

ASA 8.x: AnyConnect SSL VPN CAC-SmartCards Configuration with MAC Support

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Cisco ASA Configuration](#)

[Deployment Considerations](#)

[Authentication, Authorization, Accounting \(AAA\) Configuration](#)

[Configure LDAP Server](#)

[Manage Certificates](#)

[Generate Keys](#)

[Install Root CA Certificates](#)

[Enroll ASA and Install Identity Certificate](#)

[AnyConnect VPN Configuration](#)

[Create an IP Address Pool](#)

[Create Tunnel Group and Group Policy](#)

[Tunnel Group Interface and Image Settings](#)

[Certificate Matching Rules \(If OCSP will be used\)](#)

[Configure OCSP](#)

[Configure OCSP Responder Certificate](#)

[Configure CA to use OCSP](#)

[Configure OCSP Rules](#)

[Cisco AnyConnect Client Configuration](#)

[Downloading Cisco Anyconnect VPN Client – Mac OS X](#)

[Start Cisco AnyConnect VPN Client – Mac OS X](#)

[New Connection](#)

[Start remote access](#)

[Appendix A – LDAP Mapping and DAP](#)

[Scenario 1: Active Directory Enforcement using Remote Access Permission Dial-in – Allow/Deny Access](#)

[Active Directory Setup](#)

[ASA Configuration](#)

[Scenario 2 : Active Directory Enforcement using Group membership to Allow/Deny Access](#)

[Active Directory Setup](#)

[ASA Configuration](#)

[Scenario 3: Dynamic Access Policies for Multiple memberOf Attributes](#)

[ASA Configuration](#)

[Appendix B – ASA CLI Configuration](#)

[Appendix C- Troubleshooting](#)

[Troubleshooting AAA and LDAP](#)

[Example 1: Allowed Connection with correct attribute mapping](#)

[Example 2: Allowed Connection with mis-configured Cisco attribute mapping](#)

[Troubleshooting DAP](#)

[Example 1: Allowed connection with DAP](#)

[Example 2: Denied Connection with DAP](#)

[Troubleshooting Certificate Authority / OCSP](#)

[Appendix D – Verify LDAP Objects in MS](#)

[Introduction](#)

This document provides a sample configuration on Cisco Adaptive Security Appliance (ASA) for AnyConnect VPN remote access for MAC Support with the Common Access Card (CAC) for authentication.

The scope of this document is to cover the configuration of Cisco ASA with Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client and Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

The configuration in this guide uses Microsoft AD/LDAP server. This document also covers advanced features such as OCSP, LDAP attribute maps and Dynamic Access Policies (DAP).

[Prerequisites](#)

[Requirements](#)

A basic understanding of Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP and Public Key Infrastructure (PKI) is beneficial in the comprehension of the complete setup. Familiarity with AD group membership, user properties as well as LDAP objects help in the correlation of the authorization process between certificate attributes and AD/LDAP objects.

[Components Used](#)

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance (ASA) that runs the software version 8.0(x) and later
- Cisco Adaptive Security Device Manager (ASDM) version 6.x for ASA 8.x
- Cisco AnyConnect VPN Client 2.2 with MAC Support

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

[Cisco ASA Configuration](#)

This section covers the configuration of Cisco ASA via ASDM. It covers the necessary steps in order to deploy a VPN remote access tunnel through an SSL AnyConnect connection. The CAC certificate is used for authentication and the User Principal Name (UPN) attribute in the certificate

is populated in active directory for authorization.

Deployment Considerations

- This guide does NOT cover basic configurations such as interfaces, DNS, NTP, routing, device access, ASDM access and so forth. It is assumed that the network operator is familiar with these configurations. Refer to [Multifunction Security Appliances](#) for more information.
- The sections highlighted in RED are mandatory configurations needed for basic VPN access. For example, a VPN tunnel can be setup with the CAC card without doing OCSP checks, LDAP mappings and Dynamic Access Policy (DAP) checks. DoD mandates OCSP checking but the tunnel works without OCSP configured.
- The sections highlighted in BLUE are advanced features that can be included to add more security to the design.
- ASDM and AnyConnect/SSL VPN can not use the same ports on the same interface. It is recommended to change the ports on one or the other to gain access. For example, use port 445 for ASDM and leave 443 for AC/SSL VPN. The ASDM URL access has changed in 8.x. Use `https://<ip_address>:<port>/admin.html`.
- The ASA image required is at least 8.0.2.19 and ASDM 6.0.2.
- AnyConnect/CAC is supported with Vista.
- See [Appendix A](#) for LDAP & Dynamic Access Policy mapping examples for additional policy enforcement.
- See [Appendix D](#) on how to check LDAP objects in MS.
- See Related Information for a list of application ports for firewall configuration.

Authentication, Authorization, Accounting (AAA) Configuration

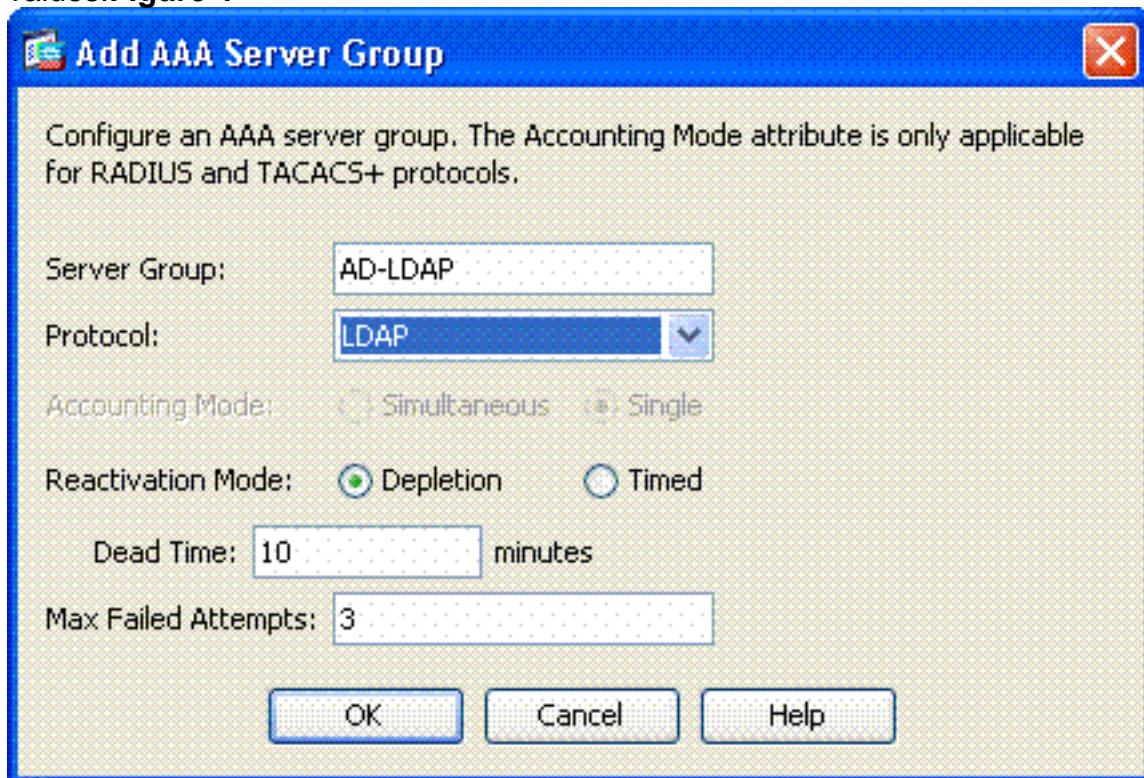
You are authenticated with the use of the certificate in their Common Access Card (CAC) through the DISACertificate Authority (CA) Server or the CA server of their own organization. The certificate must be valid for remote access to the network. In addition to authentication, you must also be authorized to use a Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) object. Department of Defense (DoD) requires the use of the User Principal Name (UPN) attribute for authorization, which is part of the Subject Alternative Name (SAN) section of the certificate. The UPN or EDI/PI must be in this format, 1234567890@mil. These configurations show how to configure AAA server in the ASA with an LDAP server for authorization. See [Appendix A](#) for additional configuration with LDAP object mapping.

Configure LDAP Server

Complete these steps:

1. Choose **Remote Access VPN > AAA Setup > AAA Server Group**.
2. In AAA server groups table, click **Add 3**.
3. Enter server group name and choose **LDAP** in the protocol radio button. See Figure 1.
4. In Servers in the selected group table, click **Add**. Make sure that the server you created is highlighted in the previous table.
5. In the edit AAA server window, complete these steps. See Figure 2. **Note:** Choose the **Enable LDAP over SSL** option if your LDAP/AD is configured for this type of

connection. Choose the interface where the LDAP is located. This guide shows inside the interface. Enter the IP address of the server. Enter **server port**. The default LDAP port is 389. Choose **Server Type**. Enter **Base DN**. Ask your AD/LDAP administrator for these values. **Figure-1**



Configure an AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group: AD-LDAP

Protocol: LDAP

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

OK Cancel Help

Under the scope option, choose the appropriate answer. This is dependent on the base DN. Ask your AD/LDAP administrator for assistance. In the naming attribute, enter **userPrincipalName**. This is the attribute that is used for user authorization in the AD/LDAP server. In the Login DN, enter the administrator DN. **Note:** You have administrative rights or rights to view/search the LDAP structure that includes user objects and group membership. In the Login Password, enter the password of the administrator. Leave the LDAP attribute to **none**. **Figure-2**

Add AAA Server

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: lministrator,CN=Users,DC=gsgseclab,DC=org

Login Password: ●●●●●●●●

LDAP Attribute Map: -- None --

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

Note: You

use this option later on the configuration to add other AD/LDAP object for authorization. Choose **OK**.

6. Choose **OK**.

Manage Certificates

There are two steps in order to install certificates on the ASA. First, install the CA certificates (Root and Subordinate Certificate Authority) needed. Secondly, enroll the ASA to a specific CA and obtain the identity certificate. DoD PKI utilizes these certificates, Root CA2, Class 3 Root, CA## Intermediate that the ASA is enrolled with, ASA ID certificate and OCSP certificate. But, if you choose not to use OCSP, the OCSP certificate does *not* need to be installed.

Note: Contact your security POC in order to obtain root certificates as well as instructions on how to enroll for an identity certificate for a device. An SSL certificate should be sufficient for the ASA for remote access. A Dual SAN certificate is *not* required.

Note: The local machine also has to have the DoD CA chain installed. The certificates can be viewed in the Microsoft Certificate Store with Internet Explorer. DoD has produced a batch file that automatically adds all of the CAs to the machine. Ask your PKI POC for more information.

Note: DoD CA2 and Class 3 Root as well as the ASA ID and CA intermediate that issued the ASA cert should be the only CAs needed for user authentication. All of the current CA intermediates fall under the CA2 and Class 3 Root chain and are trusted as long as the CA2 and Class 3 Roots are added.

Generate Keys

Complete these steps:

1. Choose **Remote Access VPN > Certificate Management > Identity Certificate > Add**.
2. Choose **Add a new id certificate** and then **New** by the key pair option.
3. In the Add Key Pair window, enter a key name, **DoD-1024**. Click on the radio to add a new key. See Figure 3. **Figure 3**

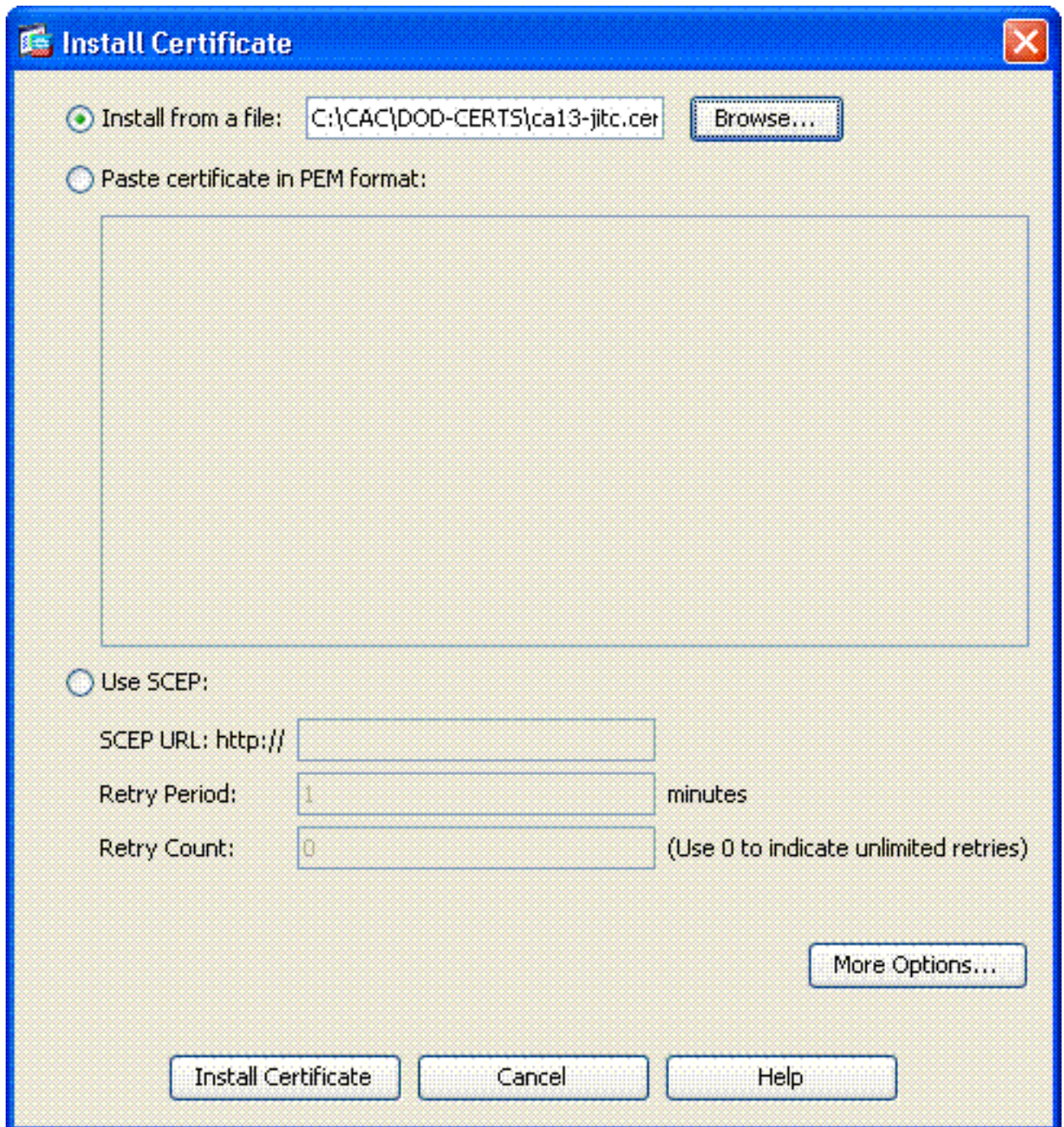


4. Choose size of the key.
5. Keep Usage to **General Purpose**.
6. Click **Generate Now**. **Note:** DoD Root CA 2 uses a 2048 bit key. A second key that uses a 2048 bit key pair should be generated to be able to use this CA. Complete the previous above steps in order to add a second key.

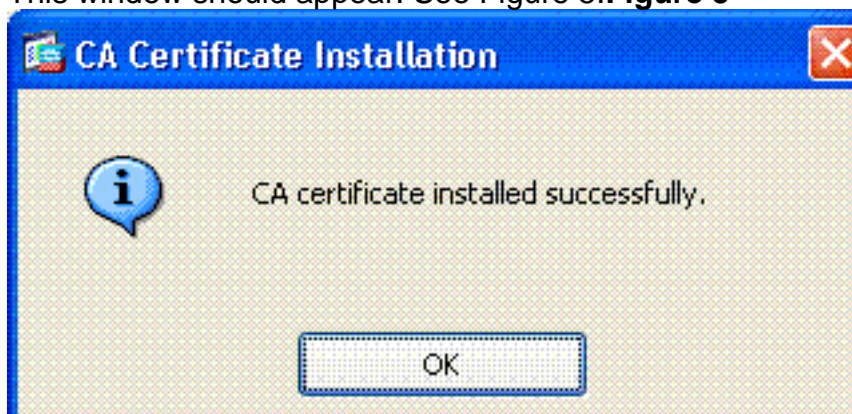
Install Root CA Certificates

Complete these steps:

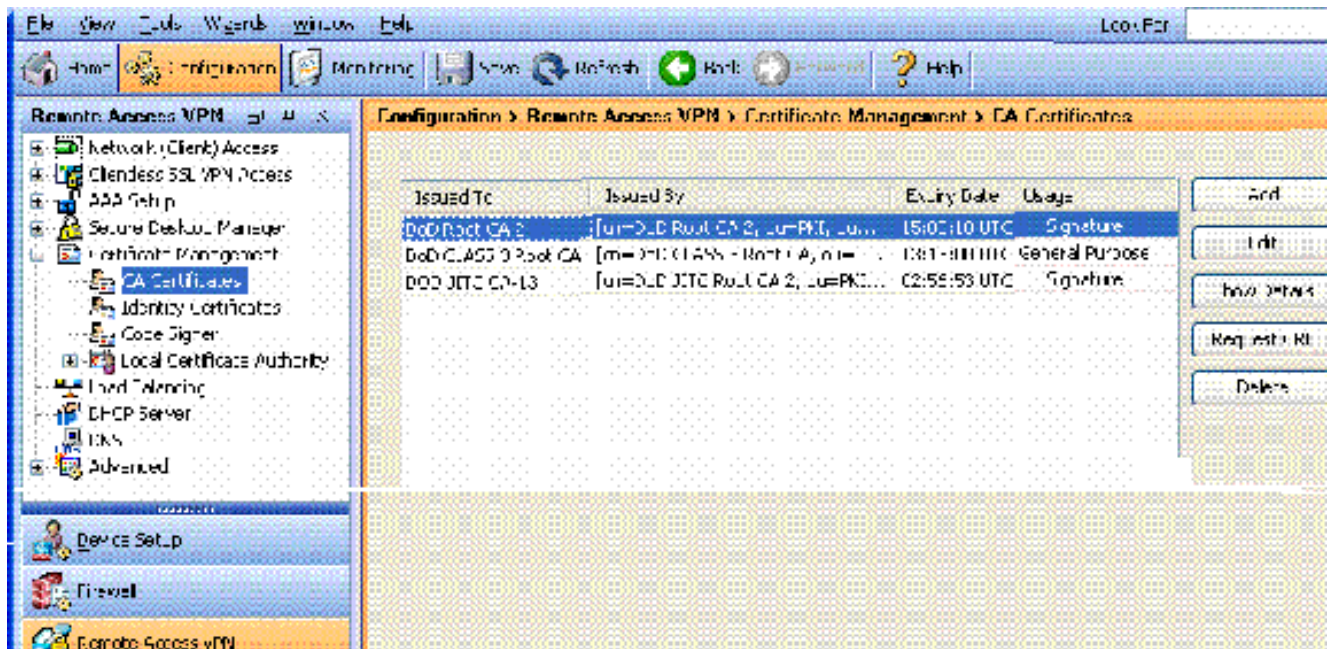
1. Choose **Remote Access VPN > Certificate Management > CA Certificate > Add**.
2. Choose **Install from File** and browse to the certificate.
3. Choose **Install Certificate**. **Figure 4: Installing Root Certificate**



4. This window should appear. See Figure 5. **Figure 5**

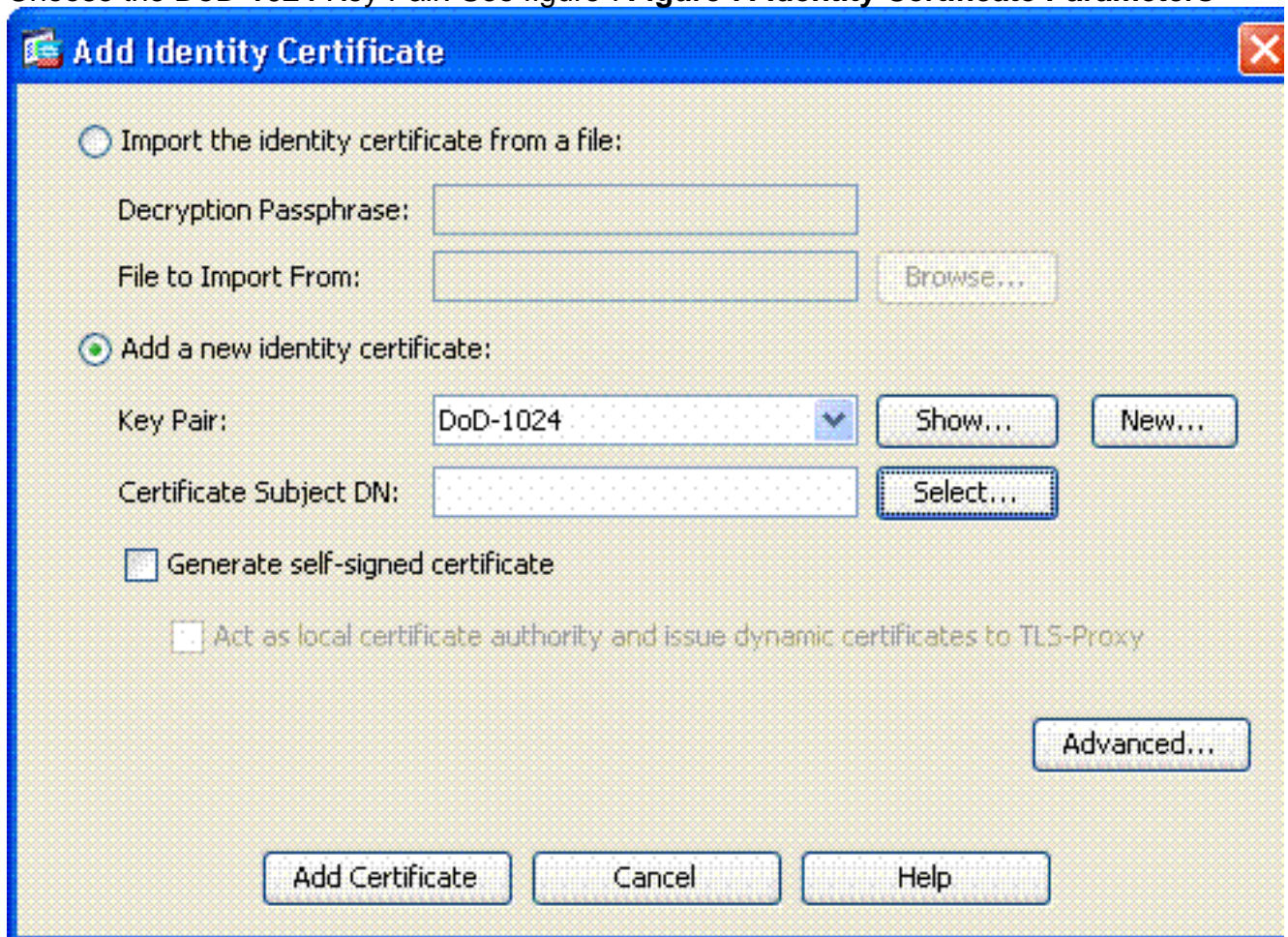


Note: Repeat steps 1 through 3 for every certificate that you want to install. DoD PKI requires a certificate for each of these: Root CA 2, Class 3 Root, CA## Intermediate, ASA ID and OCSP Server. The OCSP certificate is not needed if you do not use OCSP. **Figure 6: Installing Root Certificate**

