Cisco Secure Client - AnyConnect 5.0 for Windows 10

CC Configuration Guide

Version: 0.3
Date: December 6, 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 Windows 10. 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	July 25, 2023	Initial Version
0.2	October 18, 2023	Updates for checkout
0.3	December 6, 2023	Updates to address checkout comments

Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Secure Client - AnyConnect 5.0 for Windows 10 TOE, as it was certified under Common Criteria. The Cisco Secure Client - AnyConnect 5.0 for Windows 10 TOE 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 Cisco Secure 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	Release Notes for Cisco Secure Client (including AnyConnect), Release 5 for Universal Windows Platform	https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/release/notes/universal-windows-platform-release-5-0-x.html

TOE Overview

The TOE is the Cisco Secure Client - AnyConnect 5.0 for Windows 10 (herein after referred to as the VPN client, or the TOE). The Cisco Secure Client - AnyConnect 5.0 for Windows 10 TOE 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	The Certification Authority provides the TOE with valid certificates. The CA also provides the TOE with a method to check the certificate revocation status of the VPN Gateway.
Windows 10 OS Platform	The Windows 10 platform provides an execution platform for the TOE to run. The TOE requires one of the following Common Criteria certified Microsoft Windows 10 Operating Systems to run: ■ Microsoft Windows 10 version 2004 (May 2020 Update) The Windows 10 Operating Systems listed above have been evaluated for conformance with the Protection Profile for General Purpose Operating System and listed on the NIAP Product Compliant List (PCL).
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. The Cisco Secure Client TOE communicates only with the Cisco ASA 5500-X Series Gateway.
ASDM Management Platform	The ASDM 7.7 or later operates from any of the following operating systems: ■ Windows 7, 8, 10 ■ Windows Server 2008, 2012, 2012 R2, 2016 and Server 2019 ■ Apple OS X 10.4 or later 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 OS 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 Secure Client TOE uses network hardware resources on the OS platform to send and receive encrypted packets. The TOE does not access sensitive information repositories or other hardware resources.

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.

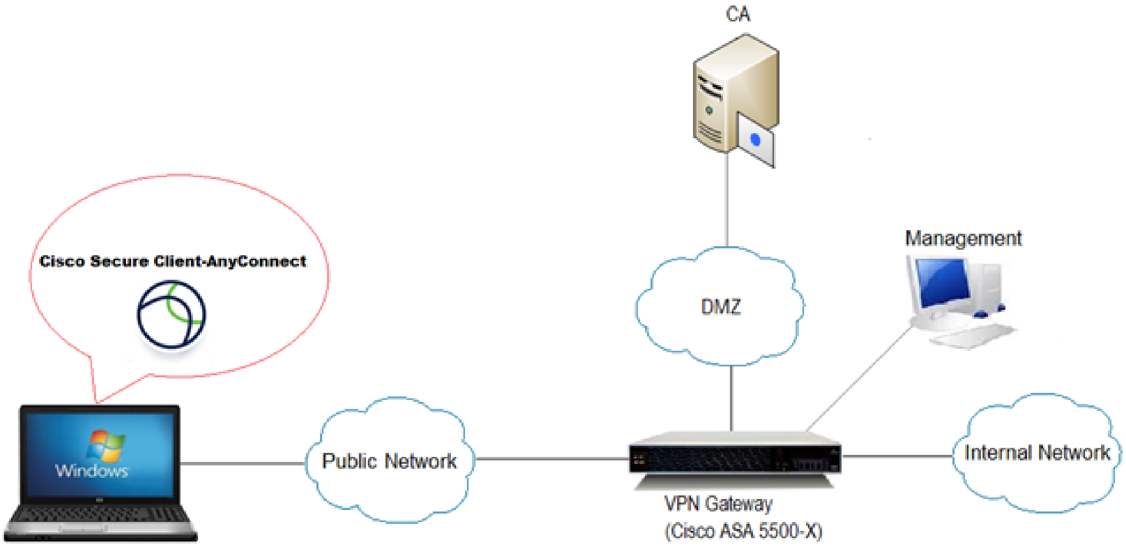
Procedures and Operational Guidance for IT Environment

