Release Notes for Cisco Secure Services Client Release 5.0.1

December, 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 5.0.1.

CSSC Release 5.0.1 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

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.

Compatibility with Other Supplicants

CSSC is compatible with Microsoft Wireless Zero Configuration (WZC) and will disable or enable WZC when CSSC is enabled or disabled respectively. CSSC is not compatible with other supplicants such as Juniper Odyssey. If possible, other supplicants should be completely uninstalled and the system should be rebooted before continuing with an installation of CSSC.

New and Changed Information

New Features

- Extended Key Usage support for client certificates - If present, the CSSC will first choose certificates with an EKU field of *client authentication*
- Supports upgrade from CSSC 4.2.

Important Notes

Novell is not supported by CCSC Release 5.0.1.

Remote Desktop

Remote desktop is supported by CCSC Release 5.0.1 as follows:

- CSSC must be configured for machine authentication.
- When a user logs in remotely, CSSC remains authenticated with the machine's credentials.
- If a local user is logged in and CSSC is authenticated to the network with the local user's credentials and a remote user logs in via remote desktop, the local user is logged off and CSSC reverts to machine authentication.

Caveats

Open Caveats

These caveats are open for CSSC Release 5.0.1:

- 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 CSSC 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.

- CSCsj31130—Connecting to a non-authenticating wired Ethernet port displays a 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 CSSC.

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

  Occasionally, when using remote desktop to access a system with the CSSC 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 CSSC client.

  Workaround: None

- CSCsj73049—Signal strength display is sometimes incorrect.

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

  Workaround: None.

- CSCsj74357—SSCMgmt Tool does not work in Windows 2000.

  The CSSC management tools does not run on Windows 2000.

  Workaround:Execute the CSSC management tool on a system running Windows XP.

- CSCsj77559—Long delay from connection list to associating.

  Some systems might experience delays of up to 30 seconds after a CSSC 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 CSSC 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.

- 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.

- 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 PC responds to pings after the current user logs off the computer.

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

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

  The basic MSI built for the CSSC 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 CSSC 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 CSSC client has been deployed.

  Workaround 2: Uninstall any previous CSSC releases before installing CSSC 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 CSSC 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 a CSSC client makes a network connection. If there is a delay, PC Group Policy Objects (GPOs) do not run at boot time.

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

Resolved Caveats

These caveats are resolved for CSSC Release 5.0.1:

- CSCsj52454—Multi-homed.

  CSCsj22835—When using a wired LAN connection, the wireless connection is not working correctly.

  If the CSSC client is connected to a wired LAN, it is possible that it might 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 CSSC 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 CSSC. You can right click on the CSSC tray icon and choose **Repair** from the menu options or you can click **Repair** (under the Help tab) on the CSSC GUI.

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

  If the CSSC 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 CSSC client receives no further EAPOL packets, then the client remains in an authenticating state.

  Workaround: Repair CSSC.

- CSCsk78629—PMKID cache is not cleared between machine and user authentication

  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 CSSC 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 CSSC client immediately establishes a connection without prompting for the user's credentials.

  Workaround: Use WPA instead of WPA2.

- CSCsk05538—Wrong Single Sign On (SSO) credentials are used after a logon or logoff.

  If a machine or user profile is created that uses SSO credentials for user connections, on logging out and in several times as different users, CSSC uses the incorrect login credentials for users (it could use the first user's credentials for the second user).

  Workaround: Repair the CSSC 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.

- 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.

- CSCsk56129—Signal strength indication does not display.

  If the scanlist is disabled, the signal strength is not shown for the connected network.

  Workaround: None.

- CSCsk64168— Long startup delay with both wired and wireless LAN available.

  An additional delay of up to 90 seconds may be experienced during startup or bootup after installing CSSC.

  Workaround: None.

- CSCsk77911—Pre-logon not waiting for user connection before allowing logon to continue.

  If a PC or user connection is configured and pre-logon is enabled and if the PC is connected at the time the user logs on, the windows logon continues immediately without waiting for the user network connection to occur. This causes scripts that depend on network connectivity at logon time to fail unexpectedly if the user VLAN is different from the PC VLAN.

  Workaround: None.

- CSCsk53241—Connection resumes the wrong session.

  When switching between configured connections, the fast session resumption information is not cleared causing one connection to connect with the credentials from the other connection.

  Workaround: None.

- CSCsk27805— Smartcard enumeration is slow.

