

# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Cisco AnyConnect

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Number:** 007-013967-001, Rev. A

**Release Date:** January 2018

# Contents

Third-Party Software Acknowledgement .....	4
Description .....	4
Applicability .....	5
Environment.....	5
Audience .....	5
CBA Flow using SafeNet Authentication Client .....	6
Prerequisites .....	6
Supported Tokens and Smart Cards in SafeNet Authentication Client .....	7
Configuring Cisco ASA .....	8
Prerequisites: .....	8
Installing Root Certificate to the ASA ASDM.....	9
Installing an Identity Certificate on the ASA ASDM .....	12
ADD / Configure AAA Server Group .....	14
Group Policy Configuration .....	17
Connection Profile .....	24
Any Connect Client Profile .....	45
Client Installation.....	51
Running the Solution .....	53
Using the Cisco AnyConnect Secure Mobility Client SSL VPN .....	53
Using the Clientless SSL VPN .....	56
Using the Cisco AnyConnect Secure Mobility Client - IPsec IKEv2 VPN .....	58
Start Before Logon (SBL) .....	60
Support Contacts .....	65
Customer Support Portal.....	65
Telephone Support.....	65

# Third-Party Software Acknowledgement

---

This document is intended to help users of Gemalto products when working with third-party software, such as Cisco AnyConnect.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

## Description

---

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is an effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. Gemalto's certificate-based tokens and smart cards provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

The Cisco ASA 5505 Appliance is a modular platform that provides security and VPN services for small and medium-sized business and enterprise applications.

The following integration guide describes how to authenticate users from workstations to the Cisco ASA, using certificates stored on Tokens/Smart Cards.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Cisco AnyConnect using Gemalto's tokens and smart cards.

It is assumed that the Cisco AnyConnect environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Cisco AnyConnect can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.



## Applicability

---

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.

For more details about different SAC installation modes, please refer to the Customization section in the *SafeNet Authentication Client Administrator Guide*.

## Environment

---

The integration environment used in this document is based on the following software versions:

- SafeNet Authentication Client (SAC) - 10.5
- Cisco AnyConnect - 4.5.02033
- Cisco ASA 5505 version 9.2.(4)
- Cisco ASDM 7.6 (1)

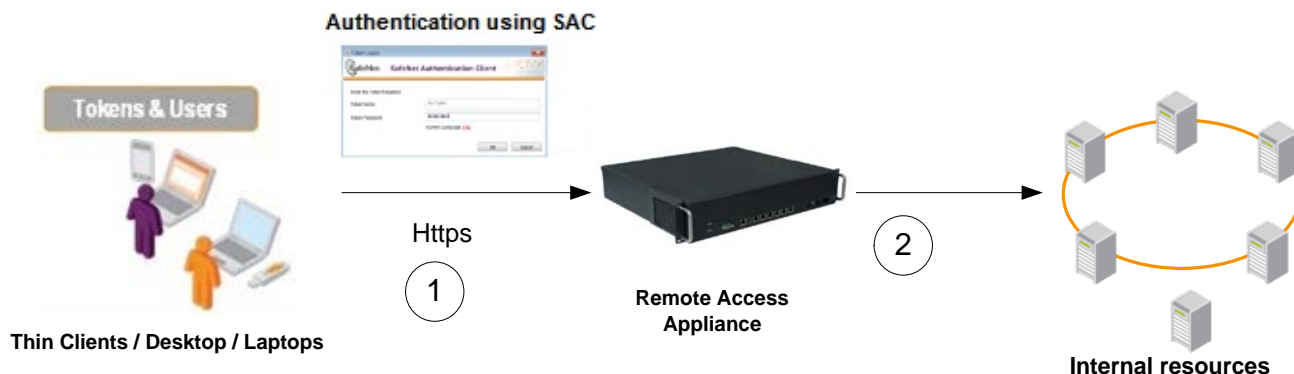
## Audience

---

This document is targeted to system administrators who are familiar with Cisco AnyConnect, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

# CBA Flow using SafeNet Authentication Client

The diagram below illustrates the flow of certificate-based authentication:



1. A user attempts to connect to the Cisco AnyConnect server using the Cisco AnyConnect client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to internal resources.

## Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Cisco AnyConnect using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token or smart card with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (10.5) should be installed on all client machines.

# Supported Tokens and Smart Cards in SafeNet Authentication Client

---

SafeNet Authentication Client (10.5) supports the following tokens and smart cards:

## **Certificate-based USB tokens**

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

## **Smart Cards**

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

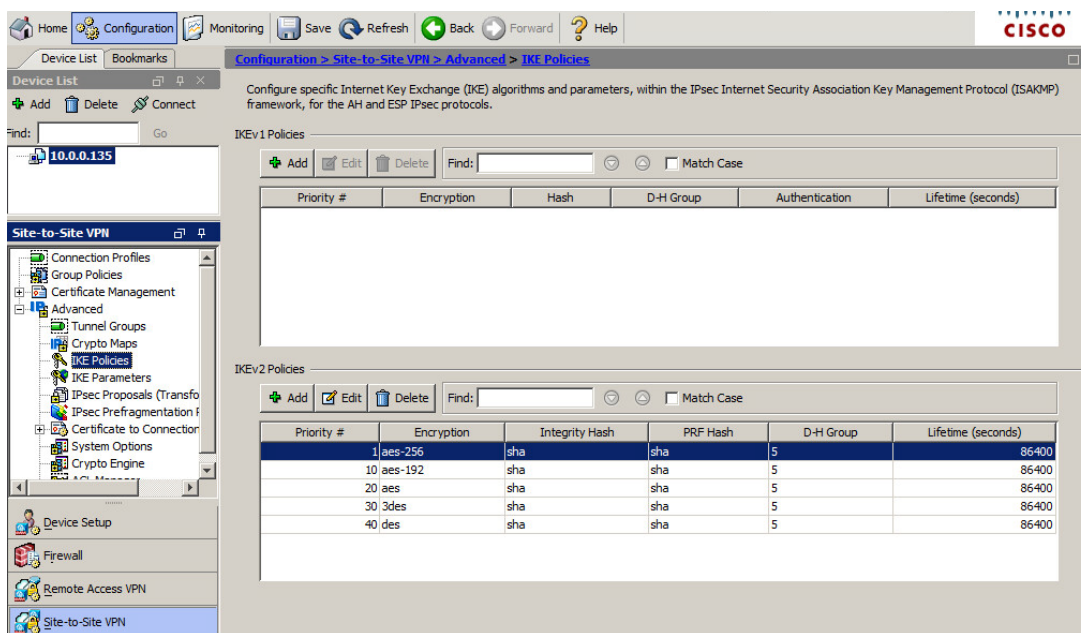
For a list of all supported devices please refer to *SafeNet Authentication Client Customer Release Notes*.

# Configuring Cisco ASA

This solution demonstrates how to use Token / Smart Card solutions incorporated with Cisco solutions. This is done by authenticating users against Cisco ASA using PKI (Smart Card User certificate) stored on the Token/Smart Card.

## Prerequisites:

- **IPsec configuration** used default options that were enabled after adding a cisco license:
  - Default IKE Parameters Default crypto map
  - NAT (Transparency enabled)
  - Default IPsec Proposals
- **IKEv2 Policies** - IKEv2 policy example configuration:



The screenshot shows the Cisco ASA configuration interface. The main window displays the 'IKEv2 Policies' configuration page. The interface includes a navigation pane on the left with 'Site-to-Site VPN' selected, and a main content area with a table of IKEv2 Policies. The table has columns for Priority #, Encryption, Integrity Hash, PRF Hash, D-H Group, and Lifetime (seconds). The table contains five rows of data.

Priority #	Encryption	Integrity Hash	PRF Hash	D-H Group	Lifetime (seconds)
1	aes-256	sha	sha	5	86400
10	aes-192	sha	sha	5	86400
20	aes	sha	sha	5	86400
30	3des	sha	sha	5	86400
40	des	sha	sha	5	86400

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

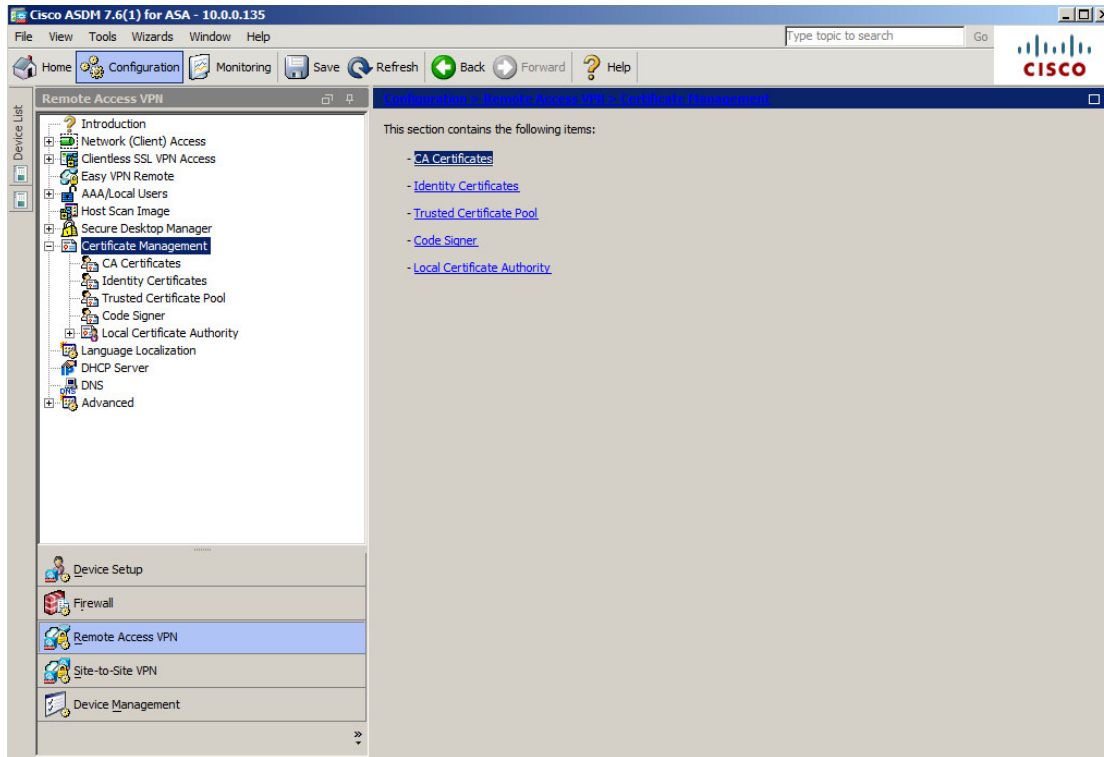
- SSL Certificate was configured on ASDM.
- For authentication using digital certificates, there must be at least one identity certificate and its issuing CA certificate on a security appliance.

## Installing Root Certificate to the ASA ASDM

**Prerequisite:** Root CA Certificate is downloaded from the CA authority. Before configuring the ASA for Remote access VPN you must enroll the Cisco ASA for the Root CA certificates and keys.

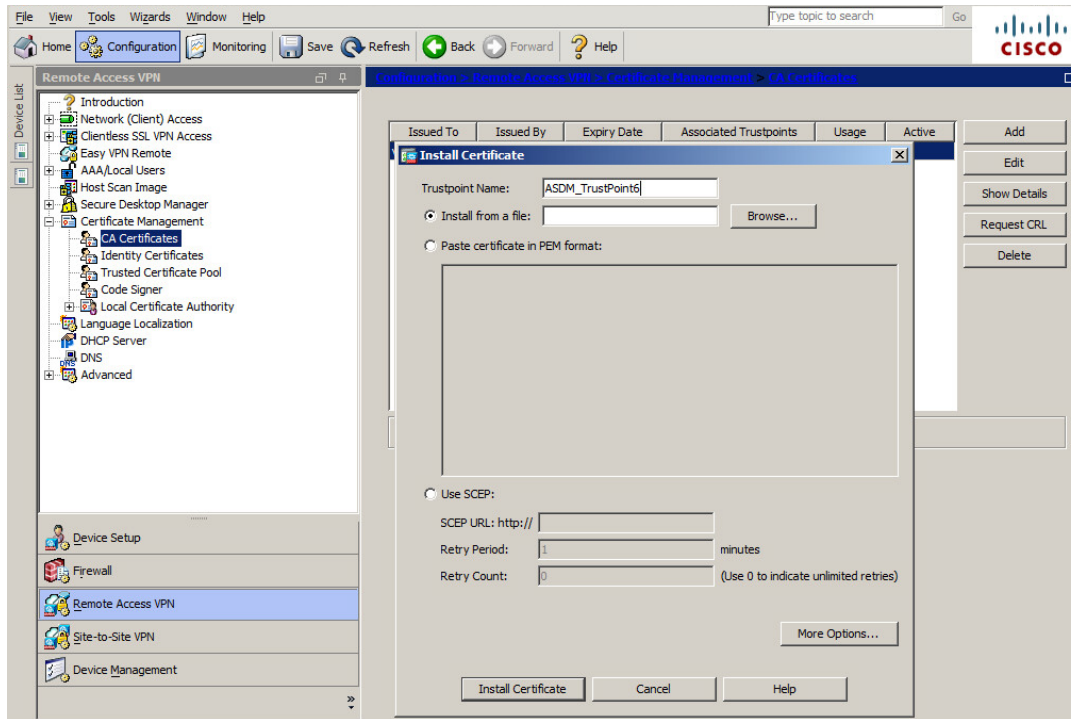
**To enroll the ASA for the Root CA certificate:**

1. From the **Cisco ASDM for ASA** screen select **Configuration> Certificate Management**, then click **CA Certificate**.



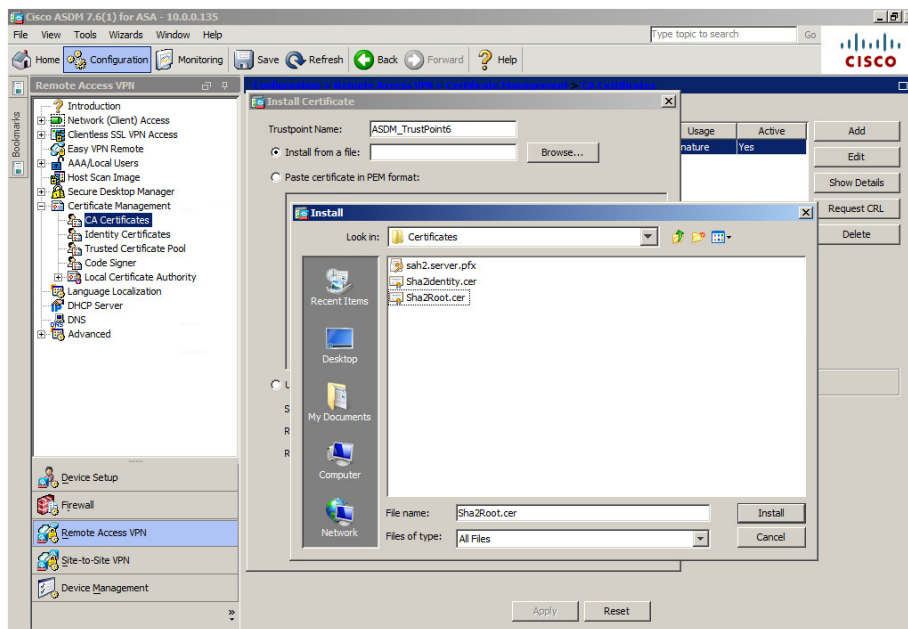
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

2. Select **CA Certificates**, then click **Add**.



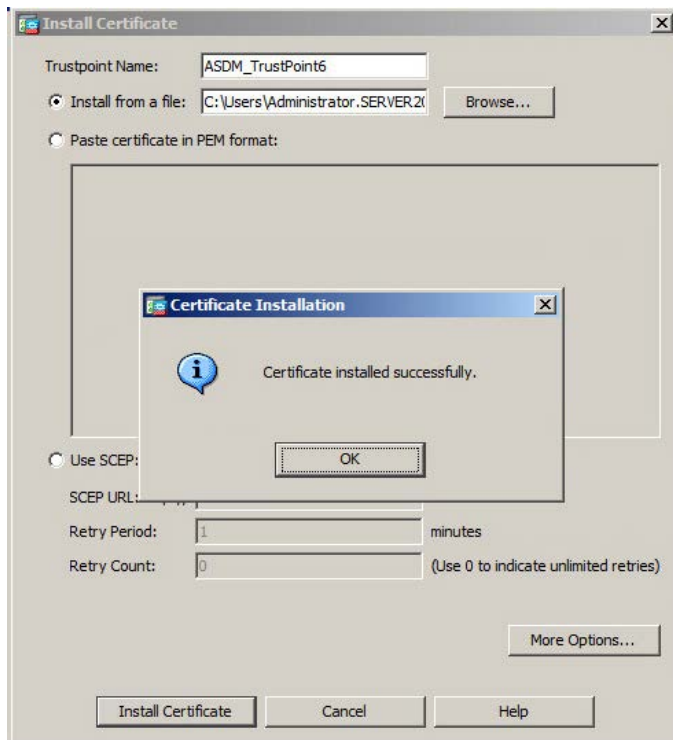
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. Under **Install from a file** click **Browse**, navigate to the path of the Root CA, and then click **Install**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. On the **CA Certificate Installed successfully** window, click **OK**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

## Installing an Identity Certificate on the ASA ASDM

Before configuring the ASA for Remote access, VPN enrollment of the ASA identity for certificates and keys is needed.

**Prerequisite:** this example demonstrates a pre-created PKCS12 certificate. The Certificate **must** contain the server authentication EKU.

**To enroll the ASA for certificate installation:**

1. From the **Cisco ASDM for ASA** screen select **Configuration> Certificate Management**, then click **Identity certificate**, and click **Add**.

The screenshot displays the Cisco ASDM 7.6(1) for ASA interface. The left sidebar shows the navigation tree with 'Identity Certificates' selected under 'Certificate Management'. The main content area shows a table of identity certificates with the following data:

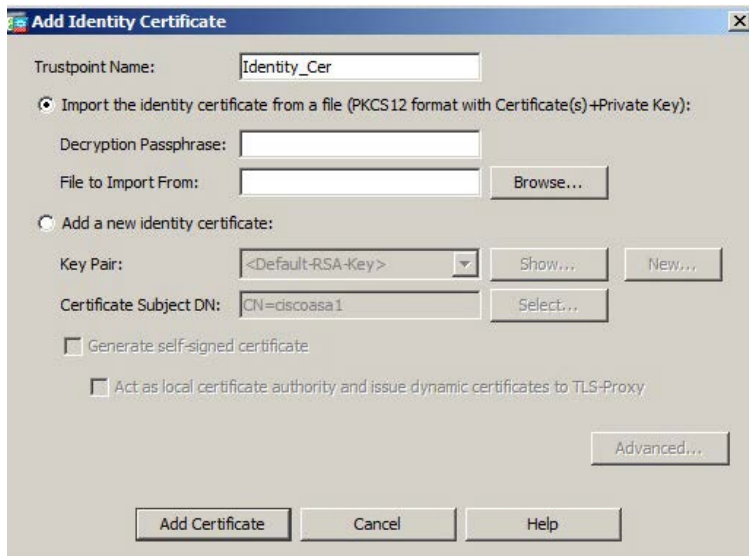
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	
cn=ciscoasa1...	cn=vm2008-A...	19:13:44 IST Ju...	ASDM_TrustPoint22	General Pu...	RSA (1024 bits)	<input type="button" value="Add"/> <input type="button" value="Show Details"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Install"/>

Below the table, there is a search field with 'End:' and a 'Match Case' checkbox. The 'Public CA Enrollment' section contains a button 'Enroll ASA SSL certificate with Entrust' and a link 'enroll with Entrust'. The 'ASDM Identity Certificate Wizard' section contains a button 'Launch ASDM Identity Certificate Wizard'. At the bottom, there are 'Apply' and 'Reset' buttons. The status bar at the bottom shows 'Data Refreshed Successfully.', 'cisco', '15', and the date '6/22/17 1:03:35 PM IST'.

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

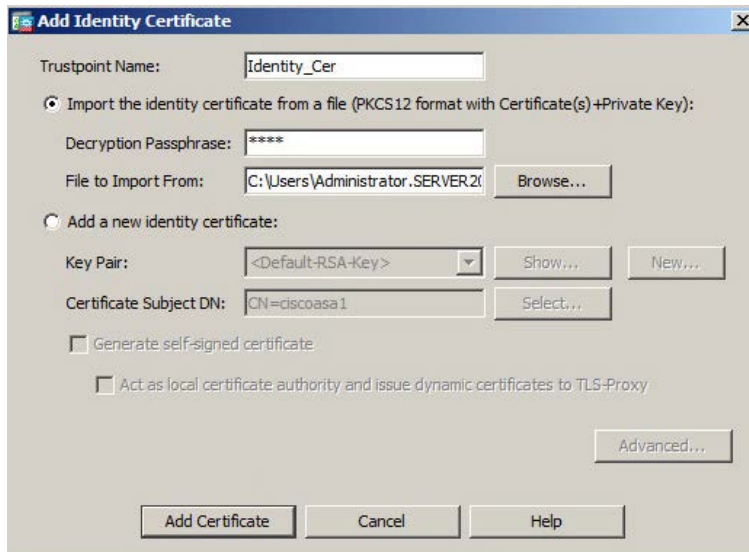


2. Enter a name in the **Trustpoint Name** field, select **Import the identity certificate from a file**, then click **Browse** and navigate to the certificate location.



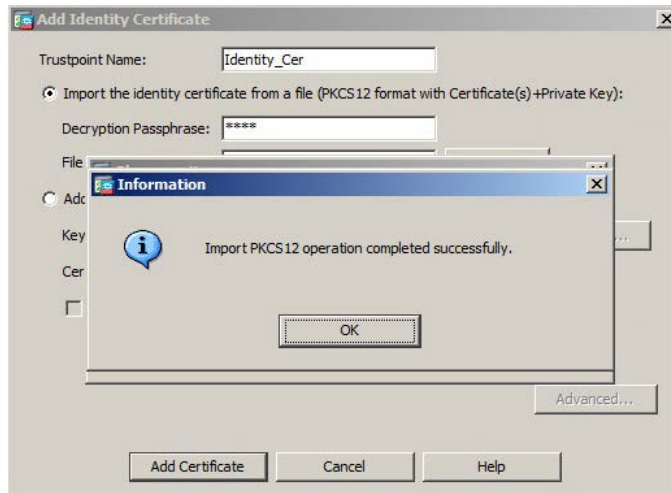
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

3. Enter the passphrase in the **Decryption Passphrase** field.
4. Next to the **File to Import From** field, click browse and navigate to the certificate, then click **Add Certificate**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

- When the Identity certificate imported successfully, click **OK**.



