Release Notes for Cisco AnyConnect Secure Mobility Client 2.4, Apple iOS 4.2 and 4.3

Updated: April 05, 2011

Content

This document includes the following sections:

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

Introduction

This document provides only Apple iOS-specific information for the Cisco Secure Mobility client. This document supplements the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*; however, you can use the same Cisco adaptive security appliances (ASAs) to deploy later releases of AnyConnect for other devices simultaneously.

This release provides remote users with secure VPN connections to the Cisco ASA 5500 Series using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

This release provides seamless and secure remote access to enterprise networks. The client provides a full tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network. It runs on the Apple iPhone and iPad, and supports connections to IPv4 and IPv6 resources over an IPv4 network tunnel. The client installation software is available on the Apple iTunes App Store. The App store provides all AnyConnect for Apple iOS distributions and updates. The ASA does *not* provide AnyConnect for Apple iOS distributions and updates.

Devices Supported

This release supports the following Apple devices:

Device	Apple iOS Release Required
iPad	4.2.1 or later
iPhone 3G	4.1 or later
iPhone 3GS	4.1 or later
iPhone 4	4.1 or later
iPod Touch (2nd Generation or later)	4.1 or later

Security Appliances and Software Supported

Only ASA models support the Cisco AnyConnect Secure Mobility client for Apple iOS. See the *Adaptive Security Appliance VPN Compatibility Reference*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html for a complete list of compatibility requirements.

Table 1 shows the minimum Cisco ASA 5500 software images that support AnyConnect.

Table 1 Software Images that Support AnyConnect, Release 2.4.4 for Apple iOS 4.2.x and 4.3.x

Image Type	Version
ASA Boot image	8.0(4) or later
Adaptive Security Device Manager (ASDM)	6.1(3) or later

Note Routers running Cisco IOS VPN do not currently support AnyConnect for Apple iOS.

AnyConnect Licensing

AnyConnect for Apple iOS connections require the following licenses on the ASA:

- AnyConnect core license. You can satisfy this requirement with one of the following options, each which supports full client access from the desktop: Cisco AnyConnect Essentials license or Cisco AnyConnect Premium Clientless SSL VPN Edition license.
- AnyConnect Mobile license for mobile device access.

These licenses are mutually exclusive per ASA, but you can configure a mixed network. Both the AnyConnect Essentials and AnyConnect Mobile licenses are nominally priced to cover Cisco support. We offer the following trial options:

- If you have an AnyConnect Essentials or Premium license and you would like to obtain a three-month trial Mobile AnyConnect license, please go to the following website: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717
- If you would like to obtain both an AnyConnect Essentials or Premium license and an AnyConnect Mobile license, or you have questions about licensing, please email us a request with the **show version** output from your ASA to ac-mobile-license-request@cisco.com.

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see Cisco Secure Remote Access: VPN Licensing Overview.

For the latest details about the AnyConnect user license options, see Managing Feature Licenses in the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*.

What's New in AnyConnect 2.4.4014

The following sections list the fixes and open bugs in AnyConnect 2.4.4014.

Fixes In AnyConnect 2.4.4014

Release 2.4.4014 resolves the following bugs:

- CSCtd34579: CSD: Group-URL Fails w/ Pre-Login Policy & Hostscan

  If one used a group URL to establish a VPN connection to an ASA with a Cisco Secure Desktop pre-login policy containing an OS check, Host Scan was enabled, and the tunnel group associated with the group-url was disabled, the ASA assigned the DefaultWEBVPNGroup tunnel group to the connection. If the tunnel group associated with the group-url was enabled, AnyConnect displayed a drop-down selection list instead of establishing the VPN connection.

- The default connection timeout of 4 seconds was too short for mobile platforms. To resolve this issue, we increased it to 15 seconds.

Open Bugs in AnyConnect 2.4.4014

Release 2.4.4014 has the following remaining known bugs:

- CSCto11909: IPv6 traffic going in the clear when physical interface has IPv6 address

  If the physical interface on the Apple iOS device has both IPv6 and IPv4 addresses and the ASA does not provide an IPv6 address, the IPv6 traffic bypasses the VPN tunnel and attempts to use another access method available to the device.

  A possible workaround for iOS 4.2 is to tunnel the IPv6 traffic to the ASA by using an IPv6 address in the VPN configuration and configuring firewall rules on the ASA to reject the IPv6 traffic. This workaround does not work with iOS 4.3 because of an inability to install default routes, an issue with the OS.

- CSCti33259: Imported host entries may not clear when new profile is received.

  If the user connects to an ASA with a tunnel group that pushes a different client profile, AnyConnect may fail to replace the profile on the device.

