Release Notes for Cisco AnyConnect VPN Client, Release 2.4.0196

Revised: September 17, 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. Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. This is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver the capabilities set forth below.

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 (32-bit and 64-bit), Windows Vista, Windows XP, Windows Mobile, Linux, and Macintosh OS X 10.5 and 10.6 (32-bit and 64-bit) 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

Contents

This document includes the following sections:

New Features

AnyConnect 2.4 supports the following new features:

- New Platforms Supported
- Split DNS Fallback
- Trusted Network Detection
- Simple Certificate Enrollment Protocol (SCEP)
- Scripting
- Proxy Support Enhancement
- CSD Integration
- PEM File Certificate Store

New Platforms Supported

AnyConnect Client 2.4 runs on the following new platforms:

- Microsoft Windows 7 (32-bit and 64-bit). See Upgrading to Windows 7.
- Mac OS X 10.6 (32-bit and 64-bit).

Split DNS Fallback

If the group policy on the security appliance specifies the names of the domains to be tunneled, AnyConnect Client tunnels only DNS queries that match those domains. It refuses all other DNS queries. The DNS resolver receives the refusal from the client and retries, this time using the public interface instead of AnyConnect Client.

This feature requires that you:

- Configure at least one DNS server
- Enable split-tunneling

To use this feature, establish an ASDM connection to the security appliance, choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies> Add or Edit > Advanced > Split Tunneling, and enter the names of the domains to be tunneled into the DNS Names text box.

Trusted Network Detection

Trusted Network Detection (TND) gives you the ability to have the AnyConnect client automatically disconnect a VPN connection when the user is inside the corporate network (the *trusted* network) and start the VPN connection when the user is outside the corporate network (the *untrusted* network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.

The AnyConnect client supports TND on Windows XP and later, and Mac OS X. TND is not supported on mobile devices.

Note If you enable TND with Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the remote computer automatically closes.

You configure TND in the AnyConnect profile (AnyConnectProfile.xml), an XML file downloaded with the client that contains settings that affect client behavior. Table 1 shows the profile parameters to configure TND and their values:

Table 1 Trusted Network Detection Parameters

Name	Possible Values and Descriptions
AutomaticVPNPolicy	*true*—Enables TND. Automatically manages when a VPN connection should be started or stopped according to the *Trusted-UntrustedPolicy* parameter. *false*—Disables TND. VPN connections can only be started and stopped manually. **Note** AutomaticVPNPolicy does not prevent users from manually controlling a VPN connection.
TrustedNetworkPolicy	*Disconnect*—Disconnects the VPN connection in the trusted network. *DoNothing*—Takes no action in the trusted network.
UntrustedNetworkPolicy	*Connect*—Initiates the VPN connection (if none exists) in the untrusted network. *DoNothing*—Takes no action in the trusted network. **Note** Setting both TrustedNetworkPolicy and UntrustedNetworkPolicy to *DoNothing* disables TND.
TrustedDNSDomains	A list of DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSDomainNames string: *.cisco.com Wildcards (*) are supported for DNS suffixes.
TrustedDNSServers	A list of DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSServers string: 161.44.124.*,64.102.6.247 Wildcards (*) are supported for DNS server addresses.

