

## Cisco Secure Services Client Release 4.0.51

PB385054

### Product Overview

This bulletin describes the contents of the Cisco® Secure Services Client Release 4.0.51. Cisco Secure Services Client 4.0.51 is a point release for the 4.0.5 product release and contains bug fixes identified from the previous product release. The release is scheduled to be generally available on December 21, 2006.

### Bug Fixes

**Table 1.** Bugs and Fixes for the Cisco Secure Services Client 4.0.51 Point Release

Bug	Included Fix
<b>More than one profile with same time stamp causes supplicant to crash</b>	Improvements have been made in handling incorrectly deployed configuration files. For example, errors in creating a deployed package and mistakenly copying both the network profile configuration XML file and the policy configuration XML file, which have the same timestamp, into the same folders. (Ref #13886)
<b>Authentication retries default value change</b>	Background: Some more intelligent access devices support special features that have, for example, the ability on a failed connection attempt to open the port but switch the user into a special VLAN. In order to support these access devices, the client provides the administrator with the capability of adjusting the number of connection retries before disconnecting, allowing the access device to make intelligent decisions based on multiple authentication failures.  The default values for 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. In this case, it is important to 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 #14434)
<b>Cisco Secure Services Client sends wrong password after Active Directory password change</b>	A fix has been made to correct the password that is sent when using single sign-on and the user is prompted to change their Active Directory password. An authentication failure and a subsequent reboot or re-logon is now avoided. (Ref CSCsf32767, CSCzd14391, CSCzd14494)
<b>Authentications while transferring from a machine to user context</b>	Improvements have been made to eliminate processing a redundant machine authentication session when logging onto Windows. (Ref CSCsd78605)
<b>Forced logoff of a user by a local administrator logon</b>	A fix has been made, in a machine-only or a machine/user connection context, so that when an administrator logs onto a user-locked computer, the network connection is maintained and the client responds normally. (Ref CSCsg71040)
<b>Upgrading from 4.0.4 to 4.0.5 may break trusted server validation</b>	A fix has been made that allows for a correct upgrade from the AEGIS SecureConnect 4.0.4 client for specific environments that are using server validation and happen to have two possible server certificate chains resident on the end station – one, an invalid Intermediate CA certificate and another, a valid Root CA certificate.  <b>Note:</b> If you have already successfully upgraded from version 4.0.4 (AEGIS SecureConnect) to 4.0.5 (Cisco Secure Services Client), this is not an issue.

### Upgrade Paths

Cisco Secure Services Client 4.0.51 is an upgrade to Cisco Secure Services Client 4.0.5. To upgrade to the 4.0.51 release, please visit

<http://www.cisco.com/en/US/products/ps7034/index.html>.

## Availability

December 21, 2006

## Ordering Information

**Table 2.** Ordering Information for Cisco Secure Services Client

Part Number	Status	Description
<a href="#">AIR-SC4.0-XP2K</a>	NONORD	Software Client 4.0 for Windows XP/2000 for wired/wireless devices
<a href="#">AIR-SC4.0-XP2K-L1</a>	ENABLE-OPT	Specified seat count up to 250
<a href="#">AIR-SC4.0-XP2K-L2</a>	ENABLE-OPT	Specified seat count in range 251–1000
<a href="#">AIR-SC4.0-XP2K-L3</a>	ENABLE-OPT	Specified seat count in range 1001–2500
<a href="#">AIR-SC4.0-XP2K-L4</a>	ENABLE-OPT	Specified seat count in range 2501–5000
<a href="#">AIR-SC4.0-XP2K-L5</a>	ENABLE-OPT	Specified seat count in range 5001–10,000
<a href="#">AIR-SC4.0-XP2K-L6</a>	ENABLE-OPT	Specified seat count in range 10,001–25,000
<a href="#">AIR-SC4.0-XP2K-L7</a>	ENABLE-OPT	Specified seat count in range 25,001–50,000
<a href="#">AIR-SC4.0-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 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 (ACS) for Windows, visit <http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html>.

**Americas Headquarters**

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

[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912

[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands

[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

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).

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)