Release Notes for Cisco Secure Services Client Release 5.0

August 20, 2007

Contents

This release note contains these sections:

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

Introduction

This document describes important notes, limitations, open caveats, and resolved caveats for Cisco Secure Services Client (CSSC) Release 5.0.

CSSC Release 5.0 is an 802.1X authentication supplicant for creating secure wired and wireless network connections. CSSC also has a GUI user interface for displaying status and accepting commands from a user. It allows your computer to connect to a network that is protected by the IEEE 802.1X security protocol. Only after successful client-server authentication will the port access control on the 802.1X-enabled access device (the wireless access point or the wired Ethernet switch) allow end-user connectivity to the network.

The out-of-the-box default wired CSSC supports:

- Wired LAN (802.3) network adapters
- EAP methods: EAP-FAST, EAP-MSCHAPv2, EAP-GTC, EAP-TLS
- Smartcard provided credentials
- Cisco trust agent (CTA) processing when CTA is also installed

A special trial license adds support for:

- Wireless LAN (802.11) network adapters
- Additional EAP methods: LEAP, EAP-PEAP, EAP-TTLS, EAP-MD5

System Requirements

Supported OS Environments

Windows XP Professional (Service Pack 2), Windows 2000 (Service Pack 4), or Windows 2003 server.

New and Changed Information

New Features

- Supports an intermediate driver for faster and smoother roaming.
- Redesigned interfaces that provides new icons, a simpler user GUI interface, and improved ADA accessibility.
- A single unified configuration file. Your deployment XML file is the same file that CSSC reads for it's configuration.
- Separate GUI and service interfaces. The service runs in it's own process space and is independent from the GUI for a simpler architecture with improved reliability.

Caveats

Open Caveats

These caveats are open for CSSC Release 5.0:

- CSCsj52454—Multi-homed.
  CSCsj22835—No wireless connection when using a wired LAN connection is not working correctly.

  If the SSC client is connected to a wired LAN, it is possible that it may also establish a simultaneous wireless connection. This happens if the user chooses the *connect exclusively* option for a wireless connection or if the client has no wired LAN connections configured and the wired LAN port is a non 802.1x port.

  Workaround: Do not use the *Connect exclusively* option for a wireless connection when you already have a wired connection.

- CSCsj77570—Never associates after a repair.

  If the SSC client is repaired and it fails to load the configuration.xml file (because it is invalid), then the client does not attempt to connect to any of its configured user connections until after a valid configuration is provided and the client is repaired again.

  Workaround: Provide a valid configuration.xml file and repair. There are two ways to repair the SSC. You can right click on the SSC tray icon and choose **Repair** from the menu options or you can click **Repair** (under the Help tab) on the SSC GUI.

- CSCsj80534—Machine Transport Layer Security (TLS) authentication is not honoring certificateId from the configuration.

  When using a static certificate for machine authentication, the *certificateId* tag is not honored by the SSC client. Instead the client is enumerating the machine store and using the first valid certificate that it finds, instead of the one specified by the *certificateId* tag.

  Workaround: Ensure the first certificate in the machine store is the certificate needed for authentication.

- CSCsj84360— Manually provisioned PAC's are not being used.

  A PAC that is manually provisioned by the user and included in the configuration file is not used during authentication.

  Workaround: None.

- CSCsj86739—Supplicant Authentication Engine (SAE) dot1x paused timers are not reset for user reauthentications.

  If the SSC client receives a single *Request ID EAPOL* packet on a connection that is configured to prompt the user for credentials and the user does not respond and the SSC client receives no further EAPOL packets, then the client remains in an authenticating state.

  Workaround: Repair SSC.

- CSCsj93475—Session resumption credentials are not being cleared with WPA2.

  When a connection is configured to use Wi-Fi Protected Access 2 (WPA2) and Prompt for Credentials and *Remember while a user is logged on* or *Never Remember*, the SSC client might make a connection to the network without asking for credentials again. This occurs because of PMK caching.

  One scenario where this might occur is when a user logs off and then logs on. In this case, the SSC client immediately establishes a connection without prompting for the user's credentials.

  Workaround: Use WPA instead of WPA2.

- CSCsj31130—Connecting to non-authenticating wired Ethernet port shows green tray icon.

  If a wired LAN connection is configured for authentication and is connected to a non-authenticating Ethernet port, the system tray icon is green instead of blue when an IP address is received.

  Workaround: Repair SSC.

- CSCsj59048—Icon is not visible on a remote desktop.

  Occasionally, when using remote desktop to access a system with the SSC client installed, the client's icon might not appear in the system tray.

  Workaround: None.

- CSCsj64800—Static shared Wired Equivalent Privacy (WEP) association modes are not being enforced in the SSC client.

  The SSC client does not enforce the static shared WEP policy.

  Workaround: None

- CSCsj73049—Signal strength display is sometimes incorrect.

  The SSC client might display the incorrect signal strength for a wireless network.

  Workaround: None.

- CSCsj74357—SSCMgmtTool does not work in Windows 2000.

