



Release Notes for Cisco AnyConnect VPN Client, Release 2.4.0134 BETA

Revised: August 10, 2009

These release notes are for the beta release of 2.4. Cisco TAC does not provide support for beta releases. Please provide feedback to anyconnect24-beta@cisco.com.

The scope of these release notes is limited to the introduction, requirements, and changes in this release. Please go to the [AnyConnect documentation](#) for additional instructions.



Caution

Beta software should not be deployed in a production network. Cisco cannot be responsible for issues caused as a result of using beta software.

Introduction

The AnyConnect client provides remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

The AnyConnect client provides remote end users running Microsoft Windows 7, Windows Vista, Windows XP, Windows Mobile, Linux, and Macintosh OS X 10.5 with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. In addition, the AnyConnect client supports connecting to IPv6 resources over an IPv4 network tunnel.

You can install the client on the security appliance to automatically download to remote users when they log in, or administrators or users can manually install it as an application on. You can configure the security appliance to uninstall AnyConnect from the endpoint after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.



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

© 2009 Cisco Systems, Inc. All rights reserved.

Contents

This document includes the following sections:

- [New Features on page 2](#)
- [System Requirements on page 3](#)
- [Caveats on page 7](#)
- [Notices/Licensing on page 9](#)
- [Related Documentation on page 10](#)

New Features

AnyConnect 2.4 supports the following new features:

- Trusted Network Detection
- Simple Certificate Enrollment Protocol (SCEP)
- FIPS

You must have a FIPS license to enable FIPS. Along with the license, we provide the transforms, binaries (non-win), and instructions to enable FIPS.

- Launching of an optional, administrator-provided script when AnyConnect client connects, and of a second script when it disconnects.
- Logging improvements
- Proxy Support Enhancement
- Next Generation Filtering Framework
- CSD Integration
- Windows 7
- Improved Reconnect and Disconnect

New Guidelines

The following guidelines are new for Release 2.4.

Changes to OSs Supported

AnyConnect 2.4 supports Microsoft Windows 7. AnyConnect 2.4 no longer supports Microsoft Windows 2000 and Mac OS X 10.4, although it may work with these OSs.

Customers running Mac OS X 10.4 must upgrade to 10.5 when upgrading to AnyConnect 2.4. We will continue to support Mac OS X 10.4 users running pre-2.4 versions until we end-of-life those versions.

AnyConnect 2.4 now supports Red Hat Enterprise Linux 5 Desktop and Ubuntu 9.x. We do not qualify other Linux distributions. We will consider requests regarding other Linux distributions for which you experience issues, and provide fixes at our discretion.

Upgrading to Windows 7

If you upgrade from Windows XP or Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it.

Flexibility in Sequence and Method Used to Install Start Before Logon and DART Components

Previously, in order to use the Start Before Logon components for Windows, the same installation method was required for both the AnyConnect client and the Start Before Logon components. Both needed to be pre-deployed or both needed to be web-deployed. AnyConnect Release 2.4 eliminates this requirement. This allows the client to be deployed by one method and, perhaps at a later time, the Start Before Logon components to be installed by the same or another method. The Start Before Logon component still has the requirement that the AnyConnect client be installed first.

Another new behavior for AnyConnect Release 2.4 is that if SBL or DART is manually uninstalled from an end-point that then connects, these components will be re-installed. This behavior will only occur if the head-end configuration specifies that these components be installed and the preferences (set on the end-point) permit upgrades. Previously these components would not be re-installed in this scenario without uninstalling and re-installing the AnyConnect client.

System Requirements

If you are using Internet Explorer, use version 5.0, Service Pack 2 or later.

AnyConnect does not support virtualization software, such as VMWare for any platform, or Parallels Desktop for Mac OS.

AnyConnect does not support sessions with a security appliance running on the same subnet as the endpoint.

Microsoft Windows

If you are using Internet Explorer, use version 5.0, Service Pack 2 or later. For WebLaunch, use Internet Explorer 6.0+ or Firefox 2.0+, and enable ActiveX or install Sun JRE 1.4+.

Windows Versions

- Windows 7
- Windows Vista—SP2 or Vista Service Pack 1 with KB952876.
- Windows XP SP2 and SP3.

Windows Requirements

- Pentium class processor or greater.
- x64 or x86 processors.
- 5 MB hard disk space.
- RAM:

- 256 MB for Windows XP.
- 512 MB for Windows Vista.
- 512 MB for Windows 7.
- Microsoft Installer, version 3.1.

Linux

The following sections show the Linux distributions and requirements.

Linux Distributions

- Red Hat Enterprise Linux 5 Desktop
- Ubuntu 9.x

We do not qualify other Linux distributions. We will consider requests regarding other Linux distributions for which you experience issues, and provide fixes at our discretion.

