# Cisco Secure Client - AnyConnect 5.0 for iOS 16

# CC Configuration Guide

**Version:** 0.2

**Date:** July 27, 2023

# Table of Contents

## Document Introduction

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides Guidance to IT personnel for the TOE, Cisco Secure Client - AnyConnect 5.0 for iOS 16. This Guidance document includes instructions to successfully install the TOE in the Operational Environment, instructions to manage the security of the TSF, and instructions to provide a protected administrative capability.

**Revision History**

| Version | Date | Change |
|---|---|---|
| 0.1 | May 1, 2023 | Initial Version |
| 0.2 | July 27, 2023 | Updates |
| | | |

# Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Secure Client-AnyConnect v5.0 for Apple iOS 16 TOE, as it was certified under Common Criteria. Cisco Secure Client-AnyConnect v5.0 for Apple iOS 16 may be referenced below by the related acronym e.g. VPN Client or simply the TOE.

## Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

## Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining AnyConnect Secure Mobility Client operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

## Document References

This section lists the Cisco Systems documentation that is also a portion of the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 1. Throughout this document, the guides will be referred to by the "#", such as [1].

**Table 1 Cisco Documentation**

| # | Title | Link |
|---|---|---|
| 1 | Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5 | https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0.html |
| 2 | Cisco AnyConnect Mobile Platforms Administrator Guide, Release 4.1 | https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/Cisco_AnyConnect_Mobile_Administrator_Guide_4-1.html |
| 3 | Apple iOS User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.6.x | https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/user/guide/Apple_iOS_AnyConnect_User_Guide_4-6-x.html |

| # | Title | Link |
|---|---|---|
| 4 | Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9 | https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/release/notes/release-notes-anyconnect-4-9.html |
| 5 | Release Notes for Cisco Secure Client (including AnyConnect), Release 5 for Apple iOS | https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/release/notes/release-notes-apple-ios-cisco-secure-client-release-5-0.html |

## TOE Overview

The TOE is the Cisco AnyConnect Secure Mobility Client (herein after referred to as the VPN client, or the TOE). The Cisco AnyConnect Secure Mobility Client provides remote users with secure IPsec (IKEv2) VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway allowing installed applications to communicate as though connected directly to the enterprise network.

## Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

**Table 2. Operational Environment Components**

| Component | Usage/Purpose Description |
|---|---|
| Certificate Authority | A Certificate Authority is used to provide valid digital certificates. |
| Mobile Platform | The TOE relies on any of the following CC validated Apple mobile device platforms:<br>■ Apple iPhone 11/XR running iOS 16 |
| ASA 5500-X series VPN Gateway | The Cisco ASA 5500-X with software version 9.2.2 or later functions as the head-end VPN Gateway. |

| | |
|---|---|
| ASDM Management Platform | The ASDM 7.7 operates from any of the following operating systems:<br>■ Windows 7, 8, 10<br>■ Windows Server 2008, 2012, 2012 R2, 2016 and Server 2019<br>■ Apple OS X 10.4 or later<br>Note that that ASDM software is installed on the ASA appliance and the management platform is used to connect to the ASA and run the ASDM. The only software installed on the management platform is a Cisco ASDM Launcher. |

The underlying Mobile platform provides some of the security functionality required in [MOD_VPNC_V2.4] and is denoted using the phrase “TOE Platform” in this document.

The Cisco AnyConnect TOE uses network hardware resources on the mobile OS platform to send and receive encrypted packets. The TOE does not access sensitive information repositories.

References in this document to “ASA” refer to a VPN Gateway

## Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

**Table 3. Excluded Functionality and Rationale**

| Function Excluded | Rationale |
|---|---|
| Non-FIPS 140-2 mode of operation | The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration. |
| SSL Tunnel with DLTS tunneling options | [MOD_VPNC_V2.4] only permits IPsec VPN tunnel. |

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the claimed Protection Profiles.

