



Migrating from CTA 802.1x Wired Client to Cisco Secure Services Client

Revised: May 23, 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13679-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Migrating from CTA 802.1x Wired Client to Cisco Secure Services Client

© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience vi

Conventions vi

Related Documentation vii

Obtaining Documentation, Obtaining Support, and Security Guidelines viii

CHAPTER 1

Cisco Secure Services Client and CTA 802.1x Wired Client Comparison 1-1

Comparing SSC and CTA 802.1x Wired Client Supplicant Functions 1-2

Method of Creating a Deployment Package 1-2

Creating New Network Connections 1-2

Public Authentication Profile 1-3

Automatic User Connection is Configurable 1-3

Pre-Windows-Logon User Authentication 1-4

Storage Options for User Credentials 1-4

Configuring EAP-FAST Connection Settings 1-4

Installation Directories 1-5

Logging Tools 1-6

Comparing SSC and CTA 802.1x Wired Client Supplicant User Interfaces 1-6

SSC Wired and Wireless License Information 1-7

Configuring User and Machine Credentials 1-10

Configuring Client Authentication Settings 1-12

Configuring Trusted Server Validation and Rules 1-14

Configuring Authentication Retry Settings 1-18

CHAPTER 2

Migrating from CTA with CTA 802.1x Wired Client to CTA with SSC 2-1

Operating System Requirements for Installation of CTA 2.1.103.0 and SSC 2-2

CTA 2.1.103.0 Installation File 2-3

SSC 4.1.2 Installation Files 2-3

Upgrade Procedures 2-4

Installing SSC for an Existing CTA 2.1.103.0 Installation 2-4

Upgrading CTA 2.1.x with CTA 802.1x Wired Client to CTA 2.1.103 and SSC 2-5

Upgrading CTA 2.0 to CTA 2.1.103.0 and Installing SSC 2-5

Upgrading CTA 2.0 with CTA 802.1x Wired Client to CTA 2.1.103 and Installing SSC 2-6

Upgrading CTA 1.0 to CTA 2.1.103.0 and Installing SSC 2-7

Uninstalling CTA and the CTA 802.1x Wired Client 2-7

Uninstalling CTA and the CTA 802.1x Wired Client Using Add or Remove Programs 2-7

Uninstalling CTA and the CTA 802.1x Wired Client Using Standard Msiexec.exe Commands 2-8

Examples of SSC Deployment Packages 2-8

Machine Authentication Deployment Package 2-9

Machine and User Authentication Deployment Package File 2-11

User Authentication Deployment Package File 2-14



Preface

The Cisco Secure Services Client (SSC) is an 802.1x authentication supplicant used to create secure wired and wireless connections to a network protected by the IEEE 802.1x security protocol.

The SSC software that customers download from Cisco.com comes with a permanent license for wired-network supplicant functionality. Customers also have the option of downloading a temporary 90 day license for wireless-network supplicant functionality if they choose.

SSC is downloaded and installed separately from Cisco Trust Agent (CTA), release 2.1.103.0.

The CTA 802.1x Wired Client is an 802.1x authentication supplicant is used to create secure wired connections to a network protected by the IEEE 802.1x security protocol. It comes with a permanent license for wired-network supplicant functionality. The CTA 802.1x Wired Client does not have the capability of performing 802.1x authentication on a wireless network.

CTA 802.1x Wired Client was previously bundled with CTA 2.1.103.0. This offering of CTA 2.1.103.0 unbundles the CTA 802.1x Wired Client software from CTA. For customers migrating from the previous bundled version of CTA 2.1.103.0, we recommend that customers uninstall the previous bundled version of CTA 2.1.103.0 and install the unbundled version of CTA 2.1.103.0 and Cisco Secure Services Client, version 4.1.2 or later.



Note

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.

Audience

The *Migrating from CTA 802.1x Wired Client to Cisco Secure Services Client* provides installation, configuration, and monitoring information to administrators responsible for deploying Cisco Trust Agent and Cisco Secure Services Client to network clients.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	boldface font
Variables for which you supply values and new or important terminology	<i>italic</i> font
Displayed session and system information, paths and filenames	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Indicates menu items to select, in the order you select them	Option > Network Preferences



Tip

Identifies information to help you get the most benefit from your product.



Note

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning**

Identifies information that you must heed to prevent injuring yourself or damaging the state of the software or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

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.

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>



CHAPTER 1

Cisco Secure Services Client and CTA 802.1x Wired Client Comparison

This chapter compares the functions, interfaces, and methods of configuration used by the Cisco Secure Services Client (SSC) and the CTA 802.1x Wired Client.

This chapter contains these sections:

- [Comparing SSC and CTA 802.1x Wired Client Supplicant Functions, page 1-2](#)
 - [Method of Creating a Deployment Package, page 1-2](#)
 - [Creating New Network Connections, page 1-2](#)
 - [Public Authentication Profile, page 1-3](#)
 - [Automatic User Connection is Configurable, page 1-3](#)
 - [Pre-Windows-Logon User Authentication, page 1-4](#)
 - [Storage Options for User Credentials, page 1-4](#)
 - [Configuring EAP-FAST Connection Settings, page 1-4](#)
 - [Installation Directories, page 1-5](#)
 - [Logging Tools, page 1-6](#)
- [Comparing SSC and CTA 802.1x Wired Client Supplicant User Interfaces, page 1-6](#)
 - [SSC Wired and Wireless License Information, page 1-7](#)
 - [Configuring User and Machine Credentials, page 1-10](#)

- [Configuring Client Authentication Settings, page 1-12](#)
- [Configuring Trusted Server Validation and Rules, page 1-14](#)
- [Configuring Authentication Retry Settings, page 1-18](#)

Comparing SSC and CTA 802.1x Wired Client Supplicant Functions

Method of Creating a Deployment Package

SSC's deployment package is a digitally signed and encrypted XML file which defines the authentication requirements for the client and defines the amount of control a user has over the SSC interface.

The XML file is created by the administrator using an XML editor. It is parsed, encrypted, and signed using administrative utilities provided with the downloaded software. After the distribution package has been created, it is compiled in the SSC installation file. When SSC is installed, the deployment package is installed at the same time.

The CTA 802.1x Wired Client deployment package consists of two XML files which define the authentication requirements for the client. The user is given minimal control over the CTA 802.1x Wired Client interface by default.

CTA 802.1x Wired Client administrators create the authentication profile XML files using a wizard which guides them through the creation process. Unlike Cisco Secure Services Client, the CTA 802.1x Wired Client authentication profile XML files are not recompiled into the CTA 802.1x Wired Client installation file; they are distributed separately.

Creating New Network Connections

SSC can be configured to allow users to create new network connections. This provides flexibility for those users who move their computers out of the enterprise network and into home or travel networks. SSC can also be configured to prevent users from creating networks. This configuration is meant for computers that will only access networks within your enterprise.

CTA 802.1x Wired Client does not allow users to create new network connections and it can not be configured to do so.

Public Authentication Profile

SSC allows for the creation of a public authentication profile. This profile is used by all users of the same computer. The public profile may require machine, user, or both machine and user authentication. Server validation can be required for a public profile.

**Note**

In order to perform machine authentication, the authentication profile must be public.

You can not create a public profile for the CTA 802.1x Wired Client.

Automatic User Connection is Configurable

After users log on to their computers, SSC can either be configured to automatically attempt to connect to the network or require the user to manually connect to the network. This is not configurable with the CTA 802.1x Wired Client. The CTA 802.1x Wired Client always attempts to connect to the network automatically.

User authentication occurs when SSC attempts to establish the connection to the network, whether automatically or manually.

A restart of the auto-connection process occurs after one of these events:

- An existing connection is lost
- A connection attempt fails on one access device
- The set of available and configured Access Devices changes based on an updated wireless scan or wired link-up and there is a network adapter available
- A new adapter becomes available
- When the machine resumes from hibernation or suspension

Pre-Windows-Logon User Authentication

SSC can be configured to delay performing Windows network logon until after 802.1x authentication is performed. This eliminates a race condition between 802.1x authentication and Windows networking tasks.

The CTA 802.1x Wired Client does not have this capability. In the case of CTA 802.1x Wired Client, 802.1x authentication and Windows networking tasks are attempted simultaneously.

Storage Options for User Credentials

When a user authentication profile requires users to be prompted for their username and password in order to log on to the network, SSC can be configured to save their credentials forever, for the current session, or for five minutes.

The CTA 802.1x Wired Client saves user credentials forever by default and can not be configured.

