Apple iOS User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x

Revised: February 2, 2018,

AnyConnect User Guide

Install and Start AnyConnect

AnyConnect Overview

The Cisco AnyConnect Secure Mobility Client for Apple iOS provides seamless and secure remote access to enterprise networks. AnyConnect allows installed applications to communicate as though connected directly to the enterprise network. AnyConnect is a sophisticated networking application that also allows you to set preferences, control the operation of AnyConnect, and use diagnostic tools and facilities on your device as recommended by your administrator.

AnyConnect may be used in your enterprise in conjunction with Mobile Device Management software. If so, work with your administrator to abide by device management rulessince these rules may include restricting VPN access to a set of approved applications. Your organization may provide additional documentation on using AnyConnect for Apple iOS.

Your Apple iOS app store provides the application for initial installation and all upgrades. 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 mobile devices.

Displaying Help

AnyConnect displays an information icon on the lower right corner of the screen if help is available. Tap this icon to display help information about the current options.

Alternatively, tap **About** to display a link that provides access to this guide.

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).

AnyConnect Versions Available for Apple iOS

Cisco AnyConnect for Apple iOS is currently available in multiple versions:

- ***Cisco AnyConnect***

  This is the initial release of this new app. *Cisco AnyConnect* is the latest and recommended version available for Apple iOS. To ensure you are always receiving the latest Apple iOS bug fixes, upgrade to the latest version. (During the Beta cycle, this version of AnyConnect was named *AnyConnect 2017*.)

  We recommend using this version with Apple iOS 10.3 and later. It uses the New Extension Framework, provided by iOS, to implement VPN and all its features. Per App VPN tunneling is fully supported feature in *AnyConnect 4.0.07x and later*, and

the New Extension Framework allows support of both TCP and UDP applications. Moving forward, this new Cisco AnyConnect version will be the only one to contain all enhancements and bug fixes. It will be the numbered 4.0.07x+.

- ***Cisco Legacy AnyConnect***

  Legacy AnyConnect is the version supporting Apple iOS 6.0 and later that has been available on the app store for some time now. This version will be phased out over time, but currently remains available to ease transition to the latest and recommended version.

  The Per App VPN tunneling feature in this Legacy AnyConnect app will not receive TAC support. Customers wanting to use Per App VPN should migrate to the new version.

  Legacy AnyConnect will only be updated for critical security issues. This release continues to be numbered 4.0.05x.

Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs. Hence:

- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x. Cisco AnyConnect 4.0.07x (or 4.6.x) is a separate app, installed with a different name and icon.
- The different versions of AnyConnect can co-exist on the mobile device, but this is not supported by Cisco. The behavior may not be as expected if you attempt to connect while having both versions of AnyConnect installed. Make sure you have only one AnyConnect app on your device and it is the appropriate version for your device and environment.
- Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release, cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.
- Current MDM profiles will not trigger the new app. EMM vendors must support VPNType (VPN), VPNSubType (com.cisco.anyconnect) and ProviderType (packet-tunnel). For integration with ISE, they must be able to pass the UniqueIdentifier to AnyConnect since AnyConnect no longer has access to this in the new framework. Please consult with your EMM vendor for how to set this up, some may require a custom VPN type and others may not have support available at release time.

Using the New Extension Framework in AnyConnect 4.0.07x and later causes the following changes in behavior from Legacy AnyConnect 4.0.05x:

- The Device ID sent to the head end is no longer the UDID in the new version, and it is different after a factory reset unless your device is restored from a backup made by the same device.
- You may use MDM deployed certificates, as well as certificates imported using one of the methods available in AnyConnect: SCEP, manually through the UI, or via the URI handler. The new version of AnyConnect can no longer use certificates imported via email or any other mechanism beyond these identified ones.
- When creating a connection entry using the UI, the user must accept the iOS security message displayed.
- A user-created entry with the same name as a downloaded host entry from the AnyConnect VPN profile will not be renamed until it disconnects, if it is active. Also, the downloaded host connection entry will appear in the UI after this disconnect, not while it remains connected.

Apple iOS Devices Supported

Cisco AnyConnect 4.0.07x and later is the latest and recommended version available on all iPhones, iPads, and iPod Touch devices running Apple iOS 10.3 and later.

