Symantec™ Managed PKI®

Integration Guide for Cisco® ASA Series Routers

Symantec™ Managed PKI® Integration Guide for Cisco® ASA VPN

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated July 8, 2013

Legal Notice

THE DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Integrating Managed PKI Certificates with Cisco® VPN

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile device they use, no matter if you have provided their devices or if they are using their own mobile devices.

Symantec Managed PKI's digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from a few to thousands of devices, and its in-the-cloud solution provides quick deployment and easy management while also offering Symantec's industry leading security that is unmatched by in-house PKI solutions.

Symantec's Managed PKI issues certificates that can be used to authenticate users for secure communications with company resources, such as VPNs and web sites.

This document describes how to integrate Managed PKI 8.7 or higher certificates with the Cisco® Adaptive Security Appliance (ASA) VPN to authenticate users to protected resources, and to secure communications between them.

Partner Information

These procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Cisco®
Product Name	Cisco® Adaptive Security Appliance (ASA) VPN
Version and Platform	Cisco® ASA 9.1

How the Cisco ASA VPN Works

The following diagram describes how the Managed PKI certificates integrate with Cisco ASA VPN to provide secure authentication.

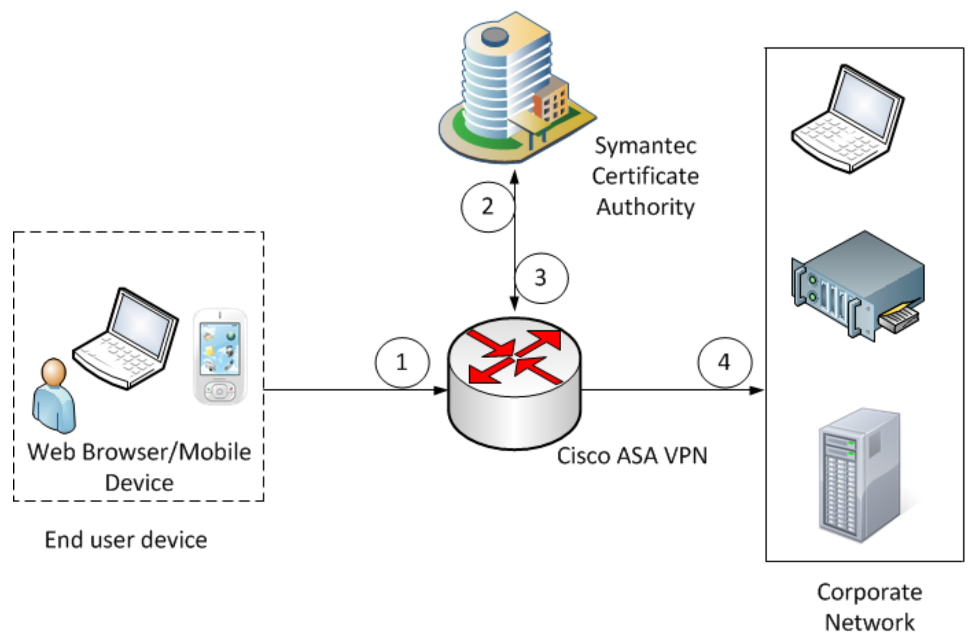


Figure 1-1 Authenticating Cisco VPN with a Managed PKI certificate

1 The end-user device accesses the corporate network through the Cisco VPN.

2 Depending upon how the VPN is configured, it attempts to obtain the status of the certificate:

- If Online Certificate Status Protocol (OCSP) is configured, the VPN communicates to the Symantec CA to obtain the real-time status of the certificate.
- If Certificate Revocation List (CRL) is configured, the VPN communicates to the Symantec CA to obtain the status of the certificate based on the most recent certificate revocation list. CRLs are updated on a regular basis.

3 When the Cisco VPN receives the certificate status, it authenticates the end-user's certificate based on the CAs it has been configured to trust.

4 Based on this authentication, the end user device is allowed access to the corporate network, and the Cisco VPN secures communication with the corporate network.

Integration Workflow

The following diagram describes the general steps required to set up the Symantec Managed PKI account and integrate Managed PKI certificates with Cisco VPN.

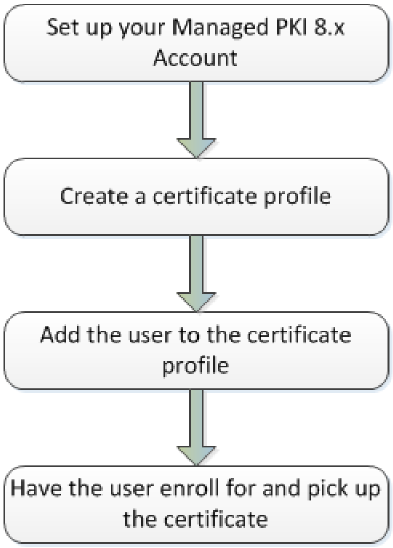

Set up your Managed PKI 8.x Account
Create a certificate profile
Add the user to the certificate profile
Have the user enroll for and pick up the certificate

Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.x account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.

- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

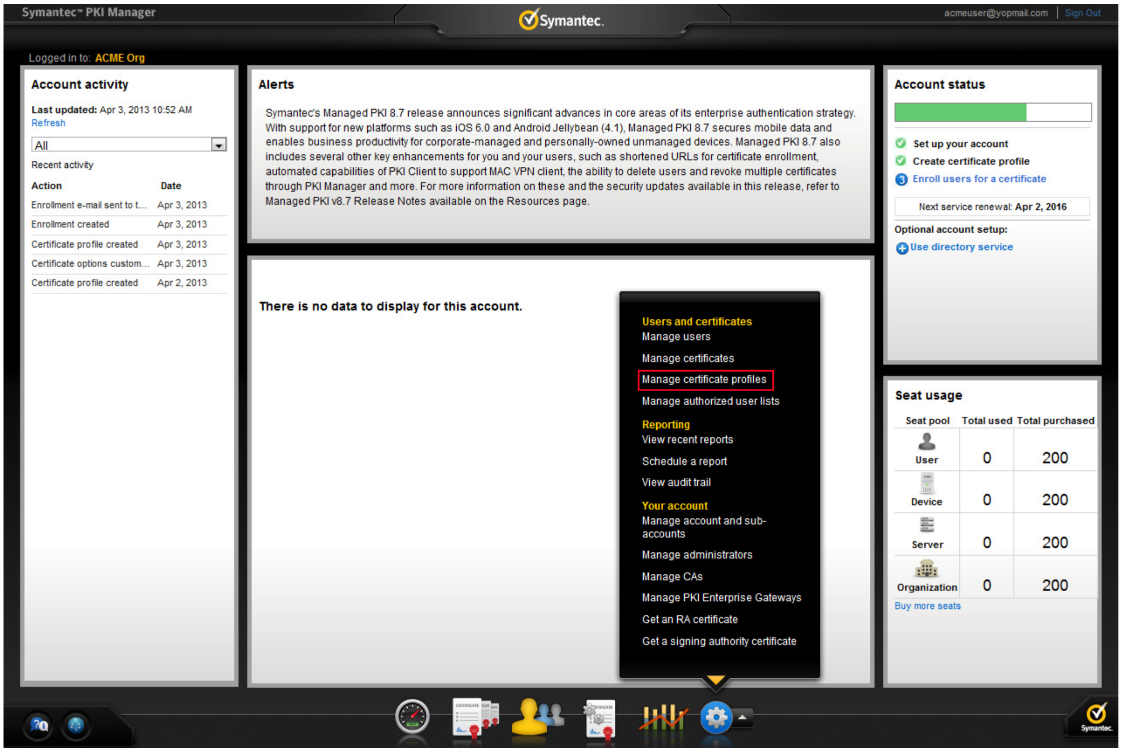
You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create a certificate profile

To obtain a certificate for the router, you first create the certificate profile that will define the certificates you will issue to your end users. Complete the following steps to create your Managed PKI Client Authentication certificate profile:

1 Log into Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.



Account activity

Last updated: Apr 3, 2013 10:52 AM
Refresh

All

Recent activity

Action	Date
Enrollment e-mail sent to t...	Apr 3, 2013
Enrollment created	Apr 3, 2013
Certificate profile created	Apr 3, 2013
Certificate options custom...	Apr 3, 2013
Certificate profile created	Apr 2, 2013

Alerts

Symantec's Managed PKI 8.7 release announces significant advances in core areas of its enterprise authentication strategy. With support for new platforms such as iOS 6.0 and Android Jellybean (4.1), Managed PKI 8.7 secures mobile data and enables business productivity for corporate-managed and personally-owned unmanaged devices. Managed PKI 8.7 also includes several other key enhancements for you and your users, such as shortened URLs for certificate enrollment, automated capabilities of PKI Client to support MAC VPN client, the ability to delete users and revoke multiple certificates through PKI Manager and more. For more information on these and the security updates available in this release, refer to Managed PKI v8.7 Release Notes available on the Resources page.

There is no data to display for this account.

Account status

✓ Set up your account
✓ Create certificate profile
3 Enroll users for a certificate

Next service renewal: Apr 2, 2016

Optional account setup:
Use directory service

Seat usage

Seat pool	Total used	Total purchased
User	0	200
Device	0	200
Server	0	200
Organization	0	200

Buy more seats

Figure 1-3 Manage Certificate Profile

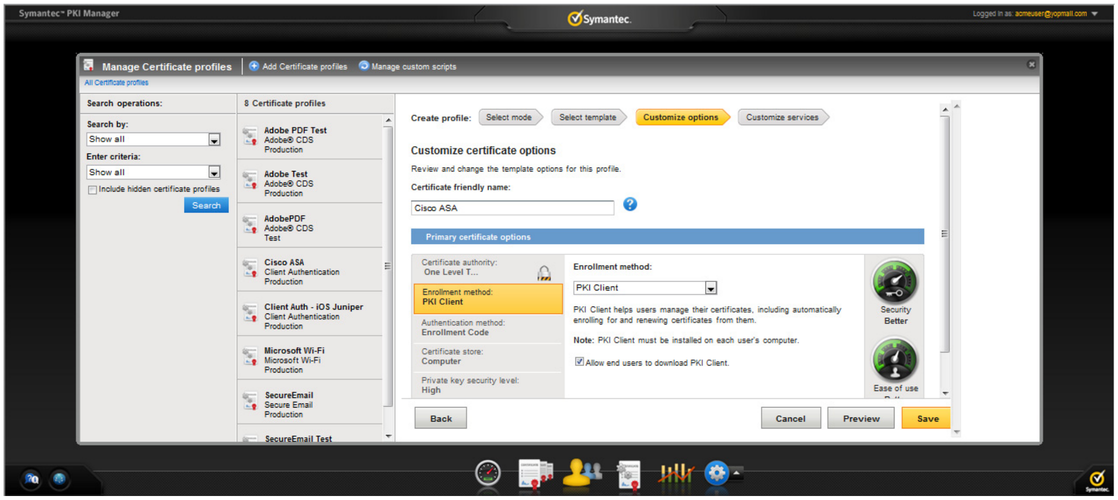
3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.

4 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.

5 Select **Client Authentication** as the certificate template and click **Continue**. The Customize certificate options page appears.

6 Set the certificate options that suits your needs, but the following configurations are required:

- Enter a profile name.



Search operations:

Search by: Show all

Enter criteria: Show all

□ Include hidden certificate profiles

8 Certificate profiles

- Adobe PDF Test
Adobe® CDS
Production
- Adobe Test
Adobe® CDS
Production
- AdobePDF
Adobe® CDS
Test
- Cisco ASA
Client Authentication
Production
- Client Auth - iOS Juniper
Client Authentication
Production
- Microsoft Wi-Fi
Microsoft Wi-Fi
Production
- SecureEmail
Secure Email
Production
- SecureEmail Test

Create profile: Select mode > Select template > Customize options > Customize services

Customize certificate options

Review and change the template options for this profile.

Certificate friendly name: Cisco ASA

Primary certificate options

Certificate authority: One Level T...

Enrollment method: PKI Client

Authentication method: Enrollment Code

Certificate store: Computer

Private key security level: High

Enrollment method: PKI Client

PKI Client helps users manage their certificates, including automatically enrolling for and renewing certificates from them.

Note: PKI Client must be installed on each user's computer.

☑ Allow end users to download PKI Client.