Configuring EAP-FAST Connection Settings

SSC provides these methods of configuring the EAP-FAST authentication session:

- Enable fast reconnect
- Protect client certificate
- Use Smartcard-based Client Certificates Only

Enable Fast Reconnect

When SSC is configured to allow for fast reconnects, SSC responds to a re-authentication request using cached credentials. This applies to both outer and inner tunnel methods. CTA 802.1x Wired Client is not able to configure this aspect of EAP-FAST authentication.

Protect Client Certificate

When SSC or the CTA 802.1x Wired Client are configured to protect the client certificate, both supplicants refuse to send the certificate to the authentication server during Phase 1 of the authentication request because this phase of the EAP-FAST authentication is unprotected. Instead, both supplicants send the client certificate during Phase 2 of the EAP-FAST authentication. In Phase 2 of the EAP-FAST authentication, the client certificate is encrypted when sent through the inner tunnel.

Use Smartcard-based Client Certificates Only

When this feature is configured, SSC sends the authentication server only a client certificate from a smartcard. If you are performing machine authentication, this option is not allowed because a machine certificate must be obtained from the OS store. CTA 802.1x Wired Client is not able to configure this aspect of EAP-FAST authentication.

Installation Directories

The installation directories are different for SSC and CTA 802.1x Wired Client.

SSC is installed by default in this directory:

C:\Program Files\Cisco Systems\Cisco Secure Services Client

CTA 802.1x Wired Client is installed by default in this directory:

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

Logging Tools

The System Report tool is available for both SSC and CTA 802.1x Wired Client.

For SSC, it can be reached by navigating Start > Programs > Cisco Secure Services Client > Cisco Secure Services Client System Report.

For the CTA 802.1x Wired Client, it can be reached by navigating Start > Programs > Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client System Report.

The System Report provides summary information about all the network adapters found on the computer, it identifies and collects authentication profile files, technical logs, and system logs. This information is stored in a zip file that is placed on the computer's desktop.

To use the System Report Tool, follow this procedure:

-
- Step 1** Open the System Report tool.
 - Step 2** Click **Collect Data**.
 - Step 3** After the output to the console has stopped, click Locate Report File. Windows Explorer opens and the report file is highlighted.

Comparing SSC and CTA 802.1x Wired Client Supplicant User Interfaces

SSC and CTA 802.1x Wired Client supplicants each provide users with an interface to configure network connections but these interfaces are used for different purposes.

SSC can be configured to allow users to create and configure network connections from their computer using a GUI. These connection profiles are created only for use on an individual computer.

SSC administrators create connection profiles, called “deployment packages,” by creating an XML file that follows the SSC distribution package schema. These deployment package files are compiled in SSC installation .msi files and distributed throughout an organization. When SSC is installed it is already configured with the attributes in the deployment package.

CTA 802.1x Wired Client users can not configure network connections for their computers using a GUI or any other method. CTA 802.1x Wired Client administrators create deployment packages using the deployment package wizard in the CTA 802.1x Wired Client. Those deployment packages can be distributed to all the users of their enterprise.

Though their purposes are different, SSC's GUI and CTA 802.1x Wired Client's deployment package wizard have many similarities. This section is intended to orient administrators who are already familiar with CTA 802.1x Wired Client's deployment package wizard with SSC's GUI interface as well as identify the XML elements in SSC's deployment package file that are equivalent to the settings in the user interfaces.

**Note**

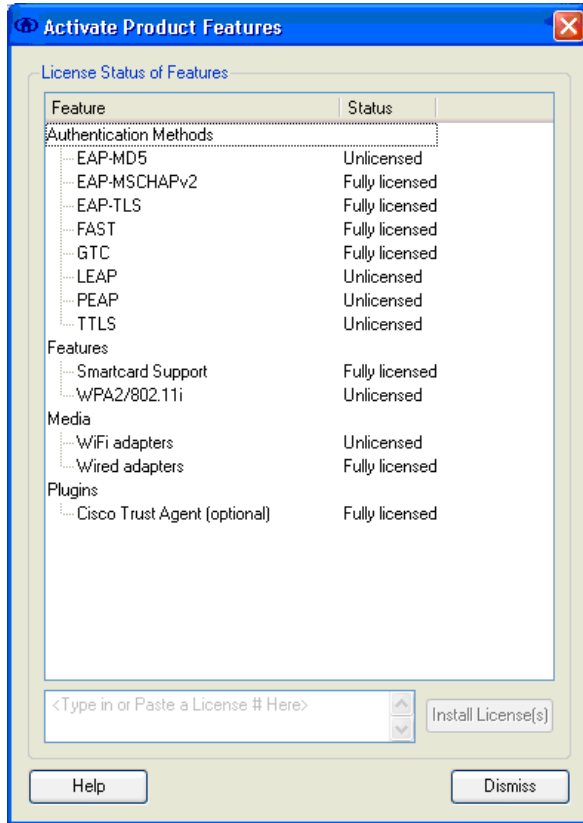
The XML elements used in the deployment package XML files are described at length in Chapter 2 of the *Cisco Secure Services Client Administrator Guide*, located here on Cisco.com:

http://www.cisco.com/en/US/products/ps7034/prod_maintenance_guides_list.html. Read that document for a complete discussion of how the elements are nested and configured in a deployment package.

SSC Wired and Wireless License Information

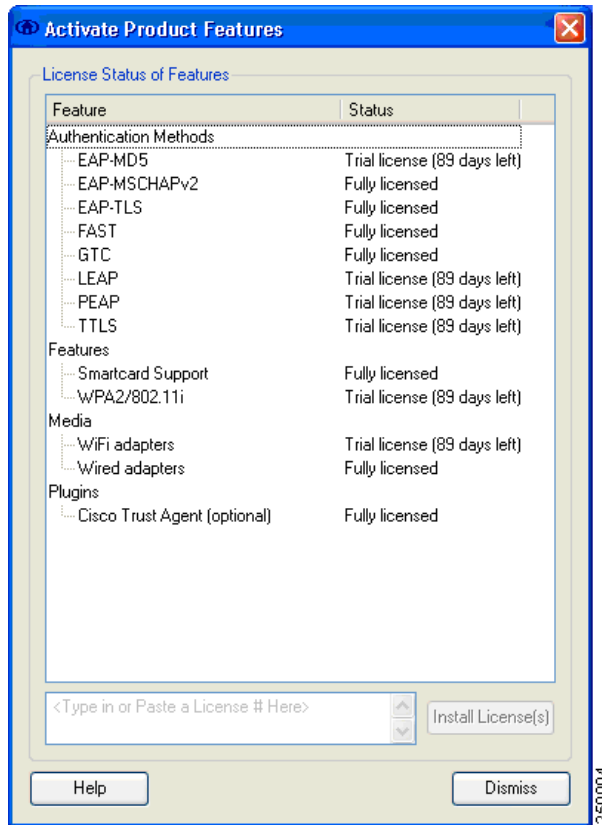
The configuration of the SSC that is obtained from the cisco.com SSC download page (the default client) is a fully licensed, non-expiring license, wired-only client. It supports EAP-FAST with EAP-MSCHAPv2, EAP-GTC and EAP-TLS (SmartCard credentials). By navigating Help > Activation, the user with the wired only license would see the dialog box in [Figure 1-1](#).

Figure 1-1 Activate Product Features dialog for a wired-only license



If demonstration of the wireless functionality is desired, a 90-day trial license for this feature is available for download at the same site. Also added is support for additional authentication methods: LEAP, EAP-PEAP, EAP-TTLS and EAP-MD5. By navigating Help > Activation, the user with the wireless trial license would see the dialog box in [Figure 1-2](#).

Figure 1-2 Activate Product Features dialog for wireless trial license



Configuring User and Machine Credentials

Figure 1-3 shows the location of where user credentials are set in the CTA 802.1x Wired Client and in SSC.

CTA 802.1x Wired Client administrators specify user authentication credentials in the Station Policy dialog box using radio buttons in the area numbered 1.

If their configuration of SSC permits, SSC users specify user authentication credentials in the SSC Network Profile dialog box. Clicking **Modify** in the area numbered 1 opens the SSC Network Authentication Dialog box. That is where user credentials can be defined as machine credentials and specify if user credentials are requested, or users are authenticated, with their Windows logon username and password.