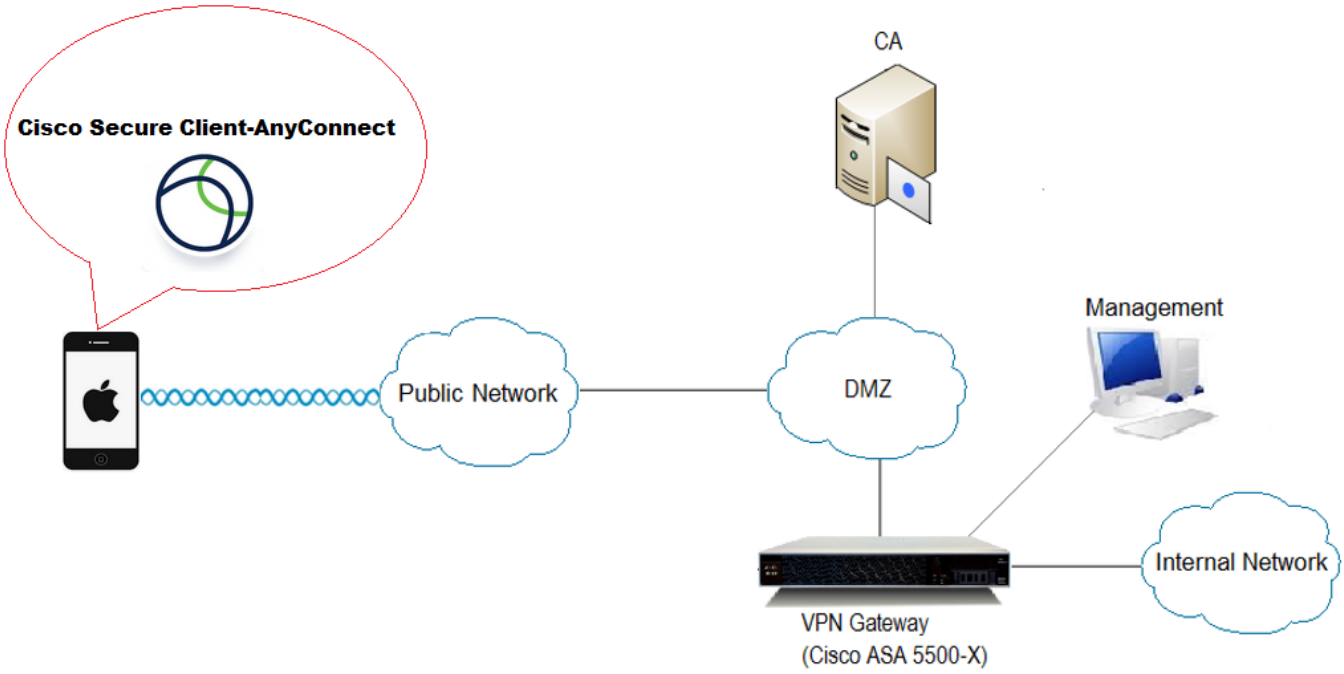
# Procedures and Operational Guidance for IT Environment

To operate in its evaluated configuration, the TOE requires a minimum one (1) Certificate Authority (CA), one (1) VPN Gateway, and one (1) Apple iPhone mobile device.

To resemble customer PKI environments, a two-tier CA solution using an Offline Root CA and an Enterprise Subordinate CA employing Microsoft 2012 R2 Certificate Authority (CA) will be referenced in this section. Other CA products in place of Microsoft may be used.

A Root CA is configured as a standalone (Workgroup) server while the Subordinate CA is configured as part of a Microsoft domain with Active Directory services enabled. The following figure provides a visual depiction of the TOE and IT Environment. The TOE is a software app running on iOS 13. The TOE boundary is denoted by the hash red line. See figure 1 below.

**Figure 1. TOE and Environment**




The Subordinate CA issues X.509 digital certificates and provides a Certificate Revocation List (CRL) to the TOE Platform and VPN Gateway.
Alternatively, one (1) single root Enterprise CA could be deployed.

