exe for CTA 1.0.55 and CTA 2.1 no longer spike CPU to 100%. Resolved in CTA Release 2.1.100.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCsg08595	Browser auto-launch does not work with default timer with 802.1x authentication.	**Symptom** Browser auto-launch feature may not work with the default timers set. **Conditions** After a 802.1x authentication, a DHCP address may be delayed getting to a client and the network may not be available to launch the browser and connect to a particular web site designated by an administrator. **Resolution** The default value of this parameter was increased to 25 seconds. This was resolved in CTA build 2.1.102.0
CSCsg23794	802.1x wired client Clear Credentials button not documented in Administrator Guide for Cisco Trust Agent, Release 2.1.	**Symptom** The Administrator Guide for Cisco Trust Agent, Release 2.1 does not explain the functionality of the Clear Credentials button in the Network Configuration Summary window of the 802.1x Wired Client user interface. **Conditions** All. **Resolution** Resolved in CTA Release 2.1.100.0. See Chapter 9 of the *Administrator Guide for Cisco Trust Agent, Release 2.1*, for more information on this feature.
CSCsg94979	Remote Desktop issue with machine state	**Symptom** When RDP session is started the machine state reported to ACS changes to booting. **Conditions** Upon starting a RDP session. Reported in CTA 2.1.100.0 **Resolution** Resolved in CTA Release 2.1.101.0

Table 9 Defects Closed or Resolved in the CTA Posture Agent (continued)

Defect ID	Headline	Description
CSCsh30297	Security vulnerability while launching a process	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). This defect has been resolved. An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml

Defects Closed or Resolved in CTA 802.1x Wired Client

This section describes defects that were resolved in CTA 802.1x Wired Client released with the beta releases of CTA 2.1. This is new information for customers upgrading from CTA 2.0, CTA 2.0.1.14, and C.1.18.0 to CTA 2.1.103.0.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client

Defect ID	Headline	Description
CSCsc68541	CTA 802.1x Wired Client will crash if no interfaces are enabled.	**Symptom** If there are no valid ethernet interfaces and the CTA 802.1x Wired Client runs, it will crash. However, the operating system stays up. If the ethernet interface is reinstalled or re-enabled, the supplicant will not restart. Only restarting the service or rebooting restarts IEEE 802.1x authentication. **Conditions** All ethernet interfaces are disabled and the client boots in an IEEE 802.1x environment. **Resolution** Resolved in CTA Release 2.1.100.0.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsd65198	PPP connection failure by installing CTA 2.0	**Symptom** PPP connection fails to be established. Windows 2000 shows Error 720 has occurred. **Conditions** VPN Client 4.8 and CTA 2.0 are installed on Windows 2000. **Resolution** Resolved in CTA Release 2.1.100.0.
CSCsd65801	Supplicant remains in connecting state client is put in auth fail vlan	**Symptom** Supplicant remains in connecting state when client is put into auth failed vlan. **Conditions** When the client user authentication fails and the switch is configured for auth failed vlan. **Resolution** Resolved in CTA Release 2.1.100.0.
CSCsd78683 (CSCsc21188)	When the CTA 802.1x Wired Client is idle, it does not respond to EAP requests from the switch.	**Symptom** When the CTA 802.1x Wired Client is idle, it does not respond to EAP requests from the switch. **Conditions** This condition occurs when a CTA machine is already connected to a port and after the port is enabled for IEEE 802.1X. **Resolution** Resolved in CTA Release 2.1.18.0
CSCsd87483 (CSCse85217)	Supplicant Kerberos subsystem encountered a PAC verification fail	**Symptom** System event view contains “The kerberos subsystem encountered a PAC verification failure” **Conditions** This issue might occur when performing machine authentication. **Resolution** Resolved in CTA Release 2.1.100.0.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsd98534	Cannot customize CTA profile - Always says Cisco Corporate	**Symptom** When using the CTA 802.1x Wired Client to create a profile, the pop-up box for the profile always says “Cisco Corporate”. End user cannot customize this text to indicate the name of their organization. **Conditions** All involving CTA 802.1x Wired Client. **Resolution** The text was changed to be more suitable. The text now reads “Please enter your credentials for network Cisco Trust Agent 802.1x wired client, access.” Resolved in CTA Release 2.1.100.0
CSCse04240	PAC provisioning fails after master key expires	**Symptom** CTA 802.1x Wired Client connection fails with “invalid PAC opaque” message. **Conditions** Master key has expired on ACS. **Resolution** After “invalid PAC opaque” message, the CTA 802.1x Wired Client automatically provisions a new PAC. Resolved in CTA Release 2.1.100.0
CSCse19030	CTA 802.1x Wired Client has long delay in acquiring DHCP address after user auth	**Symptom** CTA 802.1x wired client has a significant delay in obtaining an IP address from a DHCP server after the second user authentication. **Conditions** After authenticating a user during an 802.1x authentication, vlan attributes are downloaded to the switch port and the PC is put into a new vlan. The client never does a release and renew of the IP address. **Resolution** CTA 802.1x Wired Client now performs DHCP release / renew. This issue has been fixed in CTA release 2.1.100.0