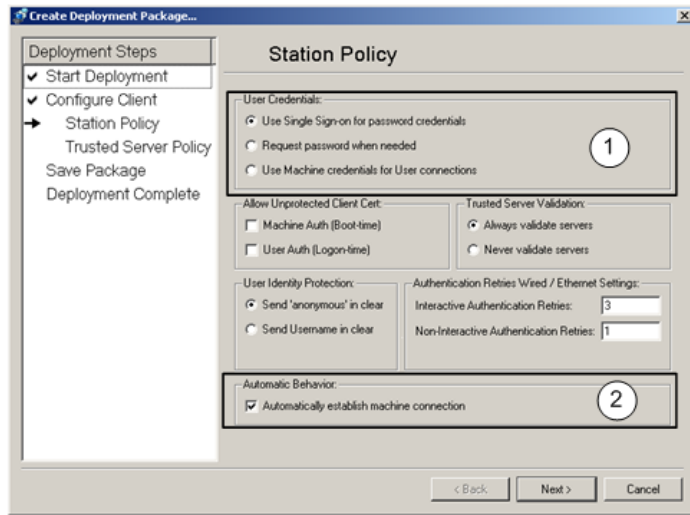
CTA 802.1x Wired Client administrators configure “Machine authentication only” by checking **Use Machine Credentials for User Credentials** check box in area 1 of the CTA 802.1x Wired Client Station Policy dialog box and by checking **Automatically establish machine connection** in area numbered 2.

SSC users create a “Machine authentication only” profile by checking **Automatically establish machine connection**, in the area numbered 2 in the SSC Network Profile Dialog box, by clicking **Modify**, and by selecting the **Use Machine Credentials** radio button in the area numbered 1 in the Network Authentication Dialog box.

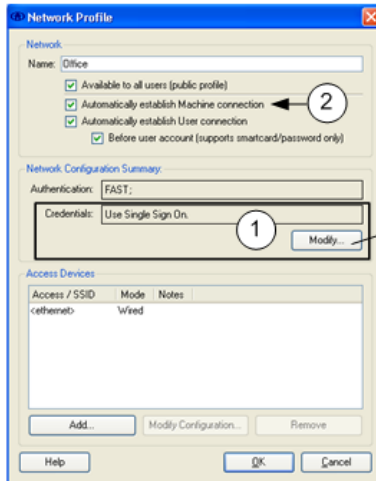
SSC administrators specify user and machine authentication credentials in the <authenticationNetwork> element of the deployment package XML file.

Figure 1-3 Location of User Credential Settings in User Interfaces

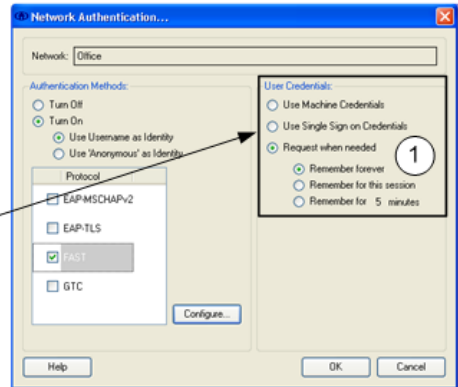
CTA 802.1x Wired Client Create Deployment Package Dialog Box



SSC Network Profile Dialog Box



SSC Network Authentication Dialog Box

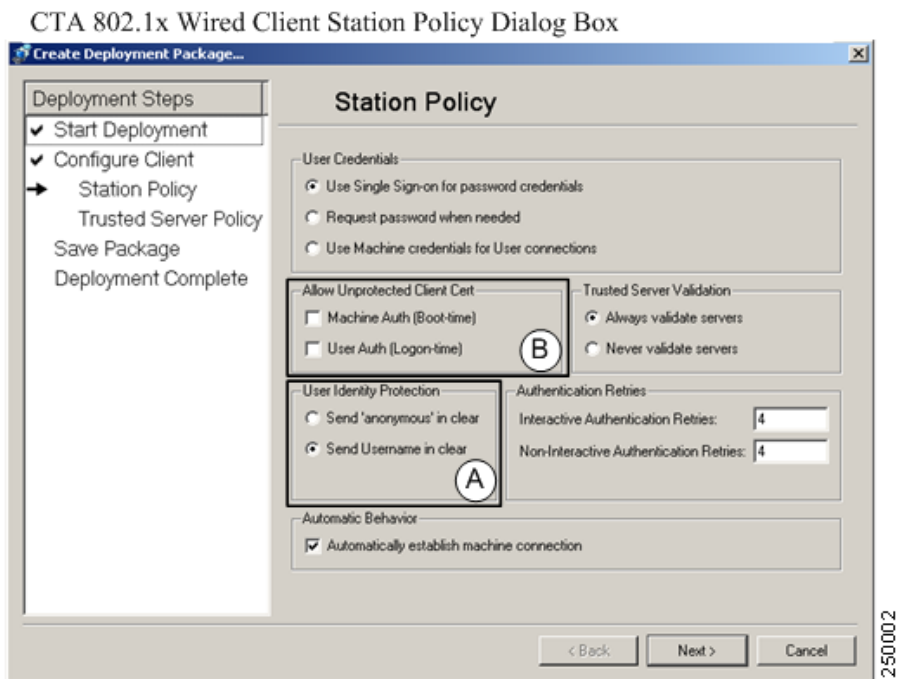


250009

Configuring Client Authentication Settings

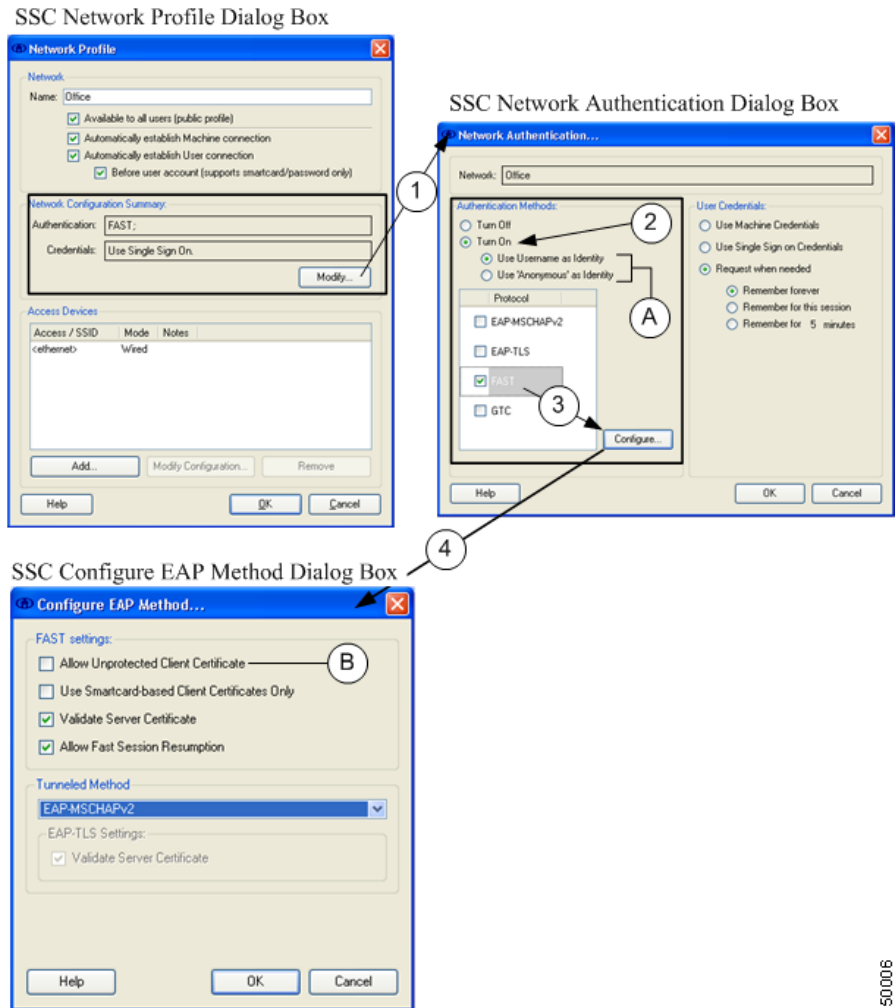
Figure 1-4 shows the client authentication settings in CTA 802.1x Wired Client and Figure 1-5 shows where these client authentication settings are found in SSC.

Figure 1-4 Client Authentication Settings in CTA 802.1x Wired Client



CTA 802.1x Wired Client administrators specify if users' username and domain are sent during Phase 1 of EAP-FAST authentication in the User Identity Protection area, labeled A. In the area labeled B, CTA 802.1x Wired Client administrators specify if the client certificate can be sent during Phase 1 of EAP-FAST authentication.