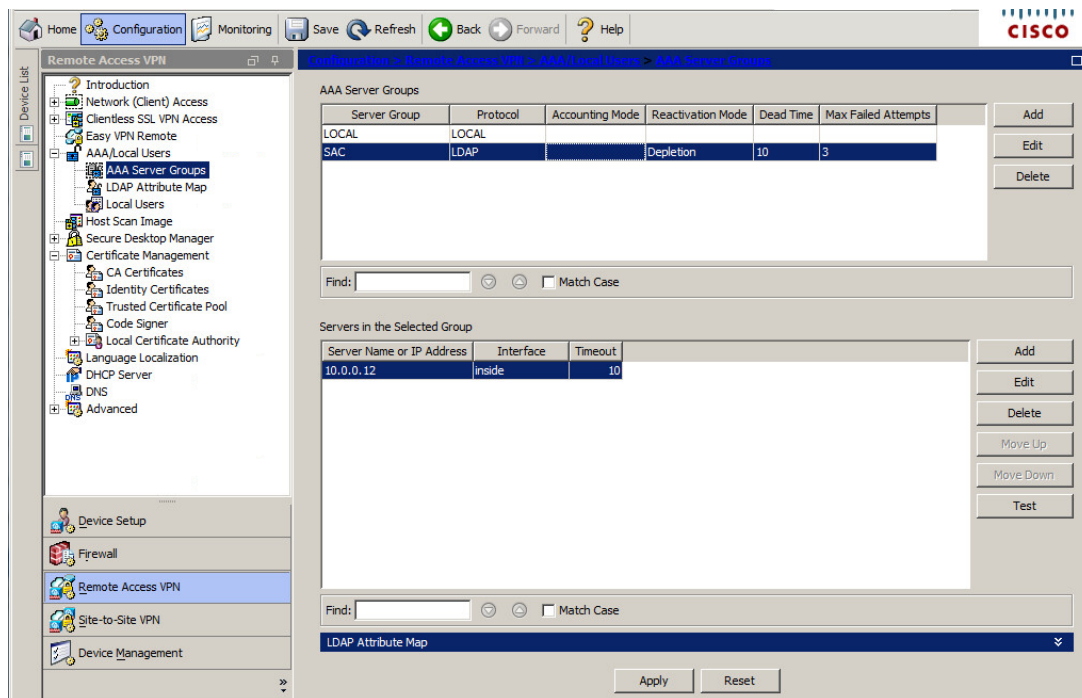
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## ADD / Configure AAA Server Group

If you want to use an external AAA server, you must first create at least one AAA server group for each AAA protocol, and add one or more servers to each group. AAA server groups are identified by name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

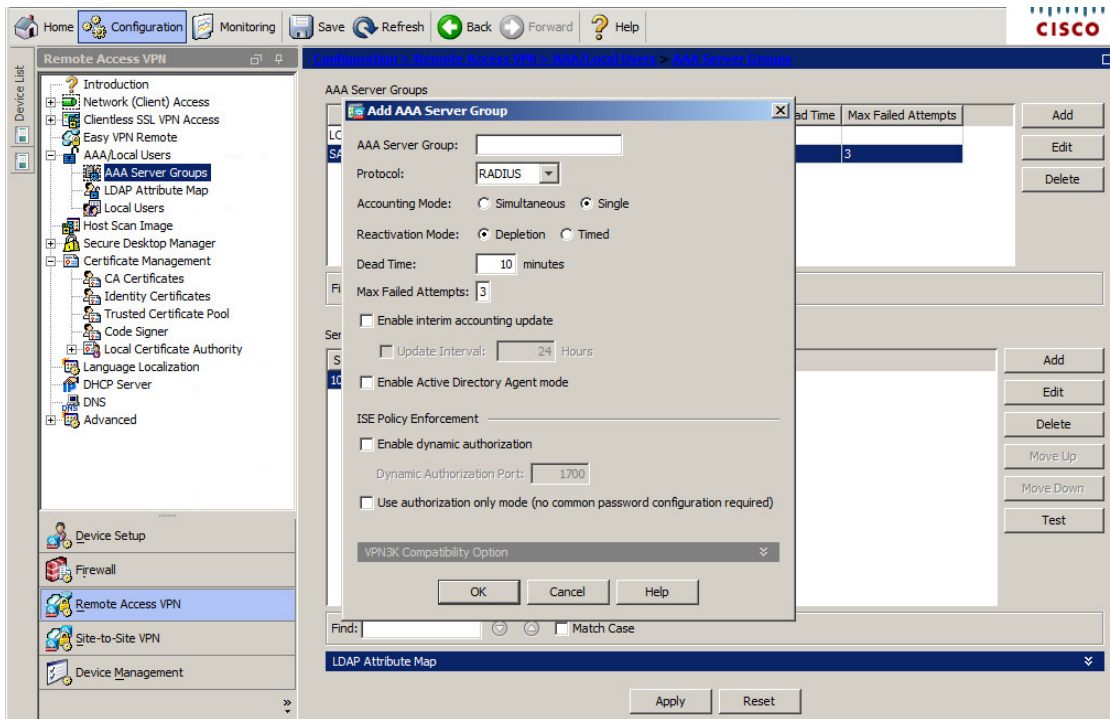
For this integration, we will use Microsoft Active Directory LDAP as AAA server for authorization.

- From the **Cisco ASDM for ASA** screen, click the **Configuration** tag, click **Remote Access VPN** and select **AAA Local users > AAA Server Group**.



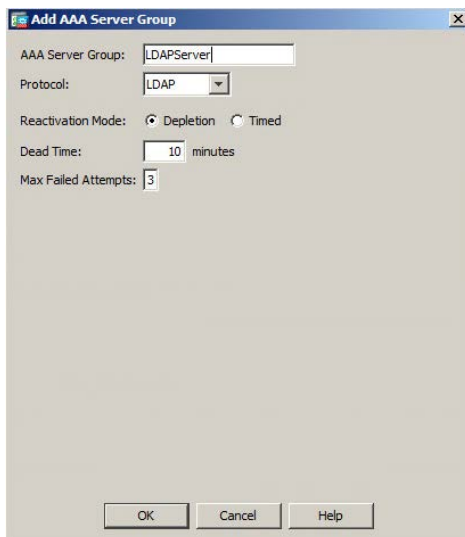
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. In the **AAA Server Groups** window, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

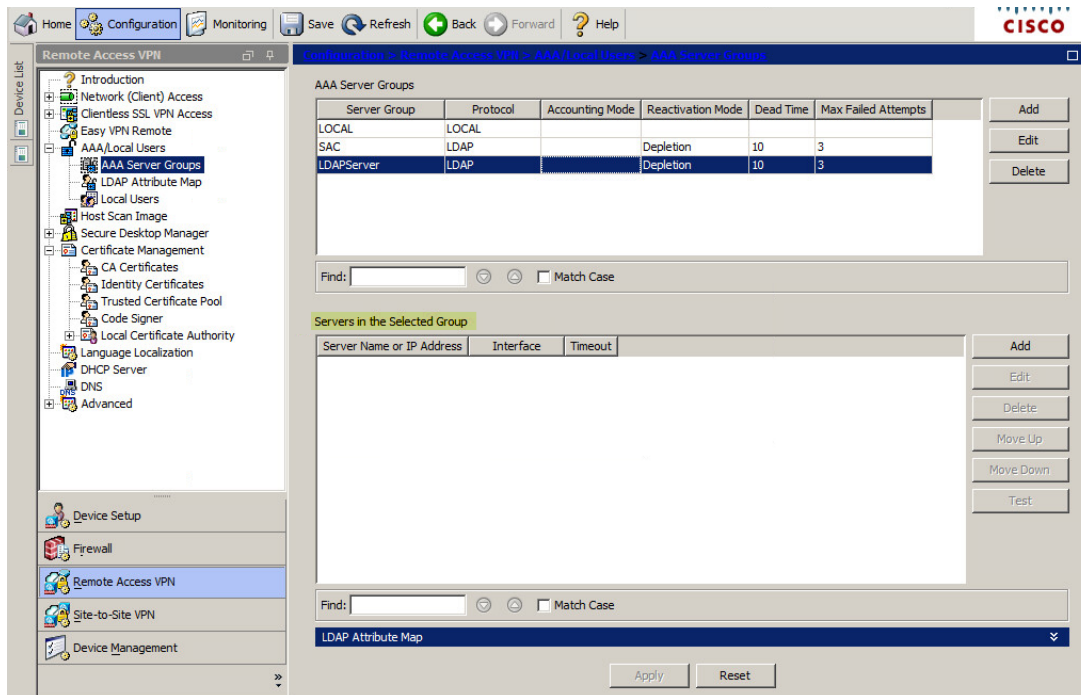
3. On the **Add AAA Server Group** window, complete the fields as described in the table below, and then click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

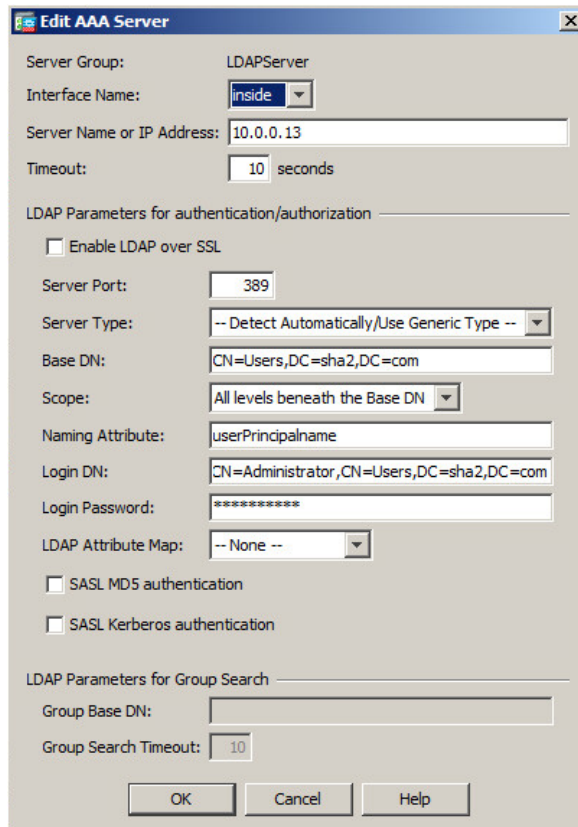
Field	Operation
<b>AAA Server Group</b>	Enter a server group name (for example, <b>LDAP server</b> )
<b>Protocol</b>	Select <b>LDAP</b> .

- Under **Servers in the selected Group** (highlighted), click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- Complete the fields as described in the table below and click **OK**:



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Field:</b>	<b>Operation:</b>
<b>Interface Name</b>	Select an appropriate interface that Cisco ASA uses in order to reach the LDAP server.
<b>IP address</b>	Enter the IP address of the server.
<b>Server Type</b>	Choose Server Type (in this example Detect Automatically was used).
<b>Server Port</b>	In this example the default LDAP port 389 was used.
<b>Base DN</b>	Enter the location in the LDAP hierarchy where the server must begin to search.
<b>Scope</b>	Under the scope option, choose the appropriate answer. In this example, the default "All Levels beneath the Base DN" was used.
<b>Naming Attribute</b>	Enter the Relative Distinguished Name attribute(s) that uniquely identifies an entry on the LDAP server; <b>userPrincipalname</b> attribute in the Microsoft Active Directory.
<b>Login DN</b>	Enter the Distinguished Name with enough privileges in order to be able to search users in the LDAP server.
<b>Login Password</b>	Enter the password for the Distinguished Name account.

## Group Policy Configuration

A group policy is a set of user-oriented attribute/value pairs for connections that are stored either internally (locally) on the device or externally. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

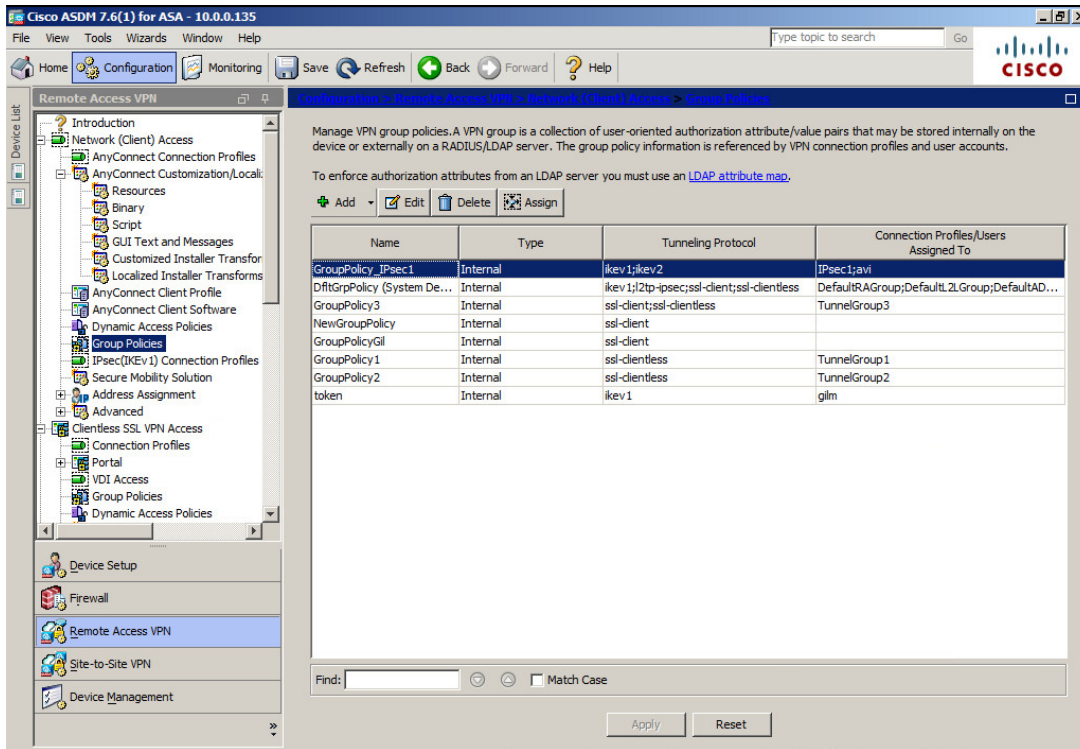
### Group Policy - SSL Protocol

In this example: Group policy with SSL protocol is demonstrated for both client and clientless users.

**To add a group policy, do the following:**

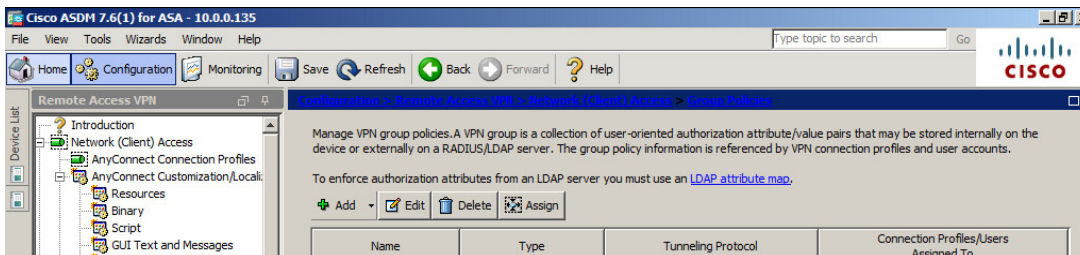
1. Open the **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.

- In the left pane, click **Remote Access VPN**, and then select **Network (Client) Access > Group Policies**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

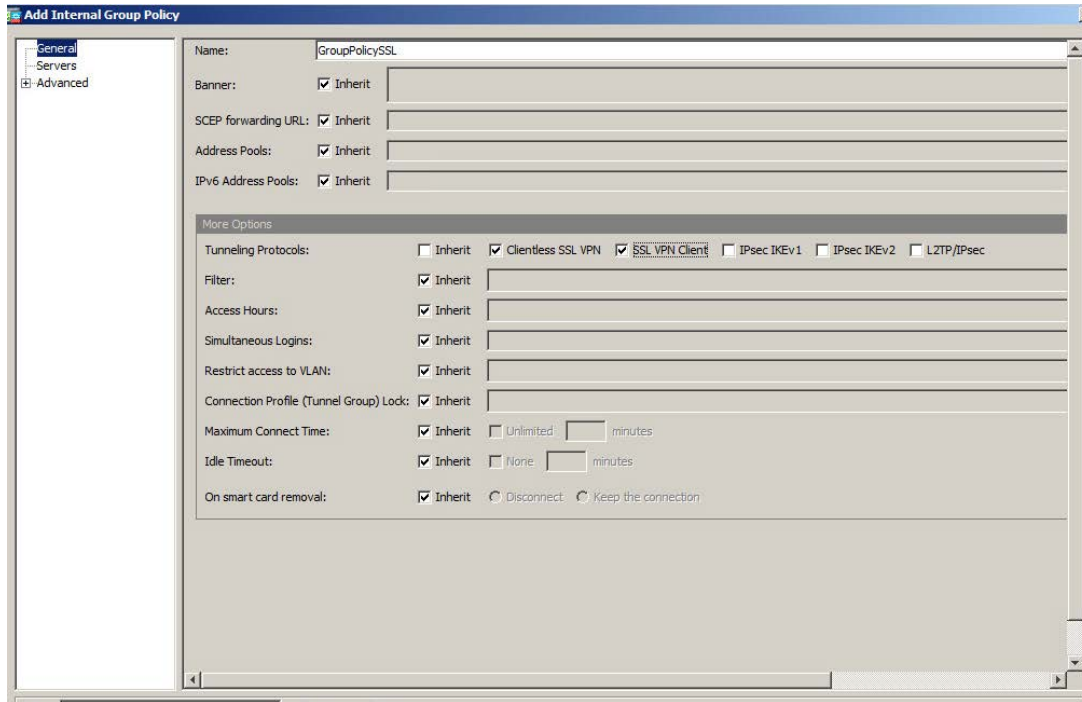
- In the center pane, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)



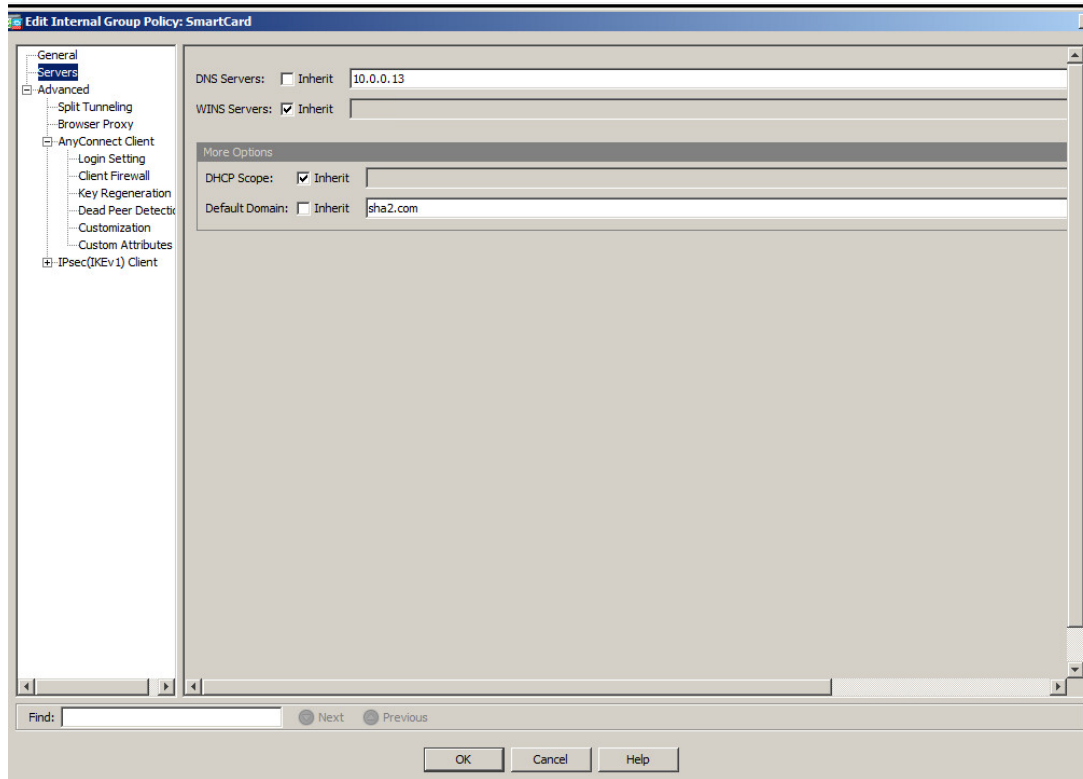
5. On the **Add Internal Group Policy** window, in the left pane, select **General** and complete the fields described in the table below.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Name</b>	Enter a name for the group policy (for example, <b>GroupPolicySSL</b> ).
<b>More Options Tunneling Protocols</b>	Click <b>More Options</b> to expand the window and then do the following in the <b>Tunneling Protocols</b> field to choose the required VPN protocol : <ol style="list-style-type: none"> <li>1. Clear <b>Inherit</b>.</li> <li>2. Select <b>Clientless SSL VPN</b>.</li> <li>3. Select <b>SSL VPN Client</b>.</li> </ol>

6. In the left pane select **Servers**.
7. Deselect **DNS servers: Inherit**, and enter the IP address.
8. Deselect **Default domain: Inherit**, and enter the domain name.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

9. Leave all other configuration fields with their default settings, and click **OK**

## Group Policy - IPsec Protocol

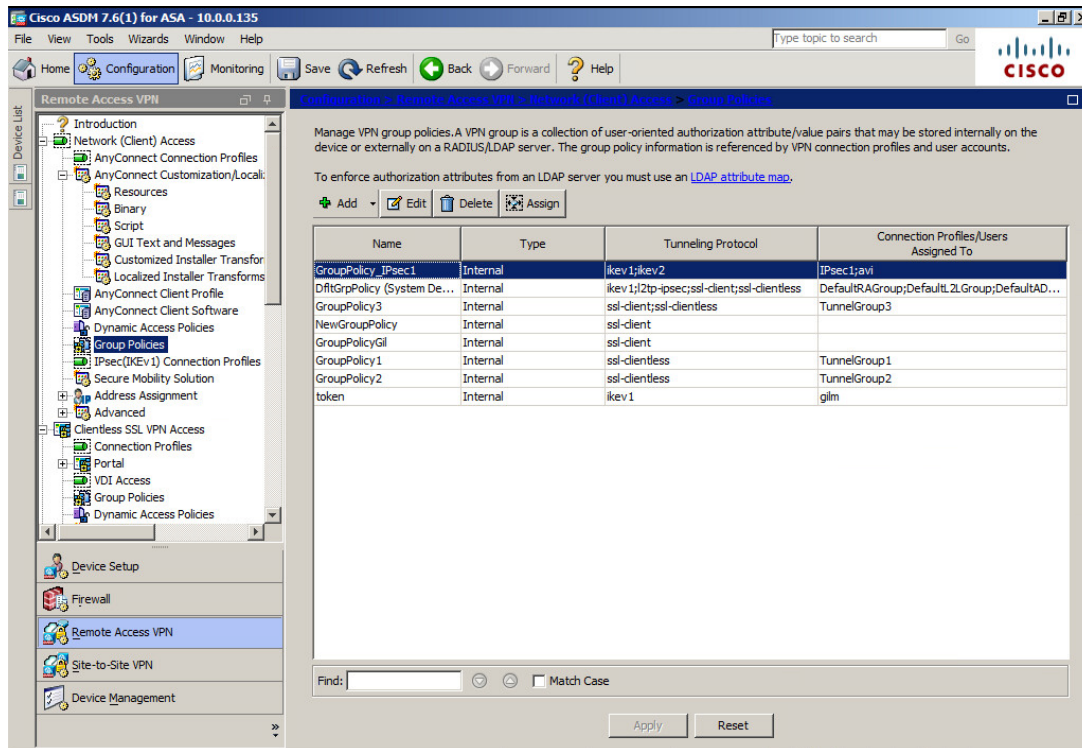
In This example: Group Policy with IPsec Protocol is demonstrated for Client only.