- Install and Configure a Certificate Authority

  If using a Microsoft two-tier CA solution, install and configure a Root (GRAYCA) and Enterprise Subordinate Certificate Authority (GRAYSUBCA1) in accordance with the guidance from the vendor. The following is a step-

by-step guide for the configuration of Microsoft Active Directory Certificate Services:
http://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx
It is assumed both the Offline Root CA (GRAYCA) certificate and the Enterprise Subordinate CA (GRAYSUBCA1) certificates depicted in figure 1 are installed and trusted to ensure a trusted certificate chain is established. If using a CA from a vendor other than Microsoft, follow that vendor's CA installation guidance.

Regardless of the CA product used, the RSA certificate on the ASA MUST have the following Key Usage and Extended Key Usage properties:

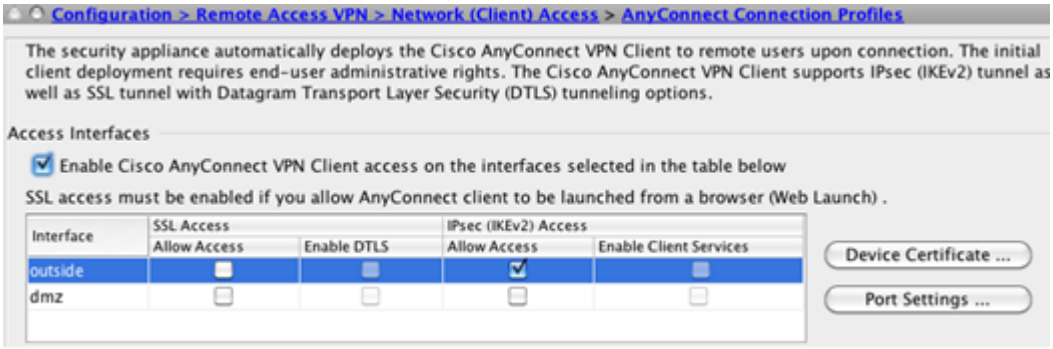
- Key Usage: Digital Signature, Key Agreement
- EKU: IP security IKE intermediate, IP end security system

The Subject Alternative Name (SAN) fields within ECDSA and RSA certificates on the ASA MUST match the connection information specified within the AnyConnect profile on the client.
.

- Install and Configure a VPN Gateway

Install Cisco ASA 9.1 (or later), optionally with ASDM, in accordance with installation guides and release notes appropriate for the versions to be installed. ASDM allows the ASA to be managed from a graphical user interface. Alternatively, if the administrator prefers, equivalent command line (CLI) configuration steps could be used.
Configuration Note: As there are parameters managed by the ASA, the Gateway Administrator must follow the steps in this section to ensure the TOE is in its evaluated configuration.

- Enable AnyConnect and IKEv2 on the ASA. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles and select Enable Cisco AnyConnect checkbox and Allow Access under IKEv2.




- On the AnyConnect Connection Profiles page mentioned above, select Device Certificate. Ensure Use the same device certificate… is NOT checked and select the EC ID certificate under the ECDSA device certificate. Then select Ok.


- Create IKEv2 crypto policy using the algorithms permitted in the Common Criteria evaluated configuration. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies and add an IKEv2 policy.

  Select Add and enter 1 for the highest priority. The range is 1 to 65535, with 1 the highest priority.

  Encryption:

  | | |
  |---|---|
  | AES | Specifies AES-CBC with a 128-bit key encryption for ESP. |
  | AES-256 | Specifies AES-CBC with a 256-bit key encryption for ESP. |
  | AES-GCM-128 | Specifies AES Galois Counter Mode 128-bit encryption |
  | AES-GCM-256 | Specifies AES Galois Counter Mode 256-bit encryption |

  D-H Group: Choose the Diffie-Hellman group identifier. This is used by each IPsec peer to derive a shared secret, without transmitting it to each other. Valid Selections are: 19 and 20.

