CHAPTER 1

Introduction to AnyConnect

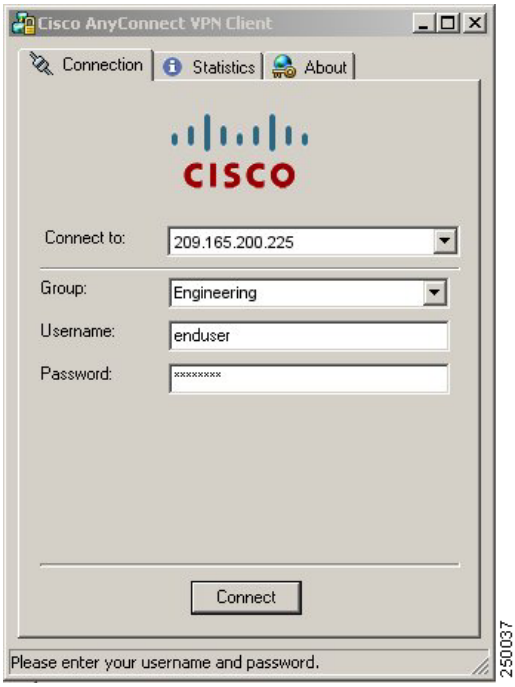
The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance running ASA version 8.0 and higher or ASDM 6.0 and higher.

This chapter includes the following sections:

Remote User Interface

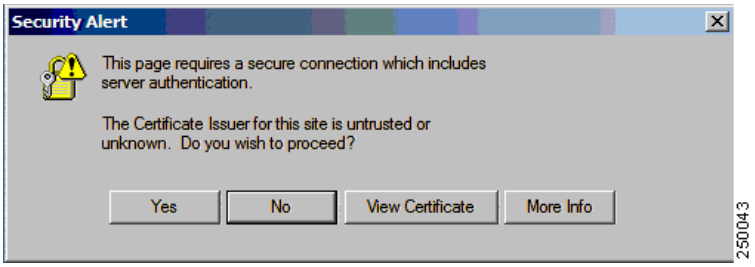
Remote users see the Cisco AnyConnect VPN Client user interface (Figure 1-1). The Connection tab provides a drop-down list of profiles for connecting to remote systems. You can optionally configure a banner message to appear on the Connection tab. The status line at the bottom of the interface shows the status of the connection.

Figure 1-1 Cisco AnyConnect VPN Client User Interface, Connection Tab



If you do not have certificates set up, you might see the dialog box shown in Figure 1-2.

Figure 1-2 Security Alert Dialog Box



Note This dialog box opens only if the correct certificate is not deployed. You can click Yes to bypass the certificate requirement.

The Security Alert dialog box appears only on the first connection attempt to a given security appliance. After the connection is successfully established, the "thumbprint" of the server certificate is saved in the preferences file, so the user is not prompted on subsequent connections to the same security appliance.

If the user switches to a different security appliance and back, the Security Alert dialog box appears again.

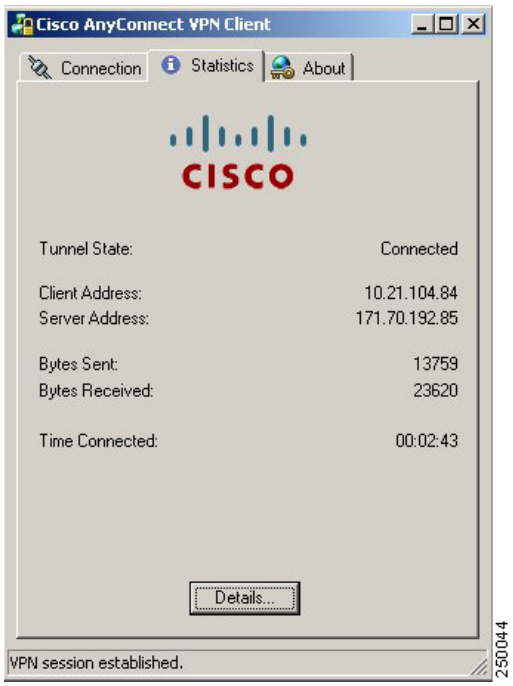
Table 1-1 shows the circumstances and results when the Security Alert dialog box appears.