To add a group policy:

1. Open the **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.

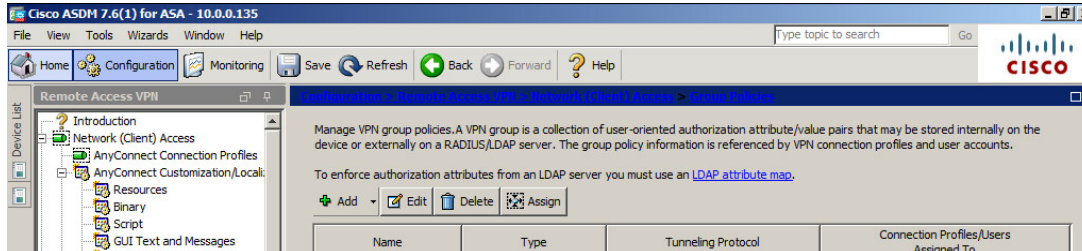


- In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Group Policies**.



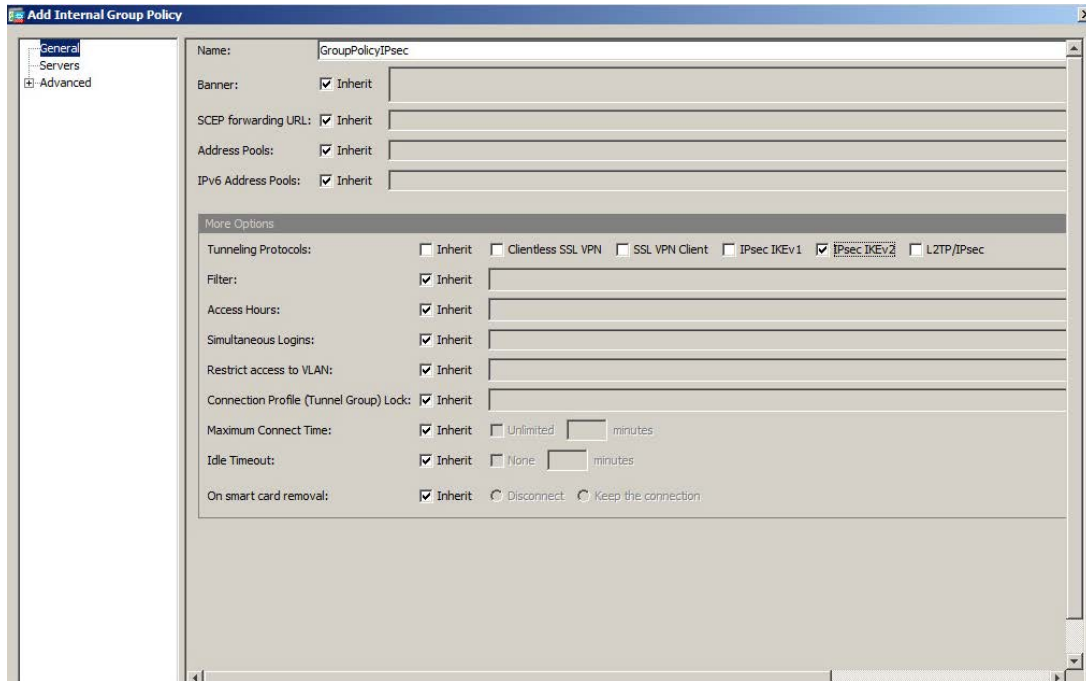
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- In the center pane, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

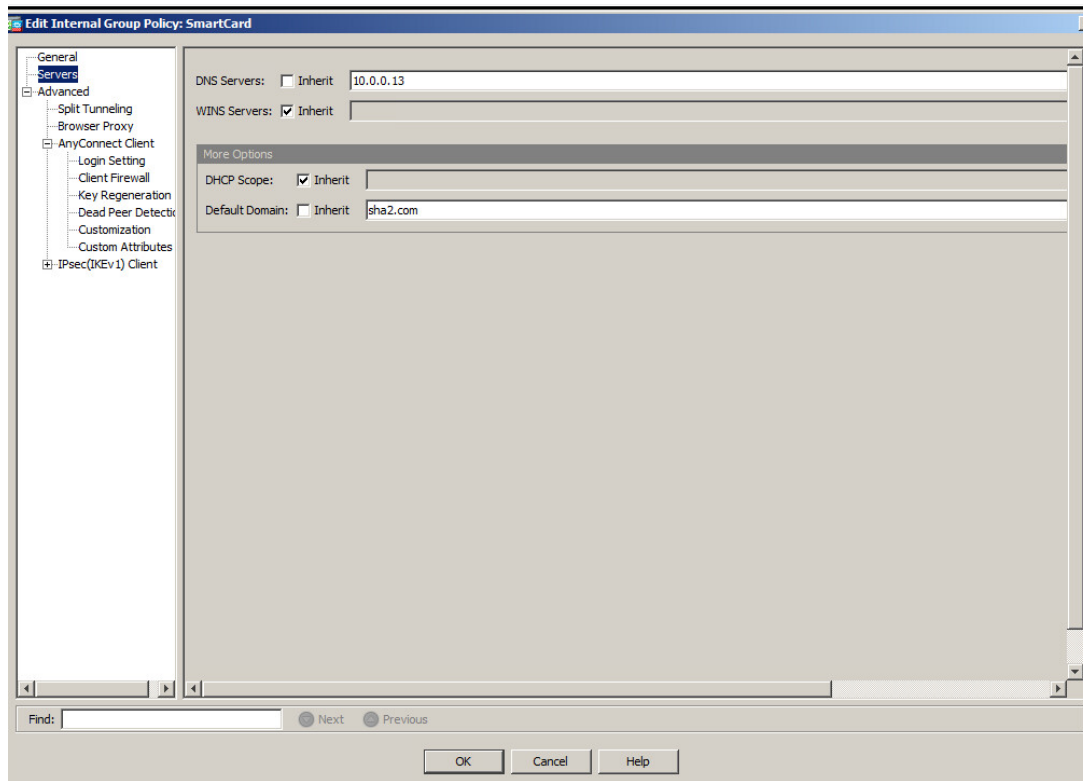
5. On the **Add Internal Group Policy** window, select **General** and complete the fields as described in the table below.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Name</b>	Enter a name for the group policy (for example, <b>GroupPolicyIPsec</b> ).
<b>More Options Tunneling Protocols</b>	Click <b>More Options</b> to expand the window and then do the following in the <b>Tunneling Protocols</b> field choose the required VPN protocol : <ol style="list-style-type: none"> <li>1. Clear <b>Inherit</b>.</li> <li>2. Select <b>IPsec IKEv2</b>.</li> </ol>

6. In the left pane select **Servers**.
7. Deselect **DNS servers: Inherit**, and enter the IP address.
8. Deselect **Default domain: Inherit**, and enter the domain name.



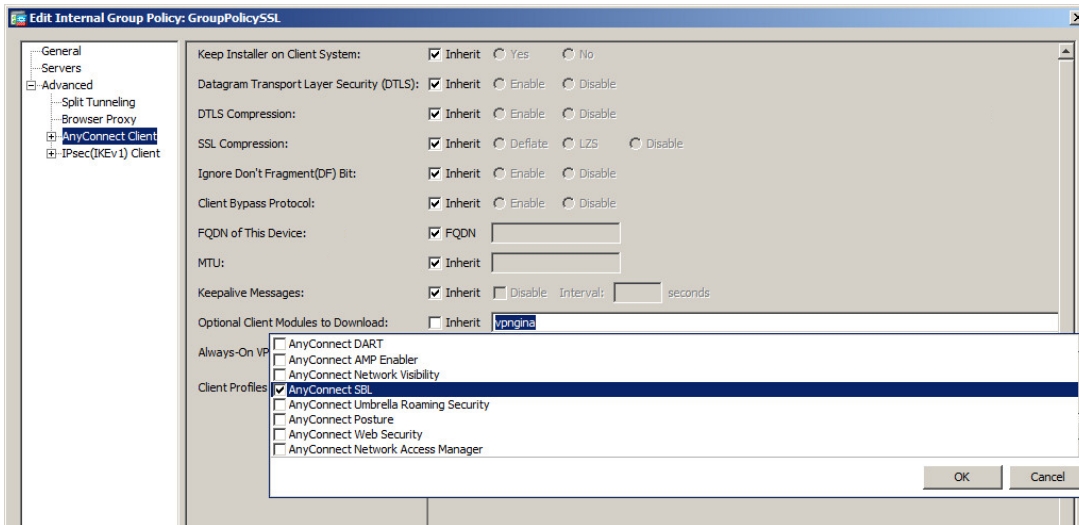
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. Leave all other configuration tabs with their default settings, and click **OK**.

## Group Policy - Enable Start before Logon (SBL)

Start Before Logon (SBL) enables the user to see the AnyConnect GUI logon window before the Windows logon window appears. SBL establishes the VPN connection first.

1. Open the **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Group Policies**.
3. In Group Policy Expand **Advanced**, deselect **Inherit** for **Optional Client Module to Download**, and choose **AnyConnect SBL** from the drop-down list.
4. Click **OK**, click **Apply**, and click **Save**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

## Connection Profile

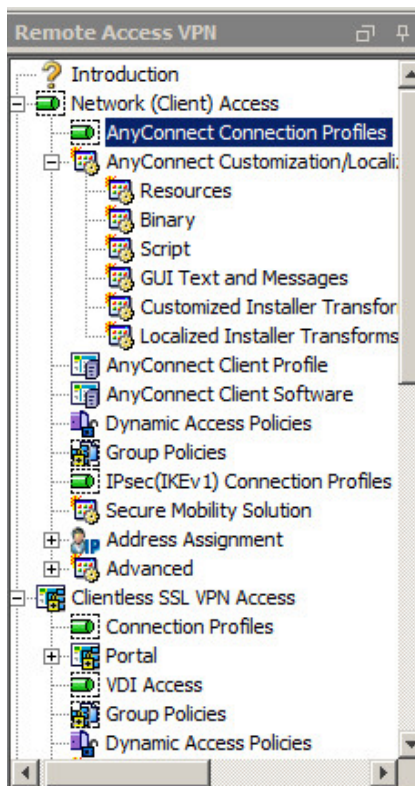
A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating the tunnel itself.

## Configuring a Connection Profile for Network (Client) Access SSL VPN Access

A connection profile consists of a set of records that determines tunnel connection policies.

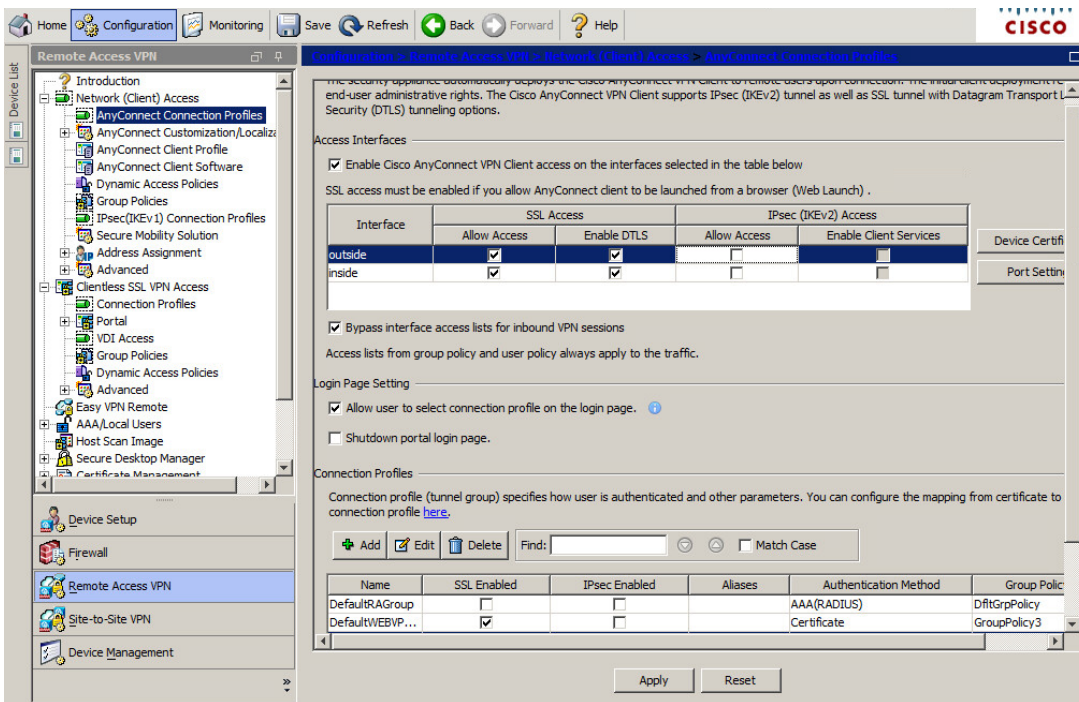
**To configure a connection profile:**

1. Open **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click **Remote Access VPN**, and then select **Network (Client) Access > AnyConnect Connection Profiles**.



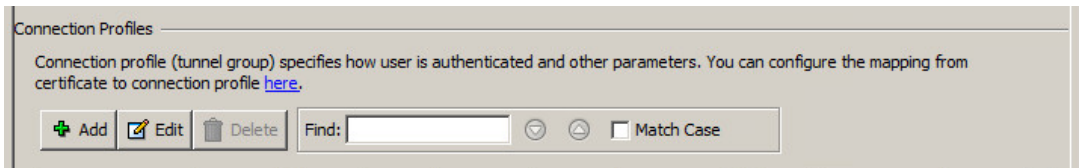
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

4. In the right pane, under **Access Interfaces**, perform the following steps:
  - a. Select **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below**.
  - b. In the Access Interface table, for outside or inside interfaces, under the **SSL Access** column, select **Allow Access and Enable DTLS**.
  - c. Select **Bypass interface access lists for inbound VPN sessions**.
  - d. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.



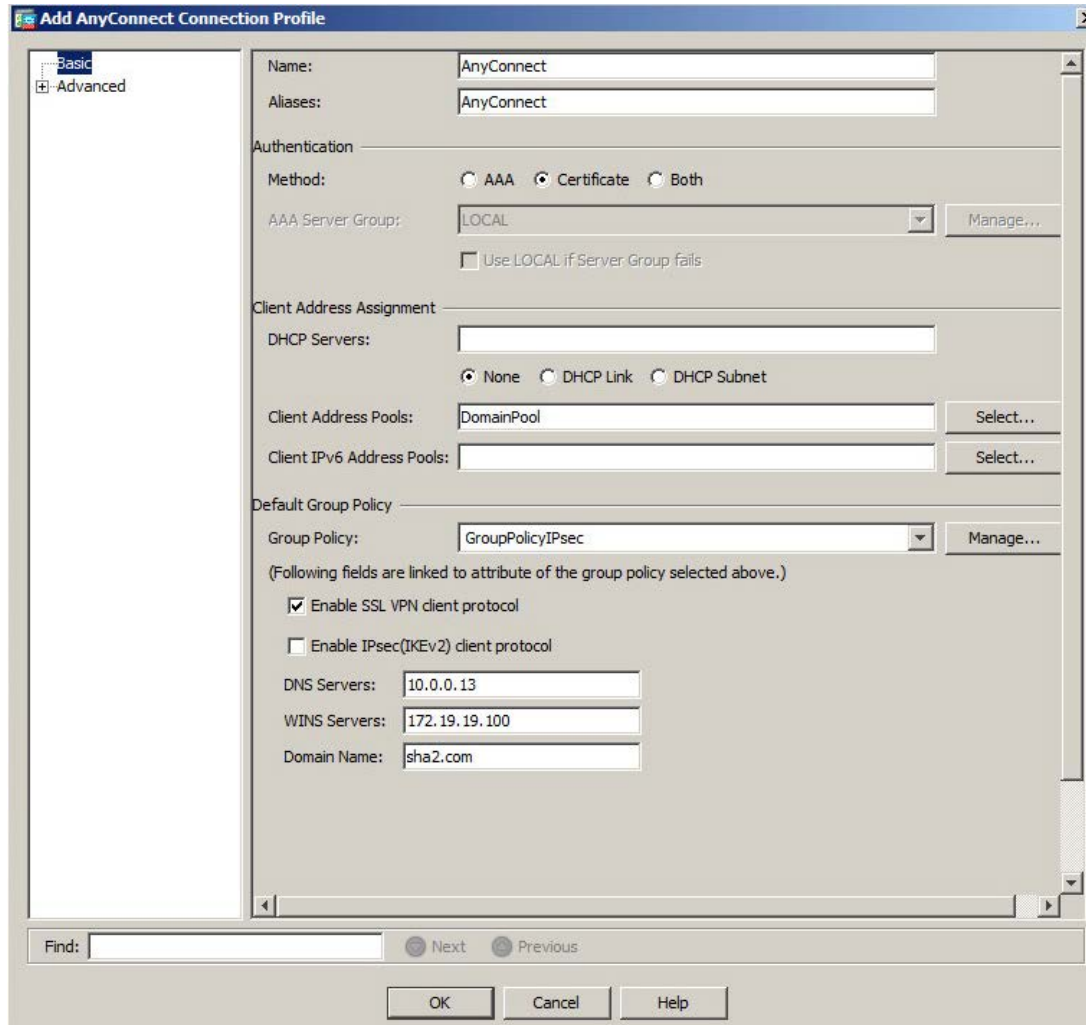
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Under **Connection Profiles**, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

6. In the **Add AnyConnect Connection Profile** window, in the left pane, click **Basic**. In the right pane, complete the fields as described in the table below.

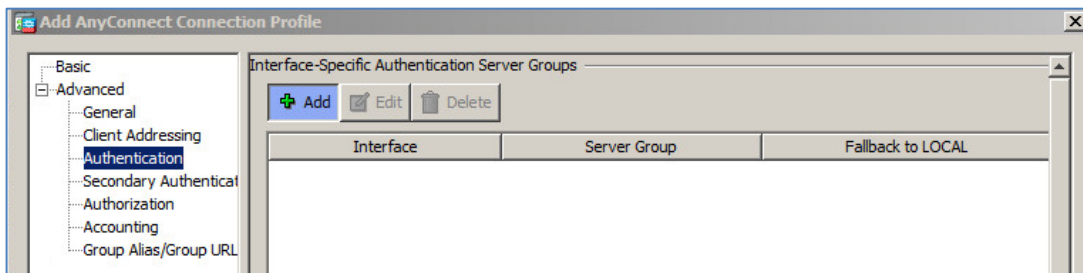


(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Field Name:</b>	Enter the name for the connection profile (for example, <b>AnyConnect</b> ).
<b>Aliases</b>	Enter the <b>Aliases</b> for the connection profile (for example, <b>AnyConnect</b> ). The alias will be displayed to the user.
<b>Authentication</b>	Select the certification authentication method associated with the connection profile.
<b>Client Address Pools</b>	Click <b>Select</b> and then assign an address pool (for example, <b>DomainPool</b> )
<b>Group Policy</b>	Select an appropriate group policy (for example, <b>GroupPolicySSL</b> )
<b>Enable SSL VPN client protocol</b>	Check and enable this option.
<b>DNS Servers</b>	Enter the DNS server details.
<b>Domain Name</b>	Enter the Domain name.

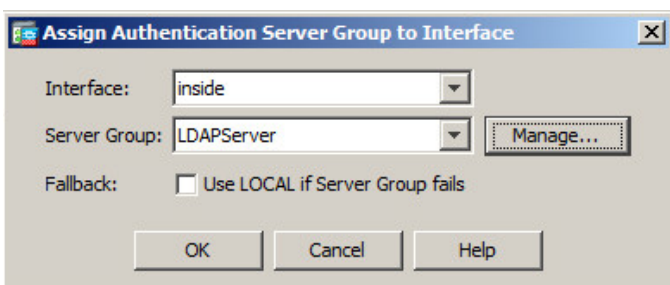


7. In the left pane select **Advanced > Authentication**, and in the right pane click **Add**.



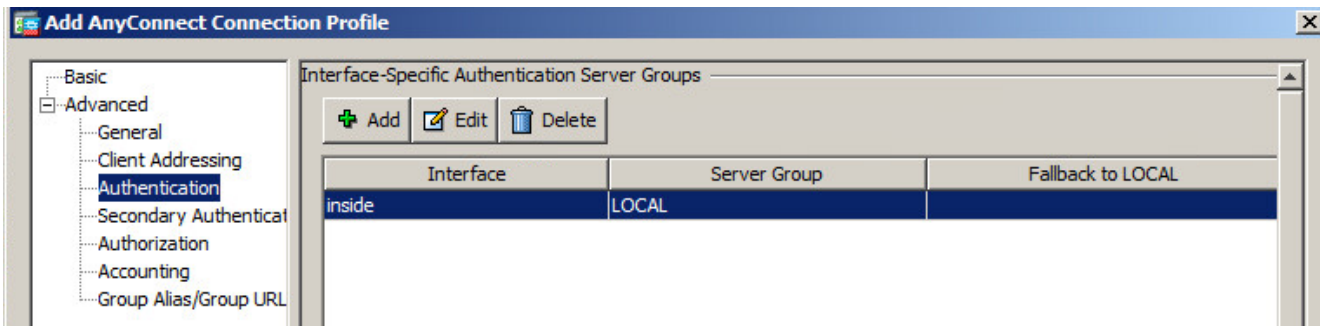
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

8. In the **Assign Authentication Server Group to Interface** window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses to reach the AAA server.
  - b. From the **Server Group** drop down list, choose the previously created AAA server group and click **OK**.



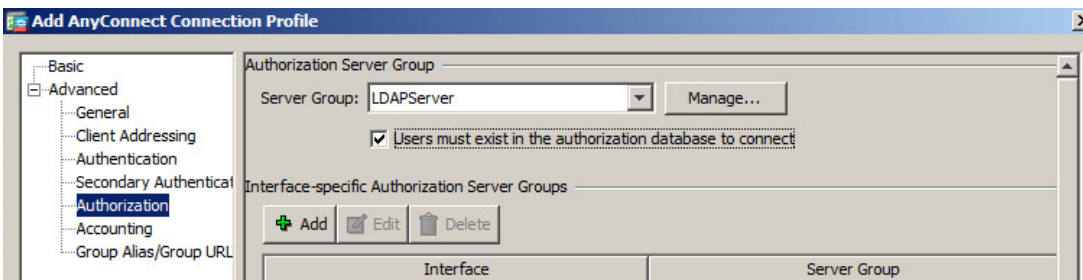
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. In **Authentication**, a server is added to the **Interface** list.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

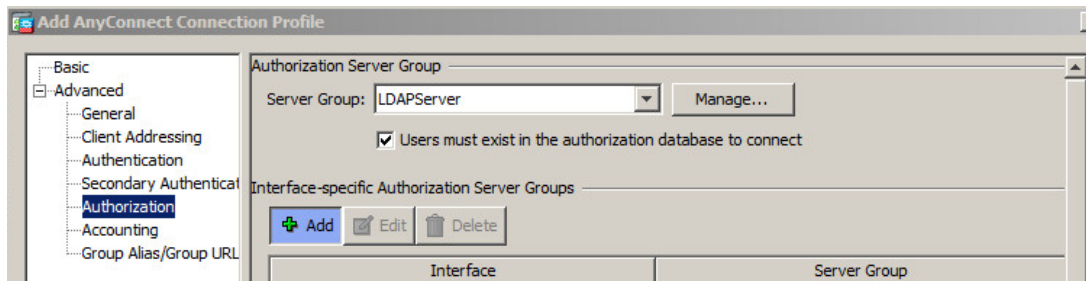
10. In the left pane, select **Advanced > Authorization** and perform the following:
  - a. In **Server Group**, select the previously created AAA server group.
  - b. Select **Users must exist in authorization database to connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)



11. Under **Authorization Server Group** in the right pane, under **Interface-specific Authorization Server Groups**, click **Add**.



