Symbian User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4

Updated: May 31, 2011

Contents

This document describes the Cisco AnyConnect Secure Mobility Client 2.4 for devices running Symbian. It includes the following sections:

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

Introduction

The Cisco AnyConnect Secure Mobility client for Symbian provides seamless and secure remote access to enterprise networks. The client allows any installed application to communicate as though connected directly to the enterprise network.

The product is installed with the standard Software Installation Script (SiS) installer which you can download directly from the ASA 5500 Series Adaptive Security Appliance operating as a secure gateway. Refer to the "Installation" section on page 2 for additional information. You must invoke the installer manually to begin installation. The Cisco Adaptive Security Appliance (ASA) is the secure gateway that admits access to the VPN, and you can get updates of AnyConnect for Symbian from the ASA.

AnyConnect for Symbian is similar to AnyConnect for Windows, Mac OS X, and Linux. Your organization may provide additional documentation on using AnyConnect on Symbian.

Devices Supported by Cisco AnyConnect 2.4

This release supports the Nokia E6 and any other Nokia device that runs a "New Symbian OS." The device must be a touchscreen phone.

Note "New Symbian OS" is the name for the latest Symbian operating system, previously referred to as Symbian^3.

What You Need Before You Can Set Up AnyConnect

You must obtain some or all of the following from your system administrator, depending on your network requirements, before you can set up AnyConnect to establish an encrypted VPN session:

- Server Address—Domain name, IP address, or Group URL of the Cisco Adaptive Security Appliance to be used as the VPN secure gateway.
- Username and password—Credentials needed to access the VPN.

If using the Symbian On-Demand VPN feature, refer to the "Setting Up On-Demand VPN" section on page 8.

Installation

You can install the Cisco AnyConnect Secure Mobility client for a Symbian device with the standard Software Installation Script (SiS) standalone installer. Follow these steps to invoke AnyConnect for a Symbian device:

Step 1 From the ASA, download the vpnsetup.sis installer file from the location provided by your administrator. The SiS installer location that is recommended to the administrator is https://exampleasa.com/getinstaller, where *exampleasa.com* is the URL of the ASA to which the user is connecting.

The SiS file has all the binary components required on the client, including VPN GUI, VPN Agent, VPNDownloader, and so on.

Step 2 When you access this URL link, you are prompted for the credentials provided by your system administrator.

Step 3 After authentication is established, you receive a download request. The AnyConnect Symbian installer is downloaded upon accepting the request.

Getting Started

To get started:

Step 1 After installation, the AnyConnect icon appears in Menu > Application (see Figure 1-1). Open the Symbian main menu and click on **Applications**. Choose **AnyConnect** from the list of installed applications.

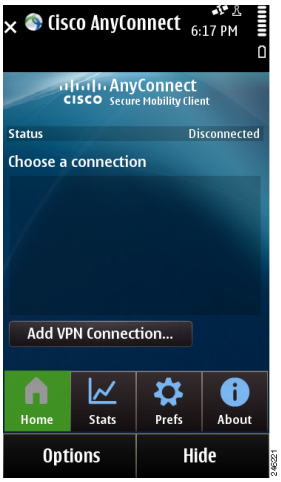
Figure 1-1 AnyConnect Icon

Step 2 A confirmation window opens the first time you start AnyConnect on the device. It conveys what network service is being used and the charge according to the network usage plan. You must accept this message to use AnyConnect. If you choose **Reject**, AnyConnect will not start.