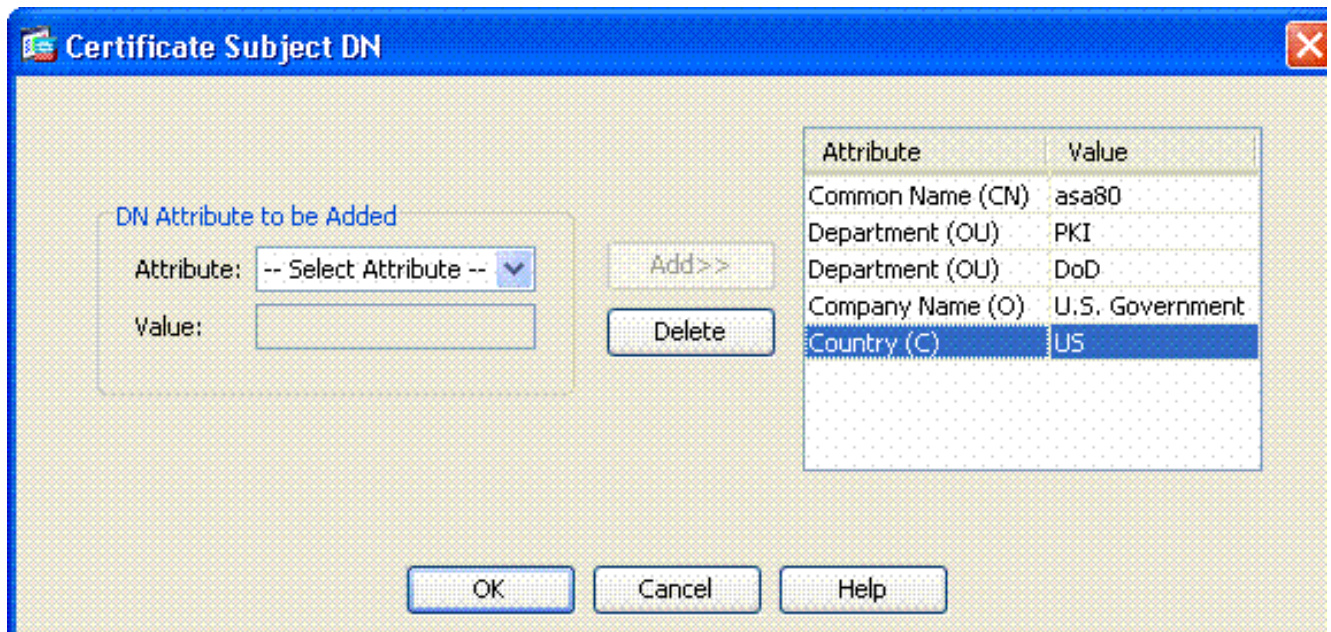


Enroll ASA and Install Identity Certificate

1. Choose **Remote Access VPN > Certificate Management > Identity Certificate > Add**.
2. Choose **Add a new id certificate**.
3. Choose the **DoD-1024** Key Pair. See figure 7 **Figure 7: Identity Certificate Parameters**

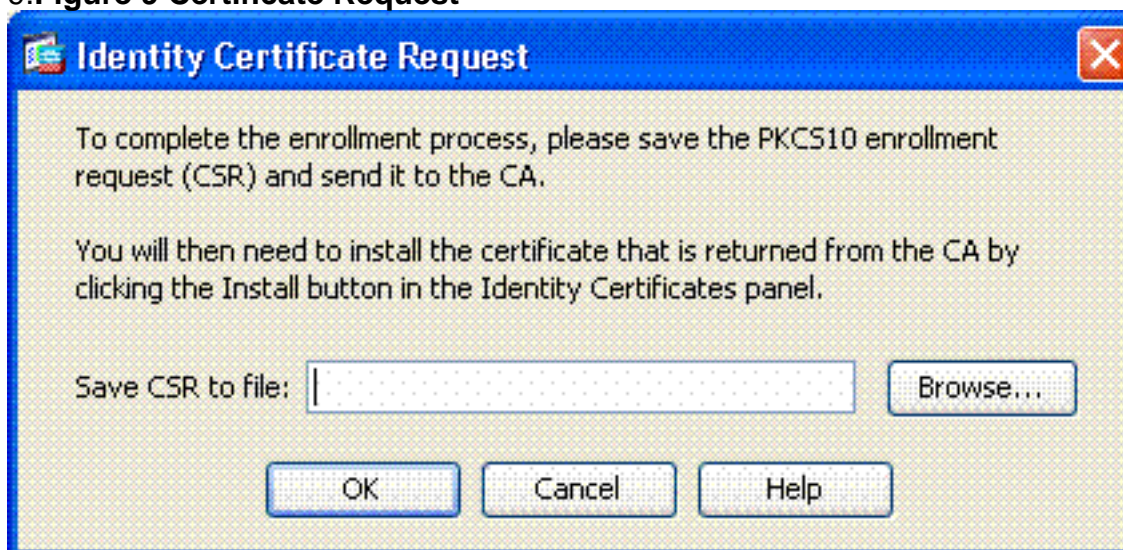


4. Go to the Certificate subject DN box and click **Select**.
5. In the Certificate Subject DN window, enter the information of the device. See Figure 8 for example. **Figure 8: Edit DN**



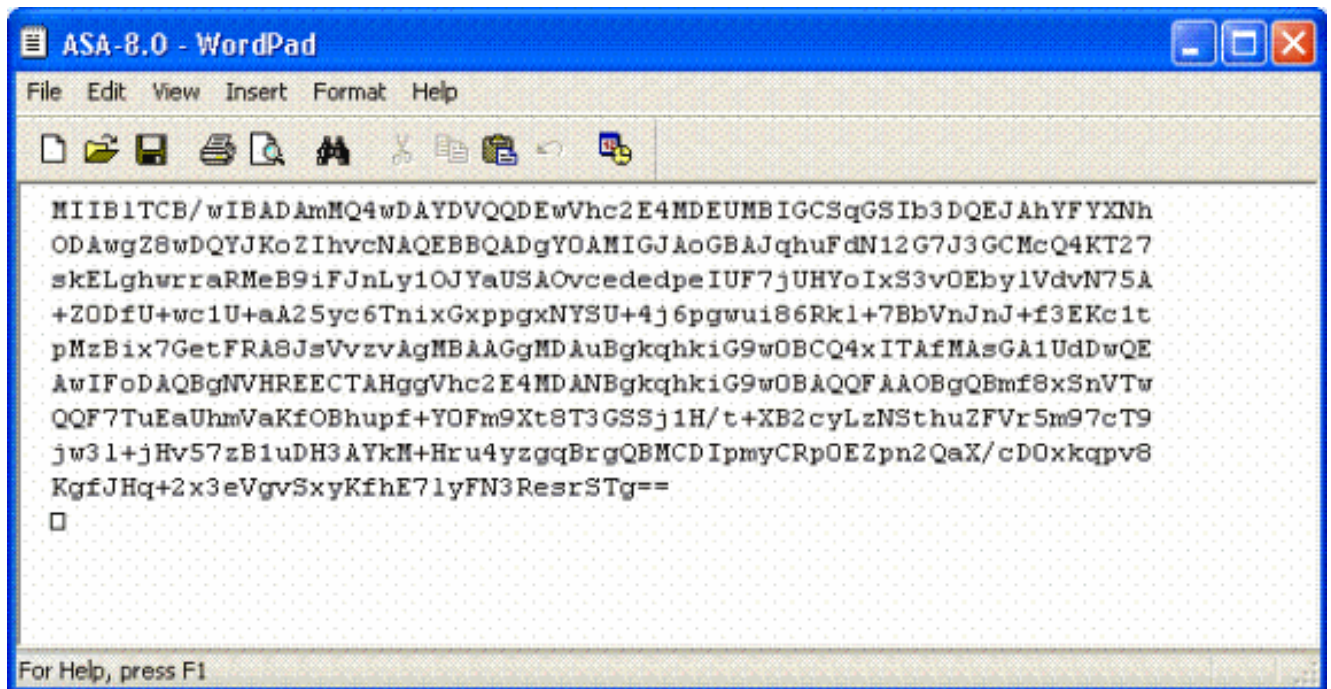
6. Choose **OK**. **Note:** Make sure that you use the hostname of the device that is configured in your system when you add the subject DN. The PKI POC can tell you the mandatory fields required.
7. Choose **Add certificate**.
8. Click **Browse** in order to select the directory where you want to save the request. See Figure 9.

Figure 9 Certificate Request

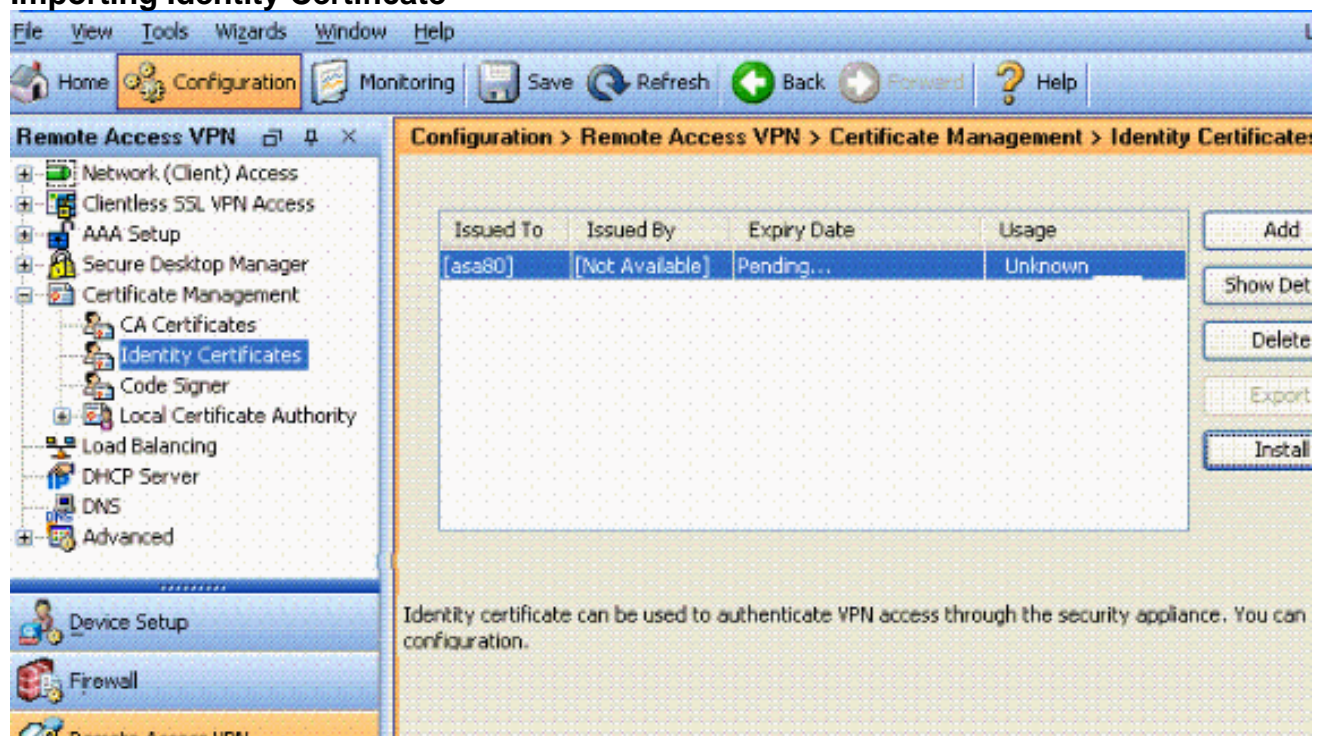


9. Open the file with WordPad, copy the request to the appropriate documentation and send to your PKI POC. See Figure 10.

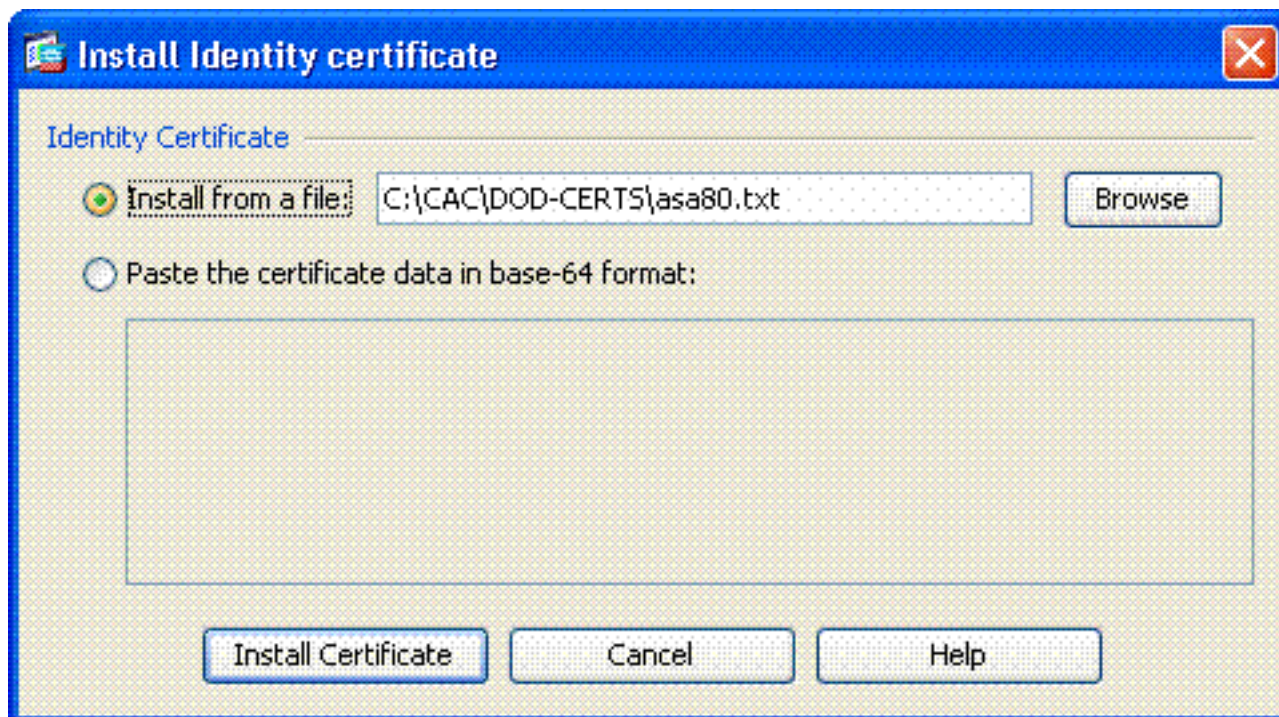
Figure 10: Enrollment Request



10. Once you have received the certificate from the CA administrator, choose **Remote Access VPN > Certificate Management > ID Certificate > Install**. See Figure 11. **Figure 11: Importing Identity Certificate**



11. In the Install certificate window, browse to the ID cert and choose **Install Certificate**. See Figure 12 for example. **Figure 12: Installing Identity Certificate**



Note: It is recommended to export the ID certificate trustpoint in order to save the issued certificate and key pairs. This allows the ASA administrator to import the certificate and key pairs to a new ASA in case of RMA or hardware failure. Refer to [Exporting and Importing Trustpoints](#) for more information. **Note:** Click **SAVE** in order to save the configuration in flash memory.

[AnyConnect VPN Configuration](#)

There are two options in order to configure the VPN parameters in ASDM. The first option is to use the SSL VPN wizard. This is an easy tool to use for users that are new to VPN configuration. The second option is to do it manually and to go through each option. This configuration guide uses the manual method.

Note: There are two methods to get the AC client to the user:

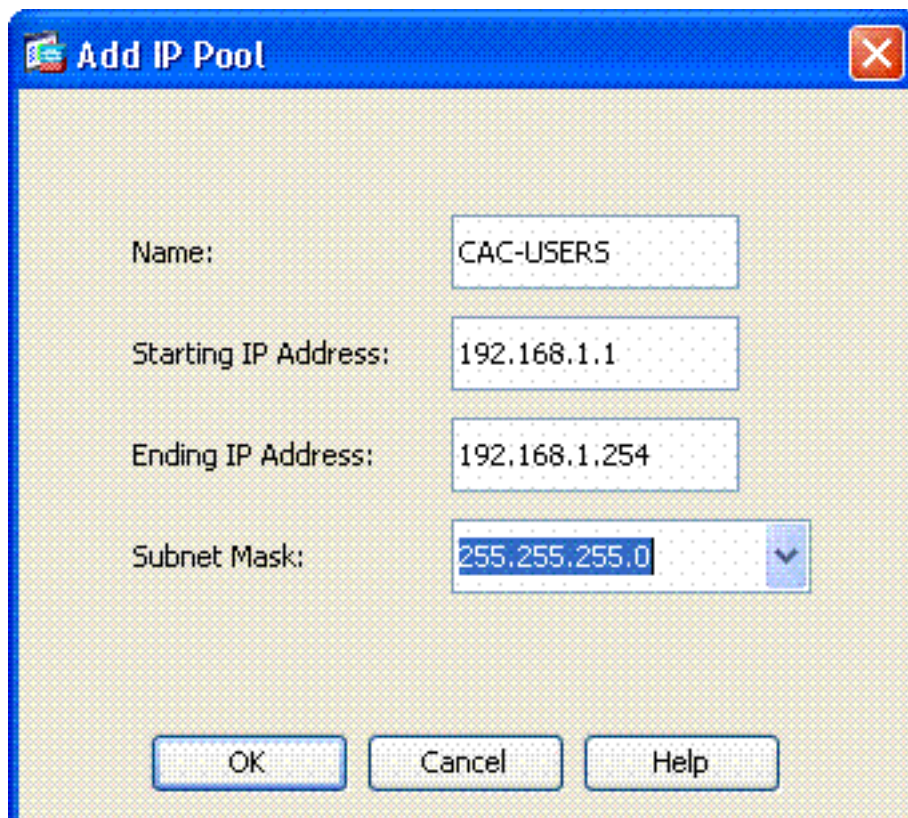
1. You can download the client from the Cisco website and install it on their machine.
2. The user can access the ASA via a web browser and the client can be downloaded.

Note: For example, <https://asa.test.com>. This guide uses the second method. Once the AC client is installed on the client machine permanently, you just launch the AC client from the application.

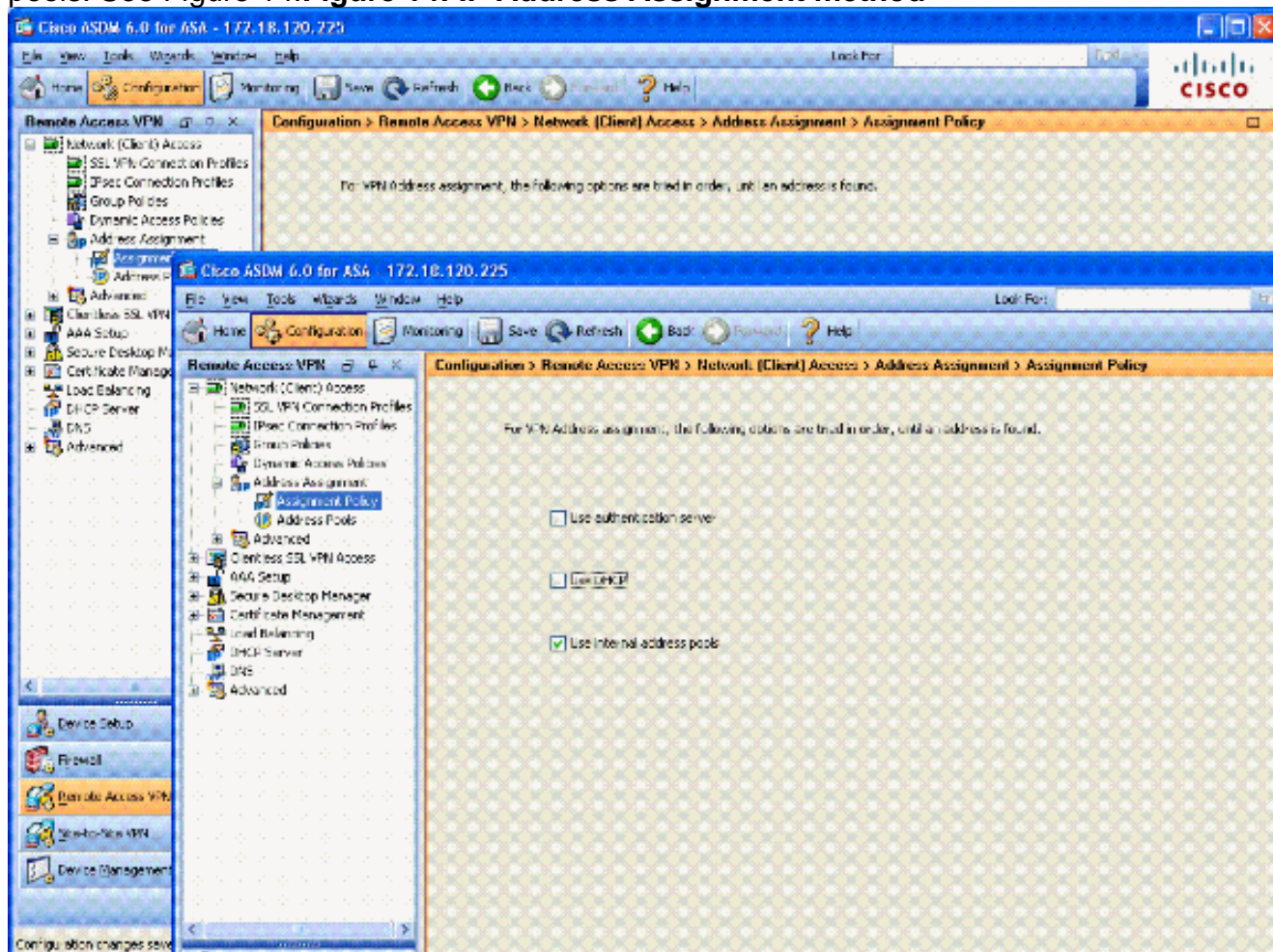
[Create an IP Address Pool](#)

This is optional if you use another method such as DHCP.

