iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x

Updated: December 13, 2013

This document describes the Cisco AnyConnect Secure Mobility Client 3.0.x 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 the installation application 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.

Apple iOS Devices Supported

(with Retina

Device	Apple iOS Release Required
iPad Air	7.0 or later
iPad 2	6.0 or later
iPad (3rd generation)	6.0 or later
iPad (4th generation)	6.0 or later
iPad mini	6.0 or later
iPad mini (with Retina display)	7.0 or later
iPhone 3GS	6.0 or later
iPhone 4	6.0 or later
iPhone 4S	6.0 or later
iPhone 5	6.0 or later
iPhone 5C	7.0 or later
iPhone 5S	7.0 or later
iPod Touch (4th generation)	6.0 or later
iPod Touch (5th generation)	6.0 or later

Note AnyConnect on the iPod Touch appears and operates as on the iPhone. Use the *iPhone User Guide for Cisco AnyConnect Secure Mobility Client* for this device.

Installing or Upgrading AnyConnect

Installing AnyConnect

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**.

Upgrading AnyConnect

Upgrades to AnyConnect 3.0 are managed through the Apple App Store. After the Apple App Store notifies users that the AnyConnect upgrade is available, follow this procedure.

You must do the following before upgrading your device:

- Disconnect an AnyConnect VPN session if one is established. If you fail to do this, AnyConnect requires a reboot of your device before using the new version of AnyConnect.
- Close the AnyConnect application if it is open.

Note If the Apple iOS Connect On Demand feature is used on your device to make VPN connections automatically, you must launch the AnyConnect app and establish a VPN connection immediately after upgrade. If this is not done, upon the next iOS system attempt to establish a VPN tunnel, the error message “The VPN Connection requires an application to start up” will display.

Step 1 Tap the **App Store** icon on the iOS home page.

Step 2 Tap the **AnyConnect upgrade notice**.

Step 3 Read about the new features.

Step 4 Click **Update**.

Step 5 Enter your **Apple ID Password**.

Step 6 Tap **OK**.

The AnyConnect upgrade proceeds.

Device Localization

The following language translations are included in the AnyConnect package:

- Czech (cs-cz)
- German (de-de)
- Latin American Spanish (es-co)
- Canadian French (fr-ca)
- Japanese (ja-jp)
- Korean (ko-kr)
- Polish (pl-pl)
- Simplified Chinese (zh-cn)

Localization data for these languages is installed on the Android device when AnyConnect is installed. The displayed language is determined by the locale specified in **Settings > General > International > Language**. AnyConnect uses the language specification, then the region specification, to determine the best match. For example, after installation, a French-Switzerland (fr-ch) locale setting results in a French-Canadian (fr-ca) display. AnyConnect UIs and messages are translated as soon as AnyConnect starts. The selected localization is noted as `Active` in the AnyConnect **Localization Management** screen.

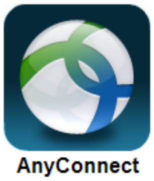
See Managing Localization for localization activity and options post-installation.

Getting Started with AnyConnect

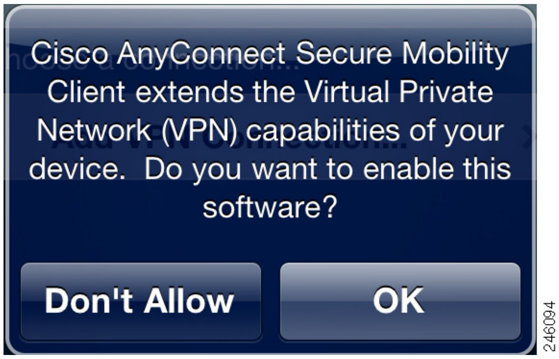
Client User Interface

If you tap the AnyConnect icon on the iPhone or iPad home screen, the AnyConnect home screen opens:

Step 1 Tap the Cisco AnyConnect Secure Mobility Client icon.



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



Cisco AnyConnect Secure Mobility Client extends the Virtual Private Network (VPN) capabilities of your device. Do you want to enable this software?

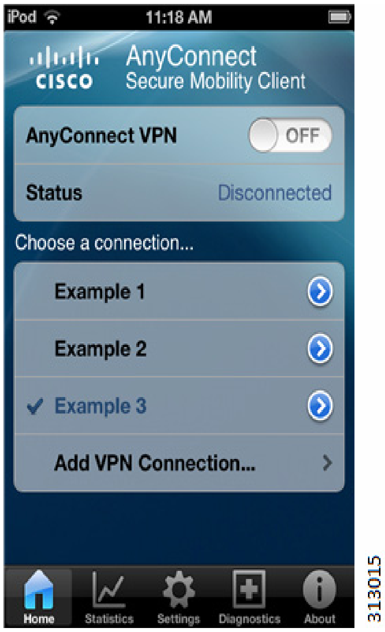
Step 2 Tap **OK**.

AnyConnect shows the VPN connection status in the AnyConnect home screen. Figure 1 shows the AnyConnect home screen for the iPhone. Figure 2 shows the AnyConnect home screen for the iPad.

The AnyConnect home screen lists the names of the VPN connection entries stored on the device, and lets you add new VPN connection entries. The slider switch near the top lets you establish a VPN connection using the connection entry indicated by the check mark. The Status parameter shows the state of the VPN connection.

