

## Cisco Secure Services Client Version 5.0

PB421396

This bulletin describes Cisco® Secure Services Client Version 5.0, a new release containing the features listed in Table 2 with a new GUI.

Cisco Secure Services Client Version 5.0 will be available in August 2007.

### New Features

Version 5.0 of the Cisco Secure Services Client includes the following new features.

#### New Graphical User Interface

The Cisco Secure Services Client 5.0 graphical user 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. End users no longer have to worry about overriding the office profile while IT administrators are assured that the corporate policies will remain intact.

The user interface 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.

#### Enterprise Client Deployment

The Cisco Secure Services Client enables large-scale enterprise deployment through the use of a single XML configuration file. The deployment file is set up by the IT administrator using any standard XML editor or the Cisco-supplied management utility a wizard that steps the IT administrator through the policy and configuration settings for users, devices, and networks.

The XML configuration file contains:

- Policy restrictions
- Network profiles
- Users file
- Trusted root certificate authority (CA) certificate
- Static Wired Equivalent Privacy (WEP) keys
- Wi-Fi Protected Access-Pre-Shared Keys (WPA-PSK)
- Trusted server validation rules
- Product license
- Platform Applicable Client (PAC)

Automatic generation of configuration files is enabled by running scripts that configure the XML file elements according to the enterprise policy.

IT staff can use the Cisco-supplied management utility to create an .msi file containing the .exe and the .xml, which can be deployed using standard deployment tools, including Microsoft Active Directory group policy objects (GPOs), Microsoft SMS, and Altiris.

### Filtering Unwanted Service Set Identifiers (SSIDs)

IT administrators also have more control with the ability to filter unwanted SSID networks. This feature is useful in an environment where there are multiple wireless networks.

### Enforcing Wired Access

During the configuration process, IT administrators can also enforce wired access when the software client is configured in automatic mode. This eliminates bridging or packet data storms between wired and wireless networks.

### Upgrade Paths and Trial Versions

The Cisco Secure Services Client 5.0 is an upgrade to the Cisco Secure Services Client version 4.0. To upgrade to the 5.0 version or to download a trial version, please visit <http://www.cisco.com/en/US/products/ps7034/index.html>. There is no additional charge to current Version 4.0, 4.1, or 4.2 license holders.

Table 1 lists the trial versions that are available for Cisco Secure Services Client 5.0.

**Table 1.** Trial Versions for Cisco Secure Services Client 5.0

License	Description
<b>90-day trial license</b>	A 90-day trial license is available for the full wired and wireless feature set of the Cisco Secure Services Client. Upon completion of the 90-day period, a valid license key must be purchased. The 90-day trial license key is posted in the download section. This license key must be entered through the activation screen of the client.
<b>Nonexpiring wired-only license</b>	A nonexpiring license is available for a wired-only version of the client with a limited feature set. (See the "New Features" section for more information.) This is the default license that comes in the download; it does not require a purchase.
<b>Nonexpiring wired and wireless license</b>	A nonexpiring license for the full feature set must be purchased using the Cisco standard ordering procedure.

### Wired and Wireless Versus Wired-Only Feature Comparison

Table 2 provides a comparison between the features available in the fully licensed wired/wireless Cisco Secure Services Client and the basic feature set available with the wired-only nonexpiring license. Note: Support for Novell networks is not included in Version 5.0 and will be provided in a following maintenance release.