Figure 1-4 Client Authentication Certificate options

- Select the appropriate Enrollment method from the following:
  - Select **iOS** if your user will enroll for certificates using iOS devices.
  - Select **Android** if your user will enroll for certificates using Android devices
  - Select **OS/browser** if your user will enroll for certificates using desktop or laptop.
  - Select **PKI Client** if your user will enroll for certificates using PKI Client.

Click **Advanced options** to view certificate options and define any additional attributes you may need.

7 Click **Save**.

On the confirmation page, you can view the attribute used for the seat ID, a mandatory attribute that authenticates the user for third party configurations or during the enrollment process. This is typically the user's email address.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

8 For certificate profiles using the Android or iOS Enrollment methods only, click **Edit** from **Provide certificate instructions** under Manage this profile. Table 1-2 describes the values that you can enter to configure VPN settings for these profiles:

Table 1-2 VPN Settings for Android/iOS Enrollment Method

Field Name	Value
Connection name	Enter a connection name.
Server Host/IP	The Fully Qualified Domain Name of the VPN. For example, https://vpn.<company>.com

Task 3. Add the user to the certificate profile

You must add the user to the certificate profile in PKI Manager before the user can enroll for and pick up a certificate.

1 In PKI Manager, click **Manage users**, or select **Manage users** from the Tasks menu on the bottom navigation bar.

2 Click **Add Users** from the top of the resulting Manage users page.

3 Enter the seat ID (typically the end user's email address) and click **Continue**.

- Enroll for a single user by entering end user's email address.
- Enroll for multiple users at one time by uploading a comma-separated value (csv) file with your user data. You can skip step 4 if you are enrolling multiple users using a .csv file.

4 Enter the First Name, Last Name, and select the **I want to enroll this user for a certificate** check box and click **Continue**.

5 Select the certificate profile you created in Task 2, "Create a certificate profile" on page 3 and click **Continue**.

6 Enter the **Other Name (UPN)**, **Email**, and select the **Have the system send the enrollment email to the user** check box (optional) and click **Continue**.

The enrollment link is displayed to the administrator along with the enrollment code required for authentication. Symantec recommends that you send the enrollment code separately from the enrollment link, and that you do not send the enrollment code by email.

Note: The enrollment link will not be displayed if you have selected **Have the system send the enrollment email to the user** in step 6.

Task 4. Have the user enroll for and pick up the certificate

Once added to the certificate profile, the user must enroll for and pick up the certificate. The following are the steps for picking up certificates for different enrollment methods.

Table 1-3 Steps for picking up certificates

Enrollment Method	How Certificates are Picked Up
iOS	1 Download the **Cisco AnyConnect VPN** application from the App Store^{SM}. 2 Open a browser on the iOS device. 3 Paste the enrollment link from the enrollment email into the browser. 4 Enter the User Id and enrollment code (provided by the administrator) and tap **Continue**. The Identity Confirmed page appears. 5 Tap **Continue**. The Install Profile page appears. 6 Tap **Install**, then tap **Install Now** from the pop-up window.
Android	**Note: If PKI Client is not already installed on the android device, the user will be prompted to install it during enrollment** 1 Download the **Cisco AnyConnect VPN** application from the Google Play^{TM}. 2 In the Android device, tap **Settings** to clear the **Block Untrusted Servers** check box option, if selected. 3 Paste the enrollment link from the enrollment email into the browser. 4 Enter the enrollment code provided by the administrator or received in an email and click **Continue**. This step authenticates the end user to ensure the correct user is picking the certificate. 5 Enter the password to import the certificate and tap **OK**. The password is displayed during certificate installation. This step is the second level of authentication to ensure the correct user is picking the certificate. 6 Tap **Install Certificate**. 7 The certificate will be automatically associated with AnyConnect. Tap **Yes** if AnyConnect prompts for certificate installation.

Table 1-3 Steps for picking up certificates

Enrollment Method	How Certificates are Picked Up
OS/browser	**Supported Browsers:** ■ For Windows XP or Windows 7 - Internet Explorer or Firefox ■ For Apple OS X - Safari or Firefox Refer the Managed PKI documentation for the exact version numbers. 1 Click the enrollment link in the email or paste it into your browser. 2 Enter the email address used for enrollment and click **Continue**. 3 Enter the enrollment code provided by the administrator or received in an email and click **Continue**. This step authenticates the end user to ensure the correct user is picking the certificate. 4 Click **Continue**. 5 Click **Install certificate** to install the certificate.
PKI Client	**If PKI Client is not already installed on the user's machine, the user will be prompted to install it during enrollment.** 1 Click the enrollment link in the email or paste it into your browser. 2 Enter the email address used for enrollment and click **Continue**. 3 Enter the enrollment code provided by the administrator or received in an email and click **Continue**. This step authenticates the end user to ensure the correct user is picking the certificate. 4 Click **Continue**. 5 Click **Install Certificate**. 6 Enter the PIN for the certificate store (PKI Client) when prompted and click **OK**.

Renewing Certificates

You must renew the certificate before it expires (typically a year after initially enrolling for it). The following are the steps for renewing certificates for different enrollment methods.

Table 1-4 Steps for renewing certificates

Enrollment Method	How Certificates are Renewed
iOS	If renewal notifications are enabled, the user receives an email containing a renewal link at some period before the certificate expires. Clicking the link prompts the user to select a credential to authenticate the renewal. The user is then taken to the PKI Certificate Services page and the renewed certificate is installed.
Android	If renewal notifications are enabled, the user receives an email containing a renewal link at some period before the certificate expires. Clicking the link prompts the user to select a credential to authenticate the renewal. The user is then taken to the PKI Certificate Services page and the renewed certificate is installed.
OS/browser	If renewal notifications are enabled, the user receives an email containing a renewal link at some period before the certificate expires. Clicking the link takes the user to the PKI Certificate Services page for a new certificate, where the user follows a renewal process similar to the enrollment process.
PKI Client	PKI Client prompts the user to renew for certificates that are PIN-protected. For certificates that are not PIN-protected, PKI Client performs the renewal and installs the new certificate transparently.

Chapter 2

Configuring Cisco ASA VPN

This chapter discusses how to configure the Cisco ASA VPN to use Managed PKI certificates for authentication. For more information, refer to the Cisco ASDM documentation for details.