From this window you can add a new VPN server and manage it or initiate the session. The status field on the home screen shows your running status messages from AnyConnect (see Figure 1-2). Refer to the following sections for additional information about the Stats, Prefs, and About options on the home screen:

- Stats—Viewing Overview Statistics
- Prefs—Setting Preferences
- About—Displaying the AnyConnect Version and Licensing Details

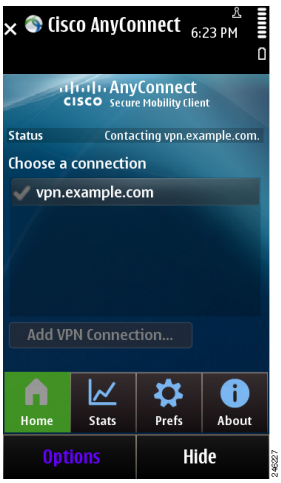
Figure 1-2 AnyConnect Main Screen



Step 3 AnyConnect shows the VPN connection status on the AnyConnect home screen. When you choose a connection, the status momentarily indicates which connection is being established (see Figure 1-3).

Note You cannot change the address once you have saved a connection.

Figure 1-3 Showing New Status After VPN Connection



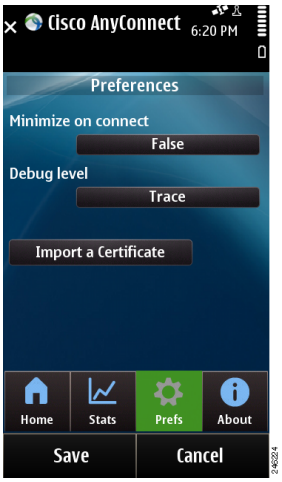
Before establishing your first VPN connection, follow the steps in the "Adding a VPN Connection Entry" section on page 6.

Setting Preferences

If you choose the **Prefs** button, you can set preferences (see Figure 1-4). The items and values are populated based on the user controller preferences from the profile. Some of the items and values include the following:

- Minimize on Connect—Controls the AnyConnect GUI behavior when a VPN session is established. By default, the GUI does not minimize when the VPN session is established (the false setting). If set to true, AnyConnect is sent to the background immediately after the VPN is connected.
- Debug Level—Specify which level you want recorded in the log file.
  - Trace—Logs debug messages, warnings, and error messages (used for troubleshooting purposes)
  - Information—Logs messages that are just informational without the Trace messages detail
  - Warning—Logs errors and warning messages
  - Error—Logs only error messages (the default configuration)
- AutoReconnect—Allows an administrator to control how a client behaves when the VPN session is interrupted. If set to true, the VPN automatically tries to reconnect when interrupted.
- AutoUpdate—Allows an administrator to turn off the dynamic update functionality of AnyConnect.

Figure 1-4 Preferences Screen



On the Preference screen, you can also choose **Import a Certificate**. Choose this option if you want to use certificate-based authentication to the secure gateway. With this option, you choose the .pfx file (PKCS12 certificates or other extensions), which carries the private key and the certificate, and the password for the .pfx file. With the credentials, you can import the certificate into the device store of the phone.

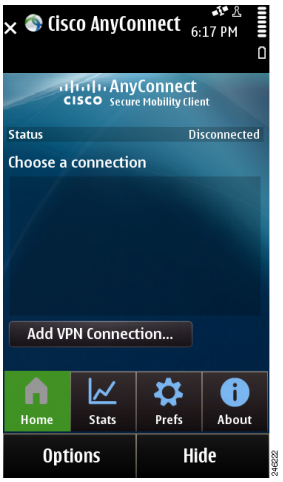
Note When importing a certificate, use only the Import a Certificate option from AnyConnect's Preferences screen. If you import a certificate directly from the Symbian UI, AnyConnect cannot access or use the certificate.

Adding a VPN Connection Entry

Before using AnyConnect to initiate an SSL VPN connection, add a VPN connection entry to identify the Cisco secure gateway, as follows:

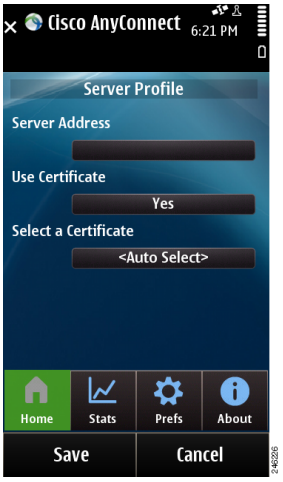
Step 1 Choose **Add VPN Connection** in the AnyConnect home screen (see Figure 1-5).