Table 1-1 Certificate, Security Alert, and Connection Status

Certificate Status	Does Security Alert Appear?	Client Connection Status
Server certificate sent to the client from the security appliance is independently verifiable *and* the certificate has no serious errors.	No	Success
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate contains serious errors.	No	Failure
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate does *not* contain serious errors.	Yes	Because the client cannot verify the certificate, it is still a security concern. The client asks the user whether to continue with the connection attempt.

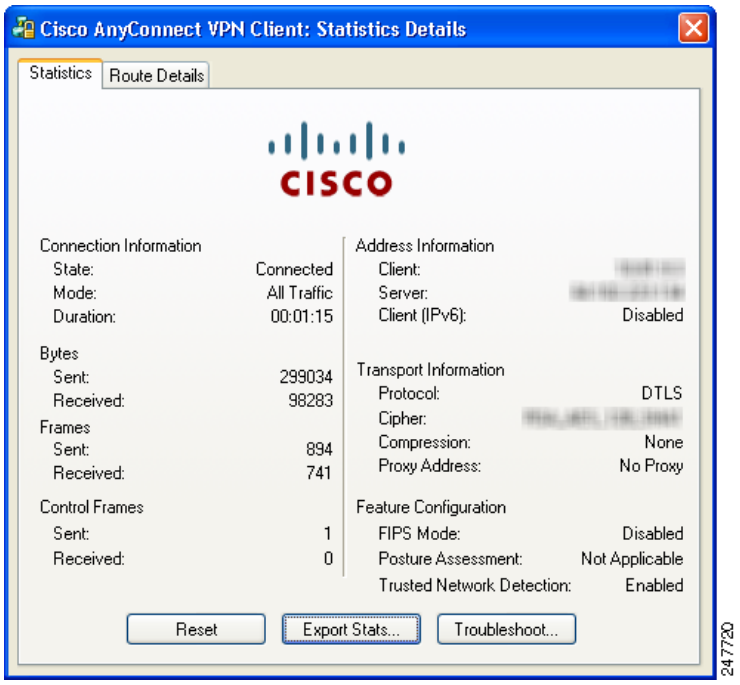
Figure 1-3 shows the Statistics tab, including current connection information.

Figure 1-3 Cisco AnyConnect VPN Client User Interface, Statistics Tab



Clicking the Details button opens the Statistics Details window (Figure 1-4).

Figure 1-4 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Statistics Details Tab

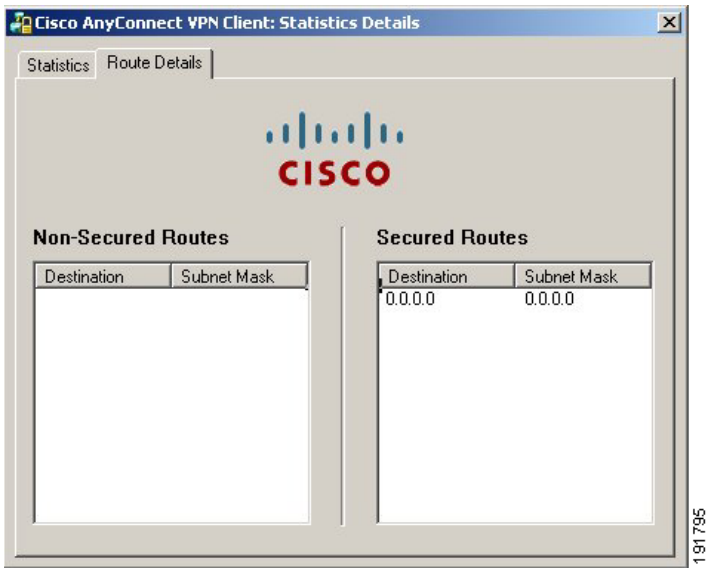


The options available in this window depend on the packages that are loaded on the client PC. If an option is not available, its radio button is not active and a "(Not Installed)" indicator appears next to the option name in the dialog box. The options are as follows:

- Clicking **Reset** resets the connection information to zero. AnyConnect immediately begins collecting new data.
- Clicking **Export Stats...** saves the connection statistics to a text file for later analysis and debugging.
- Clicking **Troubleshoot...** Launches the DART (Diagnostic AnyConnect Reporting Tool) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. See Using DART to Gather Troubleshooting Information, page 8-5 for information about the DART package.