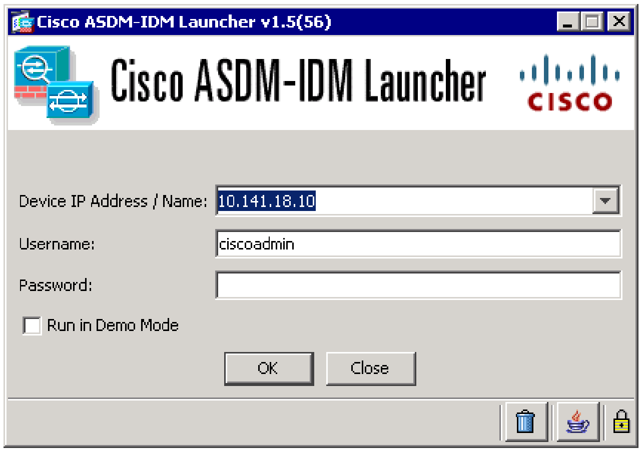
You must complete the following procedures to complete the configuration of the Cisco ASA VPN:

- "Accessing Cisco ASA VPN" on page 9
- "Setup Tunnel and Group Policies" on page 10
- "Configure CA Certificate" on page 11
- "Configure Clientless SSL VPN Access" on page 12

Accessing Cisco ASA VPN

1 Access the Cisco VPN Administrator URL.

2 Install and launch the **Cisco ASDM-IDM Launcher**. The VPN device IP address is auto-populated.



Cisco ASDM-IDM Launcher v1.5(56)

Cisco ASDM-IDM Launcher

Device IP Address / Name: 10.141.18.10

Username: ciscoadmin

Password:

□ Run in Demo Mode

Figure 2-1 Cisco ASDM-IDM Launcher

3 Verify the Device IP Address.

4 Enter the username and password.

5 Click **OK**. The Cisco ASDM window appears.

Setup Tunnel and Group Policies

This section describes how to configure a group policy and VPN tunnel group.

Group Policy

The group policies let you manage the VPN group policies.

1 Click **Configuration** → **Remote Access VPN** → **Network (Client) Access** → **Group Policies** → **Add**.

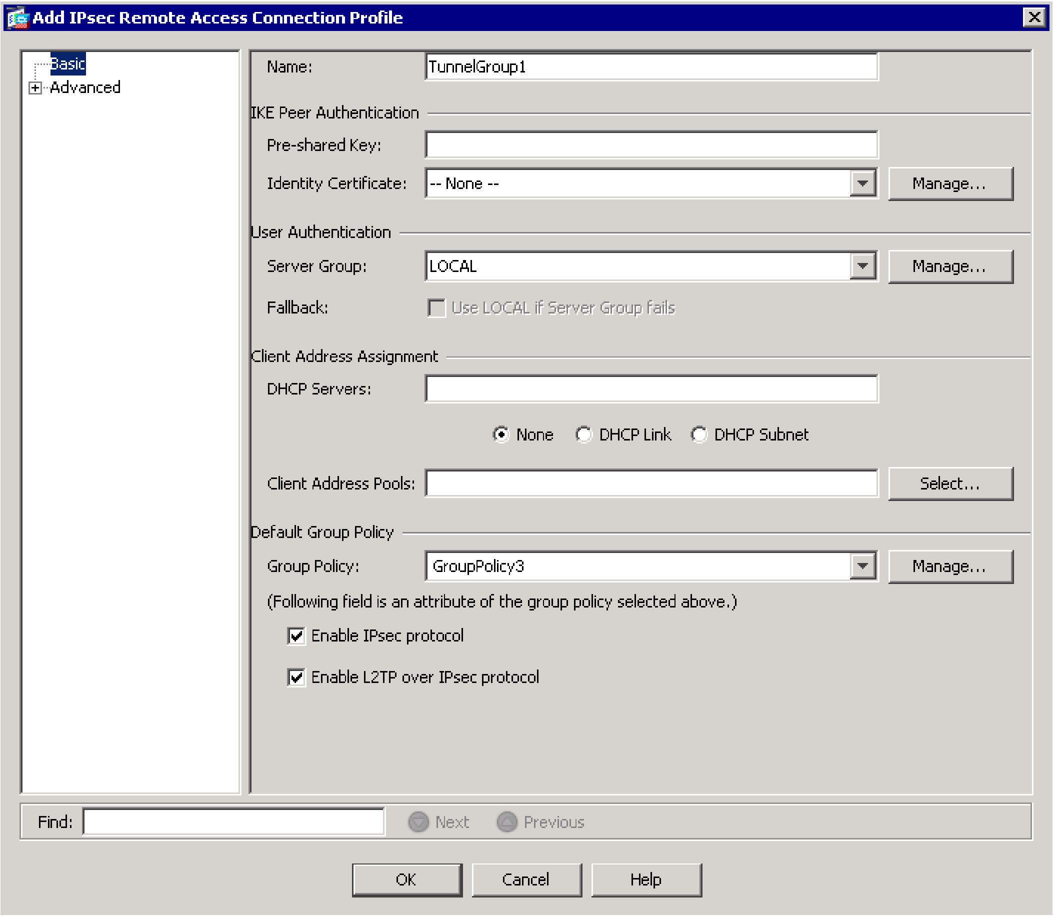
2 On the New Group Policy page, under **More** → **Tunelling Protocols**, enable IPSec, Clientless SSL VPN, and SSL VPN Client. You can use the default configuration settings from the Default Group policy for other fields.

3 Assign a name to the policy and click **Save**.

Tunnel Group

The tunnel group lets you manage the mode of access (Client Authentication or Username/password) to connect to the VPN:

1 Click **Configuration** → **Remote Access VPN** → **Network (Client) Access** → **Group Policies** → **Add**. The Add IPsec Remote Access Connection Profile dialog box is displayed.



Add IPsec Remote Access Connection Profile

Name: TunnelGroup1

IKE Peer Authentication

Pre-shared Key:

Identity Certificate: -- None --

User Authentication

Server Group: LOCAL

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools:

Default Group Policy

Group Policy: GroupPolicy3

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

☑ Enable IPsec protocol

☑ Enable L2TP over IPsec protocol

Find:

Figure 2-2 IPsec Remote Access Connection Profile

2 Under IKE Peer Authentication, select the VPN device identity certificate which was installed during device configuration.