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCse26978	Issues with supplicant sending an eapol logoff	**Symptom** The Cisco Trust Agent 802.1x wired client no longer responds to re-authentication requests, and the associated switchport is not assigned to the correct auth-fail VLAN. **Conditions** An "auth-fail VLAN" (a VLAN that the switchport should be assigned to when authentication fails) is configured on the switch. **Resolution** Resolved in CTA Release 2.1.100.0
CSCse33715	Unable to clear stored credentials	**Symptom** The button to clear stored credentials is always greyed out. **Conditions** Normal operation. **Resolution** The Clear Credentials button in the Network Configuration Summary window is now active. Resolved in CTA Release 2.1.100.0
CSCse48348 (CSCse93703)	ConnectionClient.exe crash-memory error	**Symptom** The Cisco Trust Agent 802.1x wired client may crash with a memory error. **Conditions** A user clicks on the Connect and Disconnect buttons in the Cisco Trust Agent 802.1x wired client user interface several times in a row, after logging in to an account that does not have administrative privileges. **Resolution** The memory error that caused ConnectionClient.exe to crash has been fixed. Resolved in CTA Release 2.1.100.0

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCse60387	Multiple profiles with same time stamp crashes supplicant	**Symptom** The Cisco Trust Agent 802.1x wired client service crashes. **Conditions** There is more than one profile (*.xml file) with the same timestamp in either folder Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\networks or Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\profiles\policies. **Workaround** Remove one of the profiles, or alter one of the timestamps by editing and saving the file.
CSCse62380	CTA 802.1x Wired Client's system tray icon does not appear with IBM Fingerprint Software	**Symptom** The Cisco Trust Agent 802.1x Wired Client icon does not appear in the Windows system tray. **Conditions** The Windows system is running on an IBM ThinkPad with the fingerprint recognition system. **Resolution** UPgrade to ThinkVantage Fingerprint Software 5.5.0. Prior versions exhibit interoperability problems with the wired supplicant.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCse77333	Machine authentication not attempted during Logoff/reboot on Win2k Pro SP4	**Environment**: • On ACS, configure the inner authentication method as MSCHAPv2. • Install Supplicant 2.1.0.8 on Windows 2000 with SP4. • No authentication profile have been applied to the client machine. **Description of Behavior:** 1. Boot the client. The client performs machine authentication while booting up. 2. Login as Administrator. Administrator authenticates using 802.1x and reports posture information. 3. Logoff Administrator. Client does not attempt machine authentication while loging off. The 802.1x Wired Client Interface goes down; this can cause issues with GPO and roaming profile. **Closure Comment** Shutdown scripts and GPOs are unreliable, because timing issues between the shutdown process itself and resource-dependent actions initiated by a script/GPO can cause the script/GPO to not complete. Given that such resource starvation is likely with a CTA 802.1x Wired Client and its networking nature, it has been deemed more prudent to simply not perform machine authentication at all during shutdown. Closed in CTA Release 2.1.100.0

