



Release Notes for Cisco Trust Agent, Release 2.1 Without 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. The following information is provided:

- [Cisco Trust Agent 2.1 Release, page 3](#)
 - [Qualified Deployments of CTA 2.1, page 3](#)
 - [Obtaining the CTA 2.1 Release, page 4](#)
 - [Obtaining Cisco Secure Services Client, page 5](#)
 - [Product Versioning, page 5](#)
- [Related Documentation, page 6](#)
- [System Requirements, page 7](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- System Requirements for Installations on Linux, page 7
 - System Requirements for Installations on Mac OS X, page 8
 - System Requirements for Installation on Windows, page 9
 - Operating System Requirements for Installation of SSC, page 10
- Obtaining the Latest Release of CTA, page 11
- Installation Notes, page 12
 - CTA 2.1.1.03.0 Installation Files for Windows, page 12
- Upgrade Support, page 12
 - Upgrading CTA for Mac OS X from 2.1.103.0 to 2.1.1.04.0, page 13
- CTA 2.1 Product Limitations, page 14
 - Migrating to CTA with Cisco Secure Services Client Requires Uninstallation and Reinstallation, page 14
 - Configuring Machine Authentication, page 14
 - Windows NT is Not Supported, page 14
 - CTA is No Longer Bundled with CSA, page 15
- New Features Introduced in CTA 2.1, page 15
 - New Product Versioning Methodology, page 15
 - Single RPM Installation File for Linux Installations, page 16
 - Support for CTA on Mac OS X Operating Systems, page 16
 - Microsoft Windows Installer (MSI) Installation Files, page 16
 - New Configuration Options in CTA, page 17
 - New Posture Plugin Features, page 21
- New Features Introduced in CTA 2.0.1, page 22
 - Machine Authentication Methods, page 23
- Known Defects in CTA 2.1 Posture Agent, page 24
- Known Defects in CTA 802.1x Wired Client Which Remain In SSC, page 30
- Closed and Resolved Defects in CTA, page 32
 - Defects Closed or Resolved in CTA 2.1 Posture Agent, page 33

- Defects in CTA 802.1x Wired Client Resolved by Migrating to SSC, page 39
- All Defects Closed or Resolved by CTA Release 2.0.1, page 45
- Closed or Resolved Cisco Product Defects that Affected CTA Performance, page 51
- Closed or Resolved NAC-Partner Defects that Affected CTA Performance, page 52
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 53

Cisco Trust Agent 2.1 Release

The goals of Cisco Trust Agent, Release 2.1.103.0 for Linux and Windows operating systems and CTA 2.1.104.0 for Mac OS X, (referred to collectively as 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.

This offering of CTA 2.1.103.0 does not include a bundled supplicant, for Windows installations, as the previous offering of CTA 2.1.103.0 did. We recommend that customers who want to perform 802.1x authentication install the Cisco Secure Services Client, version 4.1.2 or later in addition to CTA 2.1.103.0.



Note

Cisco Secure Services Client (SSC) replaces the CTA 802.1x Wired Client as the preferred supplicant in a deployment of the NAC security solution. NAC is supported for use in a wired network environment.

Qualified Deployments of CTA 2.1

Cisco Trust Agent 2.1.103.0 for Linux and Windows operating systems and CTA 2.1.104.0 for Mac OS X, 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 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.

Obtaining Cisco Secure Services Client

SSC is available for download for registered users of Cisco.com. Follow this procedure to download Cisco Secure Services Client:

-
- Step 1** Navigate to <http://www.cisco.com> and log on.
- Step 2** Navigate to the SSC download area here:
<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280753707>
- Step 3** Click the link to **Cisco Secure Client Services v4.0**.
- Step 4** Click the link for the **Windows 2000** or **Windows XP** operating system.
- Step 5** Click the link to version **4.1.2**.
- Step 6** Download these three objects for that release:
- Release Notes for release 4.1.2
 - Cisco_SSC-XP2K-4_1_2_5929.msi
 - SSCAdminUtils_4.1.2.5928.zip

Product Versioning

The latest version of CTA for Windows and Linux platforms 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, Without Bundled Supplicant* and the *Release Notes for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant* 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.