To operate in its evaluated configuration, the TOE requires a minimum one (1) Certificate Authority (CA), one (1) VPN Gateway, and one (1) Windows 10 OS 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 TOE is a software app running on Windows 10. 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:

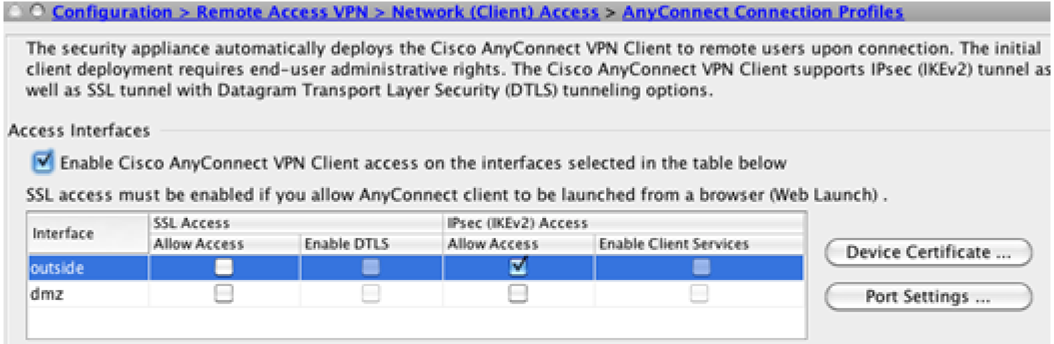
  1. Key Usage: Digital Signature, Key Agreement
  2. EKU: IP security IKE intermediate, IP end security system

  The Subject Alternative Name (SAN) fields within the RSA certificate on the ASA MUST match the connection information specified within the Cisco Secure Client 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.

1. 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.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

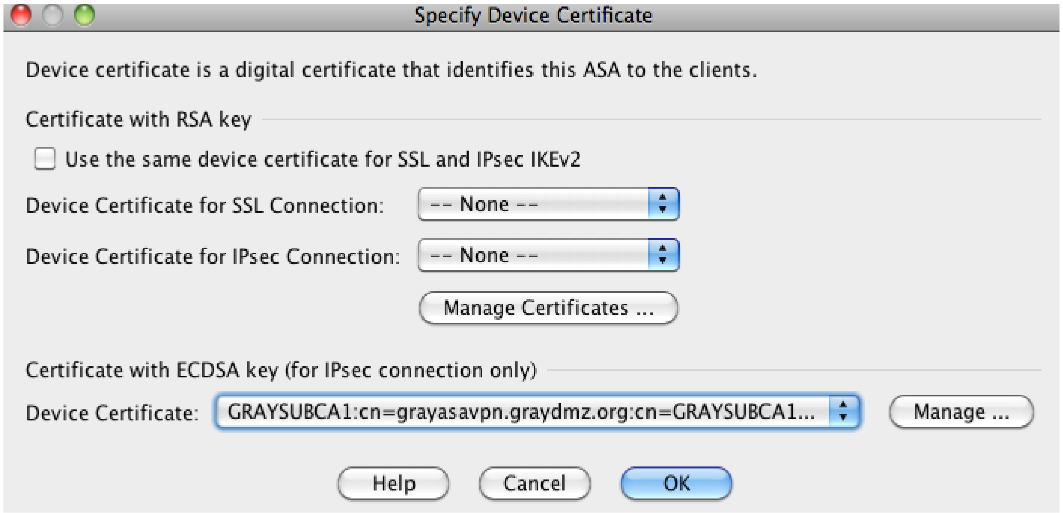
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☐	☐	☑	☐
dmz	☐	☐	☐	☐

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



Specify Device Certificate

Device certificate is a digital certificate that identifies this ASA to the clients.