3 Select the Server Group for user authentication.

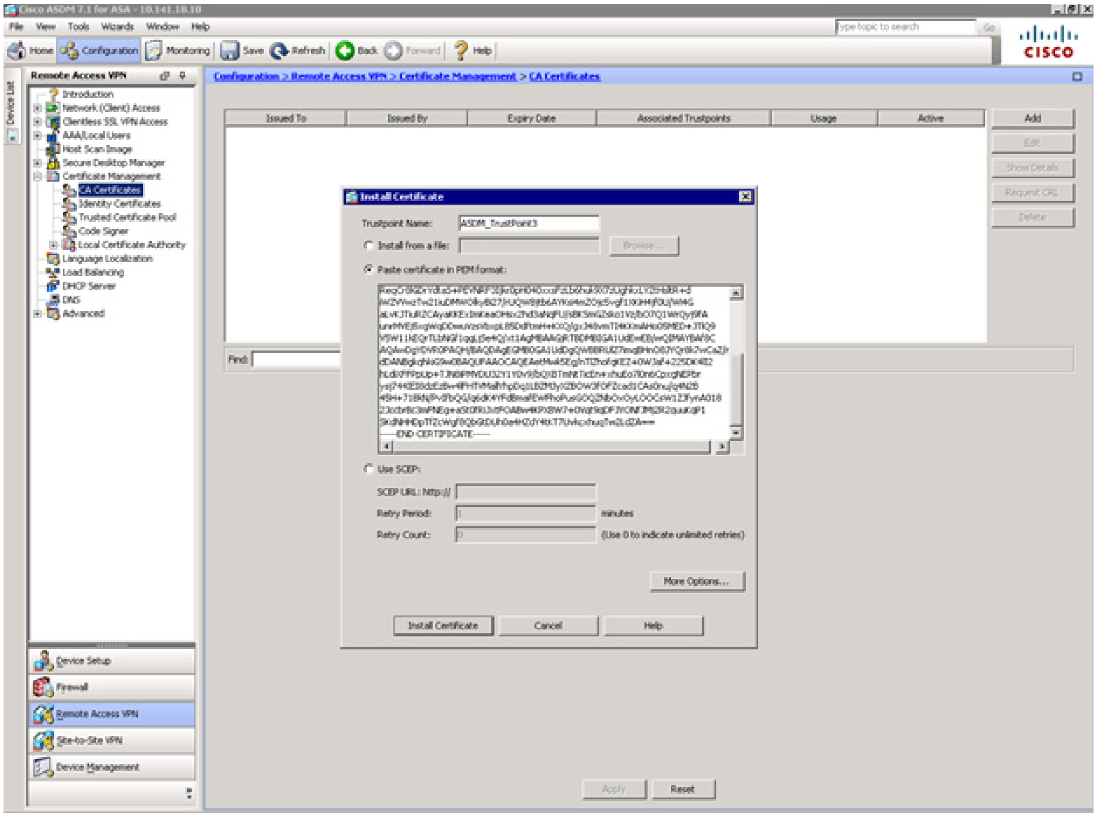
4 Under Default Group Policy, select the Group Policy created in "Group Policy" on page 10, and then select Enable IPsec Protocol.

5 Click **OK**.

6 Click **Apply**.

Configure CA Certificate

1 Click **Configuration** → **Remote Access VPN** → **Certificate Management** → **CA Certificates** → **Add**.



Trustpoint Name: ASDM_TrustPoint3

○ Install from a file:

● Paste certificate in PEM format:

```
[illegible]
-----END CERTIFICATE-----
```

○ Use SCEP:

SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

Figure 2-3 Install CA Certificate

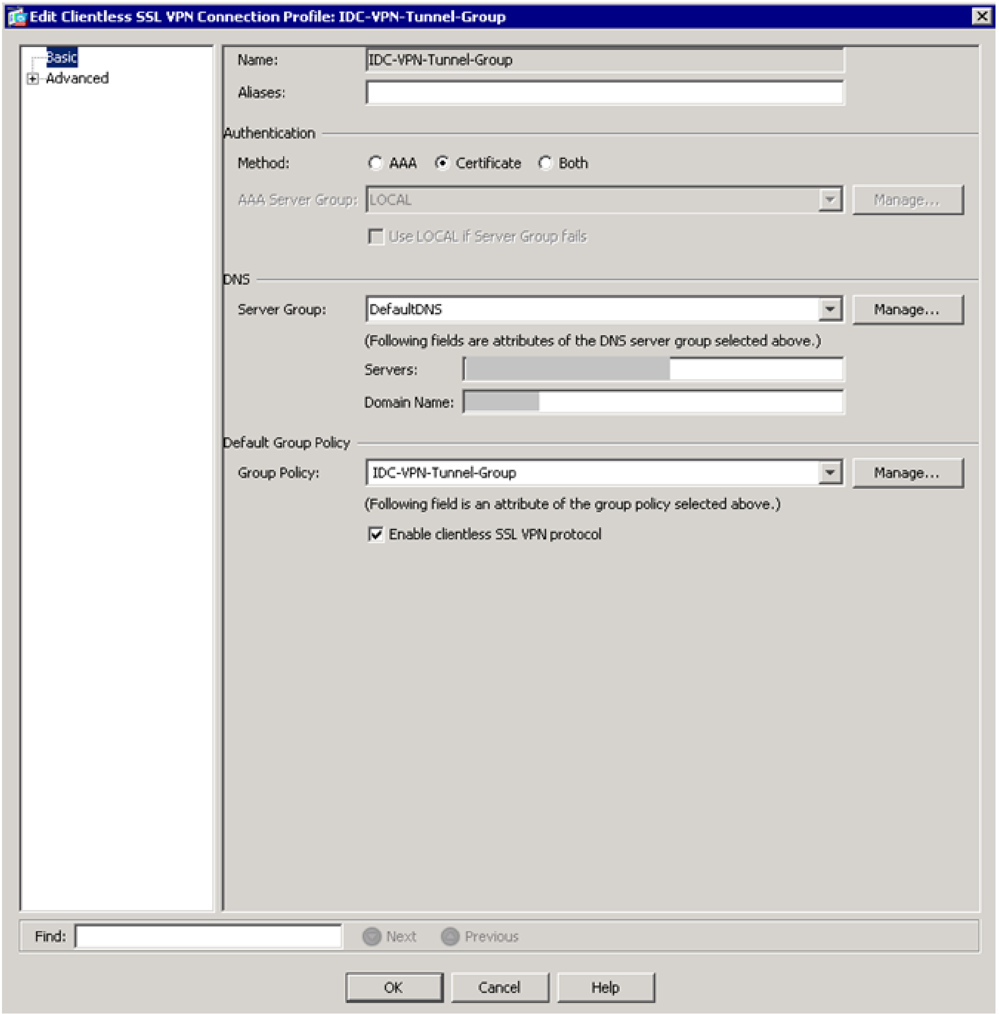
2 Install the CA certificate received from PKI Manager using one of the following options:

- **Install from a file** - Click **Browse** to locate your CA certificate on your local machine
- **Paste certificate in PEM format** - Open the certificate in a text editor and save the file as a `.pem` format. After saving the certificate as a .pem format file, copy the contents and paste it in the **Paste certificate in PEM format** text box.
- **Use SCEP** - Enter the SCEP URL received from Symantec.

