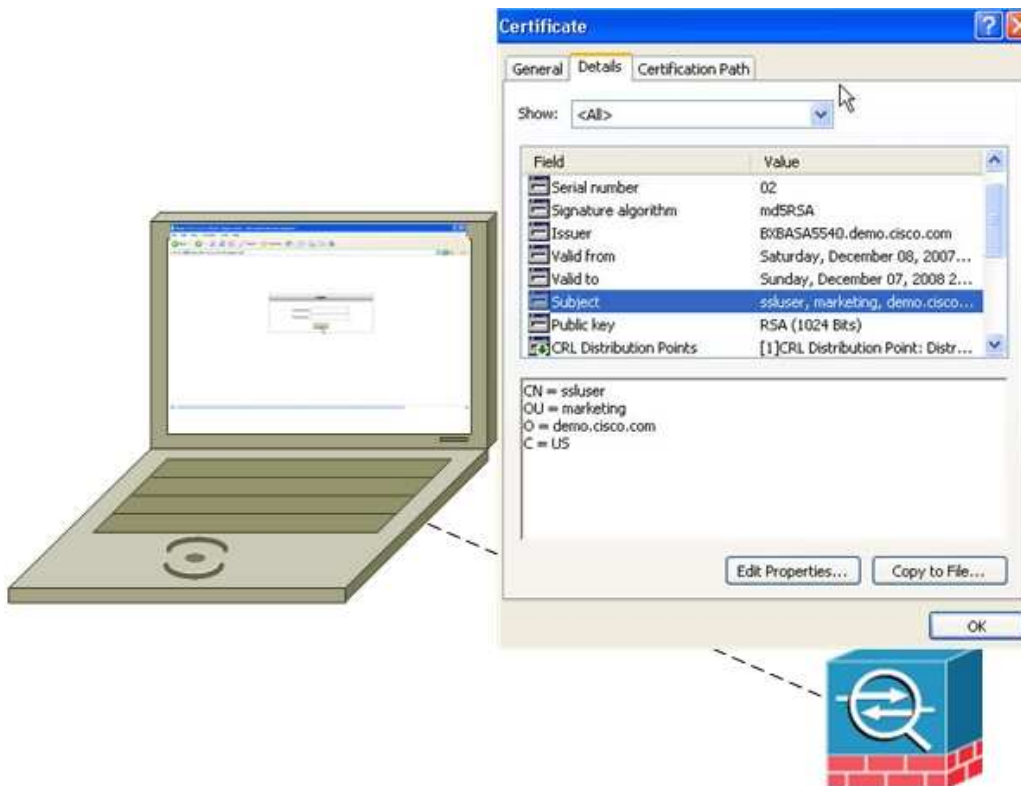


Application Note:

## Cisco ASA - Certificate To SSL VPN Connection Profile

### Overview:

This application note explains how to configure the ASA to accommodate SSL VPN sessions that utilize a certificate for authentication and use the attributes within the certificate to assign a specific Connection Profile to the user. The ability to map a user's certificate to a specific Connection Profile is also configurable for IPSEC VPN however this paper focuses solely on SSL VPN. The Connection Profile also known as a Tunnel Group consists of a set of records that determines the tunnel connection policies. We will also configure the ASA's Local Certificate Authority which we will use in this configuration example. The ASA's Local CA was introduced in v8.0 and offers basic CA features on the ASA itself without the need for an external CA. The Local CA can be used to both deploy and revoke certificates and offers users an easy enrollment mechanism.



```
tunnel-group Marketing type remote-access
tunnel-group Marketing general-attributes
authentication-server-group MS_LDAP
default-group-policy Marketing_Policy
tunnel-group Marketing webvpn-attributes
authentication certificate
group-alias marketing enable
```

```
crypto ca certificate map Marketing_Map 10
subject-name attr c eq us
subject-name attr ou eq marketing
```

## Section 1 ASA Configuration using ASDM

### Step 1. Enable the Outside Interface to require a Client Certificate

Navigate to '*Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles*' and ensure that 'Require Client Certificate' is checked off which will result in the ASA to checking for and requiring a valid certificate from the client before allowing a connection.

Figure 1 Require Client Certificate

The screenshot shows the ASDM interface for configuring Clientless SSL VPN Access. The left sidebar shows the navigation tree with 'Connection Profiles' selected. The main pane displays the configuration for the 'outside' interface. A green arrow points to the 'Require Client Certificate' checkbox, which is checked. Below the interface table, there is a table for Connection Profiles.

| Interface | Allow Access                        | Require Client Certificate          |
|-----------|-------------------------------------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Mgmt      | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Outside2  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            | <input type="checkbox"/>            |

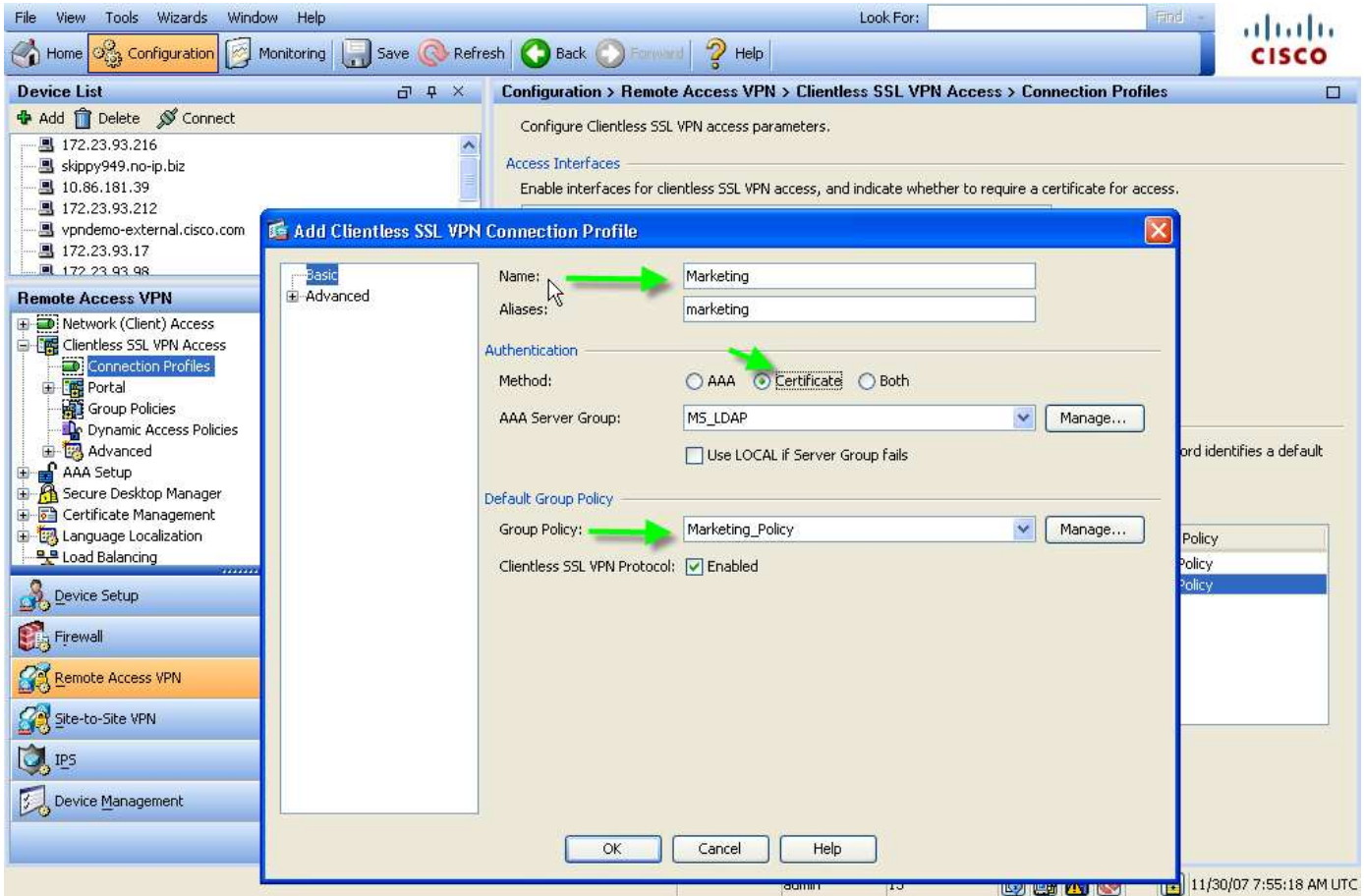
| Name               | Aliases | Clientless SSL VPN Protocol | Group Policy  |
|--------------------|---------|-----------------------------|---------------|
| DefaultRAGroup     |         | Enabled                     | DfltGrpPolicy |
| DefaultWEBVPGGroup |         | Enabled                     | DfltGrpPolicy |