**Table 2.** Wired/Wireless Versus Wired-Only Feature Set Comparison

Features	Wired-Only License	Wired/Wireless License
Wi-Fi device compatibility	No	Yes
Support for all Wi-Fi encryption modes: 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)	No	Yes
Protection of user privacy with Extensible Authentication Protocol (EAP) "anonymous" access	No	Yes
Cisco Secure Access Control Server (ACS) compatibility	Yes	Yes
Centrally deploys Microsoft Active Directory machine or user group policies	Yes	Yes
Enables automatic configuration of VLANs	Yes	Yes
Windows single sign-on (SSO)	Yes	Yes

Features	Wired-Only License	Wired/Wireless License
Interactive user passwords or Windows passwords	Yes	Yes
RSA SecureID tokens	Yes	Yes
One-time password (OTP) tokens	Yes	Yes
Smartcards	Yes	Yes
X.509 certificates	Yes	Yes
<b>EAP Methods</b>		
EAP-Transport Layer Security (TLS)	Yes	Yes
EAP-Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)	Yes	Yes
EAP-Generic Token Card (GTC)	Yes	Yes
EAP-Flexible Authentication via Secure Tunneling (FAST) (includes EAP-MSCHAPv2, EAP-GTC, and EAP-TLS)	Yes	Yes
Protected Extensible Authentication Protocol (PEAP) (includes EAP-MSCHAPv2, EAP-TLS, and EAP-GTC)	No	Yes
EAP-Message Digest 5 (MD5)	No	Yes
EAP-Tunneled TLS (TTLS) (includes Password Authentication Protocol [PAP], CHAP, MSCHAP, MSCHAPv2, EAP-MSCHAPv2, and EAP-MD5)	No	Yes
Cisco LEAP	No	Yes
<b>Media Support</b>		
Wi-Fi 802.11a, 802.11b, 802.11g	No	Yes
Wired Ethernet 802.3	Yes	Yes
Microsoft Internet Authentication Service compatibility	Yes	Yes
Active Directory and user authentication	Yes	

## Ordering Information

Table 3 lists ordering information for Cisco Secure Services Client 5.0.

**Table 3.** Ordering Information for Cisco Secure Services Client 5.0

Part Number	Status	Description
<a href="#">AIR-SC5.0-XP2K</a>	NONORD	Software Client 5.0 for Windows XP/2000 for wired/wireless devices
<a href="#">AIR-SC5.0-XP2K-L1</a>	ENABLE-OPT	Specified seat count up to 250
<a href="#">AIR-SC5.0-XP2K-L2</a>	ENABLE-OPT	Specified seat count in range 251-1000
<a href="#">AIR-SC5.0-XP2K-L3</a>	ENABLE-OPT	Specified seat count in range 1001-2500
<a href="#">AIR-SC5.0-XP2K-L4</a>	ENABLE-OPT	Specified seat count in range 2501-5000
<a href="#">AIR-SC5.0-XP2K-L5</a>	ENABLE-OPT	Specified seat count in range 5001-10,000
<a href="#">AIR-SC5.0-XP2K-L6</a>	ENABLE-OPT	Specified seat count in range 10,001-25,000
<a href="#">AIR-SC5.0-XP2K-L7</a>	ENABLE-OPT	Specified seat count in range 25,001-50,000
<a href="#">AIR-SC5.0-XP2K-L8</a>	ENABLE-OPT	Specified seat count in range 50,001-100,000

## 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 framework, visit: <http://www.cisco.com/go/unifiedwireless>

For more information about the Cisco Wireless LAN Security Solution for large enterprises, visit:  
[http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking\\_solutions\\_package.html](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](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](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>

The Cisco Secure Services Client includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://openssl.org>).

This product includes cryptographic software written by Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Cisco Secure Services Client complies with OpenSSL and SSLeay license requirements.  
<http://www.openssl.org/source/license.html>



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, CCVP, Cisco EEM, Cisco StadiumVision, the Cisco logo, CDE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play and Learn is a service mark, and Access Registrar, AnytimeOS, Bringing the Meeting To You, Catalyst, CCA, CCOR CCIE, CCOR CCNA, CCNP CCSP Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Probes, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Networking, FormShare, GigaDrive, HomeLink, Internet Quattro, IOS, iPhone, IPTV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Netwoset, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Reason Why so Increases Your Return, Unified Communications, Unified Computing, Unified Edge, 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 (USFPA).