Certificate with RSA key

☐ Use the same device certificate for SSL and IPsec IKEv2

Device Certificate for SSL Connection: -- None --

Device Certificate for IPsec Connection: -- None --

Certificate with ECDSA key (for IPsec connection only)

Device Certificate: GRAYSUBCA1:cn=grayasavpn.graydmz.org:cn=GRAYSUBCA1...

3. 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.

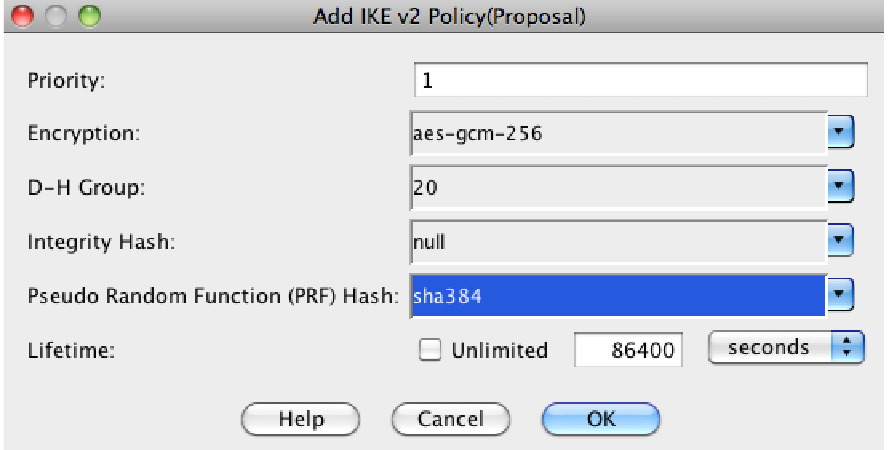
PRF Hash - Specify the PRF used for the construction of keying material for all of the cryptographic algorithms used in the SA. Valid selections are: sha256 and sha384

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**



Add IKE v2 Policy(Proposal)

Priority: 1
Encryption: aes-gcm-256
D-H Group: 20
Integrity Hash: null
Pseudo Random Function (PRF) Hash: sha384
Lifetime: □ Unlimited 86400 seconds

Select **Ok**.

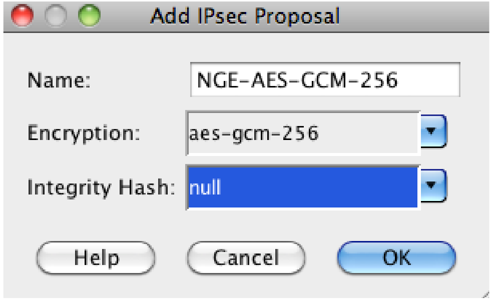
Administrator Note: Use of any Additional Encryption, DH-Group, Integrity or PRF Hash not listed above is not evaluated.

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

4. 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:



Add IPsec Proposal

Name: NGE-AES-GCM-256

Encryption: aes-gcm-256

Integrity Hash: null

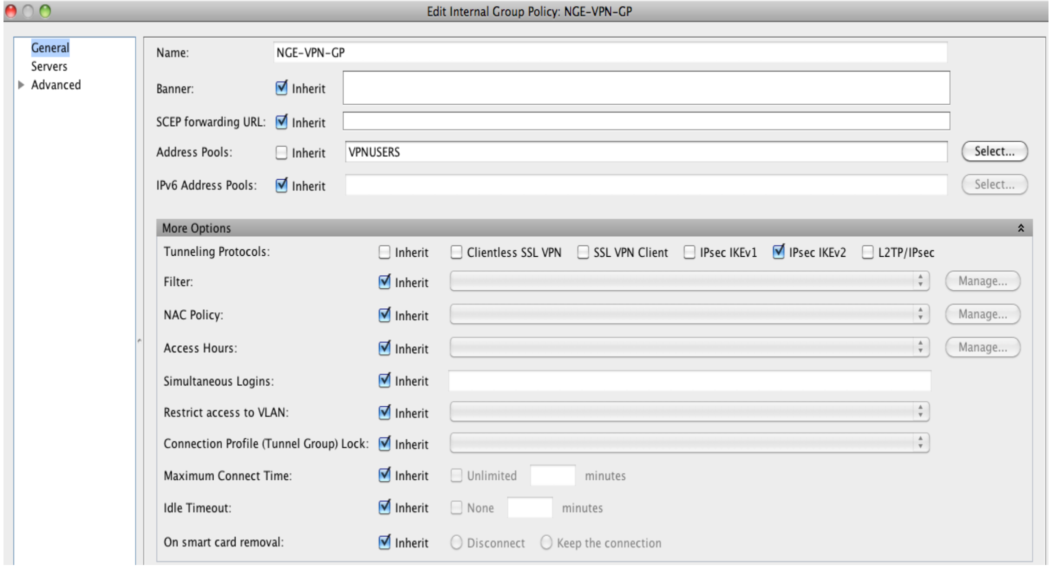
5. Create a dynamic crypto map, select the IPsec proposal and apply to the outside interface. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps. Select Add, select the outside interface and the IKEv2 proposal.
   Click the Advanced Tab. Ensure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