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCse84252	Multiple machine certificates cause 802.1x Wired Client to send empty certificate	**Symptom** An empty certificate is used for machine authentication. **Conditions** Two certificates with the same name are in the same certificate store. **Resolution** CTA 802.1x Wired Client no longer sends an empty certificate if there are two certificates with the same name in the same certificate store. Resolved in CTA Release 2.1.100.0
CSCsf12081	Re-authentication not working for single sign-on if username and password entered incorrectly	**Symptom** The network connection that is handled by the 802.1x wired client within CTA never comes up after login, and the wrong credentials are sent to ACS. **Conditions** The CTA 802.1x wired client has been configured for single sign-on and multiple retries. The user entered the wrong password in the Windows GINA dialog, and then later entered the correct password. Login completes using cached credentials. **Resolution** Resolved in CTA Release 2.1.100.0.
CSCsf14120	Privilege escalation vulnerability via Help facility	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). This defect has been resolved. An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsf15836	Privilege escalation vulnerability via web browser	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). This defect has been resolved. An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml
CSCsg07518	Machine auth fails on the first re-authentication if user does not logon to windows	**Symptom** If Radius Attribute 27 is greater than 300 seconds, the second authentication will fail. **Conditions** Increasing SQTimer to a value greater than 300 seconds does not avoid authentication failure. It does not matter if the port is configured for re-auth or not. If supplicant is sending eapol-logoff, switch will just send EAP-Failure therefore ACS will not know and will not log that in its report. **Workaround** Set radius attribute 27 to less than 300 seconds. **Closure comment** This defect was closed because it was determined the problem was caused by a DHCP misconfiguration. Resolved in CTA Release 2.1.100.0

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsg20558	ConnectionClient.exe vulnerable to Local Privilege Escalation	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). This defect has been resolved. An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml
CSCsg24700	CTA 802.1x Wired Client service does not start after upgrade from 2.0.0.30 to 2.1.x.0	**Symptom** The Cisco Trust Agent 802.1x wired client service is not started after the required reboot. **Conditions** Cisco Trust Agent has been upgraded from 2.0.0.30 (with 802.1x wired client) to 2.1.18.0 or 2.1.101.0 (with 802.1x wired client). **Workaround** Uninstall CTA 2.0.0.30 before installing CTA 2.1.x.0. **Closure Comment** The schema for the authentication profiles changed between the release of CTA 2.0.0.30 and CTA 2.1.x.0. The schema used for CTA 2.0.0.30 will not be changed to match that used in CTA 2.1.x.0. Customers of CTA 2.0.0.30 will need to use the workaround procedure to upgrade from CTA 2.0.0.30 to CTA 2.1.x.0.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsg33405	Crash seen on shutdown when previous shutdown was cancelled	**Symptom** The CTA 802.1x Wired Client icon disappears from the system tray and the CTA 802.1x Wired Client stops responding after cancelling a logoff/shutdown request. **Conditions** IEEE 802.1x connection is already established. User initiates the shutdown processing and then cancels the shutdown request. **Resolution** Resolved in CTA Release 2.1.103.0.
CSCsg34423	User's password written to log file	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml
CSCsg57507	Change default values for interactive and non-interactive retries	**Symptom** The default values for Interactive Authentication Retries and Non-Interactive Authentication Retries were less than or equal to the default "max-attempts" value needed for the auth fail vlan feature used on Cisco switches. These values needed to be manually reconfigured and distributed with the deployment profiles. **Conditions** All **Resolution** The default value of Interactive Authentication Retries and Non-Interactive Authentication Retries were changed to 4 to avoid having to manually reconfigure these parameters. Resolved in CTA 2.1.101.0.

Table 10 Defects Closed or Resolved in the CTA 802.1x Wired Client (continued)

Defect ID	Headline	Description
CSCsg71040	Forced logoff by local Admin logon causes supplicant to hang	**Symptom** When a user is forced to logoff via another user (admin) log on, the CTA 802.1x Wired Client icon disappears from the system tray and the CTA 802.1x Wired Client stops responding. **Conditions** 1. User1 is logged on. 2. User1 locks the machine by pressing ctrl+alt+del and select Lock computer. The computer locked dialog is displayed. 3. Administrator logs in and, by doing so, forces User1's session to logout. **Resolution** Resolved in CTA 802.1x Wired client 4.0.5.5137 build. Resolved in CTA 2.1.101.0.
CSCsg71048	Forced logoff via remote desktop session causes supplicant to hang	**Symptom** When a user is forced to logoff via "Remote Desktop" administrator, the CTA 802.1x Wired Client icon disappears from the system tray and the CTA 802.1x Wired Client stops responding. **Conditions** IEEE 802.1x connection is already established. Remote desktop connection is established and forces session from the current user to log out. **Resolution** Resolved in CTA 2.1.103.0
CSCsh30624	Security vulnerability while launching a process	This defect reports a product security vulnerability and has been evaluated by Cisco's Product Security Incidence Response Team (PSIRT). An explanation of the defect and of the security vulnerability can be found at this location on Cisco.com. http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml

All Defects Closed or Resolved by CTA Release 2.0.1

This section describes defects that were resolved in CTA Release 2.0.1.14. For customers upgrading from CTA 2.0 to CTA 2.1, the information about these resolved bugs is new. Customers that installed CTA 2.0.1.14 have already been notified of these defect resolutions.

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14

Defect ID	Headline	Description
CSCef09817	Install does not complete if port conflict arises.	**Symptom** If there is a port conflict with CTA on Windows NT 4.0, during the CTA installation, the Cisco Trust Agent EOU Daemon service does not start, and the user is forced to cancel the installation. However, on Windows XP and Windows 2000 you will be able to finish the installation and see the port conflict error in the CTA log. **Conditions** Occurs on Windows NT. **Workaround** The port which CTA listened can be changed in the ctad.ini file. If the port is changed to a nonconflicting port then the install continues. To change the port number look up LocalPort in the CTA Administrators Guide. **Closure Comment** This is a rare case where a port conflict will arise.

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)

Defect ID	Headline	Description
CSCsb67286	CTA does not respond to EOU hello from switch. Put in hold state.	**Symptom** CTA does not respond to an EAP over UDP hello from the switch. The switch port is put into the held state. This problem occurs even if the Windows XP firewall has been configured to allow traffic to CTA or has been configured to allow traffic over EAP over UDP. At bootup, the Windows XP firewall loads a boot policy that blocks the EAPoverUDP traffic to CTA. The boot policy is loaded even if the firewall is disabled but the firewall service is still running. This behavior occurs primarily at system boot up. You can read more about the Windows firewall at this article in the Microsoft Security Developer Center: http://msdn.microsoft.com/security/productinfo/XPSP2/networkprotection/firewall.aspx. **Conditions** Windows XP Service Pack 2 - Firewall service running. **Resolution** Microsoft has supplied a hotfix to resolve this problem. See the Microsoft Knowledge Base article 917730 at http://support.microsoft.com/?kbid=917730 for complete instructions on how to download the hotfix and edit the registry to resolve this problem.
CSCsc43747	Fatal error displayed when uninstalling CTA.	**Symptom** The error dialog, *Fatal[c0029]: Timed semaphore failed* appears when uninstalling CTA. **Workaround** Ignore the error. It is a nonfatal dialog. It does not affect the uninstall. **Resolution** Resolved in CTA Release 2.0.1.14.

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)

Defect ID	Headline	Description
CSCsc65502	Incorrect notification display for non-admin privilege user	**Symptom** The same notification message appears for a non-administrator user that earlier appeared for an administrator. **Conditions** An administrator logged onto a machine and was postured; later, a non-administrator user logs onto the same machine and (for whatever posture-related reason) should receive a different notification message. **Resolution** The temporary HTML file for notification display is now stored in a new directory, \CiscoTrustAgent\ctamsg, and removed when done processing. This directory is set to read/write for all users.
CSCsd18654	Long login and eventual supplicant crash	**Symptom** User with CTA supplicant installed on Windows XP used to encounter the following: 1. User entered their Windows domain credentials incorrectly at the Microsoft GINA window. 2. After re-entering their domain credentials properly the second time, the machine took several minutes to logon to the machine and there was a supplicant crash/runtime error displayed. 3. The 802.1x Wired client services did not start. **Resolution** This defect has been resolved. The CTA 802.1x Wired Client no longer crashes after a long login period.