If a device does not support Apple iOS 10.3 or later, only ***Legacy AnyConnect 4.0.05x***, available on all iPhones, iPads, and iPod Touch devices running Apple iO 6.0 and later, can be used. Per App tunneling in Legacy AnyConnect requires Apple iOS 8.3 or later.

Note AnyConnect on the iPod Touch appears and operates as on the iPhone.

Install the Apple iOS AnyConnect App

The Cisco AnyConnect or Legacy AnyConnect Secure Mobility client for Apple iOS is installed from the Apple App Store.

Before You Begin

App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.

Procedure

Step 1 Open the App Store.
Step 2 Select **Search**.
Step 3 In the Search Box, enter anyconnect and tap **cisco anyconnect** or **legacy anyconnect**in the suggestions list.
Step 4 Tap **AnyConnect**.
Step 5 Tap **Free**, then **INSTALL APP**.
Step 6 Select **Install**.

Upgrade AnyConnect on Apple iOS

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

Note You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x. Cisco AnyConnect 4.0.07x (or 4.6.x) is a separate app, installed with a different name and icon.

See AnyConnect Versions Available for Apple iOS, on page 2 before installing the new version, 4.0.07xxx. Cisco recommends you remove all Legacy AnyConnect app data, remove the Legacy AnyConnect app, and then install the new version.

Before You Begin

Before upgrading your device you must disconnect an AnyConnect VPN session if one is established, and close the AnyConnect application if it is open. If you fail to do this, AnyConnect requires a reboot of your device before using the new version of AnyConnect.

Note This only applies in your environment if you are running a Legacy AnyConnect release earlier than 4.0.05032, or an Apple iOS release earlier than 9.3 while using Apple Connect-on-Demand capabilities. To ensure proper establishment of Connect On-Demand VPN tunnels after updating AnyConnect, users must manually start the AnyConnect app and establish a connection. 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" displays.

Procedure

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 update proceeds.

Start AnyConnect

Procedure

Tap the AnyConnect icon on the iPhone or iPad home screen.
If this is the first time you are starting AnyConnect after installing or upgrading, choose **OK** to enable AnyConnect, allowing this app to extend the Virtual Private Network (VPN) capabilities of your device.

From the AnyConnect **Home** screen you can:

- Establish or terminate a VPN connection using the **AnyConnect VPN** ON/OFF switch.
- Identify the active connection and navigate to the **Connections** window to view or choose from other configured connection entries.
- View the status and other **Details** of the current VPN connection.
- Navigate to the **Settings**, **Diagnostics**, and **About** windows.

Configure a VPN Connection

AnyConnect requires the following to establish VPN connectivity:

- An address to a secure gateway for access to your network.

This address is configured in a connection entry. Connection entries are listed on the AnyConnect home screen. The active connection entry is identified on the AnyConnect home screen or in the Connections list. VPN connection entries are configured on your device manually, or automatically configured by your enterprise administrator.

- Authentication information to successfully complete your connection.

  This will be in the form of a username and password you must remember, or it will be contained in a digital certificate that has been configured on your device. For some VPN connections, both authentication methods may be required. Digital certificates are configured on your device manually, or automatically configured by your device administrator.

Configure your AnyConnect client as directed by your administrator. Contact your administrator if you do not have clear instructions.

Configure Connection Entries

A connection entry specifies a secure gateway that provides access to your private network, as well as other connection attributes.

Select **Connections** from the AnyConnect home screen to view the entries already configured on your device. Multiple connection entries may be listed, some under a **Per-App VPN** heading. Connection entries may have the following status:

- Enabled—This connection entry is enabled by the mobile device manager and can be used for connecting.
- Active—This marked or highlighted connection entry is currently active.
- Connected—This connection entry is the active one and is currently connected and operating.
- Disconnected—This connection entry is the active one but is currently disconnected and not operating.

Per-App VPN connection entries are configured by your enterprise's mobile device manager and may include a list of apps, these apps are the only ones that will be allowed access to the enterprise's private network.

Procedure

Connection entries are configured on your device manually or automatically in the following ways:

- Manually configured.

  You must know the address of the secure gateway to your network. The address is the domain name or the IP address of the secure gateway, and it may also specify a group that you belong to. Other connection attributes can also configured. See Add or Modify Connection Entries Manually, on page 7.

- Automatically configured by clicking on a link provided by your administrator.