1. Choose **Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**.
2. Click **Add**.
3. In the Add IP Pool window, enter the name of the IP pool, starting and ending IP address and choose a subnet mask. See Figure 13. **Figure 13: Adding IP Pool**



4. Choose **Ok**.
5. Choose **Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**.
6. Select the appropriate IP address assignment method. This guide uses the internal address pools. See Figure 14. **Figure 14: IP Address Assignment method**



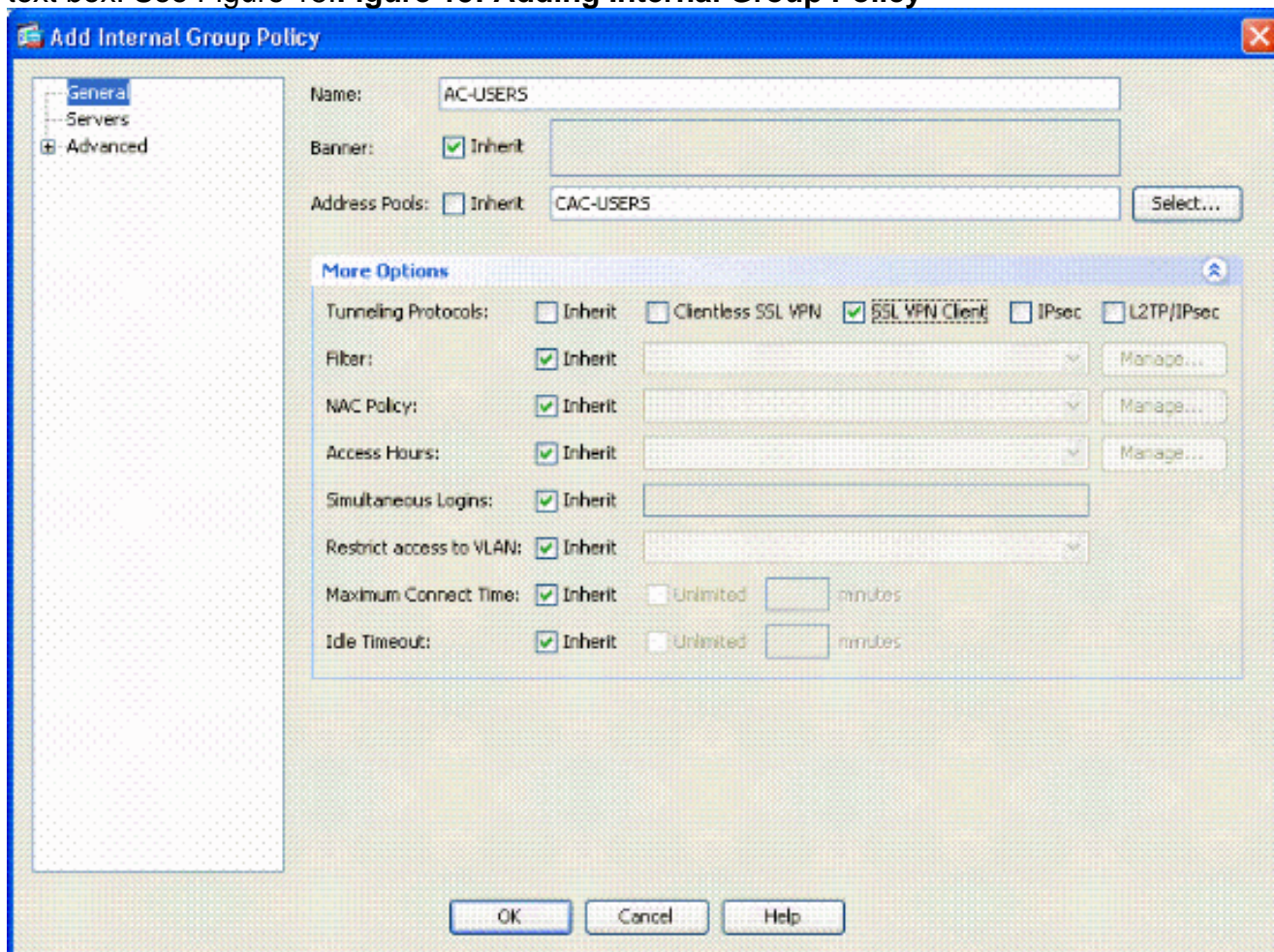
7. Click **Apply**.

Create Tunnel Group and Group Policy

Group Policy

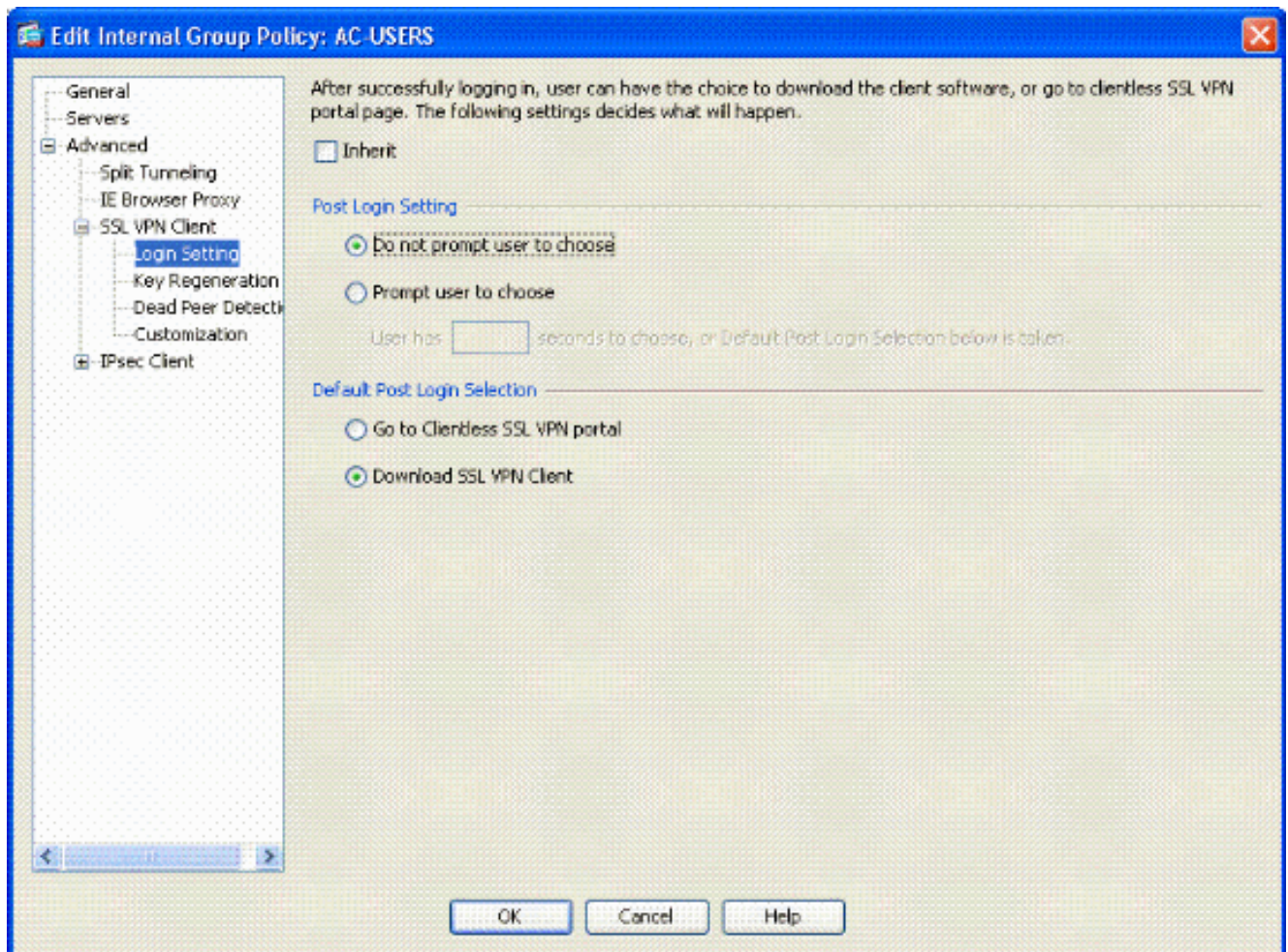
Note: If you do not want to create a new policy, you can use the default built in-group policy.

1. Choose **Remote Access VPN -> Network (Client) Access -> Group Policies**.
2. Click **Add** and choose **Internal Group Policy**.
3. In the Add Internal Group Policy window, enter the name for the Group Policy in the Name text box. See Figure 15. **Figure 15: Adding Internal Group Policy**



In the General tab, choose the **SSL VPN Client in the Tunneling Protocols** option, unless you use other protocols such as Clientless SSL. In the Servers section, uncheck the **inherit** check box and enter the IP address of DNS and WINS servers. Enter DHCP scope if applicable. In the Servers section, deselect the **inherit** check box in the Default Domain and enter the appropriate domain name. In the General tab, deselect the **inherit** check box in the address pool section and add the address pool created in the previous step. If you use another method of IP address assignment, leave this to inherit and make the appropriate change. All other configuration tabs are left to default settings. **Note:** There are two methods to get the AC client to the end users. One method is to go to Cisco.com and download the AC client. The second method is to have the ASA download the client to the user when the user tries to connect. This example shows the latter method.

4. Next, choose **Advanced > SSL VPN Client > Login Settings**. See Figure 16. **Figure 16: Adding Internal Group Policy**

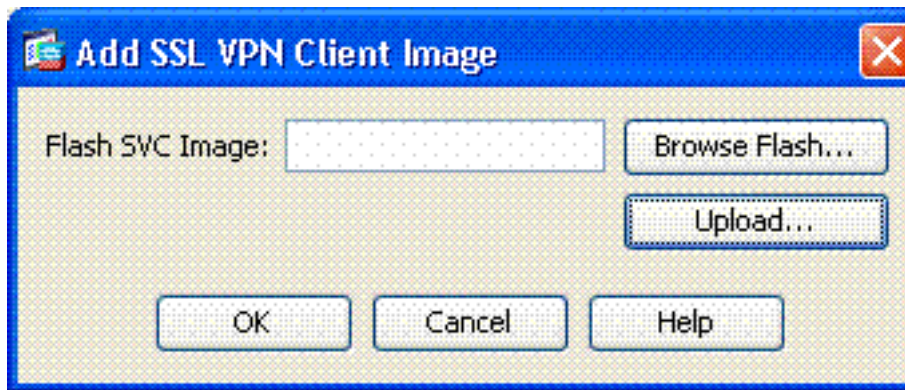


Deselect the **Inherit** checkbox. Choose the appropriate Post Login Setting that fits your environment. Choose the appropriate Default Post Login Selection that fits your environment. Choose **OK**.

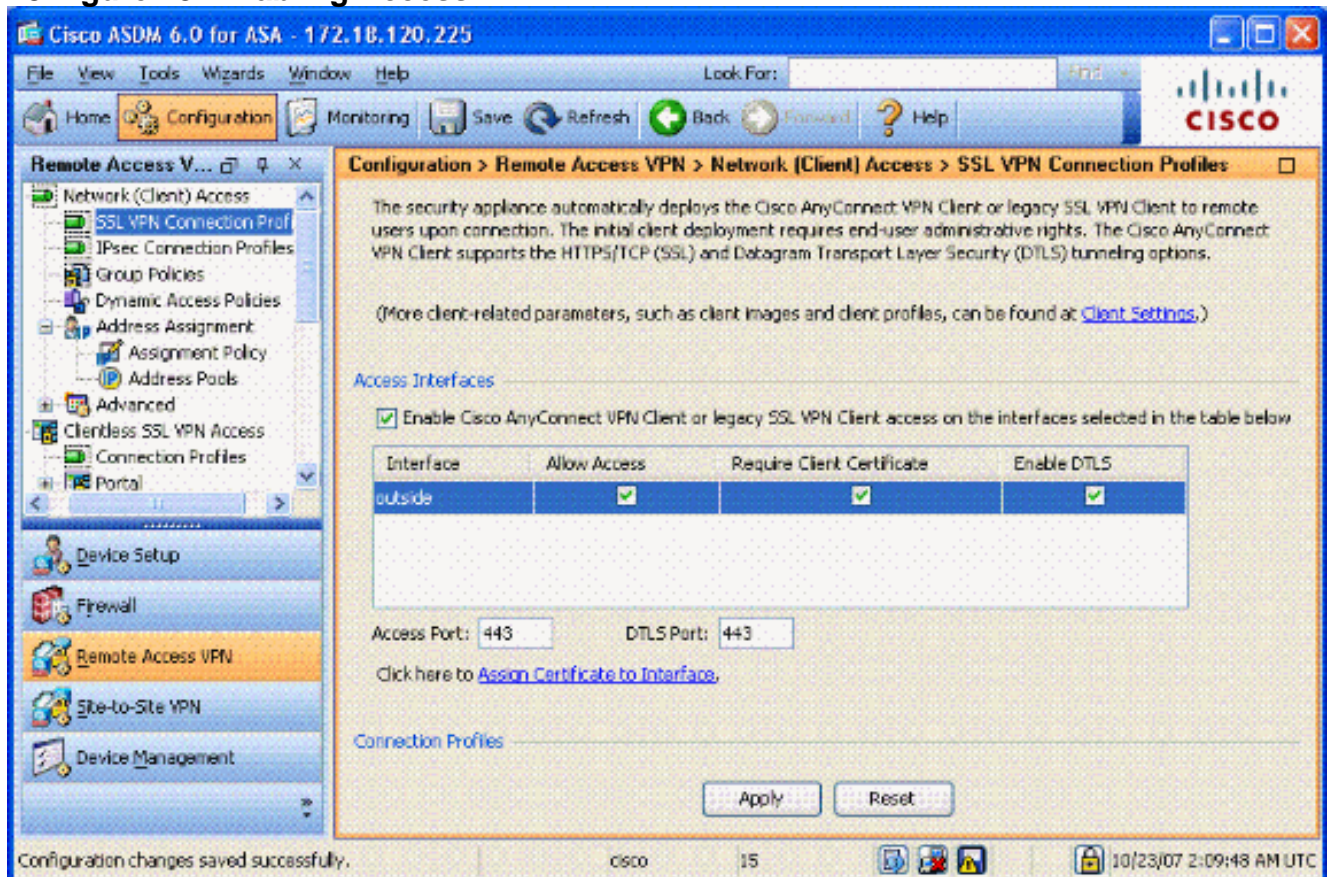
[Tunnel Group Interface and Image Settings](#)

Note: If you do not want to create a new group, you can use the default built-in group.

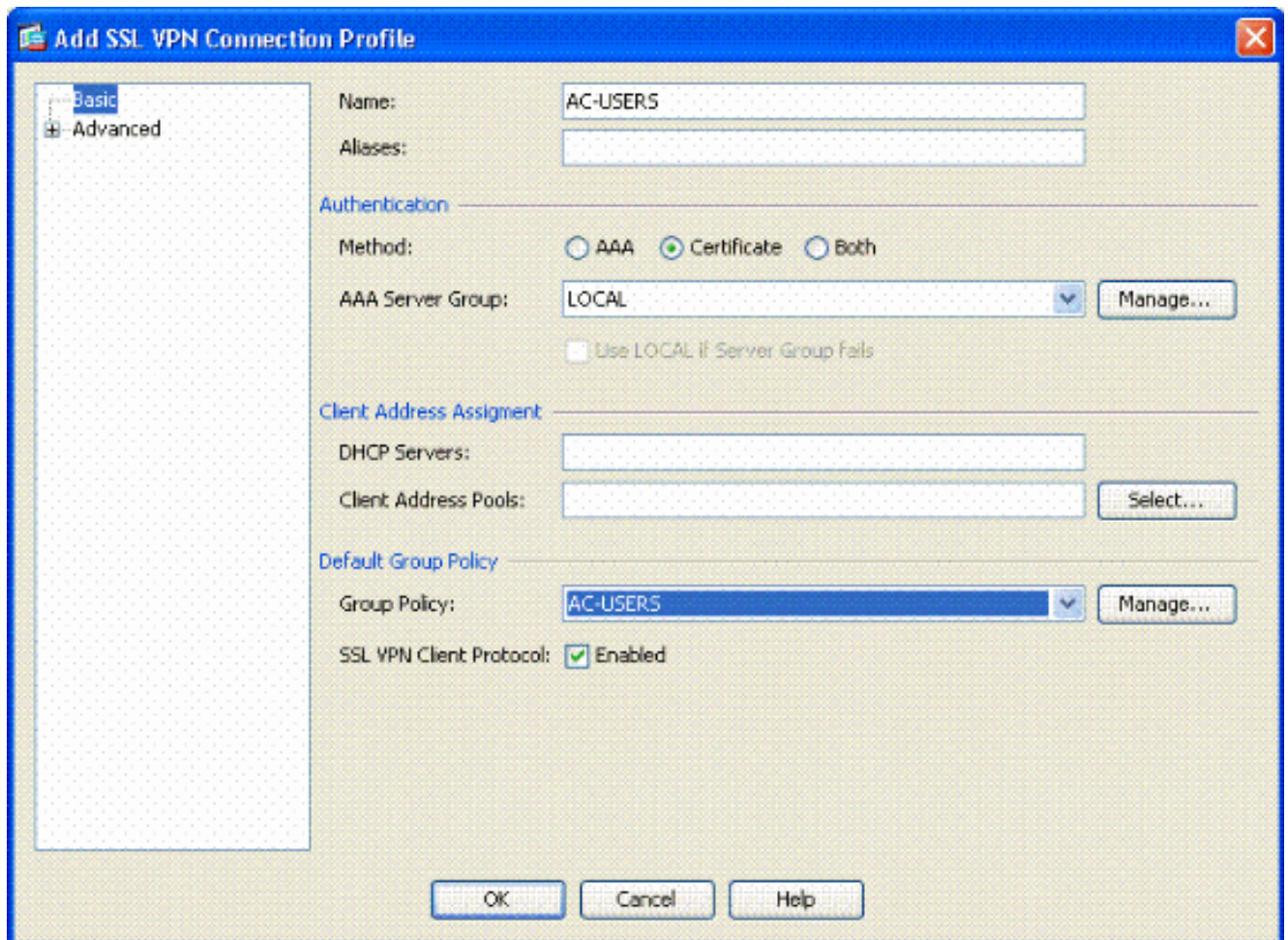
1. Choose **Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile**.
2. Choose **Enable Cisco AnyConnect Client.....**
3. A dialog box appears with the question *Would you like to designate an SVC image?*
4. Choose **Yes**.
5. If there is already an image, choose the image to use with Browse Flash. If the image is not available, choose **Upload** and browse for the file on the local computer. See Figure 17. The files can be downloaded from Cisco.com; there is a Windows, MAC and Linux file. **Figure 17: Add SSL VPN Client Image**



6. Next enable **Allow Access**, **Require Client Cert** and optionally **Enable DTLS**. See Figure 18. **Figure 18: Enabling Access**

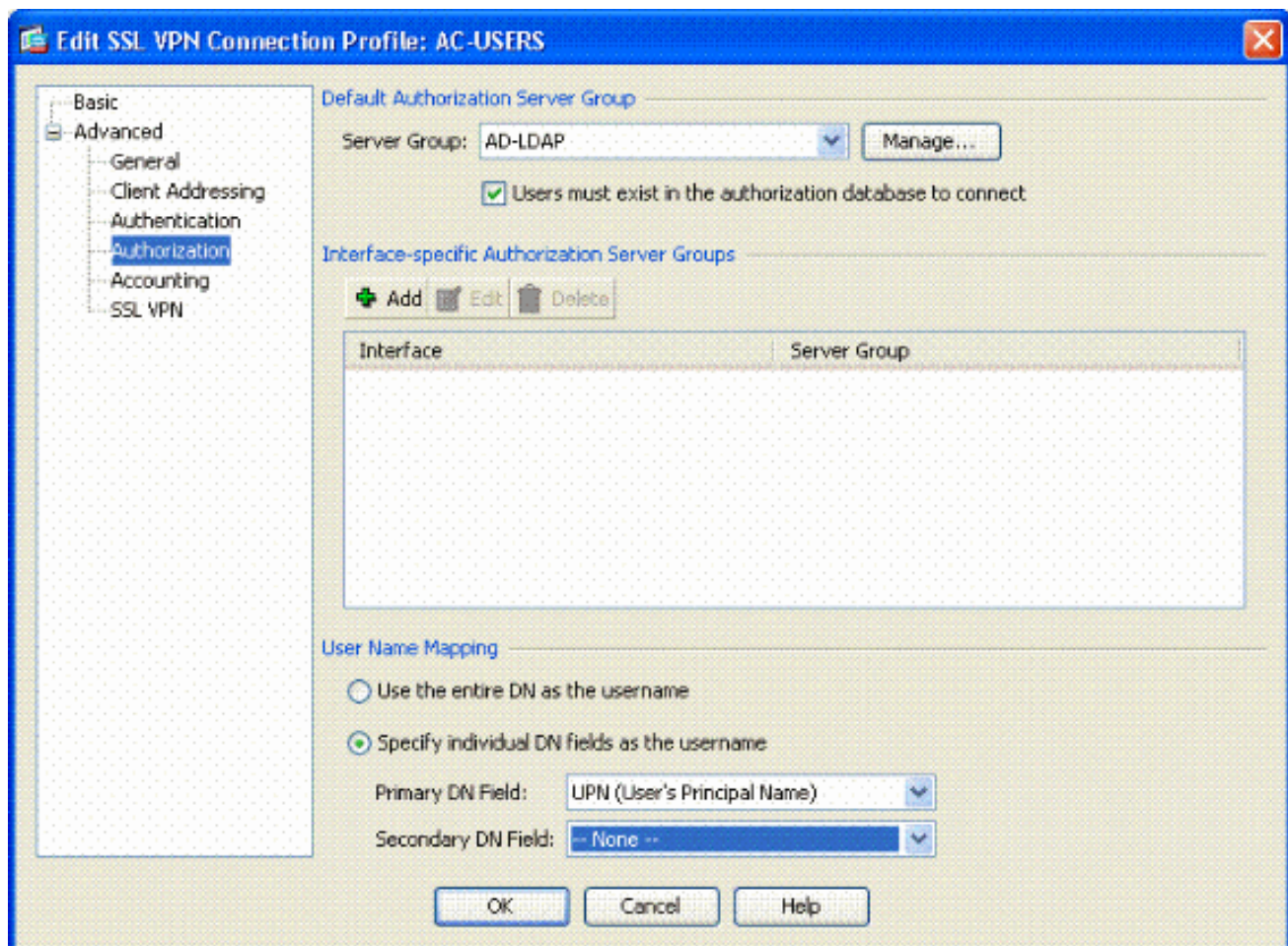


7. Click **Apply**.
8. Next, create a Connection Profile/Tunnel Group. Choose **Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile**.
9. In the Connection Profiles section, click **Add**. **Figure 19: Adding Connection Profile**



Name the group. Choose **Certificate** in the authentication method. Choose the group policy created previously. Ensure that **SSL VPN Client** is enabled. Leave other options as default.