### Step 2. Configure/Add a Connection Profile

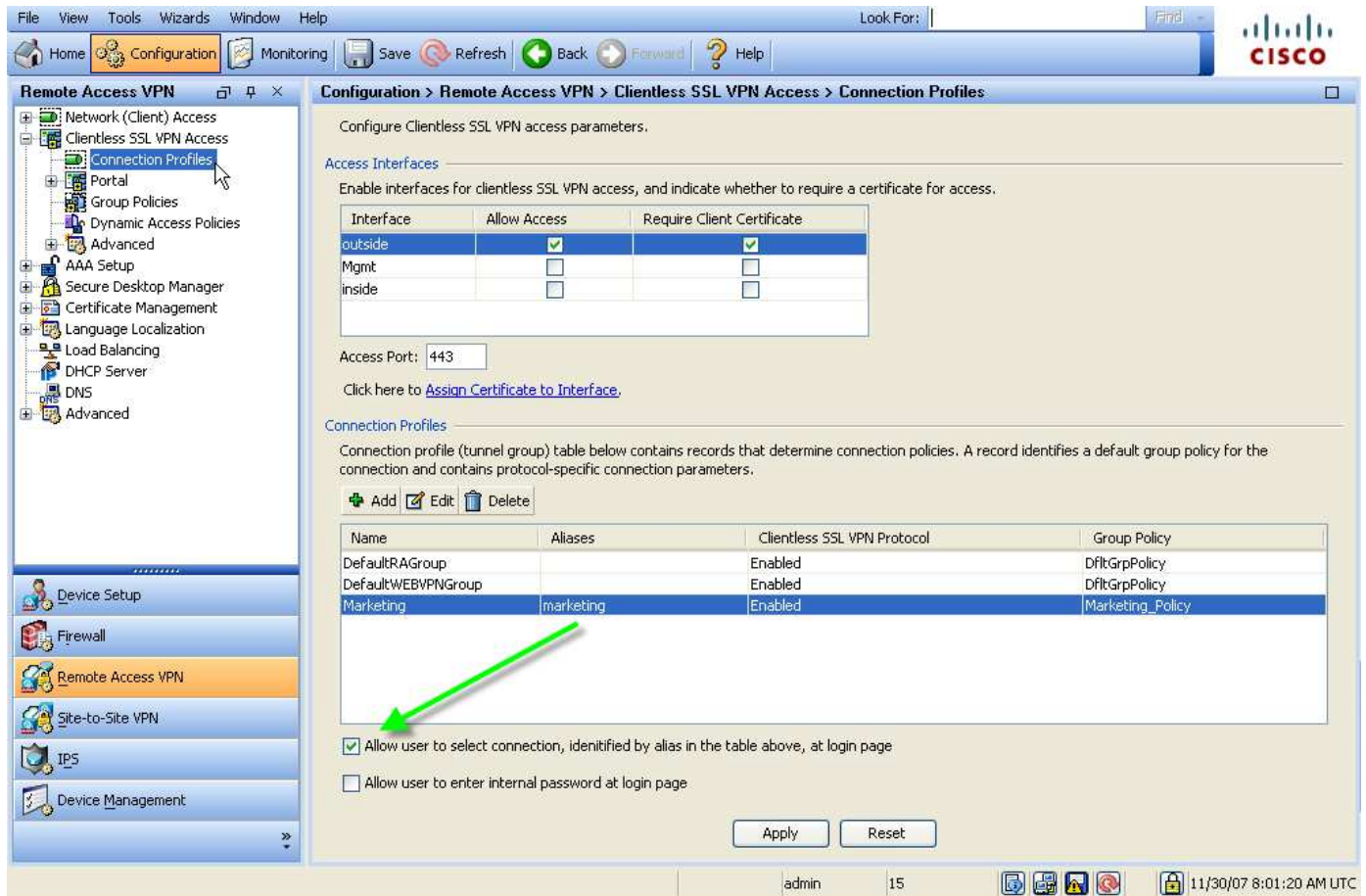
If you have already configured a Connection Profile then just edit the desired profile, however we will configure a new profile as follows.

Navigate to *'Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles'* and click 'Add'. Name the profile and create an alias for the Connection Profile. An alias specifies that an alternate name can be used for this connection as long as you also enable this feature. Also notice that we selected an alternative and existing Group Policy rather than using the default for this Connection profile but this is not necessary in order to successfully test this solution.