Figure 1-5 Client Authentication Settings in SSC



If their configuration of SSC permits, SSC users can specify if their username and domain are sent and if the client certificate is sent during Phase 1 of EAP-FAST authentication. Users start by clicking **Modify** in the Network Configuration Summary area of the Network Profile dialog box. This opens the Network Authentication dialog box. By turning on authentication methods, users specify if

their connection profile allows the username and domain or “anonymous” to be sent during Phase 1 of EAP-FAST authentication. These fields are labeled A in [Figure 1-5](#).

In either case, users can then specify EAP-FAST as the “outer method” or Phase 1 protocol by checking **FAST**. After clicking **Configure**, users specify if the client certificate is sent unprotected during Phase 1 of EAP-FAST authentication by checking or not checking **Allow Unprotected Client Certificate**; that field is labeled B in [Figure 1-5](#).

SSC administrators specify if username and domain or “anonymous” are sent during Phase 1 of EAP-FAST authentication by configuring the `<useAnonymousId>` element associated with `<machineAuthentication>`, `<userAuthentication>` or `<machineUserAuthentication>` element in the XML deployment package file. Configuring the `<protectClientCertificate>` element determines whether or not the client certificate is sent to the authentication server during Phase 1 of EAP-FAST authentication.

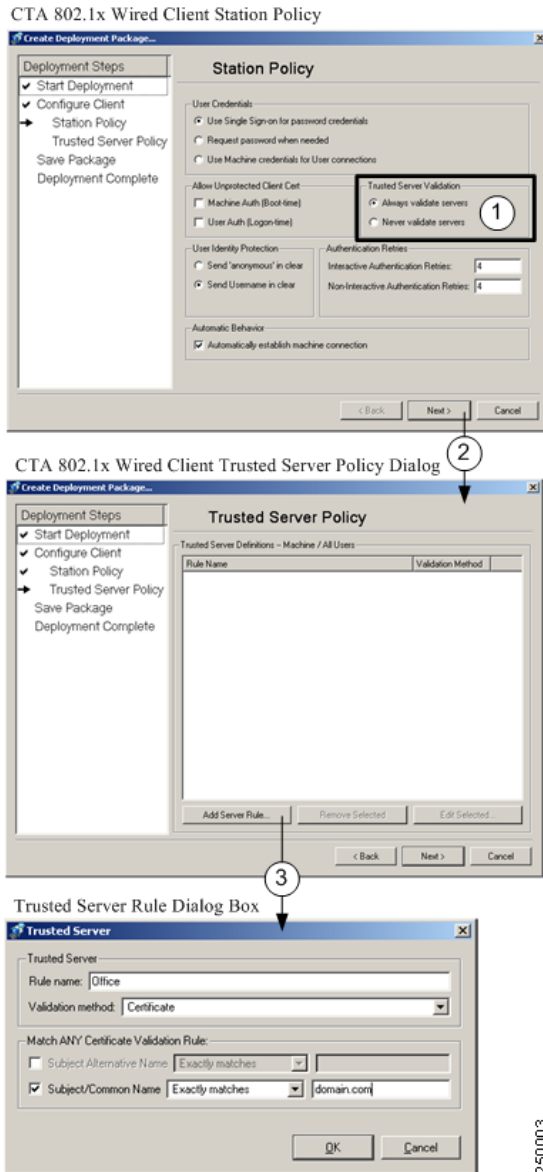
Configuring Trusted Server Validation and Rules

CTA 802.1x Wired Client administrators configure trusted servers by selecting **Always validate servers** in the Trusted Server Validation area of the Station Policy dialog box. When the administrator clicks **Next**, the Trusted Server Policy dialog opens. Clicking **Add Server Rule** allows the administrator to create the rule to validate the server certificate. These dialog boxes are illustrated in [Figure 1-6](#).

SSC users can create a connection profile using server validation rules if their distribution of SSC allows them to do so. Configuring trusted servers is done in two parts. One part is to create a trusted server rule as shown in [Figure 1-7](#). The other part is to configure EAP-FAST authentication to require that a server be validated, this is shown in [Figure 1-8](#).

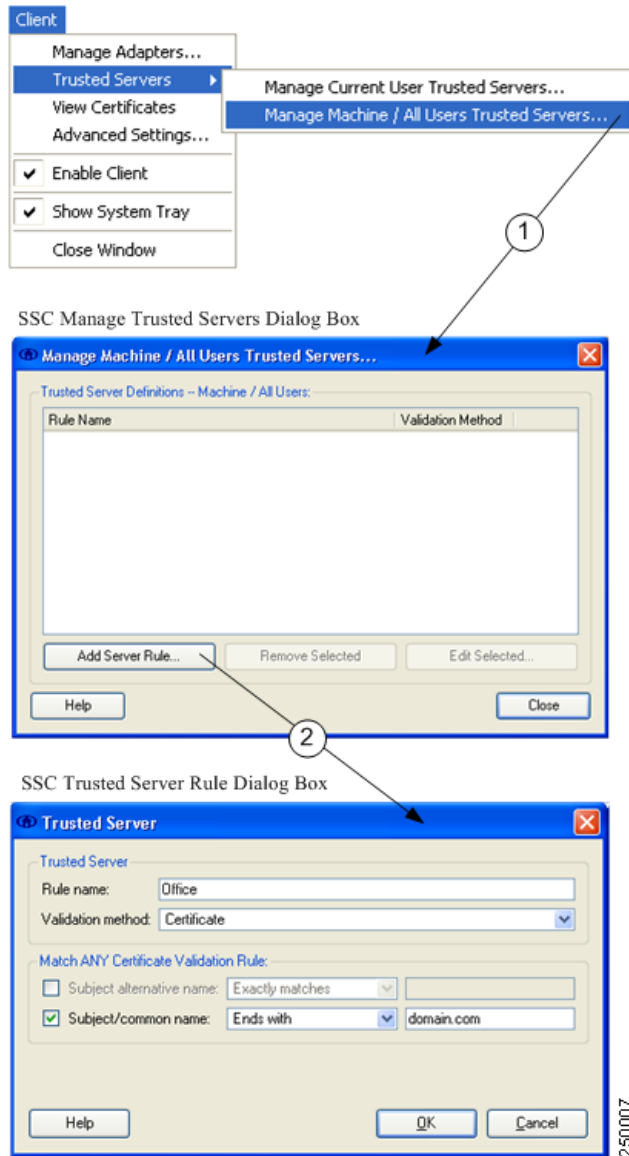
SSC administrators configure the use of trusted servers in the deployment package XML file, in two steps. When configuring the `<eapFAST>` EAP Method, the `<validateServerIdentity>` element is set to **true**. Administrators specify server validation rules in the `<validationRules>` element and which certificates to trust using the `<trustAnyrootCaFromOs/>` and `<trustedRootCaCerts>` elements. These elements are children of the `<serverValidation>` element which is a child of the `<authenticationNetwork>` element.