3 Click **Install Certificate**.

Configure Clientless SSL VPN Access

1 Click **Configuration** → **Remote Access VPN** → **Network (Client) Access** → **Group Policies** → **Add**.



Edit Clientless SSL VPN Connection Profile: IDC-VPN-Tunnel-Group

Name: IDC-VPN-Tunnel-Group

Aliases:

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers:

Domain Name:

Default Group Policy

Group Policy: IDC-VPN-Tunnel-Group

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

☑ Enable clientless SSL VPN protocol

Figure 2-4 Edit Clientless SSL VPN Connection

2 Enter an alias for the profile.

3 Select **Certificate** as the authentication method.

4 For the server group under DNS, enter a DNS name.

5 Under Default Group Policy, select the group policy that was configured in “Group Policy” on page 10.

6 Click **OK**.

Connecting to VPN

The following are various scenarios through which an end user can connect their devices to the Cisco ASA VPN to securely access company resources.

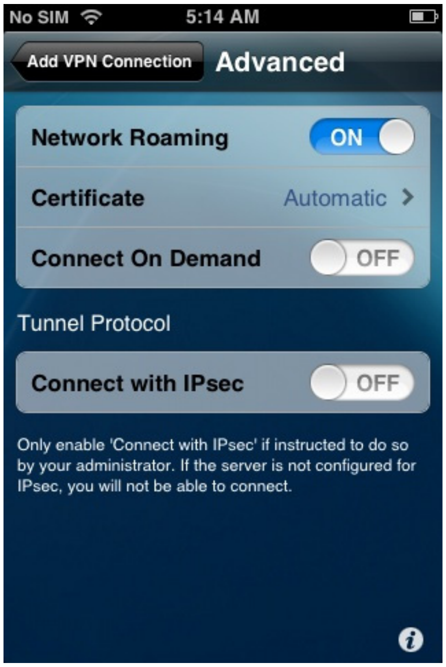
Connecting an iOS device to VPN

1 Open the **Cisco AnyConnect Application** on the iOS device.

2 Click **Add VPN Connection**.

3 Choose a connection.

4 Set Connect with IPsec to **ON** to connect to the VPN.



Network Roaming ON

Certificate Automatic

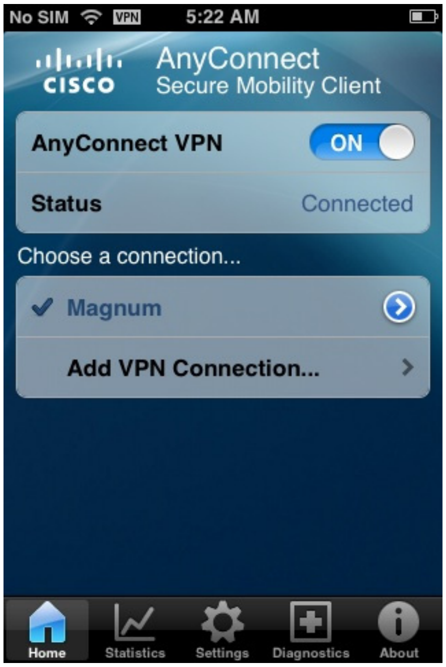
Connect On Demand OFF

Connect with IPsec OFF

Only enable 'Connect with IPsec' if instructed to do so by your administrator. If the server is not configured for IPsec, you will not be able to connect.

Figure 2-5 Cisco AnyConnect Application - Connect with IPsec

5 Select a connection. The VPN connection is established.



No SIM VPN 5:22 AM

AnyConnect
Secure Mobility Client

AnyConnect VPN: ON

Status: Connected

Choose a connection...

✓ Magnum

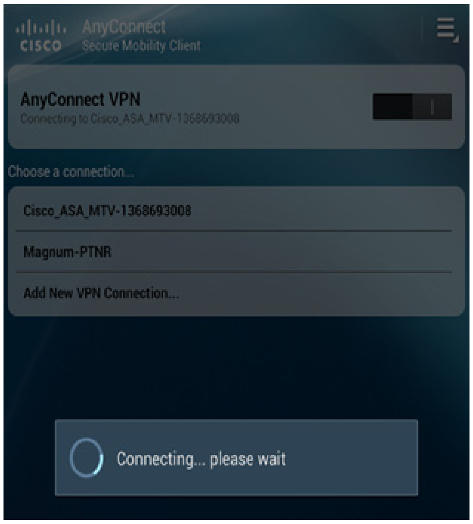
Add VPN Connection...

Figure 2-6 Cisco AnyConnect Application for iOS

Connecting an Android device to VPN

1 Open the **Cisco AnyConnect Application** on the Android device.

2 Select a connection.



AnyConnect
Secure Mobility Client

AnyConnect VPN
Connecting to Cisco_ASA_MTV-1368693008

Choose a connection...

Cisco_ASA_MTV-1368693008

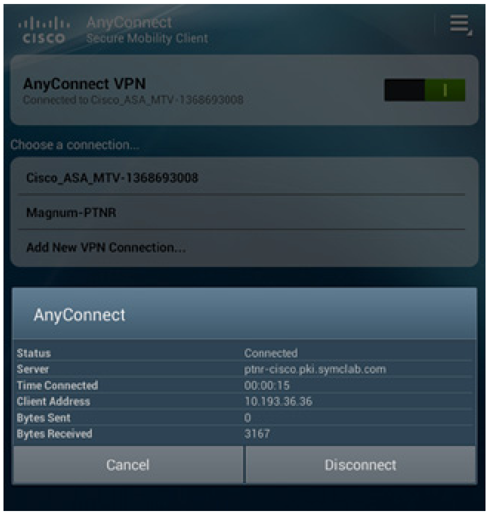
Magnum-PTNR

Add New VPN Connection...

