Release Notes for Cisco Secure Services Client Release 5.0.2

January, 2008

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 (SSC) Release 5.0.2.

Cisco SSC Release 5.0.2 is an 802.1X authentication supplicant for creating secure wired and wireless network connections. SSC 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 SSC 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

SSC is compatible with Microsoft Wireless Zero Configuration (WZC) and will disable or enable WZC when SSC is enabled or disabled respectively. SSC 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 SSC.

New and Changed Information

New Features

This is a maintenance release and there are no new features.

Important Notes

Novell is not supported by CCSC Release 5.0.2.

Remote Desktop

Remote desktop is supported by Cisco SSC Release 5.0.2 as follows:

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

Caveats

Open Caveats

These caveats are open for SSC Release 5.0.2:

- CSCsj80534—Machine Transport Layer Security (TLS) authentication is not honoring certificate ID 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.

- 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 SSC.

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

  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—SSCMgmt Tool does not work in Windows 2000.

  The SSC management tools does not run on Windows 2000.

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

- 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.

- 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 SSC msi file.

  The basic MSI built for the Cisco 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 Cisco 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 a SSC 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 Cisco SSC Release 5.0.2:

- CSCsl70825—Unauthenticated PAC provisioning breaks SSO. Even though a connection profile is configured for single sign-on and the user should not be prompted for credentials, occasionally the user is prompted for credentials. This occurs with unauthenticated pac provisioning only. This is not an issue with authenticated PAC provisioning.

  This problem occurs because an EAP-FAILURE is received from the network after unauthenticated pac provisioning. Certain EAP-FAILURES, such as when the single-sign-on credentials are invalid, should trigger the user to be prompted for new credentials. However, other EAP-FAILURES such as the failure received after pac provisioning, should not trigger the user to be prompted for new credentials.

  Workaround: 1) Use authenticated PAC provisioning. 2) Answer the credential prompt with valid credentials.

- CSCsl85145—A user created 802.1X network is not migrated from SSC 4.1 or 4.2 to SSC 5.0. The network does not appear in the SSC 5.0 list of networks.

- CSCsk99215—User identity contains an unexpected character such as @ or \. When creating an identity pattern, the pattern might contain a separator between the user and domain portions of the pattern that doesn't make sense if the domain is not present. When a user logs in to a local account this separator is still present even though the domain is not. For example, if user jsmith logs in to the Cisco domain, the following identity would be sent to the AAA server: *jsmith@Cisco*. However, if jsmith logs in to a local account, the following identity might be sent to the AAA server: *jsmith@* (it should just be *jsmith*).

  Workaround: Create a separate network connection profile which does not contain a [domain] element for local user accounts.

- CSCsl98522—After entering an incorrect username, you are not prompted again for your username, but your network authentication keeps failing. This only occurs when using a prompt for credentials network profile (rather than a Single-Sign-On network profile). If your network profile is configured to remember credentials forever, a reboot does not correct this problem.

  Workaround:If the network profile is set to remember credentials untill logout, then restarting the service will clear the username. If the network profile is set to remember the credentials forever, then restarting the service or rebooting the computer will not clear the cached username. To clear the cached username you need to delete the following file: C:\Documents and Settings\All Users\Application Data\Cisco\Cisco Secure Services Client\system\internalConfiguration.xml and restart the SSC service or reboot the computer.

  CSCsm00126—The SSC service gets stuck reporting an authenticating status and never successfully connects to the network. This typically occurs when undocking the computer or switching between a wired and a wireless connection.

  Workaround: Right click the SSC tray icon and choose **repair** to resolve this problem.

- CSCsm00157—The history.dat file doubles in size whenever the SSC service is restarted or the computer is rebooted and there are timed licenses present in the configuration file. The SSC service is slow to startup, taking several minutes before reporting any status in the GUI or initiating any network connections or authentications. Also, the file C:\Documents and Settings\Application Data\Cisco\Cisco Secure Services Client\system\history.dat is greater than 1MB.
- CSCsm17270—After the first network connection fails, prelogon is cancelled. When SSC is configured for prelogon and there are multiple networks defined that could connect the user to the network prelogon, if any of these networks fails authentication, prelogon is cancelled and the user is allowed to logon without a network connection.
- CSCsj57380—Client sends username when there is no user certificate available. When SSC is configured a certificate basedauthentication (EAP-TLS, plain or inside the tunnel) and the user has not inserted the smart card, the username or some other strange identity is sent to the AAA server for authentication. For example, this can occur whena certificate from a smart card is required but the smart card is not inserted.

Related Documentation

For more information about Cisco SSC 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.