  Workaround: If the user reconnects or establishes a new tunnel after the failure occurred, AnyConnect attempts to re-import the host entries and profile.

- CSCtj80031: Reconnects over WiFi will often take upwards of 3 minutes.

  When the iOS device wakes up from sleep, AnyConnect may try to establish a VPN connection at an inappropriate time because of known issues with Apple iOS, and the device appears to be stuck in a reconnecting state while it verifies connectivity.

  Workaround: Wait for the timeout and let AnyConnect reconnect on its own. Otherwise, manually disconnect and reconnect.

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 do not awaken the device. TLS packets, however, awaken the device if notifications or Facetime is enabled.
- 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.

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 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)
- IPv6 traffic if the ASA configuration does not assign an IPv6 address to the VPN endpoint of an Apple device running iOS 4.3 and its physical interface has an IPv6 address assigned.

  To tunnel the IPv6 traffic, configure the connection policy (that is, tunnel group) to assign an IPv6 address to the VPN endpoint.
- Core Apple services (for example, Visual Voice mail traffic)

New Features and Fixes In AnyConnect 2.4.4004

Release 2.4.4004 features the following enhancements and fixes:

- iPad support for Apple iOS 4.2.1 and later.
- iPhone support for Apple iOS 4.2.1 and later in addition to support for Apple iOS 4.1.
- Clear Profile Data—Lets users remove the hosts and policy settings that make up the AnyConnect profile imported from the ASA. The buttons are in the iPhone **Statistics > Diagnostics >** Diagnostics window and the iPad **Diagnostics >** Messages, Service, and App windows. If a user reconnects to the domain name, IP address, or Group URL of the same ASA, it reloads the profile and re-enforces the security policies.
- Application URI Handling—Lets other applications add VPN connection entries to the AnyConnect configuration, establish VPN connections, and disconnect from a VPN. See "Using the URI Handler to Automate AnyConnect Actions" on page 14 for instructions.
- Certificate Deletion— Users can use AnyConnect to delete any certificate imported via AnyConnect SCEP. To do so, swipe right on the Select Certificate window, the tap **Delete**. Users cannot use AnyConnect to delete certificates that were imported via IPCU or any source outside the AnyConnect application.

- Expanded Diagnostics and Logging—Enhanced the tools in the Diagnostics window formerly named “Troubleshooting.” These enhancements include:
  - Improvements to the usability of the log message view.
  - Removal of unnecessary log messages.
  - Separation of Application and Service level logs.
  - Device information added to the new email message that AnyConnect opens when you tap E-mail Logs.
  - Improved severity levels of log messages.
- Improved error reporting when connecting to HTTPS servers that are not secure gateways.
- Link in the About window that opens an updated iPhone or iPad user guide, depending on the device.
- Fixed crash when toggling Wi-Fi on or off.
- Performance improvements and bug fixes including smarter battery use if connecting to an ASA running releases to be announced.
- Fixes to certain situations where the tunnel would be disconnected when in a reconnecting state.
- Support for IPv6 resources accessed over the VPN connection.
- Support for a default search domain for the split DNS domain list. This fix resolves DNS domains in addition to the default search domain when using split tunneling without specifying split DNS domains. See DNS Resolution Behavior with Split DNS.
- Bandwidth graphs for the iPad.
- High contrast theme alternative to the Cisco default theme. Use the device menu button to return to the device desktop, tap **Settings**, tap **AnyConnect**, then tap the theme you want.

Other Supported Features

We support the following AnyConnect features in addition to those listed in the New Features and Fixes In AnyConnect 2.4.4004 section:

- Tunnel Protocols
  - Cisco SSL Tunneling Protocol (CSTP)
  - Cisco DTLS Tunneling Protocol (CDTP)
- SSL Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3

  - DES-CBC-SHA
- Authentication
- Client Certificate Authentication
- Routing Policy
  - Tunnel All
  - Split Include
  - Split Exclude
- Simultaneous full-tunnel and clientless connections
- Rekey
- Network Roaming
- TLS Compression
- Cisco Profile Support
- Profile Update
- IPv6 over IPv4
- Post-Login Banner
- Dead Peer Detection
- Tunnel Keep-Alive
- Backup Server List
- Default Domain
- Cluster Support
- DNS Server Configuration
- Private-side Proxy Support
- Network Change Monitoring
- Statistics
- Graphical User Interface
- Pre-login Banner
- AnyConnect Secure Certificate Enrollment Protocol (SCEP)
- Certificate Import
- The Cisco AnyConnect Secure Mobility client for Apple iOS is compatible with the Apple iOS Connect on Demand feature and certificates enrolled directly onto the device, including those enrolled with AnyConnect SCEP. For further details refer to the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

Note The SCEP references in this document apply exclusively to AnyConnect SCEP, not Apple iOS SCEP.