  An AnyConnect URI link may be included in an email or published on a web page. The application preference **External Control** must be set to either **Prompt** or **Enable** to allow this on your device. See Control the External Use of AnyConnect, on page 16

- Automatically configured after connecting to a secure gateway that downloads an AnyConnect client profile containing connection entries. See Manage the VPN Profile, on page 17.

- Configured by your enterprises' Mobile Device Management software. Device management profiles may be found on your device under the General Settings.

Add or Modify Connection Entries Manually

Before You Begin

Note You are able to modify connection entries you created, but you cannot fully edit connections that have been imported from an AnyConnect VPN Profile or the iPhone Configuration Utility mobileconfig.

Procedure

Step 1 From the AnyConnect home screen, tap **Connections**. Then select the connection you would like to modify or select **Add VPN Connection**.
If your device is being managed by your enterprise's Mobile Device Management software, you are notified as such when manually configuring a connection entry. Verify with your administrator that this is the proper way to use AnyConnect in your environment.

The basic VPN connection parameters are displayed. Tap **Cancel** to cancel the configuration process at any time or tap **Save** to save the connection entry.

Step 2 (Optional) Tap **Description** to specify 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 configure the advanced VPN connection parameters.

a) (Optional) Configure **Network Roaming** for this connection. See Configure Network Roaming.
b) (Optional) Configure **Certificate** use for this connection. See Configure Certificate Use.
c) (Optional) View **App Rules**.
If your device is being managed by your enterprise's Mobile Device Management software, you may find a list of the apps that are allowed access to the private network here. Apps are listed here if they are allowed and installed. Data flow for all other apps will not use the VPN connection but will send and receive data outside of the VPN tunnel, in the clear.
d) (Optional) Configure **Connect on Demand** for this connection. See Configure Connect on Demand.
e) (Optional) Configure this connection to **Connect with IPsec** instead of SSL. See Configure IPsec.
f) Tap **Add VPN Connection** to return to the initial configuration window.

Step 5 Tap **Save** to retain the connection values.

Configure Network Roaming

Network Roaming configures the amount of time AnyConnect 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). Network Roaming can be turned ON or OFF:

- 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 start a new VPN connection if one is necessary.

Before You Begin

Note

- Network Roaming applies to releases earlier than iOS 8 only. Release iOS 8 and later always operate as if Network Roaming is ON, attempting to re-establish a connection until it succeeds.
- This parameter does not affect data roaming or the use of multiple mobile service providers.
- VPN configurations generated by the iPhone Configuration Utility do not support Network Roaming. If you require Network Roaming on iOS 8 or earlier, your connection entry must be configured manually or by an AnyConnect VPN profile.

Procedure

From the **Advanced** connection entry configuration screen, tap ON or OFF in the **Network Roaming** field.

Configure Certificate Use

Procedure

Step 1 From the **Advanced** connection entry configuration screen, tap **Certificate** to show the **Select Certificate** screen.

Step 2 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 the VPN client profile, and then authenticates using the certificate that matches the criteria. This occurs every time you establish a VPN connection.
- *Certificate Name*—Choose the certificate you would like to use. If you already have certificates available to AnyConnect (listed on this screen), select one to be associated with this VPN connection. If not, you must import certificates.

  Note In AnyConnect release 4.0.05x or earlier, certificates are openly shared between the device's certificate store and AnyConnect.

  For AnyConnect release 4.0.07x or later, you must import certificates into the AnyConnect certificate store before they are available to choose.

Step 3 Tap **Advanced** to return to the advanced configuration window.

Configure Connect on Demand

Configure the Connect on Demand functionality by creating lists of rules that are checked when other applications initiate network connections. When matched, these rules result in one of the following Connect On Demand behaviors:

- **Never Connect—** iOS will never attempt to initiate a VPN connection when rules in this list are matched. Rules in this list take precedence over all other rules.

  When Connect On Demand is enabled, AnyConnect automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you access the server's clientless portal on a web browser. Remove this rule if you do not want this behavior.

- **Connect if Needed—** iOS will attempt to initiate a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.

- **Always Connect—**On Apple iOS 6, iOS will always attempt to initiate a VPN connection when rules in this list are matched. On iOS 7.x, Always Connect is not supported, when rules in this list are matched they behave as "Connect If Needed" rules. On later releases, "Always Connect" is not used, configured rules are moved to the "Connect If Needed" list and behave as such.