The Route Details tab (Figure 1-5) shows the secured and non-secured routes for this connection.

Figure 1-5 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Route Details Tab



Note A Secured Routes entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all traffic is tunneled.

See Viewing Detailed Statistical Information, page 8-2 for information about using the Export and View Log buttons for connection monitoring.

The About tab (Figure 1-6) shows version, copyright, and documentary information about the Cisco AnyConnect Client.

Figure 1-6 Cisco AnyConnect VPN Client User Interface, About Tab

AnyConnect License Options

The following options support full AnyConnect client functionality while specifying the number of SSL VPN sessions supported:

- Cisco AnyConnect Essentials license
- Cisco AnyConnect Premium Clientless SSL VPN Edition license
- Cisco AnyConnect Premium Clientless SSL VPN Edition shared license
- Cisco FLEX license

The first three licenses are mutually exclusive per device (that is, per security appliance), but you can configure a mixed network.

AnyConnect Standalone and WebLaunch Options

The user can use the AnyConnect Client in the following modes:

- Standalone mode—Lets the user establish a Cisco AnyConnect VPN client connection without the need to use a web browser. If you have permanently installed the AnyConnect client on the user's PC, the user can run in standalone mode. In standalone mode, a user opens the AnyConnect client just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on how you configure the system, the user might also be required to select a group. When the connection is established, the security appliance checks the version of the client on the user's PC and, if necessary, downloads the latest version.

- WebLaunch mode—Lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

  The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

Whether connecting via standalone mode or WebLaunch mode, the AnyConnect client package must be installed on the security appliance in order for the client to connect. This ensures that the security appliance is the single point of enforcement as to which versions of the client can establish a session, even if you deploy the client with an enterprise software deployment system. When you load a client package on the security appliance, you enforce a policy that only versions as new as the one loaded can connect. AnyConnect users must upgrade their clients by loading the latest version of the client with the latest security features on the security appliance.

AnyConnect Files and Components

The installation and configuration consists of two parts: what you have to do on the security appliance, and what you have to do on the remote computer. The AnyConnect client software is built into the ASA Release 8.0(1) and later. You can decide whether to make the AnyConnect client software permanently resident on the remote PC, or whether to have it resident only for the duration of the connection.

The client can be loaded on the security appliance and automatically deployed to remote users when they log in to the security appliance, or it can be installed as an application on PCs by a network administrator using standard software deployment mechanisms.

To get the AnyConnect client files and API package, go to http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect.

Installing Start Before Logon Components (Windows Only)

Table 1-2 Files Available for Download on the Cisco AnyConnect VPN Client Download Software Site

AnyConnectProfileEditor.zip	Zip file containing AnyConnect Profile Editor.
anyconnect-all-packages-AnyConnectRelease_Number-k9.zip	Zip file containing all client install packages for this release version. Does not include API.
anyconnect-dart-win-AnyConnectRelease_Number-k9.msi	Standalone MSI package with DART for Windows platforms.
anyconnect-gina-win-AnyConnectRelease_Number-pre-deploy-k9-lang.zip	Language localization transform files for Windows Start Before Login.
anyconnect-gina-win-AnyConnectRelease_Number-pre-deploy-k9.msi	Start Before Login GINA module for Windows 2k/XP/Vista.
anyconnect-gina-win-AnyConnectRelease_Number-web-deploy-k9-lang.zip	Language localization transform files for web-deploy for Windows Start Before
anyconnect-linux-AnyConnectRelease_Number-k9.pkg	Web deployment package for Linux platforms.

