Release Notes for Cisco Secure Services Client 4.2.0

August 3, 2007

Contents

- Introduction, page 1
- System Requirements, page 2
- New and Changed Information, page 2
- Limitations and Restrictions, page 2
- Important Notes, page 3
- Caveats, page 4
  - Open Caveats, page 4
  - Resolved Caveats, page 5
  - Closed Caveats, page 6
- Troubleshooting, page 6
- Related Documentation, page 6
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 7

Introduction

This document describes important notes, limitations, open caveats, and resolved caveats for Cisco Secure Services Client (CSSC) 4.2.0.

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

System Requirements

Supported OS Environments

XP Professional (SP1, SP2), 2K (SP4), Win2K Servers (SP4), Win2003 Server

Novell Client version 4.91 SP1 with Hotfix TID2972711

New and Changed Information

New Features

Configuring EAP Identity

In a deployed network configuration the administrator may specify the content of the initial EAP Response/Identity message. For tunneled EAP methods this represents the phase 1, outer (unprotected) tunnel. Additionally, the administrator may also specify the content of the EAP Identity response of any phase 2, inner tunnel (protected identity). In both cases the configuration consists of fixed text that you explicitly define and placeholder keywords that represent variable values for certain standard components of a Network Access Identifier (NAI) that are dynamically supplied by CSSC at the time of authentication processing. This flexibility enables you to use any standard or special formats compatible with your credential storage environment and the requirements of your authentication server.

Configuring Requesting for Credentials

In a deployed distribution package configuration file the administrator may configure alternate names for end-user text entry boxes in credential dialogs. Substitute text may be specified for the following:

- replacement text for the default text of “Username:”
- replacement text for the default text of “Password:”

Limitations and Restrictions

Unsupported Environmental Features

The following environmental features are not supported in release 4.0.5 or 4.1.0:

- Fingerprint scanners may not be compatible with CSSC. If you encounter problems, Cisco recommends that you disable the fingerprint scanner.

  For example, CSSC does not function properly with IBM ThinkVantage Fingerprint device software versions earlier than version 5. It is recommended that users update to the most recent version available (5.6 at the time of this note) before evaluating compatibility with their individual machine. This update can be obtained at the following URL:

  http://www-307.ibm.com/pc/support/site.wss/TVAN-EAPFPR.html

- CSSC does not support EAP-FAST authentication with an access point local RADIUS server.
- In network environments using token-based credentials, Cisco recommends disabling the Next Token feature of the authentication server. If a re-authentication session occurs between the request for the next tokencode (the multi-digit code displayed by the token device) and the sending of the next tokencode, the authentication will most likely fail. The timing of a re-authentication request is not under the control of CSSC but external stimuli such as roaming or authentication server timeouts.

Important Notes

Roaming and Disk Protection Applications

Software that is designed to protect a laptop's disk drive from physical jarring prevents any disk drive access while vibration is sensed. When using this feature, moving a laptop from one access point to another can cause roaming delays (interruptions in network connectivity). Such delays should not significantly affect applications that are designed to withstand network interruptions. Users can, at some risk, disable the disk-protection utility. Many laptop manufacturers suggest that users stabilize computers by placing them in standby mode before they are in transit which should prevent any problems. CSSC has been tested with one such application, the ThinkVantage Active Protection System, to confirm this.

Disabling Multiple Clients

Do not configure multiple client applications (such as Windows Zero Config and Cisco Aironet Desktop Utility) in addition to CSSC to control an access point with the same SSID. Allowing multiple applications to carry out write operations (as well as carry on EAPOL messaging required for making a connection) through the same network adapter might disrupt both applications, resulting in unpredictable behavior in both client applications.

If you must configure two applications with the same network, you must disable all but one of the client applications and use the enabled client to make connections.

CSSC can be disabled easily from the Client main menu or from the system icon. Individual adapters can be disabled easily from the Manage Adapter dialog. Disabling other third-party clients might not be a simple operation. If a third-party client cannot be disabled, it should be uninstalled. For example, the Cisco Aironet Desktop Utility (ADU) must be uninstalled to allow CSSC to control the wireless adapter.

User Certificates from the Windows Certificate Store

If you use user client certificates from the Windows certificate store, ensure that you understand the requirements for certificate storage and accessibility by machine and user profiles. For example, the use of client certificates from the Windows store is not supported when configuring a user-only network that requires pre-logon authentication. For more information, use the CSSC's help or user guide.

Restarting the CSSC Service

If CSSC becomes suspended inadvertently, the CSSC service must be restarted. If the service fails to stop or restart properly, you must restart the machine.

The service can always be restarted by restarting the machine.

If you have Windows administrative privileges, you can manually stop and start the CSSC service by choosing **Start > Control Panel > Administrative Tools > Services > Cisco Secure Services Client**.

