Release Notes for Cisco Secure Services Client 4.1.0

March 28, 2007

Contents

Introduction

This document describes important notes, limitations, open caveats, and resolved caveats for Cisco Secure Services Client 4.1.0.

This is the first feature upgrade for the initial Cisco Secure Services Client Release 4.0.

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 4.1.0

Downloaded SSC

The configuration of the SSC that is obtained from the cisco.com SSC download page (the default client) is now a fully (non-expiring) licensed, wired-only client. It supports EAP-FAST with EAP-MSCHAPv2, EAP-GTC and EAP-TLS (SmartCard credentials). Also the Cisco Trust Agent (CTA), when installed, is supported.

If demonstration of the wireless functionality is desired, a 90-day trial license for this feature is available for download at the same site. Also added is support for additional authentication methods: LEAP, EAP-PEAP, EAP-TTLS and EAP-MD5.

After installing the default msi package, upgrade by activating the demo license by following these steps.

Step 1 From the Help menu, select **Activation** to open the Activate Product Features dialog.

Step 2 Enter the downloaded wireless trial license string in the text box. (Avoid any leading or trailing white space when entering the license.)

Step 3 Click **Install License**.

If the trial period ends, before you purchase and update to a full wireless license, operation reverts back to the wired-only default.

Enterprise Deployment

The new deployment capability greatly reduces the complexity of creating deployment packages for large enterprises. Once created, standard deployment applications such as Altiris, SMS, email, etc., should still be utilized for the actual distribution.

Key aspects of the updated enterprise deployment include:

- A single configuration file

  Files for license, policy, networks, and secrets that had to be deployed to different folders within the SSC file structure are replaced with a single file, referred to as the distribution package file. The format of this new file is XML and its content and structure are controlled by a companion distribution package XML schema.

Cisco provides a separate command-line utility, sscConfigProcess.exe, which prepares the distribution package for deployment. The utility performs the following required operations:

  - Validates the preprocessed distribution package for both schema and business rule violations.
  - Encrypts all credentials and secrets from their original clear text.
  - Retrieves and packages any optional files referred to by reference in the input file.
  - Digitally signs the distribution package file to help prevent any tampering with its contents while it is resident in the end station.

- A single preconfigured msi installation file

  The separate deployment of the application msi file and configuration settings is replaced with the deployment of a single file.

  Cisco provides a separate command-line utility, sscPackageGen.exe, which facilitates the following enterprise deployment Windows Installer operations:

  - Installs a pre-configured SSC in a single-step.
  - Updates the configuration of an initially deployed and installed SSC.

Static Credentials

SSC now supports the configuring of static credentials, identity (username), and password by the administrator for deployment to end-user machines. In this release SSC supports static credentials for user-context connections only.

Deployment Items

With the new approach, the administrator can deploy the following items within the single distribution package .xml file:

- Certificate Authority (CA) files

  Previously CA certificates had to be deployed separately.

- Manual EAP-FAST PAC provisioning

  SSC now supports manual PAC provisioning in addition to the continued support of both anonymous and authenticated autonomous provisioning.

Changes in Release 4.1.0

Single Access Device per Network

Networks configured with the deployment distribution package are limited to a single access device, that is, a single wireless access point (identified by its SSID) or the Ethernet access.

Windows Welcome Screen and Fast User Switching

The Windows Welcome screen and its Fast User Switching feature have not been recommended for end-user environments not using network domains because of login delays and security problems, respectively. SSC now disables the Welcome Screen and Fast User Switching. All users, domain and non-domain, are now presented with the classical Windows Login screens.

Choosing between Multiple Client Certificates

The certificate selection capability is enhanced to help the user better distinguish between multiple certificates. In the Enter Your Credentials dialog for certificates, the display of information for available certificates is extended to include any enhanced key usage information. Many times the only differences between one certificate and another is the enhanced key usage. (Ref CSCsh71597)

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.

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**.

Resolved Caveats

Using SSC

- CSCsh53249, CSCzd12180—Non-administrative user limitations on managing adapters

  Non-administrative users can now properly manage adapters. When you are using the Enable/Disable SSC control, Windows Zero Config (WZC) is properly disabled/enabled, respectively. Having both enabled at the same time results in competition for control of the adapters.

- CSCsh48365—Smartcard PIN limitations

  To prevent the rejection of valid smartcards, the allowed length of the text entry for a PIN is increased to 63 from 8.

- CSCsh50305, CSCsg33405—Login attempt after cancelled shutdown

  Canceling a Windows shutdown no longer causes a fatal SSC error.

- CSCsh47156—Enabling SSC in the presence of a non-authenticated wired connection

  An existing, wired, non-authenticating network connection on an unmanaged adapter is no longer broken while SSC is being enabled.

- CSCsg83092—Non-English Windows editions

SSC now works with unicode file names. This means that non-English versions of the supported editions of Windows can properly use files not stored in the default (English-named) folders. Therefore, the display of user-defined text names such as a network profile name when associated with these files is corrected.

- CSCsh18984—Corrupted files on shutdown

  A new fail safe file backup scheme is implemented to recover from a situation when one of the internal profile files becomes corrupted.

- CSCzd12222—Clearing credentials

  The Clear Stored Credentials control in the Network Configuration Summary dialog for a preset client or locked network is now supported.

Novell Problems

- CSCzd12815—Novell login/logout with XP SP2

  Long login delays (about 1 minute), after the credentials are entered, on XP SP2 machines in large Novell VPN environments have been reduced. Premature logoff issues have also been corrected.

- CSCzd14316 - Novell Contextless LDAP query

  In a Novell network environment with LDAP Contextless Login, SSC no longer accesses the entire set of records on the LDAP server. With its new search filter, SSC lookup timing is compatible with native Novell.

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

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 for Windows 2K/XP Administrator Guide Release 4.1

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.

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.