iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4.4

Updated: January 07, 2011

Contents

This document describes the Cisco AnyConnect Secure Mobility Client 2.4.4 for Apple iOS. 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 Apple iOS 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 App Store provides installation app and all updates. The Cisco Adaptive Security Appliance (ASA) is the secure gateway that admits access to the VPN, but it does not support updates of AnyConnect for Apple iOS.

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

Devices Supported by Cisco AnyConnect 2.4.4

This release supports the following Apple devices:

Device	Apple iOS Release Required
iPad	4.2
iPhone 3G	4.1 or 4.2
iPhone 3GS	4.1 or 4.2
iPhone 4	4.1 or 4.2
iPod Touch (2nd Generation or later)	4.1 or 4.2

New Features and Fixes Since AnyConnect 2.4.2

This release features the following enhancements and fixes:

- iPad support (Apple iOS 4.2 required).
- Apple iOS 4.2 as well as 4.1 support for the iPhone.
- Clear Profile Data—Lets you remove the hosts and policy settings that make up the AnyConnect profile imported from an ASA. To access, tap **Diagnostics**. If you reconnect to the domain, IP address, or Group URL of the same ASA, it reloads the profile and re-enforces the security policies.
- Application URI Handling—Lets other applications add VPN connection entries to the AnyConnect configuration, establish VPN connections, and disconnect from a VPN. Your system administrator has the option to provide you with access to this feature.
- Certificate Deletion— Let you use AnyConnect to delete any certificate imported via AnyConnect SCEP. To do so, swipe right on the Select Certificate window, the tap **Delete**. You cannot use AnyConnect to delete certificates that were imported via IPCU or any source outside the AnyConnect application.

- Cisco Profile Deletion—You can use AnyConnect to delete the locally hosted Cisco profile. This feature allows the clean removal of imported hosts and policy settings imported from the ASA. If you reconnect to the domain name, IP address, or Group URL of the same ASA, it reloads the profile and re-enforces the security policies.
- Expanded Diagnostics and Logging—Enhanced the tools in the Diagnostics window formerly named “Troubleshooting.” These enhancements include:
  - Improvements to the usability of the log message view.
  - Removal of unnecessary log messages.
  - Separation of Application and Service level logs.
  - Device information added to the new email message that AnyConnect opens when you tap E-mail Logs.
  - Improved severity levels of log messages.
- Improved error reporting when connecting to HTTPS servers that are not secure gateways.
- Link in the About window that opens an updated iPhone or iPad user guide, depending on the device.
- Fixed crash when toggling Wi-Fi on or off.
- Fixes to certain situations where the tunnel would be disconnected when in a reconnecting state.
- Support for IPv6 resources accessed over the VPN connection.
- Bandwidth graphs for the iPad.
- High contrast theme alternative to the Cisco default theme. Access the Apple Settings and tap AnyConnect, then tap the theme you want.

What You Need Before You Can Set Up AnyConnect

You must obtain one or more of the following from your system administrator, depending on your network requirements, before you can set up AnyConnect to establish a 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 need to access the VPN.

Alternatively, your system administrator may supply a link on your corporate network that you can tap to add the required connection entries to your iPad.

The Apple iOS Connect On Demand feature, if used, supports the automation of a VPN connection as needed by the applications on your device. However, you must install a digital certificate on the device first. The certificate must be one that the secure gateway accepts. Your system administrator determines which certificate the secure gateway accepts for its respective group URLs.

You can use the following methods to install one or more certificates:

- Use an Apple iOS device configuration profile (installed via the iPhone Configuration Utility).
- Follow instructions provided by your system administrator to use AnyConnect to import a certificate.

You must specify which certificate you want to use for each VPN connection entry for which you will use a certificate. If you are not using any other form of authentication, it is best to use a Group URL supplied by your system administrator.

Installation

You can install the Cisco AnyConnect Secure Mobility client for Apple iOS from the Apple App Store, as follows:

Step 1 Open the App Store.

Step 2 Select **Search**.

Step 3 In the Search Box, enter `anyconnect` and tap **cisco anyconnect** in the Suggestions list.