Table 1-2 Files Available for Download on the Cisco AnyConnect VPN Client Download Software Site (continued)

AnyConnectProfileEditor.zip	Zip file containing AnyConnect Profile Editor.
anyconnect-linux-AnyConnectRelease_Number-k9.tar.gz	Standalone tarball package for Linux platforms.
anyconnect-macosx-i386-AnyConnectRelease_Number-k9.dmg	Standalone DMG package for Mac OS X Intel platforms.
anyconnect-macosx-i386-AnyConnectRelease_Number-k9.pkg	Web deployment package for Mac OS X Intel platforms.
anyconnect-macosx-powerpc-AnyConnectRelease_Number-k9.dmg	Standalone DMG package for Mac OS X PowerPC platforms.
anyconnect-macosx-powerpc-AnyConnectRelease_Number-k9.pkg	Web deployment package for Mac OS X PowerPC platforms.
anyconnect-no-dart-win-AnyConnectRelease_Number-k9.pkg	Web deployment package without DART for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-k9.pkg	Web deployment package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-pre-deploy-k9-lang.zip	Language localization transform files for pre-deploy package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-pre-deploy-k9.msi	Standalone MSI package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-web-deploy-k9-lang.zip	Language localization transform files for web-deploy package for Windows platforms.
anyconnect-wince-ARMv4I-AnyConnectRelease_Number-k9.cab	Standalone CAB package (signed) for Windows Mobile platforms.
anyconnect-wince-ARMv4I-AnyConnectRelease_Number-k9.pkg	Web deployment package for Windows Mobile platforms.
anyconnect-wince-ARMv4I-activesync-AnyConnectRelease_Number-k9.msi	ActiveSync MSI package for Windows Mobile platforms.

If you configure a security appliance for WebLaunch of AnyConnect, AnyConnect orders the component sequence automatically. Otherwise, the Start Before Logon components must be installed *after* the core client has been installed. Additionally, the AnyConnect 2.2 Start Before Logon components require that version 2.2, or later, of the core AnyConnect client software be installed. If you are pre-deploying the AnyConnect client and the Start Before Logon components using the MSI files (for example, you are at a big company that has its own software deployment—Altiris or Active Directory or SMS.), you must specify the components in the correct sequence.

AnyConnect Files Installed on the VPN Client Computer

AnyConnect Client downloads the following files on the local computer:

Table 1-3 AnyConnect Files on the Endpoint

File	Description
anyfilename.xml	AnyConnect Client profile. This file specifies the features and attribute values configured for a particular user type.
AnyConnectProfile.tmpl	Example AnyConnect Client Profile provided with the AnyConnect Client software.
AnyConnectProfile.xsd	Defines the XML schema format. AnyConnect uses this file to validate the profile.

AnyConnect downloads these three files to the same directory, as follows:

Table 1-4 Paths to the Profile Files on the Endpoint

OS	Directory Path
Windows 7 and Vista	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile\
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\
Mac OS X and Linux	/opt/cisco/vpn/profile/

Configuration and Deployment Overview

Use the AnyConnect Profile editor to configure the client features in the preferences file; then configure the security appliance to upload this file along with the client automatically when users use a web browser to connect to the VPN. The preference file drives the display in the user interface and defines the names and addresses of host computers. By creating and assigning different preferences files to group profiles configured on the security appliance, you can differentiate access to these features. Following assignment to the respective group profiles, the security appliance automatically pushes the one assigned to the user's group profile upon connection setup.

Profiles provide basic information about connection setup, and users cannot manage or modify them. An AnyConnect client user profile is an XML file that lets you identify the secure gateway (security appliance) hosts that you want to make accessible. In addition, the profile conveys additional connection attributes and constraints on a user.

Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. In such cases, the user selects the appropriate profile from a drop-down list. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

Alternatively, you can install or let users install the preferences file and client as an application on computers for later access. This alternative method is the only method supported for Windows Mobile devices.

AnyConnect API

Use the Application Programming Interface (API) if you want to automate a VPN connection with the AnyConnect client from another application, including the following:

- Preferences
- Set tunnel-group method

The API package contains documentation, source files, and library files to support a C++ interface for the Cisco AnyConnect VPN Client. There are libraries and example programs that can be used for building the client on Windows, Linux and Mac OS X. The API package includes project files (Makefiles) for the Windows platform. For other platforms, a platform-specific script shows how to compile the example code. You can link your application (GUI, CLI, or embedded application) with these files and libraries.