The following text shows the ClientInitialization section of the profile file with the TND parameters configured. In the example, the client is configured to automatically disconnect the VPN connection when in the trusted network, and to initiate the VPN connection in the untrusted network:

```
<AutomaticVPNPolicy>true
    <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
    <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
    <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
    <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

Table 2 shows examples of DNS suffix matching.

Table 2 DNS Suffix Matching Examples

To Match this DNS Suffix:	Use this value for TrustedDNSDomains:
cisco.com (only)	cisco.com
cisco.com AND anyconnect.cisco.com	*cisco.com OR cisco.com, anyconnect.cisco.com
asa.cisco.com AND anyconnect.cisco.com	*.cisco.com OR asa.cisco.com, anyconnect.cisco.com

Simple Certificate Enrollment Protocol (SCEP)

The AnyConnect 2.4 standalone client can employ the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate used for client authentication. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible.

In our implementation of SCEP, the AnyConnect client sends a certificate request and the certificate authority (CA) automatically accepts or denies the request. (The SCEP protocol also allows for a method where the client requests a certificate and then polls the CA until it receives an accept or deny response. The polling method is not implemented in this release.)

AnyConnect users have one task associated with this feature. If the user profile is configured to have users request a certificate manually, users see a button in the AnyConnect GUI labeled **Get Certificate or Enroll.** AnyConnect users do not need to know, and will not know, what method AnyConnect uses to retrieve the certificate.

AnyConnect administers configure the use of SCEP requests in the user profile. The user profile is maintained in the AnyConnect profile file. This file is an XML file downloaded with the client that contains settings that affect client behavior. Table 3 describes the profile elements used to configure the SCEP feature.

Table 3 Elements in the user profile used to configure SCEP

Element name	Child of	Description
CertificateEnrollment	ClientInitialization	Starting tag for certificate enrollment.
CertificateExpirationThreshold	CertificateEnrollment	Specifies the number of days prior to a certificate expiring, that the user is warned about the expiration. Default: 0 Range of Values: 0-180 The default value for this element is 0 which means no warning will be displayed. The maximum value is 180 days prior to the certificate expiring. In the example below, CertificateExpirationThreshold is set to **`14`** days.
AutomaticSCEPHost	CertificateEnrollment	The host will attempt automatic certificate retrieval if this attribute specifies the ASA host name and tunnel group for which SCEP certificate retrieval is configured. **Permitted values**: • Fully qualified domain name of the ASA\tunnel group name • IP Address of the ASA\tunnel group name In the example below, the AutomaticSCEPHost field specifies, **`asa.cisco.com`** as the host name of the ASA and **`scep_eng`** as the name of the tunnel group configured for SCEP certificate retrieval.
CAURL	CertificateEnrollment	Identifies the SCEP CA server. **Permitted values**: Fully qualified domain name or IP Address of CA server. In the example below, the CAURL field identifies **`ca01.cisco.com`** as the name of the SCEP CA server. Attributes of CAURL: **PromptForChallengePW**: Used for manual get certificate requests. After the user clicks Get Certificate, they will be prompted for their username and one time password. **Permitted values**: true, false The PromptForChallengePW attribute in the example below is configured "**`true`**." **Thumbprint**: The CA's certificate thumbprint. Use SHA1 or MD5 hashes. The Thumbprint attribute in the example below is **`8475B661202E3414D4EE554A464E6AAB8CA4970A`**.
CertificateSCEP	CertificateEnrollment	Section that defines how the contents of the certificate will be requested. See the CertificateSCEP element in the example below.
CADomain	CertificateSCEP	Domain of the certificate authority. In the example below, the CADomain is **`cisco.com`**.

Table 3 Elements in the user profile used to configure SCEP (continued)

Element name	Child of	Description
Name_CN	CertificateSCEP	Common Name in the certificate. In the example below, Name_CN ic**`USER%`** corresponds to the user's ASA username login credential.
DisplayGetCertButton	CertificateSCEP	Determines if the AnyConnect GUI displays the Get Certificate button. Administers may choose to configure this button if they think it will give their users a clearer understanding of what they are doing when interacting with the AnyConnect interface. Without this button, users see a button labeled "Enroll" along with a message box that AnyConnect is contacting the certificate authority to attempt certificate enrollment. **Default value**: false **Range of Values**: true, false If the DisplayGetCertButton attribute is set to false, the Get Certificate button will not be visible in the AnyConnect GUI. Choose false if you do not permit users to manually request provisioning or renewal of authentication certificates. If the DisplayGetCertButton attribute is set to true, the Get Certificate button will be visible to users if the certificate is set to expire within the period defined by the CertificateExpirationThreshold element, after the certificate has expired, or if no certificate is present. Choose true if you permit users to manually request provisioning or renewal of authentication certificates. Typically, these users will be able to reach the certificate authority without first needing to create a VPN tunnel. In the following example, DisplayGetCertButton is set to false.
Department_OU	CertificateSCEP	Department name specified in certificate.
Company_O	CertificateSCEP	Company name specified in certificate.
State_ST	CertificateSCEP	State identifier named in certificate.
Country_C	CertificateSCEP	Country identifier named in certificate.
Email_EA	CertificateSCEP	Email address. In the example below, Email_EA is **`%USER%.cisco.com`**. **`%USER%`** corresponds to the user's ASA username login credential.
Domain_DC	CertificateSCEP	Domain component. In the example below, Domain_DC is set to **`cisco.com`**.
ServerList	AnyConnectProfile	Starting tag for the server list. The server list is presented to users when they first launch AnyConnect. Users can choose which ASA to login to. See ServerList in the example below.
HostEntry	ServerList	Starting tag for configuring an ASA. Look at the second HostEntry element in the example below.
HostName	HostEntry	Host name of the ASA. In the second HostEntry element in the example below, the HostName element is **`Certificate Enroll`**.

Table 3 Elements in the user profile used to configure SCEP (continued)

Element name	Child of	Description
HostAddress	HostEntry	Fully qualified domain name of the ASA. In the second HostEntry element in the example below, the HostAddress element is set to **asa2.cisco.com.**
AutomaticSCEPHost	HostEntry	This element has the same definition and permitted values as the one described earlier in this table. However, if this element is configured, and the user chooses this HostEntry from the server list, this value overrides the value of AutomaticSCEPHost configured earlier in the user profile file. In the example below, for this HostEntry, AutomaticSCEPHost is set to **asa2.cisco.com/scep_eng.**
CAURL	HostEntry	This element has the same definition, permitted values, and attributes as the one described earlier in this table. However, if this element is configured, and the user chooses this HostEntry from the server list, this value overrides the value of CAURL configured earlier in the user profile file. In the example below, for this HostEntry, CAURL is set to **asa2.cisco.com/scep_eng.**

Example of SCEP Elements in User Profile