  PRF Hash - Specify the PRF used for the construction of keying material for all of the cryptographic algorithms used in the SA. Valid selections are: sha256 and sha384

  In this example configuration select:

  Priority: **1**

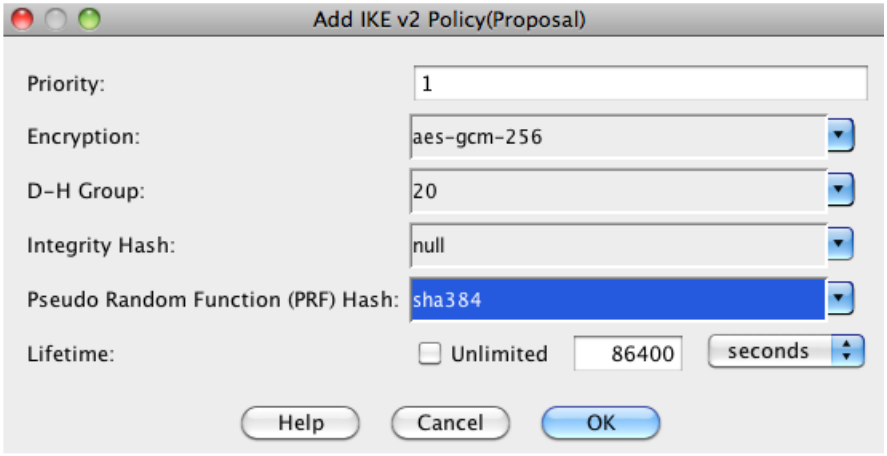
  **AES Galois Counter Mode (AES-GCM) 256-bit encryption:** When GCM is selected, it precludes the need to select an integrity algorithm. This is because the authenticity capabilities are built into GCM, unlike CBC (Cipher-Block Chaining).

  Diffie-Hellman **Group: 20**

  Integrity Hash: **Null**

PRF Hash: **sha384**

Lifetime: **86400**




Select **Ok**.

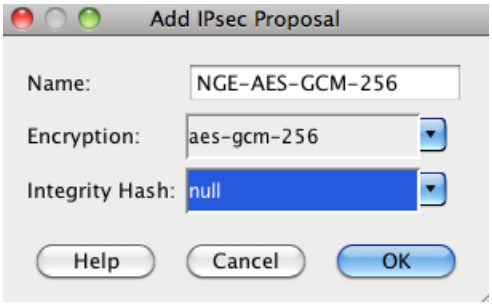
**Administrator Note**: Use of any Additional Encryption, DH-Group, Integrity or PRF Hash not listed above is not evaluated.

**Administrator Note**: The advanced tab displays the IKE strength enforcement parameter. Ensure the Security Association (SA) Strength Enforcement parameter is checked. This ensures that the strength of the IKEv2 encryption cipher is higher than the strength of its child IPsec SA's encryption ciphers. Higher strength algorithms will be downgraded.

The CLI equivalent is: crypto ipsec ikev2 sa-strength-enforcement

- Create an IPSEC proposal. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IPsec Proposals (Transform Sets) and add an IKEv2 IPsec Proposal. then select Ok.

  In the example below the name used is NGE-AES-GCM-256 with AES-GCM-256 for encryption and Null for the Integrity Hash:



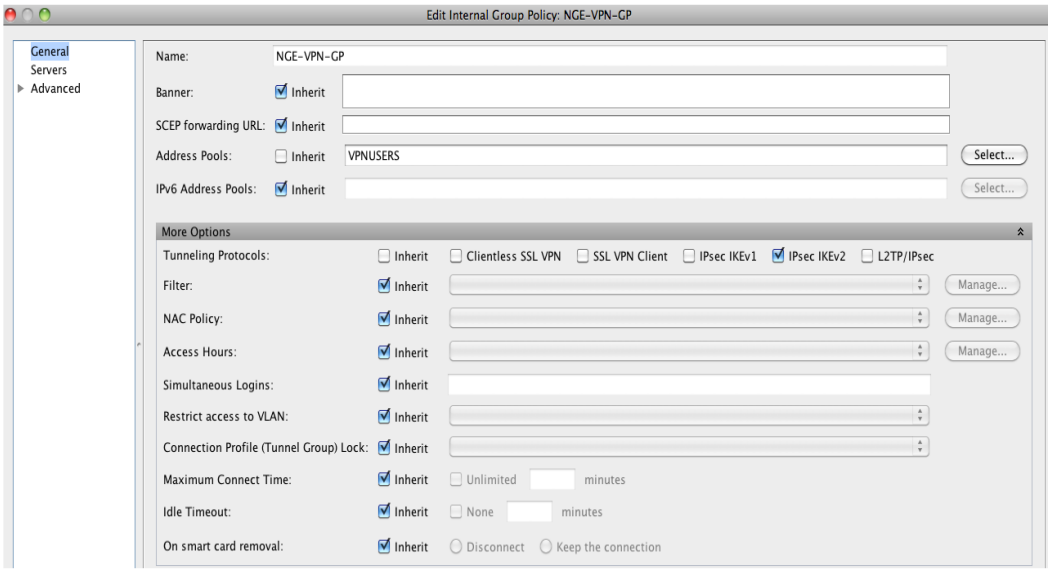

- Create a dynamic crypto map, select the IPsec proposal and apply to the outside interface. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps. Select Add, select the outside interface and the IKEv2 proposal.
  Click the Advanced Tab. Ensure the following:
  Enable NAT-T —Enables NAT Traversal (NAT-T) for this policy
  Security Association Lifetime Setting — is set to 8 hours (28800 seconds)

- Create an address pool VPNUSERS that will be assigned to VPN users. Address pools contain the following fields:
  Name—Specifies the name assigned to the IP address pool.
  Starting IP Address—Specifies the first IP address in the pool.
  Ending IP Address—Specifies the last IP address in the pool.
  Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

  In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools and add an IP pool specifying the above fields and then select Ok.

  Add a group policy that will apply the desired settings to the VPN users. Group Policies lets you manage AnyConnect VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs stored either internally on the ASA device. Configuring the VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Group Polices and Add an internal group policy. Ensure the VPN tunnel protocol is set to IKEv2 and the IP pool created above is referenced in the policy by de-selecting the Inherit check box and selecting the appropriate setting. Relevant DNS, WINS and domain names can also be added in the policy in the Servers section.