Figure 1-6 CTA 802.1x Wired Client Configuring Trusted Server



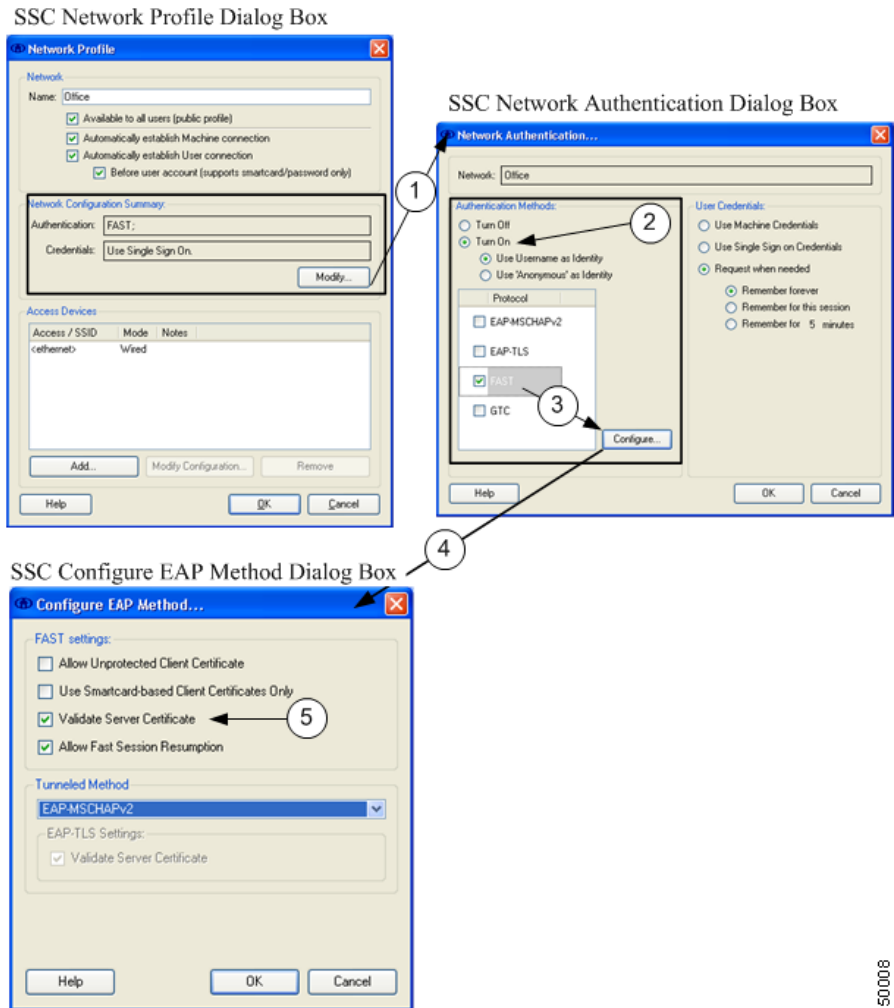
250003

Figure 1-7 SSC Create Trusted Server Rule



250007

Figure 1-8 SSC Validate Server Certificate

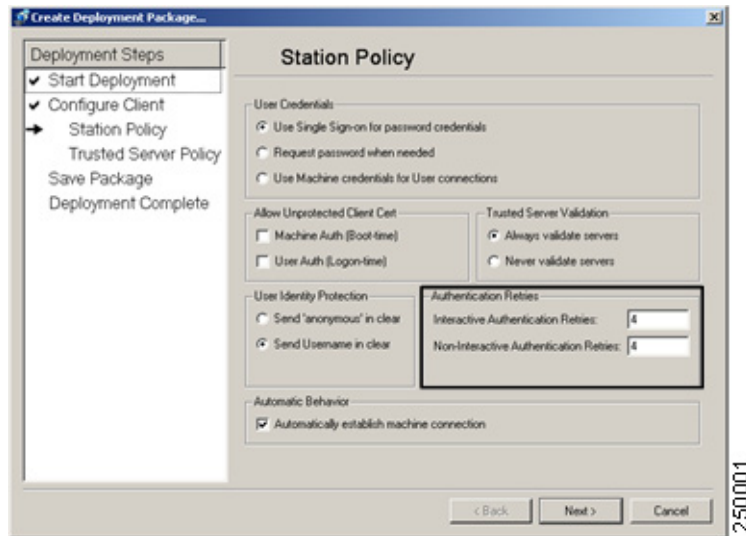


250008

Configuring Authentication Retry Settings

Some network access devices have the ability to open a port, but switch the user into a special vlan after a failed connection attempt. In order to support these access devices, the client provides the administrator with the capability of adjusting the number of connection retries before disconnecting.

Figure 1-9 CTA 802.1x Wired Client Authentication Retries Counters



CTA 802.1x Wired Client administrators specify the number of Interactive Authentication Retries and Non-interactive Authentication Retries in the Authentication Retries area of the Create Deployment Package dialog box. These fields are marked in [Figure 1-9](#).

SSC users can not configure authentication retries settings when creating a local network connection profile.

SSC administrators configure this setting using the `<interactiveAuthenticationRetries>` and `<nonInteractiveAuthenticationRetries>` elements which are children of the `<machineUserAuthentication>`, `<userAuthentication>`, or `<machineAuthentication>` elements.



CHAPTER 2

Migrating from CTA with CTA 802.1x Wired Client to CTA with SSC

The recommended version of Cisco Trust Agent is release 2.1.103.0. If you want to perform machine or user authentication using the IEEE 802.1x security protocol, Cisco recommends using the Cisco Secure Services Client supplicant, release 4.1.2 or later.

This chapter contains these sections:

- [Operating System Requirements for Installation of CTA 2.1.103.0 and SSC, page 2-2](#)
- [CTA 2.1.103.0 Installation File, page 2-3](#)
- [SSC 4.1.2 Installation Files, page 2-3](#)
- [Upgrade Procedures, page 2-4](#)
 - [Installing SSC for an Existing CTA 2.1.103.0 Installation, page 2-4](#)
 - [Upgrading CTA 2.1.x with CTA 802.1x Wired Client to CTA 2.1.103 and SSC, page 2-5](#)
 - [Upgrading CTA 2.0 to CTA 2.1.103.0 and Installing SSC, page 2-5](#)
 - [Upgrading CTA 2.0 with CTA 802.1x Wired Client to CTA 2.1.103 and Installing SSC, page 2-6](#)
 - [Upgrading CTA 1.0 to CTA 2.1.103.0 and Installing SSC, page 2-7](#)
- [Uninstalling CTA and the CTA 802.1x Wired Client, page 2-7](#)
 - [Uninstalling CTA and the CTA 802.1x Wired Client Using Add or Remove Programs, page 2-7](#)

- Uninstalling CTA and the CTA 802.1x Wired Client Using Standard Msiexec.exe Commands, page 2-8
- Examples of SSC Deployment Packages, page 2-8
 - Machine Authentication Deployment Package, page 2-9
 - Machine and User Authentication Deployment Package File, page 2-11
 - User Authentication Deployment Package File, page 2-14

Operating System Requirements for Installation of CTA 2.1.103.0 and SSC

Table 2-1 summarizes the Windows operating systems on which CTA 2.1.103.0 and SSC run 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 and the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant* for a complete list of operating systems that support CTA.

Table 2-1 CTA System Requirements

System Component	CTA 2.1.103.0 Requirement
Windows operating systems on which CTA 2.1 runs	<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

System Component	CTA 2.1.103.0 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 SP3 Windows 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, SP4 Windows XP Professional, SP1, SP2, and SP3 Windows 2003 Server

CTA 2.1.103.0 Installation File

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.

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.

SSC 4.1.2 Installation Files

Download these files to install SSC 4.1.2:

- Cisco_SSC-XP2K-4_1_2_5929.msi
- SSCAdminUtils_4.1.2.5928.zip

The Cisco_SSC-XP2K-4_1_2_5929.msi is the generic “out of the box” version of SSC. SSC as downloaded from cisco.com is not configured. It is intended for use by an IT organization that is responsible for configuring and deploying a derived, end-user version. This deployed version is appropriate for use by the various

enterprise departments and organizations that you support. The IT Administrator you have control over the user experience and the end-user's allowed choices and configuration options. The out-of-the-box version has a fully open policy that allows access to most features and requires configuring a network when initially started. However, only through a deployed distribution package file, that is, a SSC configuration file, does the IT Administrator have full access to all settings and network configurations.

The `SSCAdminUtils_4.1.2.5928.zip` file contains utilities which perform these functions:

- Validate the preprocessed distribution package for both schema and business rule violations.
- Encrypt all credentials and secrets from their original clear text.
- Retrieve and packages any optional files referred to in the input file.
- Digitally sign the distribution package file to help prevent any tampering with its contents while it resides in the end station.
- Create a new SSC installation file that incorporates the deployment package XML file in the “out of the box” installation file.

For a complete description of the contents of the SSC `SSCAdminUtils_4.1.2.5928.zip` file, the utilities it provides and how they are used, see the *Cisco Secure Services Client Administrator Guide*.

Upgrade Procedures

These procedures describe migrating from your current installation of CTA to CTA 2.1.103.0 and Cisco Secure Services Client, release 4.1.2 or later.

Installing SSC for an Existing CTA 2.1.103.0 Installation

This upgrade scenario assumes that CTA 2.1.103.0 is installed without the CTA 802.1x Wired Client and that CTA 2.1.103.0 was installed using the `CtaAdminEx-win-2.1.103.0.exe` file.



Note SSC does not control wireless adapters while configured for wired-only, however, co-existence with all 802.1x supplicants has not been qualified.

- Step 1** Install SSC according to the *Cisco Secure Services Client Administrator Guide*.
- Step 2** Reboot when prompted.

Upgrading CTA 2.1.x with CTA 802.1x Wired Client to CTA 2.1.103 and SSC

This upgrade scenario assumes that CTA 2.1.103.0 and CTA 802.1x Wired Client are installed on the computer and you want to upgrade the supplicant from CTA 802.1x Wired Client to Cisco Secure Services Client.



Note SSC does not control wireless adapters while configured for wired-only, however, co-existence with all 802.1x supplicants has not been qualified.