  The SSC management tools does not run on Windows 2000.

  Workaround: Execute the SSC management tools on a system running Windows XP.

- CSCsj74834—Using VNC with SSC default *Enable system tray notifications* turned on.

  When using Virtual Network Computing (VNC) and the username/password balloon prompt is displayed, clicking on the balloon does not display the credentials dialog.

  Workaround: Disable system notifications in the SSC client so that there is a popup window asking for credentials instead of the balloon.

- CSCsj74836—Wired network connection fails to get a DHCP address when the service is stopped.

  The system fails to get a DHCP address when the system is connected to a wired network authenticating port, the SSC client service is stopped, and then the wired connection is moved to a non-authenticating wired port.

  Workaround: Select the Windows wired network connection and then select repair.

- CSCsj77559—Long delay from connection list to associating.

  Some systems might experience delays of up to 30 seconds after a SSC client repair, before the client begins to attempt network connections again.

  Workaround: None.

- CSCzd13858—EAP identity length is limited to 255 octets while EAP protocol allows 65531 octets.

  The EAP Identity field is limited to 255 characters.

  Workaround: Use an EAP identity that is less than 255 characters.

- CSCsj62661—Credentials dialog truncates the connection name.

  On certain laptops (IBM T43 models) with screen resolutions of 1024x768, the credential dialog popup truncates the network name when the name contains a hyphen (-) character.

  Workaround: Resize the dialog box to a slightly larger size and the full name should appear.

- CSCsj50941—Compatibility issues with wireless LAN controller timers.

  On the Cisco 4400 Wireless LAN Controller (and possibly others) the default timers cause the SSC client to never succeed authentication. In addition, the client may continuously display credential prompts. The default timers are set as follows

  EAP-Identity-Request Timeout (seconds)..... 1
  EAP-Identity-Request Max Retries..... 20
  EAP Key-Index for Dynamic WEP..... 0
  EAP Max-Login Ignore Identity Response..... enable
  EAP-Request Timeout (seconds)..... 1
  EAP-Request Max Retries..... 2

  Workaround: Change the timers on the controller to allow successful authentication. To workaround the issue of continuous credential prompts, use single sign-on credentials.

- CSCsk05538—Wrong SSO credentials used after logon or logoff.

  If a Machine/User profile is created that uses Single Sign On (SSO) credentials for user connections, on logging out and in a couple of times as different users, SSC uses incorrect login credentials for users (it could use the first user's credentials for the second user).

  Workaround: Repair the SSC client after you login to ensure you authenticate with the correct user credentials. If user Group Policy Objects (GPO) must be run at login, then logout and log back in.

- CSCsj97381—A Windows 2000 user is the only connection that persists through a logoff.

  For a user only connection using static credentials over a wired network connection, the machine responds to pings after the current user logs off the computer.

  Workaround: Disconnect and reconnect the wired network connection or reboot the machine.

- CSCsk07360—Component-level upgrade does not work with the deployed SSC msi file.

  The basic MSI built for the SSC Release 5.0 is capable of component-level upgrade of the product. However, there is an interaction of the basic MSI packages with a deployment MSI containing an administrator configuration.xml file that does not support component-level upgrade. If attempted, the package appears to succeed (for example, the information in Windows Add/Remove Programs displays the latest product) but none of the system files are actually changed. The package also fails to restart the SSC GUI and the service.

  Workaround 1: Do not distribute configuration.xml files using the installation package. Use any of your enterprise deployment methods to distribute the configuration file after the SSC client has been deployed.

  Workaround 2: Uninstall any previous SSC releases before installing SSC Release 5.0.

  Workaround 3: Customers familiar with MSI technology can manually ensure that the GUID for the *ssc_distribution component* is the same between packages. If this is done, then a component-level upgrade works correctly.

- CSCsk05439—PIN is cached when certificate is remembered forever.

  If you create a configuration.xml file without using the SSC management Utility, you might encounter the following problem:

  When creating a network that authenticates with smart card certificates, you can choose different durations for remembering the certificate and remembering the Personal Identification Number (PIN). For example: If you create a configuration that remembers the certificate forever, but never remembers the PIN, once the network is successfully connected, the PIN is remembered forever (across service stops and starts).

  Workaround: Make sure you choose the same duration for both certificate and pin.

- CSCsk08999—There is a delay to get network connectivity at boot time on some Windows 2000 systems.

  On some Windows 2000 systems, there might be a delay of up to 90 seconds before an SSC client makes a network connection. If there is a delay, machine GPOs will not run at boot time.

  Workaround: Install a smartcard reader on the system experiencing delays.

- CSCsj86452—Username is remembered forever if token credentials are used.

  If token credentials are used, the username is remembered forever, even though it should be requested again when an authentication fails.

  Workaround: Choose **Never remember** for the credential duration if token credentials are used.

Related Documentation

For more information about CSSC Release 5.0, refer to this document:

- *Cisco Secure Services Client Administrator Guide, Release 5.0*

  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.

You can access this document from this Cisco.com link:

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

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