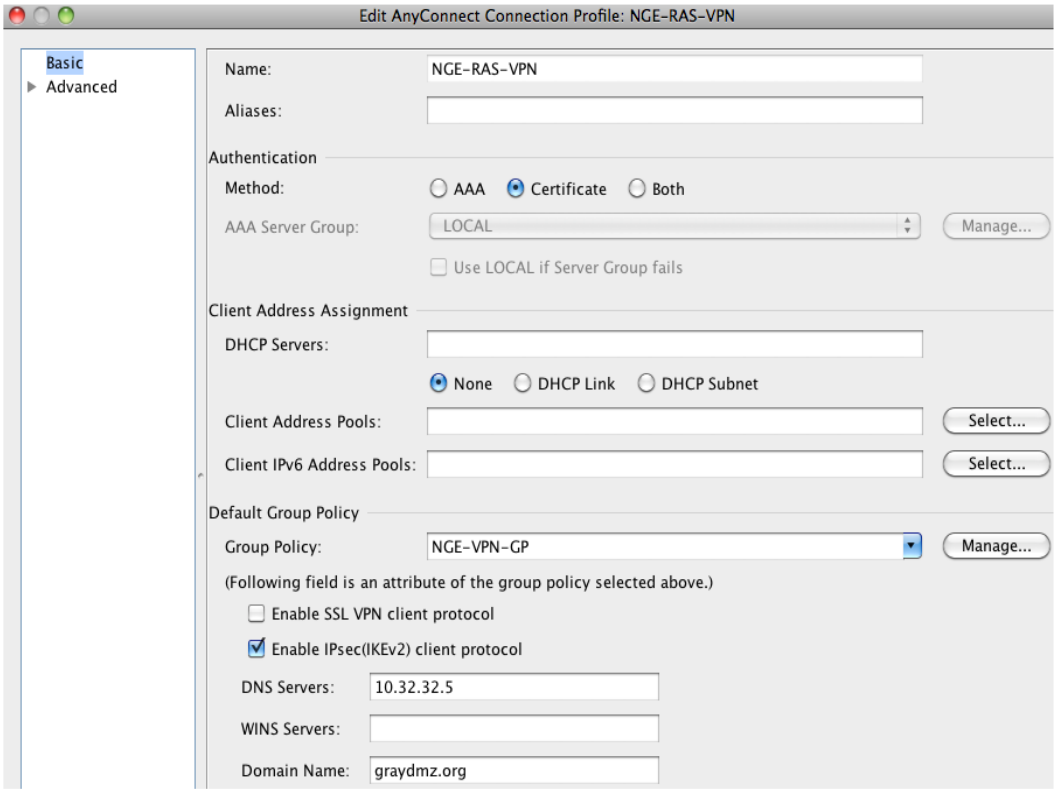
  Refer to example group policy NGE-VPN-GP below:




- Create a tunnel group name. A tunnel group contains tunnel connection policies for the IPsec connection. A connection policy can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes.

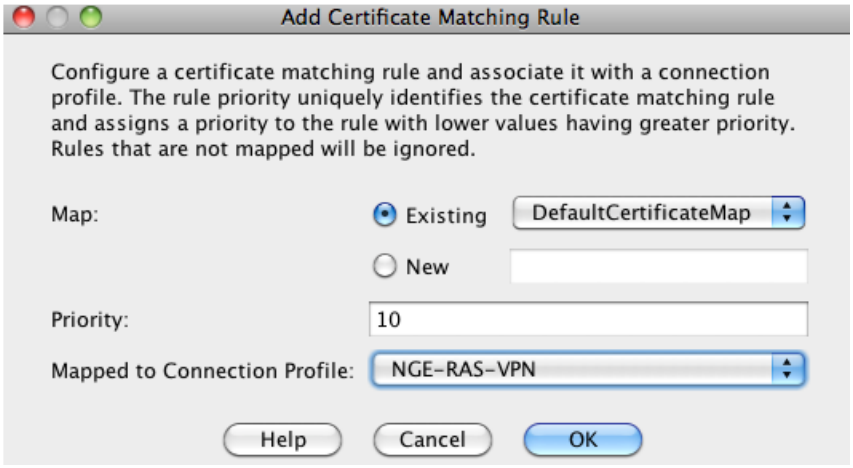
  In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. At the bottom of the page under Connection Profiles, select Add.

  In the example below the tunnel group name NGE-VPN-RAS is used.