6. 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:



Edit Internal Group Policy: NGE-VPN-GP

Name: NGE-VPN-GP

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: □ Inherit VPNUSERS

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 ☑ IPsec IKEv2 □ L2TP/IPsec

Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

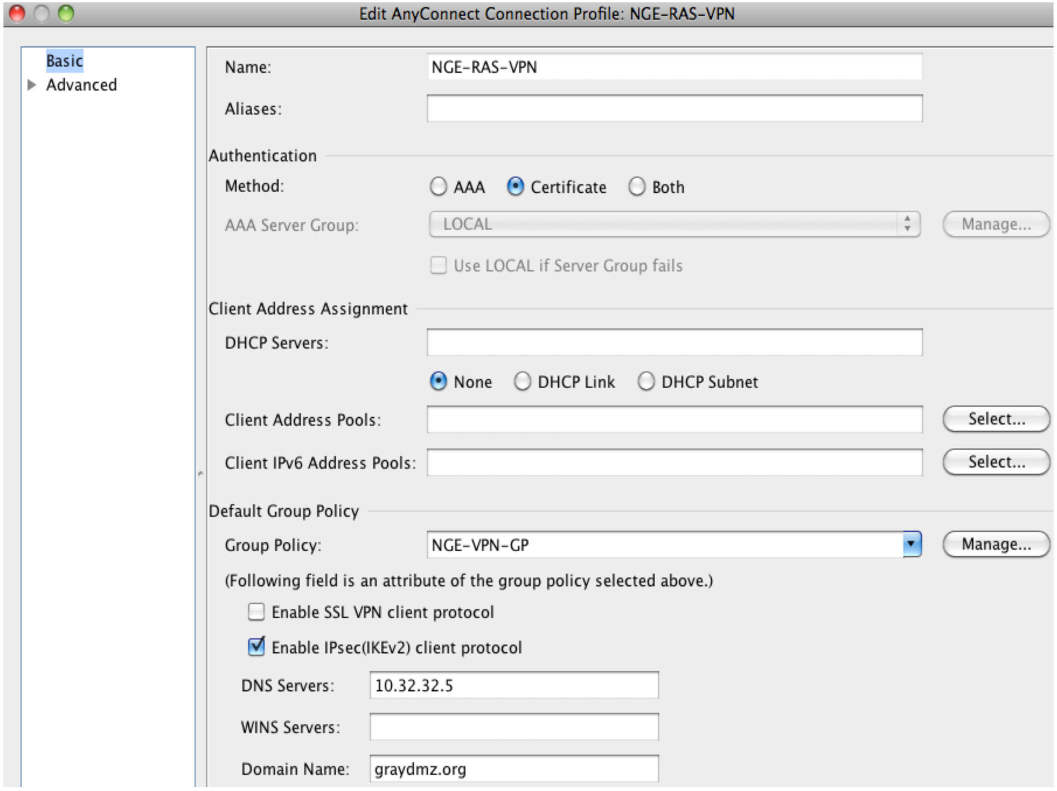
Idle Timeout: ☑ Inherit □ None minutes

On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

7. 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.