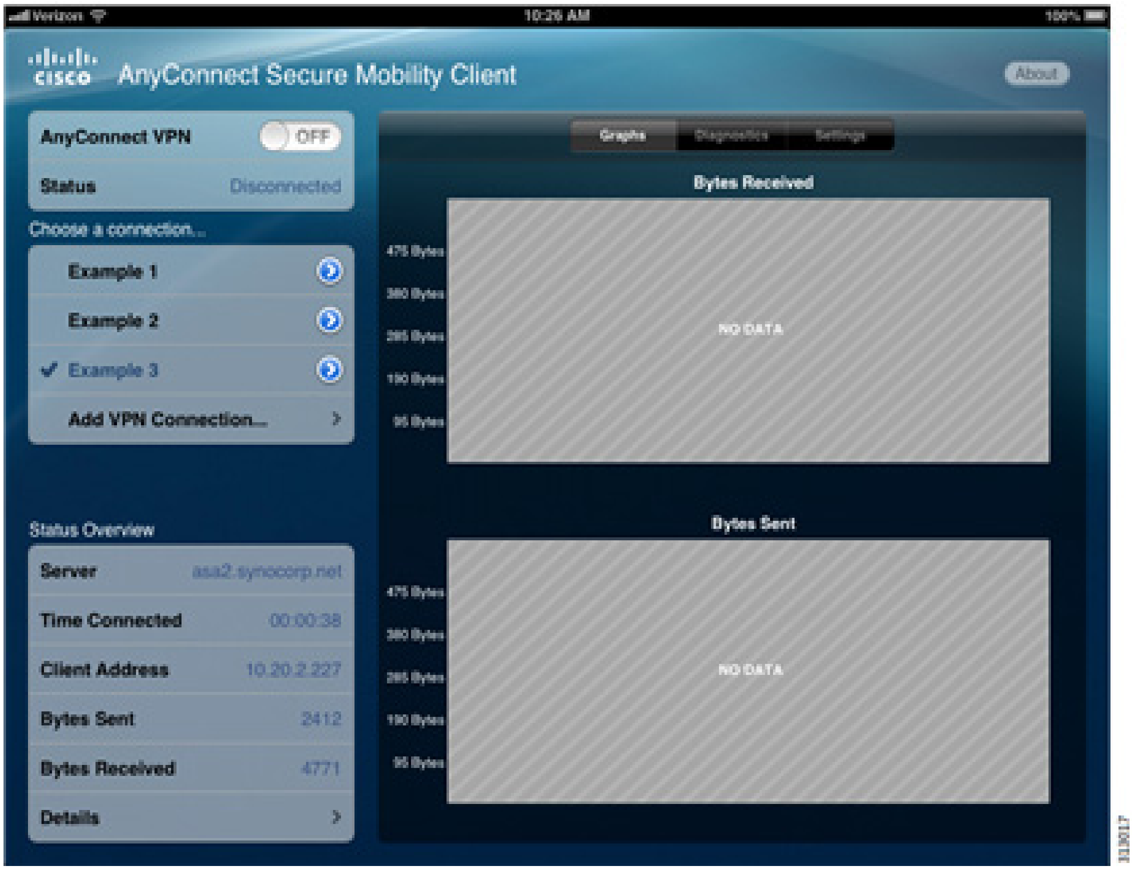
The tab bar at the bottom of each iPhone display provides navigation icons for the Home, Statistics, Diagnostics, and About windows. The iPad AnyConnect home screen integrates these functions.

Figure 1 iPhone AnyConnect home screen



Status Disconnected

Figure 2 iPad AnyConnect home screen



Status Disconnected

Server asa2.synocorp.net

Time Connected 00:00:38

Client Address 10.20.2.227

Bytes Sent 2412

Bytes Received 4771

Table 1 shows the differences between AnyConnect for the iPhone and the iPad.

Table 1 Differences between the iPhone and iPad AnyConnect UI

Feature	iPhone	iPad
Home—Opens when you tap the AnyConnect icon.	Displays VPN Connection controls. Also accessed by tapping the **Home** icon at the bottom of the AnyConnect screen.	VPN Connection controls are in the upper left of the AnyConnect home screen. This screen remains on-display.
Statistics—Connection Status Overview	Tap the **Statistics** icon at the bottomon the bottom ofthe screen in the iPhone AnyConnect app.	Status Overview panel in the lower left of the AnyConnect home screen.
Statistics > Details	Tap **Details** in the Statistics screen.	Tap **Details** in the Status Overview panel on the AnyConnect home screen.
Settings	Tap the **Settings** icon at the bottom of the screen in the iPhone AnyConnect app.	Tap **Settings** in the Status Overview panel on the AnyConnect home screen.
Diagnostics	Tap the Diagnostics icon in the tab bar to view or delete certificates, profiles or localization data stored on your device, turn on debug logging, and view and manage AnyConnect logs.	Tap the Diagnostics button on the AnyConnect home page to view or delete certificates, profiles or localization data stored on your device, turn on debug logging, and view and manage AnyConnect logs.
About—Displays the AnyConnect version and licensing details, and link to the user guide.	Tap the **About** icon at the bottom of the AnyConnect screen.	Tap **About** at the top right of the AnyConnect home screen.
Bandwidth graphs (bytes received and bytes sent).	Tap **Statistics > Graphs** to see a graphical representation of bytes received and bytes sent.	Tap **Graphs** near the top right of the AnyConnect home screen.

Step 3 Before establishing your first VPN connection, you must add a VPN Connection Entry to select. Example 1, Example 2, and so on in the figures above are configured connection entries. Follow the instructions provided by your administrator to configure a connection entry. They may involve the following activities:

a. Obtaining What You Need Before You Set Up AnyConnect.

b. Using one of the methods for Adding a VPN Connection Entry.

c. Using one of the methods for Installing a Certificate on Your Mobile Device.

d. And finally Establishing a VPN connection.

Displaying Help

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

i

Tap this icon to display help information about the current options.

Alternatively, tap **About** to display a link that provides access to this guide if you need to use it at a later time.

What You Need Before You Set Up AnyConnect

You must obtain one or more of the following from your system administrator, depending on your network requirements, before you 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 needed to access the VPN.

Alternatively, your system administrator may supply a link on your corporate network that you 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.

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.
- See Installing a Certificate on Your Mobile Device, page 12 for instructions on how to install 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.

Connecting to a VPN

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 screen. The Add VPN Connection screen shows the initial VPN connection parameters. Tap **Cancel** to cancel the configuration process at any time or tap **Save** to save the connection entry.

Step 2 (Optional) Tap **Description** to enter a unique name for the connection entry.