The latest version of CTA for Mac OS X is CTA 2.1.104.0. The *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant* has not been updated to reflect the latest version number of CTA for Mac OS X. Any references in the documentation to CTA 2.1 or CTA 2.1.103.0 for Mac OS X are referring to CTA 2.1.104.0 unless otherwise noted.

Related Documentation

**Note**

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review Cisco Trust Agent documentation on [Cisco.com](http://www.cisco.com) for any updates.

You can find the documentation for Cisco Trust Agent, Release 2.1.103.0 by navigating Cisco.com starting at this link: http://www.cisco.com/en/US/products/ps5923/tsd_products_support_series_home.html. These are the documents that describe this offering of Cisco Trust Agent 2.1.103.0:

- *Migrating from CTA 802.1x Wired Client to Cisco Secure Services Client*
- *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*
- *Release Notes for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*

You can find the documentation for Cisco Secure Services Client, Release 4.1.2 by navigating Cisco.com starting at this link:

http://www.cisco.com/en/US/products/ps7034/tsd_products_support_series_home.html. These are the documents that describe Cisco Secure Services Client:

- *Cisco Secure Services Client Administrator Guide*, for release 4.1.2.
- *Cisco Secure Services Client User Guide*, for release 4.1.2.
- *Release Notes for Cisco Secure Services Client*, for release 4.1.2.

For documentation of other Cisco Network Admission Control (NAC) Framework components follow this link

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_sub_solution_home.html.

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 1 *CTA System Requirements for Linux*

System Component	Requirement
System	<ul style="list-style-type: none">• Pentium class processor or better• Network connection
Operating System and Language Support	<p>All available internationalized versions of these Linux operating systems support CTA 2.1.:</p> <ul style="list-style-type: none">• Red Hat Enterprise Linux v3 (Enterprise, Advanced Server, and Workstation)• Red Hat Enterprise Linux v4 (Enterprise, Advanced Server, and Workstation) <p>Note Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English.</p>
Linux Installers	Red Hat Package Management (RPM) v4.2 or greater.
Hard Disk Space	20 MB
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 2 *CTA System Requirements for Mac OS X*

System Component	Requirement
System	<ul style="list-style-type: none"> 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	<p>All available internationalized versions of Mac OS X 10.3.9 and 10.4 operating systems support CTA 2.1.</p> <p>Note Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English.</p>

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 3 *CTA System Requirements for Windows*

System Component	Requirement
System	<ul style="list-style-type: none"> 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 System	<ul style="list-style-type: none"> Windows 2000 Professional and Advanced Server, SP4 and Update Rollup 1 Windows XP Professional, SP1, SP2, and SP3 Windows XP Home, SP1, SP2, and SP3 Windows 2003 Server, SP1 and R2
Language Support for localized operating systems	<p>All available localized versions of these operating systems support this release of CTA.</p> <p>Note Support for a localized operating system is different from localized version of CTA. The CTA interface and messages are presented in English.</p> <ul style="list-style-type: none"> Windows 2000 Professional and Advanced Server, SP4 and Update Rollup 1 Windows XP Professional, SP1, SP2, and SP3 Windows XP Home, SP1, SP2, and SP3 Windows 2003 Server, SP1 and R2

Operating System Requirements for Installation of SSC

Table 4 summarizes the Windows operating systems on which SSC runs as well as the operating systems they have in common.



Note See the *Cisco Secure Services Client Administrator Guide* for a complete list of operating systems that support SSC.

