Release Notes for Cisco Secure Services Client 4.0.5

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, 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 Cisco Secure Services Client (SSC).

Important Notes

Roaming and Disk Protection Applications

Users should be aware that utilizing software that is designed to protect the disk drive on a laptop from physical jarring prevents any disk drive access while vibration is sensed. This behavior is normal. Users should be aware of this behavior when using applications that eliminate vibration.

While moving from one access point to another, users may experience what appear to be roaming delays (interruptions in network connectivity) if such a utility is running and blocking disk access. This behavior is not likely to have any consequential effect on applications that are designed to withstand network interruptions. Users can, at some risk, alleviate this behavior by disabling the disk protection utility. Many laptop manufacturers suggest that users stabilize computers by placing them in standby mode before they are in transit. If users follow this suggestion, they should not experience any problems.

The client has been tested with one such application—the ThinkVantage Active Protection System—to verify this behavior.

Restarting the Client Service

If the client becomes suspended inadvertently, you must restart the Cisco Secure Service Client. If the service fails to stop or restart properly, you must restart the machine.

If you have Windows administrative privileges, manually stopping and starting the Cisco Secure Service Client can be performed via the Windows Services dialog (Start > Control Panel > Administrative Tools > Services).

Manage Adapter Errors

If you get a message that a “serious adapter problem” has been encountered and the client automatically unmanages the adapter, the recommended corrective action is to re-manage the adapter via the Client > Manage Adapters menu tab. If the attempt to reactivate the adapter via the Manage Adapter dialog is not successful, you must stop and restart the SSC service via the Windows Services dialog.

Connection Continuity

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

- The client shows that it is “Connected,” but you do not have connectivity.
- You cannot maintain connectivity after an access point reauthenticates the client.

Disabling Multiple Clients

Do not configure multiple client applications (such as Windows Zero Config and Cisco Aironet Desktop Utility) in addition to the Secure Services Client to control an access point with the same SSID. Allowing multiple applications to carry out write operations (as well as carry on EAPOL conversations 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 the Secure Services Client 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. In some cases where a simple disable of another client is not supported, such a dual, switched application environment cannot be supported.

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 the Secure Services Client 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 availability to machine and user profiles when configuring the Network Profile dialog for enabling pre-logon authentication via the “before user accounts” checkbox (usually associated with a domain login environment). For more information, use the client help or user guide.

Clearing Credential Control

The 'clear stored credentials' control in the Network Configuration Summary for a preset client or locked network is not currently supported. (Ref #12222)

Upgrading Shared Key (WEP/WPA-Personal) Networks

Release 4.0.5 contains changes to the way credentials are stored. If you are upgrading from a previous version that contained networks that use shared key credentials (WEP or WPA/2-Personal), you must reconfigure these by re-entering the shared key. (Ref #14086)

Follow these steps to enter the shared key again:

Step 1 In the Manage Network 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 new configuration.

Upgrading from AEGIS SecureConnect to Cisco Secure Services Client

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

Unsupported Environmental Features

The following environmental features are not supported in release 4.0.5:

- Fingerprint scanners—Fingerprint scanners cannot be used with the Cisco Secure Services Client. You should disable fingerprint scanners.
- Cisco access point with local RADIUS server—The Cisco Secure Services Client does not support EAP-FAST authentication with an access point local RADIUS server.

Open Caveats

The following caveats are open issues in release 4.0.5.

Using the Client

- Non-adminstrative user limitations on managing adapters

  Non-administrative users can not properly manage adapters, either via the Manage Adapter dialog or the 'active' control from the system tray icon. When remanaging (enabling) an adapter, both the Cisco Secure Service Client and Windows Zero Config may compete for control. (Ref #12180)

  Workaround: Reboot the system while Cisco Secure Service Client 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.

- Reconnecting after changing physical environments

  When switching from one physical environment to another without placing your laptop in standby mode or hibernate mode, you may not be able to auto-connect in the new environment, even when overriding the auto-connect feature and attempting manual connections. (Ref #14253, 14190)

  Workaround: To restart the auto-connect process in your new environment, disable and then enable the client from the Client main menu or from the system icon.

Novell Issues

- 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 type in the correct Novell username and password, but the computer cannot find the Novell server. (Ref #12258)

  Workaround: Wait approximately 30 seconds in order to permit the client to establish a wireless connection. Then attempt to log in to 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 inputs the new password in the Novell GINA.

