# Cisco Secure Services Client 5.1

The following questions and answers provide some background information about the Cisco® Secure Services Client and its origins. In addition, under “Product Details,” you will find in-depth information about the functions of the client and its interoperability with Cisco solutions.

**Q. What is the Cisco Secure Services Client?**

**A.** The Cisco Secure Services Client is client software that resides on the device to manage the user identity and create secure network connections. It is an endpoint security and management solution for deploying and managing identity-based network access control for enterprise networks. It provides IT managers with a Layer 2 security framework that uses an industry-standard 802.1X implementation for protecting endpoint devices. Cisco Secure Services Client works across platforms to provide a common authentication framework across wired and wireless networks. Table 1 lists some of the main features of Cisco Secure Services Client.

**Table 1.** Cisco Secure Services Client Product Specifications

| Operating systems | Windows XP, Windows 2000, Windows Vista |
|---|---|
| **EAP protocols (XP/2000)** | EAP-Message Digest 5 (MD5), EAP-Transport Layer Security (TLS), EAP-Tunneled TLS (TTLS), Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Protected Extensible Authentication Protocol (PEAP) |
| **EAP protocols (Vista)** | Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Protected Extensible Authentication Protocol (PEAP) |
| **EAP-TTLS (XP/2000)** | Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MSCHAP), MSCHAPv2, EAP-MD5 |
| **EAP-PEAP (XP/2000)** | EAP-MSCHAPv2, EAP-TLS, and EAP-Generic Token Card (GTC) |
| **EAP-PEAP (Vista)** | EAP-MSCHAPv2 and EAP-GenericToken Card (GTC) |
| **Encryption support** | WEP, WPA, WPA2, WPA-Pre-Shared Key (WPA-PSK), WPA2-PSK, Dynamic WEP (802.1X), AES, TKIP |
| **Media support** | Wired Ethernet 802.3 and Wi-Fi 802.11a, 802.11b, 802.11g, 802.11n |
| **Switch interoperability** | Any 802.1X-compatible Wi-Fi access point and wired Ethernet switch |
| **Authentication, authorization, and accounting (AAA) interoperability** | Supports standard RADIUS servers such as Cisco Secure Access Control Server (ACS) and Microsoft Internet Authentication Service (IAS) |
| **Windows SSO** | Active Directory machine and user authentication |
| **Enterprise deployment** | Export network profiles and lock user interface |
| **Integrated VPN** | Automatic VPN requires the following software to be preinstalled;<br>• Cisco IPSec VPN version 4.8 or higher on Windows XP<br>• Cisco IPSec VPN version 5.0.03.0560 or higher on Windows Vista |
| **Integrated Software Token Applications (XP/2000)** | Automatic software token generation requires the following software to be preinstalled:<br>• Secure Computing SofToken II **(**Version 2.1 or later) |

**Q. Why is the product called Cisco Secure Services Client?**

**A.** The name Cisco Secure Services Client reflects two important aspects of the product: first, that it supports the industry-leading 802.1X standard for secure, extensible device authentication across wired and wireless networks; and second, that it delivers a range of services to the client based on the identity of the user and device. These services include:

- **Authentication services:** 802.1X
- **Encryption services for data and management:** Wi-Fi Protected Access (WPA) and WPA2
- **Cisco Compatible Extensions devices and services:** Diagnostic services, voice services, and location services (for Windows Vista when used with a wireless network interface card that supports Cisco Compatible Extensions Version 5, which integrates the Vista Cisco Compatible Extensions SDK)

**Q. What are the benefits of the Cisco Secure Services Client?**

**A.** The Cisco Secure Services Client enables IT departments to design and implement an 802.1X-based security strategy that positions the endpoint device as a defensible and secure new perimeter for wired and wireless networks. As a result, IT managers can deploy identity-based network security that can simultaneously enforce machine and user authorization rights, protect the integrity of devices, and reduce security breaches to the corporate network. Furthermore, the solutions are designed to simplify and enforce wired Ethernet and Wi-Fi access control policies, regardless of device, network, or authentication technology. Table 2 lists the main features and benefits of Cisco Secure Services Client.

