Release Notes for Cisco AnyConnect VPN Client, Release 2.4, for Apple iOS

Updated: October 28, 2010

Contents

This document includes the following sections:

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

Overview

This document is intended as a supplement to the *Cisco AnyConnect 2.4 Administrator Guide* and includes only Apple iOS specific information. For additional information refer to the following topics in the 2.4 Administrator Guide:

- Chapter 3: Configuring AnyConnect Client Features
  - Configuring and Deploying the AnyConnect Client Profile
  - Configuring Simplified Certificate Enrollment Protocol
  - Configuring Certificate Matching
  - Prompting Users to Select Authentication Certificate
  - Configuring Backup Server List Parameters
  - Configuring Auto Reconnect
  - Configuring a Server List
  - Proxy Support
  - Configuring Other AnyConnect Profile Settings
- Chapter 8: Managing, Monitoring, and Troubleshooting AnyConnect Sessions
  - Disconnecting All VPN Sessions
  - Disconnecting Individual VPN Sessions
  - Viewing Detailed Statistical Information
  - Resolving VPN Connection Issues
- Additional tools and information on deploying iOS devices in an enterprise environment are available from Apple at http://www.apple.com/support/iphone/enterprise/.

Introduction

The Cisco AnyConnect Secure Mobility Client 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.

The Cisco AnyConnect Secure Mobility Client for Apple iOS 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 Apple iOS version 4.1 or later and supports connections to IPv4 and IPv6 resources over an IPv4 network tunnel. It is available from the iTunes App Store. All distribution and updates will be provided from the App Store, not the ASA.

The user interface of the application has been designed to integrate tightly with the look and feel of Apple iOS.

Devices Supported by Cisco AnyConnect 2.4 for Apple iOS

The Cisco AnyConnect Secure Mobility Client requires Apple iOS 4.1 or later and runs on the following Apple devices:

- iPhone 3G
- iPhone 3GS
- iPhone 4
- iPod Touch (2nd Generation or later)

Note Support for the iPad is expected to be available with the release of Apple iOS 4.2.

Security Appliances and Software Supported

The Cisco AnyConnect Secure Mobility Client supports all Cisco Adaptive Security Appliance models. It does not support PIX devices. 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

Image Type	Version
ASA Boot image	8.0(3).1 or later
Adaptive Security Device Manager (ASDM)	6.1(3).1 or later

Note The Cisco IOS VPN head-ends are not currently supported.

Supported Features

The following AnyConnect features are supported:

- Tunnel Protocols
  - Cisco SSL Tunnelling Protocol (CSTP)
  - Cisco DTLS Tunnelling 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)

  Note The SCEP proxy feature was introduced in AnyConnect 3.0, but only legacy SCEP is supported.

- Certificate Import

In addition, the Cisco AnyConnect Secure Mobility Client is compatible with the Apple iOS Connect on Demand feature and certificates enrolled directly on to the iPhone including those enrolled with AnyConnect SCEP. For further details refer to the AnyConnect Administrator Guide.

Note This document refers exclusively to AnyConnect SCEP as opposed to Apple iOS SCEP.

Limitations of the AnyConnect Secure Mobility Client for Apple iOS

The initial release of Cisco AnyConnect Secure Mobility Client for Apple iOS supports only the features that are strictly related to remote access.

Three types of VPN configurations are supported:

- Manually generated
- AnyConnect profile imported.
- iPhone Configuration Utility generated

For further details of the iPhone Configuration Utility see http://www.apple.com/support/iphone/enterprise/.

However, full network roaming capabilities are not supported for VPN configurations created with the iPhone Configuration Utility. If your users require this functionality you should use an AnyConnect profile.

Only a single AnyConnect XML profile is supported on the iOS device, and the contents of the generated configuration will always match the most recent profile. For example, if a user goes to vpn.example1.com and then goes to vpn.example2.com, the configuration for vpn.example1.com would be replaced with the one for vpn.example2.com unless the configurations are the same.

Tunnel Keep-Alive is supported, but this may reduce the battery life of the device if the update interval is set to the minimum value.

Other known features that are not offered because of battery life constraints:

- DART—An alternate logging and email feature is built in
- Posture assessment or NAC (Cisco Secure Desktop Host Scan)
- Always on VPN, including Web Security appliance tie-ins
- Trusted Network Detection
- IPsec (IKEv2) Transport
- Full API
- Softoken integration
- Scripting
- Head-end controlled software downloads and updates—All updates are pushed from the App Store
- AnyConnect tray icon
- Customization or localization

Note AnyConnect 2.4 for Apple iOS does not support features introduced in later versions of AnyConnect.

In addition, non-VPN features such as Network Access Manager, Web Security for ScanSafe, or Telemtry are also unsupported.

