

## Cisco Secure Services Version 5.1 Product

The Cisco<sup>®</sup> Secure Services Client is a software application that enables businesses of all sizes to deploy a single authentication framework across endpoint devices for access to both wired and wireless networks. The Cisco Secure Services Client solution delivers simplified management, robust security, and lower total cost of ownership. Through a simplified and scalable deployment mechanism, IT administrators can deploy and manage the Cisco Secure Services Client across the enterprise. The software client manages the user and device identity and the network access protocols required for secure access.

The Cisco Secure Services Client uses the IEEE 802.1X authentication standard to provide a robust first line of defense against unauthorized network intrusions. Using the 802.1X standard, access control decisions are made before the endpoint device is granted an IP address and access to the network. This gives the Cisco Secure Services Client the flexibility to deploy strong security for managing identity-based access for users and devices, and to deliver an effective port management solution. As a result, the operational cost of protecting the network is reduced.

Cisco Secure Services Client Version 5.1 contains an enterprise deployment feature that allows IT administrators to configure and deploy client profiles to the entire organization. Deploying the client from a centralized location saves significant time and ultimately helps lower the total cost of ownership (TCO) of deploying an 802.1X supplicant.

### **New Features and Benefits**

Version 5.1 of the Cisco Secure Services Client includes the following new features.

#### **Automatic VPN Feature**

- Integrated Cisco IPSec VPN.
- Integrated Secure Computing Soft Token.

#### **FIPS 140-2 Level 1 Compliant Solution**

- Federal Information Processing Standards (FIPS) drivers available (ordered separately).

#### **Cisco Enterprise Deployment Mechanism**

- Client provisioning from a unified XML file.
- Single provisioning schema independent of hardware.
- The administrator can now easily create an MSI file containing the XML and EXE file for installation.
- Files can then be deployed using standard deployment tools such as Microsoft Active Directory, Microsoft SMS, and Altiris.

#### **Filtering of Unwanted Service Set Identifiers (SSIDs)**

- Decreases the number of available networks for users.
- Enforces corporate security policies for end users.

#### **Enforcing Wired over Wireless**

- Enables wireless interface to be disabled when a wired connection is present.
- Eliminates unwanted wireless bridging to wired network.

#### **Policy Enforcement Manager**

- Enforces an 802.1X identity-based network security framework.
- Configures and enforces access policies to protect corporate resources and assets.

#### **Network Profile Manager**

- Using the administrator console, administrators can define preconfigurations, lock down client features, and deploy end-user profiles for enterprise, travel, and home connections.
- Provides network entitlement rights for employees, guests, and suppliers with different levels of security.

#### **Credential Manager**

- Windows single sign-on (SSO) capabilities, including device and user authentication.
- User-based authentication session and credential challenge.

#### **Secure Network Access**

- Authenticated access to 802.1X wired and wireless LANs.
- Compatible with Wi-Fi-certified devices.
- Support for all Wi-Fi encryption modes: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-personal mode (WPA-personal mode), WPA2-personal mode, WPA-enterprise mode, WPA2-enterprise mode, Dynamic WEP (802.1X), Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP).
- Support for a wide selection of Extensible Authentication Protocol (EAP) types.
- Protection of user privacy with EAP “anonymous” access.
- Compatible with the Cisco Secure Access Control Server (ACS).

#### **Access Management and Automated Configuration Control**

- Enterprise deployment mechanism through a unified XML file.
- Delivers user access policies to any port accessed by a user.
- Centrally deploys Microsoft Active Directory machine or user group profiles.
- Enables automatic configuration of VLANs.
- Comprehensive SSO support for the Windows login environment.

#### **Flexible Selection of User Credentials**

- Interactive user passwords or Windows passwords.
- RSA SecurID tokens.
- One-time password (OTP) tokens.
- Smartcards (Axalto, Gemplus, SafeNet iKey, Alladin).
- X.509 certificates.

## Product Specifications

Table 1 lists product specifications for Cisco Secure Services Client Version 5.1.