**Table 2.** Cisco Secure Services Client Features and Benefits

| Feature | Function | Benefit |
|---|---|---|
| **Enterprise deployment mechanism** | Ability for IT administrators to deploy user profiles throughout the entire enterprise through a single XML file. | Offers significant time and cost savings by alleviating the need for administrators to deploy the client on each desktop. |
| **Unified wired and wireless network client** | Integration of wired Ethernet and Wi-Fi security. | Reduces the number of endpoint clients, simplifying IT administration. |
| **Support for industry standards** | IEEE, IETF, Wi-Fi Alliance, and Cisco Compatible Extensions. | Provides better assurance for support across a wide array of network adapters and solutions. |
| **Integration of Cisco IPSec VPN** | Automated establishment of VPN connection. | Reduction of client agents for a simplified user experience and automated launch for increased security. |
| **Endpoint integrity** | Enforcement of quarantine and remediation of noncompliant devices. | Minimizes chances for host PCs to be compromised by rogue software that could infect other devices on the network. |
| **SSO capability** | Support for Microsoft Active Directory single sign-on (SSO). | Reduces complexity for end users, in turn decreasing operating expenses for IT departments. |
| **Simple user interface** | Interface enhancements, including a convenient “two-click connect” to office, home, and public networks. The client also provides a connection status indicator for network name, strength, connection status, and IP address. | Allows end users to connect to the network more easily and eliminates the security concerns of connecting to any open SSID. Provides the same user interface across Windows 2000, XP, and Vista operating systems. |
| **Enabling of group policies** | Ability to apply network enforcement based on identity groups (dynamic VLAN assignment, downloadable access control lists [ACLs], and so on). | Provides ability to restrict user access to networked resources in addition to admission control. |
| **Administrative control** | Ability to selectively define and restrict certain security profiles and policies. | Provides centralized provisioning and enforcement of endpoint security policies, while still enabling user-defined hotspots and home profiles. |

Additional customer benefits of the Cisco Secure Services Client include:

- Integration with the Cisco IPSec VPN client
- Support for Federal Information Processing Standard (FIPS)140-2 Level 1
- Wired and wireless LAN connections, supporting WPA2 for wireless access
- Configurable network profiles and deployment tools to streamline network access
- Network access policy enforcement of server and client certificates
- One simple and flexible user interface across Windows 2000, XP, and Vista
- Interoperability with authentication, authorization, and accounting (AAA) and RADIUS servers to eliminate costly upgrades
- Support for Cisco Compatible Extensions Version 5.0 on Windows Vista when used with a wireless network interface card that supports Version 5
- Built-in, nonexpiring license that supports a basic, wired-only feature set
- Free, 90-day, full wired and wireless trial licenses

**Q. Is the Cisco Secure Services Client supported by the Cisco Secure ACS?**

**A.** Yes. The Cisco Secure Services Client is fully supported by the Cisco Secure ACS platform. The combination of the client supplicant and back-end authentication server provides customers with a comprehensive solution for robust client authentication across wired and wireless networks.

**Q. How does the Cisco Secure Services Client work with the Cisco Unified Wireless Network?**

**A.** The Cisco Secure Services Client allows enterprises to securely authenticate a variety of client devices to the wired and wireless network. The supplicant is fully supported by the Cisco Unified Wireless Network and works with the existing Cisco portfolio of access points and wireless LAN controllers.

**Q. Will the Cisco Secure Services Client become a part of the Trusted Computing Group (TCG) and Trusted Network Connect (TNC) working groups?**

**A.** Cisco currently has no plans to join the TCG or TNC working groups. Cisco believes that the protocols required for endpoint integrity should be developed under the IETF, where other Internet protocols are standardized. Cisco is working with the members of TNC at the IETF to further advance the interest in standardizing the protocols for endpoint integrity.

**Q. What is the part number of the Cisco Secure Services Client Version 5.1, and how can I order it?**

**A.** The Cisco Secure Services Client is available on the Cisco Global Price List and can be ordered as a standard Cisco product. Use the following part numbers to place an order: AIR SC5.0-XP2K for Windows 2000 and XP and AIR-SC5.0-VISTA for Windows Vista.

## Product Details

**Q. How does Cisco Secure Services Client 5.1 interface facilitate the end user experience?**

**A.** The interface provides a convenient “two-click connect” to office, home, and public wired and wireless networks. This allows end users to connect to the network more easily and eliminates the security concerns of connecting to an open (public) wireless network. The user interface also provides a comprehensive range of features and is accessible by right-clicking the taskbar icon or using the desktop icon. End users can view the connection status indicator for

network name, strength, connection status, and IP address. Finally, the integration of the VPN client combined with its automated activation represents a significant simplification for the end user.

