Release Notes for Cisco Secure Services Client 4.1.2

May 7, 2007

Contents

Introduction

This document describes important notes, limitations, open caveats, and resolved caveats for Cisco Secure Services Client (SSC) 4.1.2.

Release 4.1.2 is the second maintenance release.

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 in Release 4.1.2

Restricting Client Certificates

For deployed networks the administrator may now restrict the set of allowed client certificates based on the certificate's Extended Key Usage field. (See the *Cisco Secure Services Client Administrator Guide Release 4.1.2* in Related Documentation, page 6 for details on deployment configuring.)

Static Credentials

In earlier releases of SSC Release 4.1, support was added for the configuring of static credentials, identity (username), and password, for user-context connections only. In this release SSC extends that support to include machine-context connections with the following additional limitation. Static credentials for machine authentication also exclude the use of EAP FAST (in addition to EAP TLS, a certificate-based, previously-excluded method).

Changes in Release 4.1.2

Deployment of Certificate Authority Files

Deployment of Certificate Authority (CA) certificates is restricted to the importing of pem file formats only.

Machine/User Context Connections

When deploying authenticating networks created with the machine/user context, you may now configure the order of the domain login and the network connection when making the transition between the machine and user contexts. In earlier 4.1 releases, the user network connection was always made post login. (See the *Cisco Secure Services Client Administrator Guide Release 4.1.2* in Related Documentation, page 6 for details on deployment configuring.) (Reference CSCsi53898)

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

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 machine.

Caveats

Open Caveats

Deploying SSC

- CSCsh88457, CSCsh88422—Multiple deployment packages

  Only a single distribution package XML file may be deployed at a time.

- CSCsi24384—Updating end-user configurations

  When using the sscPackageGen utility with the patch command, the input installation file (.msi) must be a pre-configured installation file (which contains a distribution package XML file). The use of the original SSC installation file (which does not contain a distribution package XML file) results in a patch file (.msp) that fails to install your updated distribution package file.

Configuring the Distribution Package File

- CSCsi60393—Configuring WPA pre-shared keys

  When configuring the WPA/WPA2 key format, you are limited to using the HEX option.

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

  A deployed shared key network with a machine-connection context fails to maintain the connection when the user logs in.

Using SSC

- CSCsi62319—Failure to start SSC

  On a small percentage of machines, an unusual Windows login sequence results in a 10 minute delay in the user gaining access to the desktop. Additionally the SSC tray icon is missing and no automatic network connection is established. There is no work around for this condition other than to restart the machine.

  A fix for the next maintenance release is being evaluated. If you are experiencing this problem, contact Cisco Support for the availability of an unofficial prerelease build to test with in your environment.

- 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, SSC remains in the machine context and fails to open the SSC tray icon and GUI. To recover from this problem the user must log out and then relogin to complete the password change.

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 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**.

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.