- Step 1** Uninstall CTA 2.1.103.0 with CTA 802.1x Wired Client. See [“Uninstalling CTA and the CTA 802.1x Wired Client”](#) section on page 2-7 for these instructions.
- Step 2** Reboot the computer when prompted.
- Step 3** Install CTA 2.1.103.0 using the **CtaAdminEx-win-2.1.103.0.exe** file. Follow the installation instructions in Chapter 4 of the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*.
- Step 4** Install SSC 4.1.2. or later by following the directions in the *Cisco Secure Services Client Administrator Guide*.
- Step 5** Reboot the computer when prompted.

Upgrading CTA 2.0 to CTA 2.1.103.0 and Installing SSC

This upgrade scenario assumes that CTA 2.0.0.30 is already installed and that you want to upgrade to CTA 2.1.103.0 and add the Cisco Secure Services Client.



Note SSC does not control wireless adapters while configured for wired-only, however, co-existence with all 802.1x supplicants has not been qualified.

-
- Step 1** Upgrade CTA 2.0 to CTA 2.1.103.0. To upgrade, use the **CtaAdminEx-win-2.1.103.0.exe** file and follow the installation instructions in Chapter 4, of the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*.
- Step 2** Install Cisco Secure Services Client 4.1.2 or later according to the *Cisco Secure Services Client Administrator Guide*.
- Step 3** Reboot when prompted.

Upgrading CTA 2.0 with CTA 802.1x Wired Client to CTA 2.1.103 and Installing SSC

This upgrade scenario assumes that CTA 2.0.0.30 and CTA 802.1x Wired Client are installed on the computer and you want to upgrade CTA 2.0.0.30 to CTA 2.1.103.0 and upgrade the CTA 802.1x Wired Client supplicant to Cisco Secure Services Client supplicant.



Note SSC does not control wireless adapters while configured for wired-only, however, co-existence with all 802.1x supplicants has not been qualified.

-
- Step 1** Uninstall CTA 2.0.0.30 and the CTA 802.1x Wired Client. See [“Uninstalling CTA and the CTA 802.1x Wired Client”](#) section on page 2-7 for these procedures.
- Step 2** Reboot the computer when prompted.
- Step 3** Install CTA 2.1.103.0 using the **CtaAdminEx-win-2.1.103.0.exe** file. Follow the instructions in Chapter 4, of the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant* for this procedure.
- Step 4** Install SSC 4.1.2 or later by following the instructions in the *Cisco Secure Services Client Administrator Guide*.
- Step 5** Reboot the computer when prompted.

Upgrading CTA 1.0 to CTA 2.1.103.0 and Installing SSC

This upgrade scenario assumes that CTA 1.0 is already installed and that you want to upgrade to CTA 2.1.103.0 and add the Cisco Secure Services Client.

**Note**

SSC does not control wireless adapters while configured for wired-only, however, co-existence with all 802.1x supplicants has not been qualified.

-
- Step 1** Upgrade CTA 1.0 to CTA 2.1.103.0. To upgrade, use the **CtaAdminEx-win-2.1.103.0.exe** file and follow the installation instructions in Chapter 4, of the *Administrator Guide for Cisco Trust Agent, Release 2.1, Without Bundled Supplicant*.
- Step 2** Install Cisco Secure Services Client 4.1.2 or later according to the *Cisco Secure Services Client Administrator Guide*.
- Step 3** Reboot when prompted.

Uninstalling CTA and the CTA 802.1x Wired Client

CTA 2.1.103.0 and the CTA 802.1x Wired Client were installed together using the CtaAdminex-supplicant-win-2.1.103.0.exe file. They are also uninstalled together using either the **Add or Remove Programs** interface on Windows Operating Systems or by using the **Msiexec.exe** commands.

**Note**

After uninstalling CTA and the CTA 802.1x Wired Client, you will lose wired network connectivity until after you reboot.

Uninstalling CTA and the CTA 802.1x Wired Client Using Add or Remove Programs

-
- Step 1** Navigate Start > Settings > Control Panel.
- Step 2** Double-click **Add or Remove Programs**.

- Step 3** Select **Cisco Trust Agent 2.1.103.0**.
- Step 4** Click **Remove**.
- Step 5** Click **Yes** to confirm your desire to uninstall CTA.
- Step 6** Click **Yes** to restart your computer.
- Step 7** (Optional) After the computer reboots, you can manually delete the CTA 802.1x Wired Client Directory:

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

Uninstalling CTA and the CTA 802.1x Wired Client Using Standard Msiexec.exe Commands

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

-
- Step 1** Open the Windows Registry Editor.
 - Step 2** Navigate to **HKEY_LOCAL_MACHINE\Software\Cisco Systems\Cisco Trust Agent**.

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

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

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

After running the command you will be prompted to reboot your computer.

Examples of SSC Deployment Packages

This section contains examples of SSC deployment packages that require machine authentication, machine and user authentication, and user authentication. Some of the elements are called out for explanation and others are not. For a complete description of the elements used in a deployment package XML file, and their interoperability, see Chapter 2 of the *Cisco Secure Services Administrator Guide*.

Machine Authentication Deployment Package

Example 2-1 on page 2-10 is an example of a deployment package file requiring machine authentication. These characteristics of the deployment package are numbered in the example:

1. Authenticate machine credentials only
2. Source of machine credential is the Microsoft Active Directory
3. Restrict sending the UserName in the EAP Identity response of the outer (unprotected) tunnel. Send anonymous@Domain for the Identity response.
4. EAP settings:
 - a. Use EAP-FAST for EAP method (outer method).
 - b. Do not validate server certificates
 - c. Respond to a re-authentication request using cached credentials.
 - d. Do not send client certificate unprotected during the unprotected (phase 1) portion of --FAST PAC provisioning. The client certificate will be sent after a tunnel is established. PAC provisioning.
 - e. Use “eapMschapv2” as inner EAP method
5. Set the number of non-interactive and interactive authentication retry attempts to four.



Note The elements `<interactiveAuthenticationRetries>` and `<nonInteractiveAuthenticationRetries` are both children of the `<authenticationNetwork>` element.

6. Prevent the end-user from creating new networks.
7. Allow the end-user to directly license CSSC via the Active Product Features dialog.
8. Allow only “wired” network connections.
9. The `<allowUserSimultaneousConnectionsControl>` and `<allowUserWpaHandshakeValidationControl>` elements are both children of the `<networkPolicy>` element

Example 2-1 Machine Authentication Deployment Package File

```

<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="distributionPackage.xsd" major_version="4"
minor_version="1" maintenance_version="2">
<license>SQ2G-MYVX-AKUM-T4FN-PYCQ-IFEI-4B42-2ANC-TQCR-OKBY-OSAL-UGRF-O5EM-5ENM-I4CL-I65K-V
KGV-3XYR</license>
  <networkPolicy>
    <allowedAssociationModes></allowedAssociationModes>
    <allowedEapMethods>
(4a)   <eapFast/>
    </allowedEapMethods>
    <serverValidationPolicy>
      <allowUserValidationControl/>
    </serverValidationPolicy>
(9)
<allowUserSimultaneousConnectionsControl>false</allowUserSimultaneousConnectionsControl>
  <allowedCredentialStorage>
    <forever/>
    <logonSession/>
  </allowedCredentialStorage>
(9)
<allowUserWpaHandshakeValidationControl>false</allowUserWpaHandshakeValidationControl>
  <allowPublicProfileCreation>false</allowPublicProfileCreation>
</networkPolicy>
<networks>
  <wiredNetwork>
    <displayName>TestNetwork1</displayName>
    <authenticationNetwork>
(1)   <machineAuthentication>
      <collectionMethod>
(2)   <auto/>
      </collectionMethod>
(3)   <useAnonymousId>true</useAnonymousId>
(4)   <eapMethods>
(4a)   <eapFast>
(4b)   <validateServerIdentity>false</validateServerIdentity>
(4c)   <enableFastReconnect>true</enableFastReconnect>
(4d)   <protectClientCertificate>true</protectClientCertificate>
      <innerEapMethods>
(4e)   <eapMschapv2/>
      </innerEapMethods>
    </eapFast>
    </eapMethods>
  </machineAuthentication>
(5)   <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>

```

```
(5) <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
    </authenticationNetwork>
    </wiredNetwork>
</networks>
<connectionSettings>
  <simultaneousConnections>singleHomed</simultaneousConnections>
  <validateWpaHandshake>true</validateWpaHandshake>
</connectionSettings>
<userControlPolicy>
(6)   <clientUIType>preset</clientUIType>
(7)   <allowLicensing>true</allowLicensing>
      <allowedMedia>
(8)     <wired/>
        </allowedMedia>
      </userControlPolicy>
</configuration>
```

Machine and User Authentication Deployment Package File

[Example 2-2 on page 2-12](#) is an example of a distribution package file requiring machine and user authentication. These characteristics of the deployment package are numbered in the example:

1. Authenticate both machine and user credentials
2. Source of machine credential is the Microsoft Active Directory
3. Restrict sending the UserName in the EAP Identity response of the outer (unprotected) tunnel. Send anonymous@Domain for the Identity response.
4. When the user logs into the system, automatically initiate the user-context connection process.
5. Use username/password entered by a user for the operating system login for user authentication.
6. EAP setting:
 - a. Use EAP-FAST for EAP method (outer method)
 - b. Validate server certificate
 - c. Respond to a re-authentication request using cached credentials.
 - d. Do not send client certificate unprotected during the unprotected (phase 1) portion of FAST PAC provisioning. The client certificate will be sent after a tunnel is established.

