Release Notes for Cisco Secure Services Client Release 5.1.1.21 for Windows XP, Windows 2000, and Windows 2003 Server Enterprise Edition

September 2010

Contents

This release note contains these sections:

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

Introduction

The Cisco Secure Services Client Release 5.1.1.21 (SSC 5.1.1.21) is client software that provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks. SSC manages user and device identity and the network access protocols required for secure access. It works intelligently to make it simple for employees and guests to connect to an enterprise wired or wireless network.

SSC 5.1.1.21 supports these main features:

- Wired (802.3) and wireless (802.11) network adapters
- Integrated VPN support
- Ability to launch scripts after a network connection has been established
- Remote desktop support
- Authentication using Windows machine credentials
- Single sign-on user authentication using Windows logon credentials
- Simplified and easy-to-use 802.1X configuration
- EAP methods:
  - EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC and EAP-MSCHAPv2 for 802.3 wired only).
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-TLS, and EAP-MSCHAPv2
  - EAP-FAST—EAP-GTC, EAP-TLS, and EAP-MSCHAPv2
  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 (also legacy protocols—PAP, CHAP, MSCHAP, and MSCHAPv2)
- Encryption modes:
  - Static WEP (Open or Shared), dynamic WEP (generated with 802.1X), TKIP and AES
- Key establishment protocols:
  - WPA, WPA2/802.11i and CCKM (selectively, depending on the 802.11 NIC adapter)
- Smartcard provided credentials
- Cisco Trust Agent (CTA) processing when CTA is also installed
- SSC Federal Information Processing Standards Publication (FIPS) 140-2 Level 1 module and FIPS 3eTI driver installer.

  Note FIPS validation is in process with the National Institute of Standards and Technology (NIST) as of April 2008.

  - The FIPS 3eTI driver installer must be ordered separately from Cisco.

These features are described in detail in the *Cisco Secure Services Client Administrator Guide, Release 5.1.1,* which you can access at this URL:

http://www.cisco.com/en/US/products/ps7034/prod_maintenance_guides_list.html

VPN Integration

SSC 5.1.1.21 integrates an automatic VPN connection feature but requires the Cisco IPSec VPN client (release 4.8 or later) to be installed on the user's PC. SSC minimizes user intervention when establishing a VPN connection. SSC supports these IPSec VPN authentication options:

- Password—Specifies a simple password authentication.
- Secure Computing Soft Token II—Specifies a soft token from Secure Computing SofToken-II for authentication. This option requires that Secure Computing SofToken-II to be installed on the user's PC. SSC uses the Secure Computing SofToken II APIs to get a password that is automatically passed to the VPN daemon as a credential.
- Certificate—Specifies certificate authentication and uses the connection to specify the certificate to use. Using this option, SSC does not prompt the end user for anything.

If the VPN concentrator does not require user authentication, such as when using group authentication, SSC does not prompt the user for information.

When authentication is required by the VPN concentrator, SSC prompts the user for VPN logon information:

- Softoken authentication—Prompts for username and pin for the soft token account.
- Password authentication—Prompts for username and password.
- Certificate authentication—No prompt is required.

When the VPN connection is successful, SSC maintains the user entered information for possible future VPN connection attempts while the user is logged on to the PC. If the VPN connection fails, SSC re-prompts the user for VPN logon information.

SSC deletes the user's VPN information when the user logs off, shuts down the PC, or repairs SSC.

SSC FIPS Module and 3eTI Crypto Kernel Library

FIPS is a requirement of each vendor that sells wireless infrastructure products to the United States Federal Government including the U.S. Department of Defense (DoD) and Civilian agencies as well as Canadian government agencies. In addition the DoD 8100.2 wireless LAN policy requires that wireless clients must support FIPS 140-2 validated IEEE 802.11i clients. This release of SSC supports a FIPS 140-2 Level 1 module (being validated by the NIST and provides FIPS 802.11i (WPA2)) security support.

Note For information on configuring FIPS, refer to *Chapter 7, SSC FIPS 140-2 Level 1 Validation* in the *Cisco Secure Services Client Administration Guide, Release 5.1.1*.

An administrator can choose to allow enterprise employees to perform one of these operations:

- Connect to only FIPS compliant networks.
- Connect to other non-FIPS compliant networks.

