Release Notes for Cisco Secure Services Client Release 4.2.2

April, 2008

Contents

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

Introduction

This document describes important notes, limitations, open caveats, resolved caveats, and closed caveats for Cisco Secure Services Client (SSC) Release 4.2.2.

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

This is a maintenance release and does not contain any new features.

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 SSC. If you encounter problems, Cisco recommends that you disable the fingerprint scanner.

  For example, SSC 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

- SSC 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 SSC 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. SSC 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 (WCZ) and Cisco Aironet Desktop Utility) in addition to SSC 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 multiple applications with the same network, you must disable all but one of the client applications and use the enabled client to make connections.

Note SSC disables WZC when it manages a client adapter and re-enables WZC when an adapter is unmanaged or SSC is uninstalled.

SSC 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 SSC 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 SSC's help or user guide.

Restarting the SSC Service

If SSC becomes suspended inadvertently, the SSC 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 SSC 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 SSC automatically releases control of the adapter, Cisco recommends that you reactivate control of the adapter through the SSC'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 PC.

Caveats

Open Caveats

These caveats are open for SSC Release 4.2.2:

- CSCsj89857—Machine authentication only and anonymous PAC provision loops forever. With a specific EAP-FAST configuration, SSC never uses the provisioned PAC. SSC Release 4.x. is affected.

  Workaround: None available in SSC. A possible work around is to change the ACS configuration to allow authenticated in-band provisioning.

- CSCsl04385—User is prompted for password when using deployed static credentials. With certain deployed configurations that contain static credentials (username and password), the user is prompted for the password during authentication. The expectation is that the user is not prompted for username and/or password during authentications.

  Workaround: None.

- CSCsl26737— SSC stored user PAC under an incorrect user name. With a deployment configuration that contains static credentials (username and password) and FAST, a PAC is never saved for the correct username. As a result, subsequent authentications are done with the deployed static credentials. The desired behavior is the first authentication to use the deployed credentials, and subsequent authentications to use the PAC provisioned during the first authentication.

  Workaround: None.

- CSCsm51715—When SSC is configured to request credentials and remember forever, the new credentials should be saved immediately to a file after being changed, instead of waiting until the user logs off or Windows shuts down.

  If the PC experiences a high system load during logoff, SSC may suffer from resource starvation. If the network profile stores credentials and has remember forever enabled, the credentials may not be stored properly.

  Workaround: None.

Adapter Problem

- 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 SSC 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

These caveats are resolved for SSC Release 4.2.2:

- CSCsl53329—SSC does not send an EAP-logoff when a remote user logs off the system. Windows sends a logoff packet to the remote system as well as the local system. This results in the client staying authenticated as the user when the client is in the machine context.
- CSCsl70922—Allowing a credential request to timeout causes SSC to lose management control of the adapter. The condition usually occurs after an access point connection failure.
- CSCsl85899—SSC time stamp in the clientDebug_current.txt file is incorrect.
- CSCsm44188—Authentication failure after a Windows password change. SSC is not aware that the Windows password has been changed. This problem might occur in two different scenarios:
  - Changing your password after being prompted by Windows that your password expires in a few days.
  - Changing your password by pressing CTRL–ALT—Delete and selecting the change password option.
- CSCsm51722—SSC should differentiate between an authentication failure and a TLV (type, length, value) failure. When SSC is configured to request credentials, a posture (TLV) failure causes SSC to re-prompt the user for credentials when the credentials are still valid.

Closed Caveats

These caveats are closed for SSC Release 4.2.2:

- CSCsk04839—Removal of probe breaks the login scripts when using multiple SSID's. When SSC is configured to do pre-logon authentication with a network that contains multiple SSIDs, login scripts might fail. This happens for SSC Release 4.1.x and 4.2.x.

  Workaround: Configure pre-logon networks with a single SSID. The number of hidden SSID's should be limited to the minimum possible and should not exceed a total of 4.

- CSCsl41588—SSC configured for EAP-Fast and SSO does not honor maximum configured authentication attempts. IF SSC is configured for SSO and EAP-Fast , it is re-using the wrong credentials 3 times. This causes a password lock-out.

  Workaround: Configure SSC to *Prompt for Credentials and Remember Forever*. This provides the ability to see the password retries and correct the password after the first attempt. The retries are timed, so if the user does not supply a new password within 15 seconds the authentication fails.

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 4.2

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 4.2

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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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