```
<AnyConnectProfile>
    <ClientInitialization>
        <CertificateEnrollment>
           <CertificateExpirationThreshold>14</CertificateExpirationThreshold>
           <AutomaticSCEPHost>asa.cisco.com/scep_eng</AutomaticSCEPHost>
           <CAURL PromptForChallengePW="true"
Thumbprint="8475B661202E3414D4EE554A464E6AAB8CA4970A">ca01.cisco.com</CAURL>
            <CertificateSCEP>
               <CADomain>cisco.com</CADomain>
               <Name_CN>%USER%</Name_CN>
               <DisplayGetCertButton>false</DisplayGetCertButton>
               <Department_OU>Engineering</Department_OU>
               <Company_O>Cisco Systems</Company_O>
               <State_ST>Colorado</State_ST>
               <Country_C>US</Country_C>
               <Email_EA>%USER%@cisco.com</Email_EA>
               <Domain_DC>cisco.com</Domain_DC>
            </CertificateSCEP>
        </CertificateEnrollment>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>CVC-ASA</HostName>
            <HostAddress>cvc-asa-cluster.cisco.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>Certificate Enroll</HostName>
            <HostAddress>asa2.cisco.com</HostAddress>
            <AutomaticSCEPHost>asa2.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="false"
Thumbprint="8475B655202E3414D4EE554A464E6AAB8CA4970A">ca02.cisco.com</CAURL>
        </HostEntry>
    </ServerList>
```