Managing Adapters

If you get a message that a Serious Adapter Problem has been encountered and CSSC automatically releases control of the adapter, Cisco recommends that you reactivate control of the adapter through the CSSC's Manage Adapters menu item. If this fails, you must stop and restart the Cisco Secure Services Client Service through the Windows Services dialog or restart the machine.

Caveats

Open Caveats

Using CSSC

- CSCsh86080—Windows domain-initiated password change

  For a network with the following specific characteristics only:

  - Machine and user connection context
  - single sign-on user credentials
  - auto connect user post-login

  Windows intermittently fails to prompt the user to change their password. When this happens, CSSC remains in the machine context and fails to open the CSSC tray icon and GUI. To recover from this problem the user must log out and then relogin to complete the password change.

- CSCsj49380—Cannot access local smart card over remote desktop.

  Use of a SmartCard to provide credentials for a remote session cannot be supported. The SmartCard requires physical presence (the card needs to be plugged into the machine). This is inconsistent with remote operation.

- CSCsj64335—Changing CSSC Service from auto to disabled leaves the desktop unusable.

  Manually disabling the CSSC Service (either by an administrator or a user) will cause a 10-minute delay on logon.

  Workaround: If there is a problem that requires the service to be stopped, the CSSC program should be uninstalled. Profiles are retained for a future re-installation of the client software.

- CSCsj74357—The SSCMgmtTool does not work in Windows 2000.

  The Management utility runs on an XP operating system.

  Workaround: If it is necessary to run on a Windows 2000 operating system, the file *msvcp80.dll* should be copied from the ...\CSSC Management Utilities\Microsoft.VC80.CRT directory to the ...\CSSC Management Utilities directory (up one level).

Novell Problems

- Novell dynamic password change

  If the backend password change request is initiated while a user is logged on and the authentication server issues a reauthentication request, the reauthentication fails even after the user enters the new password in the Novell GINA.

  Workaround: The user should log out and log in again so that the client can capture the updated password for use in authentication.

Adapter Problems

- Intel(R) PRO/Wireless 3945ABG network adapter

  A lockup condition has been observed that causes the current network access device to cycle between failed (red) and connecting (yellow) as observed in the Manage Networks window. Network connectivity is lost and the system tray icon is either steady-state idle (grey) or connecting (yellow).

  Workaround: Disable and then re-enabled the network adapter. (Using either the client or adapter controls of the CSSC is not sufficient.) From the Windows Network Connections window, select the Wireless Network Connection and right-click. Then click **Disable** in the resulting pop-up menu. Repeat and click **Enable**.

Resolved Caveats

Using CSSC

- CSCsi62319—Failure to start CSSC

  A fix is implemented for an unusual Windows login sequence on a small percentage of machines that results in a 10-minute delay in the user gaining access to the desktop. Now the CSSC starts properly as indicated by the presence of the tray icon and an automatic network connection is established.

Deploying CSSC

- CSCsh88457, CSCsh88422—Multiple deployment packages

  If more than one distribution package XML file is located in the deployment folder, CSSC now finds and processes the most recent valid file and then removes all other files. In the previous releases only a single distribution package file was allowed in the folder.

Configuring the Distribution Package File

- CSCsi60393—Configuring WPA pre-shared keys

  When configuring the WPA/WPA2 key format, you may now use either the HEX or ASCII option. Previously you were limited to using HEX.

- CSCsi58957—Configuring a shared key network with a machine context

  A deployed shared key network with a machine-connection context now maintains the connection when the user logs in.

Closed Caveats

Downgrading CSSC Release 4.2 to CSSC Release 4.1.2

CSCsk08325—Downgrading CSSC from Release 4.2 to Release 4.12 causes a fatal error message

Always remove the CSSC profile directory before downgrading CSSC Release 4.2 to CSSC Release 4.1.2. to eliminate a fatal error that might occur on some PCs running Windows XP.

The CSSC profile directory is located in the CSSC installation directory, typically:

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

Note You can maintain your previous CSSC profile information by renaming the profile directory.

When CSSC Release 4.1.2 is installed, a new profile directory is created. You will need to redefine your CSSC profiles and associated parameters.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at

http://www.cisco.com/en/US/support/index.html

Related Documentation

For more information about Cisco Secure Services Client, refer to the following documents:

Cisco Secure Services Client for Windows 2K/XP User Guide Release 4.1.2

http://www.cisco.com/en/US/products/ps7034/products_user_guide_list.html

The user guide contains detailed information on operating, and locally configuring the client. The single guide covers the three distinct versions of the client: the out-of-the-box version, the deployed Configurable End-User's version and the deployed Preset End-User's version. The content is taken directly from the client's embedded help system documentation.

Cisco Secure Services Client Administrator Guide Release 4.1.2

http://www.cisco.com/en/US/products/ps7034/prod_maintenance_guides_list.html

The administrator guide contains detailed information on deploying preconfigured end-user SSCs. This document describes the components of the underlying XML schema which controls the content and format of the deployment distribution package (configuration file). It also describes several Administrator utilities that are available to assist in the deployment process.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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