This name appears in the connection list of the AnyConnect home screen. We recommend using a maximum of 24 characters to ensure they fit in the connection list. Use 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
```

Step 3 Tap **Server Address** to enter the domain name, IP address, or Group URL of the Cisco Adaptive Security Appliance with which to connect. For example,

```
vpn.example.com
```

Step 4 Tap **Advanced** to open the advanced VPN connection parameters.

Tap **Add VPN Connection** at any time in this window to return to the initial configuration window to cancel or save the connection entry.

Step 5 (Optional) Configure **Network Roaming** for this connection.

Network Roaming determines whether to limit the time it takes to reconnect after the device wakes up or after a change to the connection type (such as EDGE(2G), 1xRTT(2G), 3G, or 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.

Step 6 (Optional) Configure certificate use for this connection.

a. Tap **Certificate** to show the **Select Certificate** screen.

b. Tap one of the following choices:

  - **Disabled**–(Default) A client certificate is never used for authentication.

- **Automatic**–AnyConnect automatically chooses the client certificate with which to authenticate. In this case, AnyConnect views all the installed certificates, disregards those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the user attempts to establish a VPN connection.
- **Certificate Name** — If you already have certificates installed on the device, select one to be associated with this VPN connection.

c. Tap **Advanced** to return to the advanced configuration window

Note If you are **not** going to be using certificates for authentication, **do nothing** to the certificate field and tap **Save**. The connection setting maintains the Disabled certificate setting.

If you **are** going to be using certificates to authenticate, **do nothing** to the certificate field and tap **Save**. Then, use the Installing a Certificate on Your Mobile Device procedure to import and configure certificate authentication for your connection profile.

Step 7 (Optional) Configure Connecton on Demand for this connection.

If you are using certificates to authenticate your VPN connection the **Connect on Demand** switch displays. See Configuring Connect-On-Demand Rules to configure this function.

Step 8 Configure this connection to use the IPsec VPN protocol instead of SSL.

a. (Optional) Tap **Connect with IPsec** to use IPsec instead of SSL for this VPN connection.

The **Authentication** parameter displays if you choose IPsec for your VPN connection protocol.

b. (Optional) Tap **Authentication** and choose the authentication method for this IPsec connection:

- EAP-AnyConnect (Default)
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

Tap **Advanced** to return to the Advanced configuration window. Your authentication option is shown in the Advanced Connection Editor Window.

If you have specified EAP-GTC, EAP-MD5, or EAP-MSCHAPv3 to be used for authentication,the **IKE Identity** parameter displays.

c. (Optional) Tap **IKE Identity** to enter the required client identity. This is provided by your administrator.

Step 9 Tap the connection entry name to return to the Add VPN Connection window.

Step 10 Tap **Save** to retain the connection values.

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

Installing a Certificate on Your Mobile Device

In order to authenticate your device to the secure gateway using a certificate, import the certificate to your device and then associate that certificate with a connection entry. Use one of these methods to import a certificate to your Apple iOS device:

- Importing and Installing Certificates Attached to Emails
- Importing and Installing Certificates From Hyperlinks
- Importing and Installing Certificates with a SCEP-configured Connection Alias

At the end of each procedure there is a link to Associating a Certificate with a Connection Entry.

See Managing Certificates for additional certificate related activities.

Importing and Installing Certificates Attached to Emails

Your administrator emails you a certificate to use for authentication. When you receive the certificate, follow this procedure:

Step 1 Tap the icon for the attached certificate.

Apple iOS recognizes that you have just opened a certificate, and it opens an installation wizard.

Step 2 Tap **Install**.

Step 3 Follow the prompts in the installation wizard.

Step 4 If you are prompted, enter an authentication code for the certificate.

Step 5 Tap **Next**.

Apple iOS installs the certificate.

Step 6 Continue with Associating a Certificate with a Connection Entry.

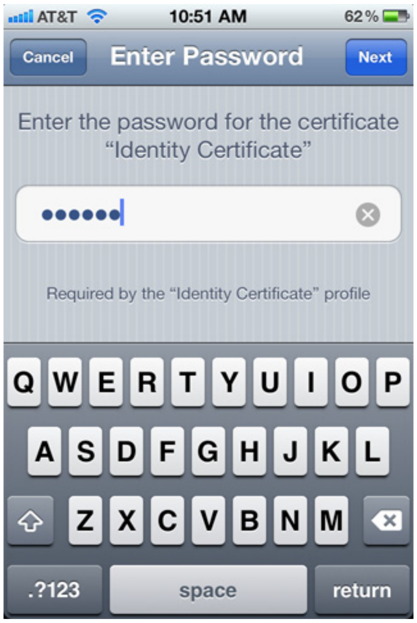
Importing and Installing Certificates From Hyperlinks

Your administrator provides you with a hyperlink to the location of a certificate that you install on your iOS device.

Note You need to set External Control to either Prompt or Enable within the AnyConnect settings to allow this activity. See Configuring External Control for more information.

Step 1 Tap the hyperlink provided by your administrator. The link may be included in an email or published on an intranet web page.

Step 2 If you are prompted, provide the authentication code for the certificate.

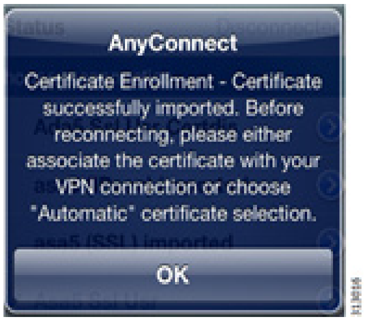


Enter the password for the certificate "Identity Certificate"

Required by the "Identity Certificate" profile

Step 3 Tap **Next**.

Apple iOS imports the certificate from the location specified in the hyperlink. After iOS successfully imports the certificate, you receive a certificate enrollment message.



Certificate Enrollment - Certificate successfully imported. Before reconnecting, please either associate the certificate with your VPN connection or choose "Automatic" certificate selection.

Step 4 Tap **OK**.

Step 5 Continue with Associating a Certificate with a Connection Entry.

Importing and Installing Certificates with a SCEP-configured Connection Alias

Your administrator may configure a connection profile that distributes certificates using the SCEP protocol. Your AnyConnect administrator needs to provide you with the name of the VPN configuration or connection profile that uses it.

There are two methods of importing and installing certificates with an SCEP-configured connection alias:

- Manually Importing and Installing Certificates
- Automatically Importing and Installing Certificates

Manually Importing and Installing Certificates

Step 1 Open the AnyConnect Secure Mobility Client application.

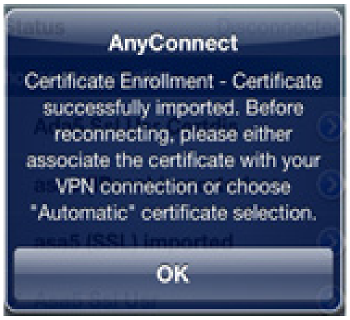
Step 2 In the **Choose a connection...** area, tap the name of the connection capable of downloading a certificate to your mobile device.

Step 3 Tap the AnyConnect **On** button.

Step 4 Tap, **Get Certificate**.

The secure gateway downloads the certificate to your device.

Your VPN session is disconnected, and then you receive the message that certificate enrollment was successful, and you need to manually assign the certificate to a group.



AnyConnect

Certificate Enrollment - Certificate successfully imported. Before reconnecting, please either associate the certificate with your VPN connection or choose "Automatic" certificate selection.

Step 5 Enter your username and password if prompted.

Step 6 Tap **OK**.

Step 7 Continue with Associating a Certificate with a Connection Entry.

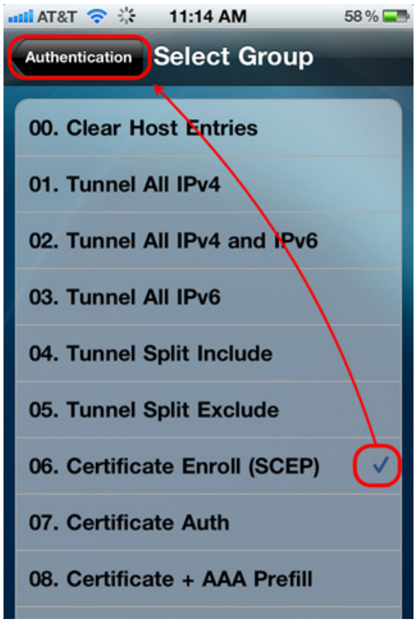
Automatically Importing and Installing Certificates

Step 1 Open the AnyConnect Secure Mobility Client application.

Step 2 In the **Choose a connection...** area, tap the name of the connection capable of downloading a certificate to your mobile device.

Step 3 Tap the AnyConnect **On** button.

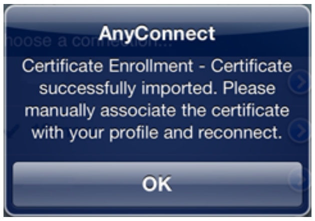
Step 4 From the Authentication screen, select the group configured to download a certificate to your mobile device and then go back to the Authentication screen.



Step 5 Enter your username and password for the connection profile and tap **Connect**.

The secure gateway downloads the certificate to your device.

Your VPN session is disconnected and then you receive the message that certificate enrollment was successful and you need to manually assign the certificate to a group.



AnyConnect

Certificate Enrollment - Certificate successfully imported. Please manually associate the certificate with your profile and reconnect.

Step 6 Tap **OK**.

Step 7 Continue with Associating a Certificate with a Connection Entry.

Associating a Certificate with a Connection Entry

You have already created a VPN connection using Adding a VPN Connection Entry or there are connection entries on your device that you can modify using Modifying a VPN Connection Entry.

Step 1 In the **Choose a conection...** panel, select the connection's detail disclosure button.

Step 2 Tap **Advanced > Certificate**.

Step 3 Tap the name of the certificate you just imported.

The certificate shows a check mark to indicate it is the one selected.

Tip When you are in the Select Certificate screen, check **Automatic** for automatic certificate selection. AnyConnect attempts to select the correct certificate for authentication if you have more than one certificate installed on your device.

Step 4 Go back to the connection details.

Step 5 (Optional) Configure Connect on Demand using Configuring Connect-On-Demand Rules.

Step 6 Tap **Save**.

Start your VPN connection by turning AnyConnect **ON** in the home screen.

Configuring 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 selected connection entry—the entry with the check mark next to it.

When a VPN connection is initiated via iOS's Connect on Demand, iOS disconnects the tunnel if the tunnel is inactive (no traffic through the tunnel) for a particular time interval. See Apple's VPN On Demand documentation for more information.

- **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 secure gateway 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`.

Note Apple iOS 7 no longer supports *Always Connect* domains. When running AnyConnect on Apple iOS 7 devices, any domains listed as *Always Connect* will be treated as *Connect if Needed* domains.

- **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 from 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 specifies a destination by using its fully-qualified domain name rather than an IP address.
- 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 domain name match.	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
Exact match of a sequence of discreet subdomains up through the top-level domain. 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.

Prerequisites

The connection entry is configured to authenticate using a valid certificate.

The connection entry is one the user created. Users cannot configure connect on demand in connection profiles downloaded from the ASA.