Limitations of the AnyConnect Secure Mobility Client for Apple iOS

This release of AnyConnect for Apple iOS supports only the features that are strictly related to remote access. It supports the following types of VPN configurations:

- Manually generated
- AnyConnect 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 XML 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 configuration profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.

This release supports the Tunnel Keep-Alive feature; however, it can reduce the battery life of the device. Increasing the update interval value can mitigate that issue.

Note AnyConnect 2.4.4 for Apple iOS does not support features introduced in later AnyConnect releases, such as AnyConnect 2.5.

Client Installation

Install the Cisco AnyConnect client from the Apple App Store. For further details, refer to one of the following guides:

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

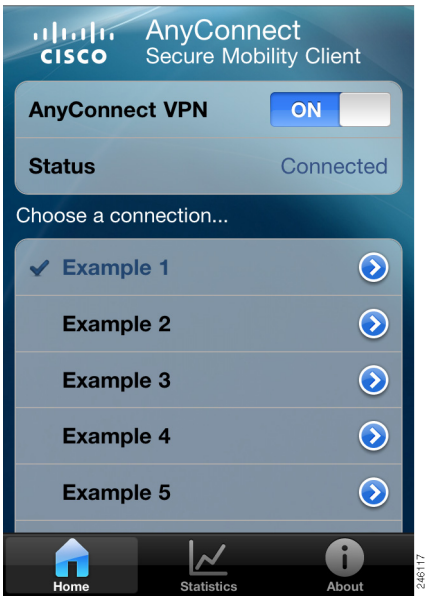
The installation instructions are the same, regardless of whether one is installing AnyConnect on the iPhone or iPad.

Client User Interface

The AnyConnect user interface for Apple iOS are designed to integrate tightly with the look and feel of Apple iOS.

If you tap the AnyConnect icon on iPhone or iPad desktop, the Home window opens. Figure 1 shows the Home Window for the iPhone.

Figure 1 iPhone AnyConnect Home Window



The Home window of both interfaces lists the names of the VPN connection entries stored on the device, and lets one add new VPN connection entries. The slider switch near the top lets one establish a VPN connection using the connection entry indicated by the check mark. The Status parameter shows the state of the VPN connection.

The icon bar at the bottom of each iPhone display provides navigation icons for the Home, Statistics, and About windows. The iPad Home window integrates these functions in a large window, rendering the icon bar unnecessary.

Figure 2 iPad AnyConnect Home Window

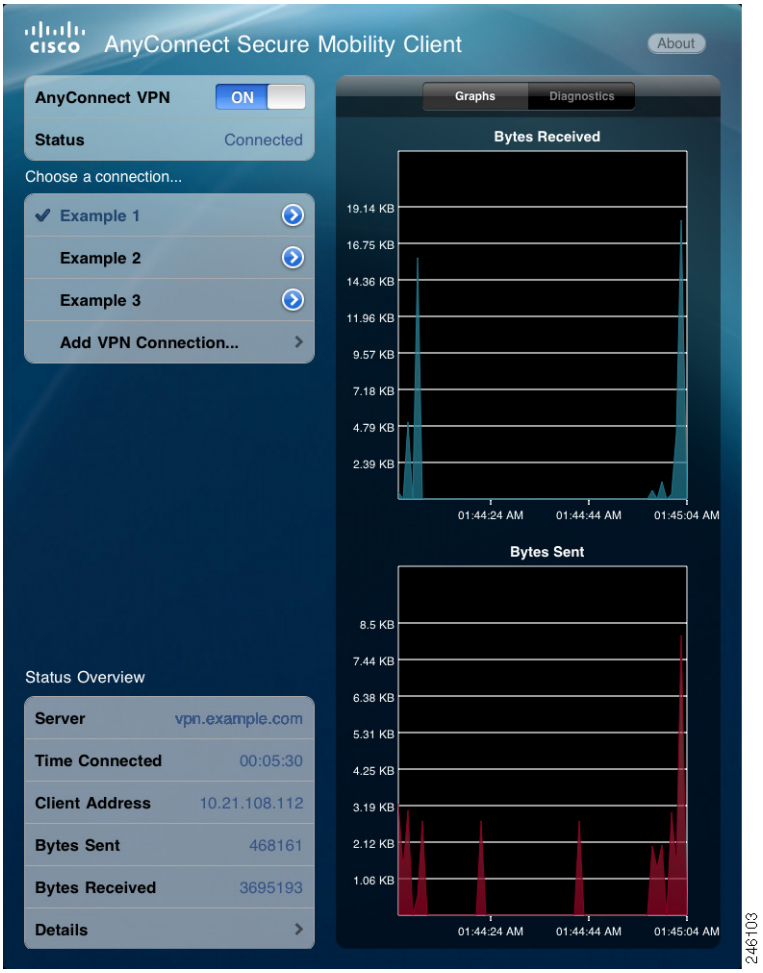


Table 2 shows the differences between AnyConnect for the iPhone and the iPad.