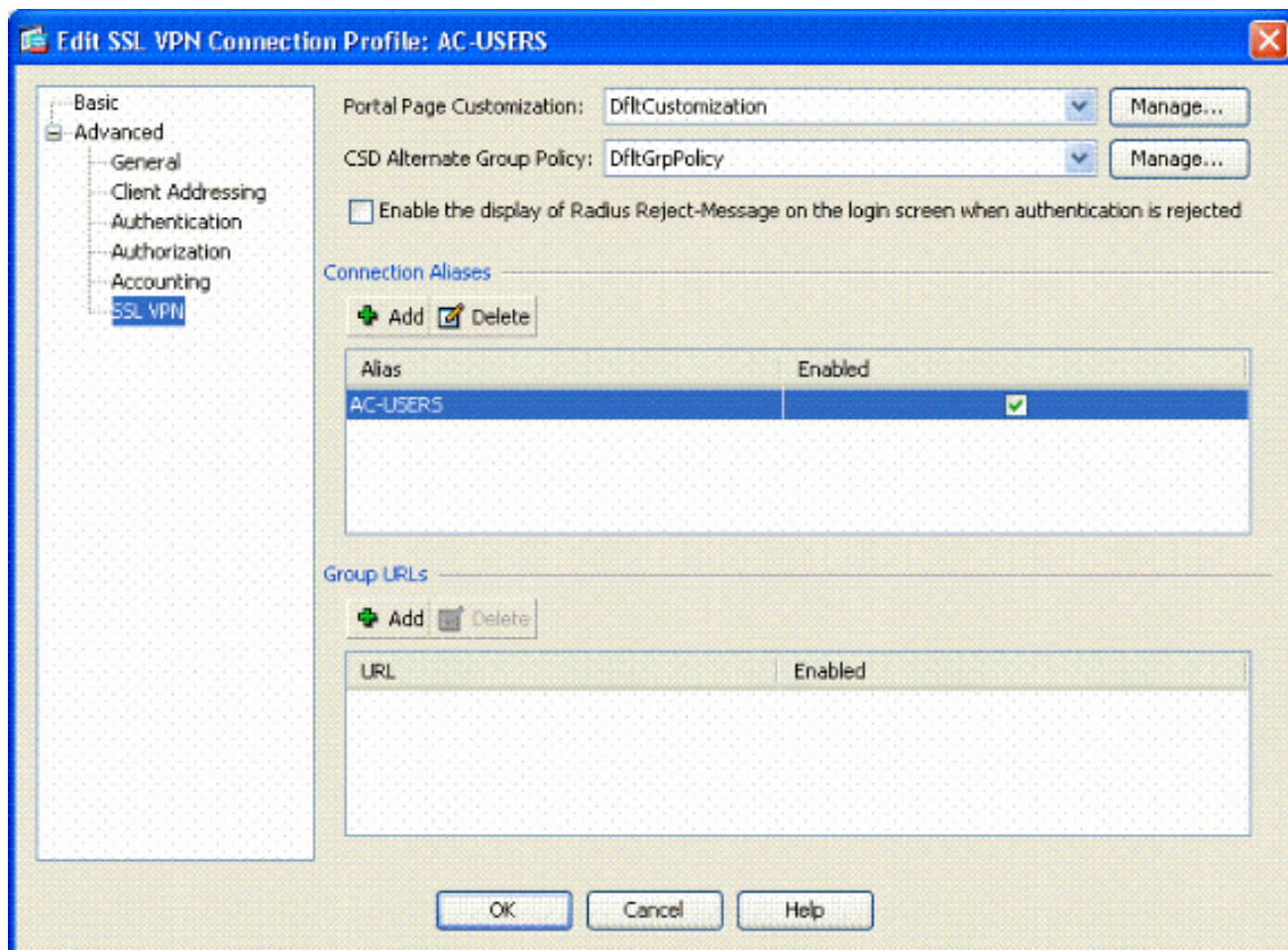
10. Next, choose **Advanced > Authorization**. See Figure 20 **Figure 20: Authorization**



Choose the AD-LDAP group previously created. Check **Users must exist...to connect**. In the mapping fields, choose **UPN** for the primary and **none** for secondary.

11. Choose the **SSL VPN** section of the menu.

12. In the Connection Aliases section, complete these steps:**Figure 21: Connection Aliases**



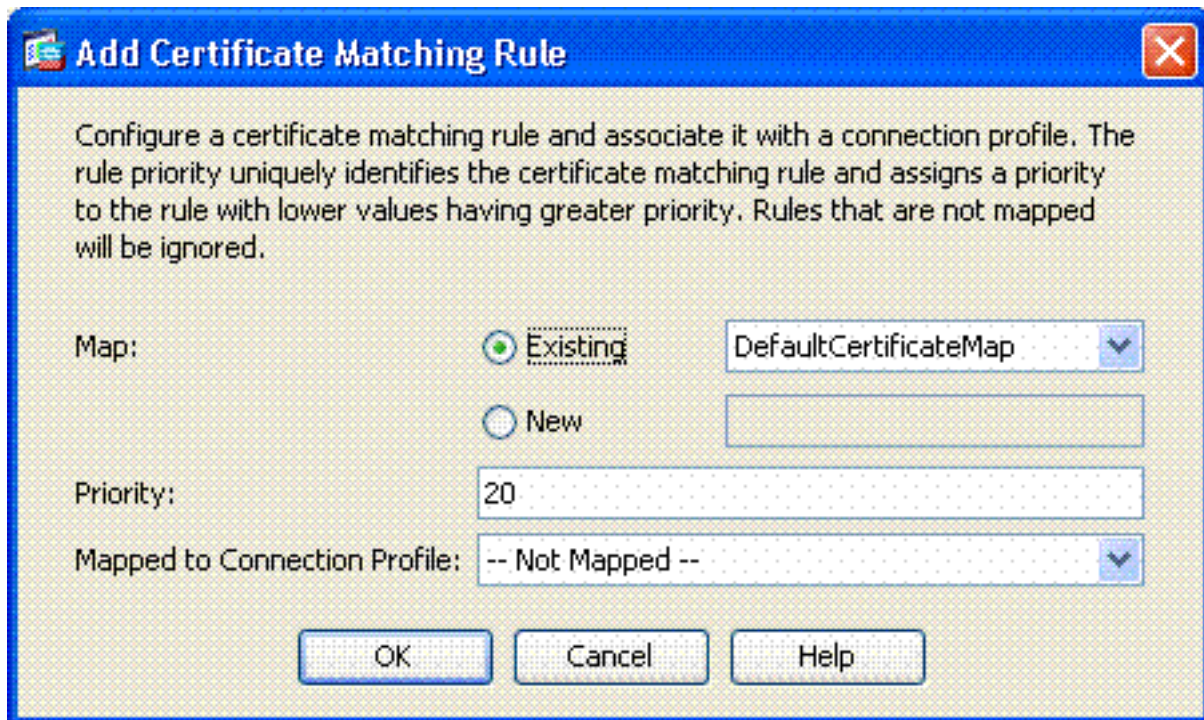
Choose **Add**. Enter the group alias you want to use. Ensure that **Enabled** is checked. See Figure 21.

13. Click **OK**.

Note: Click **Save** in order to save the configuration in flash memory.

Certificate Matching Rules (If OCSP will be used)

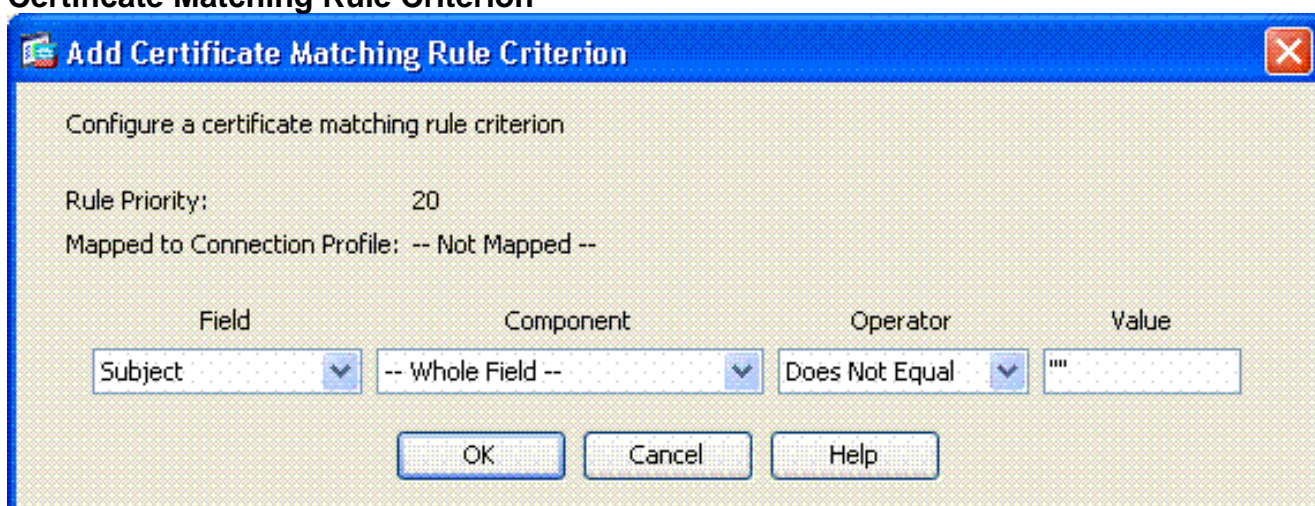
1. Choose **Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps**. See Figure 22. Choose **Add** in the Certificate to Connection Profile Maps section. You can keep the existing map as DefaultCertificateMap in the map section or create a new one if you already use cert maps for IPsec. Keep the rule priority. Under mapped group, leave as -- **Not Mapped** --. See Figure 22. **Figure 22: Adding Certificate Matching Rule**



Click

OK.

2. Click **Add** on the bottom table.
3. In the Add certificate Matching Rule Criterion window, complete these steps:**Figure 23: Certificate Matching Rule Criterion**



Keep the Field column to **Subject**. Keep the Component column to **Whole Field**. Change the Operator column to **Does Not Equal**. In the Value column, enter two double quotes "". Click **Ok** and **Apply**. See Figure 23 for example.

[Configure OCSP](#)

The configuration of an OCSP can vary and depends upon the OCSP responder vendor. Read the manual of the vender for more information.

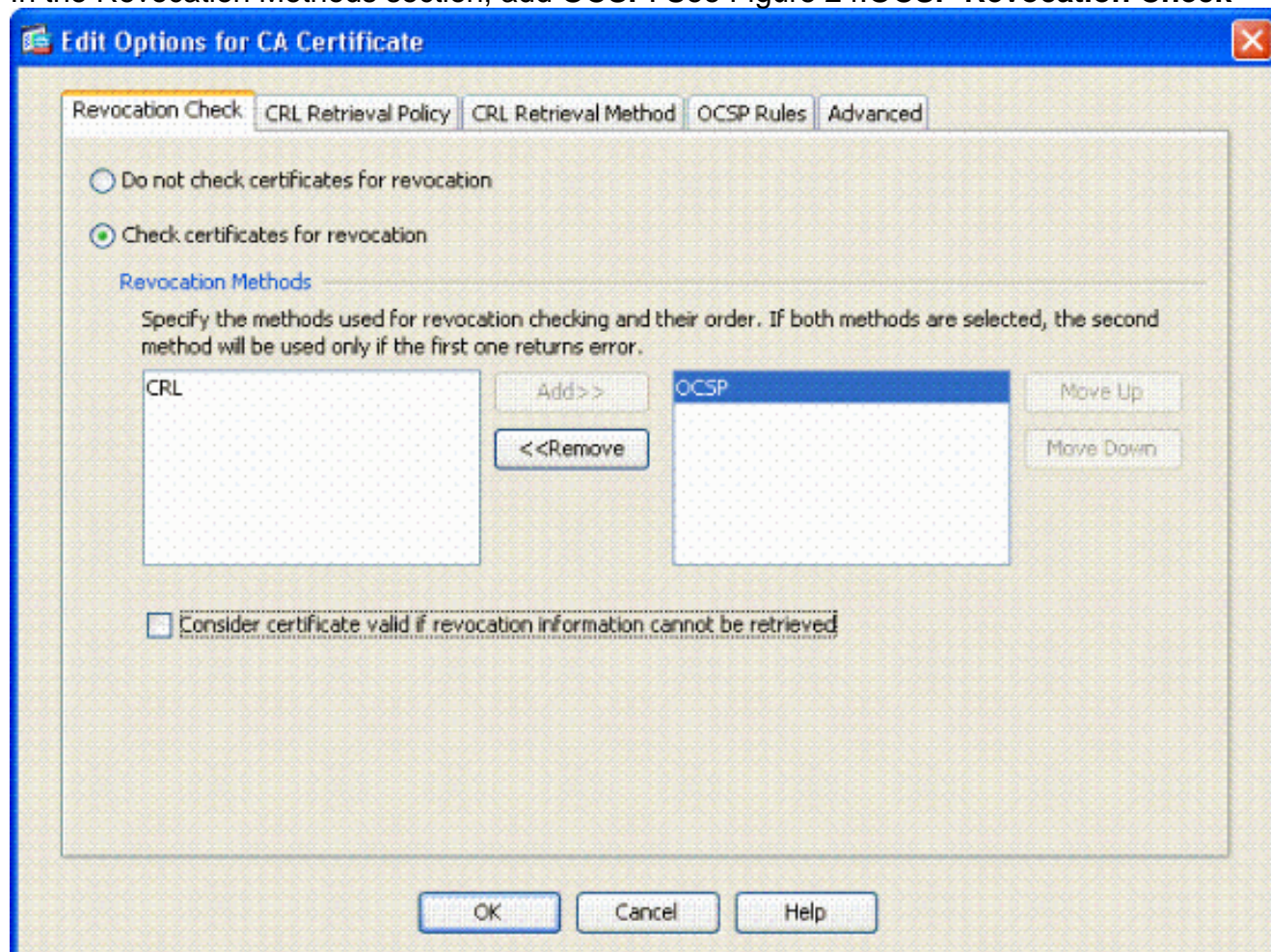
[Configure OCSP Responder Certificate](#)

1. Obtain a self-generated certificate from the OCSP responder.
2. Complete the procedures mentioned previously and install a certificate for the OSCSP server.**Note:** Make sure that **Do not check certificates for revocation** is selected for the

OCSP certificate trustpoint.

Configure CA to use OCSP

1. Choose **Remote Access VPN> Certificate Management > CA Certificates**.
2. Highlight an OCSP in order to choose a CA to configure to use OCSP.
3. Click **Edit**.
4. Ensure that **Check certificate for revocation** is checked.
5. In the Revocation Methods section, add **OCSP**. See Figure 24. **OCSP Revocation Check**



6. Ensure **Consider Certificate valid...cannot be retrieved** is unchecked if you want to follow strict OCSP checking.

Note: Configure/Edit all the CA server that uses OCSP for revocation.

Configure OCSP Rules

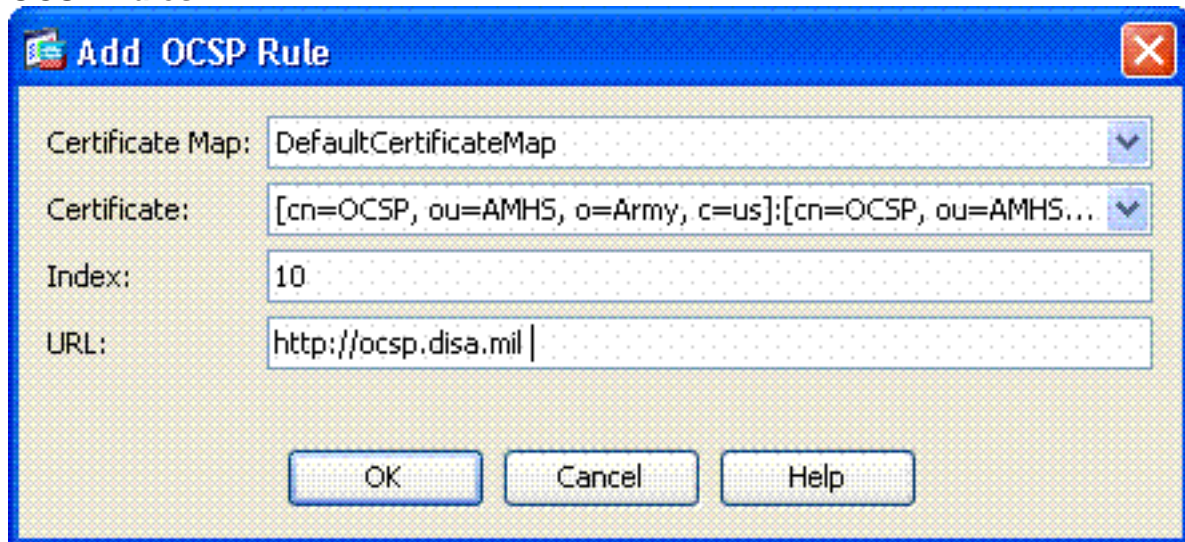
Note: Verify that a Certificate Group Matching Policy is created and the OCSP responder is configured before you complete these steps.

Note: In some OCSP implementations, a DNS A and PTR record can be needed for the ASA. This check is done in order to verify that the ASA is from a .mil site.

1. Choose **Remote Access VPN> Certificate Management > CA Certificates 2**.
2. Highlight an OCSP in order to choose a CA to configure to use OCSP.
3. Choose **Edit**.
4. Click the **OCSP Rule** tab.

5. Click **Add** .

6. In the Add OCSP Rule window, complete these steps. See Figure 25.**Figure 25: Adding OCSP Rules**



In the Certificate Map option, choose **DefaultCertificateMap** or a map created previously. In the Certificate option, choose **OCSP responder**. In the index option, enter **10**. In the URL option, enter the IP address or the hostname of the OCSP responder. If you use the hostname, make sure DNS server is configured on ASA. Click **Ok**. Click **Apply**.

[Cisco AnyConnect Client Configuration](#)

This section covers the configuration of the Cisco AnyConnect VPN client.

Assumptions—Cisco AnyConnect VPN Client and middleware application is already installed in the host PC. ActivCard Gold and ActivClient were tested.

Note: This guide uses the group-url method for initial AC client install only. Once the AC client is installed, you launch the AC application just like the IPsec client.

Note: The DoD certificate chain needs to be installed on the local machine. Check with the PKI POC in order to obtain the certificates/batch file.