Connecting... please wait

Figure 2-7 Cisco AnyConnect Application - select connection

3 Click **Accept**. The status is displayed as connected.



AnyConnect
Secure Mobility Client

AnyConnect VPN
Connected to Cisco_ASA_MTV-1368693008

Choose a connection...

Cisco_ASA_MTV-1368693008

Magnum-PTNR

Add New VPN Connection...

AnyConnect

Status	Connected
Server	ptnr-cisco.pki.symclab.com
Time Connected	00:00:15
Client Address	10.193.36.36
Bytes Sent	0
Bytes Received	3167

Figure 2-8 Cisco AnyConnect Application for Android

Connecting Desktop/Laptop to VPN

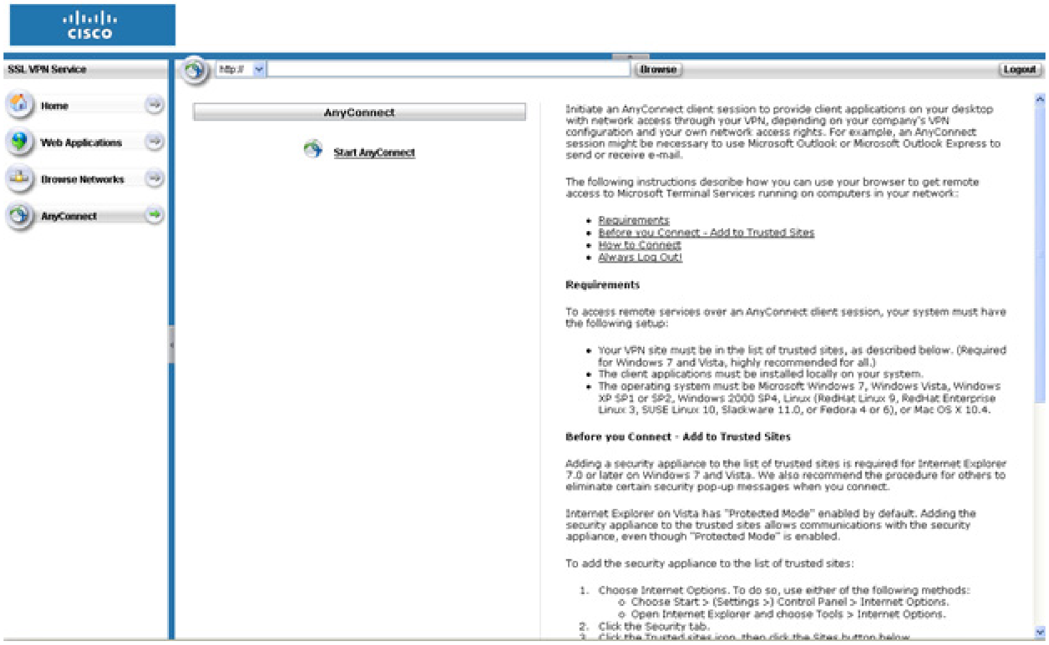
1 Open the browser where the certificate is installed.

2 Access the VPN URL.

3 Select the certificate and click **OK**.

4 Select a group from the **GROUP** drop-down list and click **Login**. The Cisco ASA Home page is displayed.

5 Click **AnyConnect** from the navigation menu.



Initiate an AnyConnect client session to provide client applications on your desktop with network access through your VPN, depending on your company's VPN configuration and your own network access rights. For example, an AnyConnect session might be necessary to use Microsoft Outlook or Microsoft Outlook Express to send or receive e-mail.

The following instructions describe how you can use your browser to get remote access to Microsoft Terminal Services running on computers in your network:

- Requirements
- Before you Connect - Add to Trusted Sites
- How to Connect
- Always Log Out!

Requirements

To access remote services over an AnyConnect client session, your system must have the following setup:

- Your VPN site must be in the list of trusted sites, as described below. (Required for Windows 7 and Vista, highly recommended for all.)
- The client applications must be installed locally on your system.
- The operating system must be Microsoft Windows 7, Windows Vista, Windows XP SP1 or SP2, Windows 2000 SP4, Linux (RedHat Linux 9, RedHat Enterprise Linux 3, SUSE Linux 10, Slackware 11.0, or Fedora 4 or 6), or Mac OS X 10.4.

Before you Connect - Add to Trusted Sites

Adding a security appliance to the list of trusted sites is required for Internet Explorer 7.0 or later on Windows 7 and Vista. We also recommend the procedure for others to eliminate certain security pop-up messages when you connect.

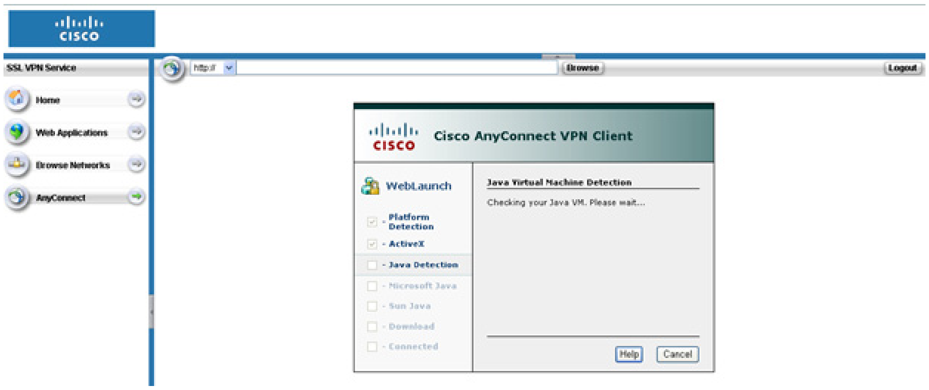
Internet Explorer on Vista has "Protected Mode" enabled by default. Adding the security appliance to the trusted sites allows communications with the security appliance, even though "Protected Mode" is enabled.

To add the security appliance to the list of trusted sites:

1. Choose Internet Options. To do so, use either of the following methods:
   - Choose Start > (Settings >) Control Panel > Internet Options.
   - Open Internet Explorer and choose Tools > Internet Options.
2. Click the Security tab.
3. Click the Trusted sites icon, then click the Sites button below.