  Workaround: The user should logout and login again so that the client can capture the updated password for use in authentication.

Resolved Caveats

The following sections include enhancements and resolved issues between release 4.0.4 and release 4.0.5.

Certificate Enhancements

- Expired certificates

  Certificates are now better organized to help prevent the unintentional selection of an expired certificate when entering credentials to gain access to a network. The user is no longer able to select a certificate if the expiration date of the certificate has passed. The user can now only select valid certificates. Also, valid certificates that are about to expire will warn the user by showing how many days are left before the certificate expires. (Ref #12884)

- Mandatory smart card usage

  The administrator is now able to configure the Secure Services Client to select only certificates from smart cards, if required by their enterprise policy. This configuration prohibits the use of locally stored certificates (Windows certificate store) and forces the use of the certificate credentials from a smart card. (Ref #13025)

- Smart cards with multiple certificates

  Smart card users are now able to store and access more than one credential from their smart card. Prior releases limited the number of smart card credentials to one. (Ref #13302)

- Smart card additions

  Support for the use of additional Windows certified smart cards to supply user certificate credentials prior to the user logging on has been added. (Ref #13215, 13216, 13217)

  The specific smart card and smart card reader models tested with this release are listed below:

  - GemPlus GemPK 64K smart cards
  - GemPlus GemPC Twin USB smart card reader
  - Dell built-in PCMCIA smart card reader for the D610 laptop

  - Dell smart card reader keyboard RT7D60

FAST PAC Security Enhancement

The Protected Access Credentials (PACs), used in the EAP-FAST authentication protocol, are now encrypted in such a way to help prevent copying PACs from one endpoint to another and potentially circumventing network access security. (Ref #12906)

A machine PAC is stored such that it is tied to the specific end station. If it is copied off to another end station, it will not be usable.

A tunnel (user) PAC is stored such that it is tied to the user for which it was created. Only a user that logs in to the account with the same username and password will be able to use it.

Authentication Enhancements

- Authentication timing improvements

  Improvements in obtaining an IP address have been made, resulting in faster connection timing. (Ref #13221)

- Visual display of authentication process

  Additional feedback is now provided to the user during the authentication process. The user can watch the authentication process via a new message display dialog that can be launched from the Secure Services Client user interface. If the process fails, the user will see this more readily with the new feedback mechanism. (Ref #13581)

Single-homed Failure to Choose Wired after Being on Standby or Hibernate

Previously in a single-homed configuration (a configuration in which a client permits only a single 802.1X connection) with both a wired and wireless adapter, if you entered standby or hibernate while having a wireless connection and if you reconnected the wired port prior to resuming, then the client would miss the availability (link-up) of the wired port and a wireless connection will be established instead. The Network View of the client's main screen would show the wired access, '<ethernet>', as 'Not Available'. This has been fixed so that now on resumption a wired connection is established as desired. (Ref #13519)

Service Shutdown Failures

Additional fixes have been made to prevent Secure Services Client from not properly shutting down when the SecureConnect Service is stopped. (Ref #13093)

Machine Group Policy

Improvements in supporting Machine GPOs when performing machine authenticated connections have been made. (Ref #12612)

Novell Contextless LDAP Lookup

Improvements in Novell Contextless LDAP lookups have been made such that username searches are now limited to the contexts given in the Novell registry under HKLM/Software/Novell/LDAP/Context/0. (Ref #13316)

Expired Trial License

The client indicates via a popup message window when features of the client expire. The message dialog also contains a link to the 'Activate Product Features' dialog to allow for changing the license.

Network Profile Deployment

Correct acceptance and processing when deploying the same network profile configuration file more than once has been fixed. (Ref #13886)

Windows Machine Certificates

Previously the client only accepted a single machine certificate in the Windows certificate store. Now, for cases when multiple certificates are present (for example, temporary overlap while provisioning a newer certificate to replace an old one or provisioning from different certificate authorities) rather than always failing authentication, the first valid certificate found is used. (Ref #13910)

File Saving with the Deployment Wizard

Improvements in saving your deployment package have been made. Now a check is made to ensure that the destination is a valid location. (Ref #12266)

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked 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.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation 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 Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems 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 Systems, 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 for networking professionals to 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

- 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.