Linux Requirements

- x86 instruction set.
- 32-bit or biarch 64-bit processor—standalone mode only; web-based install/connect is not supported.
- 32 MB RAM.
- 20 MB hard disk space.
- Superuser privileges.
- libstdc++ users must have libstdc++ version 3.3.2 (libstdc++.so.5) or higher, but below version 4.
- Firefox 2.0 or later with libnss3.so installed in /usr/local/lib, /usr/local/firefox/lib, or /usr/lib. Firefox must be installed in /usr/lib or /usr/local, or there must be a symbolic link in /usr/lib or /usr/local called firefox that points to the Firefox installation directory.
- libcurl 7.10 or later.
- openssl 0.9.7a or later.
- java 1.5 or later. The default Java package on Fedora is an open-source GNU version, called Iced Tea on Fedora 8. The only version that works for web installation is Sun Java. You must install Sun Java and configure your browser to use that instead of the default package.
- zlib or later.
- gtk 2.0.0,
gdk 2.0.0,
libpango 1.0.
- iptables 1.2.7a or later.
- tun module supplied with kernel 2.4.21 or 2.6.

Mac OS

AnyConnect 2.4 supports Mac OS X Version 10.5. It requires 50 MB hard disk space.

Windows Mobile

Cisco designed AnyConnect 2.4 for compatibility with Windows Mobile 6.1, 6.0 and 5.0 Professional and Classic for touch-screens only, but has specifically qualified only the devices listed in [Table 1](#) to ensure interoperability. While other devices might work, Cisco does not guarantee compatibility with other devices. [Table 1](#) lists the supported devices with their corresponding service providers and supported operating system versions.

Table 1 Supported Windows Mobile Devices (Touch-screens Only)

Device	OS	Wi-Fi
ATT Tilt 3.57.502.2 WWE Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	✓
Axim X51v with ROM: A03 (23092007)	Windows Mobile 6.0 Classic	✓
iPAQ 2790	Windows Mobile 5.0 PocketPC	✓
Sprint Touch with ROM: 3.03.651.4 Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	—
T-Mobile Wing 4.26.531.1 WWE	Windows Mobile 6.0 Professional	✓
Palm Treo 700wx: • Sprint TREO 700WX-1.15-SPNT	Windows Mobile 5.0+AKU2 PDA Phone	—
Palm Treo 750: • AT&T TREO750-2.27-RWE • AT&T TREO 750-2.25-ATT • T-Mobile TREO750-2.27-RWE	Windows Mobile 6.0 Professional	—
Palm Treo 800: • Sprint Treo 800w-1.03-SPNT	Windows Mobile 6.1 Professional	✓
Palm Treo Pro: • AT&T T850UNA-1.01-NAE • Sprint T850EWW-1.03-SPT • T-Mobile T850UNA-1.01-NAE	Windows Mobile 6.1 Professional	✓
Verizon XV6800 with ROM: 1.00.00.H: • Verizon 2.09.605.8 • Verizon 3.57.605.1	Windows Mobile 6.0 Professional and Windows Mobile 6.0 Professional	✓

Security Appliances and Software Supported

The Cisco AnyConnect VPN Client supports all Cisco Adaptive Security Appliance models. It does not support PIX devices. See the Adaptive Security Appliance VPN Compatibility Reference: <http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html> for a complete list of compatibility requirements.

[Table 2](#) shows the minimum Cisco ASA 5500 Adaptive Security Appliance software images that support the AnyConnect client.

Table 2 Software Images that Support the AnyConnect Client, Release 2.4

Image Type	Version
ASA Boot image	8.0(3).1 or later
Adaptive Security Device Manager (ASDM)	6.1(3).1 or later
Cisco Secure Desktop	3.2(2) ¹ or later

¹. Cisco Secure Desktop, Release 3.2(1) is compatible, but it provides more limited functions.

Installing the AnyConnect Client on a Windows Mobile Device

The security appliance does not support WebLaunch of AnyConnect on a mobile device; therefore, mobile users must download and install AnyConnect Client for Windows Mobile. Just as you can do so with corporate computers, you can pre-deploy AnyConnect on Windows Mobile devices issued to employees.

Perform the following steps to download and install AnyConnect Client for Windows Mobile.

-
- Step 1** Download any of the following files from the Cisco AnyConnect VPN Client Download Software site to get the Windows Mobile Client:
- File containing all client installation packages:
anyconnect-all-packages—*AnyConnectRelease_Number-k9.zip*
 - CAB package signed by Cisco for Windows Mobile devices:
anyconnect-wince-ARMv4I—*AnyConnectRelease_Number-k9.cab*
 - ActiveSync MSI package for Windows Mobile platforms:
anyconnect-wince-ARMv4I-activesync—*AnyConnectRelease_Number-k9.msi*
- Step 2** Unzip the anyconnect-all-packages—*AnyConnectRelease_Number-k9.zip* file if you chose to download that file.
- Step 3** Transfer the file to a corporate server if you want to provide users with a link to the client.
- Step 4** Make sure the Windows Mobile device meets the system requirements in the latest [AnyConnect Release Notes](#).
- Step 5** Use your preferred method to transfer the .cab or .msi file from your intranet server or local computer to the mobile device. Some examples include:
- Microsoft ActiveSync over radio

- HTTP, FTP, SSH, or shared files over the LAN or radio
- Bluetooth
- (USB) Cable
- Media card transfer

Step 6 Use the mobile device to open the file you transferred, and proceed with the installation wizards.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists caveats with Severities 2 and 3.