Figure 2-9 Cisco AnyConnect VPN Client

6 Click **Start AnyConnect**. The VPN connection is established.



Java Virtual Machine Detection

Checking your Java VM. Please wait...

Figure 2-10 Cisco AnyConnect VPN Client for Desktop/Laptop

Connecting Desktop/Laptop to VPN (PKI Client)

1 Open the browser where the certificate is installed.

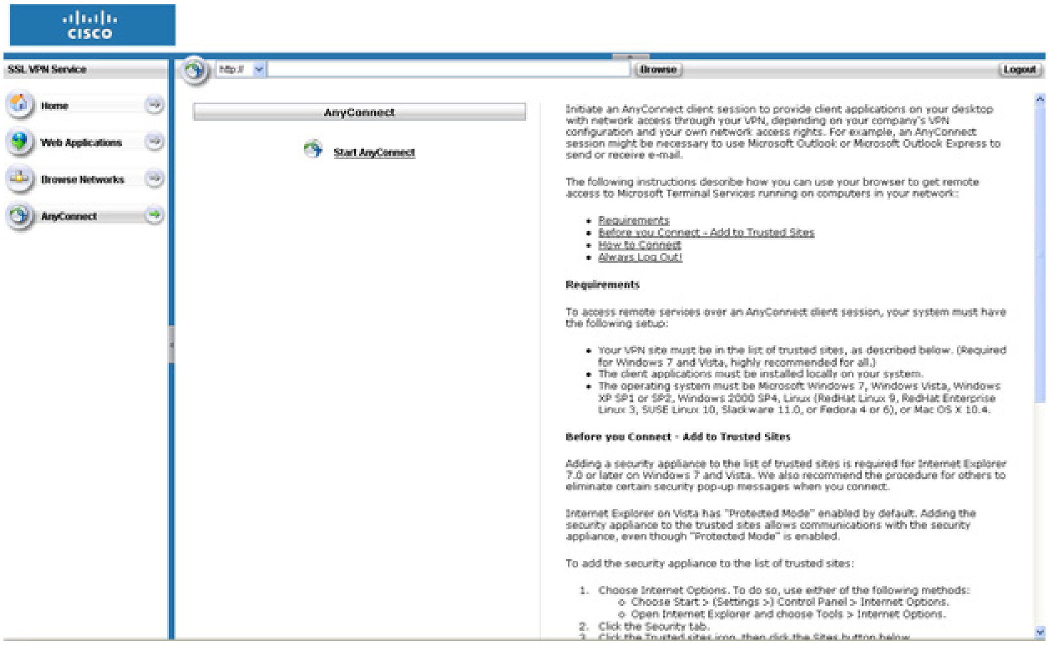
2 Access the VPN URL.

3 Select the certificate and click **OK**.

4 Enter the PIN for PKI Client when prompted, and click **OK**.

5 Select a group from the **GROUP** drop-down list and click **Login**. The Cisco ASA Home page is displayed.

6 Click **AnyConnect** from the navigation menu.



Initiate an AnyConnect client session to provide client applications on your desktop with network access through your VPN, depending on your company's VPN configuration and your own network access rights. For example, an AnyConnect session might be necessary to use Microsoft Outlook or Microsoft Outlook Express to send or receive e-mail.

The following instructions describe how you can use your browser to get remote access to Microsoft Terminal Services running on computers in your network:

- Requirements
- Before you Connect - Add to Trusted Sites
- How to Connect
- Always Log Out!

Requirements

To access remote services over an AnyConnect client session, your system must have the following setup:

- Your VPN site must be in the list of trusted sites, as described below. (Required for Windows 7 and Vista, highly recommended for all.)
- The client applications must be installed locally on your system.
- The operating system must be Microsoft Windows 7, Windows Vista, Windows XP SP1 or SP2, Windows 2000 SP4, Linux (RedHat Linux 9, RedHat Enterprise Linux 3, SUSE Linux 10, Slackware 11.0, or Fedora 4 or 6), or Mac OS X 10.4.

Before you Connect - Add to Trusted Sites

Adding a security appliance to the list of trusted sites is required for Internet Explorer 7.0 or later on Windows 7 and Vista. We also recommend the procedure for others to eliminate certain security pop-up messages when you connect.

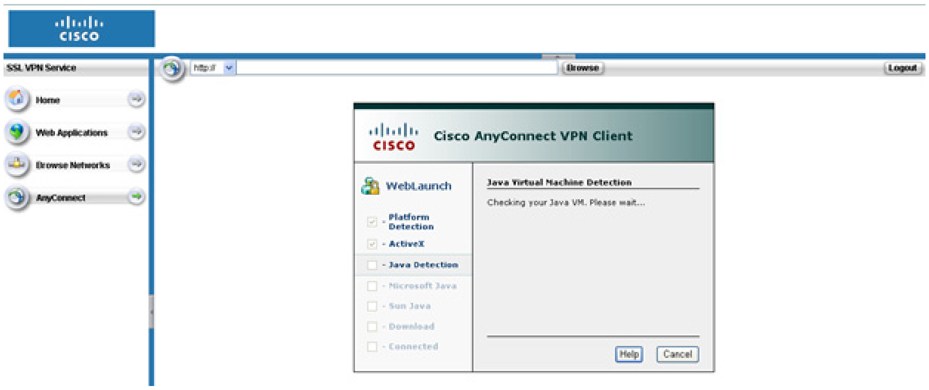
Internet Explorer on Vista has "Protected Mode" enabled by default. Adding the security appliance to the trusted sites allows communications with the security appliance, even though "Protected Mode" is enabled.

To add the security appliance to the list of trusted sites:

1. Choose Internet Options. To do so, use either of the following methods:
   - Choose Start > (Settings >) Control Panel > Internet Options.
   - Open Internet Explorer and choose Tools > Internet Options.
2. Click the Security tab.
3. Click the Trusted sites icon, then click the Sites button below.

Figure 2-11 Cisco AnyConnect VPN Client

7 Click **Start AnyConnect**. The VPN connection is established.



Java Virtual Machine Detection

Checking your Java VM. Please wait...

Figure 2-12 Cisco AnyConnect VPN Client for PKI Client