**Q. What is the Enterprise Deployment feature?**

**A.** With the new Enterprise Deployment feature that is available in Cisco Secure Services Client 5.1, IT administrators can configure and deploy user profiles through a single XML file or the Cisco supplied management utility, a wizard that steps the IT administrator through the policy and configuration settings for users, devices, and networks. This reduces the time and cost required to deploy and set up the client on end-user systems.

**Q. Can the Cisco Secure Services Client hold multiple network profiles—for example, for use both at home and at work?**

**A.** Yes, the Cisco Secure Services Client supports unlimited profiles for home, work, travel, or other locations.

**Q. Can the Cisco Secure Services Client connect to open access points as well as secured access points?**

**A.** Yes, the Cisco Secure Services Client can be configured to support open access points as well as secured ones.

**Q. Does the Cisco Secure Services Client support WPA and WPA2?**

**A.** Yes, Cisco Secure Services Client Version 5.1 is fully compliant with the Wi-Fi Alliance's WPA and WPA2 encryption standards.

**Q. Is the Cisco Secure Services Client compatible with consumer-grade access points? Can I use WPA-PSK or WPA2-PSK to secure my home network?**

**A.** Yes, the Cisco Secure Services Client 5.1 is compatible with Wi-Fi-Certified home networking equipment. Cisco recommends that users configure their equipment to use WPA-PSK or WPA2-PSK to help ensure their privacy.

**Q. What EAP authentication methods does the Cisco Secure Services Client support?**

**A.** The Cisco Secure Services Client 5.1 for Windows 2000 and XP supports EAP MD5, EAP MSCHAPv2, EAP TLS, EAP-FAST, EAP- GTC, Cisco LEAP, PEAP, and EAP TTLS. The Cisco Secure Services Client 5.1 for Windows Vista supports EAP-FAST, Cisco LEAP, and PEAP.

**Q. Does the Cisco Secure Services Client support Federal Information Processing Standard (FIPS)?**

**A.** Yes, with the AIR-SSCFIPS-DRV driver (see ordering guide), Cisco SSC for Windows 2000 and XP support FIPS 140-2 Level 1. FIPS mode includes support for EAP-TLS, EAP-FAST, and PEAP.

**Q. What encryption methods does the Cisco Secure Services Client support?**

**A.** It supports WEP, Dynamic WEP (802.1X), WPA, WPA2, AES, TKIP, WPA-PSK, and WPA2 PSK.

**Q. What versions of Cisco IPSev VPN work with the Cisco SSC 5.1?**

**A.** Cisco IPSec VPN version 4.8.0.1 or later must be preinstalled on Windows XP. Cisco IPSev VPN version 5.0.03.0560 or later must be preinstalled on Windows Vista.

**Q. Does Cisco Secure Services Client 5.1 support fast roaming?**

**A.** Yes, Cisco Secure Services Client 5.1 does support Cisco Centralized Key Management (CCKM) for optimized roaming.

**Q. What operating systems does the Cisco Secure Services Client 5.1 support?**

**A.** It supports Windows 2000, Windows XP, and Windows Vista.

**Q. Is there a trial license available?**

**A.** Yes, a 90-day trial license key is available.

**Q. What happens when my trial license expires?**

**A.** The SSC will revert to the built-in wired-only license.

**Q. What happens if I configure the client to use the unlicensed features?**

**A.** The Cisco Secure Services Client has a soft licensing mechanism designed to inform the user of a right-to-use violation but not prevent the user from connecting to the network.

**Q. What features are available in the nonexpiring, wired-only version of the Cisco Secure Services Client?**

**A.** The following features are available in the nonexpiring, wired-only license:

- EAP methods (Windows XP and 2000)
  - EAP MSCHAPv2
  - EAP TLS
  - EAP FAST
  - EAP GTC
- EAP methods (Windows Vista)
  - EAP FAST
- Smartcard support (Windows XP and 2000)
- RSA SecureID support
- Wired adapters
- Support for standard RADIUS servers such as Cisco Secure ACS
- Central deployment of Microsoft Active Directory machine or user group policies

**Q. Are there plans to support additional operating systems?**

**A.** Yes. The Cisco Secure Services Client roadmap includes major operating system support for enterprise wired and wireless devices to provide consistent and uniform endpoint security and administration across different devices, including desktops, laptops, servers, wireless phones, handheld devices, and so on.