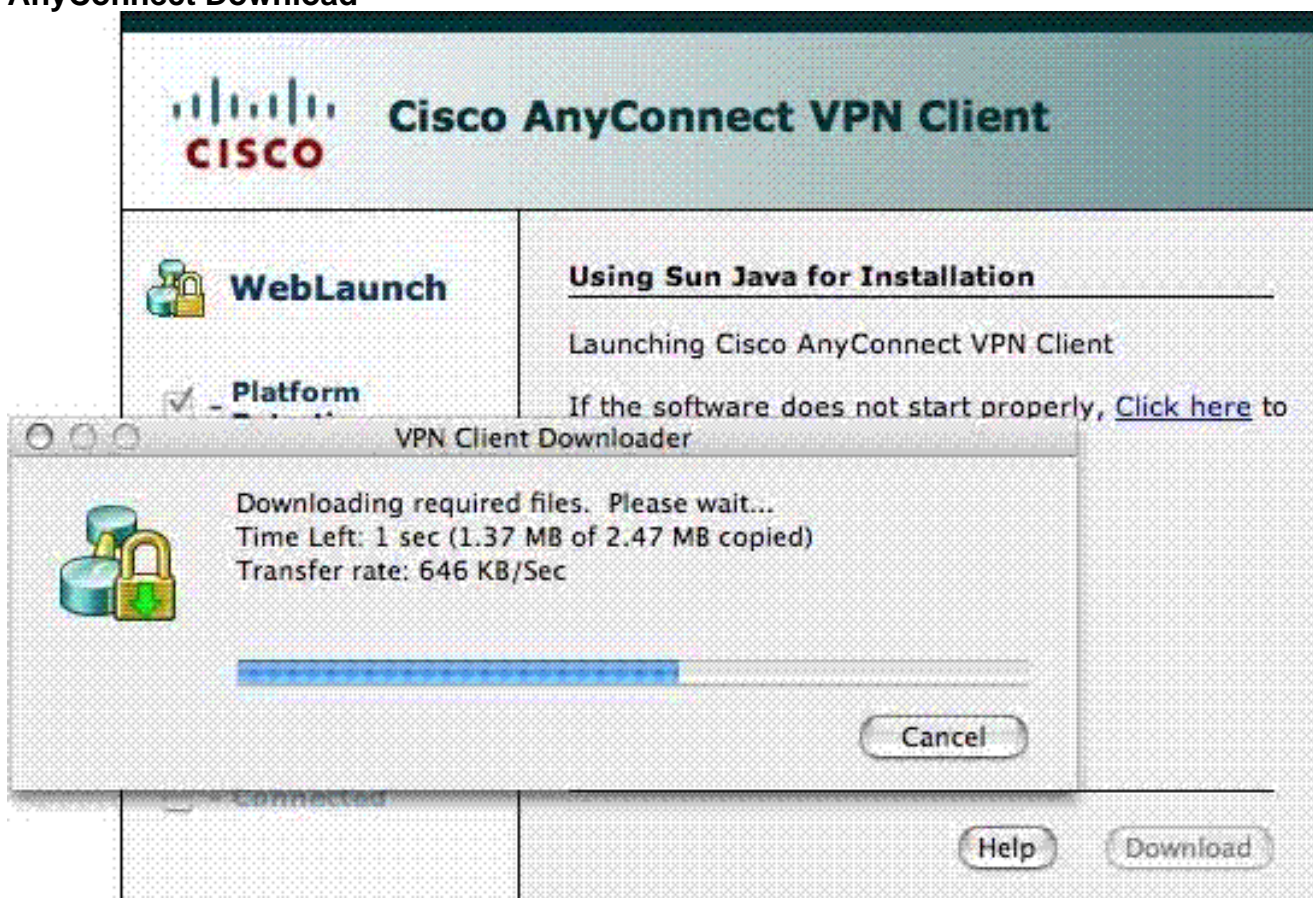
Note: The card reader driver for MAC OSX is already installed and compatible with the current OS version that you use.

[Downloading Cisco Anyconnect VPN Client – Mac OS X](#)

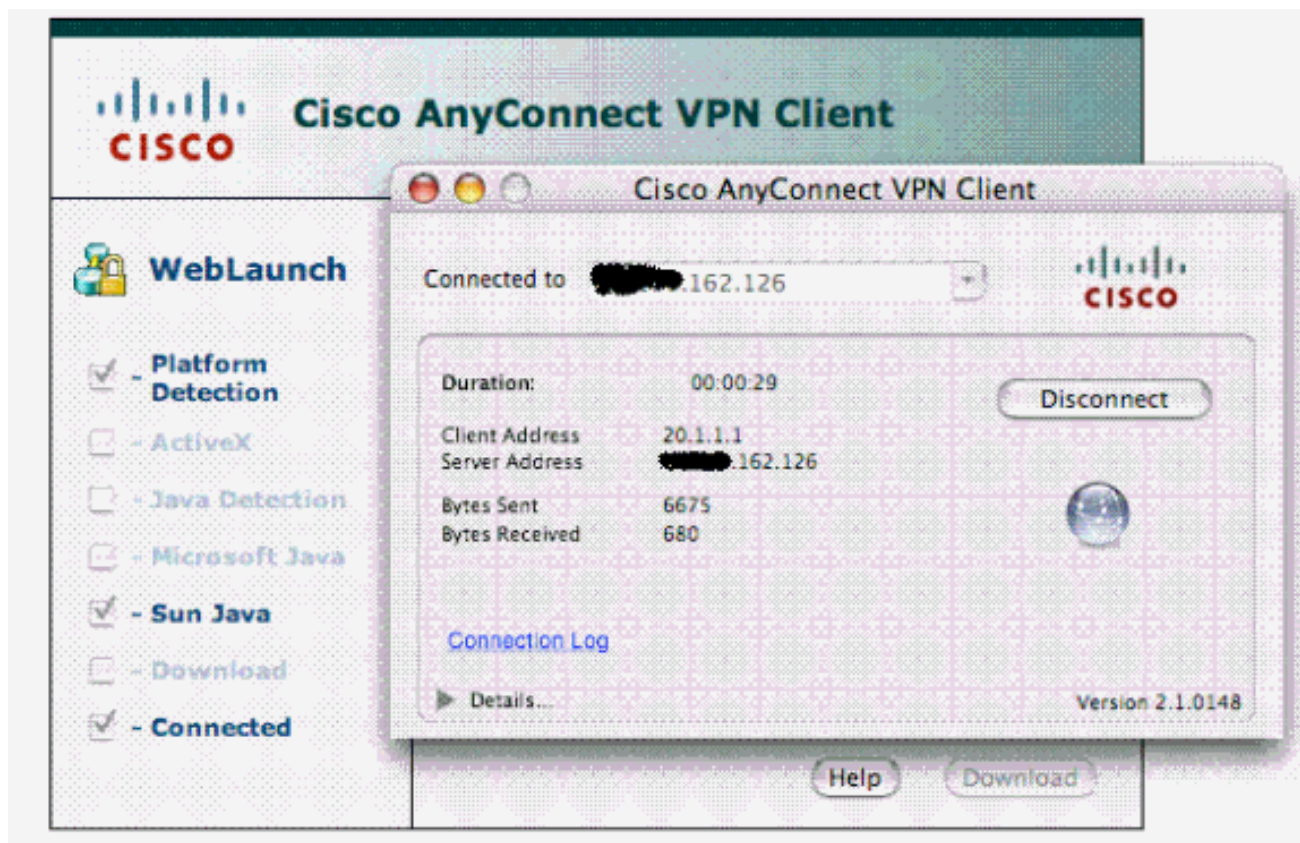
1. Launch a web session to the ASA through Safari. The address should be in the format of `https://Outside-Interface`. For example, `https://172.18.120.225`.
2. A popup window asks to verify the certificate of the ASA. Click **Continue**.
3. Another popup window appears in order to unlock the CAC keychain. Enter your pin number. See Figure 31.**Figure 31: Enter PIN**



4. After the SSL VPN-service web page appears, click **Continue**.
5. After you unlock the keychain, the browser prompts you if you trust the certificate from the ASA. Click **trust**.
6. Enter the root password in order to unlock keychain to establish secure connection, and then click **Ok**.
7. Choose the certificate to use for client authentication, and then click **Ok**.
8. The browser then asks for the root/user password in order to allow for downloading of AnyConnect clients.
9. If authenticated, the AnyConnect client starts to download. See Figure 32. **Figure 32: AnyConnect Download**



10. After the application is downloaded, the browser prompts you to accept the ASA certificate. Click **Accept**.
11. Connection is established. Figure 33. **Figure 33: AnyConnect Connected**



[Start Cisco AnyConnect VPN Client – Mac OS X](#)

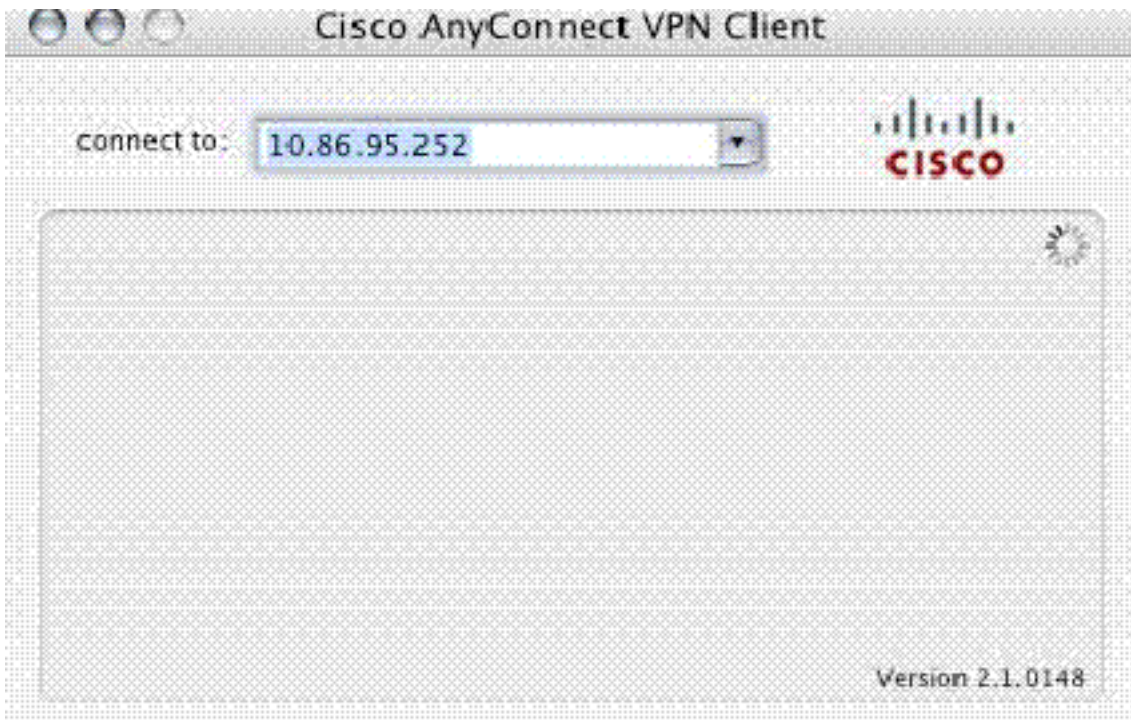
From Finder—**Applications > Cisco AnyConnect VPN Client**

Note: See Appendix E for Optional AnyConnect Client Profile Configuration.

[New Connection](#)

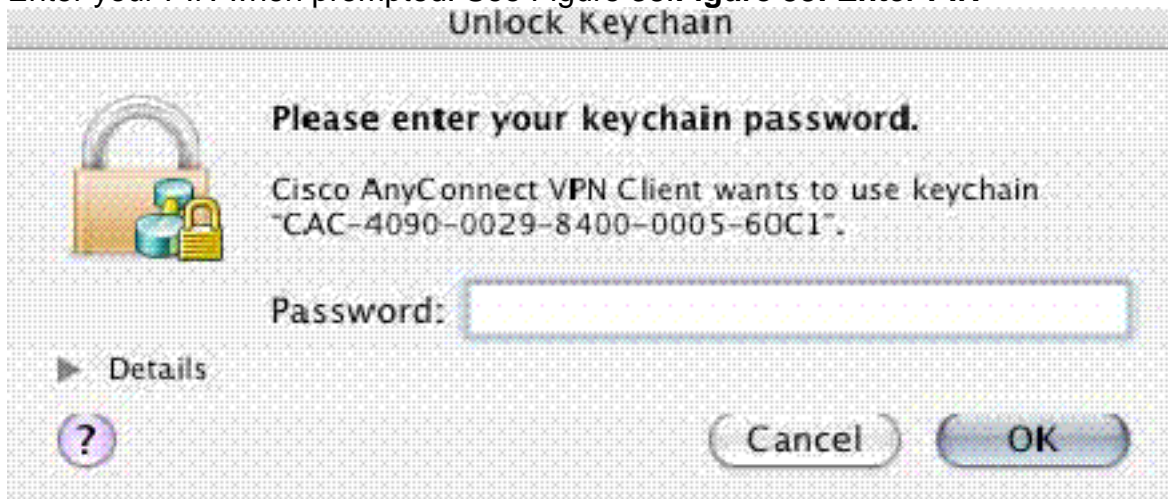
The AC window appears. See Figure 37.

Figure 37: New VPN Connection



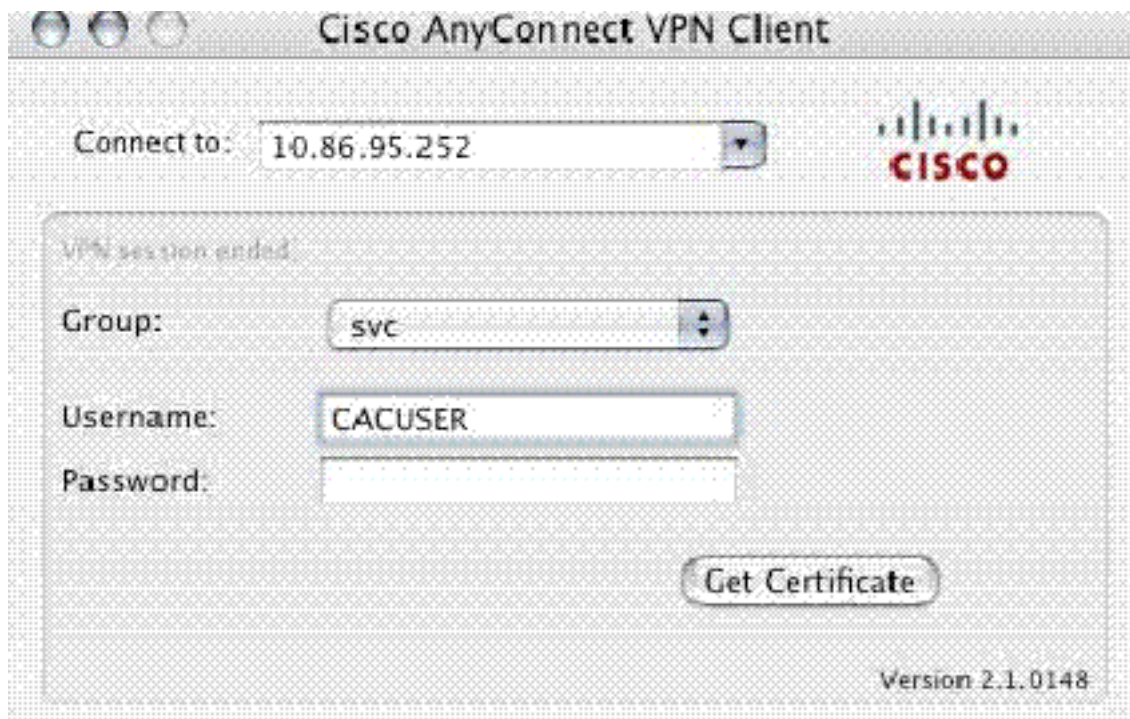
1. Choose the appropriate host if AC does not automatically try the connection.
2. Enter your PIN when prompted. See Figure 38.

Figure 38: Enter PIN
Unlock Keychain



[Start remote access](#)

1. Choose the group and host to which you want to connect.
2. Since certificates are used, choose **Connect** in order to establish the VPN. See Figure 39.**Note:** Since the connection uses certificates, there is no need to enter a username and password.**Figure 39: Connecting**



Note: See

Appendix E for Optional AnyConnect Client Profile Configuration.

[Appendix A – LDAP Mapping and DAP](#)

In ASA/PIX release 7.1(x) and later, a feature called LDAP mapping was introduced. This is a powerful feature that provides a mapping between a Cisco attribute and LDAP objects/attribute, which negates the need for LDAP schema change. For CAC authentication implementation, this can support additional policy enforcement on remote access connection. These are examples of LDAP mapping. Be aware that you need administrator rights in order to make changes in the AD/LDAP server. In ASA 8.x software, the Dynamic Access Policy (DAP) feature was introduced. DAP can work in conjunction with CAC to look at multiple AD groups as well as push policies, ACLs and so forth.

[Scenario 1: Active Directory Enforcement using Remote Access Permission Dial-in – Allow/Deny Access](#)

This example maps the AD attribute msNPAllowDailin to Cisco's attribute cVPN3000-Tunneling-Protocol.

- The AD attribute value: TRUE = Allow; FALSE = Deny
- Cisco attribute value: 1 = FALSE, 4 (IPSec) or 20 (4 IPSEC + 16 WebVPN) = TRUE,

For ALLOW condition, you map:

- TRUE = 20

For DENY dial-in condition, you map:

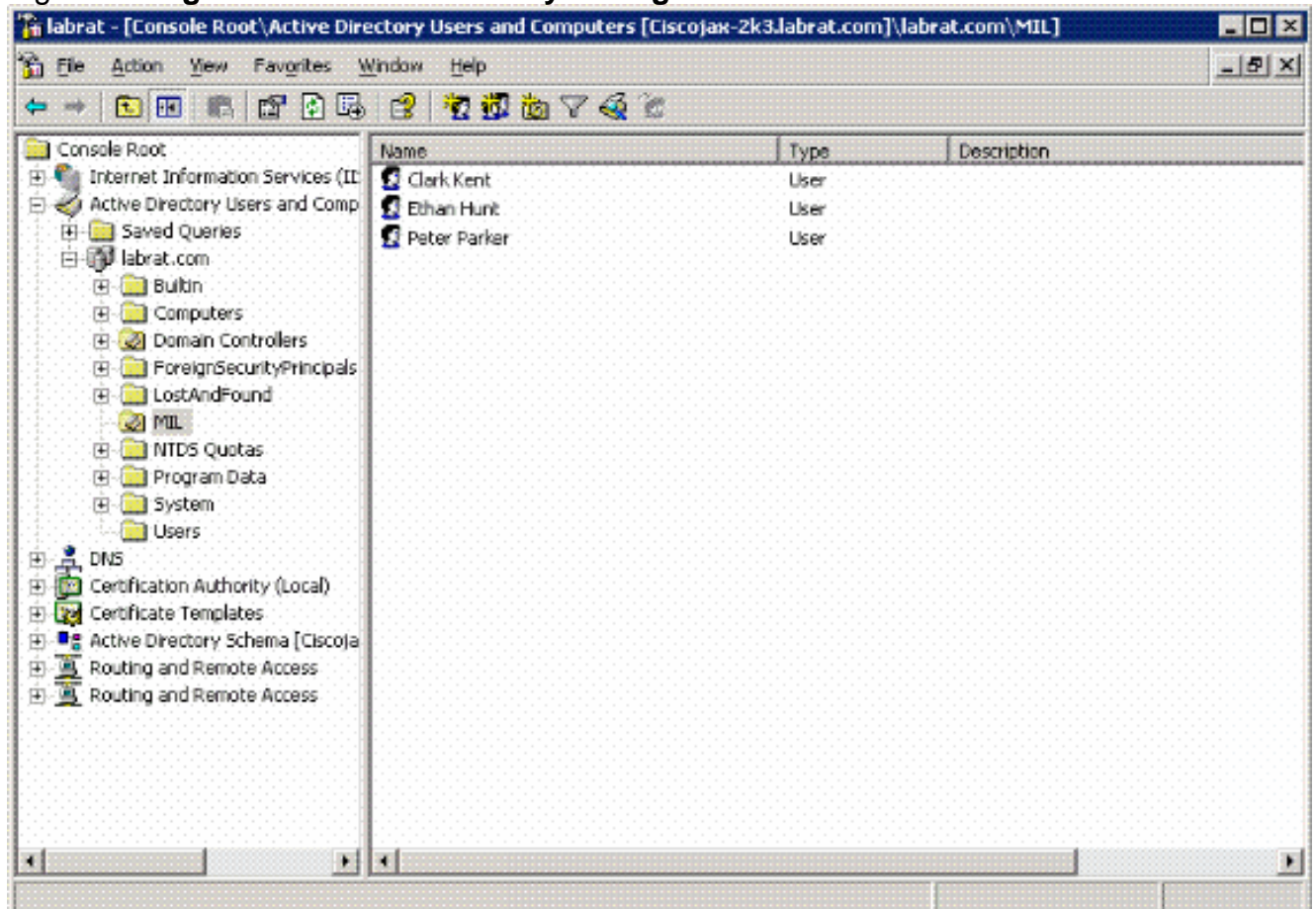
- FALSE = 1

Note: Make sure that TRUE and FALSE are in all caps. Refer to [Configuring an External Server for Security Appliance User Authorization](#) for more information.