You can restrict the allowed association and encryption modes and the authentication methods in the policy section of the SSC schema.

The SSC FIPS module supports FIPS approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X) . The SSC FIPS module also supports EAP methods including EAP-TLS, EAP-PEAP, and EAP-FAST. SSC 5.1 enables administrators to support both FIPS compliant WLAN profiles as well as optional non-compliant configurations, such as access to WiFi hotspots with client VPN security enabled.

A fully FIPS compliant solution requires three components:

- SSC 5.1.1.18 or later with the FIPS module.
- 3eTI FIPS validated Crypto Kernel Library (CKL) with supported NIC adapter drivers.
- A FIPS compliant network profile configuration created by the network administrator.

3eTI CKL Driver Installer

The driver installer is used to install 3eTI FIPS validated CKL supported drivers for supported NIC adapters.

These NIC adapter chipsets are supported by the 3eTI FIPS certified CKL:

- Intel 2100, 2200, 2915, and 3945 chipsets
- Broadcom: All BCM 43xx chipsets that support driver version 4.100.27.0 or greater
- Atheros PCI chipset based NIC adapters, including Cisco AIR-CB21 wireless client adapter cards
- Atheros: 5001, 5004, 5005, AR5211, and AR5212 chipsets

System Requirements

Supported OS Environments

The supported 32-bit operating system environments are:

- Windows XP Professional (SP2)
- Windows 2000 (SP4)
- Windows 2003 Server Enterprise Edition (SP2)

Note Other Windows XP versions, such as Media Center, Tablet PC, and Professional x64 are not supported.

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, you should completely uinstall other supplicants and the reboot the system before continuing with an installation of SSC.

Obtaining SSC Software

SSC 5.1.1.21 software is available from the Cisco Software Center:

- SSCMgmtToolKit_5.1.1.zip—Contains the sscManagementUtility and support files.
- Cisco_SSC-XP2K_5.1.1.zip—Contains the SSC files. For license information, see the "SSC License Information" section on page 5.
- CiscoClientUtilities_5.1.1.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL

http://www.cisco.com/public/sw-center/index.shtml

Click **Wireless Software > Client Adapters and Client Software > Cisco Secure Services Client** and follow the prompts to 5.1.1 under Latest Releases.

Note You must register with Cisco.com or be a registered user to download software.

SSC License Information

The SSC software obtained from the Cisco Software Center on Cisco.com contains two special licenses and their associated limitations:

- 90 day trial license for both wired and wireless functions. This license is a full featured SSC license but is limited to an evaluation period of 90 days (see http://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/product/notes/sscLicense.html). After 90 days, to use the full features, you are expected to purchase a permanent license from Cisco.
- Permanent wired-only license. This license allows a limited subset of the full featured 90 day trial SSC license. To obtain full functionality, you are expected to purchase a permanent license from Cisco.

To obtain additional information on the features supported in these special licenses, refer to the *Cisco Secure Services Client Version 5.1 Bulletin* available on Cisco.com an this URL:

http://www.cisco.com/en/US/products/ps7034/prod_bulletins_list.html

Note When the trial license period has expired and the user attempts to use a non-supported feature, SSC displays a pop-up message that instructs the user to contact their system administrator. If the license has expired, this message can occur each time SSC starts. The message continues until a non-expiring license is obtained.

The SSC 5.1.1.21 non-expiring license can be ordered from Cisco using this product number:

- AIR-SC5.0-XP2K

The FIPS 3eTI CKL supported driver installer cannot be downloaded from the Cisco Software Center and must be ordered from Cisco using this product number:

- AIR-SSCFIPS-DRV—3eTI CKL supported driver installer

  The 3eTI CKL supported driver installer software is shipped to the customer on a product CD.

Migrating From SSC 5.0 to SSC 5.1.1.21

Previously installed SSC 5.0 software with administrator pre-deployed configurations must be uninstalled and the PC rebooted prior to installing SSC 5.1.1.21. The SSC 5.1.1.21 installation process automatically detects a previous SSC 5.0 pre-deployed package installation and displays an error message indicating *Internal error 2771 Core* and fails to install. After SSC 5.0 software is uninstalled from the user's PC and the PC rebooted, SSC 5.1.1.21 can be successfully installed.