Step 4 Tap **AnyConnect**.

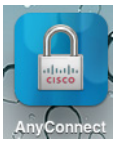
Step 5 Tap **Free**, then INSTALL APP.

Step 6 Select **Install**.

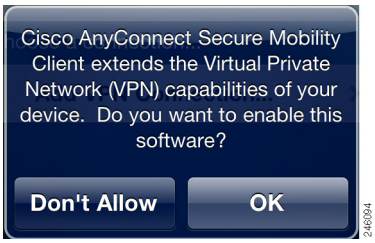
Getting Started

To get started,

Step 1 Swipe to the right of the iPad home window, then tap the Cisco AnyConnect icon.

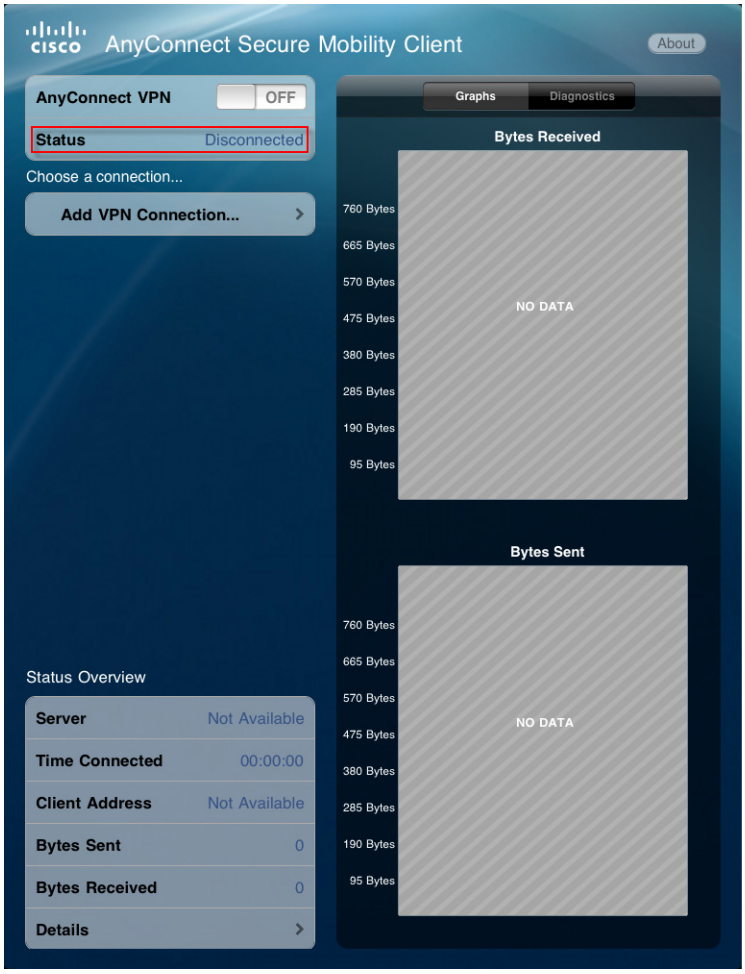


A confirmation window opens the first time you start AnyConnect on the device.



Step 2 Tap **OK**.

AnyConnect shows the VPN connection status in the AnyConnect home window.



Before establishing your first VPN connection, follow the instructions below to add a VPN connection entry.

Adding a VPN Connection Entry

These instructions may be unnecessary if your system administrator supplied you with a webpage link to tap to add connection entries to the AnyConnect configuration.

Before attempting to establish a VPN connection, add a VPN connection entry to identify the Cisco secure gateway, as follows:

Step 1 Tap **Add VPN Connection** in the AnyConnect home window.