[Active Directory Setup](#)

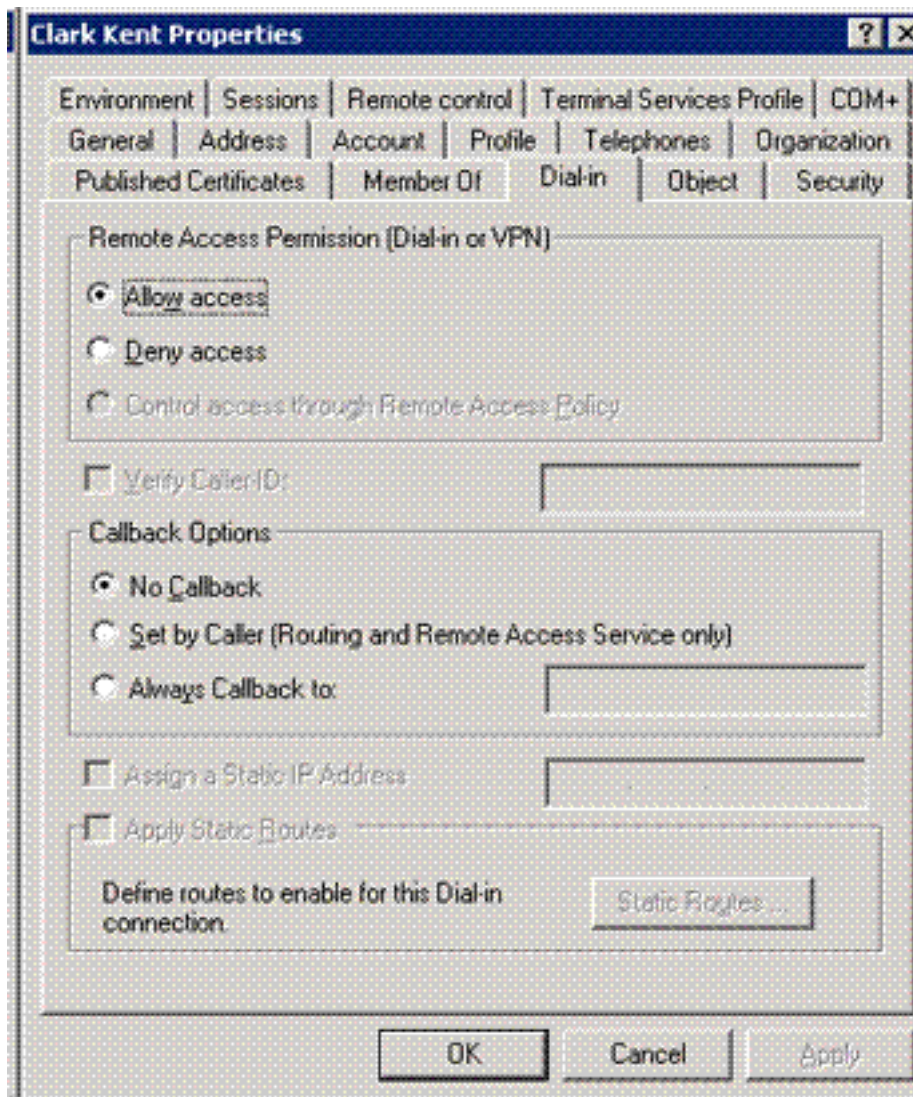
1. In the Active Directory Server, click **Start > Run**.
2. In the Open text box, type **dsa.msc** then click **Ok**. This starts the active directory management console.
3. In the Active Directory management console, click the plus sign in order to expand the Active Directory Users and Computers.
4. Click the plus sign in order to expand the domain name.
5. If you have an OU created for your users, expand the OU in order to view all users; if you have all users assigned in the Users folder, expand that folder in order to view them. See Figure A1.

Figure A1: Active Directory Management Console



6. Double-click on the user that you want to edit. Click on the Dial-in tab in the user properties page and click on **allow** or **deny**. See Figure A2.

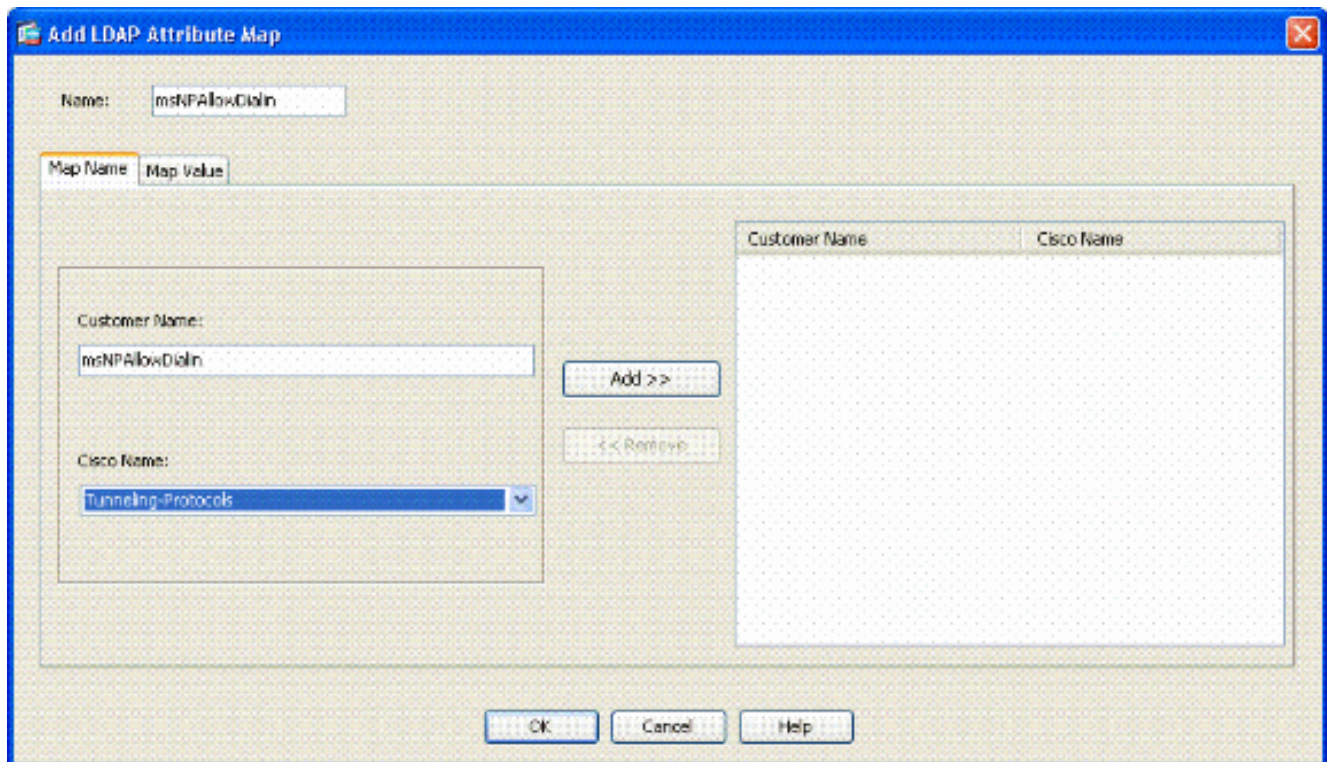
Figure A2: User Properties



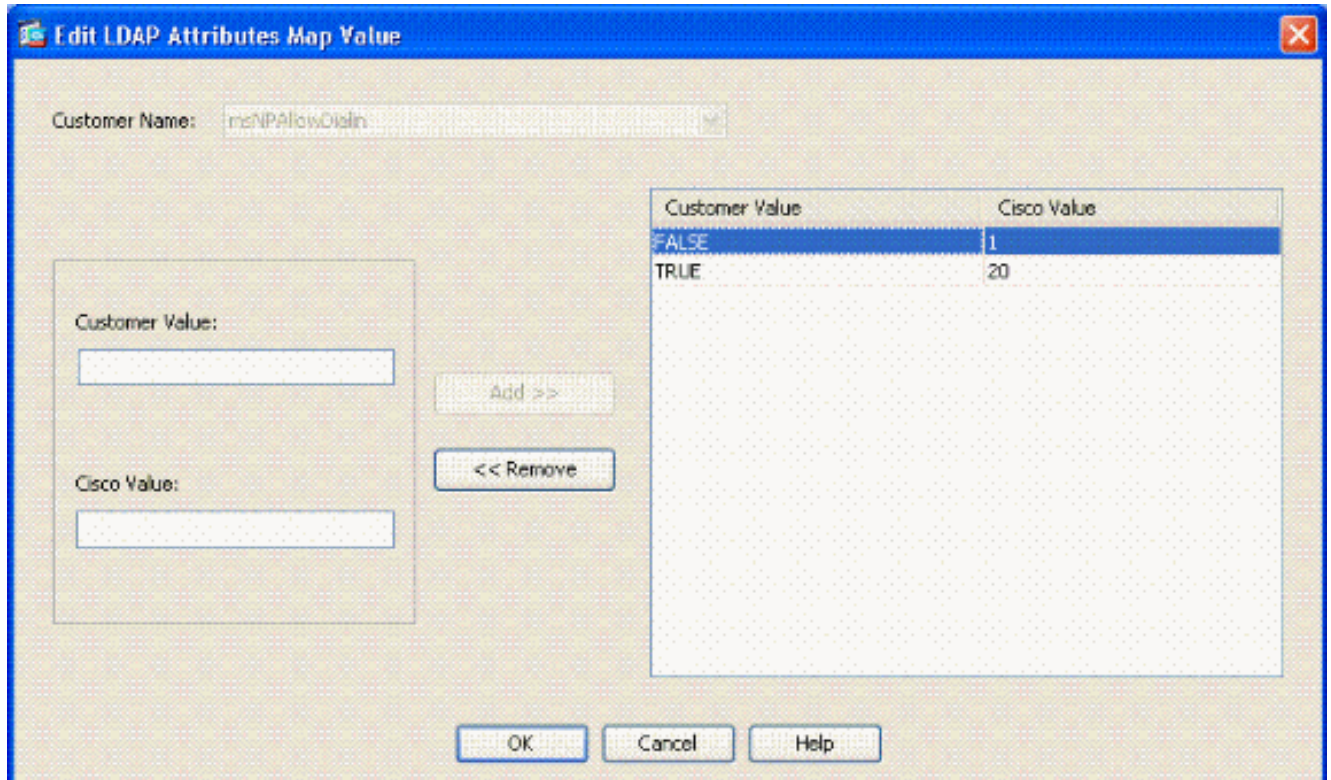
7. Then click **Ok**.

ASA Configuration

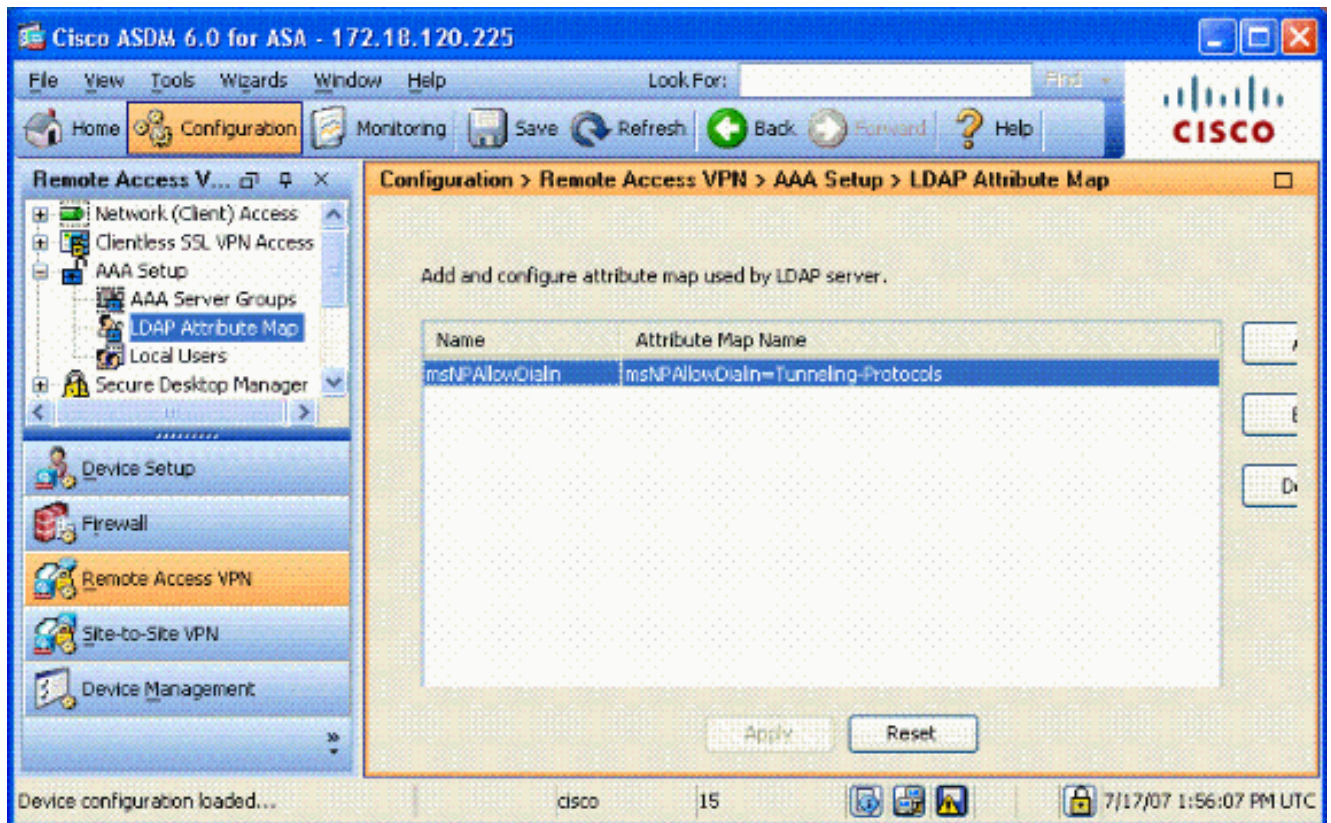
1. In ASDM, choose **Remote Access VPN> AAA Setup > LDAP Attribute Map**.
2. Click **Add**.
3. In the Add LDAP Attribute Map window, complete these steps. See Figure A3.**Figure A3: Adding LDAP Attribute Map**



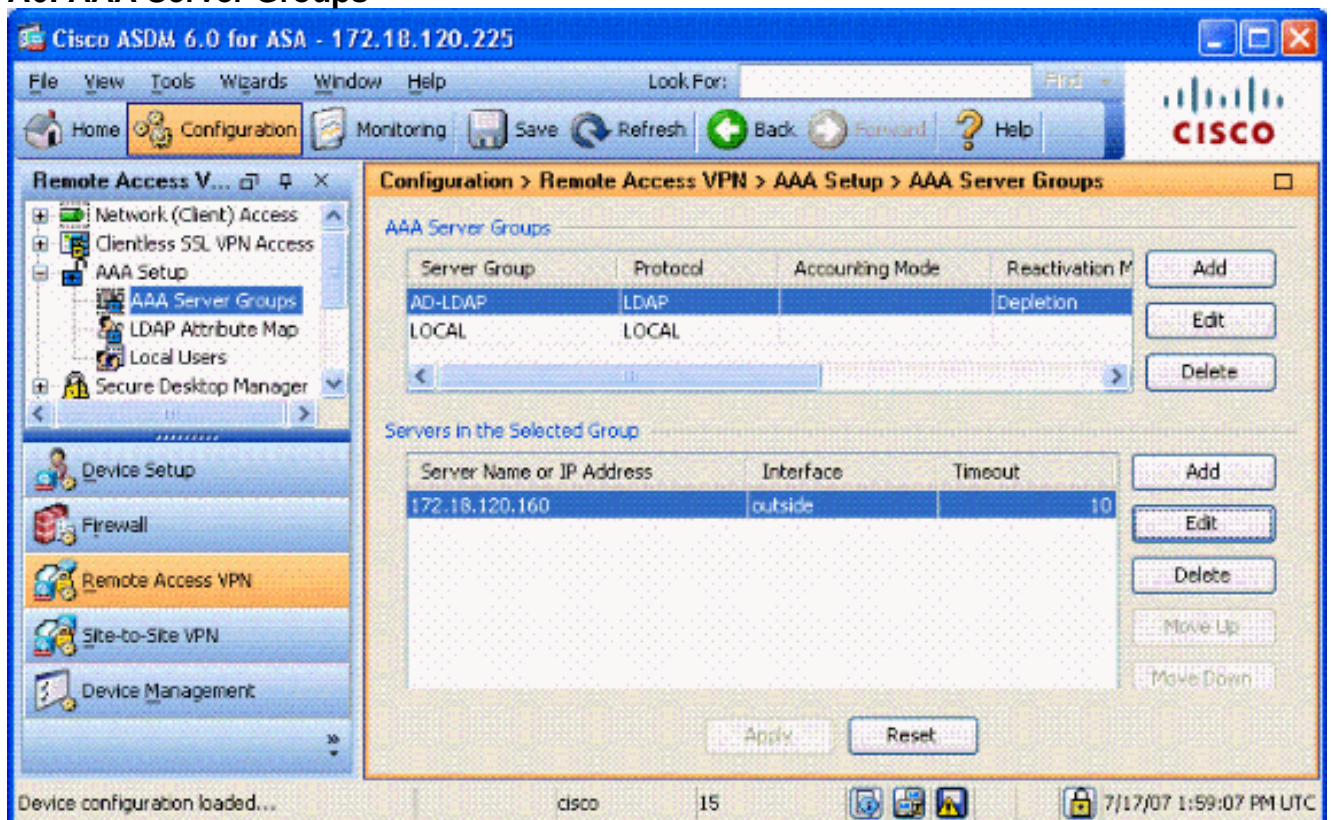
Enter a name in the Name textbox. In the Map Name Tab, type **msNPAllowDialIn** in the Customer Name text box. In the Map Name Tab, choose **Tunneling-Protocols** in the drop-down option in the Cisco Name. Click **Add**. Choose the **Map Value** tab. Click **Add**. In the Add Attribute LDAP Map Value window, type **TRUE** in the Customer Name text box and type **20** in the Cisco Value text box. Click **Add**. Type **FALSE** in the Customer Name text box and type **1** in the Cisco Value text box. See Figure A4.



Click **Ok**. Click **Ok**. Click **APPLY**. Configuration should look like Figure A5. **Figure A5: LDAP Attribute Map configuration**



4. Choose **Remote Access VPN > AAA Setup > AAA Server Groups**. See Figure A6. **Figure A6: AAA Server Groups**



5. Click on the server group that you want to edit. In the Servers in the Selected Group section, choose the server IP address or hostname, and then click **Edit**.
6. In Edit AAA Server window, in the LDAP Attribute Map text box, choose the LDAP attribute map created in the drop-down menu. See Figure A7. **Figure A7: Adding LDAP Attribute**

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: CN=Administrator,CN=Users,DC=gsgseclab,DC=o

Login Password: ●●●●●●●●

LDAP Attribute Map: msNPAllowDialin

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

Map

7. Click **Ok**.

Note: Turn on LDAP debugging while you test in order to verify if LDAP binding and attribute mapping work properly. See Appendix C for troubleshooting commands.

[Scenario 2 : Active Directory Enforcement using Group membership to Allow/Deny Access](#)

This example uses the LDAP attribute memberOf to map to the Tunneling Protocol attribute in order to establish a group membership as a condition. For this policy to work, you must have these conditions:

- Use a group that already exists or create a new group for ASA VPN users to be a member of for ALLOW conditions.
- Use a group that already exists or create a new group for non ASA users to be a member of for DENY conditions.

- Make sure to check in the LDAP viewer that you have the right DN for the group. See Appendix D. If the DN is wrong, the mapping does not work properly.

Note: Be aware that the ASA can only read the first string of the memberOf attribute in this release. Make sure that the new group created is on the top of the list. The other option is to put a special character in front of the name as AD looks at special characters first. In order to work around this caveat, use DAP in 8.x software to look at multiple groups.

Note: Make sure a user is part of the deny group or at least one other group so that the memberOf is always sent back to the ASA. You do not have to specify the FALSE deny condition but best practice is to do so. If the existing group name or the group name contains a space, enter the attribute in this manner:

```
CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org
```

Note: DAP allows the ASA to look at multiple groups in the memberOf attribute and base authorization off the groups. See the DAP section.

MAPPING

- The AD attribute value: memberOf
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org memberOf
CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Cisco attribute value: 1 = FALSE, 20 = TRUE,

For **ALLOW** condition, you map:

- memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org= 20

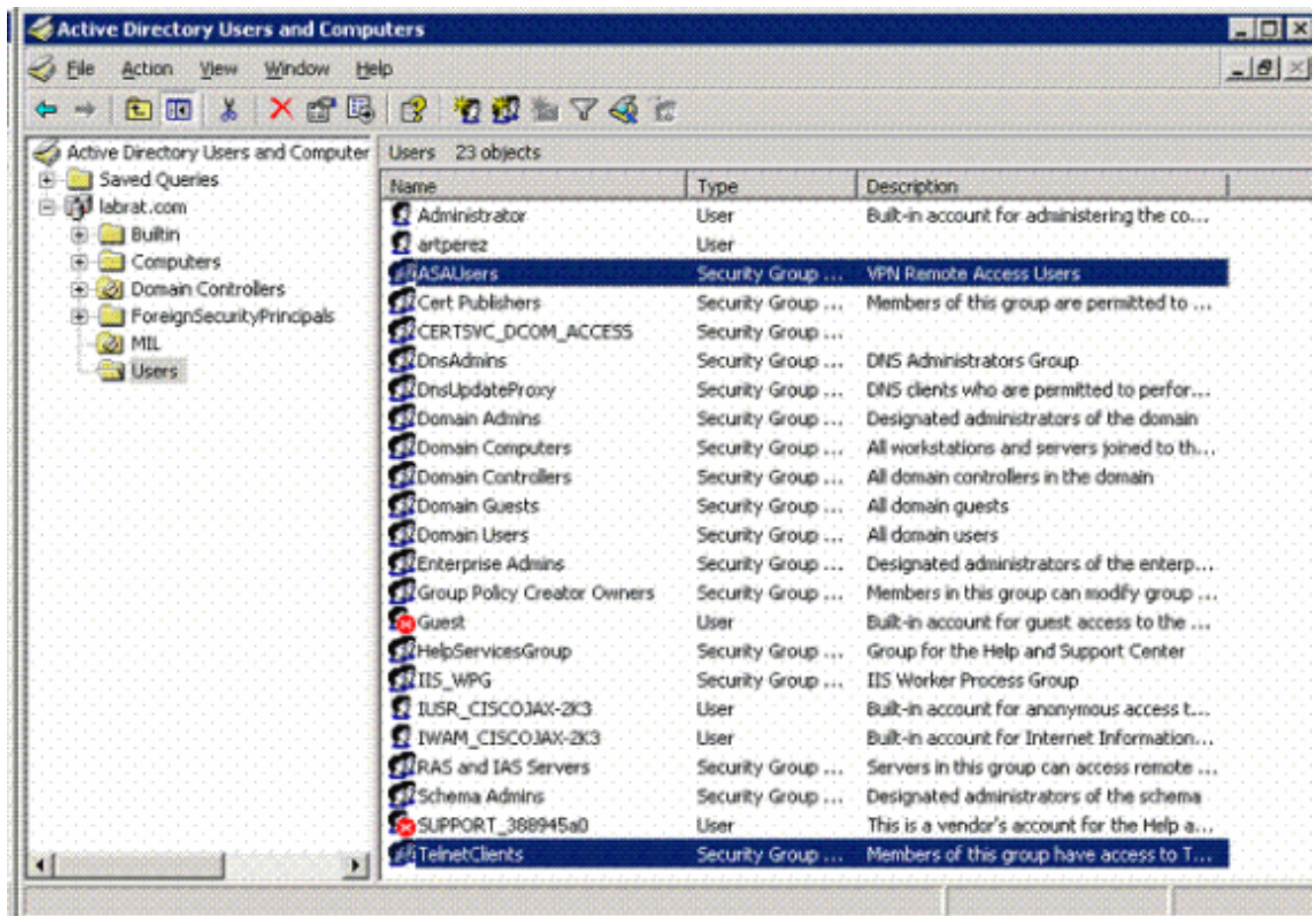
For **DENY** condition, you map:

- memberOf CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org = 1

Note: In future release, there is a Cisco attribute in order to allow and deny connection. Refer to [Configuring an External Server for Security Appliance User Authorization](#) for more information on Cisco attributes.