Figure 2 Connection Profile configuration



**Figure 3 Enable the use of alias**

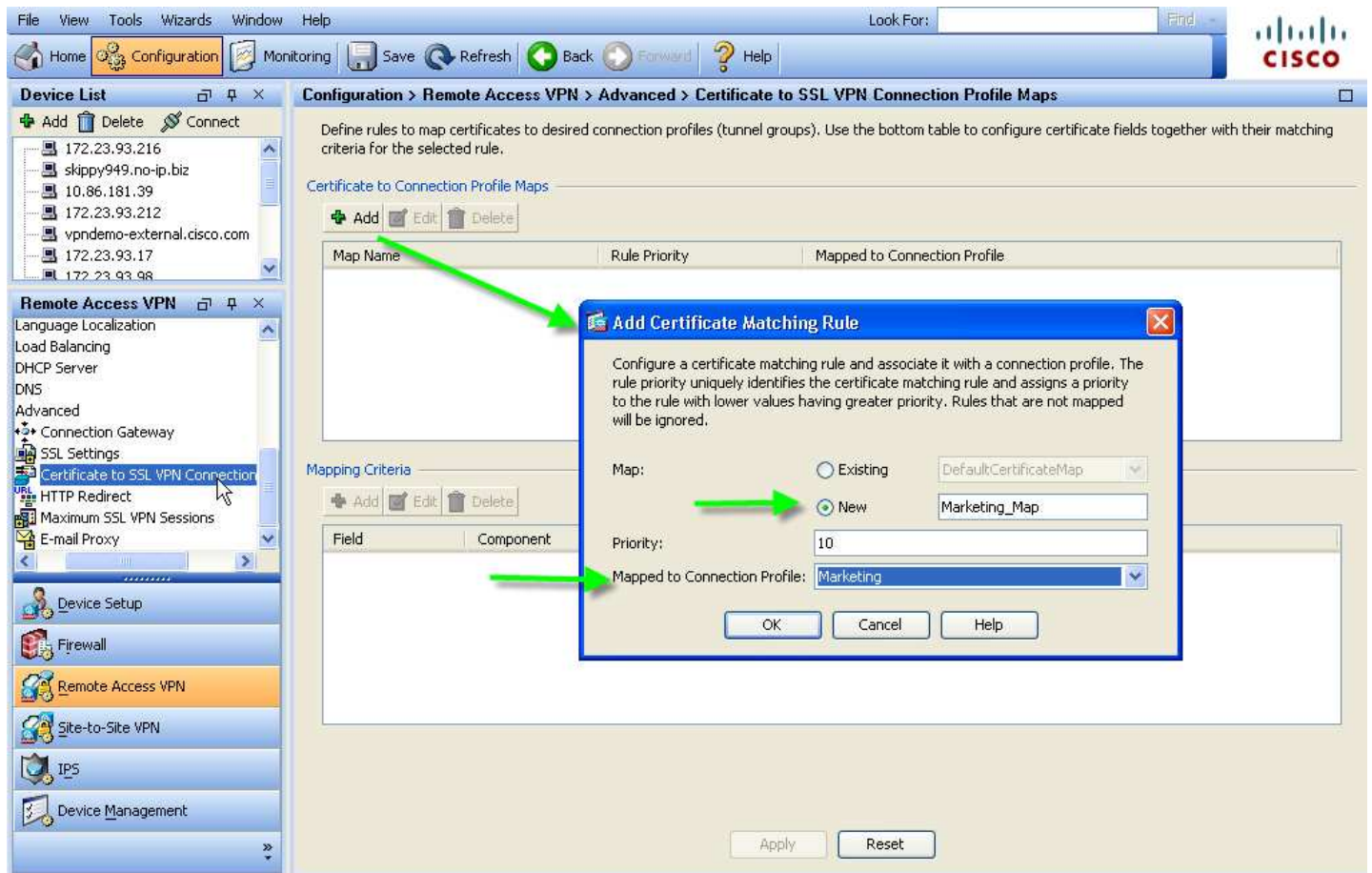


### Step 3. Configure a Certificate to SSL VPN Connection Profile Map

In order for the ASA to select a specific Connection Profile based on the attributes contained in the client's certificate we need to define a mapping rule to match users to a Connection Profile based on these attributes. Once the rules are defined they are then associated with the desired profile.

**Navigate to 'Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps'** and click on 'Add' under the 'Certificate to Connection Profile Maps'. In this example, if the certificate has OU=marketing and C=US, the user will be mapped to the 'Marketing' Connection Profile.

Figure 4 Create New Certificate Map

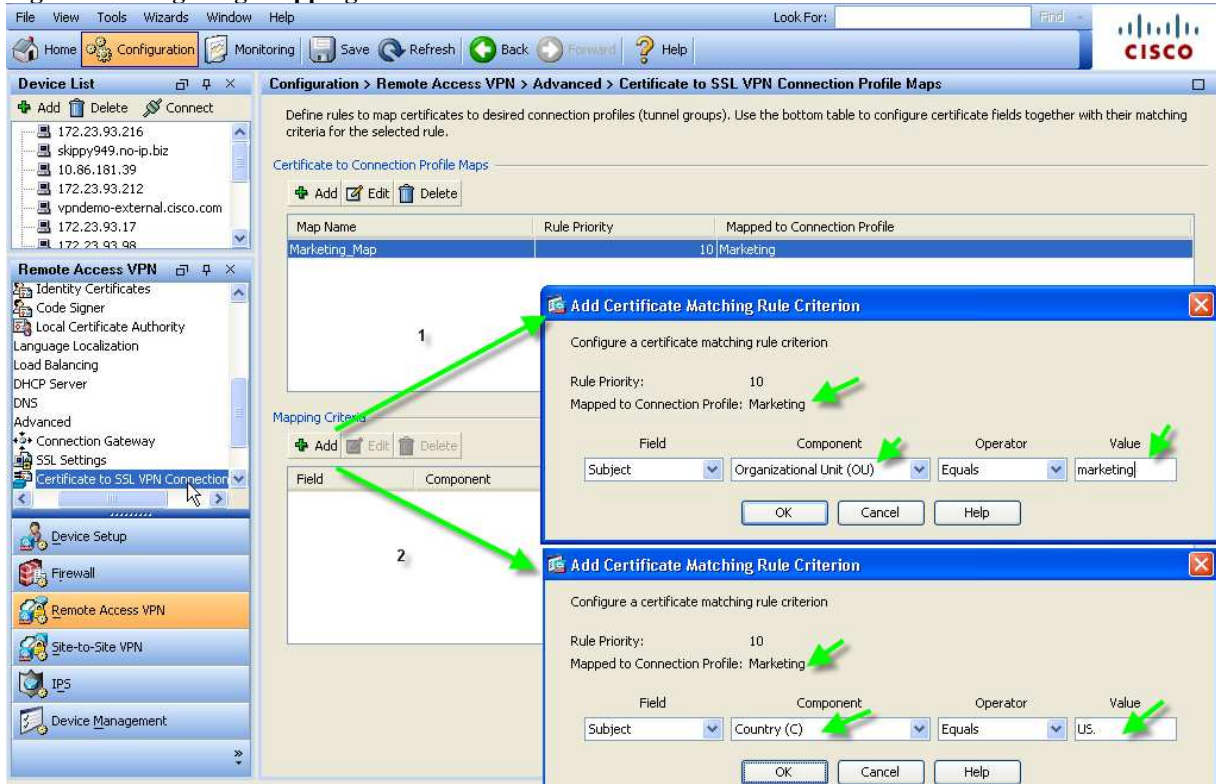


**Note:** Multiple Connection Profile Maps could exist and if this was the case then the ASA would evaluate each connection against the mapping list with the lowest priority number taking precedence.