Table 4 *SSC Operating System Requirements*

System Component	Windows Operating System Requirement
Windows operating systems on which Cisco Secure Services Client runs	<ul style="list-style-type: none">Windows 2000 Professional and Advanced Server, SP4.Windows XP Professional, SP1, SP2, and SP3Windows 2003 Server
Common Windows operating systems on which CTA 2.1 and Cisco Secure Services Client run.	<ul style="list-style-type: none">Windows 2000 Professional and Advanced Server, SP4Windows XP Professional, SP1, SP2, and SP3Windows 2003 Server

Obtaining the Latest Release of CTA

The latest release of Cisco Trust Agent 2.1 for Linux and Windows operating systems is version 2.1.103.0. The latest release of Cisco Trust Agent 2.1 for Mac OS X operating systems is version 2.1.104.0.

[Table 5](#) 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, Without Bundled Supplicant* for a complete description of content of the files and how they can be used in a CTA installation.

Table 5 *Files for CTA 2.1 Without Bundled Supplicant*

Downloadable File and Description of	Content of the File and Description
cta21ag_unbundled.pdf	Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant. This document is used for both CTA 2.1.103.0 and CTA 2.1.104.0 releases.
cta21rn_unbundled.pdf	Release Notes for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant. This document describes the CTA 2.1.103.0 and CTA 2.1.104.0 releases.
cta_ssc_migration.pdf	This document describes how to migrate from CTA with the CTA 802.1x Wired Client to CTA with the Cisco Secure Services Client.
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-2.1.104.0.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-2.1.104.0.dmg file used to install CTA.
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 or Cisco Secure Services Client.

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-win-2.1.x.0.msi`. Installation files in this format are referring to CTA release 2.1.103.0 for Linux and Windows and release 2.1.104.0 for Mac OS X.

CTA 2.1.1.03.0 Installation Files for Windows

In this offering of CTA 2.1.103.0, there is one installation file: `CtaAdminEx-win-2.1.103.0.exe`. This contains the `ctasetup-win-2.1.103.0.msi` file which allows administrators to accept the end user license agreement and install CTA 2.1.103.0. `CtaAdminEx-win-2.1.103.0.exe` does not contain CTA 802.1x Wired Client or Cisco Secure Services Client.

In the previous offering of CTA 2.1.103.0, there was an additional installation file: `CtaAdminEx-supplciant-win-2.1.103.0.exe`. This file allowed an administrator to install the CTA 802.1x Wired Client as well as CTA. `CtaAdminEx-supplciant-win-2.1.103.0.exe` is not being available in this offering of CTA 2.1.103.0.

When migrating from the CTA 802.1x Wired Client to Cisco Secure Services Client, you must uninstall CTA 2.1.103.0 and the CTA 802.1x Wired Client first and then re-install CTA 2.1.103.0 alone using the `CtaAdminEx-win-2.1.103.0.exe` file.

Upgrade Support

Cisco Trust Agent supports upgrade installations from versions 1.0, 2.0, 2.0.1, selective availability, and beta 2.1.x 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 2.1.103.0 with the Cisco Secure Services Client, the computer is disconnected from the network at the end of the uninstallation of CTA and CTA 802.1x Wired Client. Rebooting restores the network connection and it is a required step in the uninstallation process. Likewise, at the end of the installation of Cisco Secure Services Client a reboot is required to restore the network connection and complete the installation 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 2.1.x versions of CTA to CTA 2.1.103.0. See Chapter 2 and Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplciant*, for information about upgrading previous versions of CTA for Linux and Windows to CTA 2.1.

Upgrading CTA for Mac OS X from 2.1.103.0 to 2.1.104.0

Cisco Trust Agent supports upgrade installations from version CTA 2.1.103.0 to CTA 2.1.104.0. During the upgrade, the certificates, third-party posture plugins, ctad.ini, the ctalogd.ini, and log files remain in the directories in which they were installed by CTA 2.1.103.0. If CTA 2.1.104.0 is installed in a custom package which includes new certificates, third-party posture plugins, ctad.ini, or ctalogd.ini files, the new objects will overwrite the old objects if they have the same name.

To upgrade CTA 2.1.103.0 to CTA 2.1.104.0, use the instructions for installing CTA in Chapter 3 of the *Administrator Guide for Cisco Trust Agent, Release 2.1* and simply install CTA 2.1.104.0 over CTA 2.1.103.0 while it is running.