Client Installation

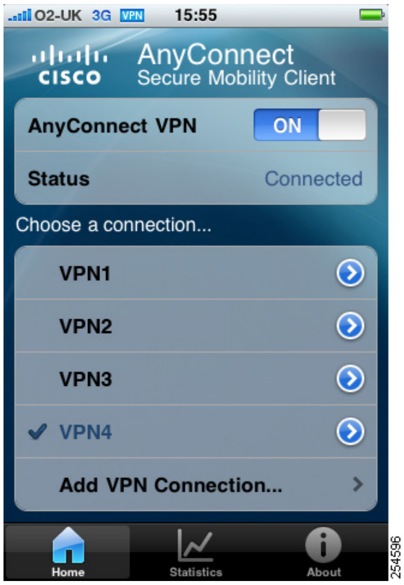
Install the AnyConnect client from Cisco AnyConnect on the Tunes App Store. For further details refer to the *Cisco AnyConnect Secure Mobility Client for Apple iOS User Guide, Release 2.4*.

Client User Interface

The Cisco AnyConnect Secure Mobility Client for Apple iOS uses its own user interface (Figure 1-1). The user interface has been designed to integrate tightly with the look and feel of Apple iOS. For detailed information, refer to the *Cisco AnyConnect Secure Mobility Client for Apple iOS User Guide, Release 2.4*.

The lower area of the **Home** tab provides a list of VPN connections for connecting to remote systems, and the option to add a new VPN connection. The slider switch enables you to switch AnyConnect on or off, and the status of the connection is displayed below.

Figure 1-1 Cisco AnyConnect Secure Mobility Client for Apple iOS User Interface

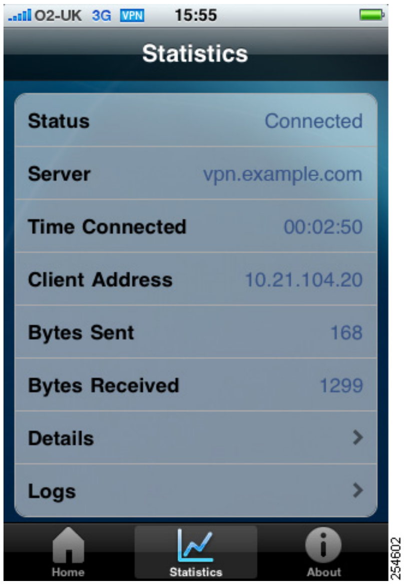


AnyConnect VPN ON

Status Connected

Figure 1-2 shows the Statistics tab, including current connection information.

Figure 1-2 Cisco AnyConnect Secure Mobility Client for Apple iOS User Interface, Statistics Tab



Status Connected

Server vpn.example.com

Time Connected 00:02:50

Client Address 10.21.104.20

Bytes Sent 168

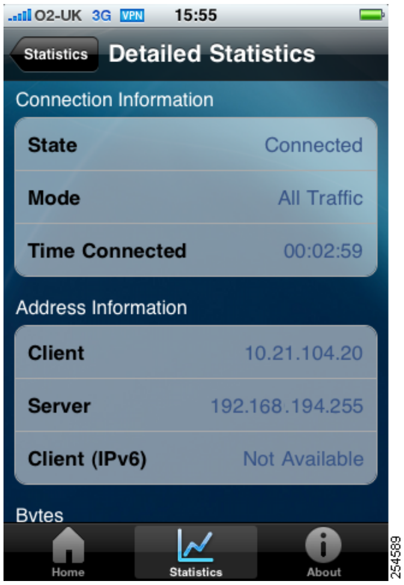
Bytes Received 1299

Details >

Logs >

Clicking the **Details** button opens the Detailed Statistics screen (Figure 3).

Figure 3 Cisco AnyConnect Secure Mobility Client for Apple iOS User Interface, Statistics Tab, Detailed Statistics Screen



Connection Information

State Connected

Mode All Traffic

Time Connected 00:02:59

Address Information

Client 10.21.104.20

Server 192.168.194.255

Client (IPv6) Not Available

Bytes

You can scroll up and down to display the following information:

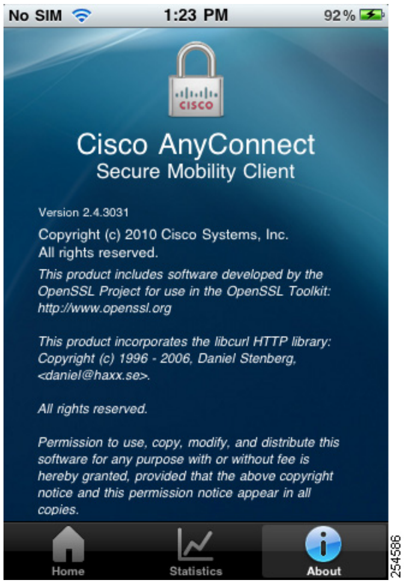
- Connection Information
  - State

  - 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 (not supported in this release)
- Secure Routes
- Non-secure Routes

Note A Secure Routes entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all traffic is tunneled.