Figure 1-5 Home Screen with Add VPN Connection Option



Step 2 The Server Profile screen shows the VPN connection parameters for a single connection entry within the AnyConnect profile (see Figure 1-6).

Figure 1-6 Server Profile Screen



The Select a Certificate option is only available if you choose **Yes** to Use Certificate.

If you want to return to the AnyConnect home screen without saving changes, choose **Cancel**.

Step 3 Choose a parameter field to assign a value. Use the on-screen keyboard to enter a value.

Complete the fields as follows:

- **Server Address**—Enter the domain name, IP address, or Group URL of the Cisco Adaptive Security Appliance with which to connect. For example,

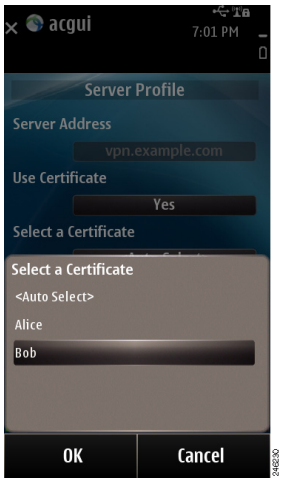
  ```
  vpn.example.com
  ```

  Note You cannot change the address once you have saved a connection.

- **Use Certificate**—(Optional, depending on VPN requirements.) Determines whether or not to use an end-point certificate for authentication. Your system administrator will provide you with instructions for installing a certificate if one is necessary to establish a VPN session. The absence of a certificate on the device prevents you from changing this setting. If a certificate is installed on the device, you can choose the following:
  - **Yes**—uses a certificate when connecting to a security appliance that requires a certificate. This option requires at least one client certificate to be installed. This option enhances network security access, is required for on-demand VPN, and is the default value.
  - **No**—uses another method to authenticate, such as logging in manually when establishing a VPN connection with a security appliance. When *No* is selected, certificates are not used even if they are valid against a given server.
- Select a Certificate—(Dimmed if Use Certificate is set to ***No***) Determines whether AnyConnect automatically chooses from the available certificates for authentication when connecting to the ASA (<Auto Select>) or chooses a certificate (see Figure 1-7).

  Note If you have multiple certificates installed on the phone and only one of them is valid against the given server, do not choose **<Auto Select>** because of the time required to scan through all certificates.

Figure 1-7 Choose a Certificate



Note Even if the certificate chosen is invalid for the server, AnyConnect will not try any other valid certificates. Choosing a certificate is more time efficient than auto-select if you know which certificate to use.

When you press **OK**, AnyConnect closes the Add VPN Connection screen and adds the entry to the home screen.

Setting Up On-Demand VPN

The Symbian On-Demand VPN feature enables an application to initiate a VPN connection when a VPN access point is chosen to open a network connection. The correct access point or destination must be chosen in the application configuration and then, outside of AnyConnect, it is determined whether the VPN is used. For example, if your official email client is configured to use the intranet destination, a connection is made automatically to the AnyConnect VPN when no other connection is available through the intranet destination. No special configuration (such as hostname or DNS) is required, but Cisco provides an implementation so that a connection is established either with or without being prompted for credentials, depending on the current default server.

AnyConnect supports different kinds of authentication, such as password-based or certificate-based. You are not required to have only certificate-based authentication during on-demand VPN.

Modifying a VPN Connection Entry

You might need to change a VPN connection entry to correct a configuration error or comply with an IT policy change. To do so:

Step 1 Open the AnyConnect home screen.

Step 2 Choose the VPN connection that you want to modify and click **Options > Edit**.

AnyConnect displays the Server Profile screen.

Step 3 Choose a parameter to change a value. You cannot modify the server name.

Step 4 Use the on-screen keyboard to enter the new value.

Note You cannot fully edit connections that have been imported from an AnyConnect VPN Profile.

For parameter instructions, see the "Adding a VPN Connection Entry" section on page 6.