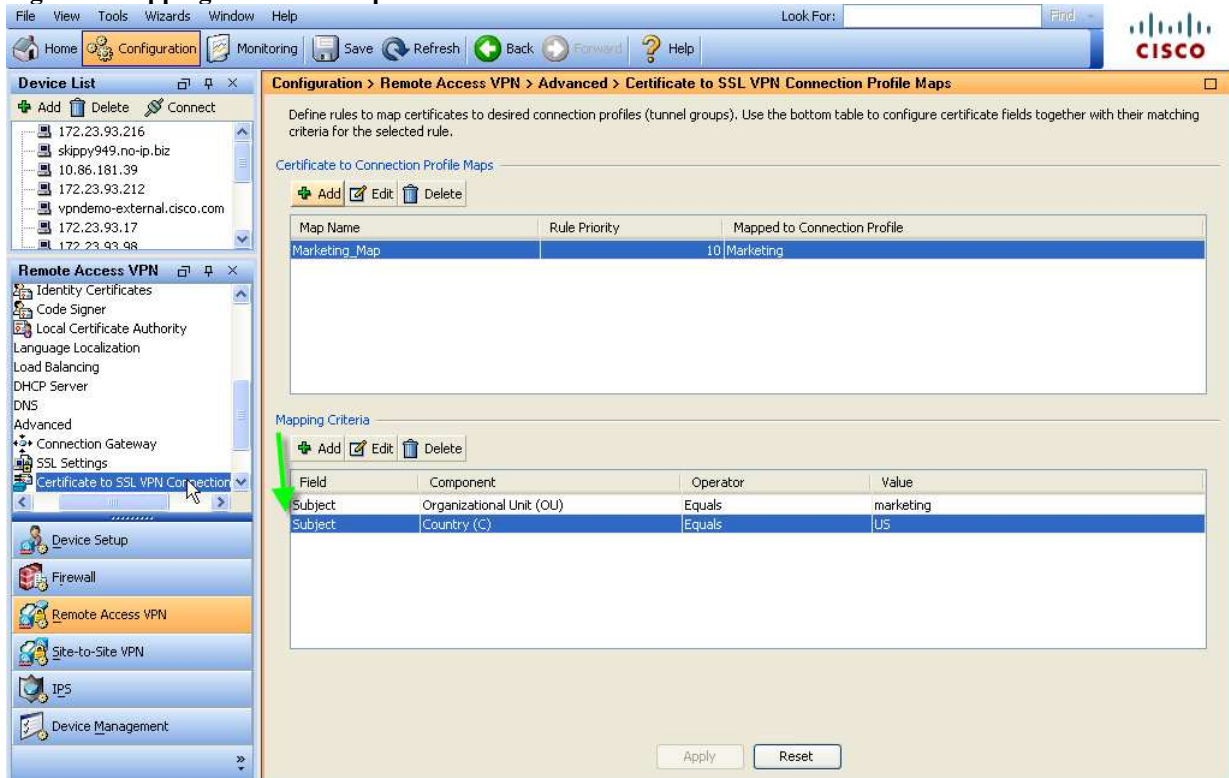
After configuring the new Connection Profile Map, the next step is to configure criteria match for the map 'Marketing\_Map' configured in the previous step. Once again the criteria we want to match is that the users certificate contains OU = marketing and C = US and if both exist the user has successfully met the criteria and will be connected to the 'Marketing' Connection Profile.

**Navigate to 'Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps'** and with the 'Marketing\_Map' highlighted use the lower pane to configure 2 rules as shown in Figure 5 and completed in Figure 6.

**Figure 5 Configuring Mapping Criteria**



**Figure 6 Mapping Criteria Completed**



**Note:** You can configure rules based on the Issuer and Subject fields of a certificate and for more information please reference the Cisco Security Appliance Command Line Configuration Guide, Version 8.0.

[http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/cert\\_cfg.html#wp1046987](http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/cert_cfg.html#wp1046987)

#### Step 4. Configure a Local Certificate Authority

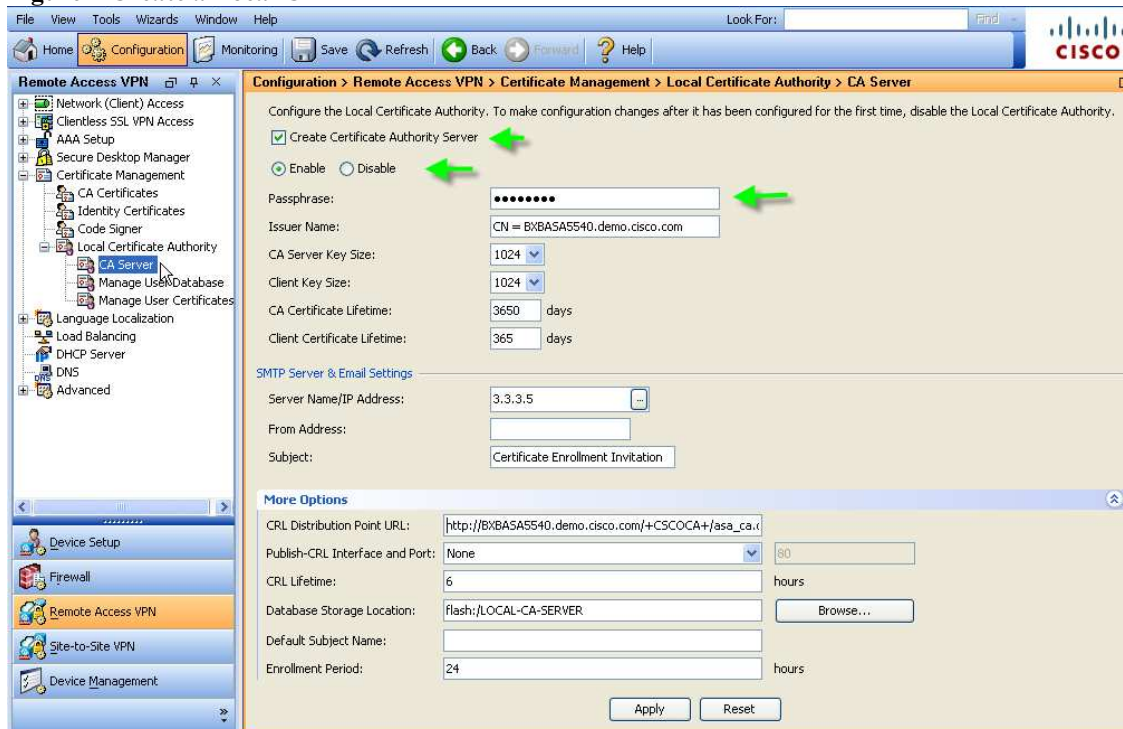
The ASA offers a Local Certificate Authority (CA) that is an in-house authority that resides directly on the appliance for certificate authentication.

- User enrollment is by browser webpage login
- Integrates basic certificate authority functionality on the ASA
- Deploys certificates
- Provides secure revocation checking of issued certificates

Navigate to **'Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server'** and Create the Certificate Authority as shown below to enable users to obtain certificates via a web browser. Optionally you could configure e-mail access for the Local CA server by configuring a Simple Mail Transfer Protocol (SMTP) e-mail server, the e-mail address from which to send e-mails to Local CA users but for the purpose of this example we will only configure HTTP.

- Check off 'Create Certificate Authority Server'
- Check off 'Enable'
- Enter a 'PassPhrase'

**Figure 7 Create a Local CA**



## Step 5. Add a user to the Local CA's User Database

The ASA's Local CA maintains a user database and the status of the users enrollment such as enrolled, allowed or revoked. In this step we will add a user 'ssluser' to the database.

Navigate to 'Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database' and select 'Add' and enter the information as shown in Figure 8.

1. Select 'Add' to add the user 'ssluser'
2. Enter the username 'ssluser'
3. Enter the Email ID (optional in this case)
4. Enter the Subject (DN String) – this can be typed directly in the box or click 'Select to enter it step by step.'
5. Click Select and configure the value for each attribute contained in the user's certificate.