Table 2 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 window.	VPN Connection controls are in the upper left of the AnyConnect Home window. This window remains on-screen.
Statistics—Connection Status Overview	Tap the **Statistics** icon at the bottom of the iPhone AnyConnect window.	Status Overview panel in the lower left of the AnyConnect Home window.
Detailed Statistics	Tap **Details** in the Statistics window.	Tap **Details** in the Status Overview panel on the AnyConnect Home window.

Table 2 Differences between the iPhone and iPad AnyConnect UI

Feature	iPhone	iPad
About—Displays the AnyConnect version and licensing details, and link to the user guide.	Tap the **About** icon at the bottom of the AnyConnect window.	Tap **About** at the top right of the AnyConnect Home window.
Bandwidth graphs (bytes received and bytes sent).	This feature is the only AnyConnect for Apple iOS feature that we do not support on the iPhone. However, the Statistics window shows the Bytes Sent and Bytes Received in numerical form.	Tap **Graphs** near the top right of the home window. These graphs are present only when the AnyConnect Home window is the active window. If one returns to the Home window, AnyConnect displays "NO DATA" and restarts the recording of graphical data. The Bytes Sent and Bytes Received displayed in numerical form in the Statistics window are not subject to this limitation.

For AnyConnect operation instructions, refer to one of the following guides:

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

Configuration and Deployment Overview

At minimum, AnyConnect requires the user to create a connection entry that requires the following:

- Description—uniquely identifies one VPN connection from another.
- Server address— Fully qualified domain name or IP address of the destination, including the URL path if the ASA VPN configuration specifies the group URL.

AnyConnect Profiles

An AnyConnect client user profile is an XML file that lets you identify a list of secure gateways (security appliances) that you want to make accessible. In addition, a profile conveys additional connection attributes and constraints on a user. Users cannot modify AnyConnect profiles; however, beginning with this release, they can delete them.

You can use the AnyConnect Profile editor to configure the client features within the profile; then configure the security appliance to upload this file when Apple iOS connect to the VPN.

Typically, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. The client will download the profile from the head-end and create VPN connections based on the host entries in the profile.

Note AnyConnect retains only one profile on the Apple iOS device at a time. However, a profile can consist of multiple connection entries.

Connection Persistence

AnyConnect for Apple iOS supports a full suite of authentication capabilities similar to AnyConnect for Windows, Mac OS X, and Linux.

To achieve the most transparent end user experience, use certificate-only authentication. When a digital certificate is issued, AnyConnect supports the Apple iOS Connect On Demand feature which enables a VPN connection to be established without user interaction. The user may also manually establish a connection.

Apple iOS Connect On Demand

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

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

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

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

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

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

The Connect-on-Demand rules support only domain names, not IP addresses. However, the domain names specified within the rules may be partial or whole domain strings.

Note The integrated Apple iOS IPsec client and AnyConnect both use the same Apple iOS VPN on Demand framework.

See "Setting Up Connect-On-Demand Rules" in the user guide or "Using the URI Handler to Generate a VPN Connection Entry" later in this document for instructions.

Network Roaming

Network Roaming, also called "reconnect," determines whether to observe a limit on the time it takes to reconnect after the device wakes up or changes in the connection type (e.g., EDGE, 3G, Wi-Fi) occur. Providing seamless mobility with a secure connection that persists across networks is useful for applications that require a connection to the enterprise.

If Network Roaming is enabled and AnyConnect loses a connection, it does not limit the time it takes to try to reconnect, so this feature could consume more battery life.

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

Policies that restrict VPN traffic could prevent the device from accessing non-corporate Internet resources. If enabled, Network Roaming requires a policy on the ASA that supports a persistent connection.

If Network Roaming is disabled and AnyConnect loses a connection, it tries to re-establish a connection for 20 seconds. The user or application must then start a new VPN connection if one is necessary.

By default, AnyConnect sends all network traffic over the VPN connection. You can enable a split tunneling policy to control traffic flow, directing traffic appropriate for the tunnel and traffic appropriate for the data network. For instructions, refer to the ASA Configuration Guide.