Edit AnyConnect Connection Profile: NGE-RAS-VPN

Name: NGE-RAS-VPN

Aliases:

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: NGE-VPN-GP

(Following field is an attribute of the group policy selected above.)

□ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

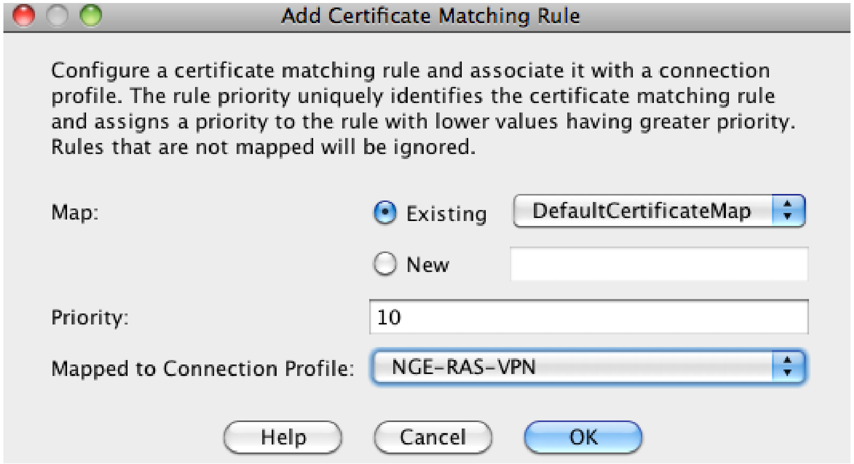
DNS Servers: 10.32.32.5

WINS Servers:

Domain Name: graydmz.org

   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.

8. 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.


Add Certificate Matching Rule

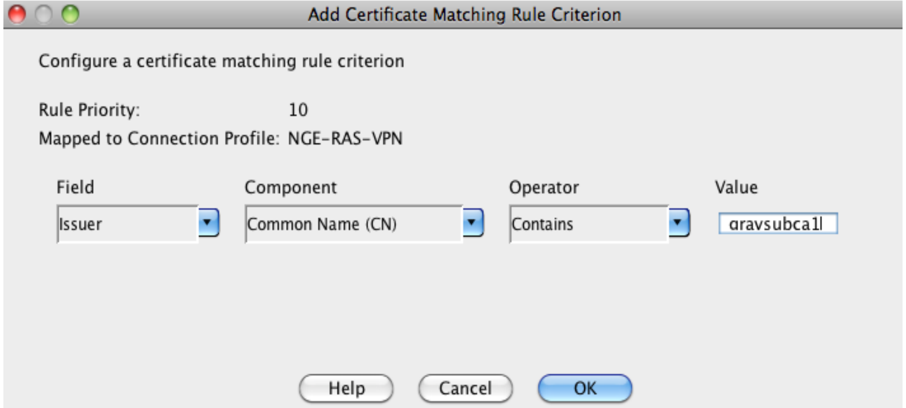
Configure a certificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the certificate matching rule and assigns a priority to the rule with lower values having greater priority. Rules that are not mapped will be ignored.

Map: ● Existing DefaultCertificateMap
○ New

Priority: 10

Mapped to Connection Profile: NGE-RAS-VPN

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.


Add Certificate Matching Rule Criterion

Configure a certificate matching rule criterion

Rule Priority: 10
Mapped to Connection Profile: NGE-RAS-VPN

Field	Component	Operator	Value
Issuer	Common Name (CN)	Contains	gravsubca1

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

9. 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 “AnyConnect VPN Wizard” section found in the Cisco ASA Series VPN ASDM Configuration Guide. Per table 2 above, ASDM version 7.7 or later can be used. The link below provides instructions for ASDM v7.7: https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/asdm77/vpn/asdm-77-vpn-config/vpn-wizard.html#ID-2217-0000005b

Preparative Procedures and Operational Guidance for the TOE

To install Cisco Secure Client - AnyConnect 5.0 for Windows, follow the steps below:

1. Download the Cisco Secure Client for Windows TOE software from https://software.cisco.com/software/csws/ws/platform/home?locale=en_US# into a directory on the TOE platform. Ensure the version download is 5.0

2. Double-Click to install. Upon installation, the TOE platform will verify the digital signature is valid.

3. (Optional) Download and install the Profile Editor 5.0. The Cisco Secure Client features and settings are enabled in profiles. Profiles are created using the profile editors, which are GUI-based configuration tools launched from ASDM. The standalone profile editor

allows users with admin privileges to manage their own profiles as an alternative to the profile editors integrated with ASDM. The installation also installs the VPN local policy editor.

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

Cisco Secure Client Profiles

The Cisco Secure Client features and settings are enabled in profiles. Profiles are created using the profile editors.

A form of the profile editor exists integrated with the ASDM tool. This form of the Profile editor is used when the ASA is used to centrally manage profiles globally for all Cisco Secure Client users.

To add a new client profile to the ASA from ASDM:

Open ASDM and select Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

There is also a standalone version of the profile editors for Windows that you can use as an alternative to the profile editors integrated with ASDM. Users with admin privileges can manage or modify their own profiles.

For initial configuration of the TOE, Secure Client profiles must either be:

- Created using the profile editors integrated with ASDM and exported to a local or remote windows host computer where the Secure Client resides. For this option refer to the Exporting an Secure Client Profile function within ASDM.
- Created using standalone version of the Profile Editor. See section below.

Cisco Secure Client Stand-Alone Profile Editor

To use the standalone version of the Profile Editor, navigate to All Programs > Cisco > Cisco Secure Client and click the Stand-Alone Profile Editor icon.

By default, the profile is located in the following location:

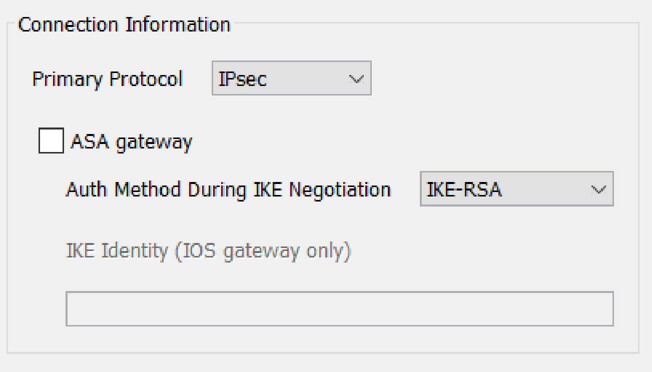
```
%ProgramData%\Cisco\Cisco Secure Client\Profile\RemoteAccessIKEv2_client_profile.xml
```

“RemoteAccessIKEv2_client_profile.xml” is an example name. The name of the Group Policy on the ASA Gateway MUST match the name of the .xml file in the location above, or profile mismatch errors will occur.

From the File Menu, Select Open. Browse to the above and click the Open Button.

Configuration Note: If this is the first time use of the Stand-Alone Profile Editor, the file should not exist. Proceed with the remainder of the steps in this section and save the file as a new .xml file in the above location.

Click on Server List. Ensure the Server List is populated correctly for the VPN gateways in your environment. Click a Server List Entry. For each server list entry, ensure IPsec is selected as the primary protocol drop-down box. Uncheck the checkbox for ASA gateway and select IKE-RSA in the “Auth Method during IKE Negotiation” drop-down box.



Connection Information

Primary Protocol: IPsec

□ ASA gateway

Auth Method During IKE Negotiation: IKE-RSA

IKE Identity (IOS gateway only)

Configuration Note: An accurate host name and address MUST match the name presented in the certificate. This means the FQDN (or IP Address) MUST match the Subject Alternative Name (SAN) that is presented in the certificate by the ASA.

From the File Menu, select Save and then Exit; Reboot the Computer.

Configuration Note: The name of the local configured profile needs to match the name of the remote access policy on the ASA.

Additional information on these settings can be found in The Secure Client VPN Profile section of [**1**].