CTA 2.1 Product Limitations

Review these limitations of CTA 2.1 before installing or upgrading to the release of CTA 2.1.103.0.

Migrating to CTA with Cisco Secure Services Client Requires Uninstallation and Reinstallation

Migrating from CTA with the CTA 802.1x Wired Client to CTA 2.1.103.0 with Cisco Secure Services Client requires you to uninstall CTA and the CTA 802.1x Wired Client then reinstall CTA 2.1.103.0 and install Cisco Secure Services Client.

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 Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*.

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

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. Cisco Secure Services Client is not available for the Mac OS X operating system.

Microsoft Windows Installer (MSI) Installation Files

You can download CtaAdminEx-win-2.1.103.0.exe to install CTA on Windows operating systems. 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.



Note

Previously the scripting interface feature could be enabled using the “/si” argument. Now that the installation files uses standard MSI commands, the /si argument is 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.



Note

CtaAdminex-supplciant-win-2.1.103.0.exe contained CTA 2.1.103.0 and the CTA 802.1x Wired Client. This installation file is no longer provided beginning with this offering of CTA 2.1.103.0.

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 6 *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 7 *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, Without Bundled Supplicant*, 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, Without Bundled Supplicant*, 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_PPMSize** 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:

- PPMSize 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, Without Bundled Supplicant*, 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, Without Bundled Supplicant*, 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, Without Bundled Supplicant* 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, Without Bundled Supplicant*, 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, Without Bundled Supplicant*, 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 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.

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, Without Bundled Supplicant* 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, Without Bundled Supplicant* for more information.

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.



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 8 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.	<p>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:</p> <pre>2 12:00:00.000 11/11/2005 Sev=Critical/1 PSDaemon/0xE3C0001A Failed to Read Registry Key, error code 2</pre> <p>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.</p> <p>Workaround No workarounds are available. Note that this log message is erroneous and does not affect the running of Cisco Trust Agent.</p>

Table 8 ***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.	<p>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.</p> <p>This message is in the ACS Failed Attempts log: “EAP-TLS or PEAP authentication failed during SSL handshake.”</p> <p>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.</p> <p>Workaround Remove this expired root certificate from the user certificate store.</p>
CSCsg08764	CTAstat incorrectly reports operational status for plugin	<p>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.</p> <p>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.</p> <p>Workaround Enable logging on the client in order to capture information about the failed plugin.</p>

Table 8 ***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	<p>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.</p> <p>Conditions Running CTA 2.1.14.0 and PPMsgSize is set to 1024 in ctad.ini and occurs on Windows operating systems.</p> <p>Workaround None.</p> <p>Note This problem is NOT reproducible with CTA 2.1.18.0 or later versions.</p>
CSCsg26209	CTA does not support downgrade of posture plugins	<p>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.”</p> <p>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.</p> <p>Workaround Uninstall the higher revision of the plugin then install the version of the plugin that corresponds to the downgraded application’s version.</p> <p>Note You can verify the version numbers of the plugin and application by viewing their properties.</p>

Table 8 **Known Defects in the CTA 2.1 Posture Agent Client (continued)**

Defect ID	Headline	Explanation
CSCsi49862	CTA should set BootTimeUDPExemptions as String Value	<p>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.</p> <p>Conditions BootTimeUDPExemptions is set to 1 in ctad.ini. This is the default setting.</p> <p>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</p>
CSCsi91317	HostPP truncates MAC addresses if there are 2 or more	<p>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.</p> <p>Conditions Host machine has more than one active IPV4 interfaces, and the host is postured of the HostPP MacAddress.</p> <p>Workaround None.</p>