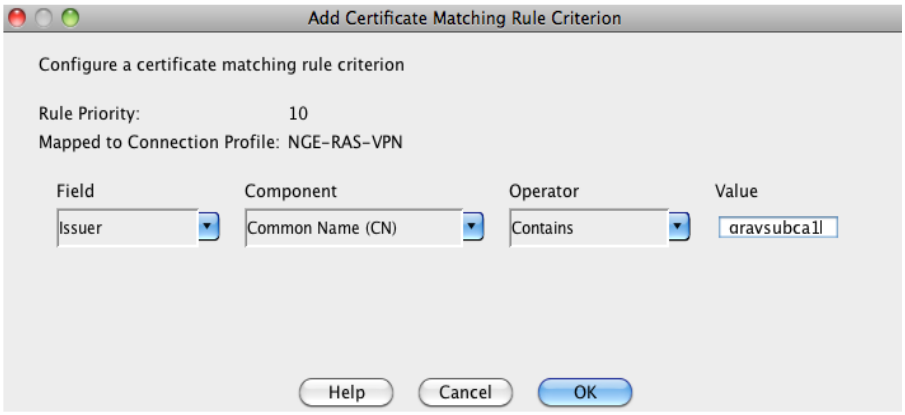



The configuration references Certificate authentication, the associated group policy NGE-VPN-GP and Enable IPsec (IKEv2). DNS and domain name can also be added here. Also ensure only IPsec is used by **not** checking the enable SSL VPN Client Protocol.

- Create a certificate map, mapping the NGE VPN users to the VPN tunnel group that was previously created. The certificate map will be applied to the AC users. In this scenario, the Subordinate CA common name was matched to ensure an incoming TOE platform request with an EC certificate issued from the Subordinate CA will be mapped to the appropriate tunnel group that was previously created. VPN users that are not issued a certificate from the EC CA will fall back to the default tunnel groups and fail authentication and will be denied access.
  In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under Certificate to Connection Profile Maps select Add. Choose the existing DefaultCertificateMap with a priority of 10 and reference the NGE-RAS-VPN tunnel group.




In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under Mapping Criteria select Add. Select Issuer for field, Common Name (CN) for component, Contains for Operator, and then select Ok.




Ensure to select APPLY on the main page and SAVE the configuration.

- Configure ASA to accept VPN connections from the AnyConnect VPN client, use the AnyConnect VPN Wizard. This wizard configures IPsec (IKEv2) VPN protocols for remote network access. Refer to the instructions here: https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/vpn/asdm-710-vpn-config/vpn-wizard.html#ID-2217-0000005b

## Preparative Procedures and Operational Guidance for the TOE

To install the Cisco Secure Client-AnyConnect TOE, follow the steps below:

1. Open the App Store.

2. Select Search
3. In the Search Box, enter Cisco Secure Client-AnyConnect
4. Tap INSTALL APP
5. Select Install

After installation the Administrator must follow the steps below to place the TOE in the evaluated configuration:

## Start Cisco Secure Client-AnyConnect

Tap the Cisco Secure Client-AnyConnect icon to start the application. If this is the first time you are starting Cisco Secure Client-AnyConnect after installing or upgrading, choose OK to enable the TOE to extend the Virtual Private Network (VPN) capabilities of your device.

### Integrity Verification

Integrity verification is performed each time the app is loaded and it will wait for the integrity verification to complete. Cryptographic services provided by the iOS platform are invoked to verify the digital signature of the TOE's executable files. If the integrity verification fails to successfully complete, the GUI will not load, rendering the app unusable. If the integrity verification is successful, the app GUI will load and operate normally.

## Configure Reference Identifier

This section specifies configuration of the reference identifier for the VPN Gateway peer. During IKE phase 1 authentication, the TOE compares the reference identifier to the identifier presented by the VPN Gateway. If the TOE determines they do not match, authentication will not succeed.

Select **Connections** from the 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.

For instructions refer to the "Add or Modify Connection Entries Manually" section of [**3**].

## Configure Certificate Use

AnyConnect requires an X.509 certificate. Refer to the "Configure Certificates" section of [**3**].

### Block Untrusted Servers

This application setting determines if AnyConnect blocks connections when it cannot identify the secure gateway. This protection is ON by default and must not be turned OFF.

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.

### Set VPN FIPS Mode

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

1. In the Cisco Secure Client-AnyConnect app, tap Settings.
2. Tap FIPS Mode to enable this setting.

To meet cryptographic requirements in the ST, FIPS mode must be enabled. Upon confirmation of your FIPS mode change, the app exits and must be restarted manually. Upon restart, your FIPS mode setting is in effect.

### Strict Certificate Trust Mode

This setting configures the Cisco Secure Client-AnyConnect TOE to disallow the certificate of the head-end VPN Gateway that it cannot verify automatically.