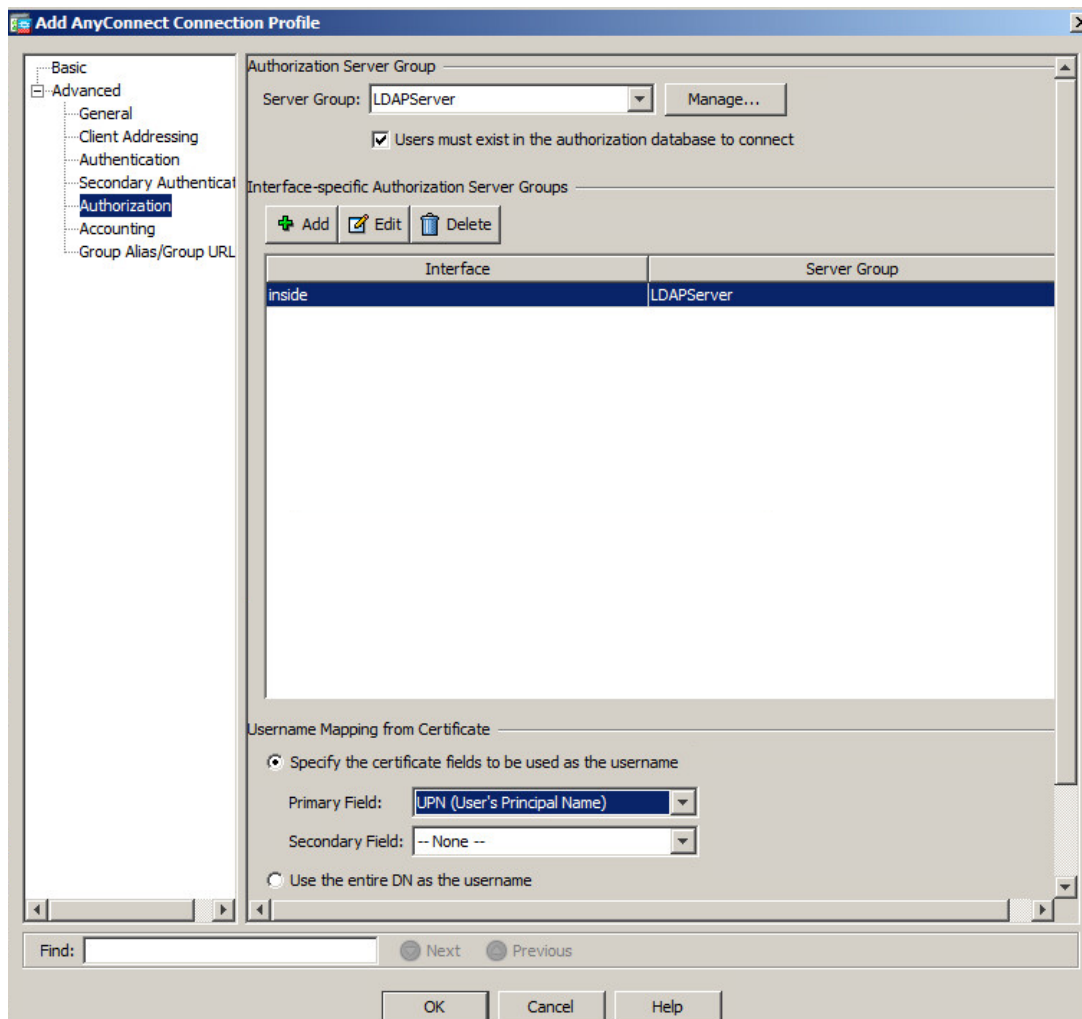
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

12. In the **Assign Authorization Server Group to Interface** window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the **Server Group** drop-down window, select the previously created AAA server group and click **OK**.



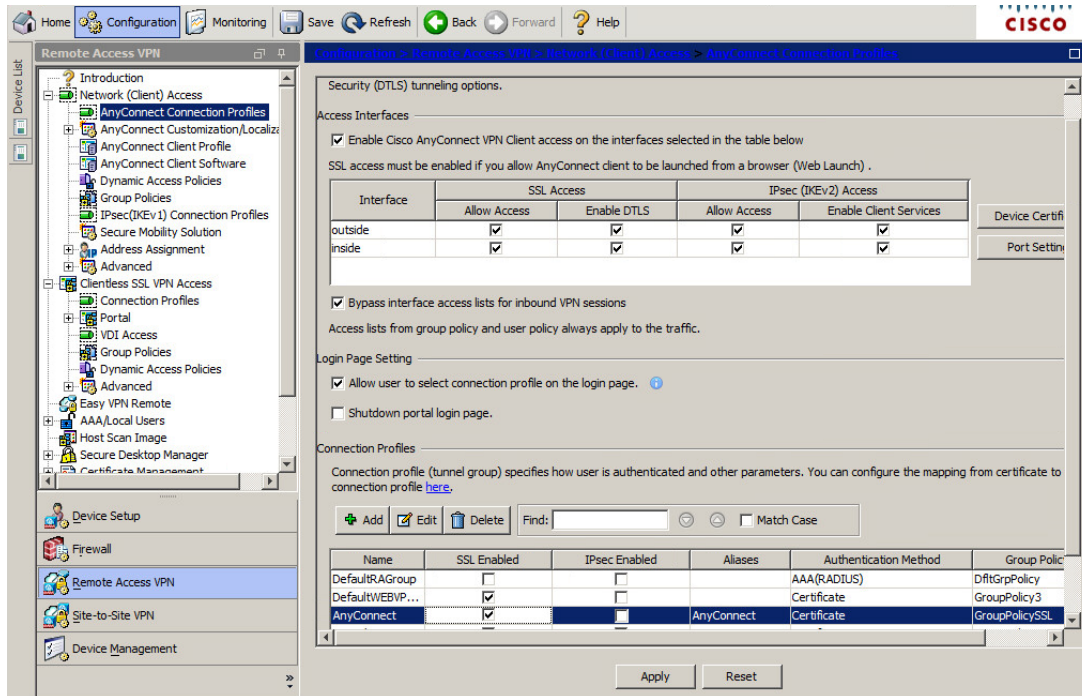
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

13. Under **Authorization Server Group** in the center pane, under **User Mapping from Certificate**, select **Specify the certificate fields to be used as the username**, and perform the following:
  - a. From the **Primary** field drop down-list, select **UPN (User's principal Name)**.
  - b. From the Secondary field drop-down list, select **None** and click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

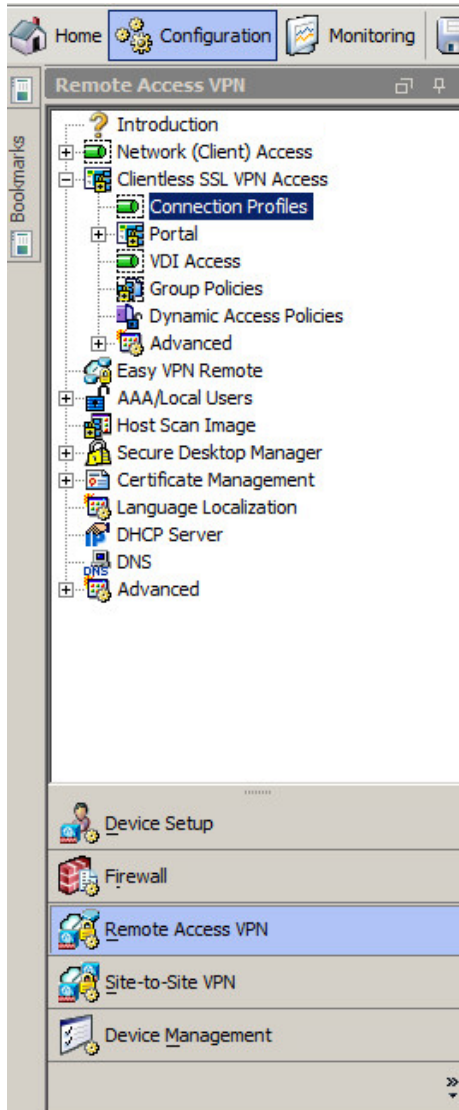
14. If the Connection Profile was added successfully, click **Apply**, then click **Save**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

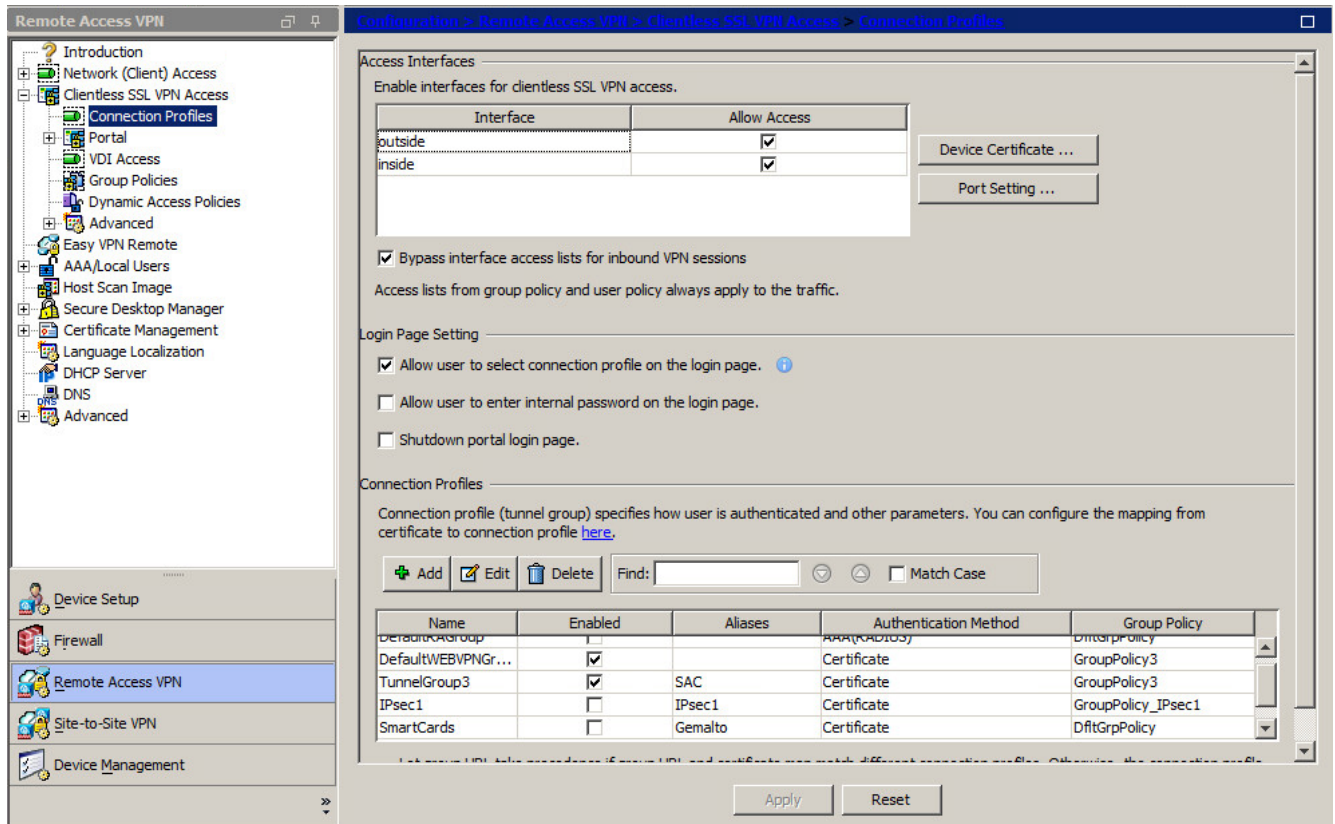
## Configuring a Connection Profile for Clientless SSL VPN Access

1. Open the **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click **Remote Access VPN**, and then select **Clientless SSL VPN Access > Connection Profile**.



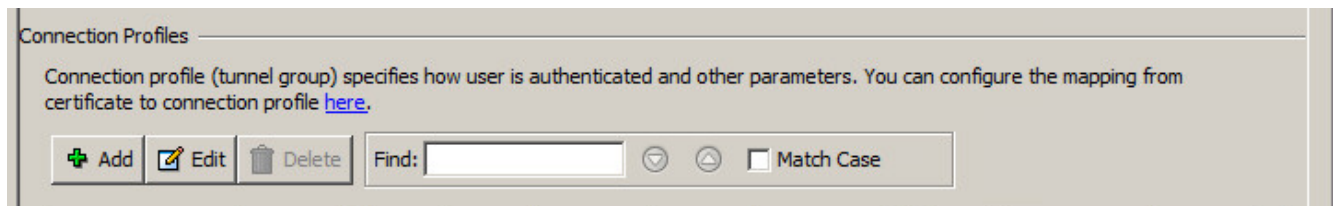
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

4. In the right pane, under **Access Interfaces**, perform the following steps:
  - a. In the **Enable interfaces for clientless SSL VPN access** table, in the **outside** and **inside** interface rows, select **Allow Access**.
  - b. Select **Bypass interface access lists for inbound VPN session**.
  - c. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.



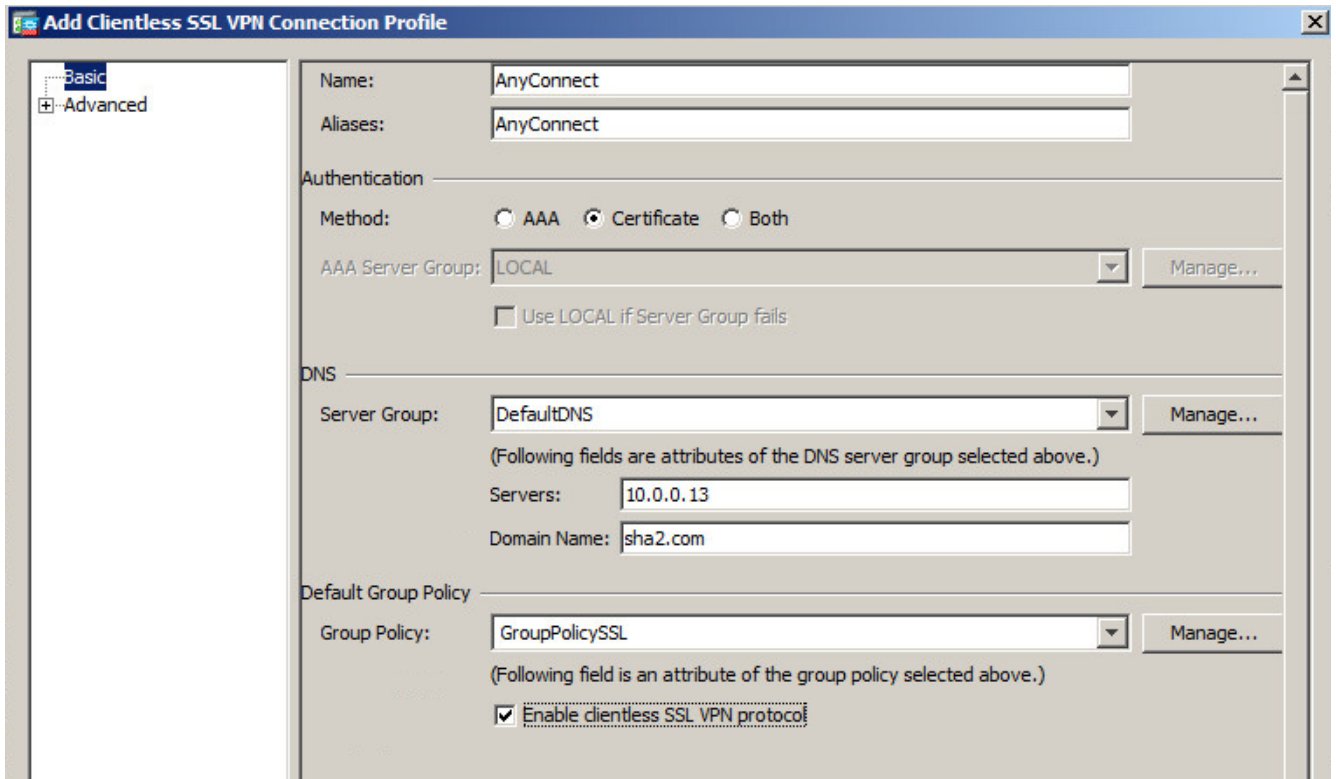
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Under **Connection Profiles** in the right pane, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

6. On the **Add Clientless SSL VPN Connection Profile** window, in the left pane, click **Basic**.
7. In the right pane, enter the fields as described in the table below.

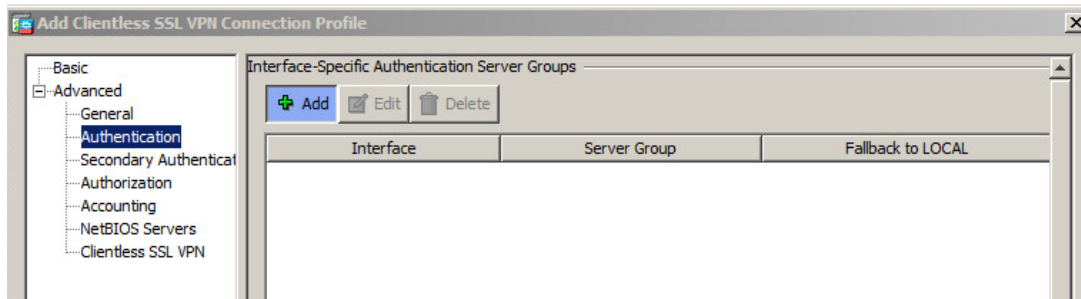


(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Field Name:</b>	Enter the name for the connection profile (for example, <b>AnyConnect</b> ).
<b>Aliases</b>	Enter the <b>Aliases</b> for the connection profile (for example, <b>AnyConnect</b> ). The alias will be displayed to the user.
<b>Authentication</b>	Select <b>Certificate</b> authentication method associated with the connection profile.
<b><i>Under DNS</i></b>	
<b>Server Group</b>	<b>Select</b> the <b>DNS</b> server group needed (DNS server group needed to be added).
<b>Servers</b>	Enter the DNS server detail.
<b>Domain Name</b>	Enter the Domain name.
<b><i>Under Default Group Policy</i></b>	
<b>Group Policy</b>	Select an appropriate group policy (for example, <b>GroupPolicySSL</b> ).
<b>Enable clientless SSL VPN protocol</b>	Check this option.

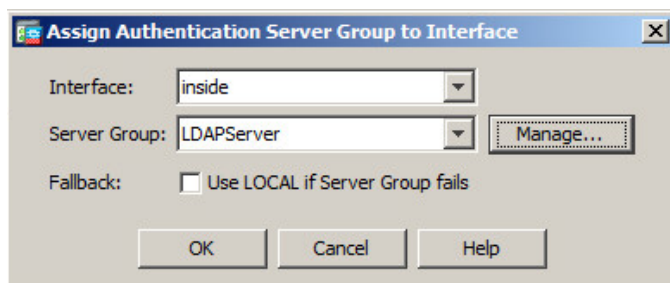


8. In the right pane select **Advanced > Authentication**, and in the center pane click **Add**.



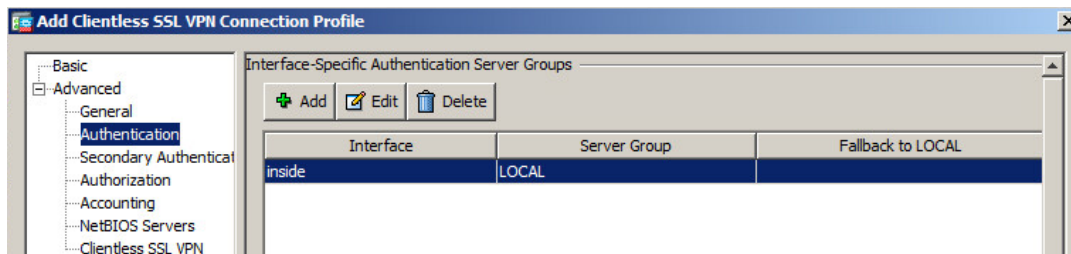
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. In the **Assign Authentication Server Group to Interface** window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the **Server Group** drop-down list, select the previously created AAA server group and click **OK**.



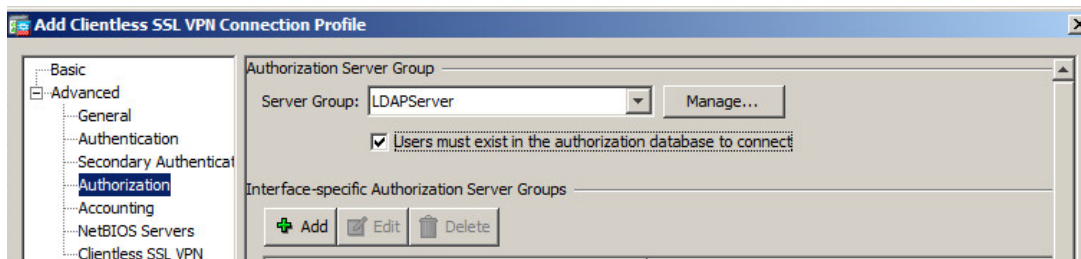
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

Under **Authentication, Interface-Specific Server Groups**, a server was added in the **Interface** column.