Table 8 **Known Defects in the CTA 2.1 Posture Agent Client (continued)**

Defect ID	Headline	Explanation
CSCsi91358	HostPP truncates MAC addresses if there are two or more	<p>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.</p> <p>Conditions Host machine has more than one active IPV4 interfaces, and the host is postured of the HostPP MacAddress.</p> <p>Workaround None.</p>
CSCsj76891	CTACERT.exe throws application exception	<p>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.</p> <p>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”</p> <p>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.</p>

Table 8 ***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.	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>Conditions This occurs in all versions of Danish Windows operating systems.</p> <p>Workaround None</p>

Known Defects in CTA 802.1x Wired Client Which Remain In SSC

This section describes the defects reported in CTA 802.1x Wired Client which are also in Cisco Secure Client Services 4.1.2.5929. These defects will be addressed in a future release of SSC.

Table 9 ***Known Defects in SSC Which Were Also in the CTA 2.1 802.1x Wired Client***

Defect ID	Headline	Explanation
CSCsd60058 (Reassigned to SSC CSCsj08723)	802.1x, EAP-GTC password change fails when password complexity requirement is enforced.	<p>Symptom Password change fails with EAP-GTC.</p> <p>Conditions ACS is configured for EAP-GTC and password complexity rule enabled on Active Directory.</p> <p>Workaround Disable password complexity rule on Active Directory.</p>

Table 9 ***Known Defects in SSC Which Were Also in the CTA 2.1 802.1x Wired Client***

Defect ID	Headline	Explanation
CSCse93282 (Reassigned to SSC using CSCsi53715)	Supplicant does not validate user certificate with user entered credentials	<p>Symptom</p> <ol style="list-style-type: none"> 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. <p>Conditions ACS is configured to use EAP-MSCHAPv2 (ONLY) as inner authentication method.</p> <p>ACS uses Windows Active Directory as back-end user database.</p> <p>The client uses an authentication profile with these attributes:</p> <ul style="list-style-type: none"> • 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. <p>Workaround There is no workaround.</p>

Table 9
Known Defects in SSC Which Were Also in the CTA 2.1 802.1x Wired Client

Defect ID	Headline	Explanation
CSCsg23722 (Reassigned to SSC using CSCsi52902)	User not allowed to change incorrect username right away.	<p>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.</p> <p>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.</p> <p>Workaround After about 30 seconds, the user receives another popup dialog box where they can enter the correct username.</p>
CSCsh39205 (Reassigned to SSC using CSCsi52889)	Cancelled shutdown causes supplicant icon to disappear	<p>Symptom The Cisco Trust Agent 802.1x wired client icon no longer appears in the Windows system tray.</p> <p>Conditions User has cancelled a Windows shutdown sequence, logged off, and re-logged in to Windows with a different user account.</p> <p>Workaround There is no workaround.</p>

Closed and Resolved Defects in CTA

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

- [Defects Closed or Resolved in CTA 2.1 Posture Agent, page 33](#)
- [Defects in CTA 802.1x Wired Client Resolved by Migrating to SSC, page 39](#)
- [All Defects Closed or Resolved by CTA Release 2.0.1, page 45](#)

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 10 *Defects Closed or Resolved in the CTA Posture Agent*

Defect ID	Headline	Description
CSCsb09542	With EnableLogonNotifies=1, strange results during logon and logoff	<p>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.</p> <p>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).</p> <p>Resolution Resolved in CTA Release 2.1.100.0</p>
CSCsd43949	Posture notification not displaying after 802.1x authentication/posture	<p>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.</p> <p>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.</p> <p>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</p>

Table 10 **Defects Closed or Resolved in the CTA Posture Agent (continued)**

Defect ID	Headline	Description
CSCse02440	Ctacert /add command needs better error codes	<p>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.</p> <p>Conditions Any error condition encountered produces the same error message. Note that using ctacert without any options at all produces the same error message.</p> <p>Resolution Resolved in CTA Release 2.1.100.0</p> <ul style="list-style-type: none"> 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 10 **Defects Closed or Resolved in the CTA Posture Agent (continued)**