Step 5 Choose **Save**.

AnyConnect closes the connection parameter screen.

Deleting a Connection Entry

To permanently delete a VPN connection entry you added manually:

Step 1 Open the AnyConnect home screen.

Step 2 Choose **Options**.

Step 3 Delete the user-added server from the list.

Step 4 Choose **OK** after the confirmation prompt.

AnyConnect closes the connection parameter screen and removes the entry from the AnyConnect screen.

Connecting to a VPN

To establish a VPN connection:

Step 1 Ensure you have a LAN connection or a connection to your service provider.

Step 2 Go to the AnyConnect home screen.

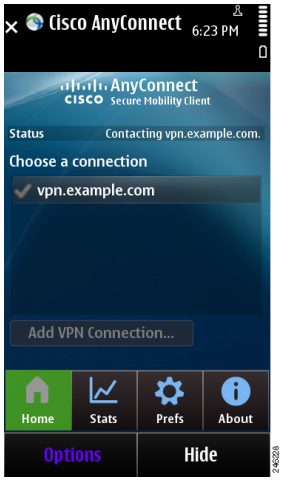
Step 3 Choose the desired connection entry listed under Choose a connection.

AnyConnect disconnects any VPN connection currently in place.

Step 4 If necessary, use the credentials supplied by your system administrator to log in.

The Status parameter reveals the new connection state (see Figure 1-8).

Figure 1-8 Status Showing Connection State



Depending on the secure gateway setup, AnyConnect retrieves connection entries and adds them to the VPN connection list in the AnyConnect home screen.

Step 5 If instructed by your system administrator to do so, choose **Select a Certificate.** This option allows you to choose a specific certificate for authentication when connecting to the ASA. When a specific certificate-based connection is specified, AnyConnect will not take the time to try all installed certificates.

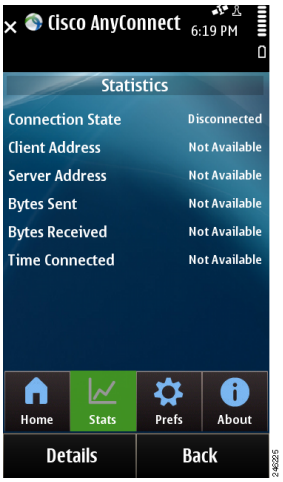
Viewing Overview Statistics

AnyConnect records statistics when a VPN connection is present and a Statistics screen is opened.

To view the overview statistics for the current VPN connection, go to the AnyConnect home screen and choose **Stats**.

The Statistics screen opens (see Figure 1-9).

Figure 1-9 Statistics



The Statistics screen displays the following:

- Connection state
- Client address
- Server address
- Bytes sent
- Bytes received
- Time connected

- **Details**—Choose to view detailed statistics (described in the next section).
- **Back**—Returns to the previous screen.

Viewing Detailed Statistics

To view the detailed statistics for the current VPN connection:

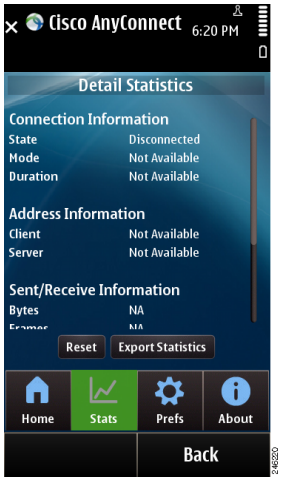
Step 1 Go to the AnyConnect Home screen.

Step 2 Choose **Stats**.

Step 3 Choose **Details**.

The Detail Statistics screen opens (see Figure 1-10).

Figure 1-10 Detail Statistics Screen



Step 4 Scroll the screen to view all of the statistics. You can reset the statistics for a renewed view or choose to export statistics for diagnostic purposes.

