Release Notes for Cisco Secure Services Client Release 5.1 for Windows Vista

October 15, 2008

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 (hereafter referred to as SSC 5.1) is client software that operates on the Windows Vista operating system. SSC 5.1 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 supports these main features:

- Wired (802.3) and wireless (802.11) network adapters
- Integrated VPN 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, and LEAP
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-MSCHAPv2
  - EAP-FAST—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS
- 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)

VPN Integration

SSC integrates an automatic VPN connection feature, but requires the Cisco IPSec VPN client (release 5.0.03.0560 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:

- Secure Computing SofToken II—Specifies a soft token for authentication.

  Note Secure Computing SofToken II is not supported for Windows Vista. When you specify SofToken II authentication in the network configuration and SSC prompts for the username and password, the user must enter the username and the unique one-time password. This requirement is different from Windows 2000 and Windows XP where the user must enter the SoftToken II application password.

- Password—Specifies a simple password authentication.
- 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:

- Soft token authentication—Prompts for username and pin for the soft token account.

Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SoftToken II application password is entered.

- 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.

System Requirements

Supported OS Environments

The supported operating system environments are:

- Windows Vista Business, Enterprise and Ultimate versions—32-bit and 64-bit
  - Required Windows Hot Fixes:

    KB952613
    KB935222 or SP1
    KB932063 or SP1

Note Other Windows Vista versions, such as Home Premium and Home Basic are not supported.

Note The latest drivers for the operating system should be loaded on the user's PC prior to installing SSC.

Note Cisco strongly recommends that you install Windows Vista Service Pack 1. However, SP1 is required if wired network connections are to be attempted before user logon.

Compatibility with Other Supplicants

SSC works in conjuction with the Windows Vista Auto Configuration Module (ACM). SSC disables or enables ACM appropriately. 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.

SSC Differences with Windows Vista

- Wired Networks—SSC supports a single wired network per group.
- These EAP methods are not supported:
  - EAP-MD5
  - EAP-MSCHAPv2
  - EAP-GTC
  - EAP-TLS
  - EAP-TTLS
  - PEAP-TLS
- Machine Authentication
  - SSC ignores all static machine credentials stored in the configuration; SSC uses the machine's password or certificate instead.
  - The [username] identity patterns specified in the configuration is always expanded to *host/(fully qualified domain name)*.
  - For EAP-FAST and PEAP, the inner EAP method specified in the configuration might be ignored; the EAP method negotiates the best inner method with the AAA server.
  - Configurations that specify a different EAP method for machine authentication from what is specified for user authentication are translated to use the same EAP method specified for user authentication.
- Credential Caching
  - The *forever* credential caching option is not supported. For configurations with the *forever* credential cashing setting, the credentials are cached until the user logs off.
- Single Sign On—When configured to use single sign on credentials with an inner method of GTC, it is possible that at some point, such as when authentication fails, the user will be prompted for their password.
- Server Validation
  - The Personal stores are not used for server validation.
  - When the configuration specifies *validateChainWithAnyCaFromOs*, the certificate must be installed in the Local Computer\Trusted Root store.
  - Any Root CA certificate included in the configuration is ignored and the configuration is translated to *validateChainWithAnyCaFromOs* . The Root CA certification must be installed by some other means.
  - The certificate store is limited to *Local Computer* during machine authentication and user authentications when the connection is attempted before Windows logon.
- EAP-LEAP
  - EAP-LEAP does not work with all versions of ACS. Versions which are known to not work include 3.2.3 and 3.3.1.11. Versions which have been tested and work include 3.3.1.16, 3.3.2.2, and 3.3.4.12.
- EAP-FAST
  - Supports anonymous TLS renegotiation.
  - All PACs contained in the configuration are ignored.

  - To use authenticated provisioning, the configuration must specify server validation. When server validation is not used, the authentication fails and the ACS server reports an *EAP type not configured error.*
  - When using TLS, the protected identity pattern is ignored.
  - Unless the radius server is configured to allow anonymous TLS renegotiation, when a PAC is received using un-authenticated provisioning, a user must wait for the connection timer to expire before an authentication attempt can be made.
- Smart Card Support—Smart cards are not supported.
- SofToken II—Not supported on Windows Vista. For configurations specifying SofToken II, SSC prompts the user for the username and the unique one-time password (OTP) rather than the username and password for the soft token account.
- Logging—The EAP log entries may appear out of order in the log file, but the time and date stamps are correct.
- Group Policy Object (GPO)—-SSC does not support working with wired and wireless group policy objects; all other types of group policy objects are supported.
- Automatic connection mode—SSC actively scans for the networks defined in the configuration file rather than attempting to sequentially connect to each configured network connect until a connection is established (called walk-the-list). Consequently, it may appear that SSC skips over networks without attempting to connect.

Obtaining SSC Software

SSC Software for the Windows Vista Operating System

SSC 5.1 software is available from the Cisco Software Center:

- SSCMgmtToolKit_5.1.1.zip—Contains the sscManagementUtility and support files.
- Cisco_SSC-Vista_5.1.0.zip —Contains the SSC files. For license information, see the "SSC License Information" section on page 6.
- CiscoClientUtilities_5.1.0.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 > Windows Vista** and follow the prompts to 5.1 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 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 non-expiring license for Windows Vista can be ordered from Cisco using this product number:

- AIR-SC5.0-VISTA

Important Notes

Novell is not supported by SSC 5.1.

Caveats

Open Caveats

These caveats are open for SSC 5.1:

- CSCsq39157—Enabling SSC 5.1 deletes all profiles stored in Vista's native profile store. The profiles are not restored when you disable or uninstall SSC.

  Workaround: None

- CSCsq39164—If SSC is managing any wired or wireless adapters, the user cannot configure EAP settings for Cisco EAP-FAST, LEAP, or PEAP with other cards that are not managed by SSC because the settings are grayed out.

  Workaround: Disable SSC (Settings > Enable Client).

- CSCsr94030—Static Credentials which are configured in a network profile are ignored when doing machine authentication. SSC uses the appropriate machine’s credentials (password or certificate).

  Workaround: None.

- CSCsr28550—Moving user defined network up and down quickly across connection groups sometimes causes the SSC service to crash and restart.

  Workaround: Move network connections up and down across connection groups at a moderate pace.

- CSCsu05644—When using EAP FAST with a CB21AG adapter on Windows Vista, EAP FAST prompts the user with a question and continues to prompt for a response after the user answers yes: "The PAC that you selected for this profile does not match the server to which the client is connecting. However, a matching PAC has been found in your PAC database. Would you like to use this matching credential authority and save it to the profile?"

  Workaround: None.

- CSCsu75164—SSC displays an unsupported option for users who attempt to create 802.1x networks with PEAP and certificates as the authentication mechanism.

  Workaround: None.

- CSCsu95923—EAP-FAST with TLS fails to apply the inner protected identity pattern.

  Workaround: None.

- CSCsu96058—SSC supports a single wired newtork and ignores additional wired newtorks defined in the configuration.

  Workaround: None.

- CSCsu96084—SSC does not support the credential caching setting *forever*. In instances where the network specifies credential caching forever, SSC caches the credentials until the user logs offs or authentication fails.

  Workaround: None.

Resolved Caveats

No caveats are resolved in this release.

Closed Caveats

These caveats have been closed and will not be resolved:

- CSCsu95934—LEAP authentication does not succeed against some versions of ACS.
- CSCsu96020—LEAP authentication fails with some versions of Steel-Belted Radius.

Related Documentation

For more information about SSC 5.1, 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.