Defect ID	Headline	Description
CSCse23586	ctaeou stops responding to NAD	<p>Symptom CTA EOU Daemon stops responding to a layer 3 network access device.</p> <p>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.</p> <p>Resolution Resolved in CTA Release 2.1.100.0</p>
CSCse27560	CTA should not remove 802.1x Wired Clients files during install/upgrade	<p>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.</p> <p>Conditions All.</p> <p>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</p>

Table 10 **Defects Closed or Resolved in the CTA Posture Agent (continued)**

Defect ID	Headline	Description
CSCse50876	Scripting interface not registering posture data file	<p>Symptom Customer posture information is not being sent via the scripting interface to ACS.</p> <p>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.</p> <p>Resolution Added the “VendorIDName=Cisco Systems” field to the description of the Information file in <i>Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant</i> and made clear that the information file must be a plain text file. Resolved in CTA Release 2.1.100.0</p>
CSCse76333	EapHandlePacket Error	<p>Symptom Although very rare, CTA Posture Server Daemon intermittently fails to return the posture data.</p> <p>Conditions No posture data is returned from CTA and an “EapHandlePacket Error” entry is logged in the CTA log.</p> <p>Resolution Resolved in CTA Release 2.1.100.0</p>

Table 10 **Defects Closed or Resolved in the CTA Posture Agent (continued)**

Defect ID	Headline	Description
CSCse90646	ctacert.exe fails on some installations	<p>Symptom Ctacert.exe fails to import a known good certificate on some CTA installs.</p> <p>Conditions This has been noticed most on Windows 2000 installations of CTA.</p> <p>Workaround Install the certificate directly into the the local certificate store using Internet Explorer, Microsoft Management Console, or the ctaCert utility. See the <i>Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant</i> for more information about the ctaCert utility.</p> <p>Closure comment This defect was closed because it was unreproducible. Closed in CTA Release 2.1.100.0</p>
CSCsf16515	hostpp on XP spk1 installed causes ctad.exe to take 100% CPU	<p>Symptom ctad.exe for CTA 1.0.55 spikes to 100%</p> <p>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).</p> <p>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</p>

Table 10 **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.	<p>Symptom Browser auto-launch feature may not work with the default timers set.</p> <p>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.</p> <p>Resolution The default value of this parameter was increased to 25 seconds. This was resolved in CTA build 2.1.102.0</p>
CSCsg23794	802.1x wired client Clear Credentials button not documented in Administrator Guide for Cisco Trust Agent, Release 2.1.	<p>Symptom The <i>Administrator Guide for Cisco Trust Agent, Release 2.1</i> does not explain the functionality of the Clear Credentials button in the Network Configuration Summary window of the 802.1x Wired Client user interface.</p> <p>Conditions All.</p> <p>Resolution Resolved in CTA Release 2.1.100.0. See Chapter 9 of the <i>Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant</i>, for more information on this feature.</p>
CSCsg94979	Remote Desktop issue with machine state	<p>Symptom When RDP session is started the machine state reported to ACS changes to booting.</p> <p>Conditions Upon starting a RDP session. Reported in CTA 2.1.100.0</p> <p>Resolution Resolved in CTA Release 2.1.101.0</p>

Table 10 **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. Registered users of Cisco.com can read an explanation of the defect and of the security vulnerability at this location: http://www.cisco.com/warp/public/707/cisco-sa-20070221-supPLICANT.shtml
CSCsi58799	Mac OS X CTA displays notification in administrator context before user logs in	Symptom 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. Registered users of Cisco.com can read an explanation of the defect and of the security vulnerability at this location: http://www.cisco.com/warp/public/707/cisco-sr-20070611-cta.shtml

Defects in CTA 802.1x Wired Client Resolved by Migrating to SSC

These are the defects in the CTA 802.1x Wired Client that was bundled and released with the previous offering of CTA 2.1.103.0.

These defects are not present in Cisco Secure Services Client, 4.1.2.5929. By migrating to SSC, you can avoid working around these known problems of CTA 802.1x Wired Client.

Table 11 **Defects in the CTA 2.1 802.1x Wired Client Resolved by Migrating to SSC**

Defect ID	Headline	Explanation
CSCsb88110	The 802.1X Wired Client pop up box is hidden during bootup with multiple interfaces.	<p>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.</p> <p>Conditions This occurs with multiple interfaces that are all getting authenticated.</p> <p>Workaround Set the EnableLogonNotifies attribute to 0 in the ctad.ini for CTA.</p>
CSCsc31219	User credentials dialog does not close upon failure to connect.	<p>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.</p> <p>Workaround Users need to manually close the user credentials dialog box.</p>

Table 11 **Defects in the CTA 2.1 802.1x Wired Client Resolved by Migrating to SSC (continued)**

Defect ID	Headline	Explanation
CSCsc39374	RSA 5.2 new pin mode does not work with CTA 802.1x Wired Client	<p>Symptom User authentication fails.</p> <p>Conditions RSA 5.2 is used for authentication. This is the behavior the user experiences:</p> <ol style="list-style-type: none"> 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. <p>Workaround There is no workaround.</p>
CSCse35094	Password entered in supplicant Credentials popup is not used.	<p>Symptom Password entered in supplicant Credentials popup is not used for authentication.</p> <p>Conditions With machine and user authentication enabled, the password entered in supplicant Credentials popup is not used for authentication.</p> <p>Workaround There is no workaround.</p>
CSCse35113	CTA 802.1x Wired Client can indicate that the ethernet interface is authenticated and connected when it is not.	<p>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.</p> <p>Conditions This error can happen when you try to reconnect after a failed authentication.</p> <p>Workaround The incorrect connection status will time out in about one minute.</p>

Table 11 *Defects in the CTA 2.1 802.1x Wired Client Resolved by Migrating to SSC (continued)*

Defect ID	Headline	Explanation
CSCse77264	CTA 802.1x Wired Client fails to launch after a reboot	<p>Symptom This problem occurs intermittently. Reboot the client on which CTA and 802.1x Wired Client is installed. You see the following behaviors:</p> <ul style="list-style-type: none"> • 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. <p>Conditions Behavior was detected on Windows 2000 Professional with Service Pack 4. 802.1x Wired Client is configured to prompt for user password.</p> <p>Workaround There is no workaround.</p>

Table 11 **Defects in the CTA 2.1 802.1x Wired Client Resolved by Migrating to SSC (continued)**

Defect ID	Headline	Explanation
CSCsf24460	CTA 802.1x Wired Client EAP-FAST Inner identity in UPN format should include domain.	<p>Symptom ACS initiates a domain controller lookup of a username in UPN format that either fails or takes a long time to complete.</p> <p>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.</p> <p>Workaround None, other than re-architect the Windows network to avoid multi-domain lookups.</p>
CSCsf29547	CTA 802.1x Wired Client remains in connecting state when certificate is revoked.	<p>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.</p> <p>Conditions CTA 802.1x Wired Client is configured for machine authentication only and it uses a revoked machine certificate.</p> <p>Workaround There is no workaround.</p>
CSCsf32767	CTA 802.1x Wired Client sends wrong password after Active Directory password change.	<p>Symptom IEEE 802.1x user authentication may fail if user has to change Active Directory password.</p> <p>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.</p> <p>Workaround Reboot or logoff the user and attempt a login with the new/correct Active Directory credentials.</p>

Table 11 **Defects in the CTA 2.1 802.1x Wired Client Resolved by Migrating to SSC (continued)**

Defect ID	Headline	Explanation
CSCsg14487	Password is cached even when GTC is configured	<p>Symptom OTP passwords are cached after a successful connection attempt until the subsequent connections (3 attempts) have failed authentication.</p> <p>Conditions GTC is enabled on ACS.</p> <p>Workaround Click “clear credentials” button in Network Configuration Summary window prior to making a connection attempt.</p>
CSCsh17908	Windows CTA 802.1x Wired Client conflicts with some Smart Card software	<p>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</p> <p>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 interfered with Windows authentication using this software.</p> <p>Workaround Current version of Cisco SSC 802.1x client combined with the non-802.1x CTA client worked in this environment.</p>