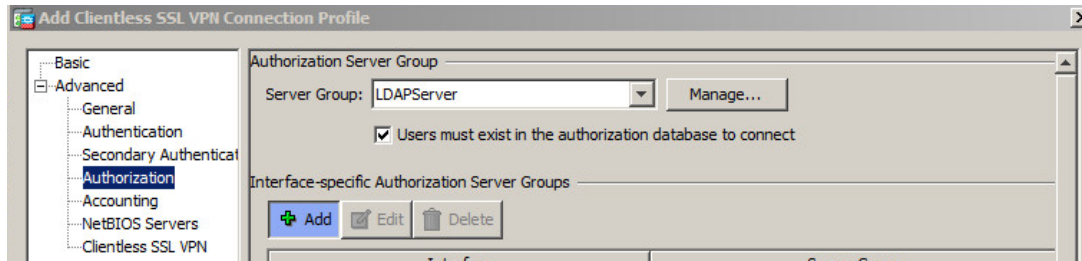
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

10. In the right pane expand **Advanced**, click on **Authorization** and perform the following:
  - a. From the **Server Group** drop-down list, select the previously created AAA server group.
  - b. Select **Users must exist in authorization database to connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

11. Under **Interface-specific Authorization Server Groups** click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

12. In the **Assign Authorization Server Group** window, perform the following:

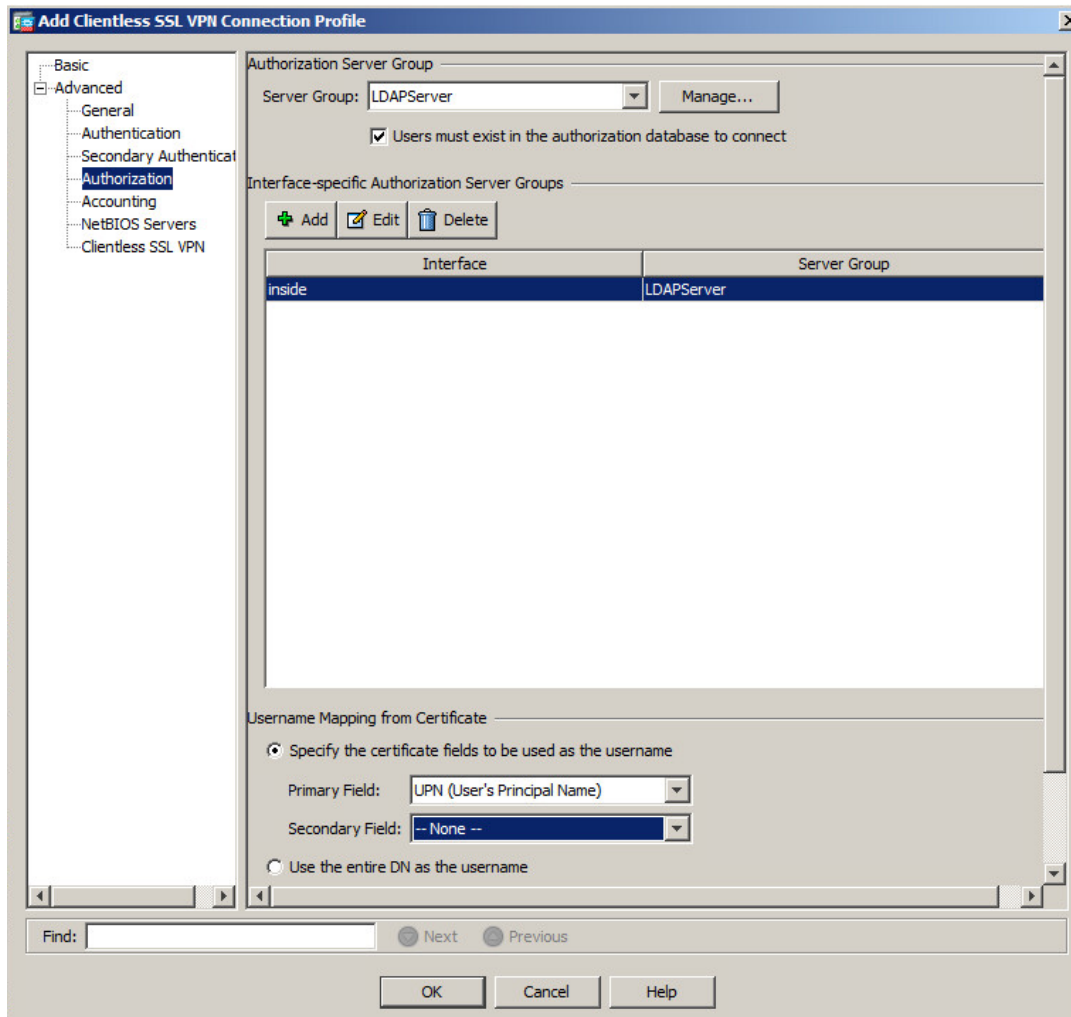
- a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server
- b. From the **Server Group** drop-down list, choose the previously created AAA server group and click **OK**



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

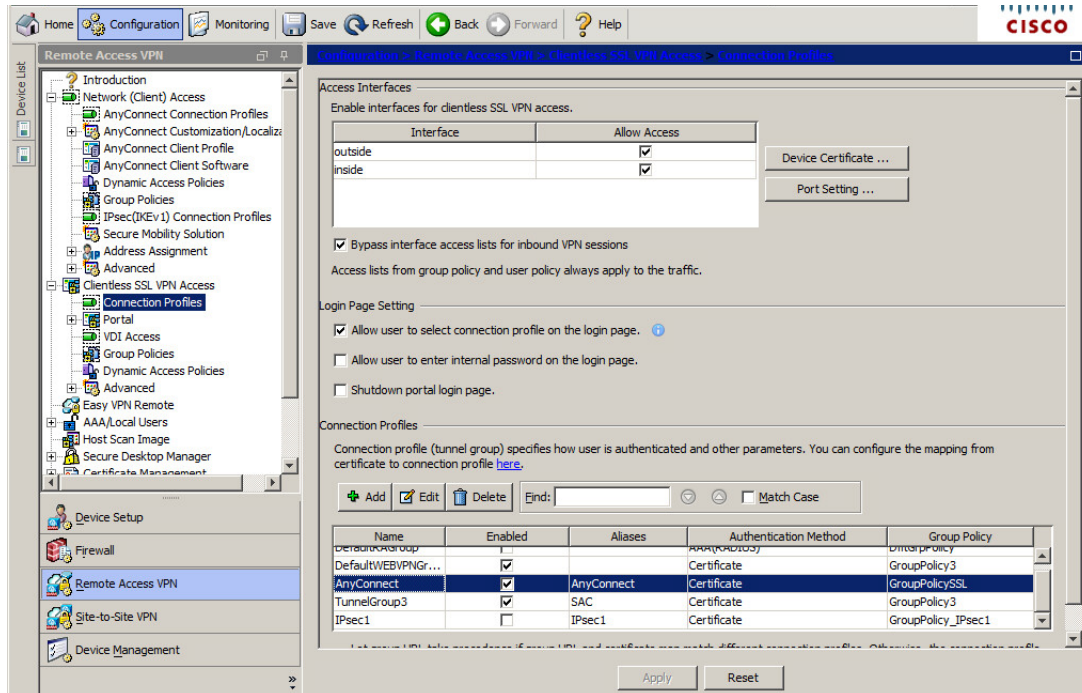


13. Under **User Mapping from Certificate** perform the following:
  - a. Select **Specify the certificate fields to be used as the username**.
  - b. From the **Primary Field** drop-down list, select **UPN (User's principal Name)**.
  - c. From the **Secondary Field** drop-down list, select **None** and click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

14. If the Connection Profile was added successfully, click **Apply** and then click **Save**.



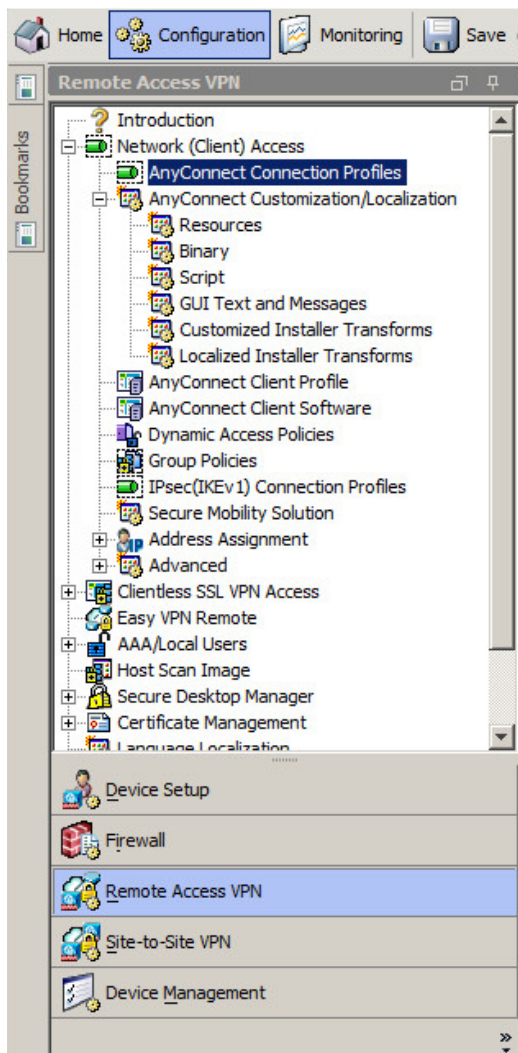
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Configuring a Connection Profile for AnyConnect Client IPSEC Remote Access VPN

A connection profile consists of a set of records that determines tunnel connection policies.

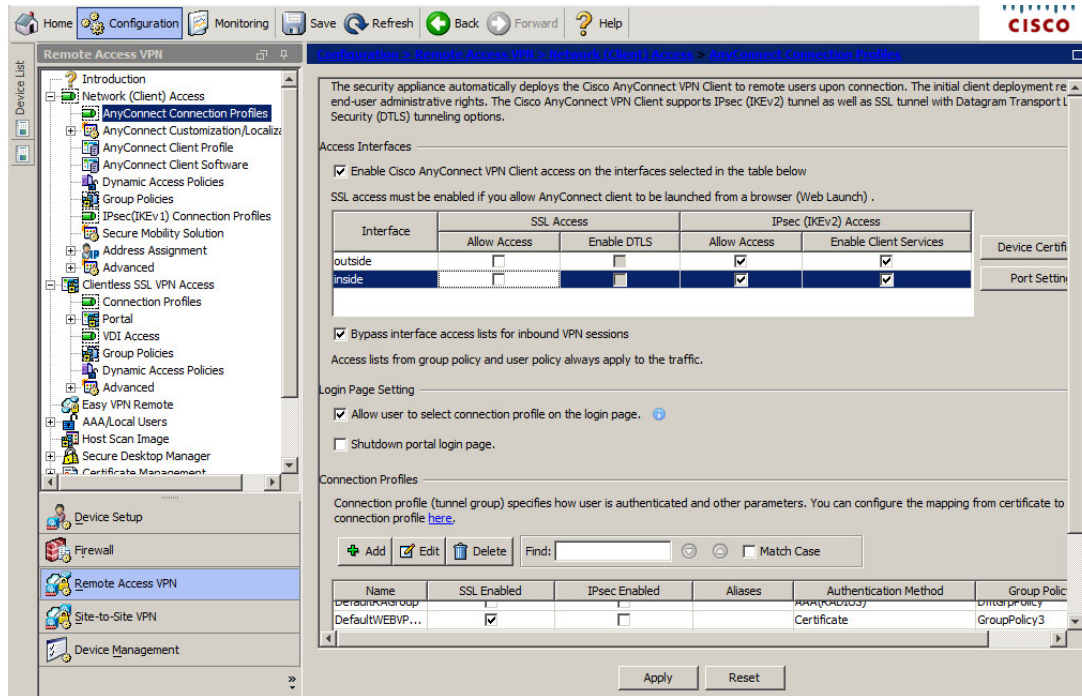
**To configure a connection profile:**

1. Open **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click **Remote Access VPN**, and then select **Network (Client) Access > AnyConnect Connection Profiles**.



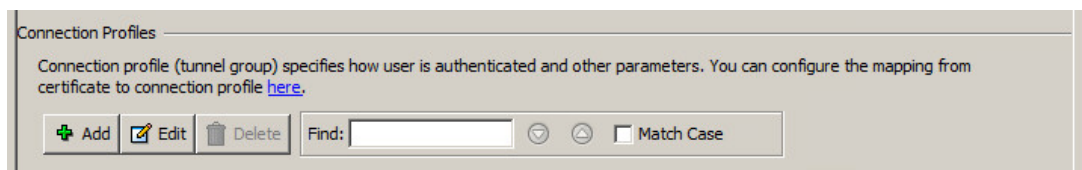
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

4. In the middle pane, under **Access Interfaces**, perform the following steps:
  - a. Select **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below**.
  - b. In the table, for outside or inside interfaces in the **IPsec (IKEv2) Access** column, select **Allow Access** and **Enable Client Services**.
  - c. Select **Bypass interface access lists for inbound VPN sessions**.
  - d. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.



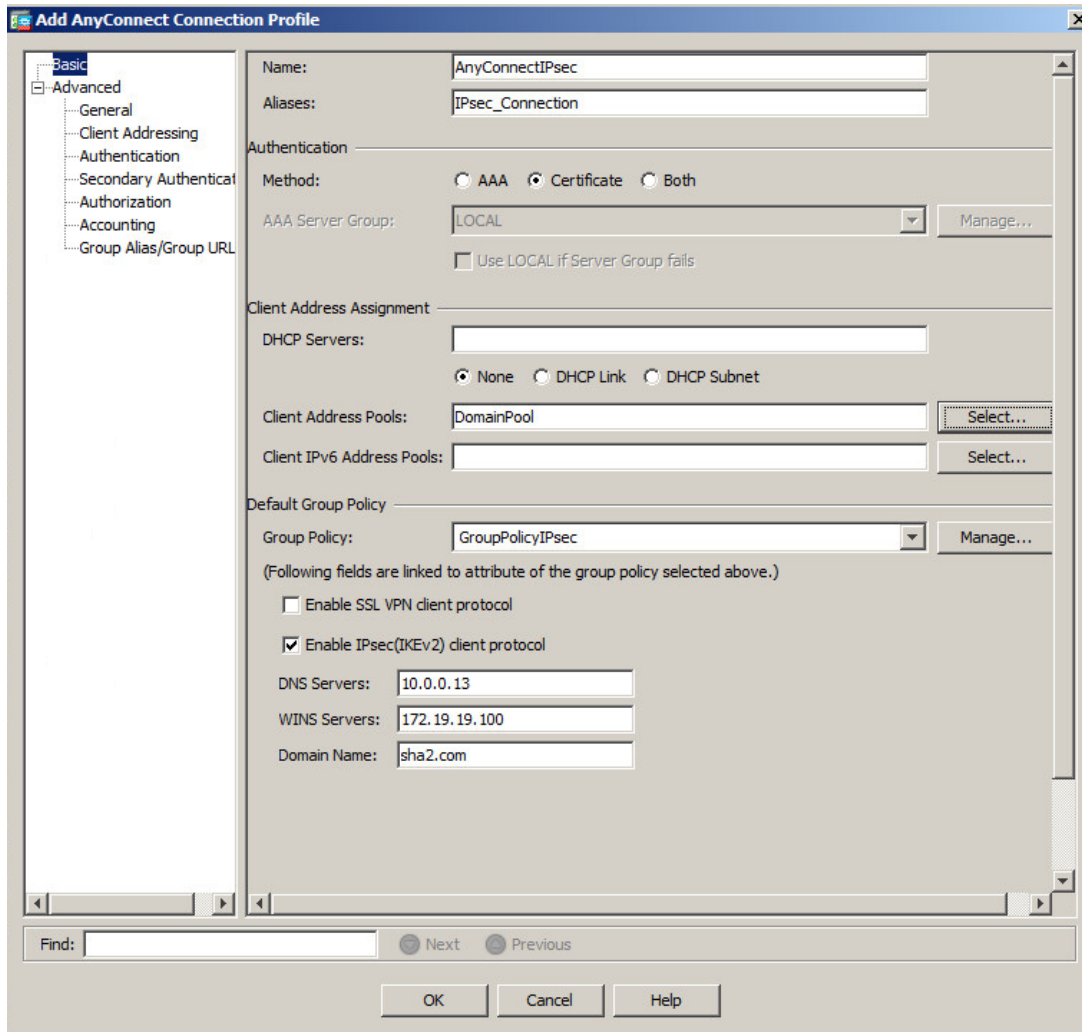
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Under **Connection Profiles**, in the middle pane, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

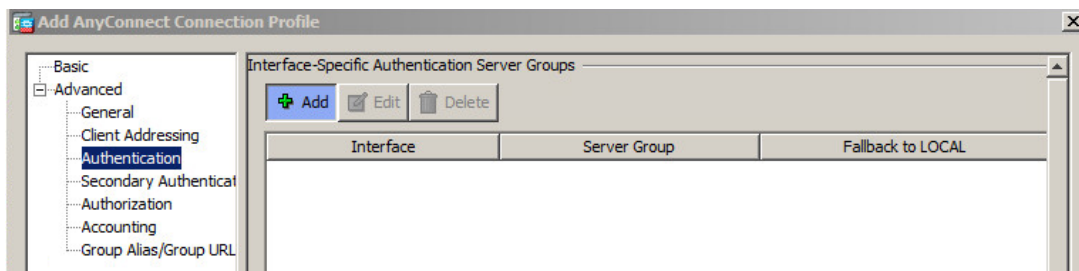
6. On the **Add AnyConnect Connection Profile** window, in the left pane, select **Basic**, and in the right pane, complete the fields as described in the table below.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

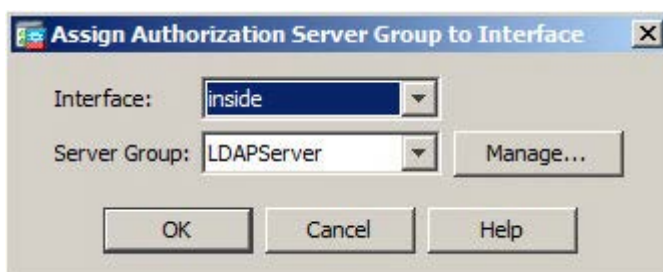
<b>Field Name:</b>	Enter the name for the connection profile (for example, <b>AnyConnectIPsec</b> ).
<b>Aliases</b>	Enter the <b>Aliases</b> for the connection profile (for example, <b>IPsec_Connection</b> ). The alias will be displayed to the user.
<b>Authentication</b>	Select <b>Certificate</b> authentication method associated with the connection profile.
<b>Client Address Pools</b>	Click <b>Select</b> and then assign an address pool (for example, <b>DomainPool</b> ).
<b>Group Policy</b>	Select an appropriate group policy (for example, <b>GroupPolicyIPsec</b> ).
<b>Enable IPsec (IKEv2) client protocol</b>	Check this option.
<b>DNS Servers</b>	Enter the DNS server detail.
<b>Domain Name</b>	Enter the Domain name.

7. In the left pane, select **Advanced > Authentication** and in the right pane click **Add**.



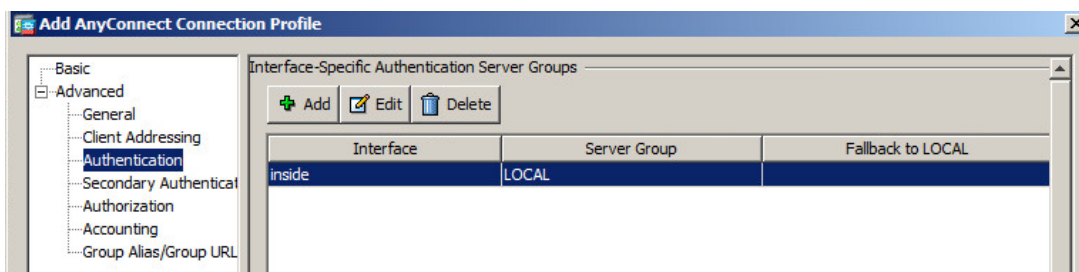
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

8. In the **Assign Authorization Server Group** window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the **Server Group** drop-down list, choose the previously created AAA server group and click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

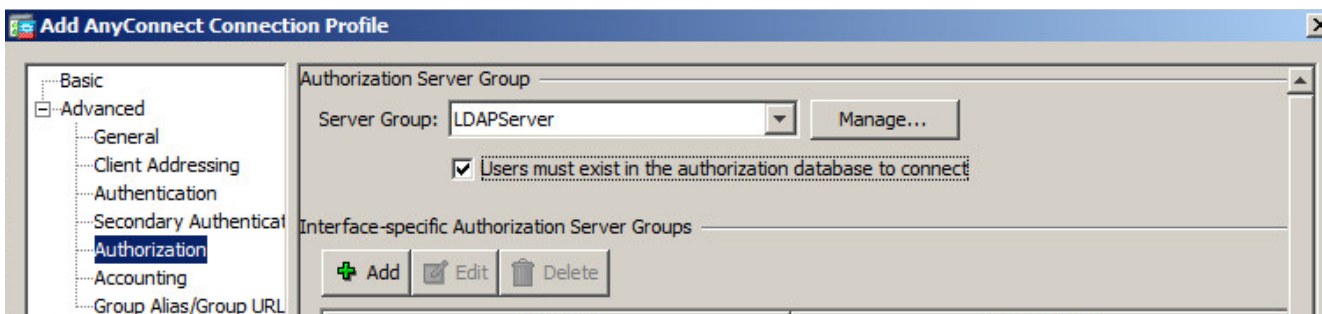
In **Authentication > Interface-Specific Authentication Server Groups**, a Server was added to the list.



(The screen

image above is from Cisco. Trademarks are the property of their respective owners.)

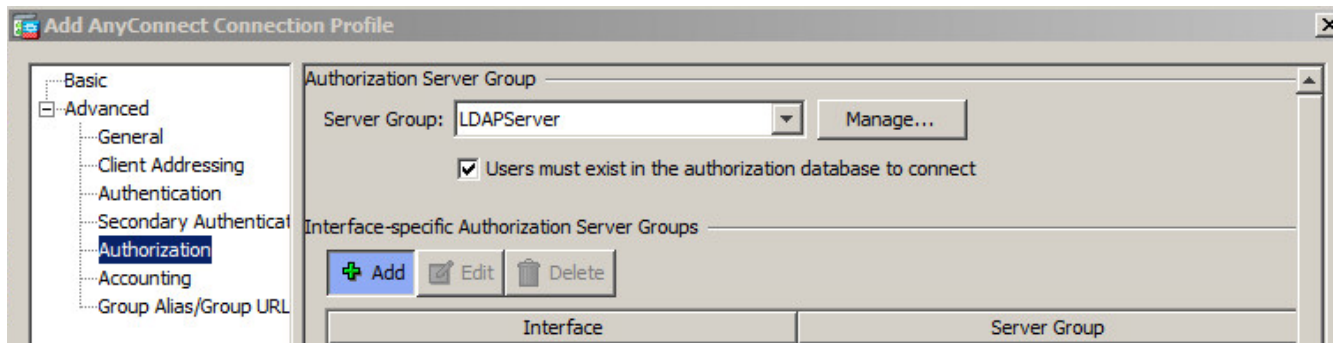
9. In the left pane, select **Advanced > Authorization** and perform the following:
  - a. In the **Server Group** field, select previously created AAA server group.
  - b. Select **Users must exist in authorization database to connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)



10. Under **Authorization Server Group**, in the center pane, under **Interface-specific Authorization Server Group**, click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

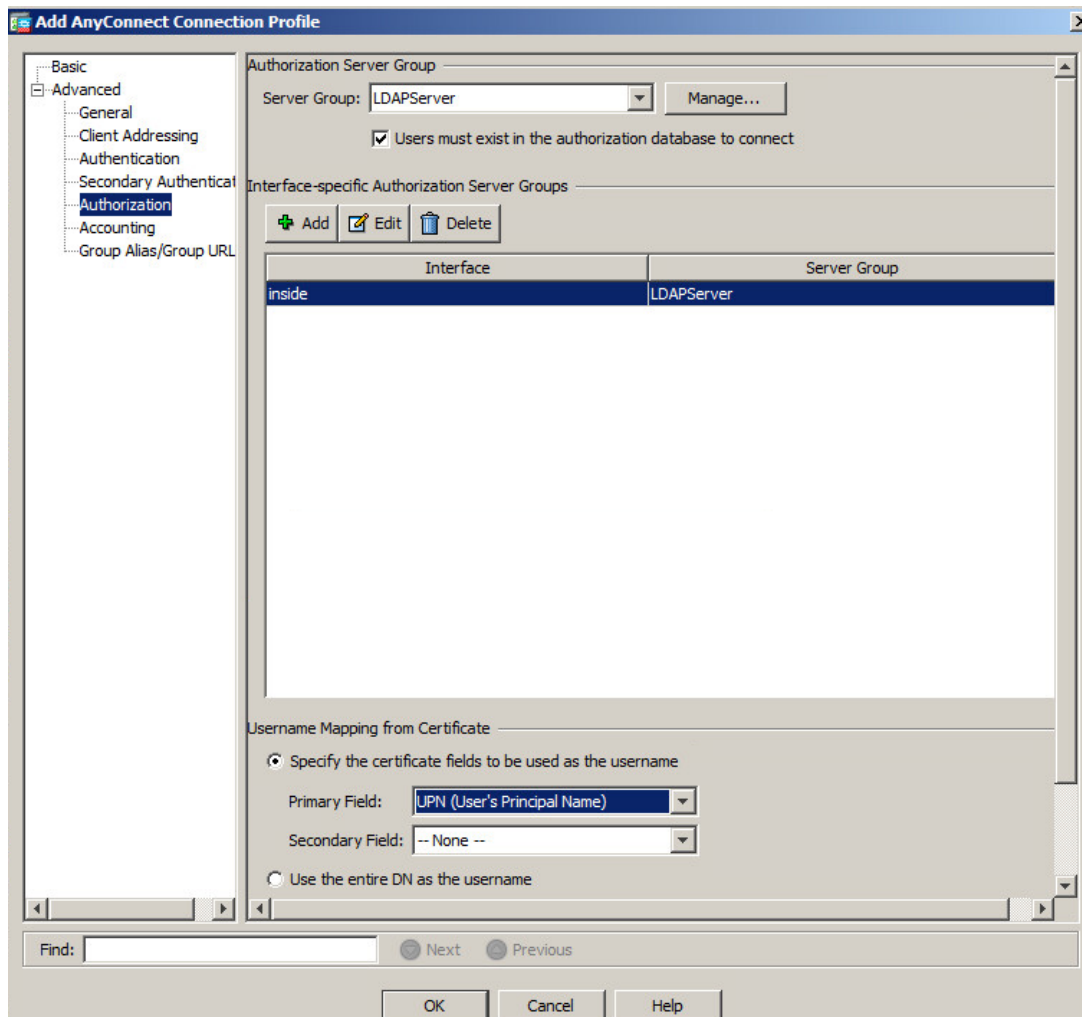
11. In the **Assign Authorization Server Group** window, perform the following:
- From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - From the **Server Group** drop-down list, choose the previously created AAA server group and click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