Detailed Steps

To configure connect on demand, follow this procedure:

Step 1 Open the AnyConnect home screen.

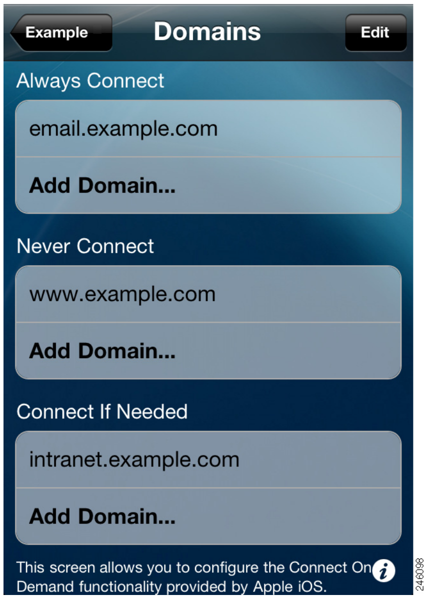
Step 2 In the **Choose a connection...** area tap the connection details icon for the connection you are going to configure for connect on demand.

Step 3 Tap **Advanced** to open the Advanced configuration window.

Step 4 Tap **ON** next to Connect On Demand.

Step 5 Tap **Domain List**.

The Domains screen shows the domain lists.



Always Connect

email.example.com

Add Domain...

Never Connect

www.example.com

Add Domain...

Connect If Needed

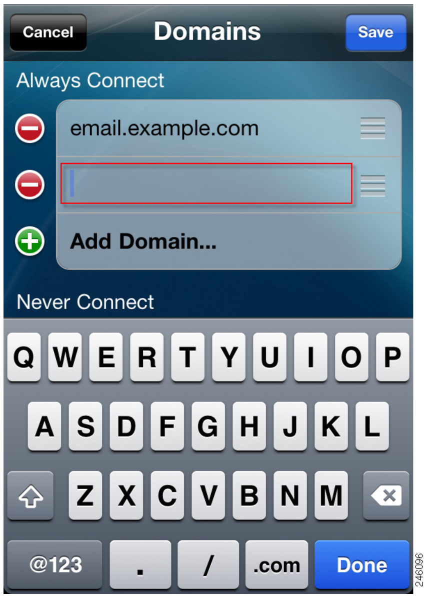
intranet.example.com

Add Domain...

This screen allows you to configure the Connect On Demand functionality provided by Apple iOS.

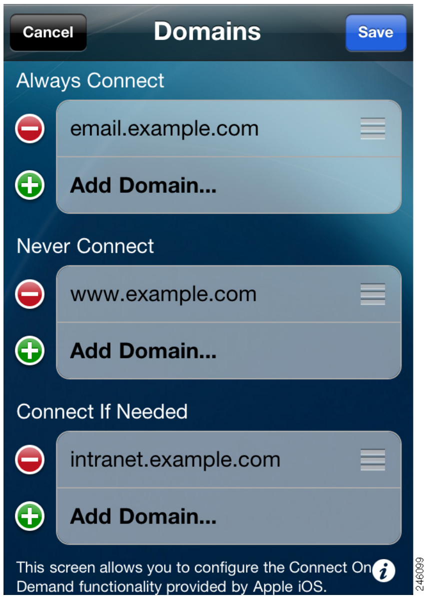
Step 6 Do either of the following:

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



email.example.com

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



email.example.com

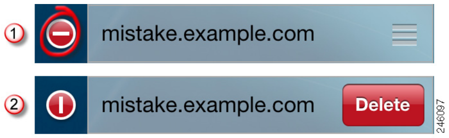
www.example.com

intranet.example.com

This screen allows you to configure the Connect On Demand functionality provided by Apple iOS.

This screen 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.



Step 7 Tap **Save**.

Establishing a VPN connection

Prerequisites

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

Detailed Steps

Step 1 Go to the AnyConnect home screen.

Step 2 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.

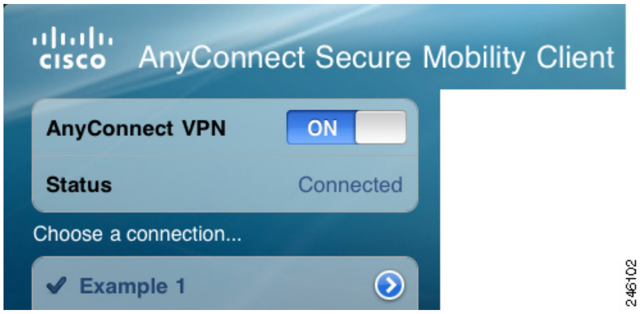
Step 3 Tap **ON** next to AnyConnect VPN.

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

Step 5 If instructed by your system administrator to do so, tap **Get Certificate**.

Step 6 If necessary, tap **Connect**.

The Status parameter reveals the new connection state


AnyConnect Secure Mobility Client

AnyConnect VPN: ON

Status: Connected

Choose a connection...

✓ Example 1

and the VPN icon is shown in the Status Bar.

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

Caution Tapping another VPN connection in the AnyConnect home screen disconnects the current VPN connection.

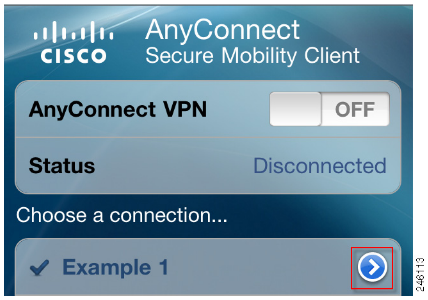
Modifying a VPN Connection Entry

You are able to modify all aspects of connection entries you create.

When the Apple iOS mobile device connects to the ASA, AnyConnect imports that VPN client profile and installs it on the device. Users cannot modify most fields in the VPN client profiles defined by an AnyConnect administrator.

Step 1 Open the AnyConnect home screen.

Step 2 Tap the detail disclosure button to the right of the VPN connection entry.



AnyConnect displays the VPN connection parameters.

Step 3 Tap **Advanced** to access additional parameters, then choose **Add VPN Connection** to return to the basic configuration screen.

Step 4 Tap any parameter in either screen to change its value.

Step 5 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 6 From the **Add VPN Connection** screen, tap **Save**.

AnyConnect closes the connection parameter screen.

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

Step 1 Open the AnyConnect home screen.

Step 2 Tap the detail disclosure button 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 screen and removes the entry from the AnyConnect home screen.

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 From the AnyConnect home screen tap **Diagnostics > Profile > Delete Profile**.

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.

Managing Anyconnect

Specifying Application Settings

Changing the Theme

AnyConnect 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 Inside the AnyConnect app, tap **Settings > Theme**.

Step 2 Tap the theme you want: **Cisco Default Theme** or **High Contrast**.

Apple iOS inserts a check mark next to the theme you selected, and changes the application theme immediatley.

Step 3 Tap **Settings** to return to the Settings screen.

Configuring External Control

Enabling external control allows you to click links your administrator sends you to perform such tasks as creating connections or importing certificates. It also allows Apple iOS to act on a command in a URI that was not sent by your AnyConnect administrator.

Step 1 Inside the AnyConnect app, tap **Settings > Theme**.

Step 2 Choose one of these options:

- **Disable**: No external control allowed. Clicking a URI in an email or on a web page results in the following error message:

  "The External Control feature is disabled. Enable it from the AnyConnect settings."

- **Prompt**: When the mobile device user clicks a URI in an email or web page, AnyConnect prompts the user to accept or reject a connection to the remote server with this message:

  "Another application has requested that AnyConnect connect to <asa.example.com>. Do you want to allow this?"

- **Enable**: When the mobile device user clicks a URI in an email or web page, AnyConnect executes the commands specified in the URI without interrupting the user.

Step 3 Tap **Settings** to return to the Settings screen,

Blocking Untrusted Servers

This application setting determines if AnyConnect automatically blocks connections if it is unable to identify the secure gateway. This protection is ON by default but can be turned OFF, this is not recommended.

AnyConnect uses the certificate received from the server to verify its identify, if there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch, the connection is blocked.

When this setting is ON, a blocking Untrusted VPN Server! notification alerts you to this security threat.

Step 1 Inside the AnyConnect app, tap **Settings > Theme**.

Step 2 Tap the **Block Unstrusted Servers** switch to enable or disable automatic blocking.

Setting FIPS Mode

FIPS Mode makes use of Federal Information Processing Standards (FIPS) cryptography algorithms for all IPsec VPN connections. Your administrator informs you if you need to enable FIPS mode on your mobile device for IPsec VPN connectivity to your network.

Step 1 Inside the AnyConnect app, tap **Settings**.

Step 2 Tap the **FIPS Mode** switch to enable or disable FIPS Mode.

Managing Certificates

Certificates are used to digitally identify each end of the VPN connection: The secure gateway, or the server, and the AnyConnect client, or the user. A server certificate identifies the secure gateway to AnyConnect, a user certificate identifies the AnyConnect user to the secure gateway. Certificates are obtained from and verified by Certificate Authorities (CAs).

When establishing a connection, AnyConnect always expects a server certificate from the secure gateway. The secure gateway only expects a certificate from AnyConnect if it has been configured to do so. Expecting the AnyConnect user to manually enter credentials is another way to authenticate a VPN connection. In fact, the secure gateway can be configured to authenticate AnyConnect users with a digital certificate, with manually entered credentials, or with both. Certificate only authentication allows VPNs to connect without user intervention.

Distribution and use of certificates to the secure gateway and to your device is directed by your administrator. Follow directions provided by your administrator to import, use, and manage server and user certificates for AnyConnect VPNs. Information and procedures in this document related to certificates and certificate management are provided for your understanding and reference.

AnyConnect stores both user and server certificates for authentication in its own certificate store. The AnyConnect certificate store is managed from the **Diagnostics > Certificates** screen.

User Certificate Management

In order for you, the AnyConnect user, to authenticate to the secure gateway using a digital certificate, you need a User certificate in the AnyConnect certificate store on your device. User certificates are imported using one of the following methods as directed by your administrator:

- Imported manually from the device's file system, the device's credential storage, or from a network server.
- Imported after clicking on a hyperlink provided by your administrator in an email or on a web page.
- Imported when connecting to a secure gateway that has been configured by your administrator to provide you with a certificate.

Once imported, the certificate is associated with a particular connection entry, or selected automatically during connection establishment to automatically authenticate.

User certificates in the AnyConnect store can be deleted if they are no longer needed for authentication.

Server Certificate Management

A server certificate received from the secure gateway during connection establishment automatically authenticates that server to AnyConnect, if and only if it is valid and trusted. Otherwise:

- A valid, but untrusted server certificate is reviewed, authorized, and imported to the AnyConnect certificate store. Once a server certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted.
- An invalid certificate cannot be imported into the AnyConnect store, but is accepted to complete the current connection. This is not recommended.

Server certificates in the AnyConnect store can be deleted if they are no longer needed for authentication.

Viewing Certificates

View User and Server certificates that have been imported into the AnyConnect certificate store by doing the following:

Step 1 From the AnyConnect menu tap **Diagnostics > Certificates**.

Step 2 Tap the **User** or **Server** tab to view certificates in the AnyConnect certificate store.

Step 3 Use this screen to take one of these actions:

- Tap the detail disclosure button for the certificate to view the certificate’s properties.
- Tap the Edit button to delete the certificate.
- Tap **Import Certificate...** to manually import a certificate.
- Tap **Delete All Certificates** to remove all certificates from the device.

Viewing and Managing the AnyConnect Profile

The AnyConnect VPN Client Profile is an XML file that specifies client behavior and identifies VPN connections. Each connection entry in the VPN Client Profile specifies a secure gateway that is accessible to this endpoint device as well as other connection attributes, policies and constraints. These connection entries, in addition to the VPN connections configured locally on the device by the user, are listed on the AnyConnect home screen to choose from when initiating a VPN connection.

Note AnyConnect retains only one VPN Client Profile on the device at a time.

Users now have the ability to manage the AnyConnect VPN Client Profile on their device. Users perform these tasks:

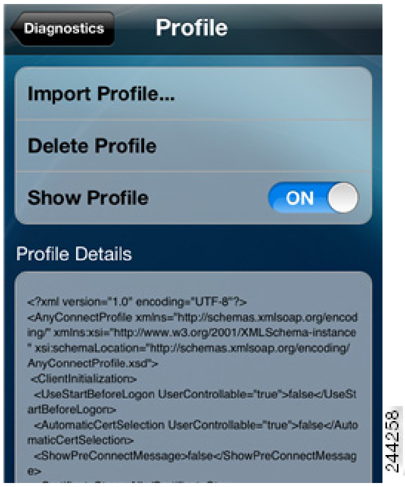
Step 1 On the AnyConnect home page, tap **Diagnostics**.

The Diagnostics screen opens.

Step 2 Tap **Management**.

Step 3 Tap **Profile**.

Use this screen to take one of these actions:



```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encod
ing/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
 <ClientInitialization>
  <UseStartBeforeLogon UserControllable="true">false</UseSt
artBeforeLogon>
  <AutomaticCertSelection UserControllable="true">false</Auto
maticCertSelection>
  <ShowPreConnectMessage>false</ShowPreConnectMessag
e>
```

- **Import Profile...**, specify the URL of the profile to be imported.
- **Delete Profile**, confirm this action to delete the current profile from the device
- **Show Profile**, tap ON to show the current profile on the device

Managing Localization

Upon AnyConnect installation, your device is localized according to the configured language. See Device Localization for the list of languages supported at installation time. Additional localization management on your device is carried out based on instructions provided by your administrator.

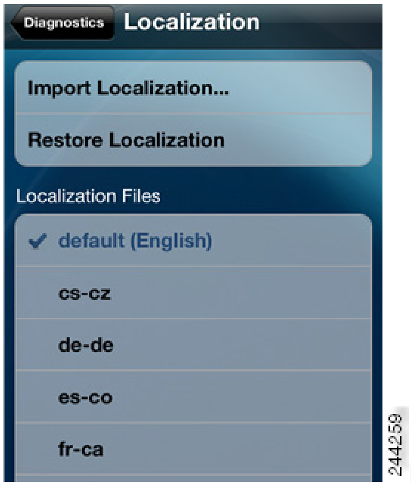
Step 1 On the AnyConnect home page, tap **Diagnostics**.

The Diagnostics screen opens.

Step 2 Tap **Management**.

Step 3 Tap **Localization**.

Use this screen to take one of these actions:



- **Import Localization...**, enter the server address and language to import. This localization data is used in place of the pre-packaged, installed localization data. See Importing Localization Data for the other ways to import localization data onto your device.
- **Restore Localization**, to remove all imported localization files, and restore the installed localization files.

Importing Localization Data

After installation, localization data for languages not supported in the AnyConnect package is imported by:

- Clicking on a hyperlink provided to you by an administrator that has been defined to import localization data.

  Your administrator provides a hyperlink in email, or on a webpage, that imports localization data when clicked. This method uses the AnyConnect URI handler, a feature available to administrators for simplifying AnyConnect configuration and management for the user.

  Note The user needs to allow this AnyConnect activity by setting External Control to either Prompt or Enable within the AnyConnect settings. See Configuring External Control for how to set this.

- Connecting to a secure gateway that an administrator has configured to provide downloadable localization data upon VPN connection.

  Your administrator provides you with appropriate VPN connection information, or a predefined connection entry in the XML profile, if this method is to be used. Upon VPN connection, localization data is downloaded to your device and put into play immediately.

- Using the Localization Management screen to manually import localization data from a specified server. This localization data is used in place of the installed localization data. See Managing Localization for the import procedure.

Removing AnyConnect

To remove AnyConnect from the device,

Step 1 On the AnyConnect home page, tap **Diagnostics**.

Step 2 Tap **Management.**

Step 3 Tap **Profile**.

Step 4 Tap **Delete Profile**.

Step 5 Press the menu button to go to the AnyConnect home screen.

Step 6 If you placed AnyConnect in a folder, open the folder.

Step 7 Tap and hold the AnyConnect icon until a delete (**X**) icon appears above it.

Step 8 Tap the delete icon.

Obtaining AnyConnect Information

Displaying the AnyConnect Version and Licensing Details

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

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.

Viewing System Information

System information relevant to AnyConnect operation is shown in the System Information screen. To view this information:

Step 1 Go to the AnyConnect home screen.

Step 2 On the AnyConnect home page, tap **Diagnostics**.

Step 3 Tap **System Information**.

The following information is displayed:

- Wi-Fi: IPv4 Address, IPv4 Subnet Mask, IPv6 Address, IPv6 Subnet Mask, MAC Address
- Cellular Data: Network IP, Subnet Mask
- DNS Servers
- Device: Platform Version, Device Type, UDID
- Routine Table

Viewing General VPN Connection Statistics

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

To view statistics for the current VPN connection. open the AnyConnect home screen.

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 4 From the AnyConnect home screen Tap **Details** in the Status Overview panel.

AnyConnect displays detailed information about the VPN connection.

Step 5 Scroll to view all of the statistics.

The Detailed Statistics screen includes 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.

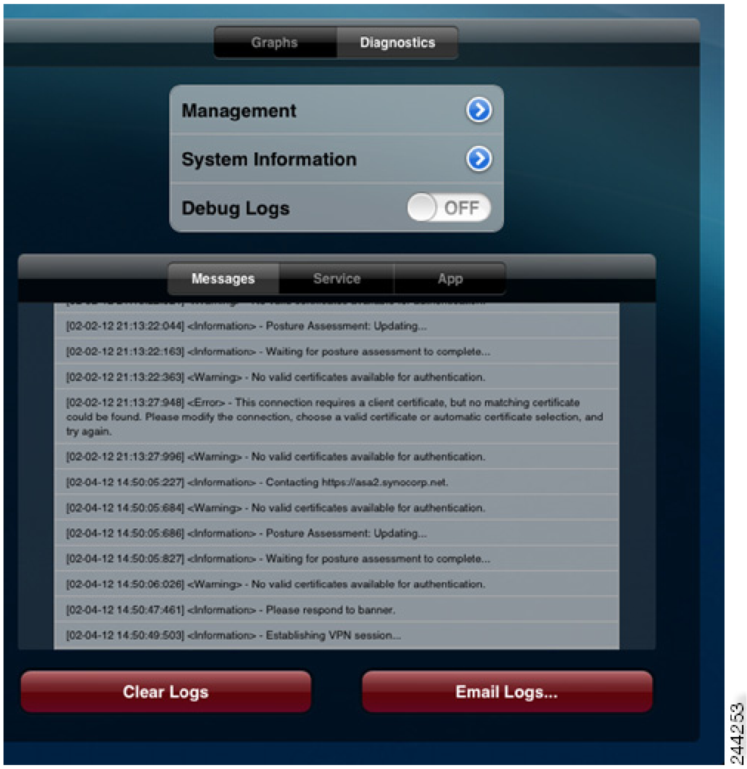
To hide the detailed statistics, tap any field in the Statistics Overview frame.

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 Tap the **Diagnostics** button in the main screen of the AnyConnect Secure Mobility Client home page.



```
[02-02-12 21:13:22:044] <Information> - Posture Assessment: Updating...
[02-02-12 21:13:22:163] <Information> - Waiting for posture assessment to complete...
[02-02-12 21:13:22:363] <Warning> - No valid certificates available for authentication.
[02-02-12 21:13:27:948] <Error> - This connection requires a client certificate, but no matching certificate
could be found. Please modify the connection, choose a valid certificate or automatic certificate selection, and
try again.
[02-02-12 21:13:27:996] <Warning> - No valid certificates available for authentication.
[02-04-12 14:50:05:227] <Information> - Contacting https://asa2.synocorp.net.
[02-04-12 14:50:05:684] <Warning> - No valid certificates available for authentication.
[02-04-12 14:50:05:686] <Information> - Posture Assessment: Updating...
[02-04-12 14:50:05:827] <Information> - Waiting for posture assessment to complete...
[02-04-12 14:50:06:026] <Warning> - No valid certificates available for authentication.
[02-04-12 14:50:47:461] <Information> - Please respond to banner.
[02-04-12 14:50:49:503] <Information> - Establishing VPN session...
```

Scroll to view additional messages.

Step 2 Use this screen to do the following:

- **Management**: Tap to manage configuration of AnyConnect certificates, profiles, and localization data.
- **System Information**: Tap to view system information relevant to AnyConnect, see **Viewing System Information.**
- **Debug Logs:** Turn debug logging ON or OFF.
- **Messages**: Tap to display the log messages. Scroll to view additional messages.
- **Service**: Tap to display the service debug log messages. Scroll to view additional messages.
- **App**: Tap to display the application debug log messages.

- **Clear Logs**: Tap if you want to remove the 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. You need to have an email account configured on your device.

Responding to AnyConnect Notifications

Responding to Untrusted VPN Server Notifications

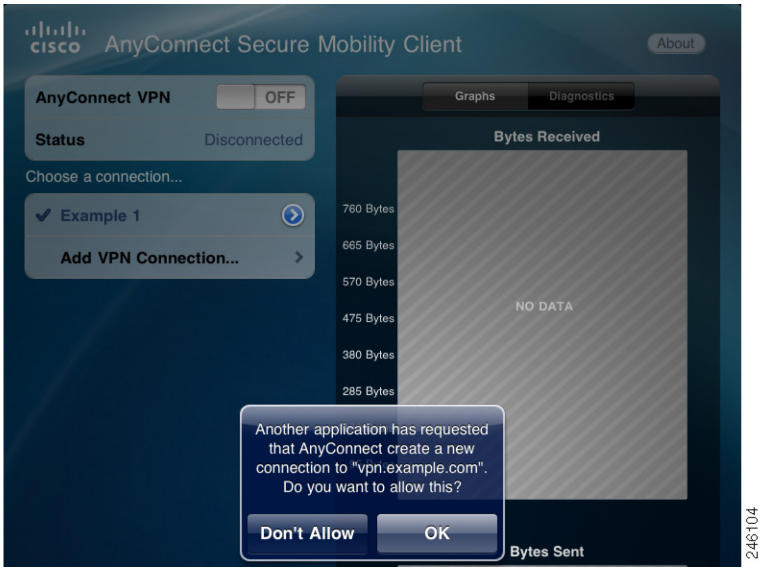
The type of Untrusted VPN Server notification displayed depends on the Block Untrusted VPN Server application preference:

- If enabled, a blocking Untrusted VPN Server! notification displays, choose:
  - Keep Me Safe to keep this setting and this blocking behavior.
  - Change Settings to turn off blocking.

  After changing the Bock Untrusted VPN Server re-initiate the VPN connection.
- If not enabled, a non-blocking Untrusted VPN Server! notification displays, choose:
  - Cancel to abort the VPN connection to the untrusted server
  - Continue to make the connection to the untrusted server, this is not recommended.
  - View Details to view certificate details and decide whether to import the server certificate into the AnyConnect certificate store for future acceptance and continue the connection, or not.

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 For example,



Another application has requested that AnyConnect create a new connection to "vpn.example.com". Do you want to allow this?

To protect your device and data, ask your system administrator whether to tap **OK** to approve of these types of the following 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?"

Note You only receive these messages if External Control is set to **Prompt**. Set External Control on your mobile device by opening your device's home page and navigating to **Settings > AnyConnect > External Control.**

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 connection profiles.**

  Your system administrator set a policy that affects host entries imported into your AnyConnect connection profile. To delete these profiles, tap **Diagnostics > Profile > 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, and network congestion often cause time-outs and unresolved host errors. If a LAN is within reach, try using your device Settings application 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(2G), 1xRTT(2G), 3G, or Wi-Fi connection.

  Note This issue may 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 display 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 > Profile > Clear Profile Data**.

Known Issues in Apple iOS Impacting VPN

We have reported the following iOS issues to Apple. They may be resolved in a future iOS release.

- A DTLS packet received while the device is asleep does not awaken it. TLS packets, however, awaken the device if notifications or Facetime is enabled. AnyConnect automatically disconnects the DTLS tunnel when the device goes to sleep to allow packets received over the TLS connection to wake the device. The DTLS tunnel is restored when the device resumes.

- Voice applications running in the background on an iPod Touch cannot receive packets over VPN. This functionality works as expected on iPhone devices.
- If a VPN configuration contains a large number of routes or split-dns rules, the Apple device cannot establish a VPN connection. This bug occurs, for example, if, upon connection, an ASA configuration pushes a VPN split-include list that has 70 or more rules that direct traffic to individual subnets. To prevent this bug from impacting users, apply a tunnel-all configuration or reduce the number of rules.
- AnyConnect may become slow or crash when there are a large number of VPN connections configured on the mobile device.
- Customers who wish to tunnel IPv6 traffic need to upgrade their iPhones and iPads to iOS 5.0 or later. Known problems exist in iOS 4.3 that prevent AnyConnect from processing IPv6 traffic properly due to the inability to set default IPv6 routes.

Apple iOS Permits All Local LAN Traffic with Tunnel-all

Apple iOS permits traffic that is essential for the core operation of the device, regardless of whether a tunnel-all policy is in force. Examples of traffic that Apple iOS sends in the clear regardless of the tunnel policy include:

- All local LAN traffic
- Scoped routes for preexisting connections (for example, a video being streamed before VPN comes up)
- Core Apple services (for example, Visual Voice mail traffic)

Limitations of AnyConnect for Apple iOS

This release of AnyConnect for Apple iOS supports only the features that are strictly related to remote access.

- AnyConnect supports the following types of VPN configurations:
  - Manually generated.
  - AnyConnect VPN client profile imported.
  - iPhone Configuration Utility generated. For details about the iPhone Configuration Utility see http://www.apple.com/support/iphone/enterprise/
- The VPN configurations generated by the iPhone Configuration Utility do not support Network Roaming. If your users require Network Roaming, use an AnyConnect profile.
- The Apple iOS device supports no more than one AnyConnect VPN client profile. The contents of the generated configuration always matches the most recent profile. For example, if a user goes to vpn.example1.com and then goes to vpn.example2.com, the AnyConnect VPN client profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it reduces battery life of the device. Increasing the update interval value mitigates this issue.
- AnyConnect collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which AnyConnect mis-reports mobile posture information if the user relies on iOS’s Connect on Demand feature to make a connection initially, or after device information, such has the OS version, has changed.

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.