Active Directory Setup

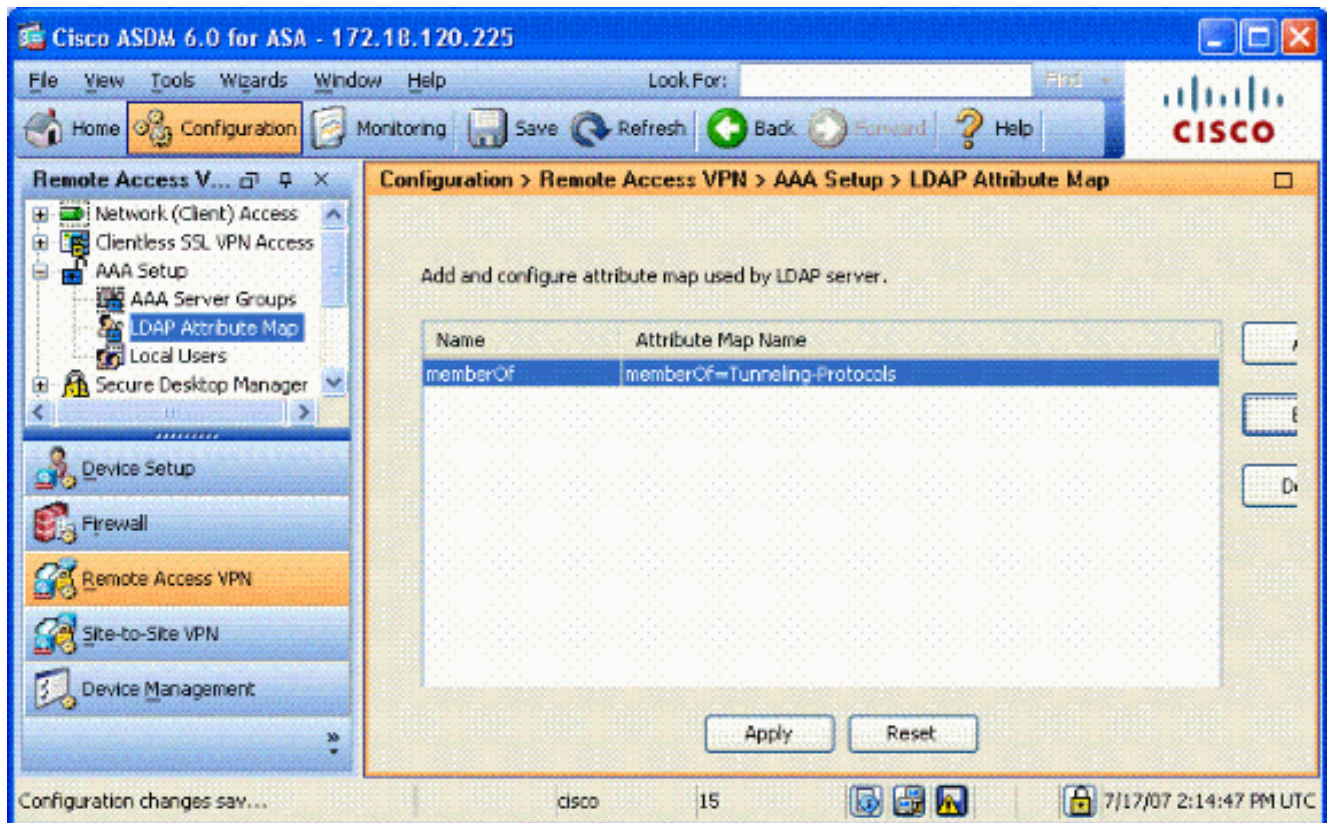
1. In the Active Directory Server, choose **Start > Run**.
2. In the Open text box, type **dsa.msc**, and then click **Ok**. This starts the active directory management console.
3. In the Active Directory management console, click the plus sign in order to expand the Active Directory Users and Computers. See Figure A8 **Figure A8: Active Directory Groups**



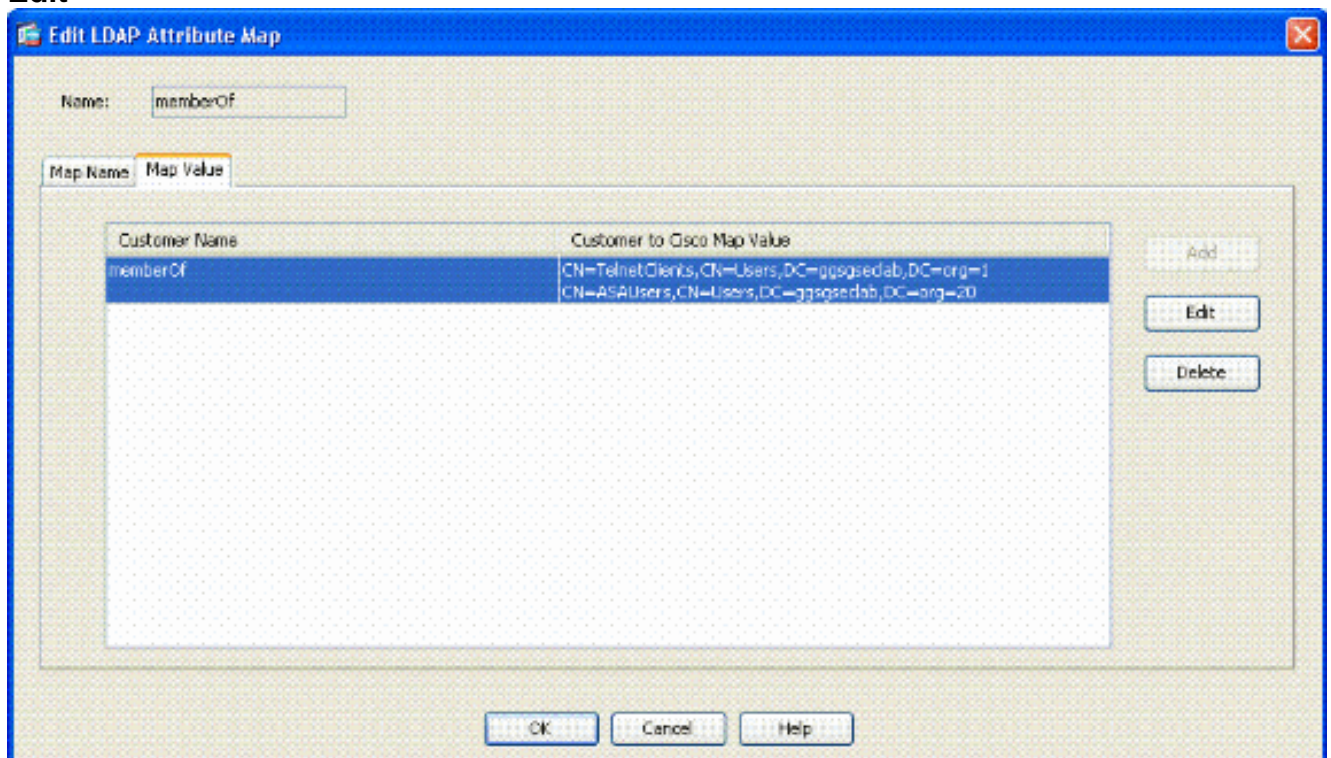
4. Click the plus sign in order to expand the domain name.
5. Right-click on the **Users** folder and choose **New > Group**.
6. Enter a Group Name. For example: ASAUsers.
7. Click **Ok**.
8. Click on the **Users** folder, and then double-click on the group you just created.
9. Choose **Members** tab, and then click **Add**.
10. Type the Name of the user you want to add, and then click **Ok**.

ASA Configuration

1. In ASDM, choose **Remote Access VPN > AAA Setup > LDAP Attribute Map**.
2. Click **Add**.
3. In the Add LDAP Attribute Map window, complete these steps. See Figure A3. Enter a name in the Name textbox. In the Map Name Tab, type **memberOf** in the Customer Name text box c. In the Map Name Tab, choose **Tunneling-Protocols** in the drop-down option in the Cisco Name. Choose **Add**. Click the **Map Value** tab. Choose **Add**. In the Add Attribute LDAP Map Value window, type **CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org** in the Customer Name text box and type **20** in the Cisco Value text box. Click **Add**. Type **CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org** in the Customer Name text box and type **1** in the Cisco Value text box. See Figure A4. Click **Ok**. Click **Ok**. Click **Apply**. Configuration should look like Figure A9. **Figure A9 LDAP Attribute Map**



4. Choose **Remote Access VPN> AAA Setup > AAA Server Groups**.
5. Click on the server group that you want to edit. In the Servers in the Selected Group section, select the server IP address or hostname, and then click **Edit**



6. In Edit AAA Server window, in the LDAP Attribute Map text box, select the LDAP attribute map created in the drop-down menu.
7. Click **Ok**.

Note: Turn on LDAP debugging while you test in order to verify LDAP binding and attribute mappings work properly. See Appendix C for troubleshooting commands.

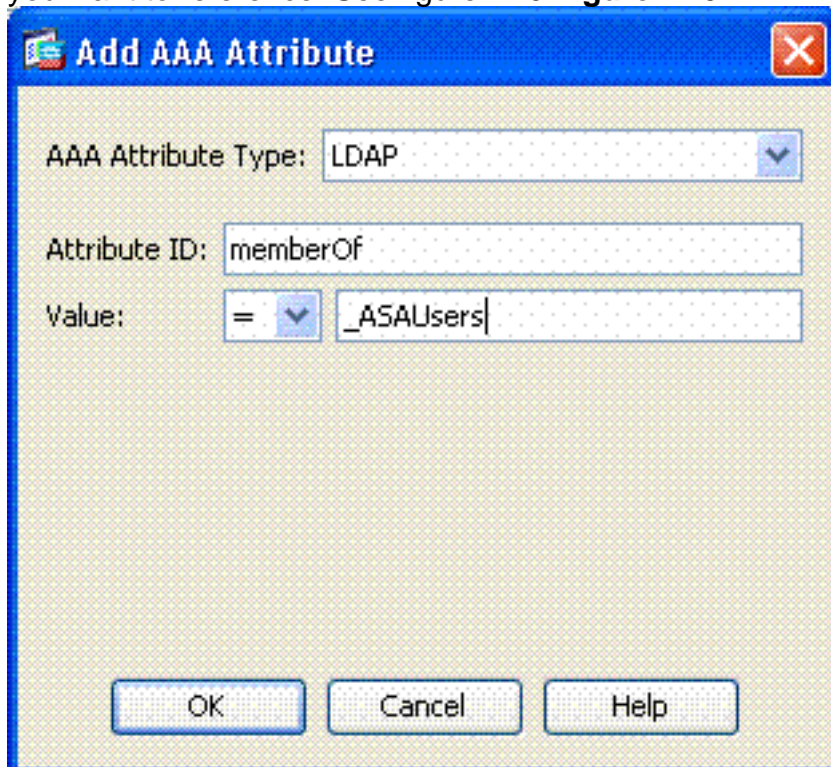
Scenario 3: Dynamic Access Policies for Multiple memberOf Attributes

This example uses DAP to look at multiple memberOf attributes in order to allow access based off of Active Directory group membership. Prior to 8.x, the ASA only read the first memberOf attribute. With 8.x and later, the ASA can look at all the memberOf attributes.

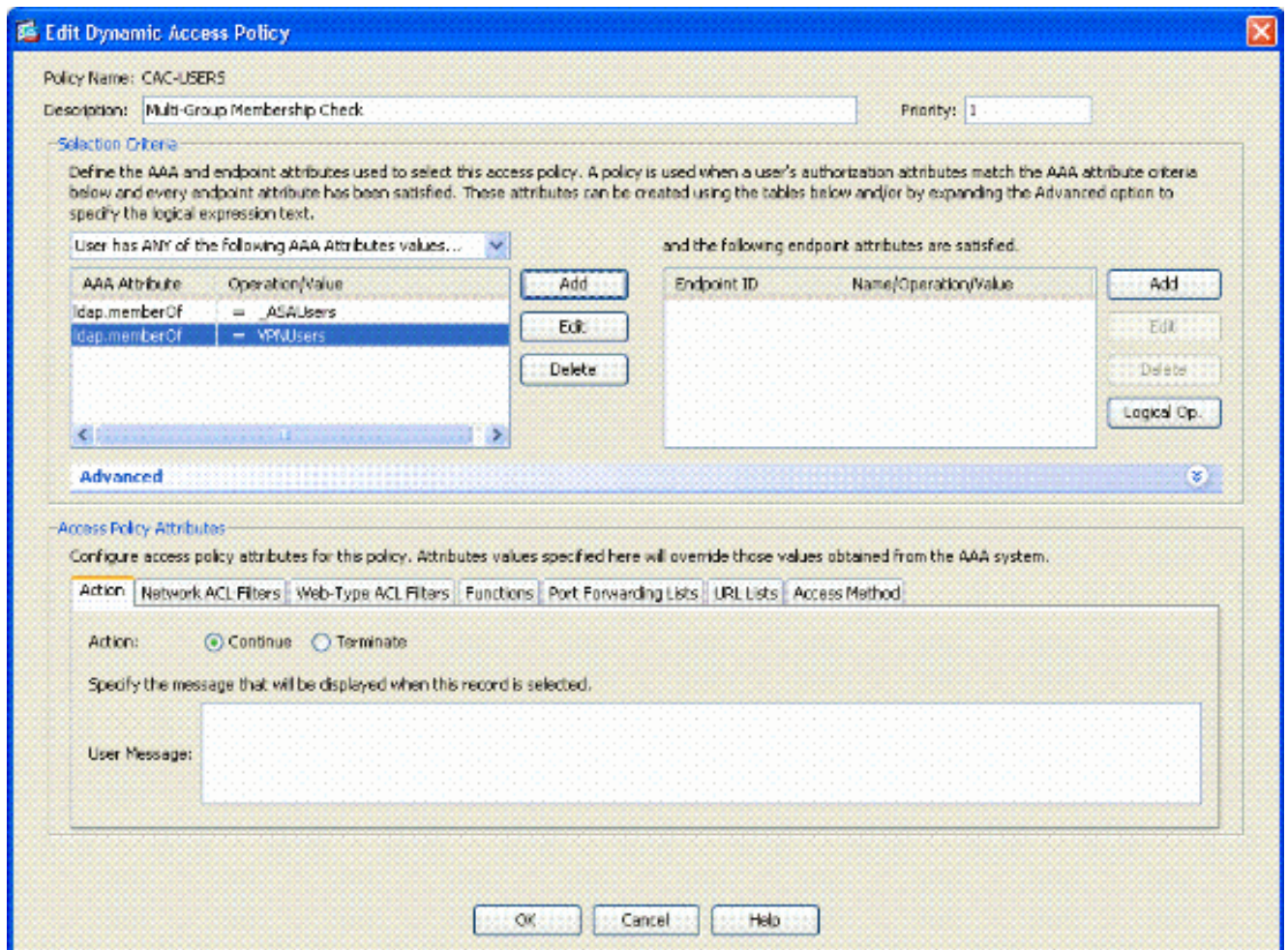
- Use a group that already exists or create a new group (or multiple groups) for ASA VPN users to be a member of for ALLOW conditions.
- Use a group that already exists or create a new group for non ASA users to be a member of for DENY conditions.
- Make sure to check in the LDAP viewer that you have the right DN for the group. See Appendix D. If the DN is wrong, the mapping does not work properly.

ASA Configuration

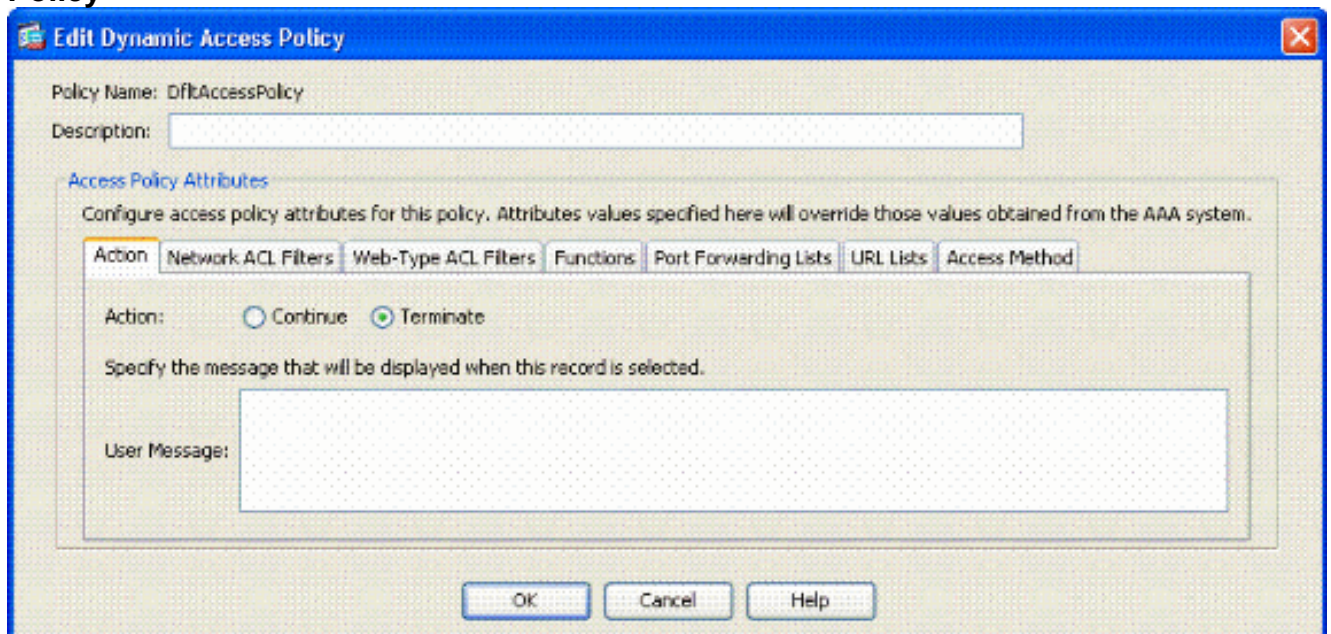
1. In ASDM, choose **Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
2. Click **Add**.
3. In the Add Dynamic Access Policy, complete these steps:
 - a. Enter a name in the Name textbox
 - b. In the priority section, enter **1**, or a number greater than 0. In the Selection Criteria, click **Add**. In the Add AAA Attribute, choose **LDAP**. In the attribute ID section, enter **memberOf**. In the value section, choose **=** and enter the AD group name. Repeat this step for each group you want to reference. See figure A10. **Figure A10 AAA Attribute Map**



Click **OK**. In the Access Policy Attributes section, choose **Continue**. See figure A11. **Figure A11 Add Dynamic Policy**



4. In ASDM, choose **Remote Access VPN> Network (Client) Access > Dynamic Access Policies**.
5. Choose **Default Access Policy** and choose **Edit**.
6. The default action should be set to **Terminate**. See figure A12.**Figure A12 Edit Dynamic Policy**



7. Click **Ok**.

Note: If **Terminate** is not selected, you are allowed in even if not in any groups because the default is to Continue.