  With certain smart cards and CSPs the enumeration of smart card certificates may be very slow (>10 seconds).

  Workaround: None.

- CSCsk08326-- Client performs authentication but tray icon is blue and status is none (TLS).

  When authenticating with PEAP-TLS, the tray icon might incorrectly indicate a blue status (indicating an unauthenticated port) and the method reported in the connection status might be none (TLS).

  Workaround: None.

- CSCsk91009—XML restricted characters in username and password do not work.

  If the user name or password has any XML restricted characters, authentication never succeeds because these characters are incorrectly parsed by the client. Special characters include: ampersand (&), less than (<), greater than (>), and semi-colon (;). This applies to both SSO and prompting configurations.

- CSCsk90590—During logoff numerous internal errors are logged in the log file.

  Workaround: None.

- CSCsl00751—Check marks in manual mode (connect exclusively) are not removed.

  If CSSC is configured to connect exclusively to a connection and the user chooses to connect exclusively to a different connection, the check mark persists on the first connection in addition to the check mark for the new connection.

  Workaround: None.

- CSCsk07228—CSSC Release 5.0 does not support an upgrade from CSSC Release 4.2.

  Workaround: None.

- CSCsl00732—When a preconfigured network is not present the signal strength is displayed as > 0.

  When a configured network is out of range, the signal strength (sometimes) displays a signal strength of less than zero.

- CSCsk65736—OpenSSL:FATAL error when modifying SSC 4.1.1 profiles in SSC Release 5.0.

  After the CSSC Release 4.1.1 user networks are migrated into CSSC Release 5.0, the user is unable to edit any of the migrated network connection's information including these user interface fields: Descriptive Name, SSID Name, Security, and Key.

  The following error also appears when deleting or adding migrated network connections:

  OpenSSL:Fatal error, .\crypto\evp\evp_enc.c(282):OpenSSL internal error, assertion failed: inl>0

  Workaround: None.

- CSCsj27945— Starting service with no wired link, causes the CSSC GUI to loose connection.

  If the CSSC service is configured with a wired only profile (the default profile), and the service is started when there is no physical link, then the CSSC GUI cannot receive network_status messages from the service.

  Reproduction Scenario:

  1) Install a fresh client.

  2) Unplug your network cable

  3) Reboot

  Workaround: None.

- CSCsk99035— EAP-PEAP(EAP-TLS) session resumption does not work.

  CSSC NAKs the server's EAP method choice (EAP-MSCHAPv2) and EAP-TLS is listed twice. This causes EAP negotiation to fail on the MS IAS 2003 server.

  Workaround: None.

- CSCsl02024—Intel 2200BG and 3945 cards do not reassociate when resuming from stand-by.

  The Intel 2200BG and 3945 wireless client cards do not reassociate when resuming from stand-by. This causes an association timeout and attempts to use a different connection profile, which removes the existing session data. Therefore a full authentication occurs instead of session resumption.

  Workaround: None.

- CSCsk96586—The CSSC Release 5.0 credential balloons do not respond under Windows 2000 Service Pack 4 (SP4).

  When CSSC 5.0 is installed on a Windows 2000 SP4 PC and an SSID is configured for authentication, the yellow credentials balloon pops-up in the system tray indicating "The network is requesting username and password. Click in this balloon to enter your username and password." When the user clicks the balloon, nothing happens. This prevents the use of CSSC with SSIDs that require authentication and are configured to ask for credentials.

  Workaround: None.

- CSCsl38084—User account is locked when the wrong SSO credentials are used.

  When CSSC Release 5.0 is used with pre- logon SSO credentials, it continuously attempts to use these credentials to authenticate against the back-end server even if the credentials are incorrect. This might cause the user account or a smart card to be locked if the incorrect smart card pin is entered.

  Workaround: None.

- CSCsl22787—CSSC uses the wrong username after connecting to a non 802.1x network.

  When connecting to an EAP-FAST SSO connection, then switching to an open guest SSID, then trying to go back to the EAP-FAST SSID, the wrong username is used (in this case [username]) and the EAP-FAST connection fails.

  Workaround: Restart the CSSC service or reset the wireless card.
- CSCsl37489—CSSC stops working during a fast session resumption.

  Workaround: None.
- CSCsk22099—CSSC crash working on shutdown.

  Workaround: None.
- CSCsk52796—CSSC might stop working when docking or undocking a laptop.

  When this happens, repair does not work.

  Workaround: Reboot the PC or stop the CSSC service.

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.

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.