These rules consist of lists of host names (host.example.com), domains (.example.com), or partial domains (.internal.example.com), but cannot include IP addresses (10.0.0.1). 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

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 and Connect on Demand is enabled.

- AnyConnect fails to match the domain request to a string in the **Never Connect** list.
- Either of the following is true:
  - AnyConnect matches the domain request to a string in the **Always Connect** list.
  - A DNS lookup failed, and AnyConnect matches the domain request to a string in the **Connect if Needed**.

Note 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 https://support.apple.com/en-us/HT203743 documentation for more information.

Before You Begin

- The connection entry must be configured to authenticate using a valid certificate, see Configure Certificate Use, on page 8 for details.
- The connection entry must be one created by the user. Users cannot configure connect on demand in connection profiles downloaded from the ASA.

Procedure

Step 1 From the **Advanced** connection entry configuration screen, tap ON next to **Connect On Demand**.

Step 2 Tap **Domain List**.

Step 3 To add domains do one of the following:

- Tap **Add Domain** under the Always Connect, Never Connect, or Connect if Needed sections to add a domain string to that list. The Domains screen 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 screen to add, edit, or delete domain strings.
  - To move a domain name from one list to another, touch the triple-bar to the right of the domain entry and drag it to the area below the title of the destination list.
  - To delete a domain name, tap the red circle to the left of the domain name, then tap **Delete** to the right of the domain.

Step 4 Tap **Save**.

Configure IPsec

Procedure

Step 1 From the **Advanced** connection entry configuration screen, 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.

Step 2 (Optional) Tap **Authentication** and choose the authentication method for this IPsec connection:

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

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

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

Step 4 (Optional) Tap **IKE Identity** to enter the required client identity. This is provided by your administrator.

Delete a Connection Entry

This procedure deletes a manually configured VPN connection entry. The only way to remove a connection entry imported from a VPN secure gateway is to remove the downloaded AnyConnect profile that contains the connection entries.

Procedure

Step 1 From the AnyConnect home screen, tap the detail disclosure button to the right of the VPN connection entry.

Step 2 Tap **Delete VPN Connection**.

Configure Certificates

About 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, and 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 to authenticate to the secure gateway using a digital certificate, a user certificate must be imported and configured for VPN use.

User certificates are imported using one of the following methods, as directed by your administrator:

- Import Certificates Attached to Emails, on page 12
- Import Certificates From Hyperlinks, on page 13
- Import Certificates Manually, on page 13
- Import Certificates Provided by a Secure Gateway, on page 14

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

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. It can only be 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.

Import Certificates Attached to Emails

Before You Begin

Your administrator must email you a certificate to use for authentication.

Procedure

Step 1 Tap the icon for the attached certificate.

Apple iOS recognizes that you have just opened a certificate and 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.

Import Certificates From Hyperlinks

Before You Begin

Ensure that **External Control** is set to either **Prompt** or **Enable** within the AnyConnect settings to allow this activity. See Control the External Use of AnyConnect, on page 16 for more information.

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

Procedure

Step 1 Tap the hyperlink provided by your administrator.

Step 2 If you are prompted, provide the authentication code for the certificate and Tap **Next**.
Apple iOS imports the certificate and displays a certificate enrollment message.

Import Certificates Manually

Before You Begin

Your administrator must provide you with the URL for a certificate.

Procedure

Step 1 From the AnyConnect home screen tap **Diagnostics** > **Certificates**.

Step 2 Tap the **User** tab.

Step 3 Tap **Import User Certificate** to manually import a certificate.

Step 4 Enter the URL provided by your administrator.

Import Certificates Provided by a Secure Gateway

Before You Begin

Your administrator must provide you with the name of a connection entry configured to distribute certificates using the SCEP protocol.

Procedure

Step 1 From the AnyConnect home screen, in the **Choose a connection** area, tap the name of the connection capable of downloading a certificate to your mobile device.

Step 2 Tap the AnyConnect **On** button.

Step 3 If present, tap **Get Certificate**, or select the group configured to download a certificate to your mobile device.

Step 4 Enter authentication information provided by your administrator.
The secure gateway downloads the certificate to your device, your VPN session is disconnected, and you receive a message that certificate enrollment was successful.

Step 5 Tap **OK**.

What to Do Next

AnyConnect can now use the certificate automatically or you can assign it to specific connection entries. See Configure Certificate Use, on page 8 for details.