Appendix B – ASA CLI Configuration

ASA 5510

```
ciscoasa#show running-config : Saved : ASA Version 8.0(2) !
hostname asa80 domain-name army.mil enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip address
x.x.x.x 255.255.255.128 ! interface GigabitEthernet0/1 nameif
inside security-level 100 no ip address ! boot system
disk0:/asa802-k8.bin ftp mode passive dns server-group
DefaultDNS domain-name army.mil ! -----ACL's-----
----- access-list out
extended permit ip any any -----
----- pager lines 24 logging
console debugging mtu outside 1500 ! -----VPN Pool-
----- ip local pool
CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0 -----
-----
- ! no failover icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin no asdm history enable arp
timeout 14400 access-group out in interface outside route
outside 0.0.0.0 0.0.0.0 172.18.120.129 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout
uauth 0:05:00 absolute ! -----LDAP Maps
& DAP----- ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols March 11, 2008 ASA -
CAC Authentication for AnyConnect VPN Access Company
Confidential. A printed copy of this document is considered
uncontrolled. 49 map-value memberOf
CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20 ldap attribute-
map msNPAllowDialin map-name msNPAllowDialin Tunneling-
Protocols map-value msNPAllowDialin FALSE 1 map-value
msNPAllowDialin TRUE 20 dynamic-access-policy-record CAC-
USERS description "Multi-Group Membership Check" priority 1
dynamic-access-policy-record DfltAccessPolicy action
terminate -----
----- ! -----LDAP Server-----
----- aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160 ldap-base-dn
CN=Users,DC=ggsgseclab,DC=org ldap-scope onelevel ldap-
naming-attribute userPrincipalName ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
-----
----- ! aaa authentication http console LOCAL http server
enable 445 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart ! -----CA
Trustpoints----- crypto ca
trustpoint ASDM_TrustPoint0 revocation-check ocs p enrollment
terminal keypair DoD-1024 match certificate
DefaultCertificateMap override ocs p trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil crl configure
crypto ca trustpoint ASDM_TrustPoint1 revocation-check ocs p
enrollment terminal fqdn asa80 subject-name
CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US keypair DoD-
1024 match certificate DefaultCertificateMap override ocs p
trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil no
client-types crl configure crypto ca trustpoint
ASDM_TrustPoint2 revocation-check ocs p enrollment terminal
```

```
keypair DoD-2048 match certificate DefaultCertificateMap
override oosp trustpoint ASDM_TrustPoint5 10 url
http://oosp.disa.mil no client-types crl configure crypto ca
trustpoint ASDM_TrustPoint3 revocation-check oosp none
enrollment terminal crl configure ! -----
Certificate Map----- crypto ca
certificate map DefaultCertificateMap 10 subject-name ne " " -
-----CA Certificates (Partial Cert is Shown)---
----- crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37 3082044c 30820334 a0030201 02020137
300d0609 2a864886 f70d0101 05050030 60310b30 09060355
04061302 55533118 30160603 55040a13 0f552e53 2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603 55040b13 03504b49 311b3019 06035504 03131244
6f44204a 49544320 526f6f74 crypto ca certificate chain
ASDM_TrustPoint1 certificate 319e 30820411 3082037a a0030201
02020231 9e300d06 092a8648 86f70d01 01050500 305c310b
30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047 6f766572 6e6d656e 74310c30 0a060355 040b1303
446f4431 0c300a06 0355040b crypto ca certificate chain
ASDM_TrustPoint2 certificate ca 37 3082044c 30820334 a0030201
02020137 300d0609 2a864886 f70d0101 05050030 60310b30
09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344
6f44310c 300a0603 55040b13 f766e045 f15ddb43 9549d1e9
a0ea6814 b64bcece 089e1b6e 1be959a5 6fc20a76 crypto ca
certificate chain ASDM_TrustPoint3 certificate ca 05 30820370
30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030 5b310b30 09060355 04061302 55533118 30160603
55040a13 0f552e53 2e20476f 7665726e 6d656e74 310c300a
06035504 0b130344 6f44310c 300a0603 55040b13 03504b49
31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d 30343132 31333135 30303130 5a170d32 39313230
35313530 3031305a 305b310b 30090603 55040613 02555331
18301606 0355040a 130f552e 532e2047 6f766572 6e6d656e
74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b 49311630 14060355 0403130d 446f4420 526f6f74
20434120 32308201 crypto ca certificate chain
ASDM_TrustPoint4 certificate ca 04 30820267 308201d0 a0030201
02020104 300d0609 2a864886 f70d0101 05050030 61310b30
09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f 7665726e 6d656e74 310c300a 06035504 0b130344
6f44310c 300a0603 55040b13 03504b49 311c301a 06035504
03131344 6f442043 4c415353 20332052 6f6f7420 !! class-map
inspection_default match default-inspection-traffic !!
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect ftp
inspect h323 h225 inspect h323 ras inspect netbios inspect
rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global ! -----
--SSL/WEBVPN----- ssl
certificate-authentication interface outside port 443 webvpn
enable outside svc image disk0:/anyconnect-win-2.0.0343-
k9.pkg 1 svc enable tunnel-group-list enable -----
-----VPN Group/Tunnel Policy-----
group-policy CAC-USERS internal ggroup-policy AC-USERS
internal group-policy AC-USERS attributes vpn-tunnel-protocol
svc address-pools value CAC-USERS webvpn svc ask none default
svc tunnel-group AC-USERS type remote-access tunnel-group AC-
USERS general-attributes authorization-server-group AD-LDAP
default-group-policy AC-USERS authorization-required
```

```
authorization-dn-attributes UPN tunnel-group AC-USERS webvpn-
attributes authentication certificate group-alias AC-USERS
enable tunnel-group-map enable rules no tunnel-group-map
enable ou no tunnel-group-map enable ike-id no tunnel-group-
map enable peer-ip -----
----- prompt hostname context
```

Appendix C- Troubleshooting

Troubleshooting AAA and LDAP

- **debug ldap 255**—Displays LDAP exchanges
- **debug aaa common 10**—Displays AAA exchanges

Example 1: Allowed Connection with correct attribute mapping

This example shows the output of **debug ldap** and **debug aaa common** during a successful connection with the scenario 2 shown in Appendix A.

Figure C1: debug LDAP and debug aaa common output – correct mapping

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap://
172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=gsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
```

```
0..50...../.....60...*.H.....0@1.0.....&...d....c
om1.0.....
&...d...
[78] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&...d....c
om1.0.....
&...d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP,
user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

```

User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP,
user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#

```

Example 2: Allowed Connection with mis-configured Cisco attribute mapping

This example shows the output of **debug ldap** and **debug aaa common** during an allowed connection with the scenario 2 shown in Appendix A.

Figure C2: debug LDAP and debug aaa common output – incorrect mapping

```

AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer

```



```
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389,
status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=gsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&...d....c
om1.0.....
&...d...
[82] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&...d....c
om1.0.....
&...d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
```

```
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP,
user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP,
user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "gsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
```

```

"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop

```

Troubleshooting DAP

- **debug dap errors**—Displays DAP errors
- **debug dap trace**—Displays DAP function trace

Example 1: Allowed connection with DAP

This example shows the output of **debug dap errors** and **debug dap trace** during a successful connection with the scenario 3 shown in Appendix A. Notice multiple memberOf attributes. You can belong to both `_ASAUsers` and `VPNUsers` or to either group, which depends on the ASA config.

Figure C3: debug DAP

```

#debug dap errors debug dap errors enabled at level 1 #debug
dap trace debug dap trace enabled at level 1 # The DAP policy
contains the following attributes for user: 1241879298@mil --
-----
----- --- 1: action = continue DAP_TRACE: DAP_open:
C8EEFA10 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.2 = person DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user DAP_TRACE: Username:
1241879298@mil, aaa.ldap.cn = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.physicalDeliveryOfficeName =
NETADMIN DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.givenName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged = 20070718151143.0Z DAP_TRACE: Username:
1241879298@mil, aaa.ldap.displayName = 1241879298 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 =
VPNUsers DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.memberOf.2 = _ASAUsers DAP_TRACE: Username:
1241879298@mil, aaa.ldap.uSNChanged = 53274 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectGUID = .....F..5.... DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userAccountControl = 328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime
= 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff

```

```
= 0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon =
0 DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userParameters = m: d. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectSid = .. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountType = 805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName = 1241879298@mil DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin
= TRUE DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.username = 1241879298@mil DAP_TRACE: Username:
1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] = "user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgseclab,DC=org"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] =
"NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] =
"0"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
```

```

dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"]
= "TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec"; DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
CAC-USERS DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1 DAP_TRACE: Username: 1241879298@mil, DAP_close:
C8EEFA10 d.

```

[Example 2: Denied Connection with DAP](#)

This example shows the output of **debug dap errors** and **debug dap trace** during an unsuccessful connection with the scenario 3 shown in Appendix A.

Figure C4: debug DAP

```

#debug dap errors debug dap errors enabled at level 1 #debug
dap trace debug dap trace enabled at level 1 # The DAP policy
contains the following attributes for user: 1241879298@mil --
-----
----- --- 1: action = terminate DAP_TRACE: DAP_open:
C91154E8 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.2 = person DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user DAP_TRACE: Username:
1241879298@mil, aaa.ldap.cn = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.physicalDeliveryOfficeName =
NETADMIN DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.givenName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged = 20070718151143.0Z DAP_TRACE: Username:
1241879298@mil, aaa.ldap.displayName = 1241879298 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf =
DnsAdmins DAP_TRACE: Username: 1241879298@mil,

```

```
aaa.ldap.uSNChanged = 53274 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.department = NETADMIN DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+.F..5... DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl = 328192 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.badPwdCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.codePage = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.countryCode = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.badPasswordTime = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogoff = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogon = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userParameters = m: d. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectSid = .. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountType = 805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName = 1241879298@mil DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPallowDialin
= TRUE DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.username = 1241879298@mil DAP_TRACE: Username:
1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] = "user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgseclab,DC=org"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
"DnsAdmins"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] =
"NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
```

```

DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] =
"0"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"]
= "TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE: Username: 1241879298@mil,
Selected DAPs: DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1

```

[Troubleshooting Certificate Authority / OCSP](#)

- **debug crypto ca 3**
- In the config mode—**logging class ca console(or buffer) debugging**

These examples show a successful certificate validation with the OCSP responder and a failed certificate group matching policy.

Figure C3 shows the debug output that has a validated certificate and a working certificate group matching Policy.

Figure C4 shows the debug output of a mis-configured certificate group matching policy.

Figure C5 shows the debug output of a user with a revoked certificate.

Figure C5: OCSP debugging – successful certificate validation

```

CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0.
Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert:

```

```

serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer
cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with
serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence
10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer
cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer
cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN
group map

```

Figure C5: Output of a failed certificate group matching policy

| Figure C5: Output of a revoked certificate |
|--|
| <pre> n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=. CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor =noct oamuthori,zed. map rule: subject-name ne "". CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap sequence: 10. Tunnel Group Match on map DefaultCertificateMap sequence # </pre> |


```

10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint
trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status: 0.
Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer cert:
serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence
10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer
cert field:
= cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org, map rule:
subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is revoked,
serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated

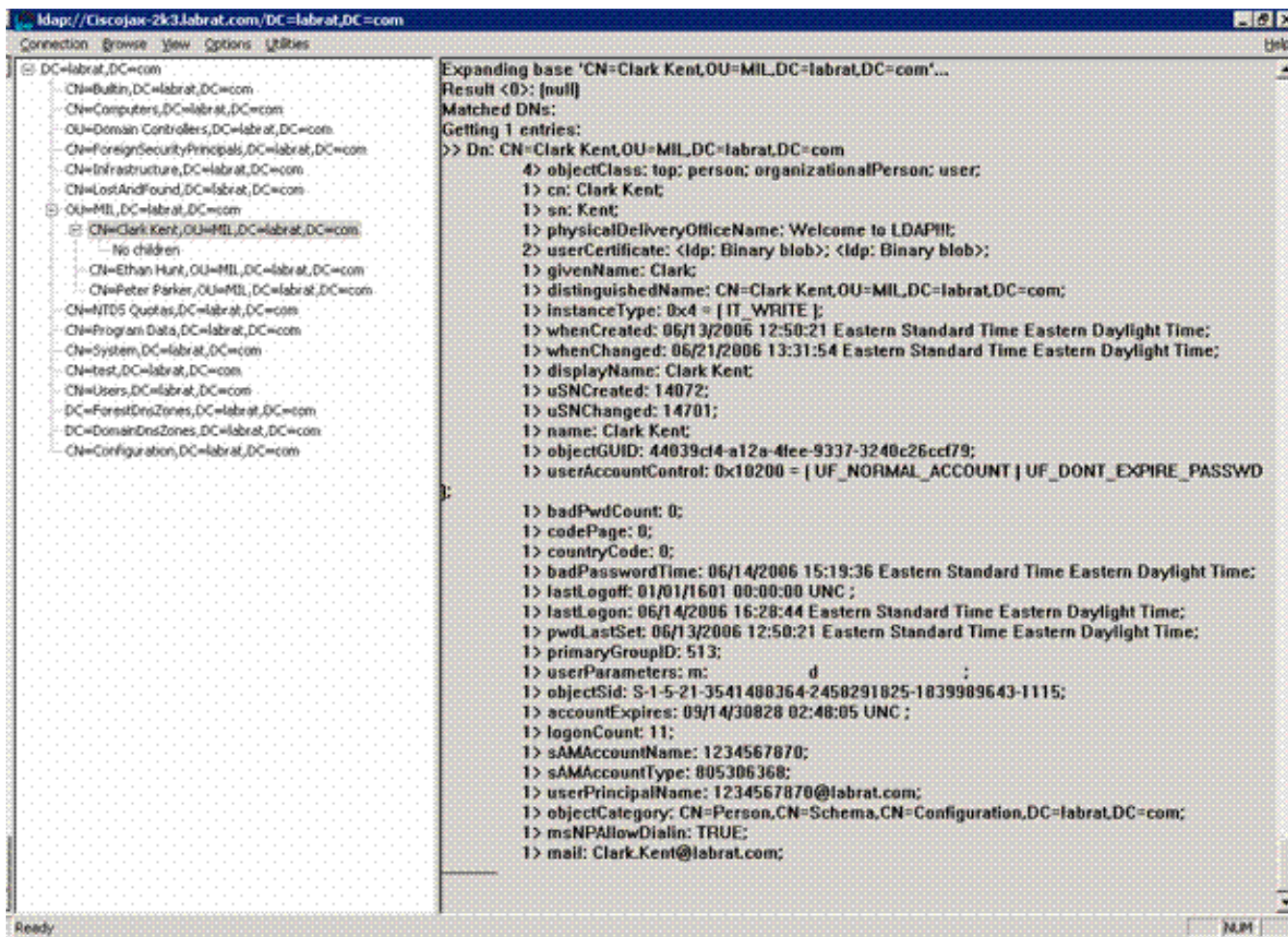
```

[Appendix D – Verify LDAP Objects in MS](#)

In Microsoft server 2003 CD, there are additional tools that can be installed in order to view the LDAP structure as well as the LDAP objects/attributes. In order to install these tools, go to the **Support** directory in the CD and then **Tools**. Install **SUPTOOLS.MSI**.

[LDAP Viewer](#)

- After installation, choose **Start > Run**.
- Type **ldp**, then click **Ok**. This starts the LDAP viewer.
- Choose **Connection > Connect**.
- Enter the server name and then click **Ok**.
- Choose **Connection > Bind**.
- Enter a username and password. **Note:** You need administrator rights.
- Click **OK**.
- View LDAP objects. See Figure D1. **Figure D1: LDAP Viewer**

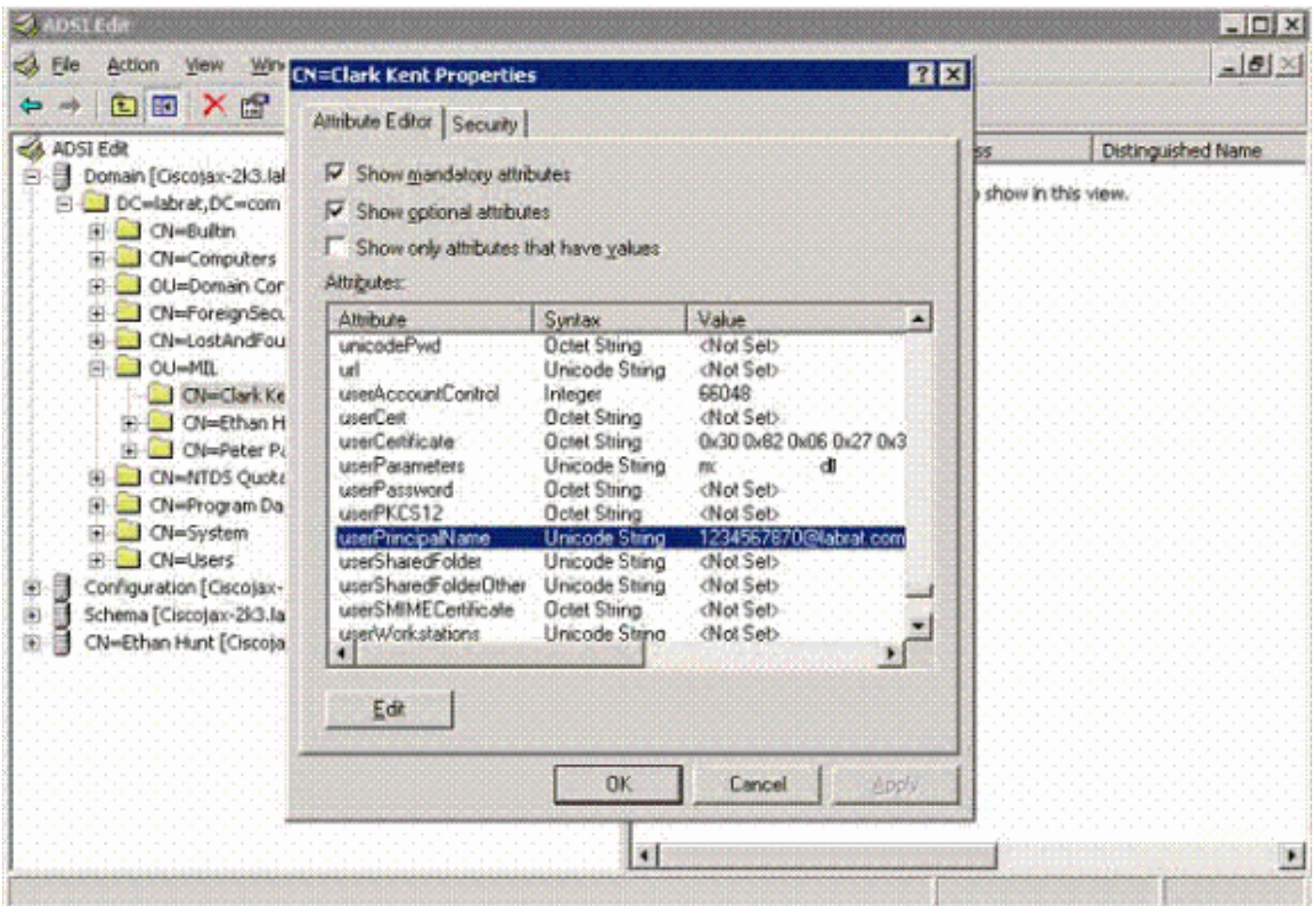


Active Directory Services Interface Editor

- In the Active Directory server, choose **Start > Run**.
- Type **adsiedit.msc**. This starts the editor.
- Right click on an object and click **Properties**.

This tool shows all attributes for specific objects. See Figure D2.

Figure D2: ADSI Edit



Appendix E

An AnyConnect profile can be created and added to a workstation. The profile can reference various values such as ASA hosts or certificate matching parameters such as distinguished name or issuer. The profile is stored as an .xml file and can be edited with Notepad. The file can be added to each client manually or pushed from the ASA through a group policy. The file is stored in:

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

Complete these steps:

1. Choose the AnyConnectProfile.tmpl and open the file with Notepad.
2. Make appropriate modifications to the file such as issuer or host IP. See Figure F1 for example.
3. When finished, save the file as an .xml.

This is a sample of a Cisco AnyConnect VPN Client Profile XML file.

Refer to the Cisco AnyConnect documentation in regards to profile management. In short:

- A Profile should be uniquely named for your Company. An example is: CiscoProfile.xml
- The profile name should be the same even if different for individual group within the company.

This file is intended to be maintained by a Secure Gateway administrator and then distributed with the client software. The profile based on this XML can be distributed to clients at any time. The distribution mechanisms supported are as a bundled file with the software distribution or as part of the automatic download mechanism. The automatic download mechanism only available with

certain Cisco Secure Gateway products.

Note: Administrators are strongly encouraged to validate the XML profile they create with the use of an online validation tool or through the profile import functionality in ASDM. Validation can be accomplished with the AnyConnectProfile.xsd found in this directory. AnyConnectProfile is the root element that represents the AnyConnect Client Profile.

```
xml version="1.0" encoding="UTF-8" - - <AnyConnectProfile
xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd"> !-- The ClientInitialization section
represents global settings !-- for the client. In some
cases, for example, BackupServerList, host specific !--
overrides are possible. !-- --> - <ClientInitialization> !--
The Start Before Logon feature can be used to activate !--
the VPN as part of the logon sequence. !-- UserControllable:
Does the administrator of this profile allow the user !-- to
control this attribute for their own use. Any user setting !-
-- associated with this attribute is stored elsewhere. -->
<UseStartBeforeLogon
UserControllable="false">>false</UseStartBeforeLogon> !--
This control enables an administrator to have a one time !--
message displayed prior to a users first connection attempt.
As an !-- example, the message can be used to remind a user
to insert their smart !-- card into its reader. !-- The
message to be used with this control is localizable and can
be !-- found in the AnyConnect message catalog. !--
(default: "This is a pre-connect reminder message.")
<ShowPreConnectMessage>>false</ShowPreConnectMessage> !-- This
section enables the definition of various attributes !--
that can be used to refine client certificate selection. -->
- <CertificateMatch> !-- Certificate Distinguished Name
matching allows for exact !-- match criteria in the choosing
of acceptable client !-- certificates. - <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal"
Wildcard="Disabled"> <Name>ISSUER-CN</Name> <Pattern>DoD-
Issuer-ABC</Pattern> </DistinguishedNameDefinition>
</DistinguishedName> </CertificateMatch>
</ClientInitialization> - !-- This section contains the list
of hosts from which !-- the user is able to select. -
<ServerList> !-- This is the data needed to attempt a
connection to a specific !-- host. --> - <HostEntry>
<HostName>host-02</HostName> <HostAddress>host-
02.dod.gov</HostAddress> </HostEntry> - <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress> </HostEntry>
</ServerList> </AnyConnectProfile>
```

[Related Information](#)

- [Certificates & CRLs specified by X.509 and RFC 3280](#) 
- [OCSP specified by RFC 2560](#) 
- [Public Key Infrastructure Introduction](#)
- ["Lightweight OCSP" profiled by draft standard](#) 
- [SSL / TLS specified by RFC 2246](#) 
- [Technical Support & Documentation - Cisco Systems](#)