1. From the home window, tap Menu > Settings.
2. Enable Strict Certificate Trust Mode.

Upon the next connection attempt, Strict Certificate Trust will be enabled.

### Check Certificate Revocation

This setting controls whether the Cisco Secure Client-AnyConnect TOE will determine the revocation status of the certificate received from the head-end VPN Gateway. This setting must be ON and must not be turned OFF.

1. From the AnyConnect home window, tap Menu > Settings.
2. Enable Check Certificate Revocation to enable this setting.

## Operational Guidance for the TOE

### Establish a VPN Connection

Refer to the "Establish a VPN Connection" section of [**3**].

The Administrator should note the following PROTECT, BYPASS, and DISCARD rules regarding the use of IPsec in AnyConnect:

- PROTECT

  Entries for PROTECT are configured through remote access group policy on the ASA using ASDM. For PROTECT entries, the traffic flows through the IPsec VPN tunnel provided by the TOE. No configuration is required for the TOE tunnel all traffic. The administrator optionally could explicitly set this behavior with the command in their Group Policy: split-tunnel-policy tunnelall

- BYPASS

  The TOE supports BYPASS operations (when split tunneling has been explicitly permitted by Remote Access policy). When split tunneling is enabled, the ASA VPN Gateway pushes a list of network segments to the TOE to PROTECT. All other traffic travels unprotected without involving the TOE thus bypassing IPsec protection.

  Split tunneling is configured in a Network (Client) Access group policy. The administrator has the following options:

  Excludespecified: Exclude only networks specified by split-tunnel-network-list

  Tunnelspecified: Tunnel only networks specified by split-tunnel-network list

  Refer to the "About Configuring Split Tunneling for AnyConnect Traffic" section in the VPN ASDM configuration guide and see steps provided in the "Configure Split-Tunneling for AnyConnect Traffic" section.

  After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy.

  BYPASS SPD entries are provided by the host platform through implicit network traffic permit rules. No configuration is required on the TOE platform to allow it to pass this traffic.

- DISCARD

  DISCARD rules are performed exclusively by the TOE platform. There is no administrative interface for specifying a DISCARD rule.

## Monitor and Troubleshoot

Refer to the Monitor and Troubleshoot section of [**3**].

## Exiting Cisco Secure Client-AnyConnect

Exiting the app terminates the current VPN connection and stops all TOE processes. Use this action sparingly. Other apps or processes on your device may be using the current VPN connection and exiting the Cisco Secure Client-AnyConnect app may adversely affect their operation.

From the home window, tap Menu > Exit.

## Cryptographic Support

The TOE provides cryptography in support of IPsec with ESP symmetric cryptography for bulk AES encryption/decryption and SHA-2 algorithm for hashing. In addition the TOE provides the cryptography to support Diffie-Hellman key exchange and derivation function used in the IKEv2 and ESP protocols. Instructions to configure cryptographic functions are described in the "Procedures and Operational Guidance for IT Environment" section of this document.

## Trusted Updates

This section provides instructions for securely accepting the TOE and any subsequent TOE updates. "Updates" are a new version of the TOE.

TOE versioning can be queried by the user. From the home screen tap "About". Versioning can also be queried through the mobile platform:

- iPhone: Open Settings and go to General > Usage. Under Storage, find the Cisco Secure Client-AnyConnect and tap. The version information will be displayed.

Updates to the Cisco Secure Client-AnyConnect TOE are managed through the Apple App Store using the procedure below.

**Note:** Before upgrading your device you must disconnect the VPN session if one is established, and close the application if it is open. If you fail to do this, a reboot of your device is required before using the new version of the Cisco Secure Client-AnyConnect TOE.

1. Tap the App Store icon on the iOS home page.
2. Tap the Cisco Secure Client-AnyConnect upgrade notice.
3. Read about the new features.
4. Click Update.
5. Enter your Apple ID Password.
6. Tap OK.

The update proceeds.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

## Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.