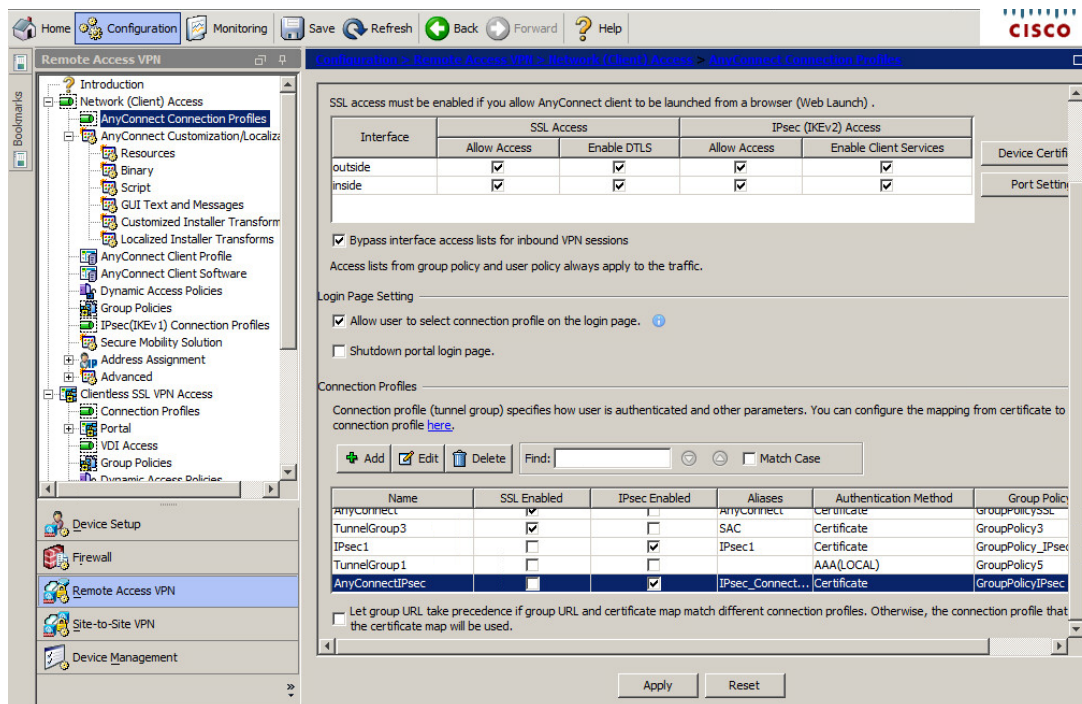


12. In Authorization Server Group, under **User Mapping from Certificate** perform the following:
  - a. Select **Specify the certificate fields to be used as the username**.
  - b. From the **Primary Field** drop-down list, select **UPN (User's principal Name)**.
  - c. Form the **Secondary Field** drop-down list, select **None** and click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

13. If the Connection Profile was added successfully, click **Apply** and then click **Save**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

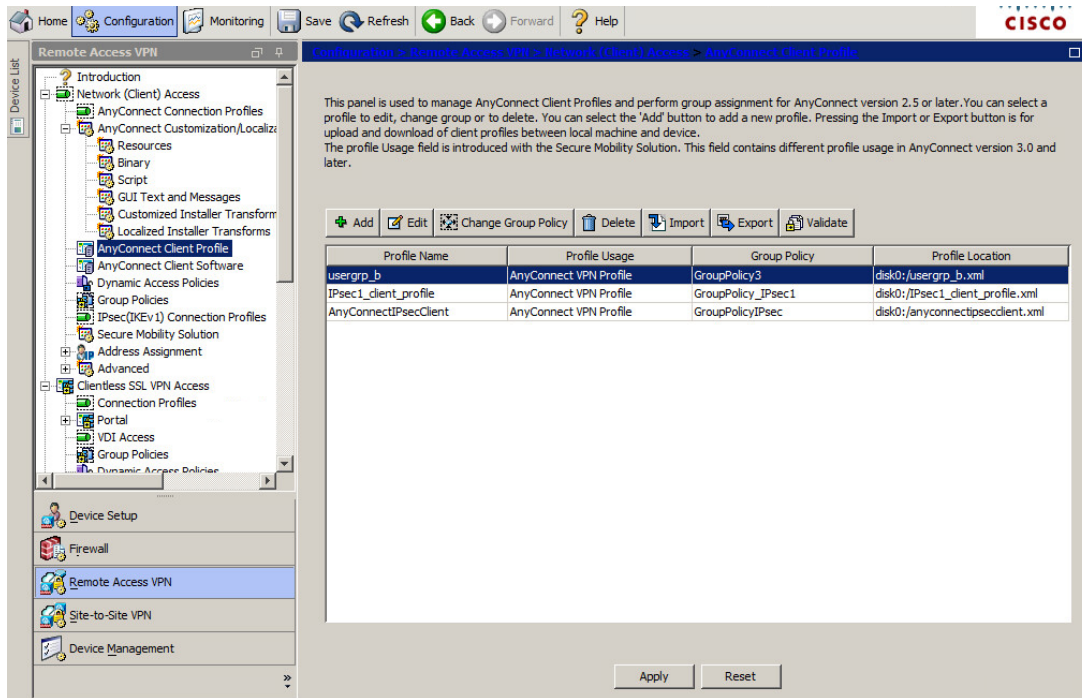
## Any Connect Client Profile

This Option is used to manage AnyConnect Client Profile. In this example the option is demonstrated with IPsec Connection.

**To configure an AnyConnect Client profile:**

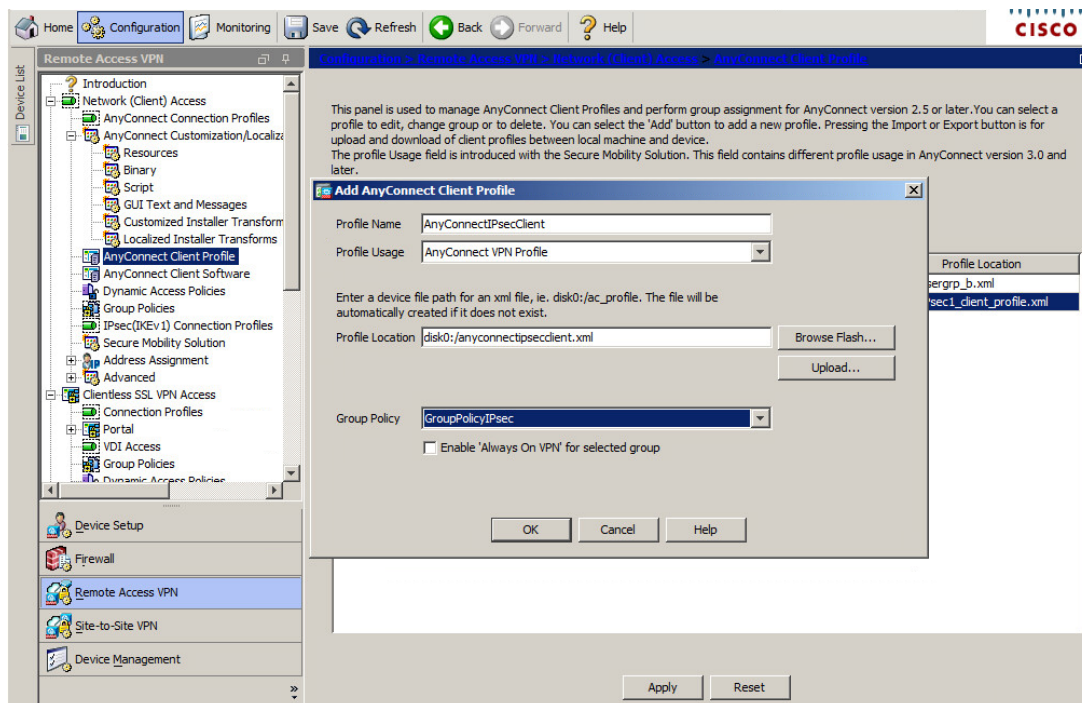
1. Open **Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA**.
2. On the main window, click the **Configuration** tab.

- In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Any Connect Client Profile**



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

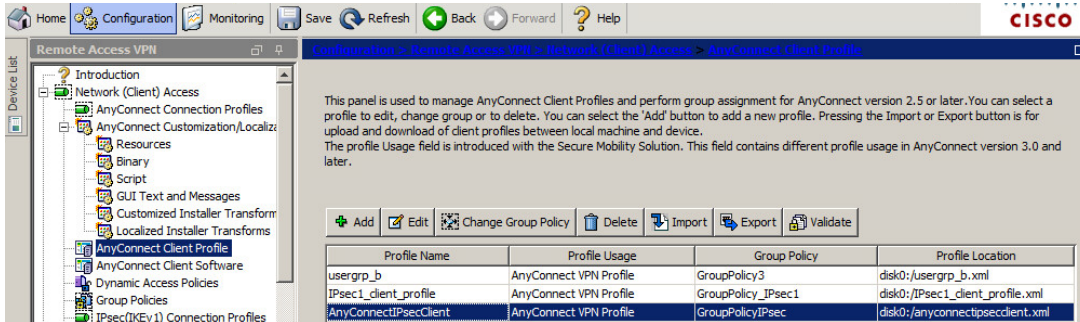
- Under **Connection Profiles**, in the right pane, click **Add** and complete the fields in the **AnyConnect Client Profile** window, as described in the table below, and then click **OK**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

<b>Profile Name</b>	Enter the name for the connection profile (for example, <b>AnyConnectIPsecClient</b> ).
<b>Profile Usage</b>	Choose <b>AnyConnect VPN Profile</b>
<b>Group Policy</b>	Select an appropriate group policy (for example, <b>GroupPolicyIPsec</b> )

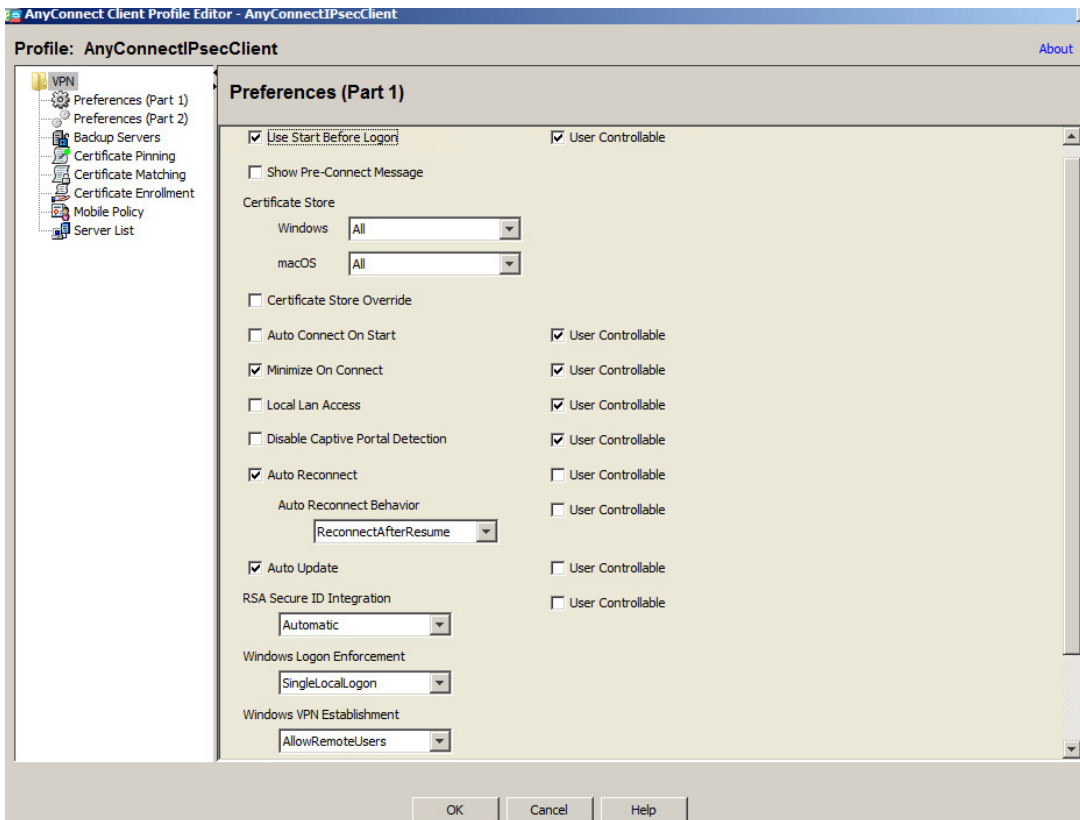
5. Click On the new profile created (In this example, **AnyConnectIPsecClient**) and in the right pane click **Edit**



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

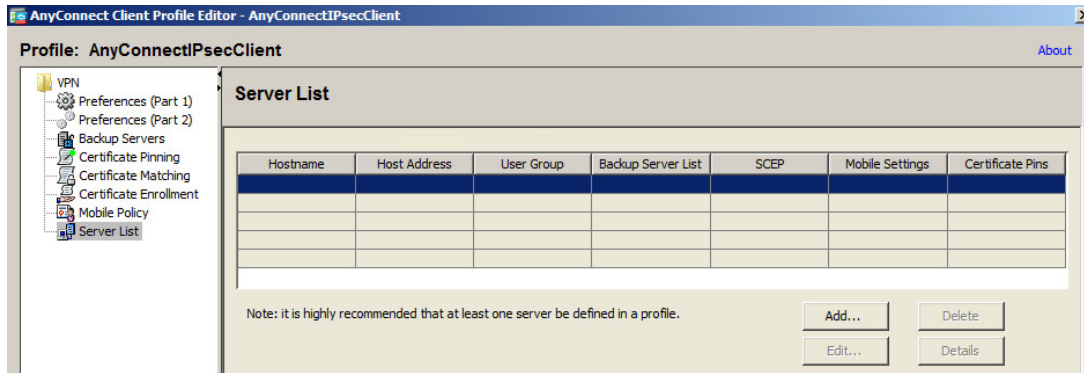
6. Under **AnyConnect Client Profile Editor** click on left pane click on **VPN** and perform the following:

- a. Select **Use Start Before Logon**.
- b. Under **Windows VPN Establishment**, from the drop-down list choose **AllowRemoteUsers**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

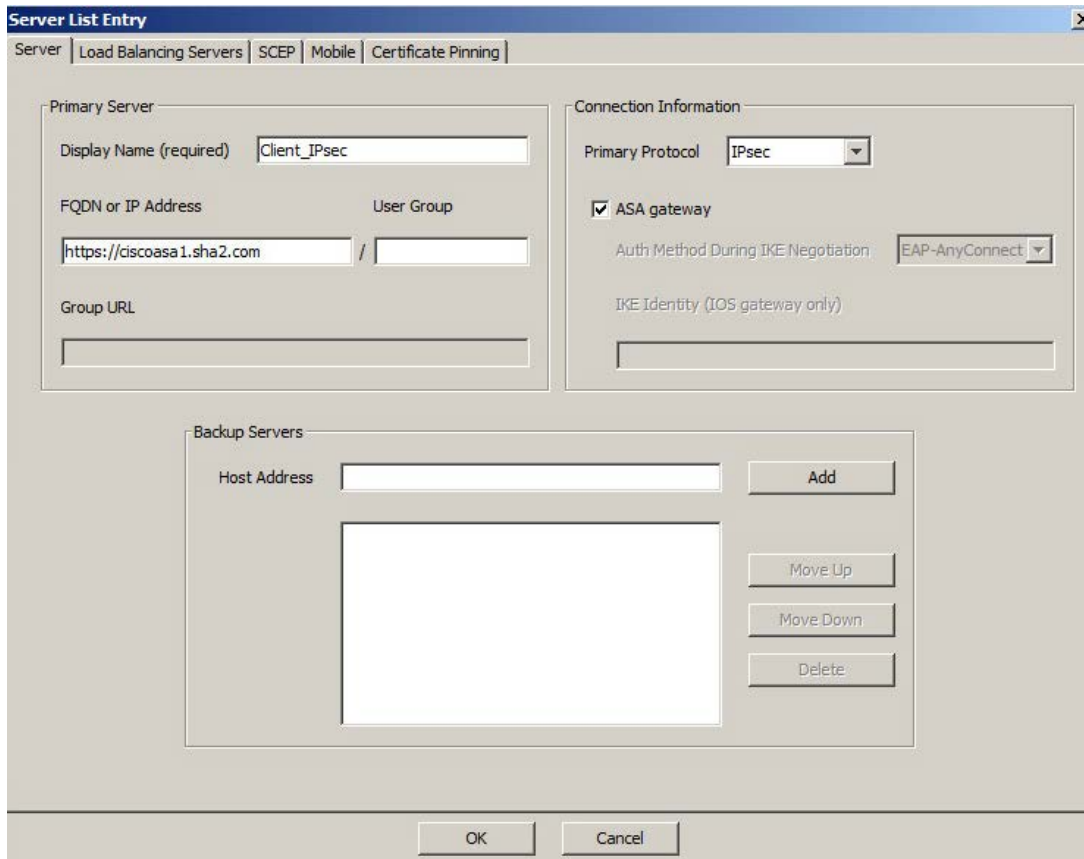
7. In the **AnyConnect Client Profile Editor** window, select **Server List** and click **Add**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

8. In the **Server List Entry** window, perform the following and click **OK**:

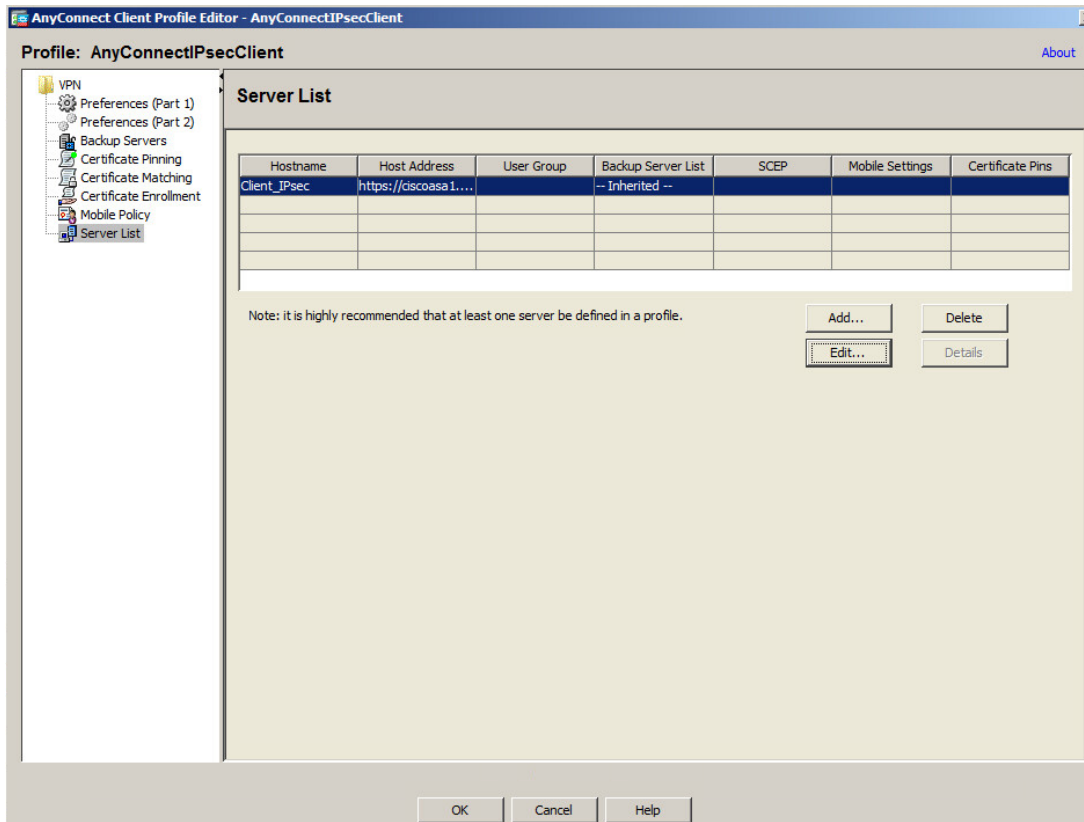
- a. In the **Display Name (required)** field, enter in the name that will be displayed on the client.
- b. In the **FQDN or IP Address** field, enter the ASA Gateway FQDN or IP Address.
- c. Under **Connection Information**, in the **Primary Protocol** field, select **IPsec**.
- d. Select **ASA Gateway**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

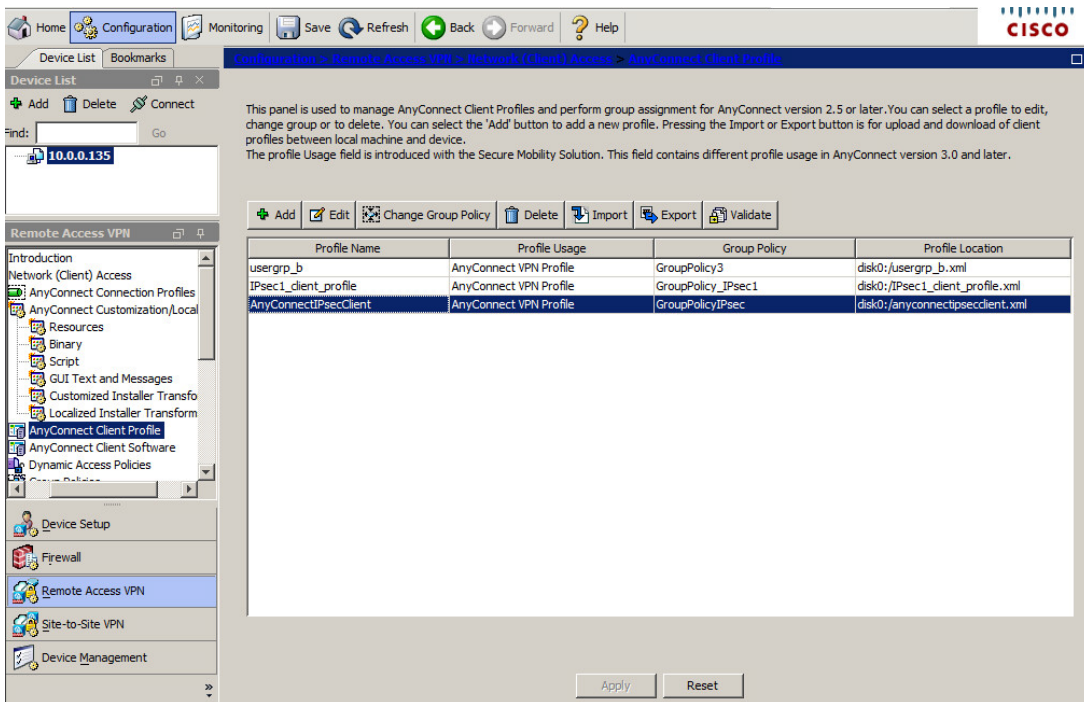


9. If the server list was added successfully, click **OK**, click **Apply**, and click **Save**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

10. The client profile XML file is created. Click **Export** to save this XML profile.



**NOTE:**

In this example the XML file is imported to the client manually after Client Installation is performed (see page 51).