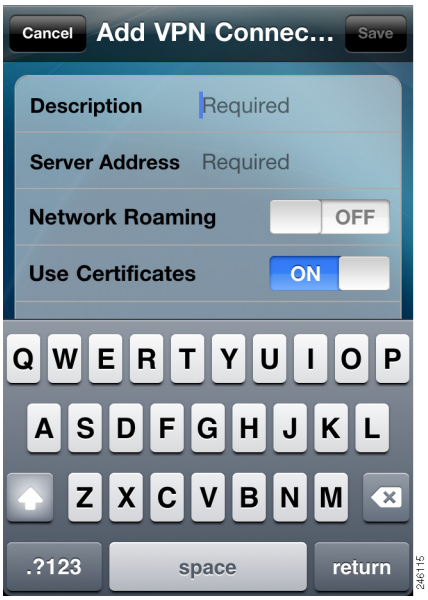
The Add VPN Connection window shows the VPN connection parameters.

The Selected Certificate and Connect on Demand options appear only if you tap **ON** next to Use Certificates.

AnyConnect dims the Save button until you complete all the required fields.

If you want to return to the AnyConnect home window without saving changes, tap **Cancel**.

Step 2 Tap a parameter field to assign a value.



Use the on-screen keyboard to enter a value.

Step 3 Complete the fields, as follows:

Description—Enter a unique name for the connection entry to appear in the connection list of the AnyConnect home window. We recommend using a maximum of 24 characters to ensure they fit in the connection list. You can use any letters, spaces, numbers, or symbols on the keyboard. AnyConnect retains the letters in the upper- or lower-case letters you specify. For example,

```
Example 1
```