View and Delete Certificates

Procedure

Step 1 From the AnyConnect home screen tap **Diagnostics > Certificates**.

Step 2 Tap the **User** tab to view user certificates in the AnyConnect certificate store.
Tap **Edit** to delete a single certificate or tap **Delete All User Certificates** to delete all user certificates.

Step 3 Tap the **Server** tab to view server certificates in the AnyConnect certificate store.
Tap **Edit** to delete a single certificate or tap **Delete All Server Certificates** to delete all server certificates.

Establish a VPN Connection

Before You Begin

- You must have an active Wi-Fi connection, or a connection to your service provider to connect to a VPN.
- To initiate a VPN connection, you must have at least one connection entry listed under Choose a Connection on your AnyConnect home window.
- To complete a VPN connection, you must have the authentication information expected by your secure gateway.

Procedure

Step 1 On the AnyConnect home screen 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 2 Tap **ON** next to **AnyConnect VPN**.

Step 3 If necessary, use the credentials supplied by your system administrator to log in.

Step 4 If instructed by your system administrator to do so, tap **Get Certificate**.

Step 5 If necessary, tap **Connect**.
Depending on the secure gateway configuration, AnyConnect may retrieve connection entries and add them to the **Connections** list.

The VPN icon is shown in the status bar and the VPN is shown as `Connected`.

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

Respond to AnyConnect Notifications

Respond 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 **Block Untrusted VPN Server**, re-initiate the VPN connection.
- If not enabled, a nonblocking **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 option 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.

Respond to Another App

To protect your device, AnyConnect alerts you when an external app attempts to use AnyConnect. This occurs when the AnyConnect application preference **External Control** is set to **Prompt**.

Ask your administrator whether to tap **Yes** in response to the following prompts:

- `Another application has requested that AnyConnect create a new connection to host. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect connect to host. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import localization files. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import profiles. Do you want to allow this? [Yes | No]`

Optional AnyConnect Configuration and Management

Control the External Use of AnyConnect

The External Control application setting specifies how the AnyConnect application responds to external URI requests. External requests create connection entries; connect or disconnect a VPN; and import client profiles, certificates, or localization files.

External requests are typically provided by your administrator in emails or on web pages. Your administrator will instruct you to use one of the following values:

- Enabled—The AnyConnect application automatically allows all URI commands.
- Disabled—The AnyConnect application automatically disallows all URI commands.
- Prompt—The AnyConnect application prompts you each time an AnyConnect URI is accessed on the device. You allow or disallow the URI request. See Respond to Another App, on page 15 for details.

Procedure

Step 1 In the AnyConnect app, tap **Settings**.
Step 2 Tap **External Control**.
Step 3 Tap **Enabled**, **Disabled**, or **Prompt**.
Step 4 Tap **Settings** to return to the Settings screen.

Block Untrusted Servers

This application setting determines if AnyConnect blocks connections when it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF, but 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.

Procedure

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

Step 2 Tap the **Block Untrusted Servers** checkbox to enable or disable this preference.

Set FIPS Mode

FIPS Mode makes use of Federal Information Processing Standards (FIPS) cryptography algorithms for all VPN connections.

Before You Begin

Your administrator will inform you if you need to enable FIPS mode on your mobile device for connectivity to your network.

Procedure

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

Step 2 Tap **FIPS Mode** to enable or disable this preference.

Manage the VPN Profile

VPN profile management on your device should be carried out based on instructions provided by your administrator.

The AnyConnect VPN Client Profile is an XML file downloaded from the secure gateway 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 manually on the device, are available to choose from when initiating a VPN connection.

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

Procedure

Step 1 From the AnyConnect home page, tap **Diagnostics** > **Profile**.

Step 2 Choose:

- **Import Profile—**to specify the URL of a VPN profile to import.
- **Delete Profile—**to delete the current VPN profile from the device.

  Note If you reconnect to the domain, IP address, or Group URL of the same ASA, AnyConnect reloads the VPN profile and re-enforces the security policies.
- **Show Profile—**to show or hide the current VPN profile on your device.