Figure 8 Add user to the database

The screenshot shows the Cisco ASA configuration interface. The main window is titled 'Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database'. The 'Add User' dialog box is open, showing the following fields:

- Username: ssluser
- Email ID: ssluser@demo.cisco.com
- Subject (DN String): [Empty]
- Allow enrollment

The 'Certificate Subject DN' dialog box is also open, showing the following table:

| Attribute        | Value          |
|------------------|----------------|
| Common Name (CN) | ssluser        |
| Department (OU)  | marketing      |
| Company Name (O) | demo.cisco.com |
| Country (C)      | US             |

Green arrows indicate the steps: 1. Click 'Add' button; 2. Enter 'ssluser' in the Username field; 3. Enter 'ssluser@demo.cisco.com' in the Email ID field; 4. Click 'Select...' button; 5. Click 'Add>>' button in the 'Certificate Subject DN' dialog.



After adding the user the status of the user will be that enrollment is allowed but not yet enrolled as shown in figure 9 below and also note the One Time Password that was automatically generated for the user and required for enrollment, but note this OTP is not required once the user has successfully enrolled.

**Figure 9 User configuration complete**

The screenshot shows the Cisco configuration interface for the Local Certificate Authority's Manage User Database. The interface includes a menu bar (File, View, Tools, Wizards, Window, Help) and a toolbar with icons for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The breadcrumb trail is Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database. The main area displays a table of users with the following data:

| Username | Email                  | Subject Name                                  | Enrollment Status | Certificate Holder |
|----------|------------------------|---|-------------------|--------------------|
| ssluser  | ssluser@demo.cisco.com | CN=ssluser,OU=marketing,O=demo.cisco.com,C=US | allowed           | no                 |

Green arrows point to the 'ssluser' row in the table. A 'View & Re-generate OTP' dialog box is open, showing the user's details and the generated OTP: 'F1C35C8072CE96F2'. A green arrow points from the 'View/Re-generate OTP' button in the right-hand panel to the dialog box. The dialog box also includes a 'Re-generate OTP' button and 'OK', 'Cancel', and 'Help' buttons. At the bottom of the main window are 'Apply' and 'Reset' buttons.

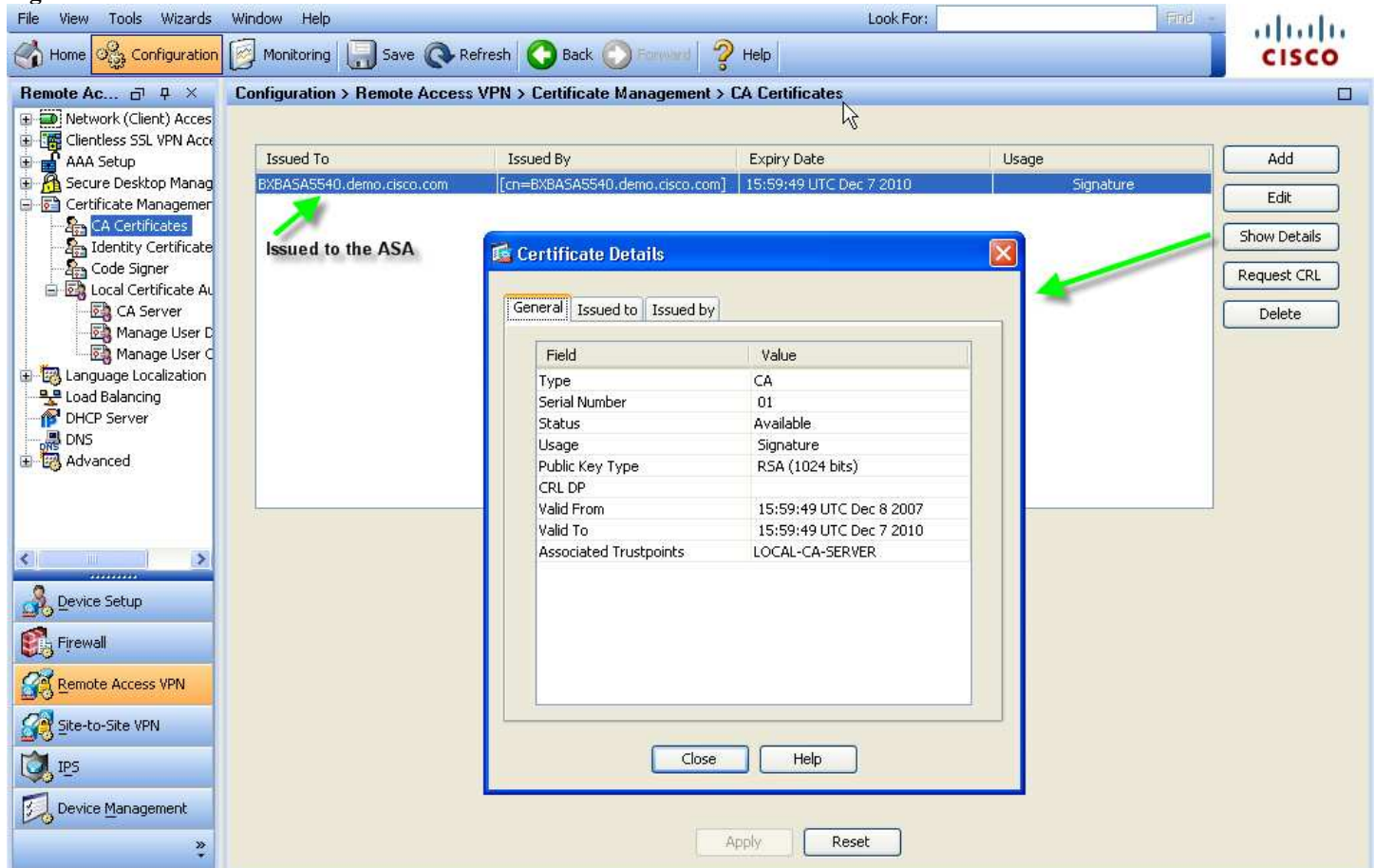
## Step 6. Verify the Local CA's Certificate

When we created the Local CA on the ASA a local certificate should have been created for the ASA, ensure that it is present.

**Note:** If the Certificate does not appear, save the configuration and refresh ASDM.

**Navigate to 'Configuration > Remote Access VPN > Certificate Management > CA Certificates'**

**Figure 10 ASA's CA Certificate**



The screenshot displays the ASDM interface for configuring CA Certificates. The main window shows a table of certificates with the following data:

| Issued To                 | Issued By                      | Expiry Date             | Usage     |
|---------------------------|--------------------------------|-------------------------|-----------|
| BXBASAS540.demo.cisco.com | [cn=BXBASAS540.demo.cisco.com] | 15:59:49 UTC Dec 7 2010 | Signature |

A green arrow points to the 'Issued To' field, which is labeled 'Issued to the ASA'. A 'Certificate Details' dialog box is open, showing the following information:

| Field                  | Value                   |
|------------------------|-------------------------|
| Type                   | CA                      |
| Serial Number          | 01                      |
| Status                 | Available               |
| Usage                  | Signature               |
| Public Key Type        | RSA (1024 bits)         |
| CRL DP                 |                         |
| Valid From             | 15:59:49 UTC Dec 8 2007 |
| Valid To               | 15:59:49 UTC Dec 7 2010 |
| Associated Trustpoints | LOCAL-CA-SERVER         |

