



Release Notes for Cisco Secure Services Client Release 5.1.1 for Windows XP, Windows 2000, and Windows 2003 Server Enterprise Edition

November, 2008

Contents

This release note contains these sections:

- [Contents, page 1](#)
- [Introduction, page 2](#)
- [System Requirements, page 4](#)
- [Obtaining SSC Software, page 5](#)
- [Migrating From SSC 5.0 to SSC 5.1.1, page 6](#)
- [Important Notes, page 6](#)
- [Caveats, page 6](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation and Submitting a Service Request, page 9](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco Secure Services Client Release 5.1.1 (SSC 5.1.1) 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 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 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 minimize 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.

This can be achieved by restricting 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 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, other supplicants should be completely uninstalled and the system should be rebooted before continuing with an installation of SSC.

Obtaining SSC Software

SSC 5.1.1 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. 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 at 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 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

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. The SSC 5.1.1 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 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.

After the SSC 5.1.1 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.

Caveats

Open Caveats

These caveats are open for SSC 5.1.1:

- 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, there is no GUI indication.
Workaround: None
- CSCsk90874—Remembered credentials are used when the cache credentials are set to never remember.
If an administrator deploys a configuration with credential storage set to remember forever and then re-deploys a configuration with credential storage set to never remember, the credentials that the user entered with the initial configuration are still remembered by SSC.
Workaround: Delete the *Documents and Settings\All Users\Application Data\Cisco\Cisco Secure Services Client\system\internalConfiguration.xml* file, then repair the SSC service.

- CSCsm57889—Moving a non-connected network between groups using the SSC GUI Configure Groups dialog, causes SSC to temporarily drop the active connection.
Workaround: SSC automatically re-establishes the connection without user intervention.
- CSCso23071—The wired open connection is shown as connected on a wired 802.1X port.
Workaround: Unplug the wired connection and then replug it.
- CSCso33390—The VPN credential response is dropped if there is not an active attempt to connect.
If the VPN credential prompt is ignored and you reply to it after the VPN connection attempt has timed out, you are reprompted for your credentials when the VPN connection is attempted again.
Workaround: Enter the VPN credentials again when you are prompted.
- CSCso52859—VPN fails with a failed to enable VPN adapter error upon docking and undocking.
After docking or undocking the PC, the Cisco VPN adapter sometimes gets enabled. When SSC tries to establish a VPN connection with the Cisco VPN adapter enabled, SSC fails to make a VPN connection and indicates a VPN_ERROR_VA_ENABLE_FAILED error.
Workaround: Go to Device Manager and disable the Cisco Systems VPN adapter. You might have to enable it first and then disable 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
- CSCso78352: Disabling and enabling the client from the GUI Settings menu, enables the radio (even if it was previously disabled).
Workaround: Disable the radio from the GUI Settings menu.
- CSCso86311: When VPN is set to auto-connect, sometimes the user might need to manually initiate the VPN connection after logging into the system.
Workaround: Right click the SSC tray icon and choose **VPN Connect** to initiate the VPN connection.
- 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.
- CSCsq14534—The license nag message is not displayed when a user creates an 802.1X network without a valid license.
Workaround: None.
- 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 their 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 their 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 user receives the password change failed notification at logon, the user should click **Cancel** until prompted by SSC to supply credentials for the password change. If the user supplies the correct logon credentials, the password change will be successful.

- CSCsu84121—TCP/IP disassociates from the cell card connection after you install SSC 5.1. 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>

- 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*.

- CSCsv18237—SSC 5.x sometimes improperly displays a license violation screen when the client is configured with a wired-only profile and a wired-only license.

Workaround: None.

- 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 Driver Issues with SSC

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

Resolved Caveats

These caveats are resolved for SSC 5.1.1:

- CSCsl68717—SSC GUI gets confused when two wireless adapters are available.
- CSCsr63264—When there are no wireless networks to associate to, users cannot see the scanlist.
- CSCsu87666—When a machine with Broadcom Gigabit NetExtreme 57xx wired card comes out of a suspend, SSC gets stuck on *Acquiring IP Address* state on the wired network. This is incorrect because there is no wire plugged in to the machine.

Closed Caveats

These caveats have been closed and will not be resolved:

- CSCso58028—While using the 3eti driver package, the adapter never associates to a shared WEP network.
- CSCsu84232—SSC IMD does not install properly when ActiveCard IPSEC client is installed.

Related Documentation

For more information about SSC 5.1.1, refer to this document:

- *Cisco Secure Services Client Administrator Guide, Release 5.1.1*

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2008 Cisco Systems, Inc. All rights reserved.