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats in Cisco AnyConnect VPN Client, Release 2.4 Beta

Table 3 lists the caveats that are unresolved in the Cisco AnyConnect VPN client, Release 2.4 Beta.

Table 3 *Open Caveats in Cisco AnyConnect VPN Client, Release 2.4 Beta*

ID	Headline
CSCsh51779	Client-side proxy & AoN tunneling: must stop direct access to proxy.
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client.
CSCsi00491	Standalone can connect to wrong ASA from within SecureDesktop.
CSCsi35149	Transcend: unable to clear session from GW after setting MSIE proxy V
CSCsi44045	Difficult to clear the VPN program after tunnel cleared from GW
CSCsm92424	Random client DPD disconnects with McAfee HIPS SW.
CSCsq02996	Auto-resume sometimes fails even though head-end not timed out.
CSCsq88383	AnyConnect user authentication fails in some scenarios.
CSCsr23029	Standalone client fails to connect if CSD and Authenticating proxy.
CSCsu08798	AnyConnect Linux with certs fails if browser master password defined.
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt.
CSCsu70199	IPv6: Network error: windows has detected and IP address conflict.
CSCsv49773	Multiple local profiles for SG may result in using wrong settings.
CSCsw28876	AnyConnect: Need to reboot PC to get localization catalog to load.
CSCsw30030	Vista: Unable to process response from using standalone AnyConnect.
CSCsw37980	AC needs more certificate matching events.
CSCsw40079	Failed to initialize VPN API aborting message while launching AC.

Table 3 *Open Caveats in Cisco AnyConnect VPN Client, Release 2.4 Beta*

ID	Headline
CSCsw85805	AnyConnect only waits 12 seconds for auth response from headend.
CSCsw97163	AC should not re-use tg cookie if group-url w/ new tg is being used.
CSCsx14838	XP:DART application not installed while connecting AC in some scenarios.
CSCsx21485	VPN agent "caches" cert information.
CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
CSCsx70548	Linux: user logoff does not disconnect VPN connection
CSCsy34111	SVC MSIE proxy option auto does not work
CSCsy48762	Split tunnel not working with Anyconnect and Windows Mobile
CSCsy73171	AnyConnect roam from EVDO car to 802.11 never reconnected
CSCsz19269	AnyConnect ignoring exclusion lists and using proxy server
CSCsz27811	Anyconnect: After cert validation error, get Connection failure unknown
CSCsz95464	Anyconnect fails to connect with special character password "<>"
CSCsz28004	AnyConnect failed authorization after certs, Connect button errors
CSCsz97362	Need to document some 3rd Party inter-operability issues
CSCsz99190	AnyConnect Mac: Installer leaves vpnclient.dmg in root directory
CSCta63379	Voice mails thru an Anyconnect tunnel on a Mac OS is garbled
CSCtb11342	Global and user preferences files may get out of sync

Resolved Caveats

The following sections identify the caveats that Release 2.4 resolves.

Caveats Resolved in AnyConnect Release 2.4 Beta

Table 4 shows the caveats that AnyConnect VPN Client, Release 2.4 Beta resolves.

Table 4 *Resolved Caveats by Cisco AnyConnect VPN Client, Release 2.4 Beta*

ID	Headline
CSCsq49102	AnyConnect incompatibility with Citrix advanced gateway client 2.2.1
CSCsx14777	DART:AC Standalone AnyConnect Client shows AnyConnect 2.3.xx instead of AnyConnect dart 2.3.xx.
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCsz67246	Anyconnect SBL: XML parsing prevents concurrent connections
CSCsz78112	Long-term fix for Anyconnect with IPv6: non-English Vista
CSCta01109	file move operation fails
CSCta11649	AnyConnect on Mac OS should be able to verify Certs from KeyChain

Table 4 *Resolved Caveats by Cisco AnyConnect VPN Client, Release 2.4 Beta*

ID	Headline
CSCta31173	Allow mDNS through filters with Local LAN
CSCta36014	AnyConnect API Package incorrect dependency
CSCta39434	AC - If CertificateMatch in Profile selects 0 certs, AC will use any
CSCta55059	AnyConnect: Admin unable to use Local Machine certificates
CSCta59527	Anyconnect picks invalid certificate
CSCta59878	DART install gets out-of-sync with local manifest
CSCta73252	AnyConnect connection failure due to wrong windows shell registry

Notices/Licensing

Two kinds of licenses affect the Cisco AnyConnect VPN Client:

- [End-User License Agreement on page 9](#) (End User License Agreement)
- [OpenSSL/Open SSL Project on page 9](#)

The following sections provide information about these licenses.

End-User License Agreement

For information on the end-user license agreement, go to:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

For Open Source License information for this product, please see the following link:

<http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html#wp50053>.

Related Documentation

For more information, refer to the following documentation:

- For additional information about the security appliance or ASDM or its platforms, see *Navigating the Cisco ASA 5500 Series Documentation*:
<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html>
- *Cisco AnyConnect VPN Client, Release 2.3, Administrator Guide*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.