The Detailed Statistics screen shows the following:

- Connection information
  - State
  - Mode
  - Duration
- Address Information
  - Client
  - Server

- Bytes sent and received
- Frames sent and received
- Control frames sent and received
- Transport Information
  - Protocol
  - Cipher
  - Compression

Viewing and Managing Log Messages

AnyConnect writes its own log file and places it in the install drive (C:\Data\AnyConnect\Logs). The file is named AnyConnectLog.txt and is set by default to log only errors and warnings; however, you can change the log level in user preferences. The logger has the following capabilities:

- Supports multi-process logging into the same file
- Performs log rotation when the log file reaches a pre-configured size (LogMaxSize)
- Deletes old log files when there are more than the maximum allowed (LogMaxFiles)

For diagnostic purposes, you may be asked to email the log messages. For this purpose, store all log files in c:\data\anyconnect\logs\folder.

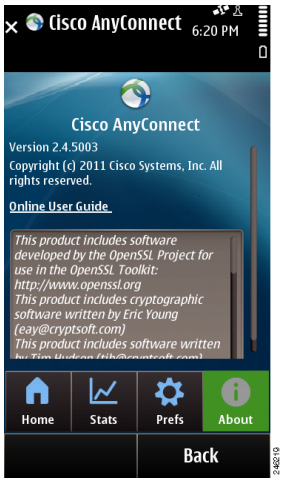
An example of the type of log returned is shown below:

```
AnyConnect displays the most recent log messages (such as [2010-07-19 18:43:21:270 +05.30
INFO (vpnagent)] VPN tunnel established with gateway anycon-bgl-asa.mycompany.com
```

Displaying the AnyConnect Version and Licensing Details

To display the AnyConnect version and licensing details, choose the **About** tab (see Figure 1-11).

Figure 1-11 About Screen



If you click **Online User Guide**, you can access the location of this user guide on Cisco.com.

Troubleshooting

This section describes solutions to common problems related to AnyConnect for Symbian. If problems still persist after trying these solutions, contact your organization's IT support department.

- **I cannot edit/delete some profiles.**

  Your system administrator sets a policy that affects host entries imported into your AnyConnect profile.

- **Connection time-outs and unresolved hosts.**

  Internet connectivity issues, a low cell signal level, or a congested network resource can often cause time-outs and unresolved host errors. If a LAN is within reach, try using your device Settings app to establish a connection with the LAN first. Retrying multiple times in response to time-outs often results in success.

- **VPN client driver encountered an error**

  After the session initiation starts, the connection times out if the session is not established within the stipulated timeframe (currently defaulted to five minutes). If a timeout occurs and this error appears, invoke a retry.

- **Certificate-based authentication does not work.**

  Check the validity and expiration of the certificate if you succeeded with it before. Check with your system administrator to make sure you are using the appropriate certificate for the connection.

- **AnyConnect failed to establish a connection but no error message was displayed.**

  Messages can be displayed only when the AnyConnect application is open.

- **A profile called Cisco AnyConnect exists that cannot be deleted.**

  Try restarting the application.

- **When I remove the AnyConnect application, VPN configurations still appear in the Symbian network settings.**

  Manually delete the VPN configuration or (Internet Access Point (IAP) from the intranet destination using **Menu > Settings > Connectivity > Settings > Destinations > Intranet**.

- **AnyConnect VPN Connection does not migrate to the new Internet WiFi network.**

  To conserve battery life, Symbian does not do real-time scanning for wireless access points. WiFi scanning might be delayed as much as 10 minutes (default). The timeout is configurable in the WiFi settings on the phone. Based on this timeout value, it might take time for AnyConnect to discover a new WiFi network and migrate to it, even if the phone is in the range of a known high-priority WiFi access point.

Removing AnyConnect

To remove AnyConnect from the device, follow these steps:

Step 1 Using the Application Manager (such as **Menu > Settings > Application Manager > installed apps**), find the AnyConnect listing.

Step 2 Click on AnyConnect from the list and hold it for some time. A menu appears.

Step 3 Choose **Uninstall** from the menu.

Step 4 Accept the confirmation dialog to remove AnyConnect from the device.

Open Software License Notices

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).