```
</AnyConnectProfile>
```

Scripting

AnyConnect Release 2.4 lets you download and run scripts when the following events occur:

- Upon initial VPN connection of the AnyConnect client to the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- After VPN disconnection of the AnyConnect client from the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logon to a service upon VPN connection, and log off after disconnection.

Note These instructions assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.

Scripting Requirements and Limitations

AnyConnect runs up to one OnConnect and up to one on DisConnect script, but these scripts may launch other scripts.

AnyConnect does not require the script to be written in a specific language, but does require an application that can run the script to be installed on the client computer. Thus, for AnyConnect to launch the script, the script must be capable of running from the command line.

AnyConnect supports script launching on all Microsoft Windows, Mac OS X, and Linux OSs supported by AnyConnect. Microsoft Windows Mobile does not provide native support for scripting languages; however, you can create and automatically run an OnConnect application and an OnDisconnect application as long as it complies with the AnyConnect scripting filename prefix and directory requirements.

On Microsoft Windows, AnyConnect can only launch scripts after the user logs onto Windows and establishes a VPN session. Thus, the restrictions imposed by the user's security environment apply to these scripts; scripts cannot execute functions that require administrator privileges.

AnyConnect supports script launching during WebLaunch and standalone launches.

By default, AnyConnect does not launch scripts.Use the AnyConnect profile EnableScripting parameter to enable scripts. AnyConnect does not require the presence of scripts if you do so.

Client GUI termination does not necessarily terminate the VPN session; the OnDisconnect script runs after session termination.

Other requirements apply, as indicated in the next section.

Writing, Testing, and Deploying Scripts

Deploy AnyConnect scripts as follows:

Step 1 Write and test the script using the OS type on which it will run when AnyConnect launches it.

Note Scripts written on Microsoft Windows computers have different line endings than scripts written on Mac OS and Linux. Therefore, you should write and test the script on the targeted OS. If a script cannot run properly from the command line on the native OS, AnyConnect cannot run it properly either.

Step 2 Do one of the following to deploy the scripts:

- Use binary AnyConnect customization to deploy the scripts from the security appliance.

  Note Microsoft Windows Mobile does not support this option. You must deploy scripts using the manual method for this OS.

  If you use binary AnyConnect customization to deploy scripts, the filenames of the scripts or applications must have the following prefixes:

  – scripts-OnConnect

  – scripts-OnDisconnect

  AnyConnect uses the `scripts-` prefix to identify the files as scripts and write them to the proper target directory on the VPN endpoint. As it does so, it removes the `scripts-` prefix, leaving the remaining `OnConnect` or `OnDisconnect` prefix.

  To ensure the scripts run reliably, configure all security appliances to deploy the same scripts. If you want to modify or replace a script, use the same name as the previous version and assign the replacement script to all of the security appliances that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Or transfer the scripts manually to the VPN endpoints on which you want to run the them.

  If you use this method, use the script filename prefixes below.

  – OnConnect

  – OnDisconnect

  Install the scripts in the directory shown in Table 4.

Table 4 Required Script Locations

OS	Directory
Microsoft Windows 7 and Vista	%ALLUSERPROFILE%\Cisco\Cisco AnyConnect VPN Client\Scripts
Microsoft Windows XP	%ALLUSERPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN Client\ Scripts
Linux[1]	/opt/cisco/vpn/scripts
Mac OS X	/opt/cisco/vpn/scripts
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client\Scripts

[1] On Linux, assign execute permissions to the file for User, Group and Other.

Configuring the AnyConnect Profile for Scripting

To enable scripting you must insert the EnableScripting parameter into the AnyConnect profile. Table 5 describes the scripting parameters you can insert into the AnyConnect profile. Examples follow the table.

Table 5 Scripting Parameters

Name	Possible Values and Descriptions
EnableScripting	true—Launches OnConnect and OnDisconnect scripts if present. false—(Default) Does not launch scripts.
UserControllable	**Note**: If used, this parameter must be embedded within the EnableScripting tag, as shown in Example 2 below this table. The possible values are: • true—Lets users enable or disable the running of OnConnect and OnDisconnect scripts. • false—(Default) Prevents users from controlling the scripting feature.

Table 5 Scripting Parameters (continued)

TerminateScriptOnNextEvent	This parameter has meaning only if the EnableScripting is set to true. **Note**: If used, this parameter must be embedded within the EnableScripting tag, as shown in Example 2 below this table. The possible values are: • true—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if AnyConnect starts a new VPN session. On Microsoft Windows, AnyConnect also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On Mac OS and Linux, AnyConnect terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts. • false—(Default) Does not terminate a script process if a transition to another scriptable event occurs.
EnablePostSBLOnConnectScript	This parameter has meaning only if the EnableScripting is set to true, and only if the VPN endpoint is running Microsoft Windows 7, XP, or Vista. **Note**: If used, this parameter must be embedded within the EnableScripting tag, as shown in Example 2 below this table. The possible values are: • false—Prevents launching of the OnConnect script if SBL establishes the VPN session. • true—(Default) Launches the OnConnect script if present if SBL establishes the VPN session.

Insert these parameters anywhere inside the `ClientInitialization` section of the AnyConnect profile.

Example 1

This example enables scripting and uses the default values for the other scripting parameters:

```
<ClientInitialization>

<EnableScripting>true</EnableScripting>

</ClientInitialization>
```

Example 2

This example enables scripting and overrides the default values for the other scripting parameters:

```
<ClientInitialization>

<EnableScripting UserControllable="true">true
    <TerminateScriptOnNextEvent>true</TerminateScriptOnNextEvent>
    <EnablePostSBLOnConnectScript>false</EnablePostSBLOnConnectScript>
</EnableScripting>

</ClientInitialization>
```

Note Be sure to add the AnyConnect profile to the security appliance group policy to download it to the VPN endpoint.

Troubleshooting Scripts

If a script fails to run, try resolving the problem as follows:

Step 1 Make sure the script has an `OnConnect` or `OnDisconnect` prefix name. Table 4 shows the required scripts directory for each OS.

Step 2 Try running the script from the command line. AnyConnect cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that OS.

Step 3 Make sure the scripts directory on the VPN endpoint contains only one OnConnect and only one OnDisconnect script. If one security appliance downloads one OnConnect script and during a subsequent connection a second security appliance downloads an OnConnect script with a different filename suffix, AnyConnect might run the unwanted script. If the script path contains more than one OnConnect or DisConnect script and you are using binary AnyConnect customization to deploy scripts, remove the contents of the scripts directory and re-establish an AnyConnect VPN session. If the script path contains more than one OnConnect or DisConnect script and you are using the manual deployment method, remove the unwanted scripts and re-establish an AnyConnect VPN session.

Step 4 If the OS is Linux, make sure the script file permissions are set to execute.

Step 5 Make sure the AnyConnect profile includes the EnableScripting parameter set to true.

Proxy Support Enhancement

The proxy support enhancement features the following components new to AnyConnect Release 2.4.

Mac/Safari Private Proxy

AnyConnect downloads the proxy settings configured in the group policy to the Safari browser after the tunnel is established. The settings return to their original state after the VPN session ends.

To access the proxy settings, establish an ASDM session with the security appliance and choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > IE Browser Proxy. The proxy service configured in this window now applies to both Internet Explorer and Safari. The Do not use proxy parameter, if enabled, removes the proxy settings from Safari for the duration of the session because AnyConnect does not support a public-side proxy (that is, one used to establish the tunnel) on Mac OS.

Internet Explorer Connections Tab Lockdown

Under certain conditions, AnyConnect hides the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies regarding that tab. The conditions under which this lockdown occurs are either of the following:

- The security appliance configuration specifies a private-side proxy.
- AnyConnect uses a public-side proxy defined by Internet Explorer to establish the tunnel. In this case, the split tunneling policy on the security appliance must be set to Tunnel All Networks.

Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the security appliance require extra AnyConnect configuration to continue to allow clientless portal access through a proxy server after establishing an AnyConnect session. AnyConnect now uses a proxy auto-configuration (PAC) file to modify the client-side proxy settings to let this to occur. AnyConnect generates this file only if the ASA does not specify private-side proxy settings.

CSD Integration

AnyConnect 2.4 is more tightly integrated with Cisco Secure Desktop (CSD) beginning with CSD 3.5. With this enhancement, the user prompts are displayed as soon as the pre-login scan completes. Typically, this is faster than waiting for the entire hostscan process to run its course.

The integration of AnyConnect and CSD begins with AnyConnect 2.4 and CSD 3.5. If your site uses AnyConnect 2.4 with CSD 3.4 or earlier, or if your site uses AnyConnect 2.3 with CSD 3.5, you will not receive the benefits of this integration.

We ensure that CSD 3.5 is still compatible with earlier versions of AnyConnect and AnyConnect 2.4 is still compatible with earlier versions of CSD. If an AnyConnect user is configured to use CSD, AnyConnect 2.4 will deploy the version of CSD installed on the ASA, even if a later version of CSD is already installed on the host.

AnyConnect 2.4 will display and log descriptive posture assessment messages and installation messages passed to it from CSD 3.5. Other than these messages, AnyConnect users will have no interaction with this enhancement in 2.4.

PEM File Certificate Store

The AnyConnect client supports certificate authentication using a file store. Instead of relying on browsers to verify and sign certificates, the client reads Privacy Enhanced Mail (PEM) format certificate files from the file system on the remote computer, and verifies and signs them.

The AnyConnect client supports the PEM file certificate store for all Linux and Mac OS X platforms currently supported by the client.

In order for the AnyConnect client to acquire the appropriate certificates under all circumstances, ensure that your files meet the following requirements:

- All certificate files must end with the extension **.pem**.
- All private key files must end with the extension **.key**.

- A client certificate and its corresponding private key must have the same filename. For example: client.pem and client.key

Note Instead of keeping copies of the PEM files, you can use soft links to PEM files.

Storing User Certificates

To create the PEM file certificate store, create the paths and folders listed in Table 6. Place the appropriate certificates in these folders:

Table 6 PEM File Certificate Store Folders and Types of Certificates Stored

PEM File Certificate Store Folders	Type of Certificates Stored
~/.cisco/certificates/ca[1]	Trusted CA and root certificates
~/.cisco/certificates/client	Client certificates
~/.cisco/certificates/client/	Private keys

[1] ~ is the home directory.

Note The requirements for machine certificates are the same as for PEM file certificates, with the exception of the root directory. For machine certificates, substitute /opt/.cisco for ~/.cisco. Otherwise, the paths, folders, and types of certificates listed in Table 6 apply.

New Guidelines

The following guidelines are new for Release 2.4.

Changes to OSs Supported

AnyConnect 2.4 now supports Microsoft Windows 7 (32-bit and 64-bit) and Mac OS X 10.6 (32-bit and 64-bit). 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 before 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 validate other Linux distributions. We will consider requests to validate 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 an 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 (32-bit and 64-bit)
- 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 validate other Linux distributions. We will consider requests to validate 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 and 10.6 (32-bit and 64-bit). AnyConnect requires 50MB of 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 7 to ensure interoperability. While other devices might work, Cisco does not guarantee compatibility with other devices. Table 7 lists the supported devices with their corresponding service providers and supported operating system versions.

Table 7 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 8 shows the minimum Cisco ASA 5500 Adaptive Security Appliance software images that support the AnyConnect client.

Table 8 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 device meets the Windows Mobile system requirements.

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

\

Table 9 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.
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.
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

Table 9 Open Caveats in Cisco AnyConnect VPN Client, Release 2.4 Beta (continued)

ID	Headline
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
CSCsz28004	AnyConnect failed authorization after certs, Connect button errors
CSCsz95464	Anyconnect fails to connect with special character password “<>”
CSCsz97362	Need to document some 3rd Party inter-operability issues
CSCtb11342	Global and user preferences files may get out of sync
CSCtb70879	AnyConnect fails to connect if Ignore Proxy is enabled with CSD
CSCtb73046	Linux: Single user at time of connection establishment not enforced
CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
CSCtb80457	AnyConnect and ASA need to negotiate time-to-wait for authentication

Resolved Caveats

The following sections identify the caveats that Release 2.4 resolves.

Caveats Resolved in AnyConnect Release 2.4 Beta

Table 10 shows the caveats that AnyConnect VPN Client, Release 2.4 Beta resolves.

Table 10 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
CSCsx79055	Upgrade during SBL incomplete
CSCsy00749	AnyConnect: Failed to initialize connection to subsystem upon reconnect
CSCsy44786	GUI fails when users log off using SBL
CSCsz67246	Anyconnect SBL: XML parsing prevents concurrent connections
CSCsz78112	Long-term fix for Anyconnect with IPv6: non-English Vista
CSCsz99190	AnyConnect Mac: Installer leaves vpnclient.dmg in root directory
CSCta01109	file move operation fails
CSCta13784	Post SBL script launch fails on Vista with access denied error
CSCta21437	AnyConnect: Safesign CSP prompts for PIN using AAA

Table 10 Resolved Caveats by Cisco AnyConnect VPN Client, Release 2.4 Beta (continued)

ID	Headline
CSCta31173	Allow mDNS through filters with Local LAN
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
CSCta70161	HCP renew clobbers DNS settings on Linux AnyConnect
CSCta73252	AnyConnect connection failure due to wrong windows shell registry
CSCta63379	Voice mails through an Anyconnect tunnel on a Mac OS is garbled
CSCtb63734	UserControllable variable broken for SBL
CSCtb51693	Installer MST causes Anyconnect install/auto-update to fail
CSCtb76577	Anyconnect connection failure with IPv6

Notices/Licensing

Two kinds of licenses affect the Cisco AnyConnect VPN Client:

- End-User License Agreement on page 21 (End User License Agreement)
- OpenSSL/Open SSL Project on page 21

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*

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.