If the SSC 5.0 software does not contain a pre-deployed configuration, there is no need to uninstall the SSC software prior to installing SSC 5.1.1.21.

After the SSC 5.1.1.21 installation, you must reboot the PC for the SSC software changes to take effect.

Important Notes

Novell is not supported by SSC 5.1.1.21.

Caveats

Open Caveats

These caveats are open for SSC 5.1.1.21:

- 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.

- 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.

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

  Workaround: None

- CSCsk54277—When a user types an incorrect smartcard PIN, a GUI indication is not given.

  Workaround: None.

- CSCso23071—The wired open connection shows as open rather than as connected on a wired 802.1X port.

  Workaround: Unplug the wired connection and then replug it.

- CSCso73826—When the scanlist display is turned off in the configuration, the signal strength for configured connections with beaconing SSIDs is displayed as zero even though the access points are in range.

  Workaround: None

- CSCsq01225—The SSC GUI shows no status information in the main window when only a wired profile is configured and an Ethernet cable is not plugged in.

  Workaround: When an Ethernet cable is plugged in, SSC attempts to make a wired connection and reflects the correct status information.

- CSCsq21205—The user's password change fails when the SSC configuration contains both a wired and a wireless authenticating profile and the user ignores a password change request on the wireless network but attempts to change their password on the wired connection when the wired network is established.

  Workaround: When the wired connection becomes available, the user must repair SSC and then can successfully change the password on the wired connection.

- CSCsq24766—User receives Windows Error 1359 when attempting to change their password.

  In configurations where the credential source is set to logon, if the user receives a password change request on the desktop and attempts to change the password using Windows, the old password is not pre-populated for the user. If an incorrect old password is entered or the new password does not meet the complexity rules during the logon password change dialog, the password change fails (as expected). However, the password change continues to fail even when the user enters the correct old password.

  Workaround: When users receive the password change failed notification at logon, they should click **Cancel** until prompted by SSC to supply credentials for the password change. The password change succeeds if the user supplies the correct logon credentials.

- CSCsv12399—Client devices sometimes fail to authenticate when SSC does not append .com to a username and the domain when it sends the username and domain to the authentication server.

  Workaround: Configure the client to use *username@domain*.com.

- 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.

Known 3rd Party Issues with SSC

Driver Issues

SSC testing discovered that the following 3rd party drivers might fail to maintain an FTP session while roaming:

- Intel 2200BG-CSCsm44687
- Intel 2915-CSCsm44098, CSCso85220, CSCsq27281
- Broadcom 1490-CSCsm44189
- Atheros-CSCso85442
- Dell 1490-CSCso85191

VZ Access Manger Software and the Cisco Secure Services Client

When running the Verizon VZ Access Manger software and the Cisco Secure Services Client, the TCP/IP Protocol may become unbound from all of the network adapters in the system.

Workaround: Perform the steps in the Microsoft knowledge base article to repair TCP/IP. You can find the article at this URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;810979

Resolved Caveats

These caveats are resolved for SSC 5.1.1.21:

-
- CSCsx47443—SSC is now recognizing the VPN Client default location in the IPsec VPN configuration file. With this fix, customers can use the default setting to balance out the load across all of their VPN locations and also minimize overload of VPN sites that are first in the list.
- CSCtb89686—The log packager now limits its execution to a subset of executable files instead of all files in the directory.
- CSCtd36880—When the SSC is configured with an open wired user connection, the client now properly blocks network traffic during the boot up of the device.
- CSCtd63236—Some previous problematic characters in a user's password are now acceptable and will not result in authentication failure.
- CSCtg48005—Even though the SSC was configured to connect exclusively to a WLAN, the wired adapter was still getting an IP address when a user disabled the wired interface and re-enabled it. This issue has been corrected.
- CSCth05422—The PC running Windows XP or 2K using certain Crypto Service Provides no longer hangs after multiple smart card insertions at the Window logon.
- CSCsm36113—When the SSC is configured with an open wired user connection, the client now properly blocks network traffic during the boot up of the device.
- CSCsy54541—The additional carriage return, line feed, and period appended at the end of the VPN banner message has been removed.

Related Documentation

For more information about SSC 5.1.1.21, refer to this document:

- *Cisco Secure Services Client Administrator Guide, Release 5.1*

  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 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.