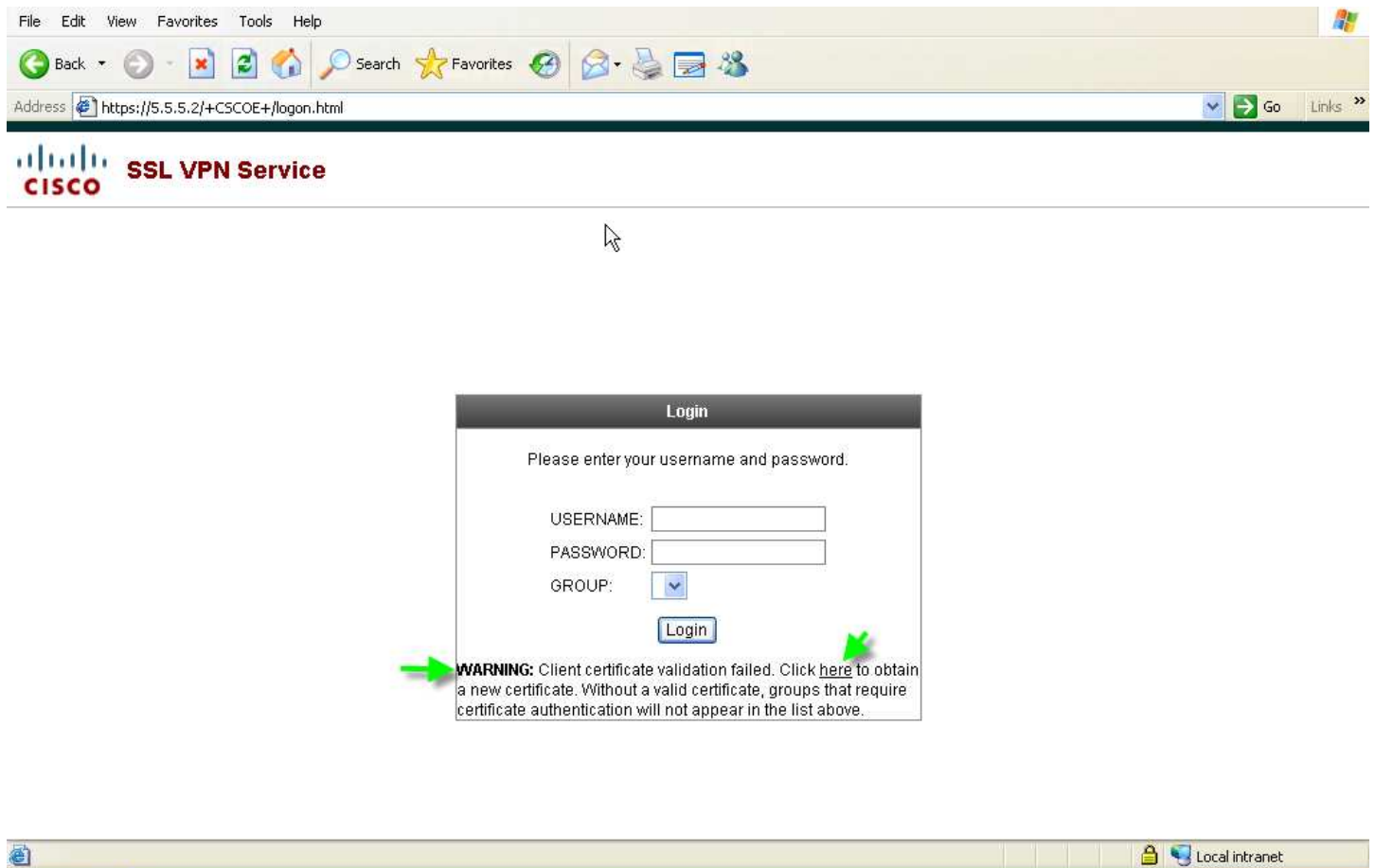
**Note:** This completes the ASA Configuration.

## Section 2 SSL VPN Clientless User Configuration

### Step 1. Enroll the user with the ASA's Local Certificate Authority

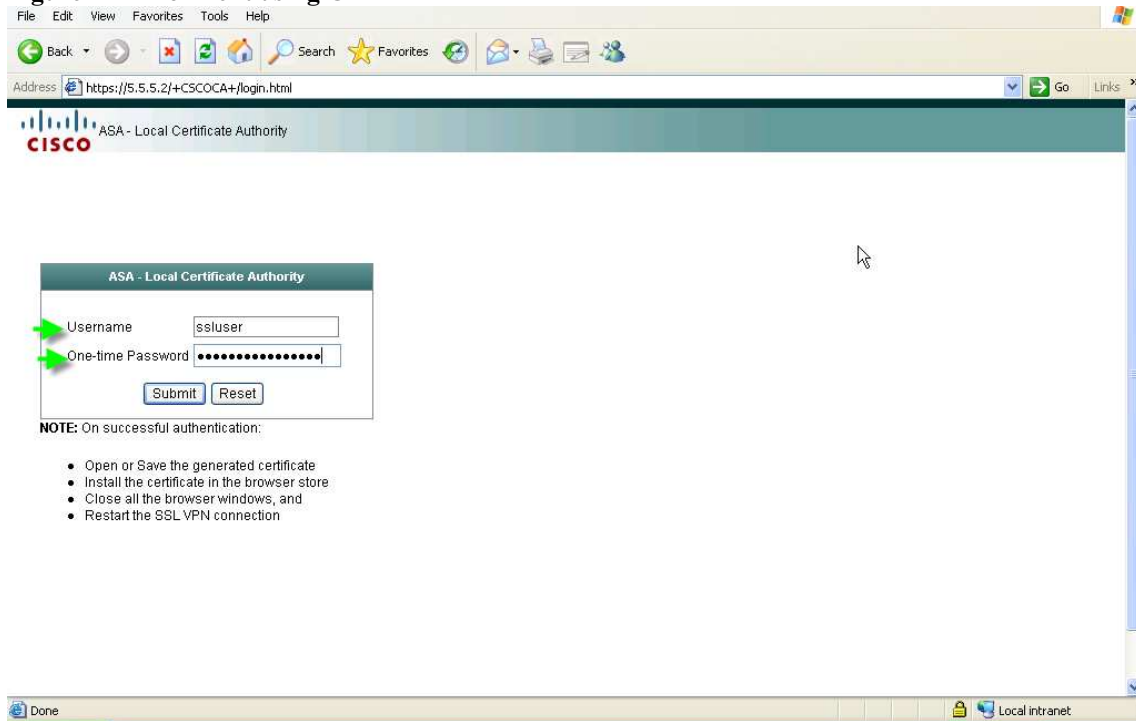
Using Internet Explorer connect via the enrollment URL shown in Figure 11. The first login screen you should receive will warn you that the certificate does not yet exist and will prompt you to obtain the certificate.