**Win 7 Client Profile Import Path:**

%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

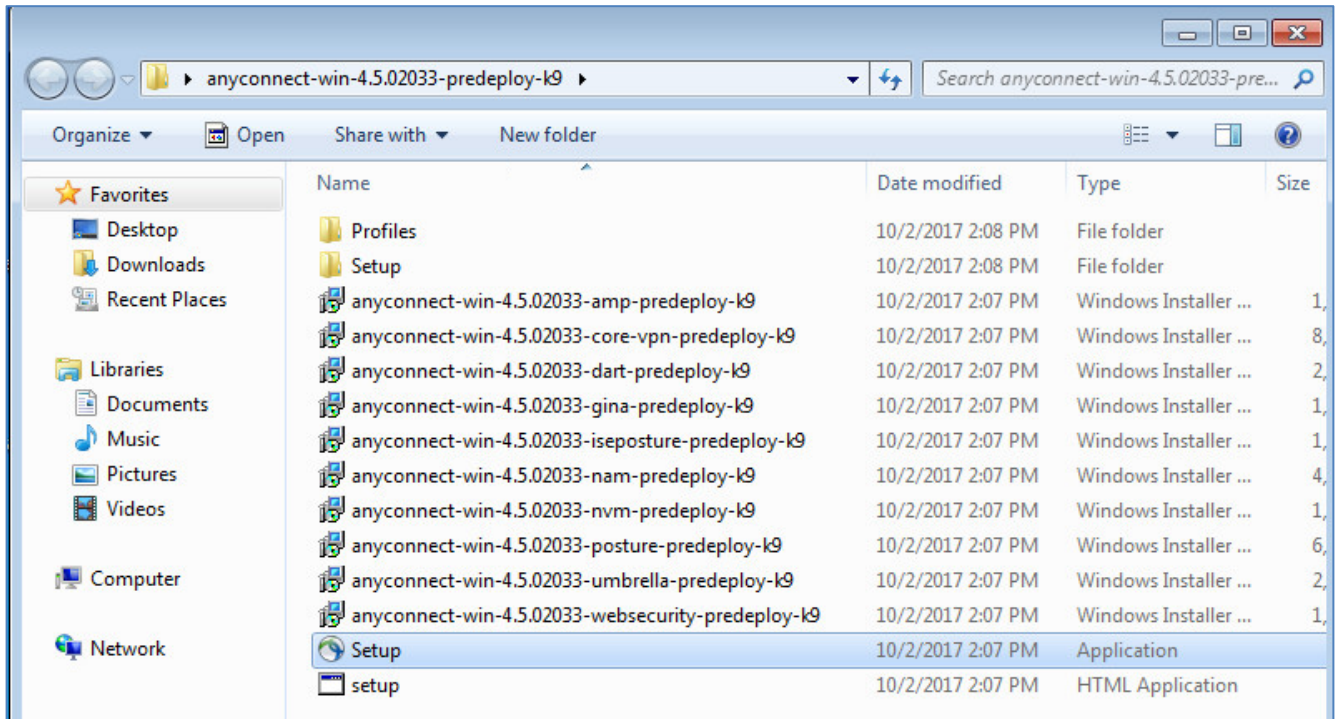
---



# Client Installation

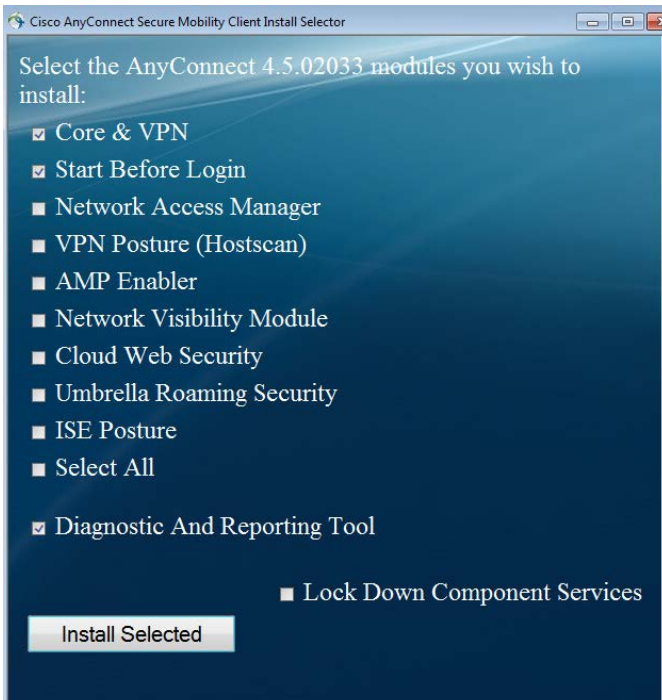
In this example, Cisco AnyConnect - 4.5.02033 predeploy was installed with an MSI installer.

1. Click **Setup**



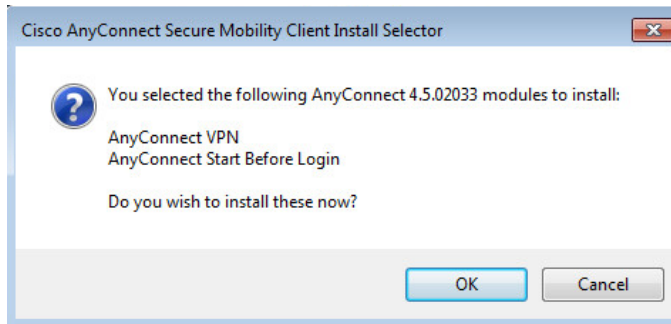
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. In the **Cisco AnyConnect Secure Mobility Client Install Selector**, select **Core & VPN** and **Start Before Login**, and then click **Install Selected**.



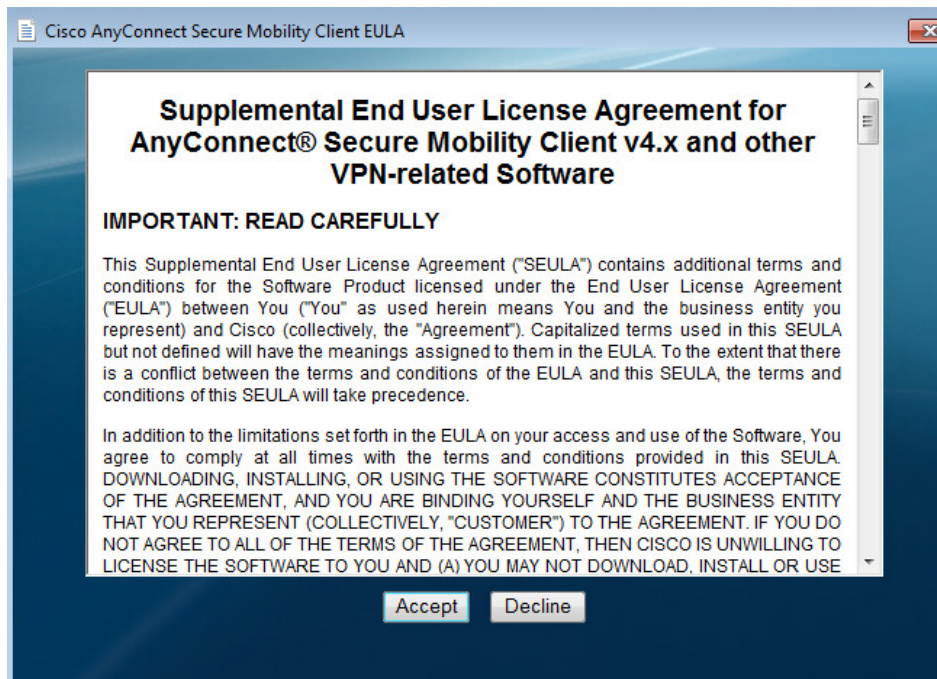
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. Click **Ok**



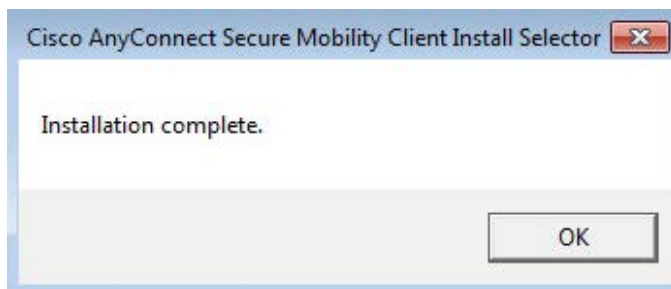
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

4. To accept the End User License Agreement (EULA), click **Accept**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

5. Click **OK** on Installation complete



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

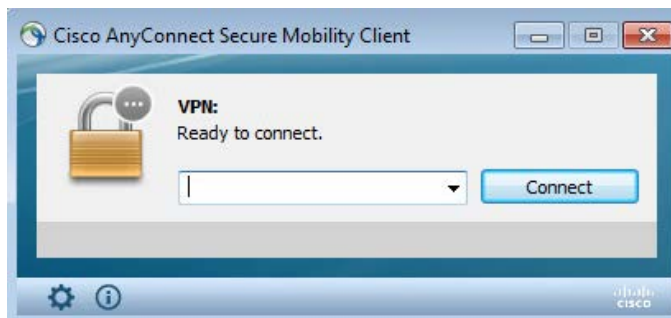
# Running the Solution

## Using the Cisco AnyConnect Secure Mobility Client SSL VPN

The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to the Cisco ASA.

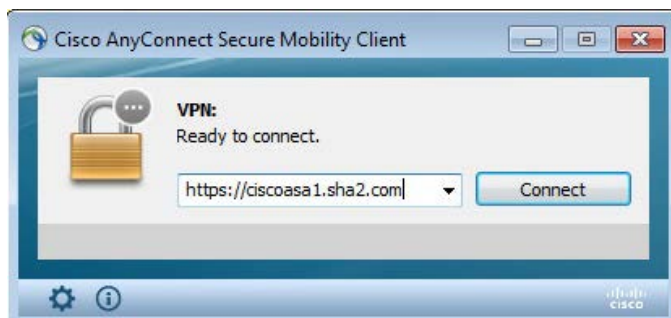
In this example, a connected Token/Smart Card is used with an **Alice** smart card user certificate.

1. Select **Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client**.



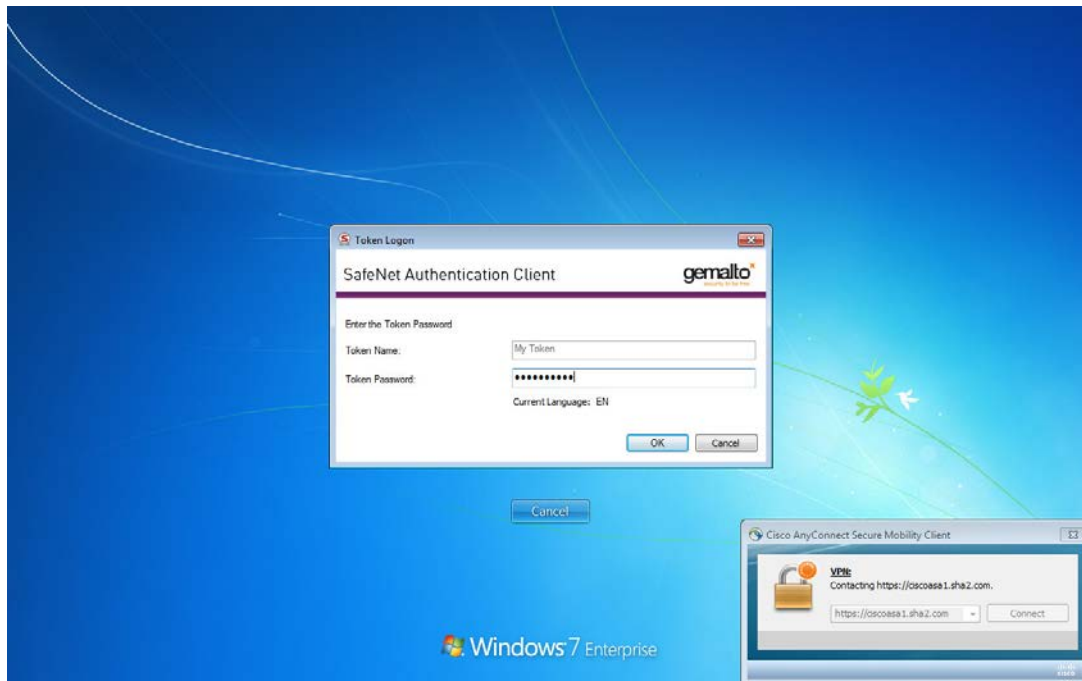
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

2. On the **Cisco AnyConnect Secure Mobility Client** window, in the field, enter the fully qualified domain name or IP address for Cisco ASA, and then click **Connect**.



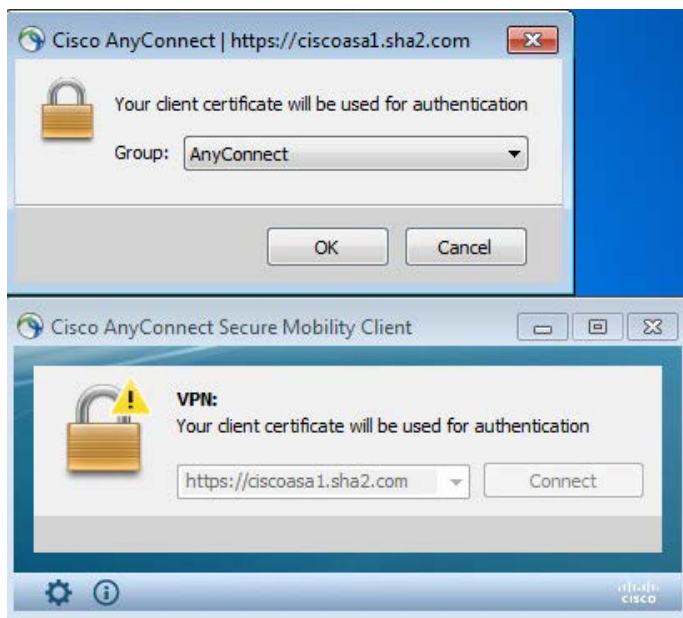
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

3. In SafeNet Authentication Client **Token Logon** window, enter the **Token Name** and **Token Password** and click **OK**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

4. When the message “**Your client certificate will be used for authentication**” appears, Select the appropriate configured group alias (for example, **AnyConnect**) and click **OK**.



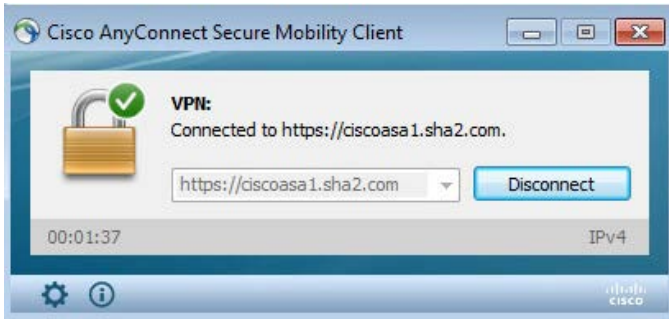
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

The VPN Connection is established.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*





(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Cisco ASA Monitoring VPN connection

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

1. Click the **Monitoring** tab
2. Click **VPN** in the left pane
3. In the center pane, in the **Filter by** field, select the required filter from the drop-down list.

In this example, a Cisco AnyConnect Secure Mobility Client SSL VPN is established

Type	Active	Cumulative	Peak Concurrent	Inactive
AnyConnect Client	1	11	1	0
SSL/TLS/DTLS	1	6	1	0
IKEv2 IPsec	0	5	1	0

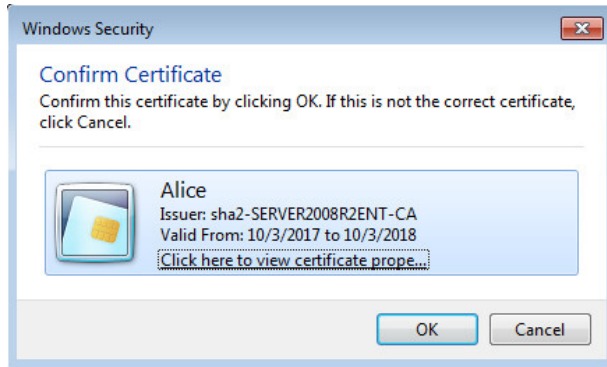
Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Details
alice@sha2.com	GroupPolicySSL	172.19.19.23	AnyConnect-Parent SSL-Tunnel DTLS-	15:17:06 IST Mon ..	155
	AnyConnect	10.0.0.200	AnyConnect-Parent: (1)none SSL-Tu...	0h:01m:45s	229

## Using the Clientless SSL VPN

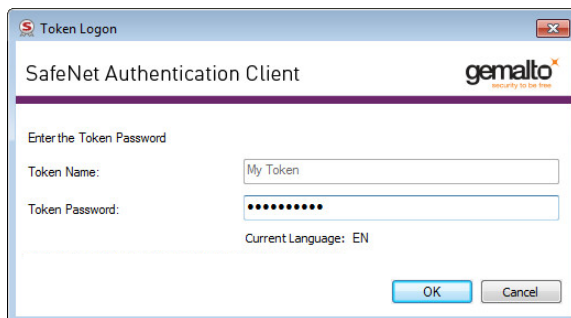
The clientless SSL VPN creates a secure, remote-access VPN tunnel to Cisco ASA using a web browser without requiring a software or hardware client.

In this, example, a connected Token/Smart Card is used with an **Alice** smart card user certificate

1. Open the following URL in a web browser: **https://<Public IP or Address of Cisco ASA>**
2. On the **Confirm Certificate** window, click **OK**.

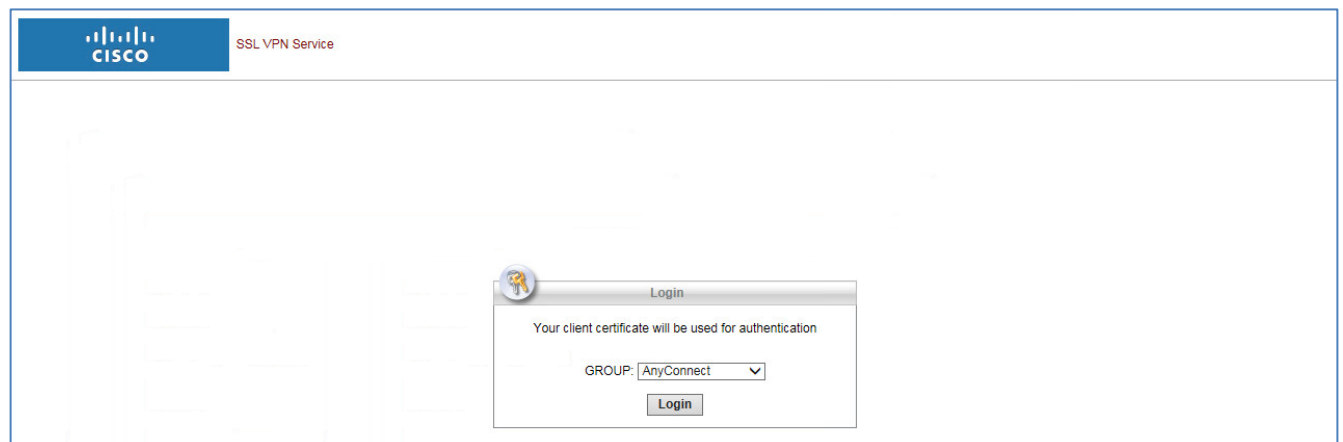


3. In the SAC Token Logon windows enter the **Token Name** and **Token Password** and click **OK**



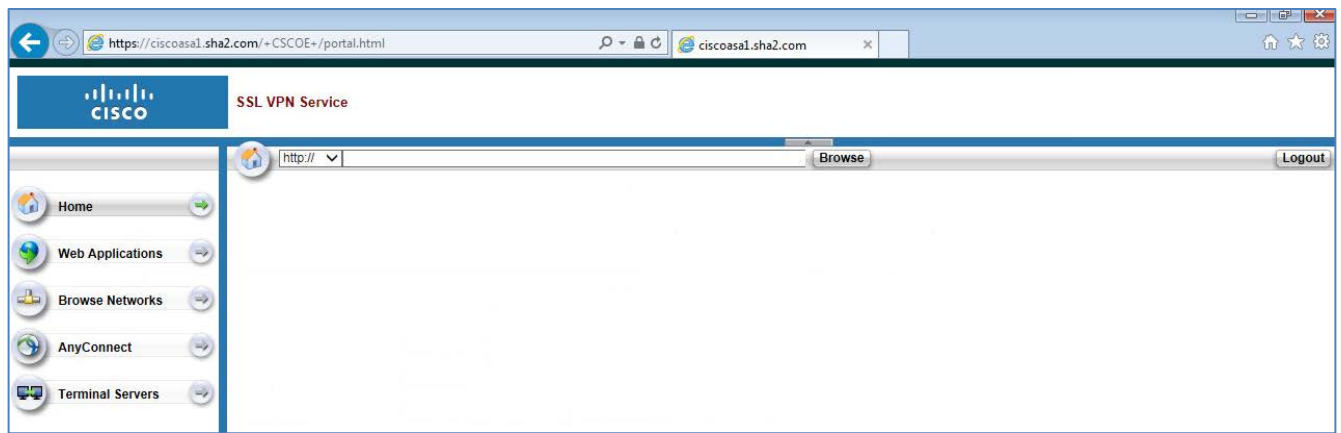
The Login window a message “**Your client certificate will be used for authentication**” opens.

4. Select the appropriate configured group alias (in this Example **AnyConnect**) and click **Login**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

The user is logged in.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Cisco ASA Monitoring VPN connection

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

1. Click **Monitoring** and then, in the left pane, click **VPN**.
2. In the right pane, select the required filter in the **Filter By** field.