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
```

Network Roaming—(Optional) Determines whether to limit the time it takes to reconnect after the device wakes up or after a change to the connection type (e.g., EDGE, 3G, Wi-Fi).

Note This parameter does *not* affect data roaming or the use of multiple mobile service providers.

Tap this switch, as follows:

- ON—(Default) This option optimizes VPN access. If AnyConnect loses a connection, it tries to establish a new one until it succeeds. This setting lets applications rely on a sustained connection to the VPN. AnyConnect does not impose a limit on the time it takes to reconnect.
- OFF—This option optimizes battery life. If AnyConnect loses a connection, it tries to establish a new one for 20 seconds and then stops trying. You must then start a new VPN connection if one is necessary.

Use Certificates—(Optional, depending on VPN requirements.) Your system administrator will provide you with instructions for installing a certificate if one is necessary to establish a VPN session. AnyConnect detects the installation of one or more certificates on the device. The absence of a certificate on the device prevents you from changing this setting. If a certificate is installed on the device, you can tap this switch as follows:

- ON—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, and is required for Connect on Demand.
- OFF—uses another method to authenticate, such as logging in manually when establishing a VPN connection with a security appliance.

Selected Certificate—(Displayed only if Use Certificates is set to ON.) Tap to choose the certificate to be used for authentication when connecting to the ASA. The Select Certificate windows shows the Certificate Name, Issuer, and Expiration Date of each certificate installed on the device.

Step 4 (Optional) Tap the certificate required for access to the VPN. AnyConnect reads the values embedded in the certificate and displays them in the Select Certificate Details window. Tap **Select Certificate** at the top of this window.

Step 5 (Optional) Complete the remaining parameters, as follows:

Connect on Demand—(Displayed only if Use Certificates is set to ON.) Tap this switch, as follows:

- ON—Lets applications start a VPN connection when they attempt to access a domain specified in the domain list below. This option requires a certificate.
- OFF—Prevents applications from starting a VPN connection. Using this option is the only way to prevent an application that makes a DNS request from potentially triggering a VPN connection.

Domain List—(Displayed only if Connect on Demand is set to ON.) Lists the domains for which Connect on Demand match rules apply. For instructions, see the next section.

Step 6 (Optional) Tap **Save** to retain the connection values.

AnyConnect closes the Add VPN Connection window and adds the entry to the home window.

Setting Up Connect-On-Demand Rules

The Apple iOS Connect On Demand feature lets an application such as Safari initiate a VPN connection. AnyConnect evaluates the domain requested by an application against the strings in the domain lists within the *active* connection entry—the entry with the check mark next to it.

- **Never Connect**—AnyConnect evaluates domain requests for a match against the contents of this list first. If a string in this list matches the domain, Apple iOS ignores the domain request. This list lets you exclude certain resources. For example, you might not want an automatic VPN connection over a public facing Web server. An example value is `www.example.com`.

Note If you or the user enable Connect On Demand, AnyConnect adds the server address in the VPN configuration to the Never Connect list to prevent VPN connections from starting when you use a web browser to connect to a secure gateway. Leaving the rule in place does not have an adverse effect on Connect on Demand.

- **Always Connect**—AnyConnect evaluates domain requests for a match against the contents of this list next. If a string in this list matches the domain, Apple iOS attempts to establish a VPN connection. The most common use case for this list is to obtain brief access to internal resources. An example value list is `email.example.com`.
- **Connect if Needed**—AnyConnect evaluates a domain request for a match against this list if a DNS error occurred. If a string in this list matches the domain, Apple iOS attempts to establish a VPN connection. The most common use case for this list is to obtain brief access to an internal resource that is not accessible in a LAN within the corporate network. An example value is `intranet.example.com`.

Apple IOS establishes a VPN connection on behalf of an application only if all of the following are true:

- A VPN connection is not already established.
- An application compatible with the Apple iOS Connect on Demand framework requests a domain.
- The connection entry is configured to use a valid certificate.
- Connect on Demand is enabled in the connection entry.
- AnyConnect fails to match a string in the *Never Connect* list to the domain request.
- *Either* of the following is true:
  - AnyConnect matches a string in the *Always Connect* list to the domain request.
  - A DNS lookup failed and AnyConnect matches a string in the *Connect if Needed* list to the domain request.

The domain lists specify the Connect on-Demand rules. These rules support only domain names, not IP addresses. The domain names specified within the rules may be partial or whole domain strings. Use a comma to separate list entries. AnyConnect is flexible about the domain name format of each list entry, as follows:

Match	Instruction	Example Entry	Example Matches	Example Match Failures
Exact prefix and domain name only.	Enter the prefix, dot, and domain name.	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org

Match	Instruction	Example Entry	Example Matches	Example Match Failures
Any prefix with the exact domain name. The leading dot prevents connections to hosts ending with *example.com, such as notexample.com.	Enter a dot followed by the domain name to be matched.	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
Any domain name ending with the text you specify.	Enter the end of the domain name to be matched.	example.net	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

AnyConnect does not limit the maximum number of domains in a list.

To open a VPN connection when an application requests access to one or more specific domains:

Step 1 Open the AnyConnect home window.

Step 2 Tap the icon to the right of the connection entry or tap **Add VPN Connection**.

Step 3 Enter a name for the VPN connection into the Description field.

Step 4 Enter the domain name, IP address, or Group URL of the Cisco Adaptive Security Appliance provided by your system administrator.

Step 5 Tap **ON** next to Use Certificates.

Step 6 Select the certificate required for the connection as provided by your system administrator and tap **Add VPN Connect**.

AnyConnect returns to the Add VPN Connection window.

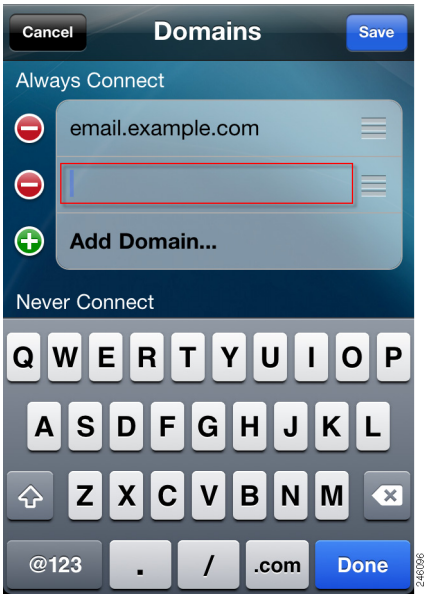
Step 7 Tap **ON** next to Connect On Demand.

Step 8 Tap **Domain List**.

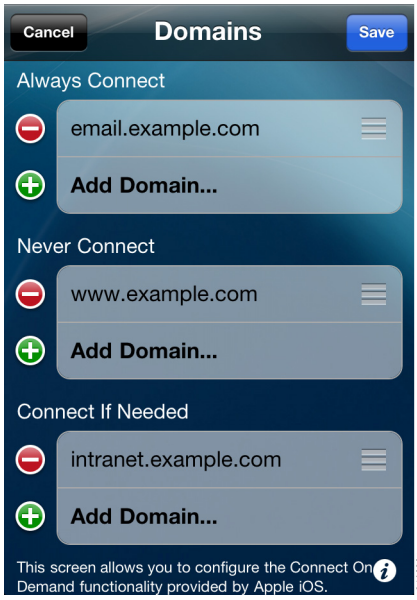
The Domains window shows the domain lists.

Step 9 Do either of the following:

- Tap **Add Domain** to add a domain string to the list shown. The Domains window adds a row to the list and displays an on-screen keyboard for you to enter the domain string.



- Tap **Edit** at the top of the window to add, edit, or delete domain strings.



This window lets you:

- Add a domain name to a list. To do so, tap **Add Domain**. AnyConnect adds a blank row to the list and displays an on-screen keyboard for you to add the list entry.
- Move a domain name from one list to another. To do so, touch the triple-bar to the right of the domain entry and drag it to the area below the title of the destination list.
- Delete—Tap the red circle to the left of the domain name, then tap **Delete** to the right of the domain.

Tap **Save**.

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 window.

Step 2 Tap the icon to the right of the VPN connection entry.

AnyConnect displays the VPN connection parameters.

Step 3 Tap a parameter to change a value.

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 or the iPhone Configuration Utility mobileconfig.

For parameter instructions, use the online help or go to Adding a VPN Connection Entry.

Step 5 Tap **Save**.

AnyConnect closes the connection parameter window.

Deleting a Connection Entry

AnyConnect provides two procedures for deleting a connection entry, depending on whether you added it or the secure gateway added it.

Deleting a Connection Entry You Added

To permanently delete a VPN connection entry you added manually:

Step 1 Open the AnyConnect home window.

Step 2 Tap the icon to the right of the connection entry to be deleted.

Step 3 Tap **Delete VPN Connection**.

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

AnyConnect closes the connection parameter window and removes the entry from the AnyConnect home window.

Deleting a Connection Entry that Was Added Automatically

To permanently delete all VPN connection entries added by a secure gateway, remove the AnyConnect profile:

Step 1 Open the AnyConnect home window.

Step 2 Tap **Diagnostics**.

Step 3 Tap **Clear Profile Data**.

Note If you reconnect to the domain, IP address, or Group URL of the same ASA, it reloads the profile and re-enforces the security policies.

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 window.

Step 3 Tap the connection entry to be used.

AnyConnect repositions the check mark next to the connection entry and disconnects any VPN connection currently in place.

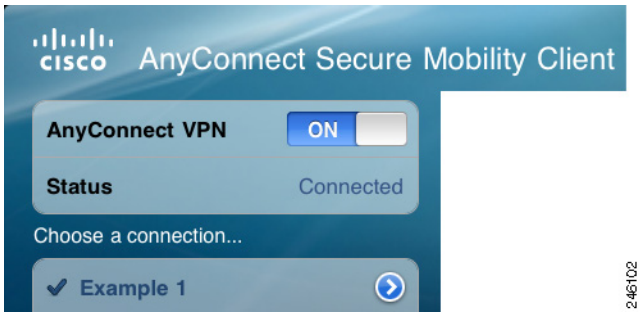
Step 4 Tap **ON** next to AnyConnect VPN.

Step 5 If necessary, use the credentials supplied by your system administrator to log in.

Step 6 If instructed by your system administrator to do so, tap **Get Certificate**.

Step 7 If necessary, tap **Connect**.

The Status parameter reveals the new connection state.



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

Displaying Online Help

AnyConnect displays an information icon (***i***) on the lower right corner of the window if online help is available.

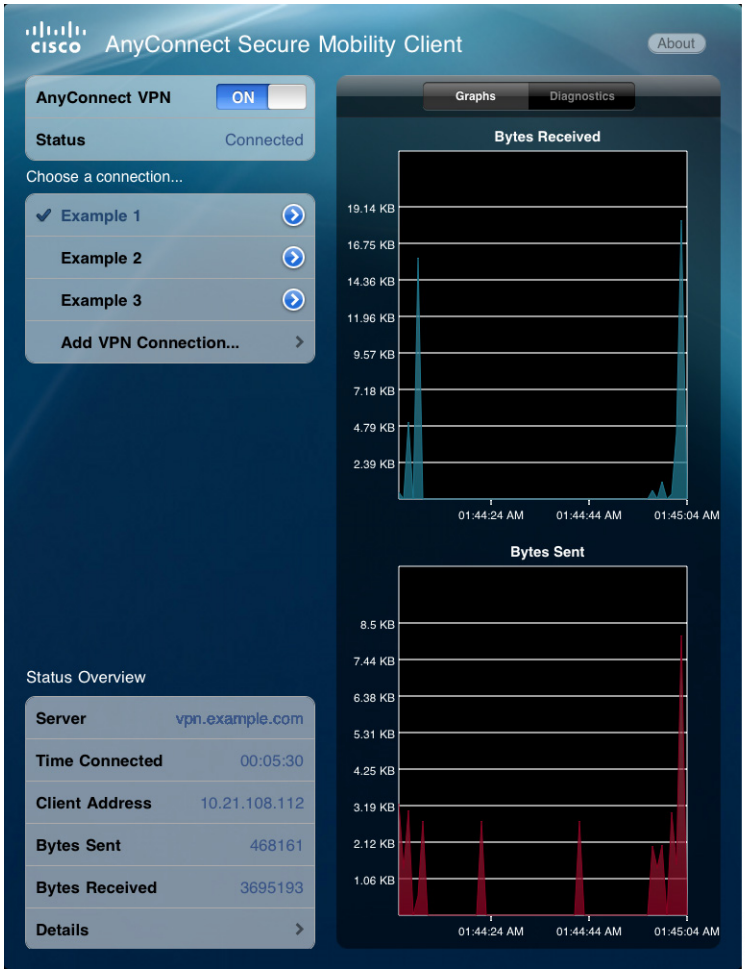
Tap this icon to display the help.

Alternatively, you can tap **About** in the upper right corner of the AnyConnect home window to display a link that provides access to this guide.

Viewing Overview Statistics

AnyConnect records statistics when a VPN connection is present and you have opened the Statistics window.

To view the overview statistics for the current VPN connection, open the AnyConnect home window.



AnyConnect displays the statistics for the current VPN connection in the Status Overview panel on the lower left.

AnyConnect displays “No Data” in the boxes on the right, then begins replacing them with live, graphical representations of the bytes received and bytes sent.

The Status Overview panel shows the following statistics:

- Status (of the connection).
- Server (address).
- Time Connected.
- Client Address.
- Bytes Sent.
- Bytes Received.

- **Details**—Tap to view detailed statistics (described in the next section).

Viewing Detailed Statistics

To view the detailed statistics for the current VPN connection:

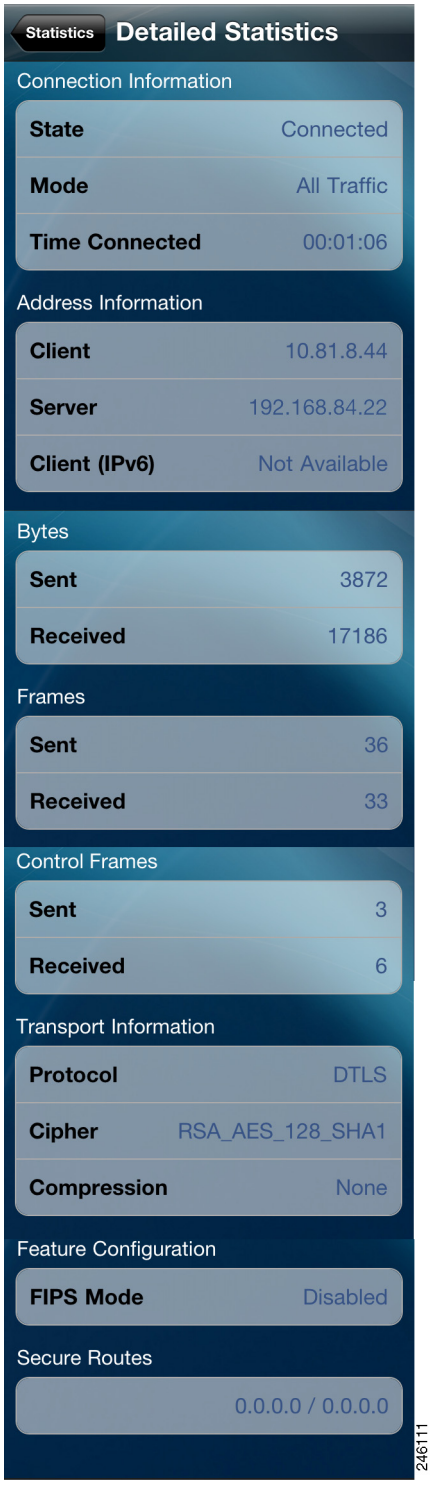
Step 1 Go to the AnyConnect Home window.

Step 2 Tap **Details** in the Status Overview panel.

AnyConnect displays the detailed statistics on the right side of the home window.

Step 3 Scroll the window to view all of the statistics.

The following illustration combines them into a single image:



The Detailed Statistics window shows the following:

- Connection Information
  - State
  - Mode

  - Time Connected
- Address Information
  - Client
  - Server
  - Client (IPv6)
- Bytes
  - Sent
  - Received
- Frames
  - Sent
  - Received
- Control Frames
  - Sent
  - Received
- Transport Information
  - Protocol
  - Cipher
  - Compression
- Feature Configuration: FIPS Mode
- Secure Routes—An entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all VPN traffic is encrypted and sent or received over the VPN connection.

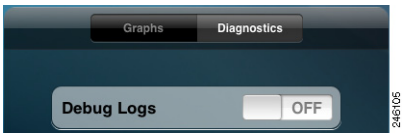
To hide the detailed statistics, tap any field in the Statistics Overview frame.

Viewing and Managing Log Messages

To prevent an unnecessary load on device resources, AnyConnect does not log messages by default. Enable logging for troubleshooting only.

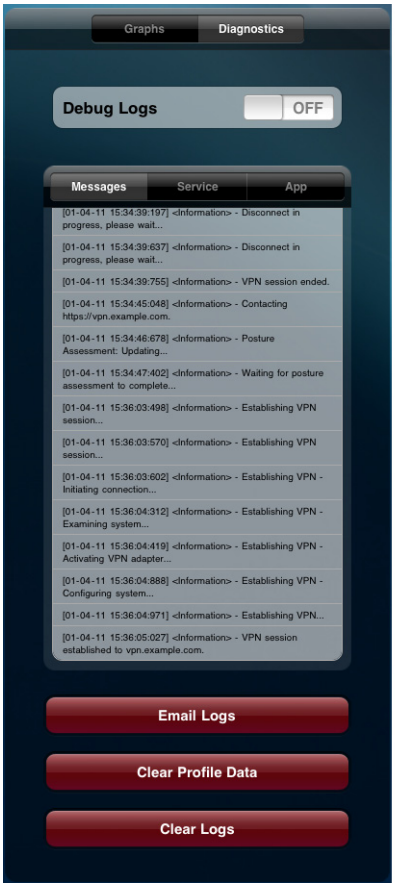
To enable, view, and manage log messages:

Step 1 Go to the AnyConnect home window and tap **Diagnostics** near the top right.



Step 2 Tap **ON** next to Debug Logs to enable logging.

AnyConnect displays the most recent log messages.



Scroll the window to view additional messages.

The buttons and functions in this window are:

- **Messages**—Tap to display the log messages.
- **Service**—Tap to display the service debug log messages.
- **App**—Tap to display the application debug log messages.
- **Email Logs**—Tap to send the log messages to an email address. The email application creates an email message containing the current logs.
- **Delete Profiles**—Tap to remove profiles retrieved from a Cisco Adaptive Security Appliance.
- **Clear Logs**—Tap to remove the log messages.

Changing the Theme

AnyConnect now features two themes:

- Cisco Default Theme—Color contrast, emphasizing shades of blue, similar to the Apple iOS interface.
- High Contrast—alternative to the Cisco default theme. This theme emphasizes black and white, although it does use some color. It might be preferable for visually impaired users or for viewing in bright light.

To change the theme of the AnyConnect user interface,

Step 1 Use the device menu button to return to the iPad home window.

Step 2 Tap **Settings**.

Step 3 Find the Apps list, then tap **AnyConnect**.

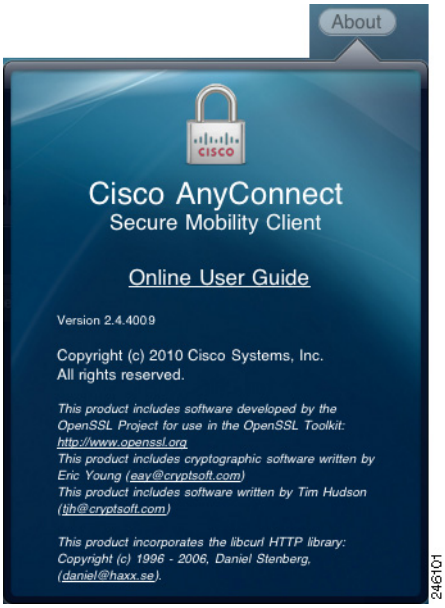
Step 4 Tap **Selected**.

Step 5 Tap the theme you want: **Cisco Default Theme** or **High Contrast**.

Apple iOS inserts a check mark next to the theme you selected.

Displaying the AnyConnect Version and Licensing Details

To display the AnyConnect version and licensing details, tap **About** at the top right of the home window.



Tip Tap the link to use Safari to open the latest updated version of this guide. Use it as a resource if you need to use these instructions at a later time.

Responding to "Another Application has requested that AnyConnect...Do you want to allow this?"

To protect your device, AnyConnect informs you when another application attempts to generate a connection profile, establish a VPN connection, or disconnect from a VPN, and prompts you whether it is OK. For example,

The Connect on Demand feature permits these features; however, to protect your device and data, please ask your system administrator whether to tap **OK** to approve of these types of prompts:

- Create—"Another application has requested that AnyConnect create a new connection to '*host*'. Do you want to allow this?"
- Connect—"Another application has requested that AnyConnect connect to '*host*'. Do you want to allow this?"
- Connect—"Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this?"

Troubleshooting

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

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

  Your system administrator set a policy that affects host entries imported into your AnyConnect profile. To delete these profiles, tap **Diagnostics** and tap **Clear Profile Data**.

- **Errors while trying to save or edit configuration.**

  A known issue with the operating system is the cause. Apple is working to resolve it. As a workaround, try restarting the application.

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

  Internet connectivity issues, a low cell signal level, or congested network resource 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 connection is not re-established when the device wakes from sleep.**

  Enable Network Roaming in the VPN connection entry. If enabling network roaming does not resolve the issue, check your EDGE, 3G, or Wi-Fi connection.

  Note This issue could be expected behavior depending on how your organization has configured the VPN.

- **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.

- **The Apple iOS Connect On Demand feature is not working or connecting unexpectedly.**

  Ensure the connection does not have a conflicting rule in the Never Connect list. If a Connect If Needed rule exists for the connection, try replacing it with an Always Connect rule.

- **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 Apple iOS VPN settings.**

  To delete these profiles, reinstall AnyConnect, tap **Diagnostics**, and tap **Clear Profile Data**.

Removing AnyConnect

To remove AnyConnect from the device,

Step 1 Open AnyConnect, tap **Diagnostics**, and tap **Clear Profile Data** to remove it from the Apple iOS VPN settings.

Step 2 Press the menu button to go to the iPad home window.

Step 3 If you placed AnyConnect in a folder, open the folder.

Step 4 Tap and hold the AnyConnect icon until a delete (**X**) icon appears above it.

Step 5 Tap the delete icon.

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).