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 12 **Defects Closed or Resolved by CTA Release 2.0.1.14**

Defect ID	Headline	Description
CSCef09817	Install does not complete if port conflict arises.	<p>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.</p> <p>Conditions Occurs on Windows NT.</p> <p>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.</p> <p>Closure Comment This is a rare case where a port conflict will arise.</p>

Table 12 **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.	<p>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.</p> <p>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.</p> <p>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.</p> <p>Conditions Windows XP Service Pack 2 - Firewall service running.</p> <p>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.</p>
CSCsc43747	Fatal error displayed when uninstalling CTA.	<p>Symptom The error dialog, <i>Fatal[c0029]: Timed semaphore failed</i> appears when uninstalling CTA.</p> <p>Workaround Ignore the error. It is a nonfatal dialog. It does not affect the uninstall.</p> <p>Resolution Resolved in CTA Release 2.0.1.14.</p>

Table 12 **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	<p>Symptom The same notification message appears for a non-administrator user that earlier appeared for an administrator.</p> <p>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.</p> <p>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.</p>
CSCsd18654	Long login and eventual supplicant crash	<p>Symptom User with CTA supplicant installed on Windows XP used to encounter the following:</p> <ol style="list-style-type: none"> 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. <p>Resolution This defect has been resolved. The CTA 802.1x Wired Client no longer crashes after a long login period.</p>

Table 12 **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.	<p>Symptom Startup scripts do not run and Group Policy Object (GPO) policies do not download.</p> <p>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.</p> <p>Conditions Client machine is connected to an Active Directory (AD) domain.</p> <p>Resolution This defect has been resolved. IEEE 802.1x connection is properly achieved and startup scripts and GPO policies download correctly.</p>
CSCsd47790	Supplicant loses association with the NIC	<p>Symptom Supplicant loses association with the NIC.</p> <p>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.</p> <p>Resolution CTA 802.1x Wired Client no longer loses association with the NIC.</p>

Table 12 **Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)**

Defect ID	Headline	Description
CSCsd47821	Supplicant crashes upon service shutdown	<p>Symptom CTA 802.1x Wired Client crashed upon service shutdown</p> <p>Conditions System icon disappears from the tray.</p> <ol style="list-style-type: none"> 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 <p>Resolution CTA 802.1x Wired Client no longer crashes upon service shutdown.</p>
CSCsd50977	Roaming profiles do not work unless supplicant is disabled	<p>Symptom Roaming profile can not be saved or downloaded from windows active directory server when logging in or out of the domain.</p> <p>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.</p> <p>Resolution Resolved in CTA release 2.0.1.14</p>
CSCsd96348	CTA 802.1x Wired Client crashes with Novell's ZenWorks agent installed on PC	<p>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.</p> <p>Resolution Resolved in CTA release 2.0.1.14</p>

Table 12 *Defects Closed or Resolved by CTA Release 2.0.1.14 (continued)*

Defect ID	Headline	Description
CSCse17576	CTA fatal error in PACTrust.cpp	<p>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.</p> <p>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.</p> <p>Resolution Now setting up machine authentication works correctly without fatal error.</p>

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 13 *Closed or Resolved Cisco NAC Component Defects*

Defect ID	Headline	Explanation
CSCsc06942	Failure when EAP-FAST/PEAP credentials/posture data size is > 1K	<p>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.</p> <p>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.</p> <p>Usually fragmentation threshold is driven from the detected MTU size (Ethernet is 1.5K).</p> <p>Resolution Resolved ACS 4.1.</p>

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 14 *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.	<p>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.</p> <p>Conditions Occurs on Windows operating systems.</p> <p>Resolution The Symantec plugin can now use an application-specific <i>PluginName_PPMsgSize</i> parameter while other posture plugins use the value of the PPMsgSize parameter.</p>

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>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