**Table 1.** Product Specifications for Cisco Secure Services Client Version 5.1

Operating systems	Windows XP, Windows 2000, Windows Vista
<b>EAP protocols (XP/2000)</b>	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)
<b>EAP protocols (Vista)</b>	Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Protected Extensible Authentication Protocol (PEAP)
<b>EAP-TTLS (XP/2000)</b>	Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MSCHAP), MSCHAPv2, EAP-MD5
<b>EAP-PEAP (XP/2000)</b>	EAP-MSCHAPv2, EAP-TLS, and EAP-Generic Token Card (GTC)
<b>EAP-PEAP (Vista)</b>	EAP-MSCHAPv2 and EAP-GenericToken Card (GTC)
<b>Encryption support</b>	WEP, WPA, WPA2, WPA-Pre-Shared Key (WPA-PSK), WPA2-PSK, Dynamic WEP (802.1X), AES, TKIP
<b>Media support</b>	Wired Ethernet 802.3 and Wi-Fi 802.11a, 802.11b, 802.11g, 802.11n
<b>Switch interoperability</b>	Any 802.1X-compatible Wi-Fi access point and wired Ethernet switch
<b>Authentication, authorization, and accounting (AAA) interoperability</b>	Supports standard RADIUS servers such as Cisco Secure ACS and Microsoft Internet Authentication Service (IAS)
<b>Windows SSO</b>	Active Directory machine and user authentication
<b>Enterprise deployment</b>	Export network profiles and lock user interface
<b>Integrated VPN</b>	Automatic VPN require the following software to be pre-installed; <ul style="list-style-type: none"> <li>• Cisco IPSec VPN version 4.8 or higher on Windows XP</li> <li>• Cisco IPSec VPN version 5.0.03.0560 or higher on Windows Vista</li> </ul>
<b>Integrated Software Token Applications (XP/2000)</b>	Automatic software PIN generation requires the following software to be preinstalled; <ul style="list-style-type: none"> <li>• Secure Computing <b>SofToken II</b> (Version 2.1 or later)</li> </ul>
<b>FIPS Solution (XP)</b>	Meets Federal Information Processing Standard 140-2 Level 1. <ul style="list-style-type: none"> <li>• Requires the purchase of separate drivers for a complete FIPS 140-2 Level 1 client solution on Windows XP. Driver part numbers are AIR-SSCFIPS-DRV (see ordering guide for more detail).</li> <li>• Supports Intel, Broadcom, and Atheros Wi-Fi chipsets</li> <li>• FIPS mode includes support EAP-TLS, EAP-FAST and PEAP association methods</li> </ul>

## System Requirements

Table 2 lists minimum system requirements for Cisco Secure Services Client Version 5.1.

**Table 2.** System Requirements for Cisco Secure Services Client Version 5.1

System	Minimum Requirements
<b>Disk space</b>	30 MB
<b>Hardware</b>	Pentium III 500 MHz (minimum), wired or wireless network card with a driver that supports NDIS 5.1 (wireless card should have the Wi-Fi Alliance stamp or logo)
<b>FIPS driver compatibility on Windows XP</b>	The drivers required for FIPS compliance (AIR-SSCFIPS-DRV) require the following Wi-Fi chipsets: <ul style="list-style-type: none"> <li>• Intel: 2100, 2200, 2915, 3945</li> <li>• Broadcom: All BCM 43XX</li> <li>• Atheros: 5001, 5004, 5005, AR5211, AR5212</li> </ul>
<b>Memory</b>	128-MB RAM
<b>Software</b>	Windows Vista (Business, Enterprise, or Ultimate), Windows XP (Home, Tablet, or Pro) SP1/SP2, Windows 2000 Pro SP4, Windows 2000 (Advanced) Server SP4, Windows 2003 Server (Standard, Enterprise)

## Ordering Information

Table 3 lists the part number for Cisco Secure Services Client Version 5.1 as well as the drivers that are required for FIPS on Windows XP. The FIPS drivers are typically required only for FIPS environments such as the Department of Defense and other U.S. and Canadian government entities.

To download the Cisco Secure Services Client, visit the [Cisco Ordering Home Page](#).

**Table 3.** Ordering Information for Cisco Secure Services Client Version 5.1

Product Name	Part Number
Cisco Secure Services Client (XP/2000)	AIR-SC5.0-XP2K
Cisco Secure Services Client (Vista)	AIR-SSC-VISTA
SSC FIPS Drivers (XP only)	AIR-SSCFIPS-DRV

## Service and Support

Cisco and our Wireless LAN Specialized Partners offer a broad portfolio of end-to-end services based on proven methodologies for planning, designing, implementing, operating, and optimizing the performance of a variety of secure voice and data wireless network solutions, technologies, and strategies. Cisco Wireless LAN Specialized Partners bring application expertise to help deliver a secure enterprise mobility solution with a low total cost of ownership. For more information about Cisco Services for wireless LAN, visit: <http://www.cisco.com/go/wirelesslanservices>.

## For More Information

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

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



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](http://www.cisco.com/go/offices).

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)