In this example Cisco AnyConnect Secure Mobility Clientless SSL VPN is established

Type	Active	Cumulative	Peak Concurrent	Inactive
AnyConnect Client	0	57	1	0
SSL/TLS/DTLS	0	32	1	0
IKEv2 IPsec	0	25	1	0
Clientless VPN	1	12	3	3
Browser	1	12	3	3

Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Details
alice@sha2.com	GroupPolicySSL AnyConnect	10.0.0.200	Clientless Clientless: (1)AES128	11:42:05 IST Tue ... 203 0h:00m:27s 3359	Logout Ping

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

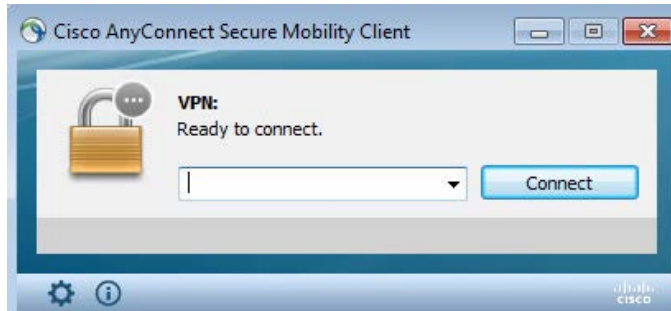


## Using the Cisco AnyConnect Secure Mobility Client - IPsec IKEv2 VPN

**Prerequisites:** See “Any Connect Client Profile”, on page 45.

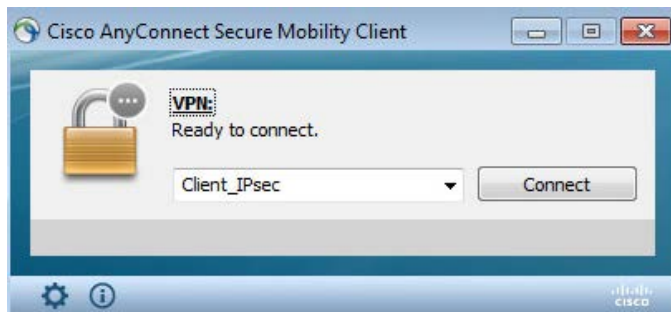
In this example, a connected Token/Smart Card is used with an **Alice** smart card user certificate

1. Click **Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client**.



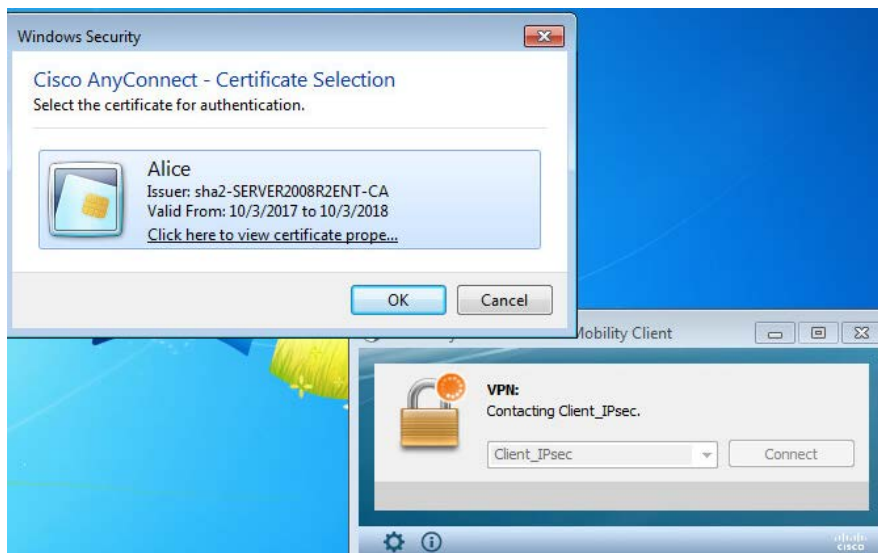
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

2. On the **Cisco AnyConnect Secure Mobility Client** window, select the appropriate display name as configured in “Any Connect Client Profile” on page 45 (in this example **Client\_IPsec**) and then click **Connect**.



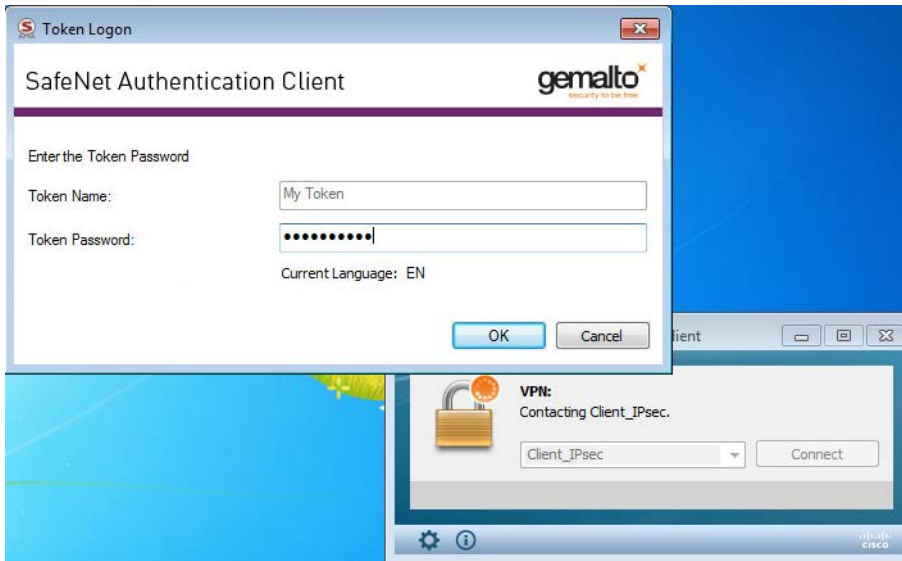
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

3. On the **Cisco AnyConnect - Certificate Selection** window, click **OK**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

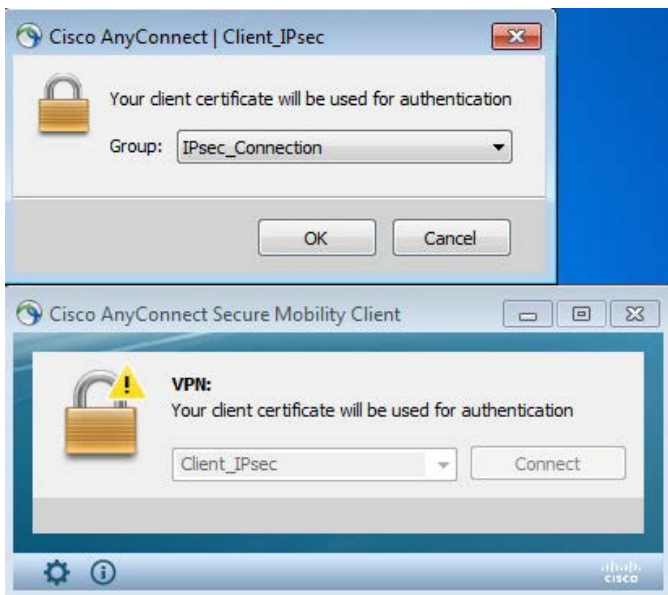
4. In the SAC **Token Logon** window, enter **Token Name** and **Token Password**, and click **OK**



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

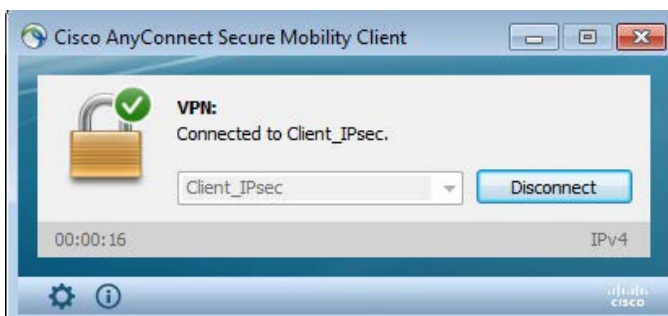
The message “**Your client certificate will be used for authentication**” is displayed.

5. Select the appropriate configured group alias (in this example, **IPsec Connection**) and click **OK**.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

The VPN connection is established.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

## Cisco ASA Monitoring VPN connection

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

1. Select the **Monitoring** tab, and click on **VPN** in the left pane
2. In the right pane, select the required filter in the **Filter By** field.

In this example, Cisco AnyConnect Secure Mobility Client IPsec VPN is established

Type	Active	Cumulative	Peak Concurrent	Inactive
AnyConnect Client	1	55	1	0
SSL/TLS/DTLS	0	31	1	0
IKEv2 IPsec	1	24	1	0
Clientless VPN	0	11	3	0
Browser	0	11	3	0

Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Details
alice@sha2.com	GroupPolicyIPsec AnyConnectIPsec	10.0.0.200 172.19.19.25	IKEv2 IPsecOverNat AnyConnect-Pa... IKEv2: (1)AES256 IPsecOverNat: (1...	11:35:54 IST Tue ... 0h:00m:11s 290	Logout Ping

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Start Before Logon (SBL)

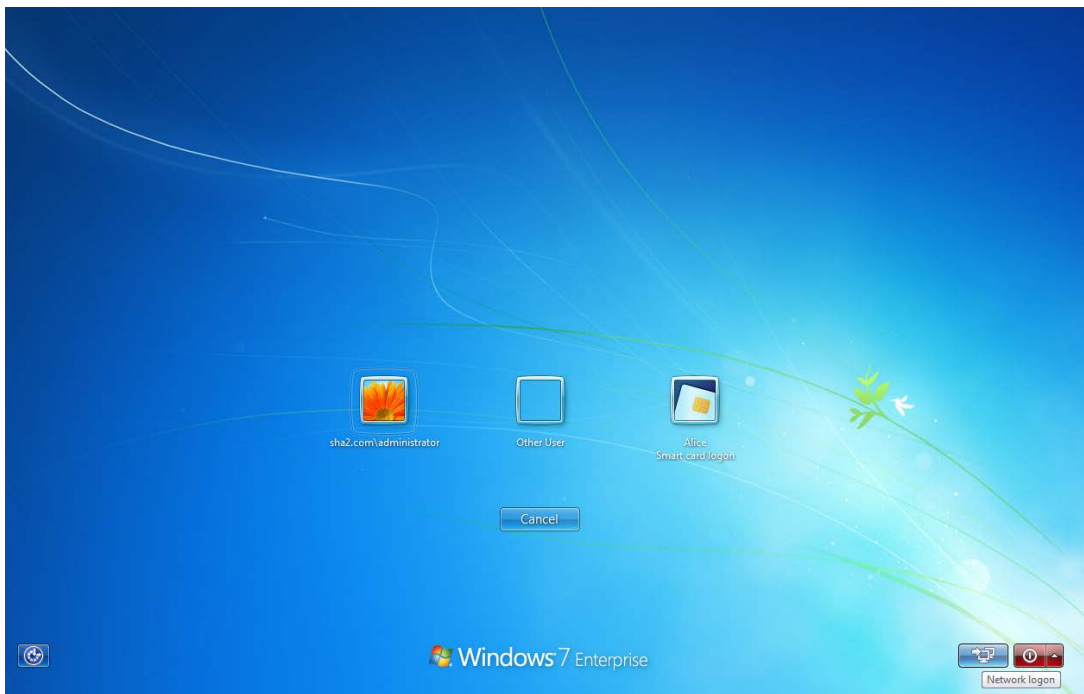
**Start Before Logon** is a feature of the Cisco AnyConnect Client that allows the user to establish a VPN connection before logging onto the computer.

In this example, SSL VPN is demonstrated using a connected Token/Smart Card with the **Alice** smart card user certificate.

1. In User Log on Screen click **Switch User**.

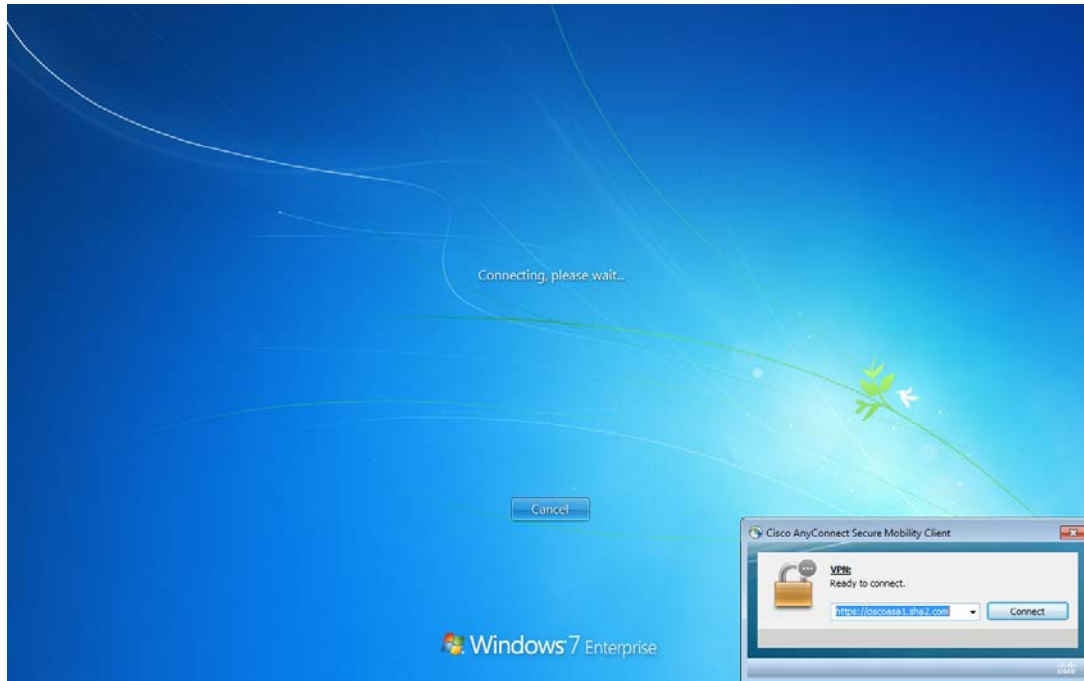


2. Click **Network Logon** button (next to the shut-down button).



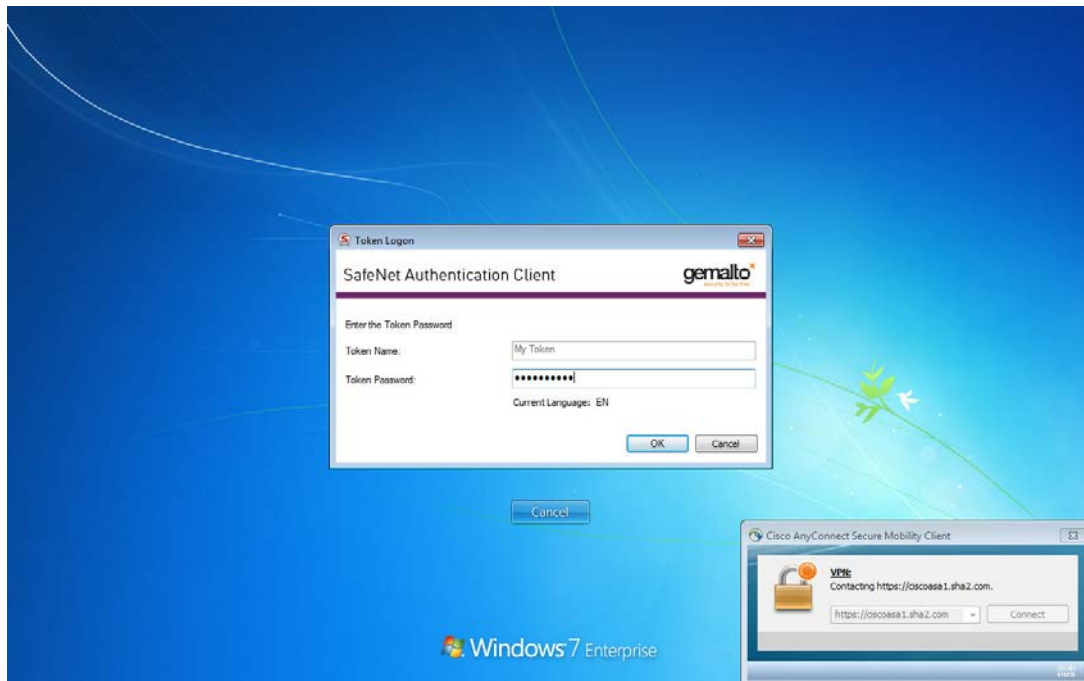
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

3. On the **Cisco AnyConnect Secure Mobility Client** window, enter the fully qualified domain name or IP address for Cisco ASA, then click **Connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. In the SAC **Token Logon** window, enter the **Token Name** and **Token Password** and click **OK**.

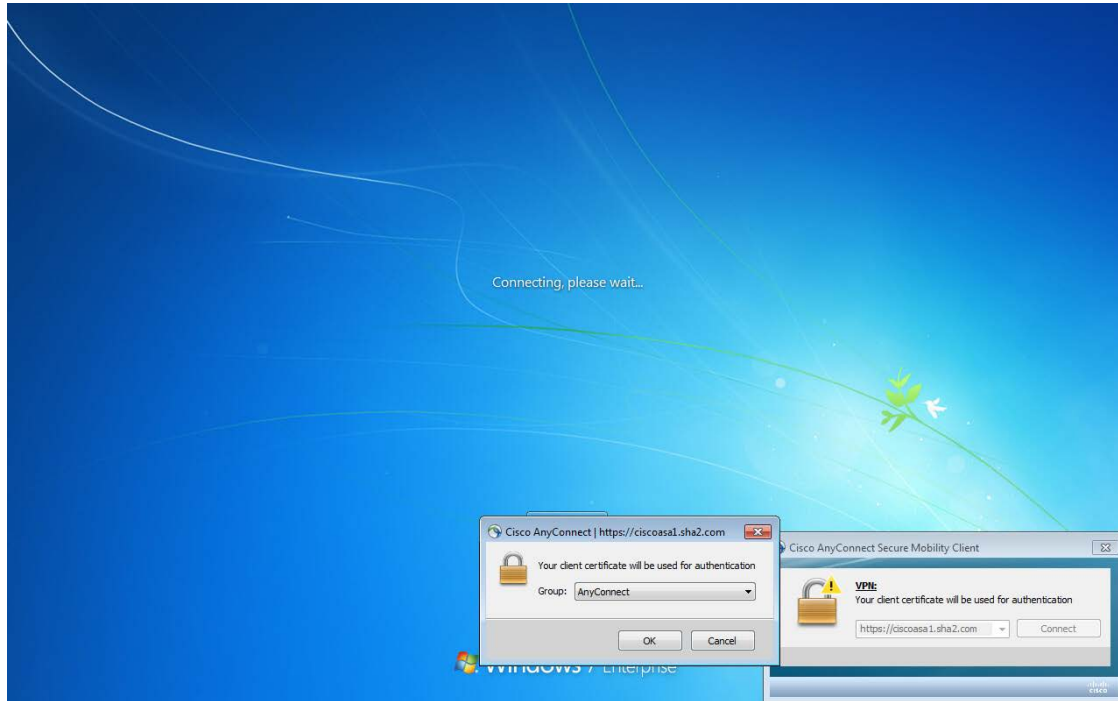


(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The message **“Your client certificate will be used for authentication”** is displayed

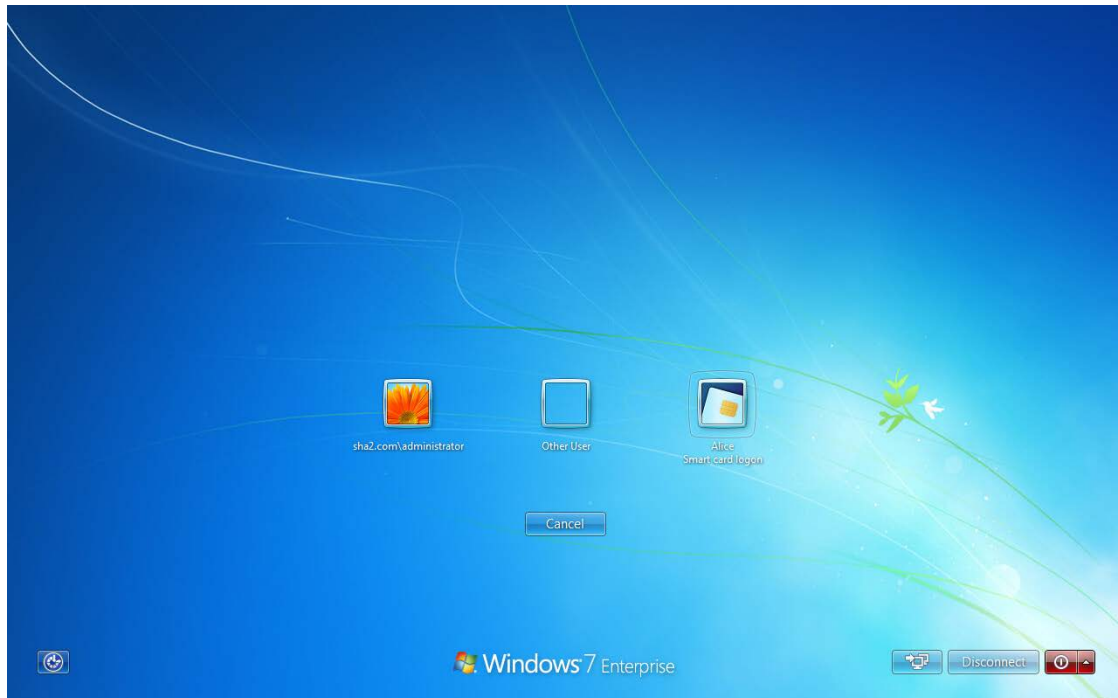


5. Select the appropriate configured group alias (for example, **AnyConnect**) and click **OK**.



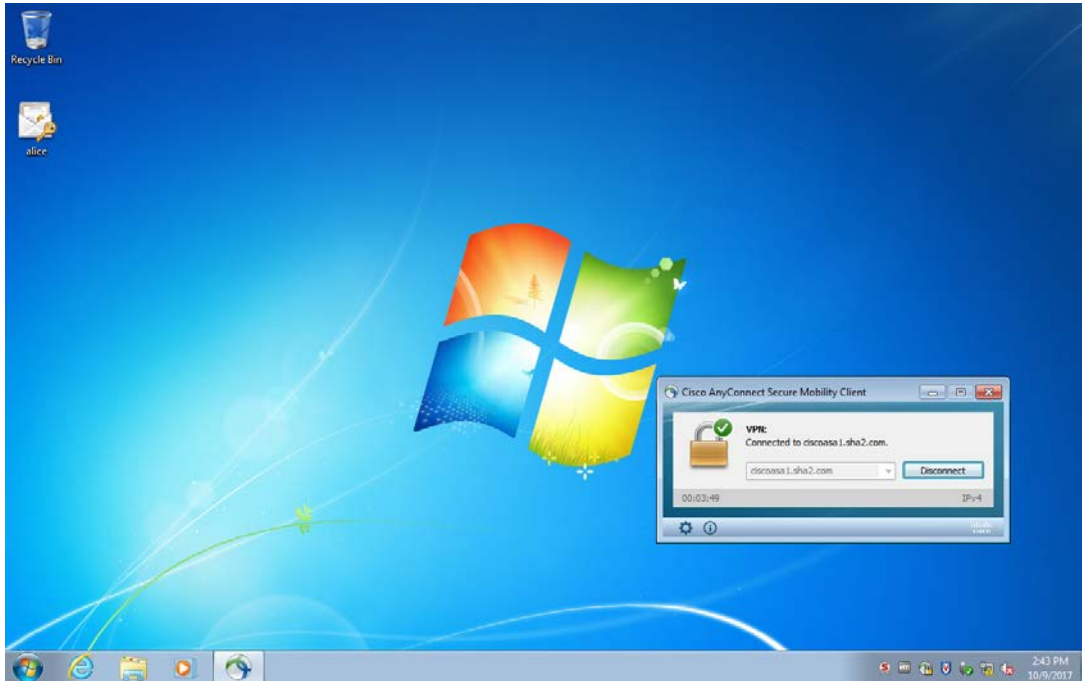
*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

The VPN connection is established successfully before the user is logged in.



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

6. After logging on to windows, the AnyConnect Client is already connected



*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*



## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.



**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

---

### Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421

<b>Region</b>	<b>Telephone number</b> (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608