**Q. What smartcards and readers does the Cisco Secure Services Client support?**

**A.** The Windows 2000 and XP Cisco Secure Services Clients are designed to support smartcards that use standard Windows mechanisms for retrieving credentials from the card. Smartcards that use nonstandard credential retrieval mechanisms may not work with Secure Services Client. Table 3 lists some of the smartcards and smartcard reader combinations that Cisco Secure Services Client has been tested with.

**Table 3.** Smartcard Readers and Smartcards Supported by Cisco Secure Services Client

| Smartcard Readers | Smartcards |
|---|---|

| | Cryptoflex 8K | Cryptoflex 32K | Raak |
|---|---|---|---|
| **Axalto Reflex 20 v3 (PCMCIA reader)** | Yes | Yes | No |
| **Axalto Reflex 72 v2 (serial port)** | Yes | Yes | No |
| **Axalto Reflex USB v3 (USB)** | Yes | Yes | No |
| **Axalto Reflex USB v2 (USB)** | Yes | Yes | No |
| **Schlumberger/Raak egate reader (USB)** | No | No | Yes |
| **Aladdin eToken Pro 32K**[1] | No | No | No |
| **Gemplus Cryptoflex 32/64k** | Yes | Yes | No |
| **Gemplus Cyberflex 32/64k** | Yes | Yes | No |

**Q. Does the Cisco Secure Services Client allow the wireless adapter radio to be turned off and on?**

**A.** Yes. However, not all wireless cards support the mechanism used to control power on the card, so it will not work with all devices. It should be noted that turning the adapter radio off puts the adapter in standby mode, and standby mode is not the same as disabling or uninstalling the adapter.

**Q. Can both device and user group policy object (GPO) functions be used with the Cisco Secure Services Client?**

**A.** In Windows Vista, SSC does not work in conjunction with wired and wireless GPOs. All other types of GPOs are supported on both x32 and x64 Windows Vista platforms.

**Q. Can different authentication methods be used for device and user authentication?**

**A.** Separate authentication methods can be used for machine and user authentication. This function is under the control of the RADIUS server. For this reason, at present you need to use a RADIUS server, such as Cisco Secure ACS, that can filter on the host and identity prefixes sent during device authentication. Because the server will then know that the authentication is for a device, it can be configured to use the desired method.

**Q. Is the Cisco Secure Services Client interoperable with Cisco LAN switches?**

**A.** The Cisco Secure Services Client is interoperable with any Cisco LAN switch that supports the IEEE 802.1X protocol for authentication.

**Q. Does the Cisco Secure Services Client allow network administrators to define a “work” network for end users that is locked, but that still allows them to create their own network access profiles?**

**A.** Yes, by using the deployment wizard to create a set of deployment files. By selecting Configurable Client as the Client Type on the Station Policy, end users can define their own networks. Administrators can control the types of networks that the end user defines using the Network Policy, Wi-Fi Policy, and Authentication Policy categories. During the deployment, administrators define the “work” network and copy these files to the end users’ workstations. As part of the client deployment, the access profile entitled “work” is automatically locked, and end users cannot modify them. Additionally, end users can create new networks within the policy boundaries set by the administrator.

[1] Aladdin eToken Pro 32K is an integrated reader and card and thus does not work with other smartcards

## For More Information

For more information about Cisco Secure Services Client, visit: http://www.cisco.com/en/US/products/ps7034/index.html or contact your local Cisco account representative.

For more information about the Cisco Unified Wireless Network framework, visit: http://www.cisco.com/go/unifiedwireless

For more information about the wireless LAN security solution for large enterprises, visit: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_package.html

For more information about the Cisco Self-Defending Network, visit: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html

For more information about Network Admission Control, visit: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

For more information about the Cisco Secure Access Control Server for Windows, visit: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

For more information about Cisco Wireless LAN Services, visit: http://www.cisco.com/go/wirelesslanservices

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA C67-421397-01 10/08