Release Notes for Cisco Secure Services Client 4.0.51

Contents

This document contains the following sections:

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

Introduction

This document describes important notes, limitations, open caveats, and resolved caveats for Cisco Secure Services Client 4.0.51.

This is the first maintenance patch for the initial Cisco Secure Services Client release, 4.0.5.

Cisco Secure Services Client was formerly known as Meetinghouse AEGIS SecureConnect. For this release and subsequent releases, all technical documentation refers to the Meetinghouse AEGIS SecureConnect product as the Cisco Secure Services Client (SSC).

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.

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.

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 tab. If this fails, you must stop and restart the Cisco Secure Services Client Service through the Windows Services dialog.

Connection Continuity

If you have problems maintaining or initiating a connection, manually disconnect and then manually reconnect. Common problems include the following:

- SSC shows that it is connected, but you do not have connectivity.
- You cannot maintain connectivity after an access point reauthenticates.

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.

Disabling SSC can be done easily from the Client main menu or from the system icon. Disabling an individual adapter can be done easily from the Manage Adapter dialog. Disabling other third-party clients might or 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 accessability by machine and user profiles. For example, when configuring a user-only network profile for enabling pre-logon authentication via the Before user accounts check box (usually associated with a domain login environment), specifying the use of client certificates from the Windows store is not supported. For more information, use the SSC's help or user's guide.

Clearing Credential Control

The Clear Stored Credentials control in the Network Configuration Summary dialog for a preset client or locked network is not currently supported. (Ref CSCzd12222)

Upgrading Shared Key (WEP/WPA-Personal) Networks

Cisco SSC 4.0.5 (and later releases) contains changes to the way credentials are stored. If you are upgrading from a previous release (4.0.4 or lower) that contained networks that use shared key credentials (WEP or WPA/2-Personal), you must reconfigure these by re-entering the shared key. (Ref CSCzd14086)

Follow these steps to enter the shared key again:

Step 1 In the Manage Networks main screen, select the shared key network and click **Configure**.

Step 2 In the Network Profile dialog, select the shared key Access/SSID and click **Modify Configuration**.

Step 3 In the Configure Access Device dialog, enter the shared key again.

Step 4 Click **OK** for each dialog to accept the new configuration.

Upgrading from AEGIS SecureConnect to Cisco Secure Services Client

If you install SSC with AEGIS SecureConnect (ASC) loaded, your ASC network profile configuration and license correctly migrates to SSC. If you uninstall the ASC first and then install SSC, the configurations and license do not migrate to SSC.

Unsupported Environmental Features

The following environmental features are not supported in release 4.0.5 or later:

- Fingerprint scanners cannot be used with SSC. You should disable fingerprint scanners.
- SSC does not support EAP-FAST authentication with an access point local RADIUS server.

Open Caveats

The following caveats are open in release 4.0.51.

Using SSC

- Non-adminstrative user limitations on managing adapters

  Non-administrative users cannot properly manage adapters. When enabling an adapter, either via the Manage Adapter dialog or the Enable Client control from the system tray icon, both SSC and Windows Zero Config (WZC) may compete for control. (Ref CSCzd12180)

  Workaround: Reboot the system while SSC is set to control.
- Using smart cards

  Do not remove the smart card while attempting to authenticate and connect to your network. Wait until the connection is established or the attempt fails.

  Workaround: If removing an active smart card causes problems with the client, you might have to restart the service or reboot the machine.
- Docking your laptop

  Placing your laptop onto its docking station while the laptop is in standby mode may fail to automatically reconnect your wired network.

  Workaround: To restore your wired connection perform one of the following:

  - In the Manage Networks main screen, select the wired network and click **Connect**.
  - If the Status of the wired network in the Manage Networks main screen is Not Available, unplug your Ethernet cable from your docking station and then reconnect the cable.

Novell Problems

- Novell login when recovering from standby or hibernate

  When coming out of standby or hibernate, the client does not wait for the Novell GINA. The user can enter the correct Novell username and password, but the computer cannot find the Novell server. (Ref CSCzd12258)

Workaround: Wait approximately 30 seconds in order to permit the client to establish a wireless connection. Then attempt to log into the Novell server and the desktop again.

- 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.

Resolved Caveats

The following sections include enhancements and resolved items between release 4.0.5 and release 4.0.51.

Reconnecting after Changing Physical Environments

When switching from one physical environment to another without placing your laptop in standby mode or hibernate mode, you will now properly auto-connect in the new environment. (Ref CSCzd14190)

Authentication Retries Default Value Change

Some network access devices support special features for handling authentication failures, for example, the ability to open the port but switch the user into a special VLAN. In order to support these network access devices, the client provides the administrator with configurable parameters. These parameters adjust the number of connection retries made before disconnecting, allowing the access device to make intelligent decisions based on multiple authentication failures.

The default values for the administrator control over the retry counts made during authentication have been changed in order to better support the Failed Authentication VLAN feature of Cisco switches. Set the supplicant to be one more than what the switch is set to for retries. This is so that the supplicant tries one more time to get onto the restricted VLAN. (Ref CSCzd14434)

Deploying Configuration Files

The handling of incorrectly deployed configuration files has been improved. For example, an error resulting from mistakenly copying both the network profile and the policy configuration XML files into the same folder no longer causes SSC to fail. (Ref CSCzd13886)

Wrong Password after Active Directory Password Change

The correct password is nowsent when configured for single sign-on and the user is prompted to change his or her Active Directory password. An authentication failure and a subsequent reboot or re-logon is now avoided. (Ref CSCsf32767, CSCzd14391, CSCzd14494)

Authentications while Transferring from a Machine to User Context

The client no longer processes a redundant machine authentication session when logging into Windows. (Ref CSCsd78605)

Forced Logoff of a User by a Local Admin Logon

When an Admin logs into a user locked computer in a machine-only or a machine/user connection context the network connection is now maintained and SSC responds normally. (Ref CSCsg71040)

Reacquiring/Reconnecting to an SSID

After moving your laptop out of range of an SSID and then back into range, SSC now properly restores the network connection. (Ref CSCsg71279)

SSC 4.0.5 May Break Trusted Server Validation

Note If you have already successfully installed SSC or upgraded from AEGIS SecureConnect 4.0.4 to SSC 4.0.5, you should not have this problem.

A correct install or upgrade from the AEGIS SecureConnect 4.0.4 client is now performed if both of the following conditions exist:

- Your network profile is using server validation.
- Both of the following server certificate chains reside on the end station:
  - an invalid Intermediate CA certificate.
  - a valid Root CA certificate.

(Ref CSCzd14498)

Getting Bug Information on Cisco.com

If you are a Cisco registered user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you to identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit today at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

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

Click **Hardware Support** > **Wireless Devices**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Related Documentation

For more information about Cisco Secure Services Client, refer to the following document:

Cisco Secure Services Client for Windows 2K/XP User's Guide

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

The User's Guide contains detailed information on operating, configuring and deploying the client. The single guide covers the three distinct versions of the client: the Administrator's version (a.k.a., 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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302

- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific:	+61 2 8446 7411
Australia:	1 800 805 227
EMEA:	+32 2 704 55 55
USA:	1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation"section.