- e. Use “eapMschapv2” or “eapGtc” as inner EAP method
7. Server certificate trust rule:
 - a. SubjectAltName (DNS name) must end with “cisco.com”.
 - b. Trust any CA certificates that have been placed in the proper Windows Certificate Store
 8. Set the number of non-interactive and interactive authentication retry attempts to four.



Note The elements <interactiveAuthenticationRetries> and <nonInteractiveAuthenticationRetries> are both children of the <authenticationNetwork> element.

9. Prevent the end-user from creating new networks
10. Do not allow licensing by the user interface. Licensing can be controlled only from the distribution package.
11. Allow only “wired” network connections.
12. The <allowUserSimultaneousConnectionsControl> and <allowUserWpaHandshakeValidationControl> elements are both children of the <networkPolicy> element.

Example 2-2 Machine and User Authentication Deployment Package

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="distributionPackage.xsd" major_version="4"
minor_version="1">

<license>SQ2G-MYVX-AKUM-T4FN-PYCQ-IFEI-4B42-2ANC-TQCR-OKBY-OSAL-UGRF-O5EM-5ENM-I4CL-I65K-V
KGV-3XYR</license>
  <networkPolicy>
    <allowedAssociationModes>
      <open/>
    </allowedAssociationModes>
    <allowedEapMethods>
      <eapFast/>
    </allowedEapMethods>
    <serverValidationPolicy>
      <allowUserValidationControl/>
    </serverValidationPolicy>
  </networkPolicy>
</configuration>
```

(6a)

```

(12)
<allowUserSimultaneousConnectionsControl>>false</allowUserSimultaneousConnectionsControl>
  <allowedCredentialStorage>
    <forever/>
    <logonSession/>
    <duration>60</duration>
  </allowedCredentialStorage>
(12)
<allowUserWpaHandshakeValidationControl>>true</allowUserWpaHandshakeValidationControl>
  <allowPublicProfileCreation>>false</allowPublicProfileCreation>
</networkPolicy>
<networks>
  <wiredNetwork>
    <displayName>CorporateNetwork</displayName>
    <authenticationNetwork>
(1)      <machineUserAuthentication>
          <machine>
(2)            <collectionMethod>
                <auto/>
            </collectionMethod>
(3)            <useAnonymousId>true</useAnonymousId>
          </machine>
          <user>
(4)            <autoConnect>true</autoConnect>
            <collectionMethod>
(5)              <singleSignOn/>
            </collectionMethod>
(3)            <useAnonymousId>true</useAnonymousId>
          </user>
(6)      <eapMethods>
(6a)        <eapFast>
(6b)          <validateServerIdentity>true</validateServerIdentity>
(6c)          <enableFastReconnect>true</enableFastReconnect>
(6d)          <protectClientCertificate>true</protectClientCertificate>
          <innerEapMethods>
(6e)            <eapMschapv2/>
(6e)            <eapGtc/>
          </innerEapMethods>
        </eapFast>
      </eapMethods>
    </machineUserAuthentication>
(7)  <serverValidation>
      <validationRules>
(7a)        <matchSubjectAlternativeName match="endsWith"
            name="altName1">cisco.com</matchSubjectAlternativeName>
      </validationRules>
(7b)        <trustAnyRootCaFromOs/>
    </serverValidation>

```

```

(8)         <interactiveAuthenticationRetries>5</interactiveAuthenticationRetries>
(8) <nonInteractiveAuthenticationRetries>5</nonInteractiveAuthenticationRetries>
         </authenticationNetwork>
         </wiredNetwork>
</networks>
<connectionSettings>
  <simultaneousConnections>singleHomed</simultaneousConnections>
  <validateWpaHandshake>true</validateWpaHandshake>
</connectionSettings>
<userControlPolicy>
(9)   <clientUIType>preset</clientUIType>
(10)  <allowLicensing>false</allowLicensing>
      <allowedMedia>
(11)   <wired/>
      </allowedMedia>
</userControlPolicy>
</configuration>

```

User Authentication Deployment Package File

[Example 2-3 on page 2-15](#) is an example of a distribution package file requiring user authentication. These characteristics of the deployment package are numbered in the example:

1. Authenticate user credentials only
2. When the user logs into the system, automatically initiate the user-context connection process.
3. Attempt to connect to the network before the user logs into Windows.
4. Use username/password entered by a user for the operating system login for user authentication.
5. Restrict sending the UserName in the EAP Identity response of the outer (unprotected) tunnel. Send anonymous@Domain for the Identity response.
6. EAP setting:
 - a. Use EAP-FAST for EAP method (outer method)
 - b. Validate server certificate
 - c. Respond to a re-authentication request using cached credentials

- d. Do not send client certificate unprotected during the unprotected (phase 1) portion of FAST PAC provisioning. The client certificate will be sent after a tunnel is established
 - e. Use “eapMschapv2” or “eapGtc” as inner EAP method
7. Server certificate trust rule:
 - a. subject name (common name or domain name) must end with “cisco.com”
 - b. Trust any CA certificates that have been placed in the proper Windows Certificate Store
 8. Set the number of non-interactive and interactive authentication retry attempts to four



Note The elements <interactiveAuthenticationRetries> and <nonInteractiveAuthenticationRetries> are both children of the <authenticationNetwork> element.

9. Prevent the end-user from creating new networks
10. Do not allow licensing by the user interface. Licensing can be controlled only from the distribution package.
11. Allow only “wired” network connections
12. The <allowUserSimultaneousConnectionsControl> and <allowUserWpaHandshakeValidationControl> elements are both children of the <networkPolicy> element

Example 2-3 User Authentication Deployment Package File

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="distributionPackage.xsd" major_version="4"
minor_version="1">

<license>SQ2G-MYVX-AKUM-T4FN-PYCQ-IFEI-4B42-2ANC-TQCR-OKBY-OSAL-UGRF-O5EM-5ENM-I4CL-I65K-V
KGV-3XYR</license>
  <networkPolicy>
    <allowedAssociationModes>
      <open/>
    </allowedAssociationModes>
    (6a) <allowedEapMethods>
```

Examples of SSC Deployment Packages

```

    <eapFast/>
  </allowedEapMethods>
  <serverValidationPolicy>
    <alwaysValidate>
      <allowUserTrustedServers>false</allowUserTrustedServers>
    </alwaysValidate>
  </serverValidationPolicy>
(12)
<allowUserSimultaneousConnectionsControl>false</allowUserSimultaneousConnectionsControl>
  <allowedCredentialStorage>
    <forever/>
    <logonSession/>
    <duration>60</duration>
  </allowedCredentialStorage>
(12)
<allowUserWpaHandshakeValidationControl>true</allowUserWpaHandshakeValidationControl>
  <allowPublicProfileCreation>false</allowPublicProfileCreation>
</networkPolicy>
<networks>
  <wiredNetwork>
    <displayName>CorporateNetwork</displayName>
    <authenticationNetwork>
(1)      <userAuthentication>
(2)        <autoConnect>
(3)          <connectBeforeLogon>true</connectBeforeLogon>
        </autoConnect>
        <collectionMethod>
(4)          <singleSignOn/>
        </collectionMethod>
(5)        <useAnonymousId>true</useAnonymousId>
(6)        <eapMethods>
(6a)          <eapFast>
(6b)            <validateServerIdentity>true</validateServerIdentity>
(6c)            <enableFastReconnect>true</enableFastReconnect>
(6d)            <protectClientCertificate>true</protectClientCertificate>
            <innerEapMethods>
(6e)              <eapMschapv2/>
(6e)              <eapGtc/>
            </innerEapMethods>
          </eapFast>
        </eapMethods>
      </userAuthentication>
    </authenticationNetwork>
  </wiredNetwork>
(7) <serverValidation>
(7a)   <validationRules>
        <matchSubjectName match="endsWith"
          name="subjectName1">cisco.com</matchSubjectName>
      </validationRules>
(7b)   <trustAnyRootCaFromOs/>