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)

Defect ID	Headline	Description
CSCsd33592	Scripts do not run and computer and user policies are not applied.	**Symptom** Startup scripts do not run and Group Policy Object (GPO) polices do not download. The client machine would attempted to download the startup script and download GPOs before IEEE 802.1x authentication would complete. Because IEEE 802.1x was not complete, there would be no network connection, thus scripts and GPO policy downloads would fail. **Conditions** Client machine is connected to an Active Directory (AD) domain. **Resolution** This defect has been resolved. IEEE 802.1x connection is properly achieved and startup scripts and GPO policies download correctly.
CSCsd47790	Supplicant loses association with the NIC	**Symptom** Supplicant loses association with the NIC. **Conditions** After re-authenticating many times the NIC may disappear from the supplicant list. This as been seen with short re-authentication timers, such as 5 minutes. **Resolution** CTA 802.1x Wired Client no longer loses association with the NIC.

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)

Defect ID	Headline	Description
CSCsd47821	Supplicant crashes upon service shutdown	**Symptom** CTA 802.1x Wired Client crashed upon service shutdown **Conditions** System icon disappears from the tray. 1. Login as local Admin 2. Click on cancel when prompted for user credential (by default the supplicant is set for user authentication) 3. Create a deployment profile 4. Reboot 5. Connection Client crashes on shutdown **Resolution** CTA 802.1x Wired Client no longer crashes upon service shutdown.
CSCsd50977	Roaming profiles do not work unless supplicant is disabled	**Symptom** Roaming profile can not be saved or downloaded from windows active directory server when logging in or out of the domain. If the AD username has been configured to use a roaming profile then CTA changes the local cached profile on the PC to a local profile. So this PC will not use the roaming profile anymore for this user. **Resolution** Resolved in CTA release 2.0.1.14
CSCsd96348	CTA 802.1x Wired Client crashes with Novell's ZenWorks agent installed on PC	**Symptom** CTA 802.1x Wired Client in release 2.0.0.30 will crash with Novell's ZENWorks desktop agent installed on a Windows XP machine. **Resolution** Resolved in CTA release 2.0.1.14

Table 11 Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)

Defect ID	Headline	Description
CSCse17576	CTA fatal error in PACTrust.cpp	**Symptom** When installing CTA agent for the first time, certain IBM laptops have problems with the posture-agent. There is a fatal error in the internal CTA code. **Conditions** New install of CTA. Trying to setup machine authentication for the first time, there is difficulty setting up the PAC the first time, CTA PAC process gets fatal error. **Resolution** Now setting up machine authentication works correctly without fatal error.

Closed or Resolved Cisco Product Defects that Affected CTA Performance

This section contains defects in other Cisco NAC components that affect the performance of CTA.

Table 12 Closed or Resolved Cisco NAC Component Defects

Defect ID	Headline	Explanation
CSCsc06942	Failure when EAP-FAST/PEAP credentials/posture data size is > 1K	**Symptom** When the Cisco Trust Agent 802.1x Wired Client attempts to pass more than 1002 bytes of posture data to the Cisco Secure Access Control Server (ACS), using a tunneled protocol that uses fragmentation, such as EAP-FAST, authentication fails. **Conditions** This applies only to tunneled protocols that use fragmentation (MS-PEAP, CISCO-PEAP, and EAP-FAST). It happens only when the supplicant uses the tunneled protocol fragmentation option and only if a fragment of an EAP tunnel is larger than 1002 bytes. Usually fragmentation threshold is driven from the detected MTU size (Ethernet is 1.5K). **Resolution** Resolved ACS 4.1.

Closed or Resolved NAC-Partner Defects that Affected CTA Performance

This section contains defects in third party NAC-partner products components that affect the performance of CTA.

Table 13 Resolved and Closed Defects of Third Party NAC Partner Components

Defect ID	Headline	Explanation
CSCsg04200	Posture daemon crashes when there is a Symantec plugin installed on the client and PPMsgSize is greater than 1KB.	**Symptom** If there is a Symantec posture plugin installed on the client, and PPMsgSize is set to greater than 1024 bytes (1KB), then either no data is returned from the Symantec posture plugin or Cisco Trust Agent Posture Server Daemon crashes. **Conditions** Occurs on Windows operating systems. **Resolution** The Symantec plugin can now use an application-specific ***PluginName*_PPMsgSize** parameter while other posture plugins use the value of the PPMsgSize parameter.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the Obtaining Documentation section.