The About tab (Figure 1-4) shows version, copyright, and documentary information about the Cisco AnyConnect Secure Mobility Client for Apple iOS.

Figure 1-4 Cisco AnyConnect Secure Mobility Client User Interface, About Tab



Version 2.4.3031

Copyright (c) 2010 Cisco Systems, Inc.
All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: http://www.openssl.org

This product incorporates the libcurl HTTP library: Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

Configuration and Deployment Overview

There are very few steps required to set up the Cisco AnyConnect Secure Mobility Client. The client needs only:

- a description; used to uniquely identify one VPN connection from another
- the server address; the fully qualified domain name or IP address of the destination including any URL path if a specific group is configured.

AnyConnect Profiles

Profiles provide basic information about connection setup, and users cannot manage or modify them. 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, the profile conveys additional connection attributes and constraints on a user.

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 Only one profile is retained on the iOS device at a time.

Connection Persistence

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

To achieve the most transparent end user experience, you should 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

When Use Certificates is configured and the appropriate certificate is selected, the Apple iOS Connect On Demand feature can be enabled. In the Connect on Demand configuration, the client can be configured to always connect when traffic is sent to certain resources or domains. For example anything at example.com is configured by placing .example.com in Always Connect. The leading period (.) prevents connections to hosts ending with *example.com, such as notexamle.com. Never Connect allows a company to exclude certain resources, for example if you don't want a VPN connection to establish automatically when connecting to a public facing Web server. The most common use case for Connect On Demand is a user briefly accessing normal internal resources.

Note Connect On Demand using the integrated Apple iOS IPsec client and AnyConnect both leverage the same Apple iOS VPN on Demand framework.

Network Roaming

The Network Roaming, or reconnect, feature enables AnyConnect to re-establish VPN connectivity when switching between networks, for example EDGE, 3G and Wi-Fi. This provides the user with seamless mobility and a secure connection that persists across networks. Network Roaming will consume more of the device's resources but when it is switched off, the connection will time out if it cannot be re-established within 20 seconds.

Note In certain situations when Network Roaming is enabled, the client may keep the tunnel open when it is not required. This can lead to data that should not be sent through the tunnel being passed through your organization. If you have any policies that restrict VPN traffic, these could prevent the device from accessing non-corporate Internet resources.

The ASA administrator has full control over the tunneling policy. You can require all network traffic to the corporate network to use the VPN connection or enable a split tunnelling policy that will tunnel only certain networks. For further details refer to your ASA Administrator Guide.

Recommended 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 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). This enables the client to remain in Reconnecting state without requiring the user to re-authenticate.

Apple iOS Specific Considerations

The following considerations should be taken into account when deploying the Cisco AnyConnect Security Mobility Client 2.4 to 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 iPhone.
- Network Roaming, which enables the VPN connection to persist when changing between connections such as 3G and Wi-Fi, is useful for applications which require a connection to the enterprise network. If Network Roaming is switched off, the client will attempt to connect for 20 seconds. If you are deploying your own iOS applications this should be taken into account.
- 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.
- When configuring rules, Cisco recommends using the Connect if Needed option. However, this requires correct DNS configuration so that host names within the enterprise are only resolved using internal DNS servers. A Connect if Needed rule will initiate a CPN connection if the DNS lookup to an internal host fails.
- Keep-alive should be switched off in user profiles to conserve battery life. It is switched off by default. In the tunnel-group's group policy, svc keepalive should also be switched off.
- 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 Due to the constraints of Apple iOS, push email notifications will not work via VPN. However, AnyConnect can be used in parallel with externally accessible ActiveSync connections which can be excluded from the tunneling policy.

Troubleshooting

Initially you should enable logging and follow the troubleshooting steps in the *Cisco AnyConnect Secure Mobility Client for Apple iOS User Guide, Release 2.4*. If you are unable to resolve the issue by following those steps then 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 Notices and Licensing on page 12 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 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. This is required when a connection must be established outside the application using certificate-only authentication.

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.

Notices and Licensing

See the following sections for Cisco AnyConnect Secure Mobility Client license information.

The following options support full AnyConnect client functionality while specifying the number of SSL VPN sessions supported:

- Cisco AnyConnect Essentials license
- Cisco AnyConnect Premium Clientless SSL VPN Edition license

These licenses are mutually exclusive per device (that is, per security appliance), but you can configure a mixed network. A nominally priced AnyConnect Mobile license is also required.

License Options

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

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:

- *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 Secure Mobility Client for Apple iOS User Guide, Release 2.4*
- For additional information about the security appliance or ASDM or its platforms, see *Navigating the Cisco ASA 5500 Series Documentation*:

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

Additional information on using VPN connections with 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

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.