After initial configuration has completed, the profile editors integrated with ASDM must be used to centrally store and manage the configuration options defined in the profiles for all Cisco Secure Client users.

Cisco Secure Client Local Policy

If you installed the Profile Editor, the VPN Local Policy Editor will also be installed. Navigate to All Programs > Cisco > Cisco Secure Client and click on the VPN Local Policy Editor.

The **AnyConnectLocalPolicy.xml** is an XML file on the client containing security settings. This file is not deployed or managed by the ASA VPN Gateway. By default, the AnyConnectLocalPolicy.xml file is located in the following location:

```
%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml
```

From the File Menu, Select **Open**. Browse to the above and click the **Open** Button. The following settings must be enabled with a check-box:

- FIPS Mode
- Strict Certificate Trust
- Enable CRL Check

The “Bypass Downloader” setting must be unchecked.

Strict Certificate Trust prevents users the ability to accept a certificate that could not be successfully verified.

Additional information on these settings can be found in The Cisco Secure Client Local Policy section of [**1**].

From the File Menu, select Save and then Exit.

The **AnyConnectLocalPolicy.xml** file can also be manually edited.

Integrity Verification

Integrity verification is performed each time the Cisco Secure Client app is loaded and it will wait for the integrity verification to complete. Cryptographic services provided by the Windows 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 Cisco Secure Client App compares the reference identifier to the identifier presented by the VPN Gateway. If the Secure Client App determines they do not match, authentication will not succeed.

Select **Connections** from the Secure Client home screen to view the entries already configured on your device.

For instructions to add a new VPN connection refer to the "Configure VPN Connection Servers" section of [**1**].

Configure Certificate Use

The Microsoft "MMC" Certificate snap-in tool should be used to both generate a CSR and import certificates. Information on the use of MMC can be found here: http://technet.microsoft.com/en-us/library/dd632619.aspx

The TOE platform administrator needs to follow the steps below from Microsoft to complete a manual CSR on a Windows machine: http://technet.microsoft.com/en-us/library/cc730929.aspx

Configuration Note: In step 4, select: (No template) CNG key

Configuration Note: In step 6, select: PKCS #10

Configuration Note: In step 8, the properties of the Certificate Request, ensure the following is selected:

- Click the Subject tab. Provide a Value for Subject name/Full DN.
- Click the Private Key tab. Select the ECDSA_P384, Microsoft Software Key Storage Provider.
  - **Configuration Note**: If using RSA, the TOE platform administrator will choose RSA, Microsoft Software Key Storage Provider instead of ECDSA.
- Click the drop-down box to select the Hash Algorithm. Select sha384 and click OK.
- Click the Extensions tab
  - Click the drop-down box Under Key usage and select Digital Signature and select Add and OK.
  - Click the drop-down box Under Extended Key Usage and Select Server Authentication and select Add and OK.

After completing Step 9, save the CSR to a location and select "OK"

The CSR will now need to be sent to the CA administrator and processed to obtain the TOE platform identity certificate. If using a CA from a vendor other than Microsoft, follow that vendor's guidance for use of templates and certificate generation.

Import the CA certificates and the TOE platform identity certificate into the Windows certificate store. To import certificates, refer to the following instructions from Microsoft: http://technet.microsoft.com/en-us/library/cc754489.aspx

Operational Guidance for the TOE

Establish Connection

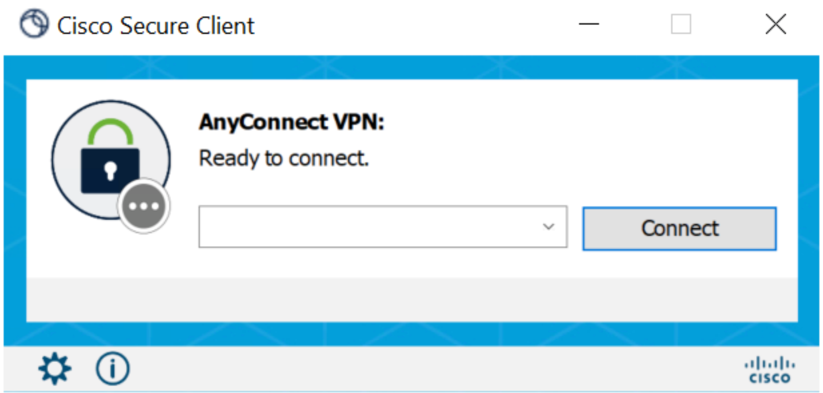
Launch the Cisco Secure Client.