Recommended ASA Configurations

For the best user experience, Cisco recommends using multiple tunnel-groups for mobile devices, depending on the authentication configuration. You will have to decide how best to balance user experience with security.

- For certificate-based authentication tunnel-groups for mobile devices that have Connect on Demand configured, the tunnel-group should have an idle timeout (vpn-idle-timeout) specified that is very short (such as 60 seconds). You may want to set the idle timeout if your VPN session is not critical for an application and does not need to be connected all the time. This allows the Apple device to close the VPN connection when it is no longer needed, for example when the device goes into sleep mode. The default time-out for an idle tunnel-group is 60 minutes.
- For AAA-based authentication tunnel-groups for mobile devices, the tunnel-group should have a very long idle-timeout, such as 24 hours, to let the client remain in a reconnecting state without requiring the user to re-authenticate.

DNS Resolution Behavior with Split DNS

The ASA split tunneling feature lets you specify which traffic goes over the VPN tunnel and which goes in the clear. An associated feature, called split DNS, lets you lets you specify which DNS traffic is eligible for DNS resolution over the VPN tunnel and which DNS traffic the endpoint DNS resolver handles.

AnyConnect for Apple iOS supports the optional **split-dns** command to specify the DNS queries to resolve; however, the command works differently than it does on other devices if you also configure split tunnel VPN.

The **split-dns** command, entered in group-policy configuration mode, lists the domains to be resolved through the VPN session, as follows:

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
```

If the **split-dns** command is not present, the group policy inherits any that are present in the default group policy. To prevent inheriting a split tunneling domain list, use the **split-dns none** command.

AnyConnect for Apple iOS responds to this command, as follows:

- Encrypts only DNS queries for domains in the **split-dns** list—AnyConnect tunnels only the DNS queries for the domains specified in the command, and sends all other DNS to the local DNS resolver for resolution in-the-clear. For example, AnyConnect tunnels only the DNS queries for example1.com and example2.com in response to the following command:

  ```
  hostname(config-group-policy)# split-dns example1.com example2.com
  ```

- Encrypts only DNS queries for the domain in the **default-domain** command—If the **split-dns none** command is present and the **default-domain** command specifies a domain, AnyConnect tunnels only DNS queries for that domain, and sends all other DNS to the local DNS resolver for resolution in-the-clear. For example, AnyConnect tunnels only the DNS queries for example1.com in response to the following commands:

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```

- Sends all DNS queries in the clear—If the **split-dns none** and **default-domain none** commands are present in the group policy; or these commands are absent from the group policy but present in the default group policy, AnyConnect sends all DNS to the local DNS resolver for resolution in-the-clear.

Using the URI Handler to Automate AnyConnect Actions

The URI handler supported by Apple lets applications pass action requests in the form of Universal Resource Indicator (URIs). You can use URIs to generate VPN connection entries, connect to a VPN, and disconnect.

You can insert the URIs into webpages or applications. Example uses of this feature include:

- Creating a webpage for Apple iOS users to visit to configure the client. Use this method to simplify the AnyConnect user setup process.
- Let applications other than AnyConnect start VPN connections to access internal resources as needed, then disconnect.

As a security measure, AnyConnect prompts the user whenever an application uses the URI handler to pass an action it supports. Please instruct users of the conditions under which they can tap **OK** in response to the prompt if you set up URI handling. The actions and associated prompts are as follows:

- 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?"

The following sections show the syntax, examples, and parameter descriptions of the supported actions.

Note The introduction to each set of parameter descriptions shows the action name in what appears to be a hypertext link. If you hover your cursor over it, an example of the action appears embedded within the word. Of course, you might want to encode the action within a term or expression that is more meaningful to your users, such as:

> Tap here to save a *YourCompanyName* VPN connection entry to your iPhone or iPad. Then, to establish a VPN connection at any time, you can open AnyConnect, tap the **YourCompanyName** name in the connection list, and tap **ON** next to "AnyConnect VPN." Tap **OK** in response to the prompt, "Another application has requested that AnyConnect create a new connection to *host*. Do you want to allow this?"

Using the URI Handler to Generate a VPN Connection Entry

You can use the AnyConnect URI handler create action to simplify the generation of an AnyConnect connection entry for users.

Insert a separate link for each connection entry you want to add to the device. We do not support multiple create actions in a single link.

Use the following syntax to insert the create action to add an AnyConnect connection entry to the endpoint configuration:

anyconnect:[**//**]**create**[**/**]**?name=***Description***&host=***ServerAddress*[**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

Examples:

anyconnect://create/?name=*SimpleExample*&host=vpn.example.com

anyconnect:create?name=*SimpleExample*&host=vpn.example.com

anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true&usecert=false

anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true&domainlistalways=email.example.com,pay.examplecloud.com&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com

The slashes (/) are optional. The create action requires that you specify the `name` and `host`, the minimum required to create an AnyConnect record. All other parameters are optional. When the action runs on the device, AnyConnect saves all of the parameter values you enter to the connection entry associated with that `name` and `host`. Enter the parameter values, as follows:

- **name**—unique name for the connection entry to appear in the connection list of the AnyConnect home window and the Description field of the AnyConnect connection entry. AnyConnect responds only if the name is unique. We recommend using a maximum of 24 characters to ensure they fit in the connection list. You can use any letters, numbers, or symbols on the keyboard displayed on the device when you enter text into a field. The letters are case-sensitive. To indicate a space, you must enter **%20**. For example, to name a connection entry `Example Connection 1`, enter **Example%20Connection%201**.
- **host**—Enter the domain name, IP address, or Group URL of the ASA with which to connect. AnyConnect inserts the value of this parameter into the Server Address field of the AnyConnect connection entry. For example,

  `vpn.example.com`

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

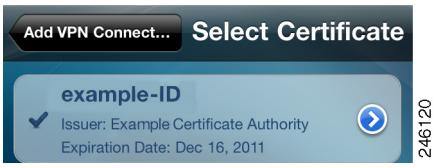
  Note This parameter does *not* affect data roaming or the use of multiple mobile service providers.

  The valid values are:

  - true—(Default) This option optimizes VPN access. AnyConnect inserts the value ON into the Network Roaming field of the AnyConnect connection entry. 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.
  - false—This option optimizes battery life. AnyConnect associates this value with the OFF value in the Network Roaming field of the AnyConnect connection entry. If AnyConnect loses a connection, it tries to establish a a new one for 20 seconds and then stops trying. The user or application must start a new VPN connection if one is necessary.

- **usecert** (optional)—Determines whether to use a digital certificate preinstalled on the device when establishing a VPN connection to the `host`. The valid values are:
  - true—This option enhances network security access, and is required for Connect on Demand. AnyConnect inserts the value ON into the Use Certificates field of the AnyConnect connection entry. AnyConnect then uses a digital certificate while establishing a VPN connection with the `host`. You must enter this option if the `host` configuration requires the use of a digital certificate for VPN access. AnyConnect uses this value only if you specify a `certcommonname`.
  - false (default)—Use this option if VPN access does not require a digital certificate. AnyConnect associates this value with the OFF value in the Use Certificates field of the AnyConnect connection entry.
- **certcommonname** (optional, but requires the `usecert` parameter)—Matches the Common Name of a valid certificate pre-installed on the device. AnyConnect inserts the value into the Selected Certificate field of the AnyConnect connection entry. To view this value on a certificate installed on the device, tap the icon to the right of a connection entry, tap **On** next to Use Certificates, and tap the Selected Certificate field. AnyConnect displays the value in bold in the first line of the certificate associated with the issuer. The common name of the following example certificate is `example-id`.

Figure 3 Select Certificate Window



You might need to scroll to view the certificate required by the `host`. You can also tap the icon to the right of the certificate summary record to view the Common Name parameter read from the certificate, as well as the other values.

- **useondemand** (optional, but requires the `usecert` and `certcommonname` parameters)—Determines whether applications, such as Safari, can start VPN connections.
  - true—Lets an application use Apple iOS to start a VPN connection. If you set the useondemand parameter to true, AnyConnect inserts the value ON into the Connect on Demand field of the AnyConnect connection entry.
  - false (Default)—Prevents applications from starting a VPN connection. Using this option is the only way to prevent an application that makes a DNS request from potentially triggering a VPN connection. AnyConnect associates this option with the OFF value in the Connect on Demand field of the AnyConnect connection entry.
- **domainlistnever** (optional)—Lists the domains to evaluate for a match to disqualify the use of the Connect on Demand feature. This list is the first one AnyConnect uses to evaluate domain requests for a match. If a domain request matches, AnyConnect ignores the domain request. AnyConnect inserts this list into the Never Connect field of the AnyConnect connection entry. 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`.
- **domainlistalways** (optional, but required with the `useondemand` parameter)—Lists the domains to evaluate for a match for the Connect on Demand feature. This list is the second one AnyConnect uses to evaluate domain requests for a match. If an application requests access to one of the domains specified by this parameter and a VPN connection is not already in progress, Apple iOS attempts to establish a VPN connection. AnyConnect inserts this list into the Always Connect field of the AnyConnect connection entry. An example value list is `email.example.com,pay.examplecloud.com`.
- **domainlistifneeded** (optional)—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. AnyConnect inserts this list into the Connect if Needed field of the AnyConnect connection entry. The most common use case for this list is to obtain brief access to an internal resource that is not accessible in a LAN within the corporate network. An example value is `intranet.example.com`.

Use a comma-delimited list to specify multiple domains. The Connect-on-Demand rules support only domain names, not IP addresses. However, AnyConnect is flexible about the domain name format of each list entry, as follows:

Figure 4 AnyConnect Domain Matching

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

Using the URI Handler to Establish a VPN Connection

Use either syntax expression to insert the connect action:

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]
anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress*

Examples:

```
anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
```

The slashes (/) are optional. The connect action requires either the `name` and `host` parameters, but allows both. Otherwise, if all the parameter values in the statement match those of an AnyConnect connection entry on the device, Apple iOS uses the remaining parameters in the record to establish the connection. If AnyConnect does not match all parameters in the statement to those in a connection entry and the name parameter is unique, it generates a new configuration record. Apple iOS then attempts the VPN connection. Enter the parameter values, as follows:

- **name**—Name of the connection entry as it appears in the connection list of the AnyConnect home window. AnyConnect evaluates this value against the Description field of the AnyConnect connection entries, also called `name` if you used the previous instructions to generate the record on the Apple iOS device. The value is case-sensitive; AnyConnect does not match this field if the case of the letters in the statement differ from those in the connection entries. To match a space, enter **%20**. For example, to match a connection entry named `Example Connection 1`, enter **Example%20Connection%201**.
- **host**—Enter the domain name, IP address, or Group URL of the ASA to match the Server Address field of an AnyConnect connection entry, also called the host if you used the previous instructions to generate the record on the Apple iOS device.

Using the URI Handler to Disconnect from a VPN

Use the following syntax to insert the disconnect action:

```
anyconnect:[//]disconnect[/]
```

Examples:

```
anyconnect://disconnect/
anyconnect:disconnect
```

The slashes (/) are optional. The disconnect action takes no parameters.

Other Apple iOS Specific Considerations

The following considerations should be taken into account to support AnyConnect on Apple iOS devices:

- You can use the iPhone Configuration Utility, available from Apple for Windows or Mac OS X, to create and deploy configurations to an Apple iOS device.
- Apple iOS does not support discerning between trusted and untrusted networks. The Apple iOS Connect On Demand feature will start a VPN connection when a user attempts to access any destination with a hostname specified in the appropriate domains list. For example, if '.example.com' is in the Always Connect list, when a user goes to internal.example.com, the client will start a VPN connection regardless of the network to which the device is currently connected.
- We recommend using the Connect if Needed option if you configure rules. A Connect if Needed rule initiates a VPN connection if the DNS lookup to an internal host fails. It requires a correct DNS configuration so that host names within the enterprise are only resolved using internal DNS servers.
- The tunnel-group group policy svc keepalive should be switched off to conserve battery life.
- Server-sided DPD should be switched off as it will prevent the device from sleeping. However, client-side DPD should remain switched on as it will enable the client to determine when the tunnel is terminated due to a lack of network connectivity.

Note Push email notifications do not work via VPN because of Apple iOS constraints. However, one can use AnyConnect in parallel with externally accessible ActiveSync connections, which the tunnel policy can exclude from the session.

Troubleshooting

Please enable logging on the device and follow the user troubleshooting steps in either of the following guides:

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

The user troubleshooting steps are the same for the iPhone and iPad, although the user interfaces do differ. If you are unable to resolve the issue by following those steps, try the following:

- Check to see if the same problem occurs with the desktop client.

- Ensure the AnyConnect Mobile license is installed on the ASAs. See AnyConnect Licensing on page 3 for more information.
- If the VPN connection is not restored after the device wakes up, ensure Network Roaming is enabled and that Auto-Reconnect is enabled in the profile.