Figure 11 Initial login screen <https://5.5.5.2/+CSCOE+/enroll.html>



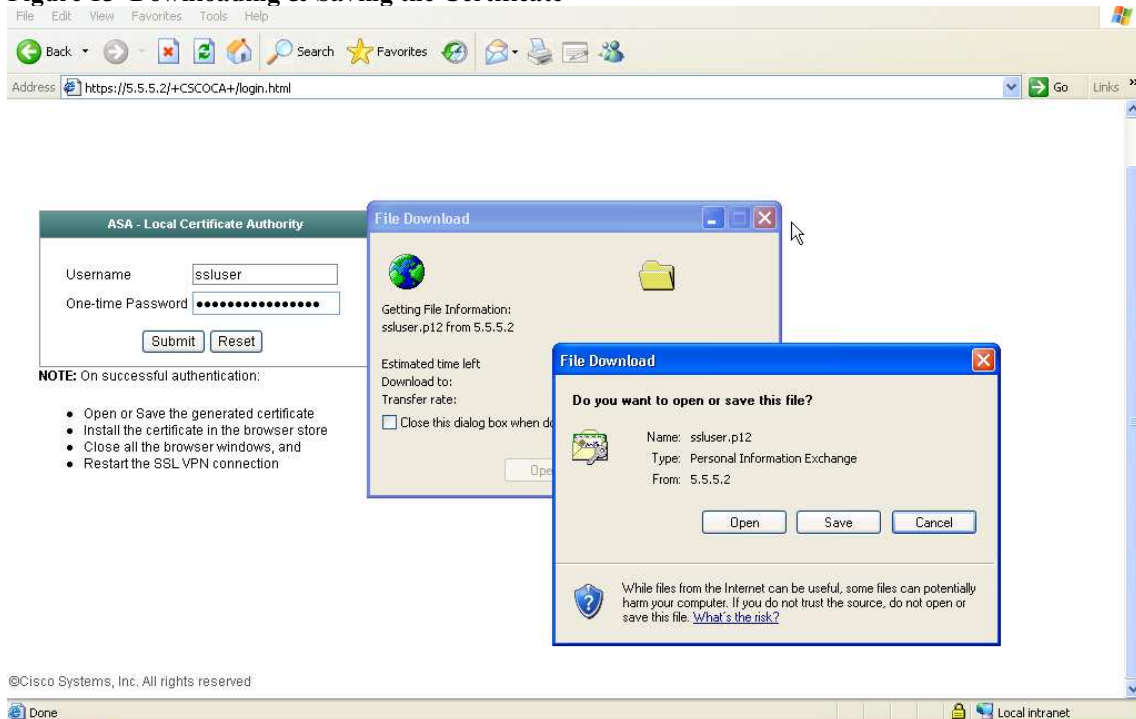
## Step 2. Enter in the user name 'ssluser' and the OTP shown earlier in Step 5 and Figure 9.

Figure 12 Enrollment using OTP



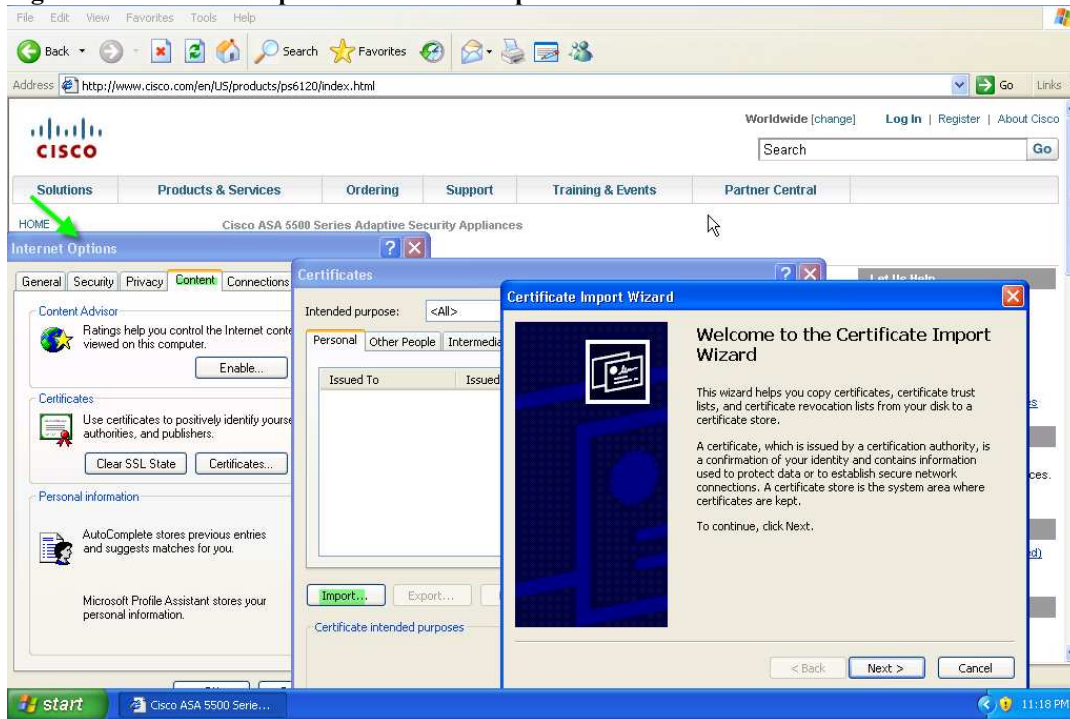
## Step 3. Download and save the certificate to the Desktop.

Figure 13 Downloading & Saving the Certificate



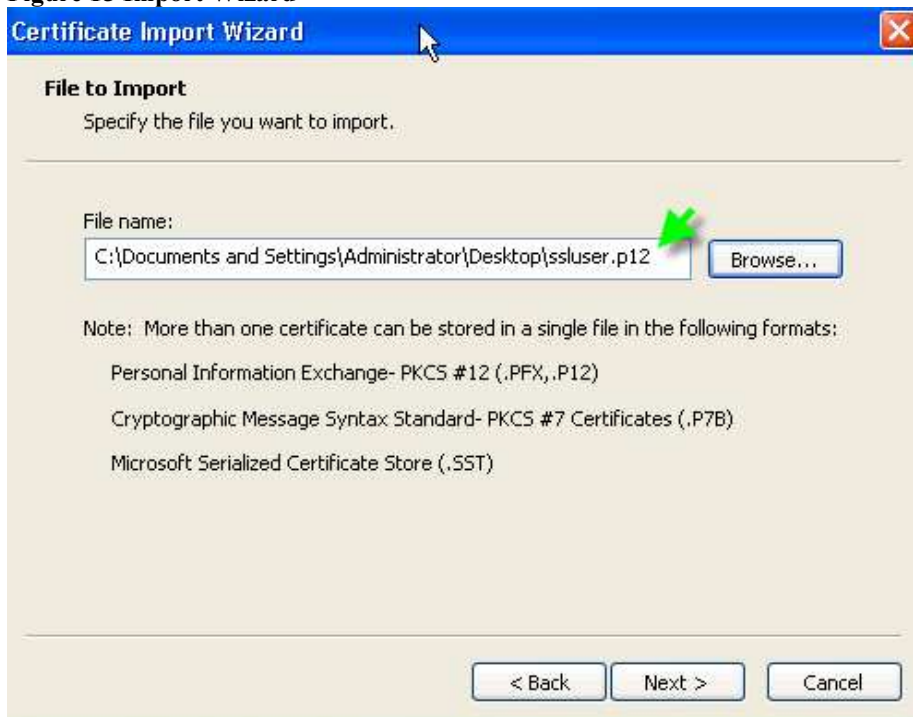
**Step 4. Open up ‘Tools/Internet Options/Content/Certificates/Import’ and select ‘Next’ to begin the import process.**