Note: As a remote access client accessing resources behind the ASA gateway, the TOE operates only in tunnel mode and does not operate in transport mode. No configuration is required for the TOE to operate in tunnel mode.

Note: The TOE implements IKEv2 and does not support IKEv1. No configuration is required for the TOE to operate using IKEv2.

Note: Should the Cisco Secure Client fail to start, examine the contents of the Application and System log in the Windows Event Viewer. Should the TOE executable for some reason become corrupt or illegitimate, the TOE will fail a signature verification checked performed by the platform on the executable files. The system log will state the Cisco Secure Client is not a valid Win32 application.

Click the Connect Button to connect to one of the predefined VPN Gateways.



Cisco Secure Client

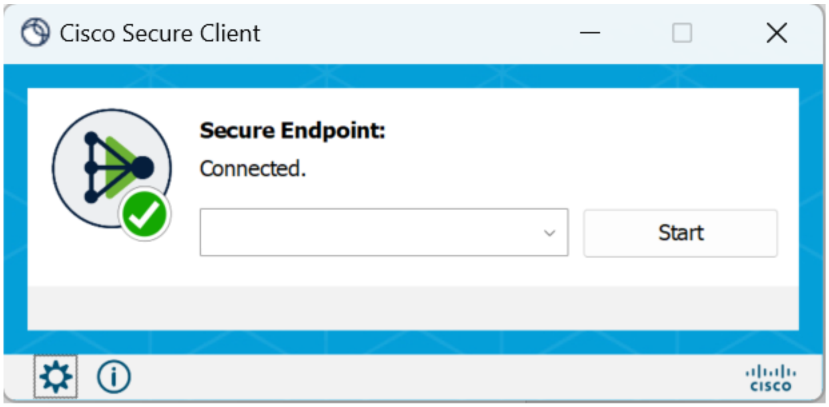
AnyConnect VPN:
Ready to connect.

Acceptance of the Gateway Certificate

If the VPN gateway certificate is valid and this is the first connection to the gateway you will be prompted to accept the certificate into the Windows certificate store.

The TOE automatically determines which client certificate to use from the Windows Certificate Store. If the Gateway is configured for additional authentication with user credentials, you will be prompted to enter them.

The connection should then be established. To verify click the Cisco Secure Client icon in the System Tray. You should see a green checkbox stating it is connected to the VPN Gateway (Server).



Cisco Secure Client

Secure Endpoint:
Connected.

To end the VPN Session, click the Disconnect Button.

Administrator Note: If the VPN gateway certificate is invalid or fails the CRL check, Cisco Secure Client will disallow the connection.:

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

- 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 "Configure Split-Tunneling for AnyConnect Traffic " section in the Cisco ASA Series VPN ASDM Configuration Guide. Per table 2 above, ASDM version 7.7 or later can be used. The link below provides instructions for ASDM v7.7:

  https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/asdm77/vpn/asdm-77-vpn-config/vpn-asdm-setup.html#ID-2188-00000218

  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 Troubleshoot Cisco Secure Client section of [**1**].

Exiting Secure Client

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

From the Secure Client applet click Disconnect.

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 Elliptic-Curve 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 by clicking the ‘About’ button which will display version information.

The administrator can check for software updates at Cisco Software Central which is available at: https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#

Customers can also subscribe to the Cisco Notification Service allows users to subscribe and receive important information regarding product updates. Full information is provide in the Cisco Security Vulnerability Policy available at: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

When there is an update for Cisco Secure Client the process to update is the same as a new installation. Refer to steps 1 – 3 on page 13 of this document.

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.