- If certificate authentication fails, ensure the correct certificate has been selected. Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage. Ensure the certificate matching rules in the AnyConnect profile are not filtering out the user's selected certificate. Even if a user has selected a certificate, the certificate will not be used for authentication if it does not match the filtering rules in the profile. If your authentication mechanism uses any associated accounting policy to an ASA, verify that the user can successfully authenticate. If problems persist, enable logging on the client and enable debug logging on the ASA.
- If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a Group URL and ensure that secondary authentication is not configured for the tunnel group. For further details refer to your ASA Administrator Guide.

If Apple iOS prompts you to start a connection using the AnyConnect application when certificate authentication and the Apple iOS Connect On Demand feature are configured for the connection, configure the connection to use a Group URL. Both a Group URL and certificate-only authentication are requirements for Connect on Demand.

Preventing Apple iOS Devices from Establishing SSL VPN Connections

An ASA must be activated with an AnyConnect Mobile license to support Apple iOS SSL VPN connections. If an ASA is not activated with an AnyConnect Mobile license, it automatically denies these connection attempts.

By default, an ASA activated with an AnyConnect Mobile license lets any user who can authenticate log in from an Apple iOS device running AnyConnect. You can configure an ASA to prevent these connections; however, at this time, doing so requires both of the following:

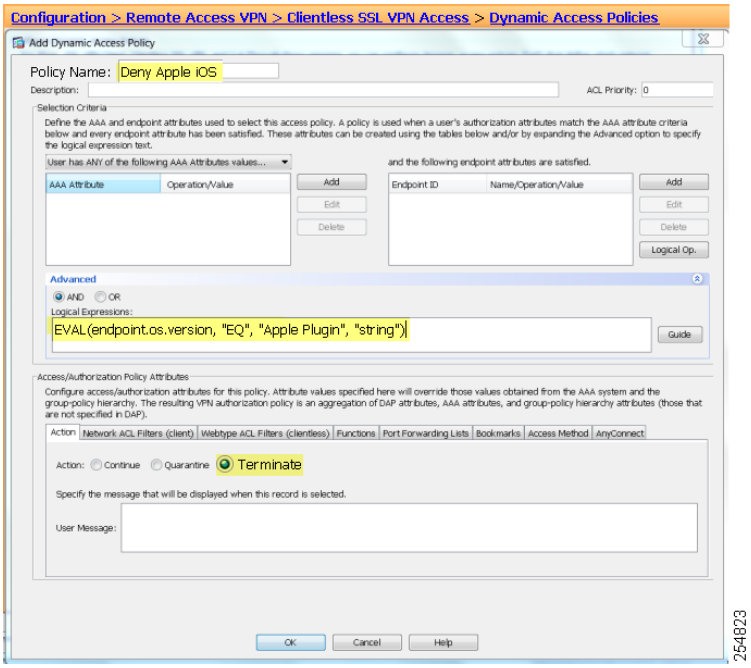
- The ASA must be activated with an AnyConnect Premium license. This is a technical requirement. We are considering an enhancement request to eliminate it.
- CSD must be enabled.

To configure an ASA to prevent SSL VPN connections from Apple iOS, add a dynamic access policy, as follows:

Step 1 Establish an ASDM session with the ASA.

Step 2 Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add**.

Figure 5 DAP to Prevent SSL VPN Connections from Apple iOS Devices



Step 3 Name the policy (for example, `Deny Apple iOS`).

Step 4 Click **Advanced**.

Step 5 Enter the following into the Logical Expressions text box:

```
EVAL(endpoint.os.version, "EQ", "Apple Plugin", "string")
```

Step 6 Click **Terminate** under the Action tab.

Step 7 Click **OK** and **Apply**.

AnyConnect Support Policy

Cisco supports all AnyConnect software versions downloaded from the iTunes App Store; however, fixes and enhancements are provided only in the most recently released version. Cisco is not able to provide earlier versions of AnyConnect for Apple iOS as only the most recently released version is available from the iTunes App Store.

End-User License Agreement

For the end-user license agreement, go to:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

OpenSSL Project

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).

For Open Source License information for this product, please see the following link: http://www.cisco.com/en/US/docs/security/asa/asa83/license/opensrce.html#wp50053.

Related Documentation

For more information, refer to the following documentation:

- *iPhone User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4.4*

  http://www.cisco.com/US/docs/security/vpn_client/anyconnect/anyconnect24/ios4.2-user/guide/iphone-ugac-ios4.2.html

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

  http://www.cisco.com/US/docs/security/vpn_client/anyconnect/anyconnect24/ios4.2-user/guide/ipad-ugac-ios4.2.html

- *Release Notes for Cisco AnyConnect VPN Client Release 2.4:*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/release/notes/anyconnect24rn.html

- *Cisco AnyConnect VPN Client, Release 2.4, Administrator Guide*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/anyconnectadmin24.html

- *Navigating the Cisco ASA 5500 Series Documentation*:

  http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Additional information on using VPN connections with Apple iOS devices is available from Apple:

- http://developer.apple.com/library/ios/search/?q=VPN+Server+Configuration
- http://support.apple.com/kb/HT1424
- http://images.apple.com/iphone/business/docs/iPhone_VPN.pdf

---