```

```

        </serverValidation>
(8)        <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
(8)
<nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
        </authenticationNetwork>
        </wiredNetwork>
</networks>
<connectionSettings>
        <simultaneousConnections>singleHomed</simultaneousConnections>
        <validateWpaHandshake>true</validateWpaHandshake>
</connectionSettings>
<userControlPolicy>
(9)   <clientUIType>preset</clientUIType>
(10)  <allowLicensing>>false</allowLicensing>
        <allowedMedia>
(11)   <wired/>
        </allowedMedia>
        </userControlPolicy>
</configuration>
```

■ Examples of SSC Deployment Packages



INDEX

A

Administrator Guide for Cisco Trust Agent, Release 2.1 [2-5](#), [2-6](#), [2-7](#)

authentication retry attempts [2-9](#), [2-10](#), [2-12](#), [2-14](#), [2-15](#), [2-17](#)

C

cached credentials [1-4](#)

certificate trust rule [2-12](#), [2-13](#), [2-15](#), [2-16](#)

Cisco_SSC-XP2K-4_1_2_5929.msi [2-3](#)

Cisco Secure Services Client (SSC) [v](#)

- authenticating with log on credentials [2-11](#), [2-13](#), [2-14](#), [2-16](#)

- automatic user connections [1-3](#)

- comparing to CTA 802.1x Wired Client functions [1-2](#)

- comparing to CTA 802.1x Wired Client user interface [1-6](#)

- configuring authentication retry attempts [2-9](#), [2-10](#), [2-12](#), [2-14](#), [2-15](#), [2-17](#)

- configuring automatic connection [2-9](#), [2-10](#), [2-11](#), [2-13](#), [2-14](#), [2-16](#)

- configuring certificate trust rule [2-12](#), [2-13](#), [2-15](#), [2-16](#)

- configuring EAP settings [2-9](#), [2-10](#), [2-11](#), [2-12](#), [2-13](#), [2-14](#), [2-15](#), [2-16](#)

- configuring interaction with Windows logon [1-4](#), [2-14](#), [2-16](#)

- configuring machine and user credentials [2-11](#), [2-13](#)

- configuring machine credentials [2-9](#), [2-10](#)

- configuring single sign-on [2-11](#), [2-13](#), [2-14](#), [2-16](#)

- configuring trusted servers [2-12](#), [2-13](#), [2-15](#), [2-16](#)

- configuring user control [2-9](#), [2-11](#), [2-12](#), [2-14](#), [2-15](#), [2-17](#)

- configuring user credentials [2-14](#), [2-16](#)

- configuring wired or wireless connection [2-9](#), [2-11](#), [2-12](#), [2-14](#), [2-15](#), [2-17](#)

- creating network connections [1-2](#)

- deployment packages [1-2](#), [2-8](#)

- documentation of [vii](#)

- EAP-FAST connection settings [1-4](#)

- installation [v](#), [2-4](#), [2-5](#), [2-7](#)

- installation directory [1-5](#)

- installation files [2-3](#)

- license information [1-7](#)

- machine and user authentication deployment package example [2-11](#), [2-12](#)

- machine authentication deployment package example [2-9, 2-10](#)
- public authentication profiles [1-3](#)
- role in NAC [v](#)
- sending username or anonymous [2-9, 2-10, 2-11, 2-13, 2-14, 2-16](#)
- sending username or anonymous in Phase 1 [2-13](#)
- storage of user credentials [1-4](#)
- supported protocols [1-7](#)
- system report tool [1-6](#)
- use of Microsoft Active Directory [2-9, 2-10, 2-11, 2-13, 2-14, 2-16](#)
- user authentication deployment package example [2-14, 2-15](#)
- user interface [1-6](#)
- utilities [2-4](#)
- Windows operating system support [2-3](#)
- Cisco Secure Services Client Administrator Guide [2-4, 2-5, 2-6, 2-7](#)
- Cisco Trust Agent (CTA) [vii, 2-3](#)
 - documentation of [vii](#)
 - installation files [2-3](#)
 - location of GUID [2-8](#)
 - uninstalling [2-7](#)
 - upgrading to 2.1.103.0 [2-5, 2-6, 2-7](#)
 - upgrading to CTA 2.1.103.0 [2-4](#)
- configuring Cisco Secure Services Client
 - authenticating with log on credentials [2-11, 2-13, 2-14](#)
 - authentication retry attempts [2-9, 2-10, 2-12, 2-14, 2-15, 2-17](#)
 - automatic connection [2-9, 2-10, 2-11, 2-13, 2-14, 2-16](#)
 - certificate trust rule [2-12, 2-13, 2-15, 2-16](#)
 - configuring single sign-on [2-11, 2-13, 2-14](#)
 - configuring wired or wireless connections [2-9, 2-11, 2-12, 2-14, 2-15, 2-17](#)
 - EAP Settings [2-11, 2-12, 2-13, 2-14, 2-16](#)
 - EAP settings [2-9, 2-10](#)
 - interaction with Windows logon [2-14, 2-16](#)
 - machine and user credentials [2-11, 2-13](#)
 - machine credentials [2-9, 2-10](#)
 - sending username or anonymous [2-9, 2-10, 2-11, 2-13, 2-14, 2-16](#)
 - trusted servers [2-12, 2-13, 2-15, 2-16](#)
 - use of Microsoft Active Directory [2-9, 2-10, 2-11, 2-13, 2-14](#)
 - user control [2-9, 2-11, 2-12, 2-14, 2-15, 2-17](#)
 - user credentials [2-14, 2-16](#)
 - configuring wired or wireless connections [2-9, 2-11, 2-12, 2-14, 2-15, 2-17](#)
- CTA 802.1x Wired Client [v](#)
 - automatic user connections [1-3](#)
 - comparing to Cisco Secure Services Client functions [1-2](#)
 - comparing to Cisco Secure Services Client user interface [1-6](#)
 - configuring interaction with Windows logon [1-4](#)
 - creating network connections [1-2](#)
 - deployment packages [1-2](#)
 - EAP-FAST connection settings [1-4](#)
 - installation directory [1-5](#)

public authentication profiles [1-3](#)
 storage of user credentials [1-4](#)
 system report tool [1-6](#)
 uninstalling [2-7](#)
 upgrading to Cisco Secure Services Client [2-4, 2-5, 2-6](#)
 user interface [1-6](#)
 Windows operating system support [2-2](#)
 CtaAdminEx-suppllicant-win-2.1.103.0.exe [2-3](#)

D

deployment package example
 machine and user authentication [2-11, 2-12](#)
 machine authentication [2-9, 2-10](#)
 user authentication [2-14, 2-15](#)
 documentation
 additional reading [vii](#)
 of Cisco Secure Services Client [vii](#)
 of Cisco Trust Agent [vii](#)
 of Network Admission Control [viii](#)

E

EAP-FAST
 cached credentials [1-4](#)
 protecting client certificate [1-5](#)
 EAP settings [2-9, 2-10, 2-11, 2-12, 2-13, 2-14, 2-16](#)

I

installation directories [1-5](#)
 installing SSC [2-4](#)

M

machine and user credentials [2-11, 2-13](#)
 machine authentication deployment package example [2-9](#)
 Microsoft Active Directory [2-9, 2-10, 2-11, 2-13](#)
 migration procedures [2-4](#)

N

Network Admission Control (NAC) [v, viii](#)

S

sending username or anonymous [2-9, 2-10, 2-11, 2-13, 2-14, 2-16](#)
 Smartcards use of certificates [1-5](#)
 SSC
 see Cisco Secure Services Client [v](#)
 SSCAdminUtils_4.1.2.5928.zip [2-3, 2-4](#)
 System Report tool [1-6](#)
 system requirements [2-2](#)

T

Text conventions [vi](#)

trusted servers [2-12](#), [2-13](#), [2-15](#), [2-16](#)

U

upgrade procedures [2-4](#)

user credentials [2-14](#), [2-16](#)

users changing licensing [2-9](#), [2-11](#), [2-12](#), [2-14](#), [2-15](#),
[2-17](#)

users creating networks [2-9](#), [2-11](#), [2-12](#), [2-14](#), [2-15](#),
[2-17](#)

W

Windows operating system requirements [2-2](#)