**Figure 14 IE Internet Options Certificate Import**



**Step 5. When prompted select the certificate that was saved to the desktop in step 3.**

**Figure 15 Import Wizard**



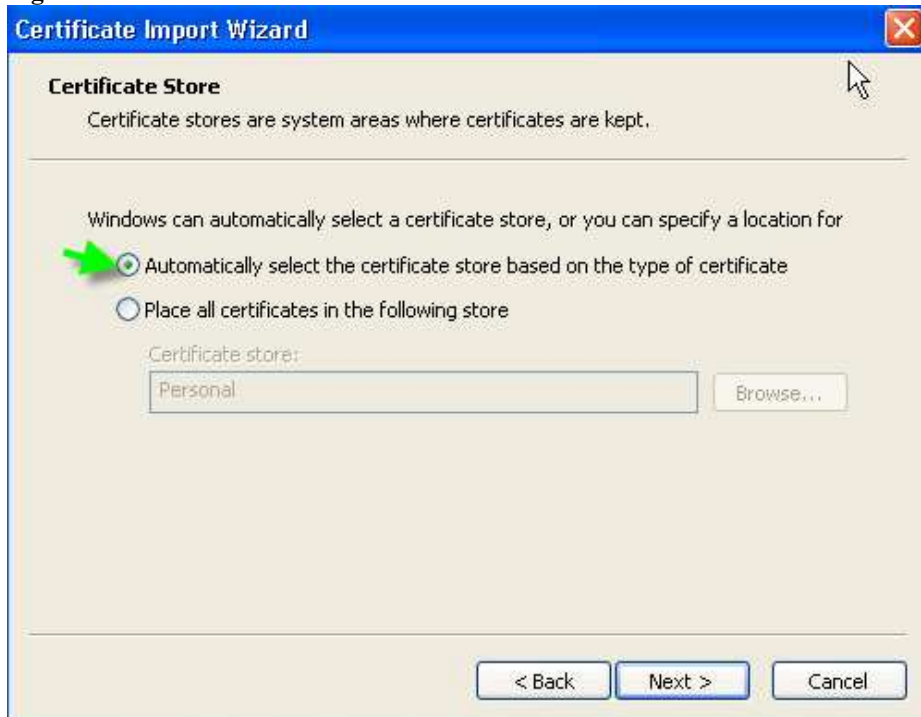
**Step 6. Enter the OTP when prompted for the password.**

**Figure 16 OTP Required by Wizard**



**Step 7. Allow IE to determine the proper Certificate Store for the newly imported certificate.**

**Figure 17 Certificate store**



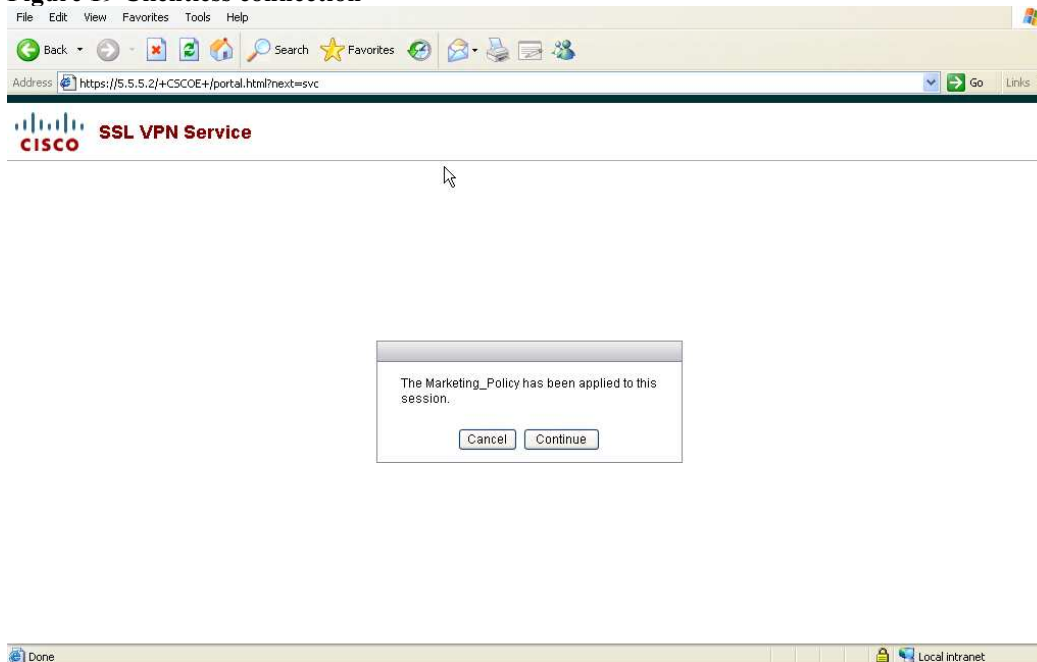
**Figure 18 Certificate Import completed**



### Step 8. Make a Clientless SSL VPN Connection

The expected result is that the user upon establishing the connection to the ASA will be prompted to acknowledge a banner configured on the group-policy associated with the marketing connection profile and then given the portal.

**Figure 19 Clientless connection**



## Step 9. Verifying the session using ASDM and the CLI

Figure 20 ASDM Monitoring

The screenshot shows the ASDM Monitoring interface for VPN Statistics > Sessions. The interface includes a navigation tree on the left, a top menu bar, and a main content area. The main content area displays a table of sessions with the following data:

| Remote Access | Site-to-Site | SSL VPN | Clientless | With Client | Total | E-mail Proxy | VPN Load Balancing | Total | Total Cumulative |
|---------------|--------------|---------|------------|-------------|-------|--------------|--------------------|-------|------------------|
| 0             | 0            | 1       | 0          | 1           | 0     | 0            | 1                  | 12    |                  |

Below the table, a filter is set to 'Clientless SSL VPN'. The session table shows one entry for 'ssluser' with IP address 10.86.181.70, connected to the 'Marketing\_Policy' profile. A message below the table states: 'The user 'ssluser' is connected to the 'Marketing' Connection Profile as specified by the certificate'.

Figure 21 CLI command

```
BXBASA5540# sho vpn-sessiondb detail webvpn
```

Session Type: WebVPN Detailed

```

Username   : ssluser           Index      : 12
Public IP  : 10.86.181.70
Protocol   : Clientless
License    : SSL VPN
Encryption : RC4             Hashing    : SHA1
Bytes Tx   : 420538          Bytes Rx   : 181632
Pkts Tx    : 4              Pkts Rx    : 1
Pkts Tx Drop : 0           Pkts Rx Drop : 0
Group Policy : Marketing_Policy   Tunnel Group : Marketing
Login Time : 21:30:56 UTC Sat Dec 8 2007
Duration   : 0h:07m:15s
NAC Result : Unknown
VLAN Mapping : N/A          VLAN       : none

Clientless Tunnels: 1
    
```



**References:**

<http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/webvpn.html#wp1021682>

[http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/cert\\_cfg.html#wp1067484](http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/cert_cfg.html#wp1067484)

[http://www.cisco.com/en/US/partner/docs/security/asa/asa80/asdm60/user/guide/vpn\\_web.html#wp1057037](http://www.cisco.com/en/US/partner/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html#wp1057037)