Managing Localization

Viewing Installed Localization Data

Upon AnyConnect installation, your mobile device is localized if the device's specified locale matches one of the packaged language translations. The following language translations are included in the AnyConnect package:

- Canadian French (fr-ca)
- Chinese (Taiwan) (zh-tw)
- Czech (cs-cz)
- Dutch (nl-nl)
- French (fr-fr)
- German (de-de)
- Hungarian (hu-hu)
- Italian (it-it)
- Japanese (ja-jp)
- Korean (ko-kr)
- Latin American Spanish (es-co)
- Polish (pl-pl)
- Portuguese (Brazil) (pt-br)
- Russian (ru-ru)
- Simplified Chinese (zh-cn)
- Spanish (es-es)

The installed language is determined by the locale specified in **Settings** > **General** > **International** > **Language**. AnyConnect UIs and messages are translated as soon as AnyConnect starts.

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.

Procedure

Step 1 In the AnyConnect app, tap **Diagnostics** > **Localization**.

Step 2 View the list of Localization Files installed on your mobile device.

The indicated language is the one currently being used by AnyConnect.

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 can provide a hyperlink in email, or on a web page, that imports localization data when clicked. This method uses the AnyConnect URI handler, a feature available to administrators for simplifying AnyConnect configuration and management.

  Note You must allow this AnyConnect activity by setting External Control to either Prompt or Enable within the AnyConnect settings. See Control the External Use of AnyConnect, on page 16 for how to set this.

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

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

- Manually imported using the **Import Localization** option on the AnyConnect Localization Management Activity Screen as described below.

Procedure

Step 1 In the AnyConnect app, tap **Diagnostics** > **Localization**.

Step 2 Tap **Import Localization**.

Step 3 Specify the address of the secure gateway and the locale.
The locale is specified per ISO 639-1, with the country code added if applicable (for example, en-US, fr-CA, ar-IQ, and so on).

You will be notified that the `Localization file has been successfully imported`.

This localization data is used in place of the pre-packaged, installed localization data.

Restoring Localization Data

Procedure

Step 1 In the AnyConnect app, tap **Diagnostics** > **Localization**.

Step 2 Tap **Restore Localization**.

Restores the use of the pre-loaded localization data from the AnyConnect package and deletes all imported localization data.

The restored language is chosen based on the device's locale specified in **Settings** > **General** > **International** > **Language**.

Remove AnyConnect

Procedure

Step 1 From the AnyConnect home page, tap **Diagnostics** > **Profile** > **Delete Profile**.
Step 2 (Optional) From the AnyConnect home page, tap **Diagnostics** > **Certificates** > **Delete Certificates**.
Step 3 Return to the device's home screen.
Step 4 If you placed AnyConnect in a folder, open the folder.
Step 5 Tap and hold the AnyConnect icon until a delete (X) icon appears above it.
Step 6 Tap the delete icon.

Monitor and Troubleshoot AnyConnect

Display the AnyConnect Version and Licenses

Procedure

From the AnyConnect home screen, tap **About**.

What to Do Next

Tap the link in the **About** window to open the latest version of this guide.

View AnyConnect Statistics

AnyConnect records statistics when a VPN connection is present.

Procedure

From the AnyConnect home screen, tap **Details** > **Statistics**.

Detailed statistics include the following values:

- 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.
- Non-Secure Routes—Shown only if 0.0.0.0/0.0.0.0 is present under SecureRoutes.Traffic destinations, as determined by the VPNsecure gateway, that are excluded from the encryptedconnection.

View System Information

Procedure

From the AnyConnect home screen, tap **Diagnostics** > **System Information**.

View and Manage Log Messages

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

Procedure

Step 1 From the AnyConnect home screen, tap **Diagnostics**.

Step 2 Turn **VPN Debug Logs** on to enable logging.

Step 3 Tap **Logs**.

Step 4 Choose:

- **Messages—**to display the log messages. Scroll to view additional messages.
- **Service—**to display the service debug log messages. Scroll to view additional messages.
- **App—**to display the application debug log messages. Scroll to view additional messages.
- **Clear Logs—**to remove all log messages.
- **Diagnostics—**to return to the Diagnostics screen.

Send Log Messages

Before You Begin

You must have an email account configured on your device and **VPN Debug Logs** must be ON.

Procedure

Step 1 From the AnyConnect home screen, tap **Diagnostics** > **Email Logs**.

Step 2 Describe the problem, the steps to reproduce it, and tap **Send**.

Step 3 Choose to send the logs to your **Administrator** or to **Cisco** and deliver it using your email application.

Common Apple iOS Problems

This topic describes solutions to common problems. If problems still persist after trying these solutions, 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**.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands