

PIX/ASA 7.x: CAC – SmartCards Authentication for Cisco VPN Client

Document ID: 107273

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Cisco ASA Configuration

- Deployment Considerations

Authentication, Authorization, Accounting (AAA) Configuration

- Configure LDAP Server

Manage Trustpoints

- Generate Keys
- Install CA Trustpoints
- Install Root Certificates
- Enroll ASA and Install Identity Certificate

VPN Configuration

- Create Tunnel Group and Group Policy
- Tunnel Group Interface and Image Settings
- Configure IKE/ISAKMP Parameters
- Configure IPsec Parameters

Configure OCSP

- Configure OCSP Responder Certificate
- Configure CA to Use OCSP
- Configure OCSP Rules

Cisco VPN Client Configuration

- Start Cisco VPN Client
- New Connection
- Start Remote Access

Appendix A LDAP Mapping

Scenario 1: Active Directory Enforcement with Remote Access Permission Dial-in Allow/Deny Access

- Active Directory Setup
- ASA Configuration

Scenario 2 : Active Directory Enforcement with Group Membership to Allow/Deny Access

- Active Directory Setup
- 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 Misconfigured Cisco Attribute Mapping

Troubleshooting Certificate Authority / OCSP

Troubleshooting IPSEC

Appendix D Verify LDAP Objects in MS

- LDAP Viewer

Related Information

Introduction

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

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

The configuration in this guide uses the Microsoft AD/LDAP server. This document also covers advanced features, such as OCSP and LDAP attribute maps.

Prerequisites

Requirements

A basic knowledge of Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP, and Public Key Infrastructure (PKI) is beneficial to understand the complete setup. Familiarity with AD group membership and user properties, as well as LDAP objects helps to correlate the authorization process between the 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 7.2(2)
- Cisco Adaptive Security Device Manager (ASDM) Version 5.2(1)
- Cisco VPN Client 4.x

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 through ASDM. It covers the necessary steps to deploy a VPN remote access tunnel through an IPsec 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, or ASDM access, etc. It is assumed that the network operator is familiar with these configurations.

For more information, refer to Multifunction Security Appliances.

- Some sections are mandatory configurations needed for basic VPN access. For example, a VPN tunnel can be setup with the CAC card without OCSP checks, LDAP mappings checks. DoD mandates OCSP checking, but the tunnel works without the OCSP configured.
- The basic ASA/PIX image required is 7.2(2) and ASDM 5.2(1), but this guide uses an interim build of 7.2.2.10 and ASDM 5.2.2.54.
- No LDAP schema change is necessary.
- 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 the Related Information section for a list of RFCs.

Authentication, Authorization, Accounting (AAA) Configuration

Users are authenticated with the certificate in their Common Access Card (CAC) through the DISA Certificate Authority (CA) Server or the CA server of their own organizations. The certificate must be valid for remote access to the network. In addition to authentication, the users must also be authorized with a Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) object. The 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. The configurations below show how to configure the AAA server in the ASA with an LDAP server for authorization. See Appendix A for additional configurations with LDAP object mapping.

Configure LDAP Server

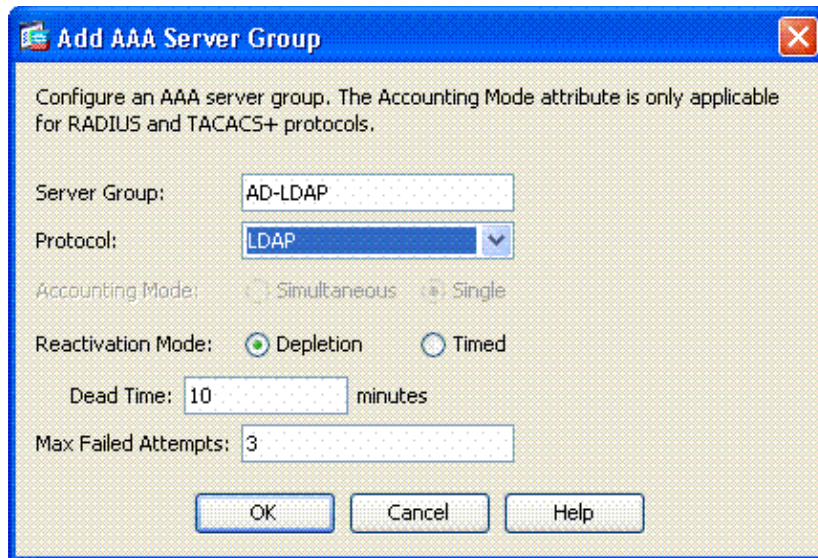
Follow these instructions:

1. Go to **Remote Access VPN > AAA Setup > AAA Server Group**.
2. In the AAA server groups table, click **Add**.
3. Enter the server group name, and choose **LDAP** in the protocol radio button. See Figure 1.
4. In the Servers in the selected group table, click **Add**. Make sure that the server you create is highlighted in this table.
5. In the edit AAA server window, see Figure 2.

Note: Choose the Enable LDAP over SSL option if your LDAP/AD is configured for this type of connection.

- a. Choose the interface in which the LDAP is located. This guide shows the inside interface.
- b. Enter the IP address of the server.
- c. Enter the Server Port. The default LDAP port is 389.
- d. Choose the Server Type.
- e. Enter the Base DN. Ask your AD/LDAP administrator for these values.

Figure 1: Add a Server Group



- f. Under the Scope option, choose whichever is appropriate. This is dependent upon the base DN. Ask your AD/LDAP administrator for assistance.
- g. In the Naming Attribute field, enter **userPrincipalName**. This attribute is used for user authorization in the AD/LDAP server.
- h. In the Login DN field, enter the administrator DN.

Note: The user needs administrative rights or rights to view/search the LDAP structure that includes user objects and group membership.

- i. In the Login Password field, enter the password of the administrator.
- j. Leave the LDAP attribute to **none**.

Figure 2

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

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

k. Click **OK**.

6. Click **OK**.

Manage Trustpoints

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

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

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

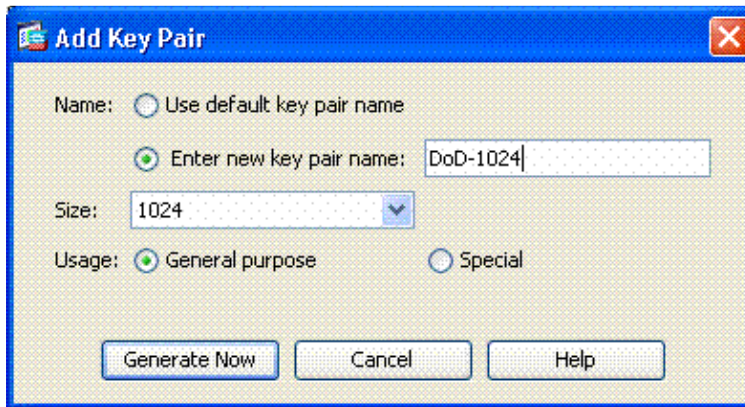
Note: DoD CA2 and Class 3 Root (as well as the ASA ID and CA intermediate that issued the ASA certificate) are usually the only CAs needed for user authentication. All the current CA intermediates fall under the CA2 and Class 3 Root chain and are trusted as long as the CA2 and Class 3 Roots are added.

Generate Keys

Follow these instructions:

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

Figure 3



4. Choose the size of the key.
5. Keep Usage to **General purpose**.
6. Click the **Generate Now** button.

Note: The DoD Root CA 2 uses a 2048 bit key. A second key that uses a 2048 bit key pair must be generated to be able to use this CA. Follow the above steps to add a second key.

Install CA Trustpoints

Follow these instructions:

1. Go to **Configuration > Properties > Certificate > Trustpoint > Configuration**. See Figure 4.
2. Enter the name in the Trustpoint Name field.
3. In the Enrollment Settings tab, choose the key generated in the previous step when you click the arrow. Choose the 2048 key for the Root CA 2 trustpoint.
4. In the Enrollment Mode section, choose **Use Manual Enrollment, OK, and Apply**.

Figure 4: Install Root Certificate

Add Trustpoint Configuration

Trustpoint Name:

Generate a self-signed certificate on enrollment
If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Key Pair:

Challenge Password: Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.

Enrollment Mode

Use manual enrollment
 Use automatic enrollment

Enrollment URL:

Retry Period: minutes

Retry Count: (Use 0 to indicate unlimited retries)

Note: Repeat steps 1–4 for every trustpoint you want to add. There are no hard numbers for the number of trustpoints that you can install since this is all based on memory in the device. DoD PKI requires a trustpoint for each of these: Root CA 2, Class 3 Root, CA## Intermediate and OCSP Server. The OCSP trustpoint is not needed if you do not use OCSP.

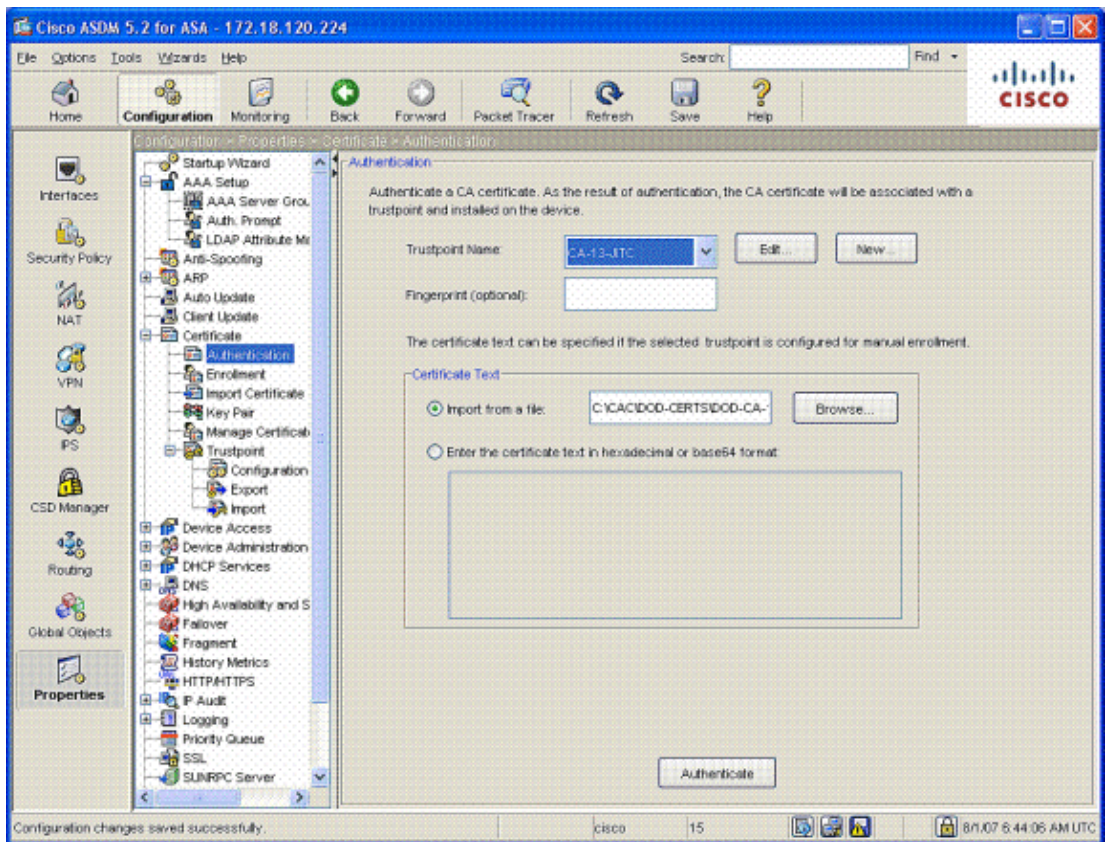
Install Root Certificates

Follow these instructions:

1. Go to **Configuration > Properties > Certificate > Authentication**.
2. In the Trustpoint Name field, choose the trustpoint configured in the previous step.
3. In the Certificate Text section, either import the certificate with a file or cut and paste the base64 encoded text (Control C and V).

Note: The import only accepts .txt files in this version of code, but the file that you receive from your CA administrator is in .cer format. You can also change the extension to .txt and open the file then cut and paste the text in the text box.

Figure 5: Authentication of CA



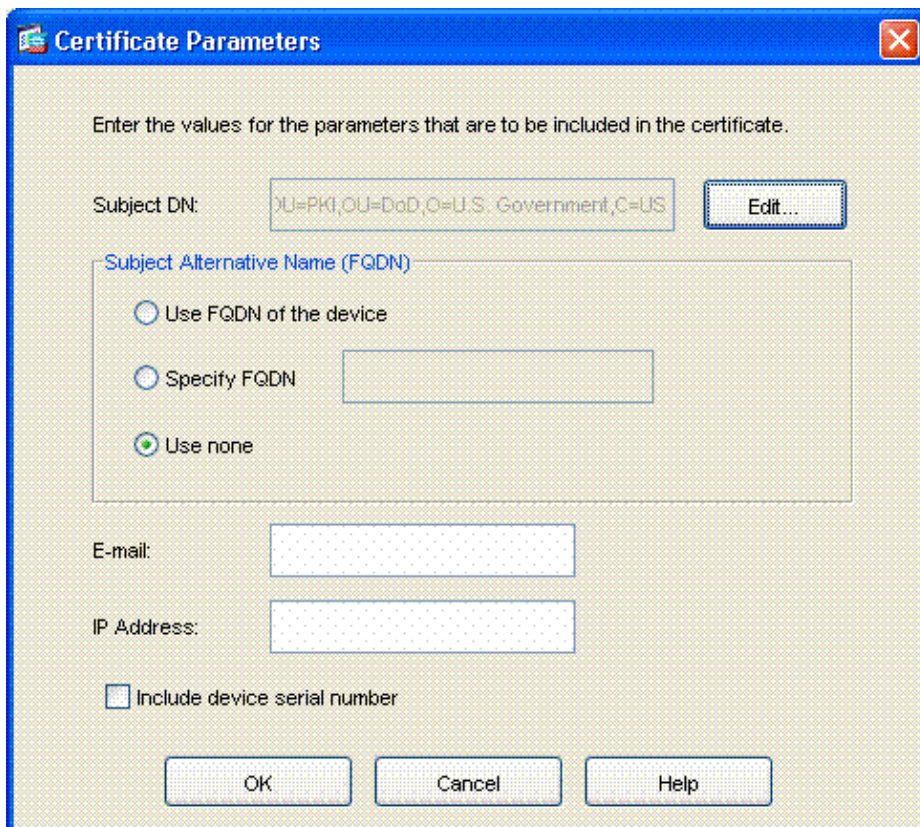
4. Click **Authenticate**.

Enroll ASA and Install Identity Certificate

Follow these instructions:

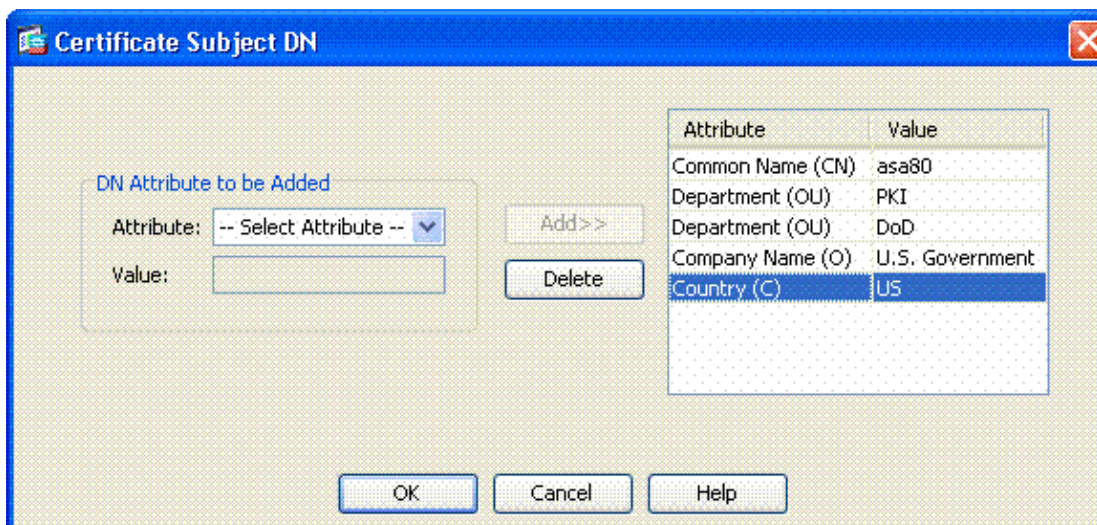
1. Go to **Configuration > Properties > Certificate > Enrollment**.
2. Choose a trustpoint. Click the down arrow on the radio button to choose the intermediate trustpoint where you would like to enroll the ASA device.
3. Click the **Edit** button.
4. In the Edit Trustpoint Configuration window, click **Certificate Parameters**.
5. In the Certificate Parameters window, choose the **Use none** option for the FQDN, and click **Edit** on the subject DN. See Figure 6.

Figure 6: Identity Certificate Parameters



6. In the Certificate Subject DN window, enter the information of the device. See Figure 7 for an example.
7. Click **OK**.

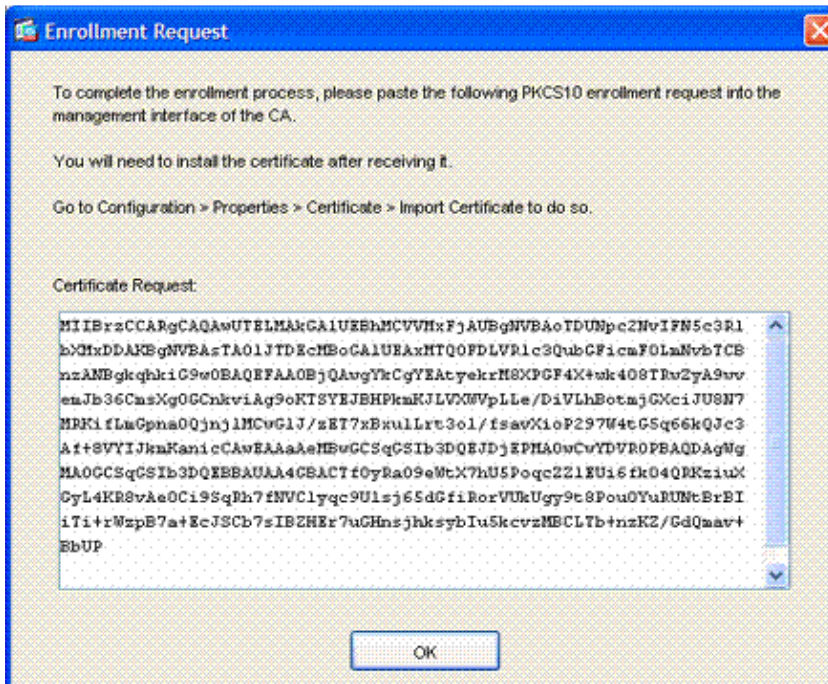
Figure 7: Edit DN



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 that are required.

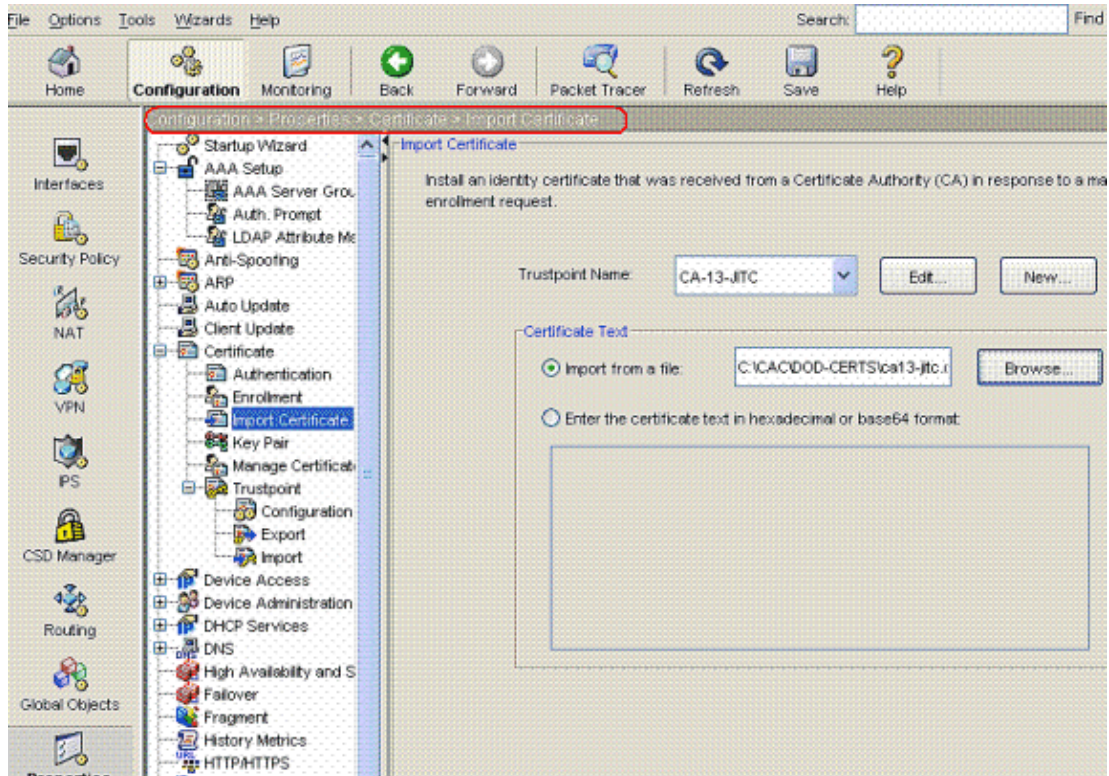
8. Click **OK** on the Certificate Parameters window, and click **OK** on the Edit Trustpoint Configuration window.
9. In the enrollment window, click **Enroll**.
10. Cut and paste the information from the Enrollment Request window; save it to a Notepad, and click **OK**. This is the information that needs to be sent to the CA administrator to request an identity certificate for the ASA. See Figure 8.

Figure 8: Certificate Request



11. Once you receive the certificate from the CA administrator, go to **Configuration > Properties > Certificate > Import Certificate**.
12. In the Import Certificate window, choose the trustpoint where you enrolled the ASA device.
13. In the certificate text, either import the file or cut and paste the base64 or DER encoded file that you received from your CA administrator. See Figure 9.

Figure 9: Import the Certificate



Note: The import only accepts .txt files in this version of code, but the file that you receive from your CA administrator is in .cer format. You can also change the extension to .txt, open the file, and then

cut and paste the text in the text box.

14. Choose **Import**.

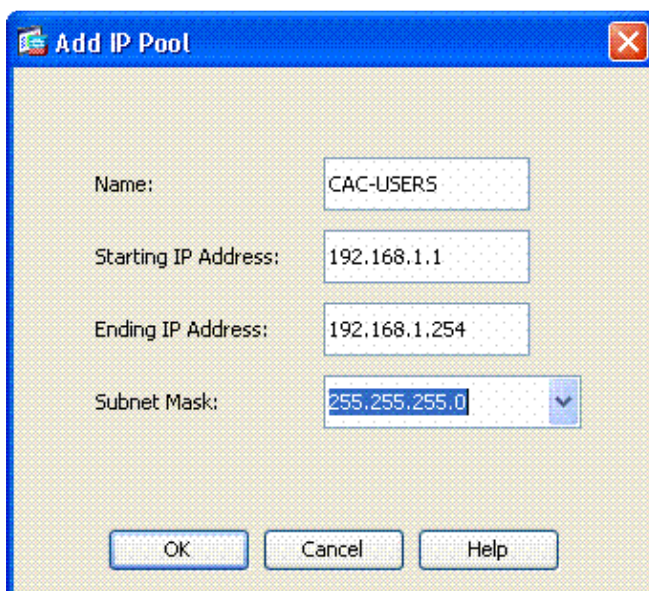
Note: Click the **SAVE** button to save the configuration in flash memory.

VPN Configuration

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

1. Go to **Configuration > VPN > IP Address Management > IP Pools**.
2. Click **Add**.
3. In the Add IP Pool window, enter the name of the IP pool, starting and ending IP addresses, and choose a subnet mask. See Figure 10.

Figure 10: Add IP Pool



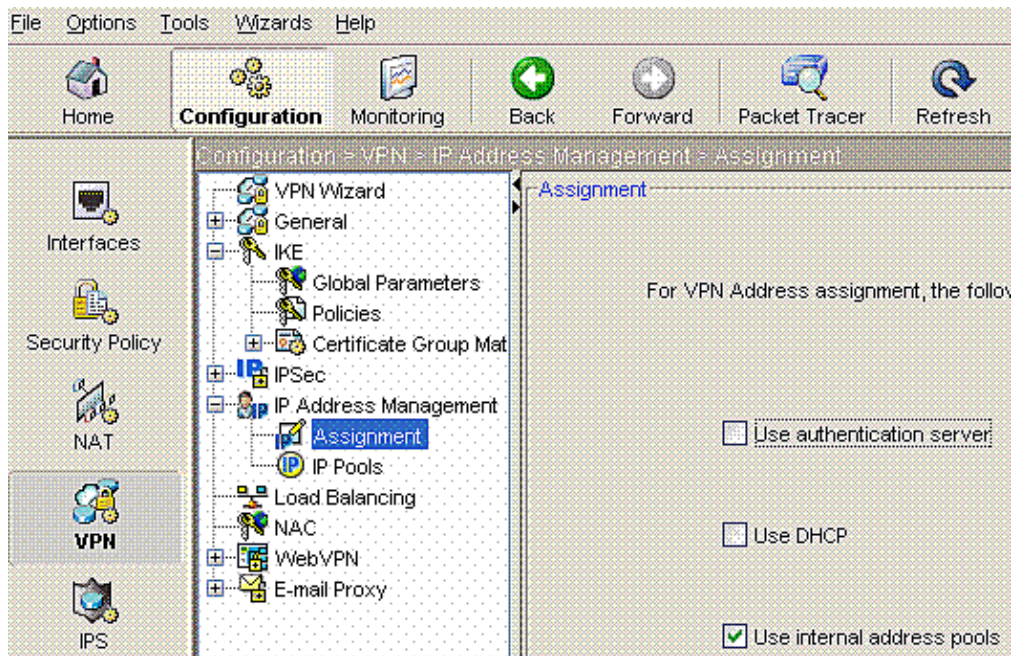
The screenshot shows a dialog box titled "Add IP Pool". It contains the following fields and values:

Field	Value
Name	CAC-USERS
Starting IP Address	192.168.1.1
Ending IP Address	192.168.1.254
Subnet Mask	255.255.255.0

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

4. Click **OK**.
5. Go to **Configuration > VPN > IP Address Management > Assignment**.
6. Choose the appropriate IP address assignment method. This guide uses the internal address pools. See Figure 11.

Figure 11: IP Address Assignment Method



7. Click **Apply**.

Create Tunnel Group and Group Policy

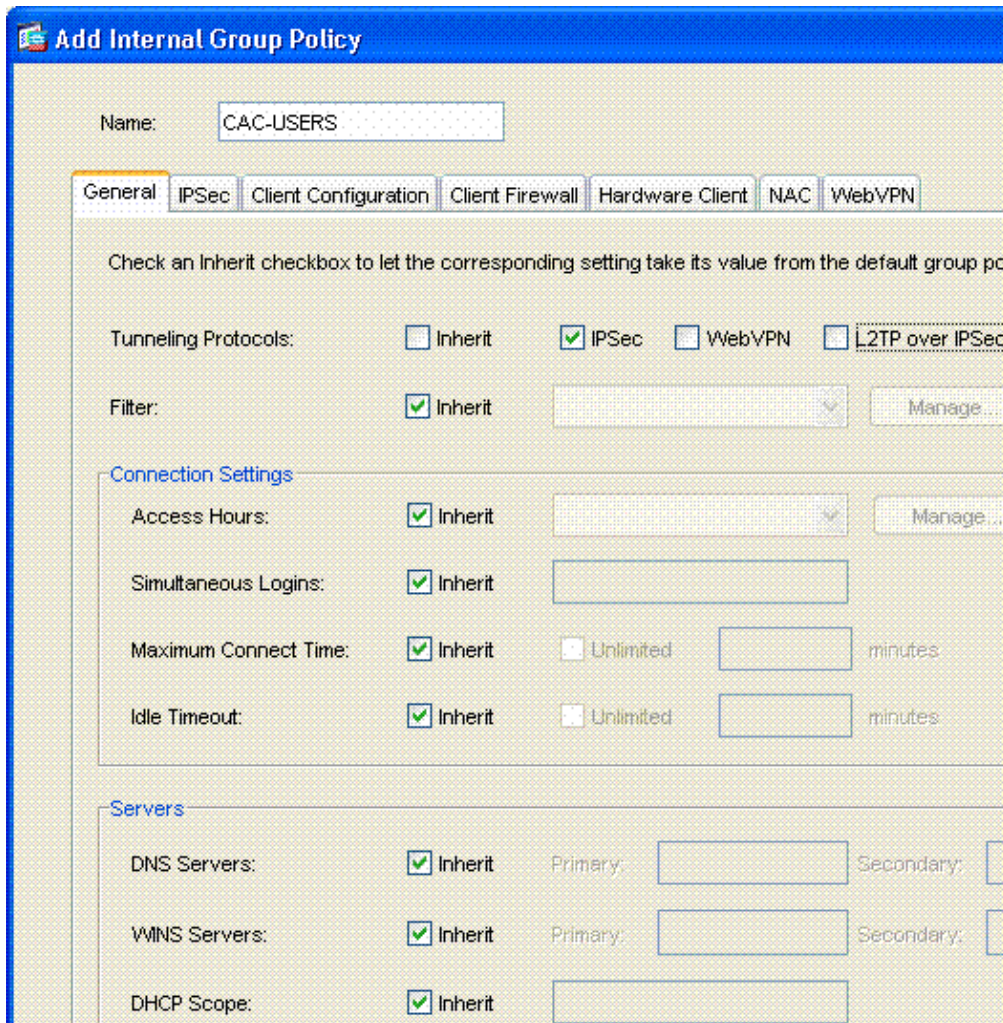
Note: Before you create a tunnel group and group policy, go to **Configuration > VPN > General > VPN System Options** and make sure that the box is checked for the **Enable inbound IPSEC** option.

Group Policy

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

1. Go to **Configuration > VPN > General > Group Policy**.
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 12.

Figure 12: Add Internal Group Policy



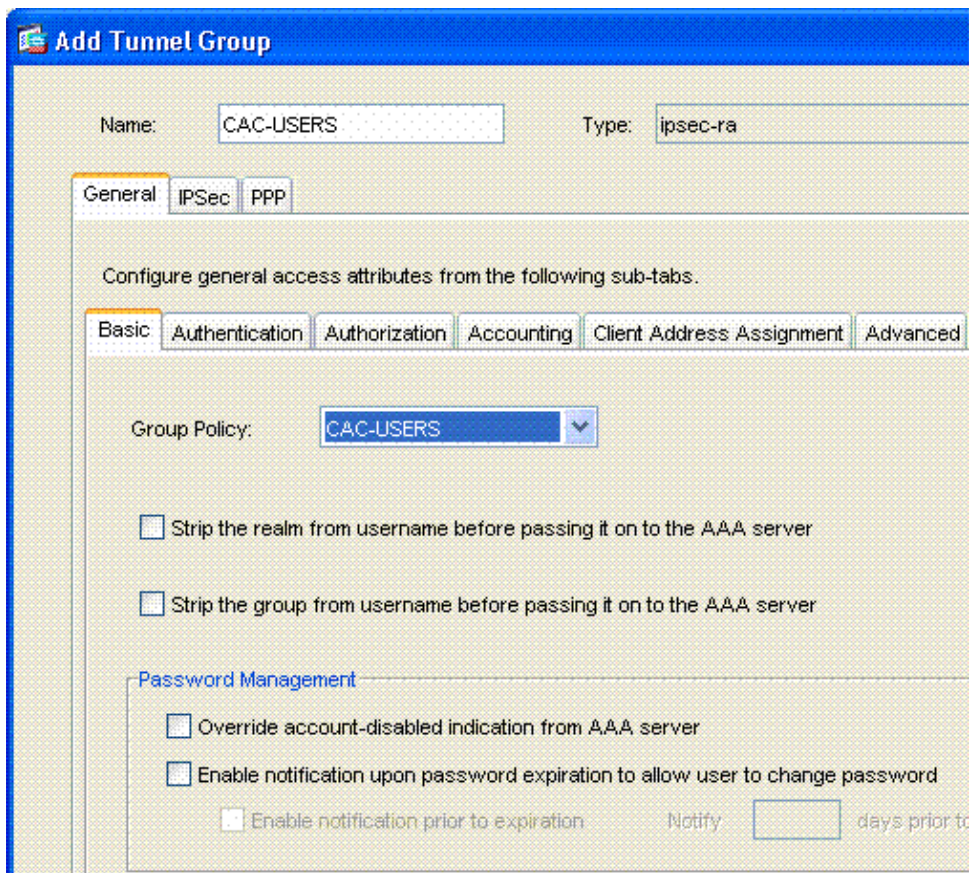
- a. In the General tab, choose the **IPsec** in the Tunneling Protocols option.
 - b. In the Servers section, uncheck the **Inherit** check box and enter the IP address of DNS and WINS servers. Enter the DHCP scope, if applicable.
 - c. In the IPsec tab, leave them all in the default settings: **Inherit**. Make any appropriate changes, if necessary.
 - d. In the Client configuration tab, in General Client Parameters, uncheck the **Inherit** check box in the Default Domain, and enter the appropriate domain name.
 - e. In the Client configuration tab, in General Client Parameters, uncheck the **Inherit** check box in the Address Pool section and add the address pool created in the previous step. Click the name of the address pool, and then click **Add**. If you use another method of IP address assignment, leave this as **Inherit**, and make the appropriate change.
 - f. All other configuration tab are left at the default settings.
4. Click **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. Go to **Configuration > VPN > General > Tunnel Group**. See Figure 13.

Figure 13: Add Tunnel Group



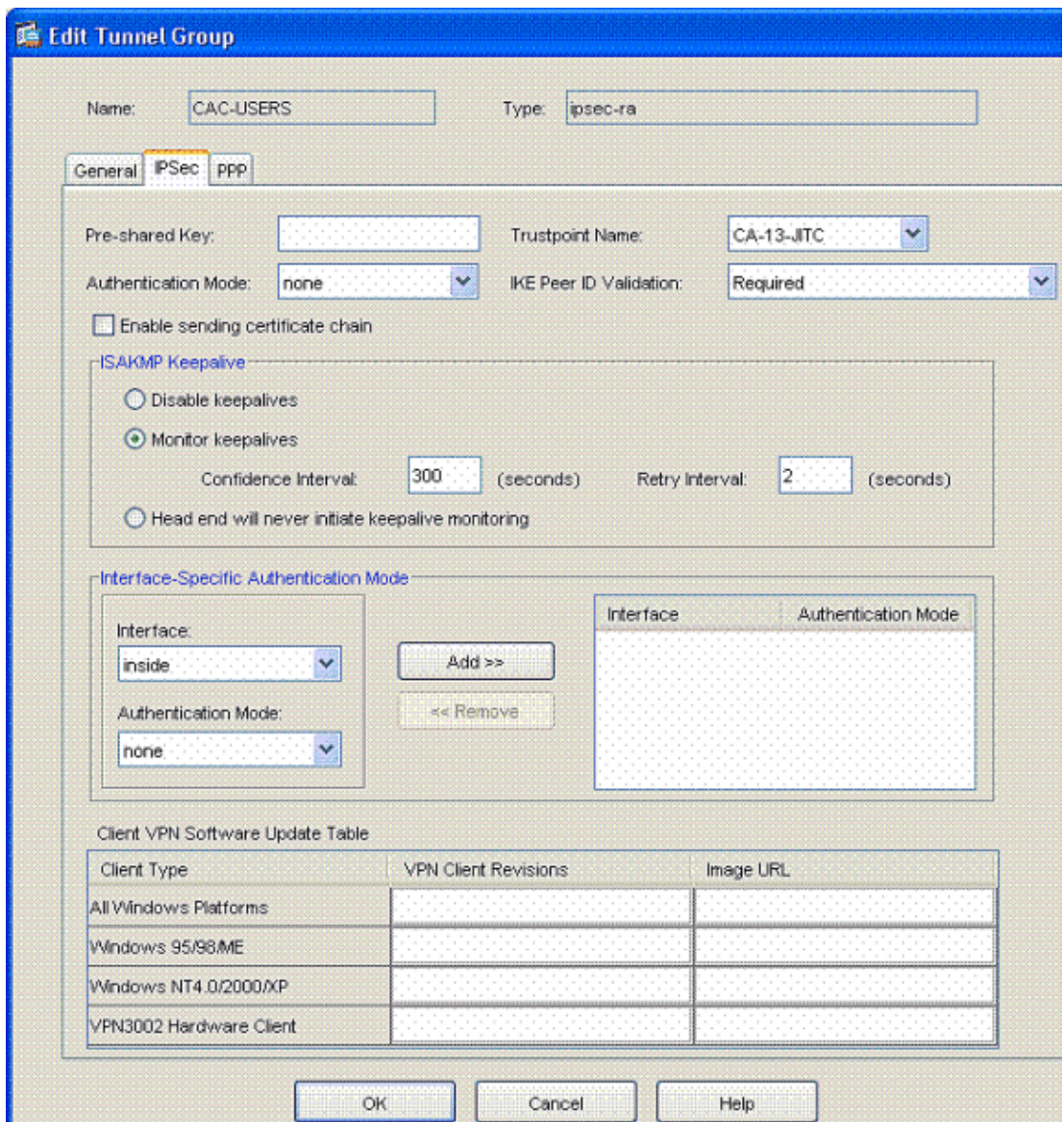
Note: ASDM automatically configures local as the option for authentication if none is chosen. You see a message when you hit OK at the end of this configuration.

```
ERROR: The authentication-server-group none command has been
depreciated.
```

Note: The `isakmp ikev1-user-authentication none` command in the `ipsec-attributes` must be used instead. Set the authentication mode to **none**. See Figure 14.

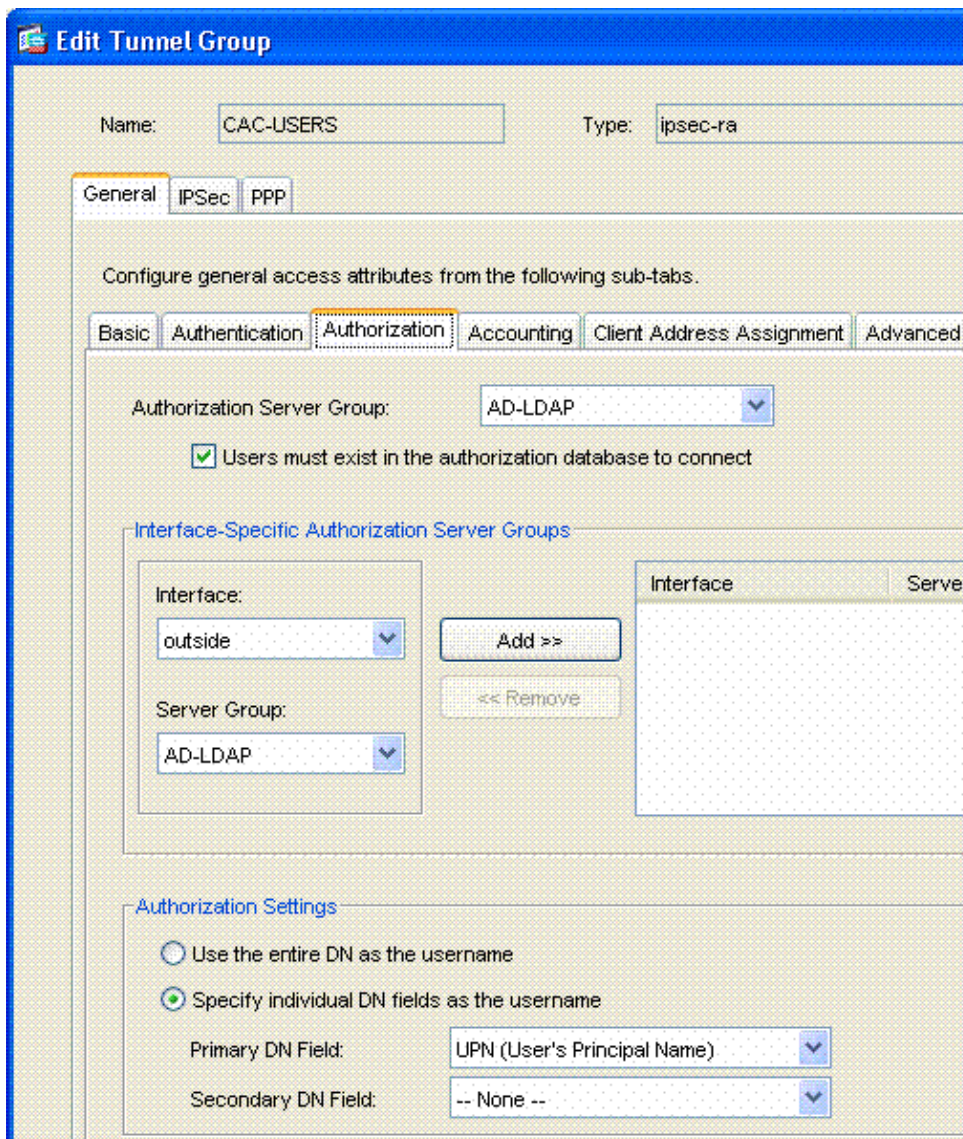
2. Click **Add** and choose IPsec for remote access.
3. In the Add Profile window, enter a name for the tunnel group in the Name text box.
4. In the Add Tunnel Group window, choose the **General tab > Basic tab**, and choose the group policy created in the previous step.
5. Click the **Authentication tab**, and leave everything at the default options.
6. In the Add Tunnel Group window, click the **IPSec tab**.

Figure 14: IPsec Authentication Mode



7. In the Trustpoint Name option, choose the trustpoint created in the previous section.
8. Set the Authentication Mode to **none** as mentioned in the note above. See Figure 14.
9. Click **OK**.
10. Click the Authorization tab. In the Authorization Server Group, choose the LDAP server group created in the earlier steps, and check the box for **Users must exist in authorization database to connect**.

Figure 15: UPN Configuration



11. Choose the **UPN** in the Primary DN Field and **None** in the Secondary DN Field. See Figure 15.
12. Click **OK**.

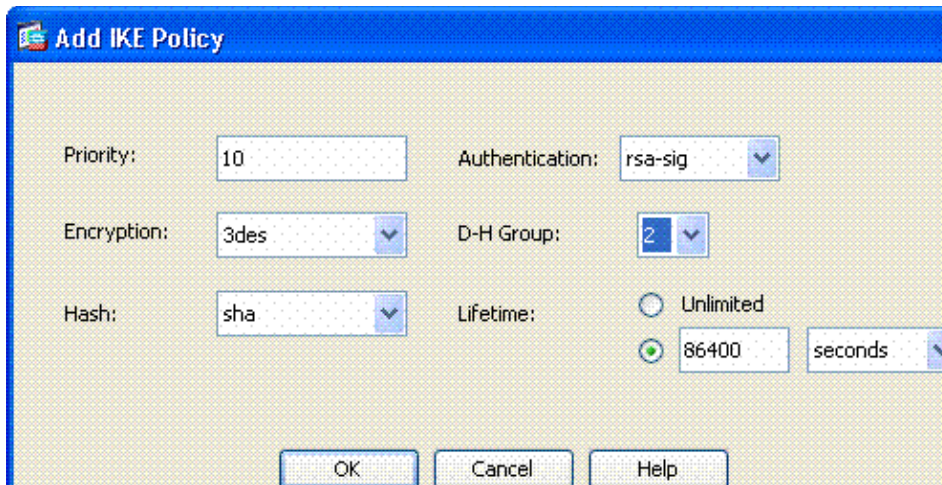
Note: Click the **Save** button to save the configuration in flash memory.

Configure IKE/ISAKMP Parameters

Follow these instructions:

1. Go to **Configuration > VPN > IKE > Global Parameters**.
2. In the Enable IKE section, make sure that the outside interface shows **YES** in the enabled column. If not, highlight the outside interface, click **Enable**, and leave everything else as default.
3. Go to **Configuration > IKE > Policies**.
4. Click **Add**. Enter **10** for the priority number, choose **3DES** for encryption, **sha** for hash, **rsa-sig** for authentication, and **2** for the DH-group; leave the lifetime at default. See Figure 16 for an example.
5. Click **OK**.

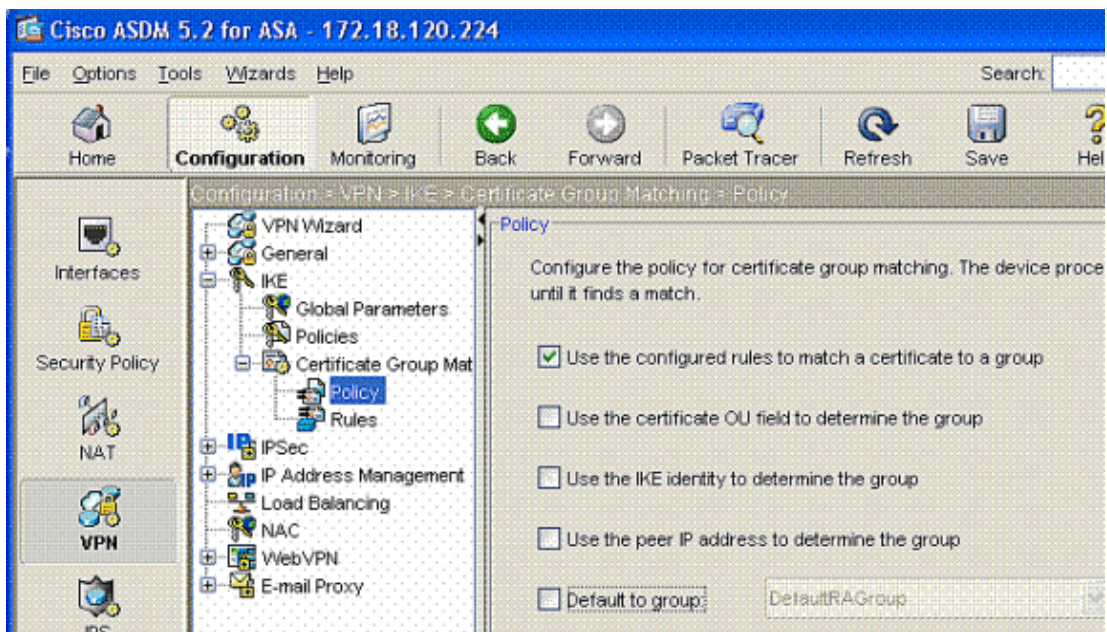
Figure 16: Add IKE/ISAKMP Policy



Note: You can add multiple IKE/ISAKMP policies, if needed.

6. Go to **Configuration > VPN > IKE > Certificate Group Matching > Policy**. See Figure 17.
7. In the policy section, uncheck all check boxes except for **Use the configured rules to match a certificate to a group**.
8. Go to **Configuration > VPN > IKE > Certificate Group Matching > Rules**.
9. Click **Add** on the top table.

Figure 17: Certificate Group Matching Policy



10. In the **Add Certificate Matching Rule** window, follow these instructions:

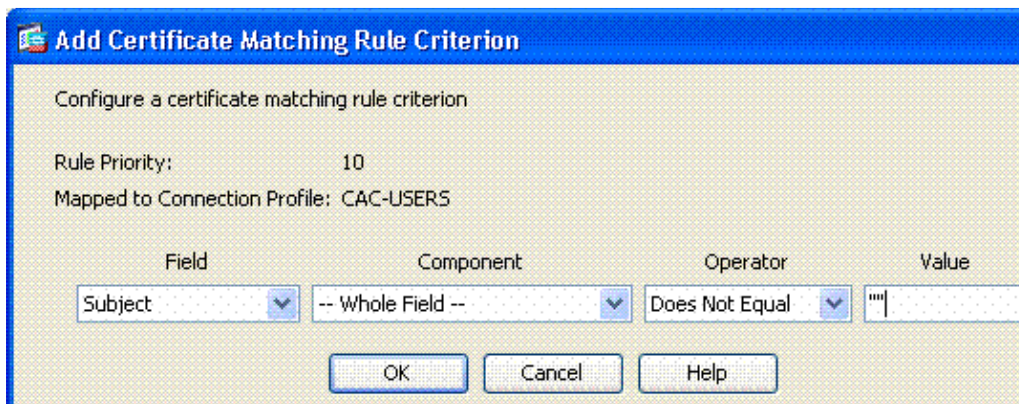
- a. Keep the existing map **DefaultCertificateMap** in the map section.
- b. Keep **10** as the rule priority.
- c. Under the mapped group, choose the tunnel group created in the earlier section when you click the down radio button. See Figure 18.
- d. Click **OK**.

Figure 18: Add Certificate Matching Rule



11. Click **Add** on the bottom table.
12. In the Add Certificate Matching Rule Criterion window, follow these instructions:

Figure 19: Certificate Matching Rule Criterion



- a. Keep the Field column set to **Subject**.
- b. Keep the Component column set to **Whole Field**.
- c. Change the Operator column to **Does Not Equal**.
- d. In the Value column, enter two double quotes (").
- e. Click **OK** and **Apply**. See Figure 19 for an example.

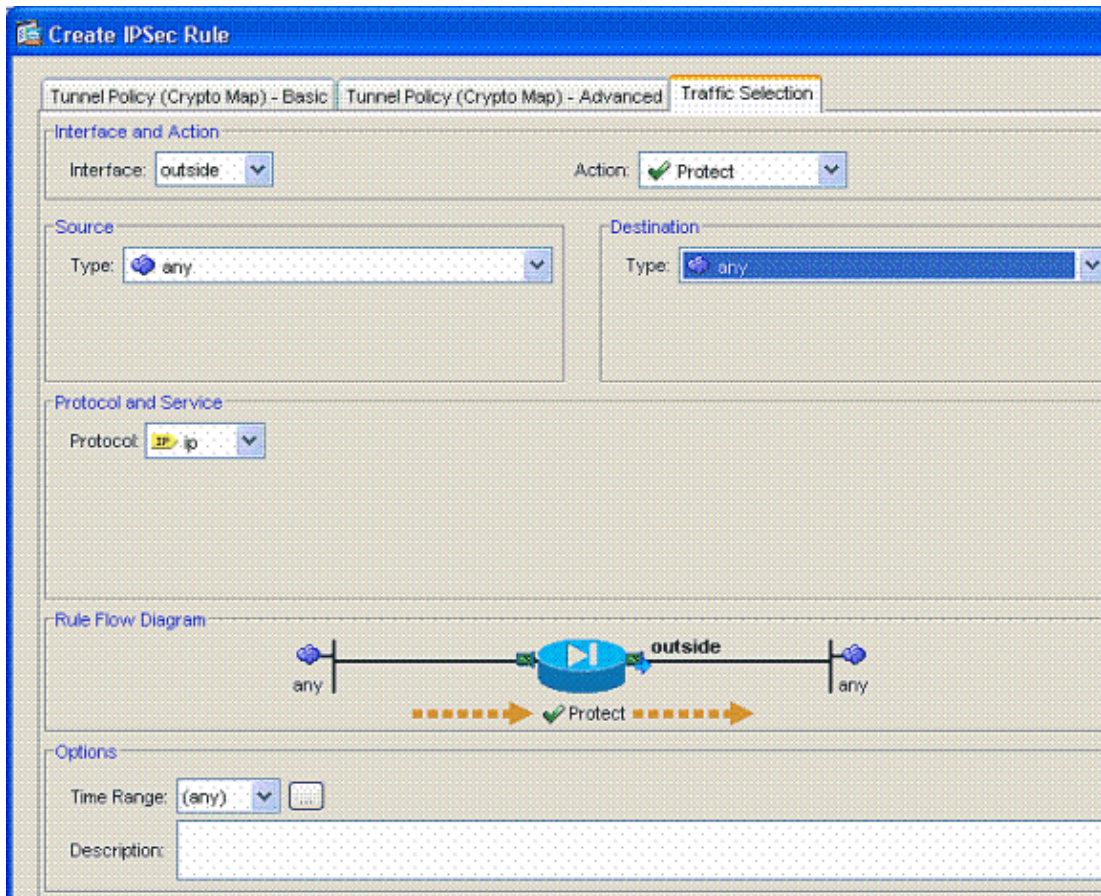
Configure IPSec Parameters

Follow these instructions:

1. Go to **Configuration > VPN > IPSec > IPSec Rules**.
2. Click **Add**.
3. In the Create IPSec Rule window, in the Basic tab, follow these instructions:
 - a. Choose **outside** for the interface.
 - b. Choose **dynamic** for the policy type.
 - c. Enter a priority number.
 - d. Choose a transform-set and click **Add**. This guide uses ESP-AES-256-SHA. You can add multiple transform-set, if needed.
4. Click the **Traffic Selection** tab.
5. In the Interface and Action section, choose **outside** for the Interface and **Protect** for the Action.
6. In the Source section, choose **any**.

7. In the Destination section, choose the IP address of the pool created earlier or **any**.
8. Click **OK**.
9. Click **Apply**.

Figure 20: Add IPsec Rule



Configure OCSP

Configure OCSP Responder Certificate

The OCSP configuration can vary dependent upon the OCSP responder vendor. Read the manual of the vendor for more information.

1. Obtain a self-generated certificate from the OCSP responder.
2. Follow the procedures mentioned previously and install a certificate for the OCSP server.

Note: Make sure that revocation-check is set to **none**. OCSP checks do not need to happen on the actual OCSP server.

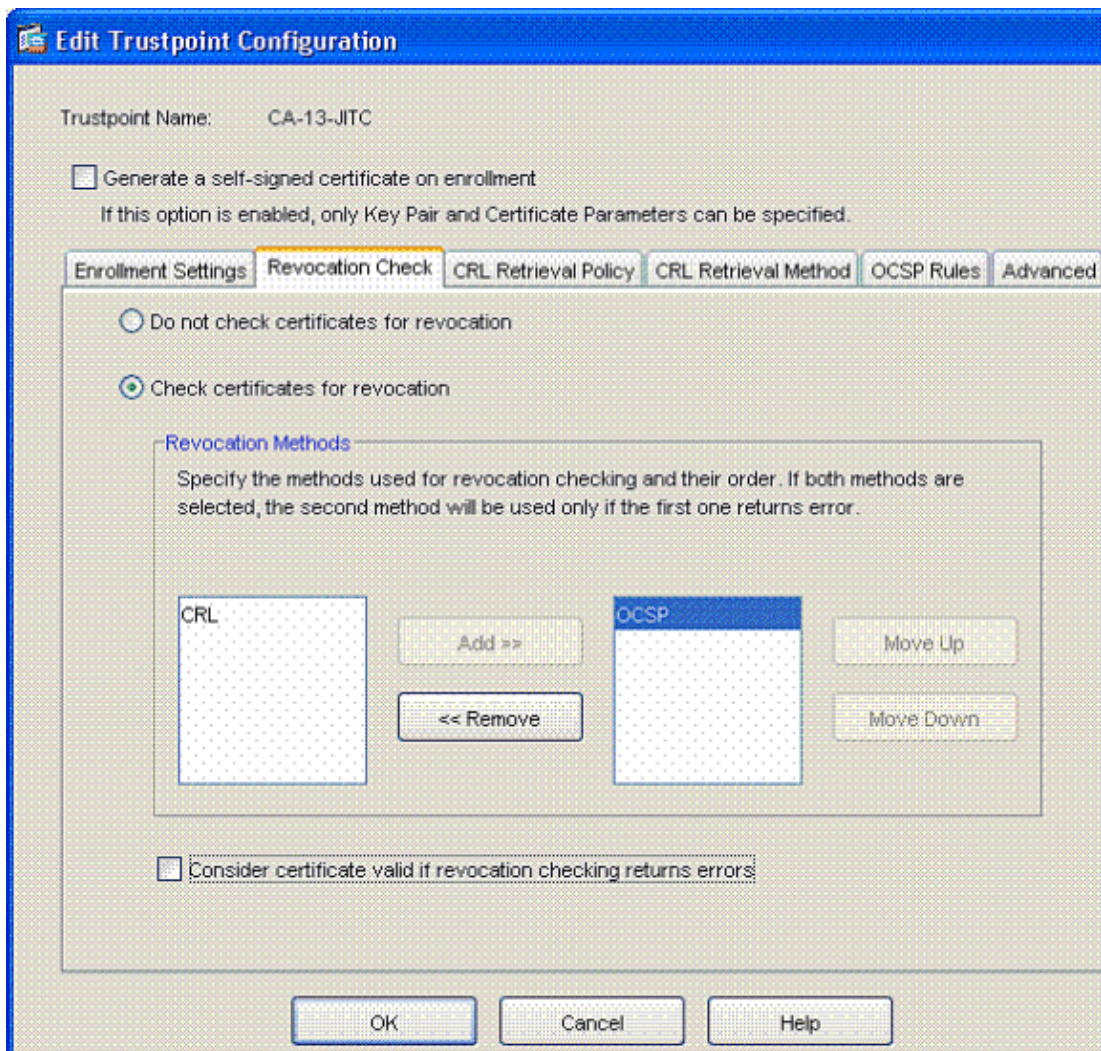
Configure CA to Use OCSP

Follow these instructions:

1. Go to **Configuration > Properties > Certificate > Trustpoint > Configuration**.
2. Choose a CA to configure in order to use OCSP when you highlight it in the table.
3. Click **Edit**.

4. Click the Revocation Check tab, highlight the OCSP in the Revocation Method, and then click **Add**. In the Revocation Methods section, add **OCSP**. See Figure 21.
5. Ensure that the **Consider Certificate valid&cannot be retrieved** is unchecked if you want to follow strict OCSP checking.

Figure 21: OCSP Revocation Check



Note: Configure/edit all the CA servers that use OCSP for revocation.

6. Leave all the default options in these tabs: CRL Retrieval Policy, CRL Retrieval Method, and OCSP Rules.
7. Click the **Advanced** tab.
 - a. Uncheck the **Enforce Next CRL Update** in the CRL options.
 - b. Leave the **Disable nonce extension** unchecked.
 - c. Leave all other options checked.
8. Click **OK**.

Configure OCSP Rules

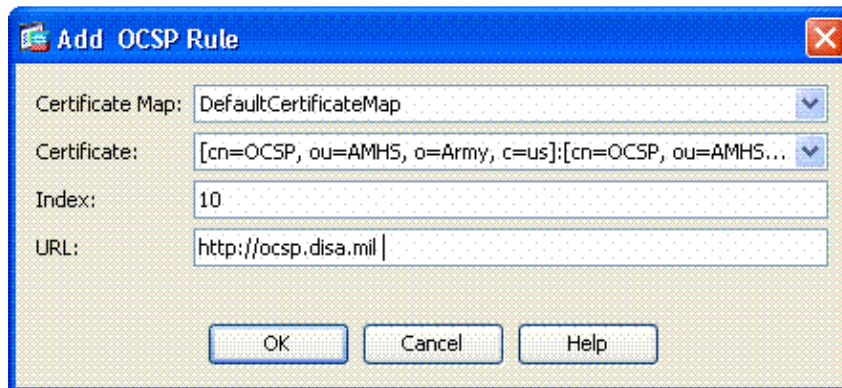
Note: Verify that a Certificate Group Matching Policy is created and the OCSP responder is configured before you follow these procedures.

Note: Make sure that all CAs are configured with the OCSP rules except for the OCSP server itself.

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

1. Go to **Configuration > Properties > Certificate > Trustpoint > Configuration**.
2. Choose a trustpoint to configure in order to use OCSP when you highlight it in the table.
3. Click **Edit**.
4. Click the **OCSP Rule** tab.
5. Click **Add**.
6. In the Add OCSP Rule window, follow these instructions: See Figure 22.

Figure 22: Add OCSP Rules



- a. In the Certificate Map option, choose the map created in the IKE/ISAKMP parameters section: **DefaultCertificateMap**.
- b. In the Certificate option, choose the **OCSP responder**.
- c. In the index option, enter **10**.
- d. In the URL option, enter the **IP address** or the **hostname** of the OCSP responder. If you use the hostname, make sure that the DNS server is configured on ASA.)
- e. Click **OK**.
- f. Click **Apply**.

Cisco VPN Client Configuration

This section covers the configuration of the Cisco VPN client.

Assumptions: The Cisco VPN Client and middleware application are already installed in the host PC. The Cisco VPN client supports these middleware applications: GemPLUS (GemSAFE Workstation 2.0 or later), Activcard (Activcard Gold Version 2.0.1 or later), and Aladdin (eToken Runtime Environment (RTE) Version 2.6 or later).

Start Cisco VPN Client

From the host PC, click **Start > Programs > Cisco Systems VPN Client > VPN Client**.

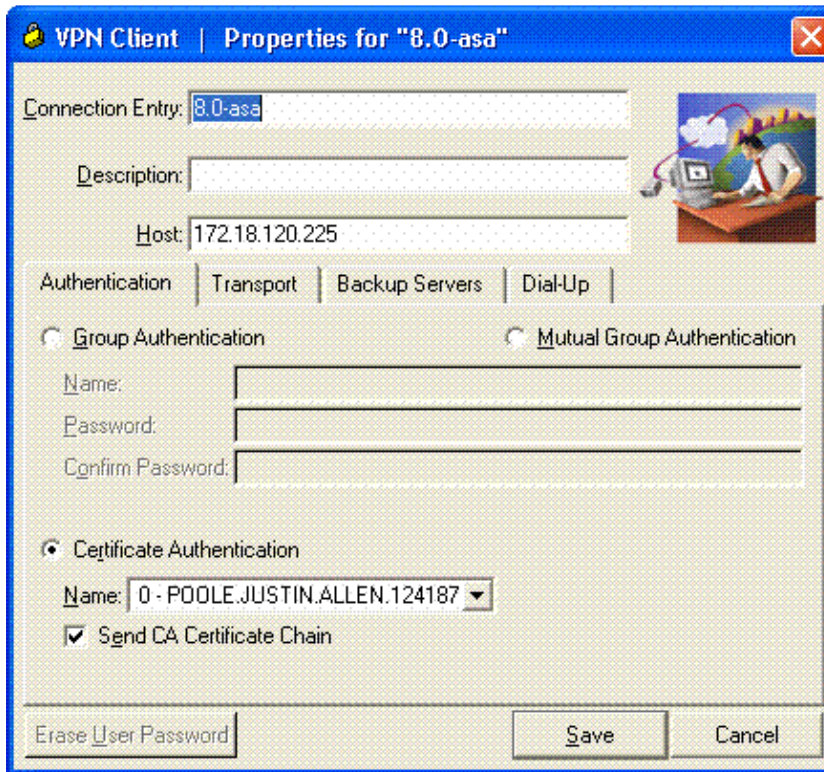
New Connection

Follow these instructions:

1. Click **Connection Entries**.
2. Click **New** and then enter the description of the connection and IP address or hostname of the VPN server. See Figure 23.

3. Under the Authentication tab, choose **Certificate Authentication**.
4. In the Name option, choose your signature certificate and check **Send CA Certificate Chain**.
(Usually the default certificate that is chosen works, but you can try the other certificates if it fails.)
5. Click **Save**.

Figure 23: Create New VPN Connection



Start Remote Access

Follow these instructions:

1. Double-click the entry created in the previous step.
2. Enter your PIN number.
3. Click **OK**.

Appendix A LDAP Mapping

With ASA/PIX release 7.1(x), 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. Below are examples of LDAP mapping. Be aware that you need administrator rights to make changes in the AD/LDAP server.

Scenario 1: Active Directory Enforcement with Remote Access Permission Dial-in Allow/Deny Access

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

- The AD attribute value: TRUE = Allow; FALSE = Deny

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

For ALLOW condition, we map

- TRUE = 20

For DENY dial-in condition, we map

- FALSE = 1

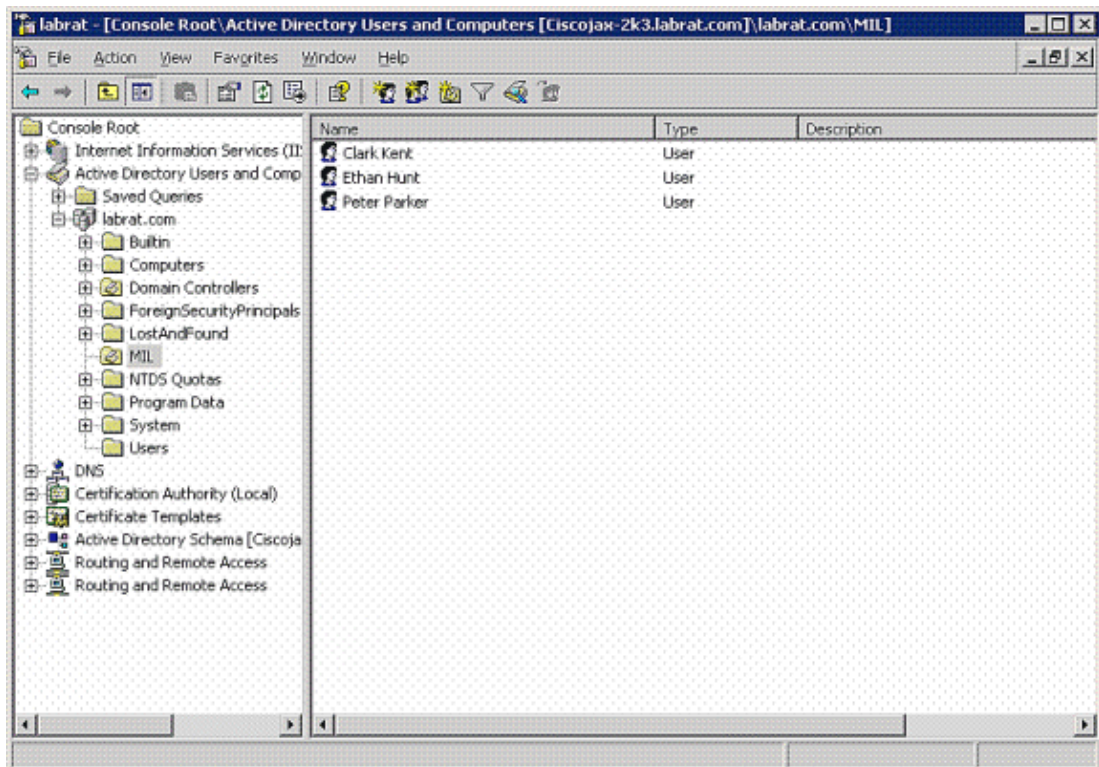
Note: Make sure that TRUE and FALSE are in all caps. For more information on the Cisco attributes, refer to Configuring an External Server for Security Appliance User Authorization.

Active Directory Setup

Follow these instructions:

1. In the Active Directory Server, click **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** to expand the Active Directory Users and Computers.
4. Click the **plus sign** to expand the domain name.
5. If you have an OU created for your users, expand the OU to view all users; if you have all users assigned in the Users folder, expand that folder to view them. See Figure A1.

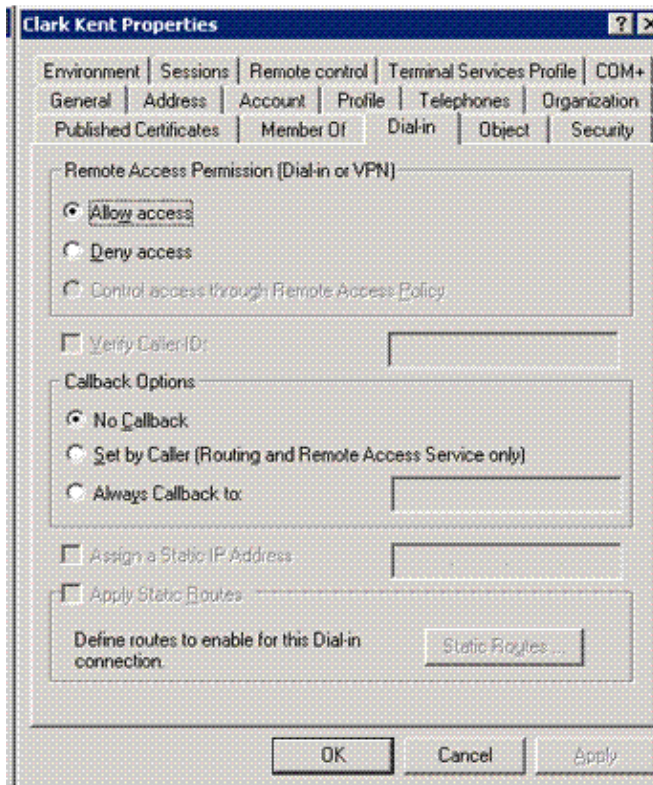
Figure A1: Active Directory Management Console



6. Double-click the user that you want to edit.

Click the **Dial-in** tab in the user properties page and click **allow** or **deny**. See Figure A2.

Figure A2: User Properties



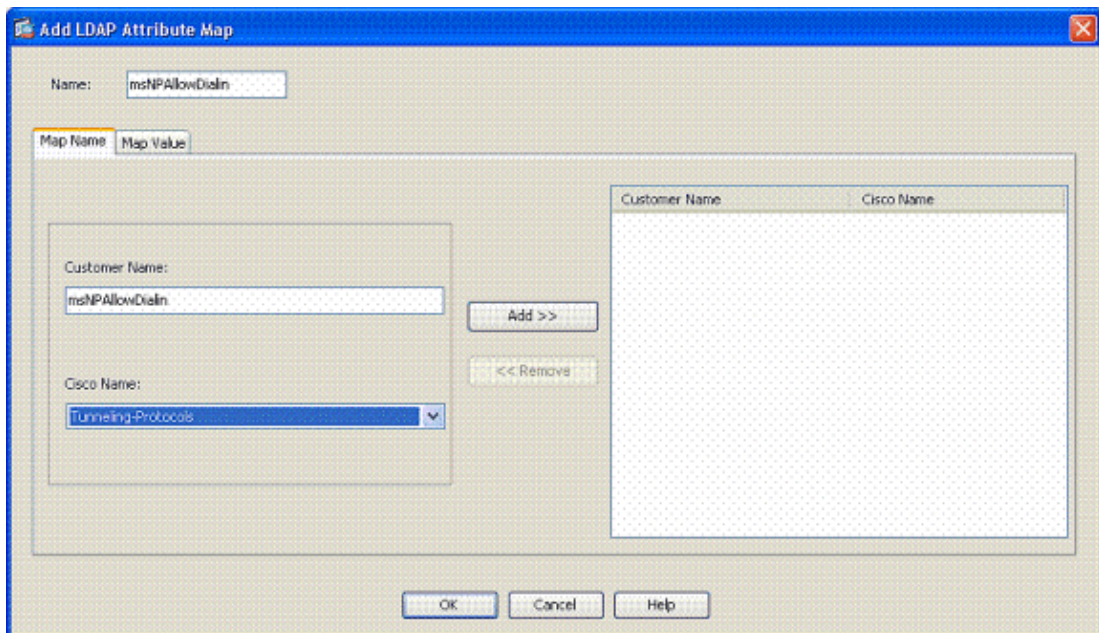
7. Click **OK**.

ASA Configuration

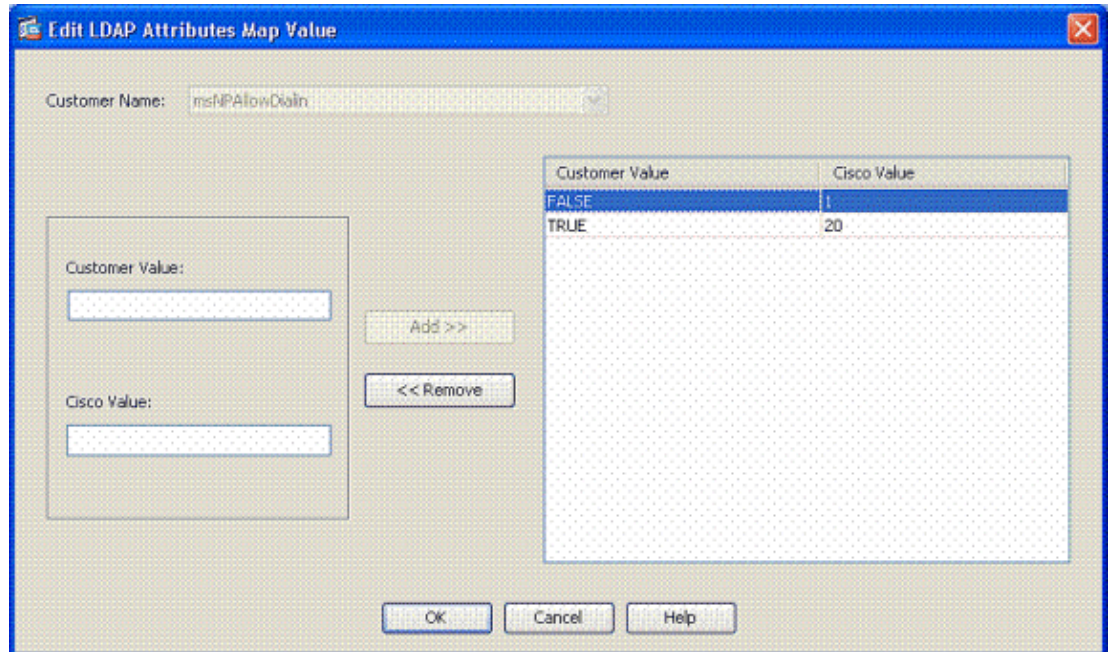
Follow these instructions:

1. In ASDM, go to **Configuration > Properties > AAA > LDAP Attribute Map**.
2. Click **Add**.
3. In the Add LDAP Attribute Map window, follow these instructions: See Figure A3.

Figure A3: Add LDAP Attribute Map

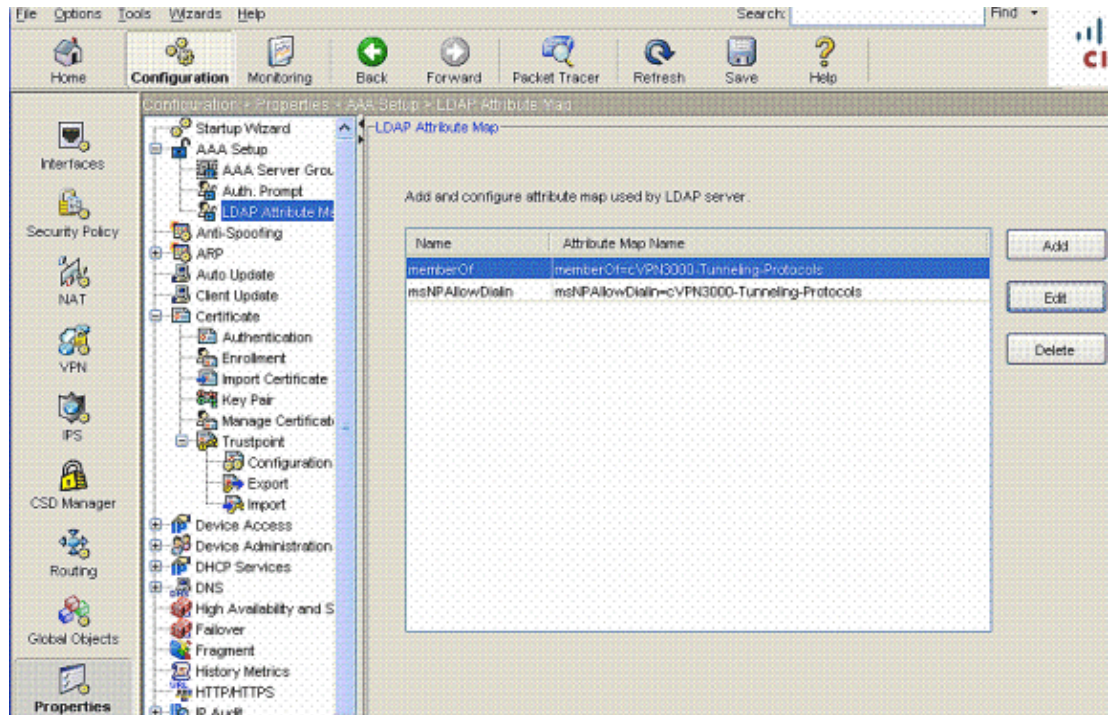


- a. Enter a name in the Name text box.
- b. In the Map Name tab, type **msNPAllowDialin** in the Customer Name text box.
- c. In the Map Name tab, choose **Tunneling-Protocols** in the drop-down option in the Cisco Name.
- d. Click **Add**.
- e. Click the **Map Value** tab.
- f. Click **Add**.
- g. 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.
- h. Click **Add**.
- i. Type **FALSE** in the Customer Name text box, and type **1** in the Cisco Value text box. See Figure A4.



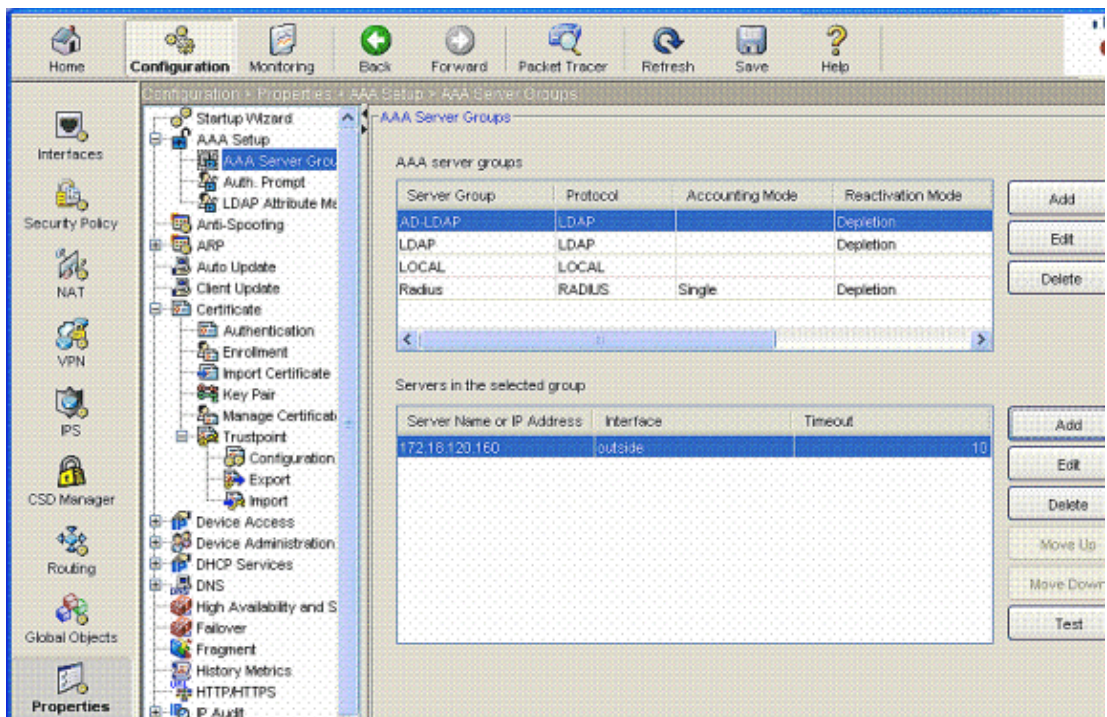
- j. Click **OK**.
- k. Click **OK**.
- l. Click **APPLY**.
- m. The configuration looks like Figure A5.

Figure A5: LDAP Attribute Map Configuration



4. Go to **Configuration > Properties > AAA Setup > AAA Server Groups**. See Figure A6.

Figure A6: AAA Server Groups



5. Click the server group that you want to edit. In the Servers of 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 button. See Figure A7.

Figure A7: Add LDAP Attribute Map

7. Click **OK**.

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

Scenario 2 : Active Directory Enforcement with Group Membership to Allow/Deny Access

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

- Use an existent group or create a new group for ASA VPN users for ALLOW conditions.
- Use an existent group or create a new group for non-ASA users for DENY conditions.
- Make sure to check in the LDAP viewer that you have the correct 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 at the top of the list. The other option is to put a special character in front of the name since AD looks at special characters first. In order to get around this caveat, use DAP in 8.x software to look at multiple groups.

Note: Make sure that 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 existent group name or new group name contains a space, enter the attribute in this manner: CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org .

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 the **ALLOW** condition, map

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

For the **DENY** condition, map

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

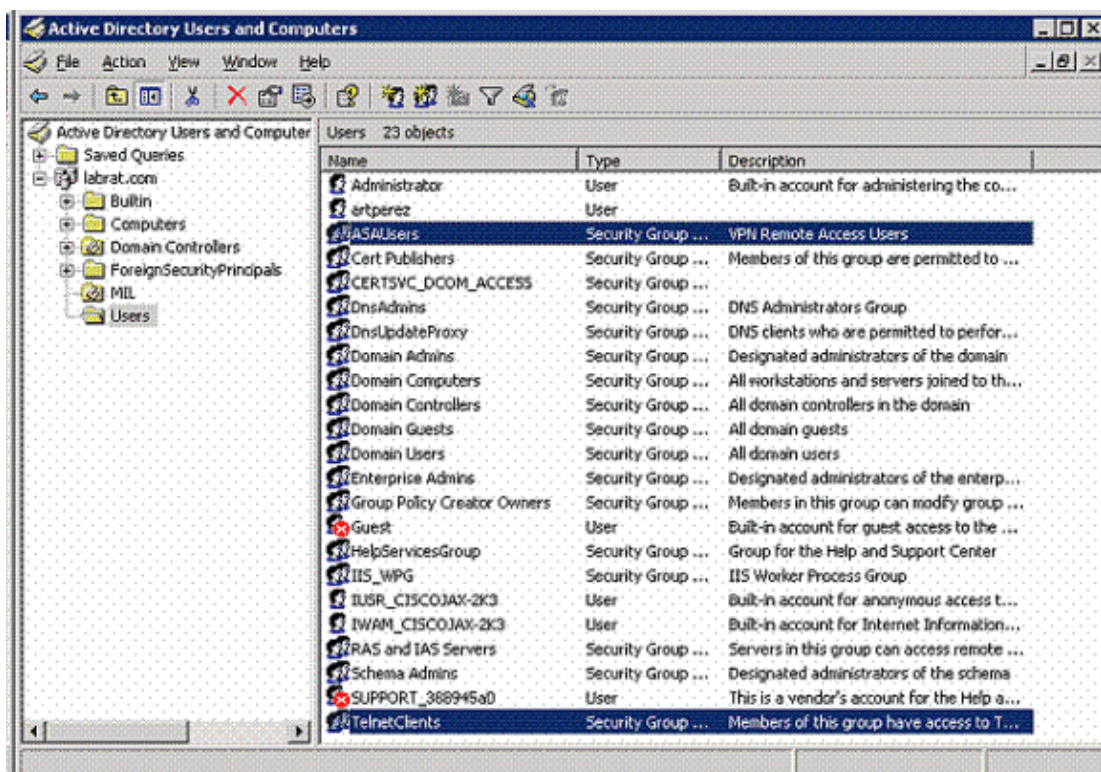
Note: In a future release, there is a Cisco attribute to allow and deny connection. For more information on the Cisco attribute, refer to Configuring an External Server for Security Appliance User Authorization.

Active Directory Setup

Follow these instructions:

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

Figure A8: Active Directory Groups



4. Click the **plus sign** to expand the domain name.

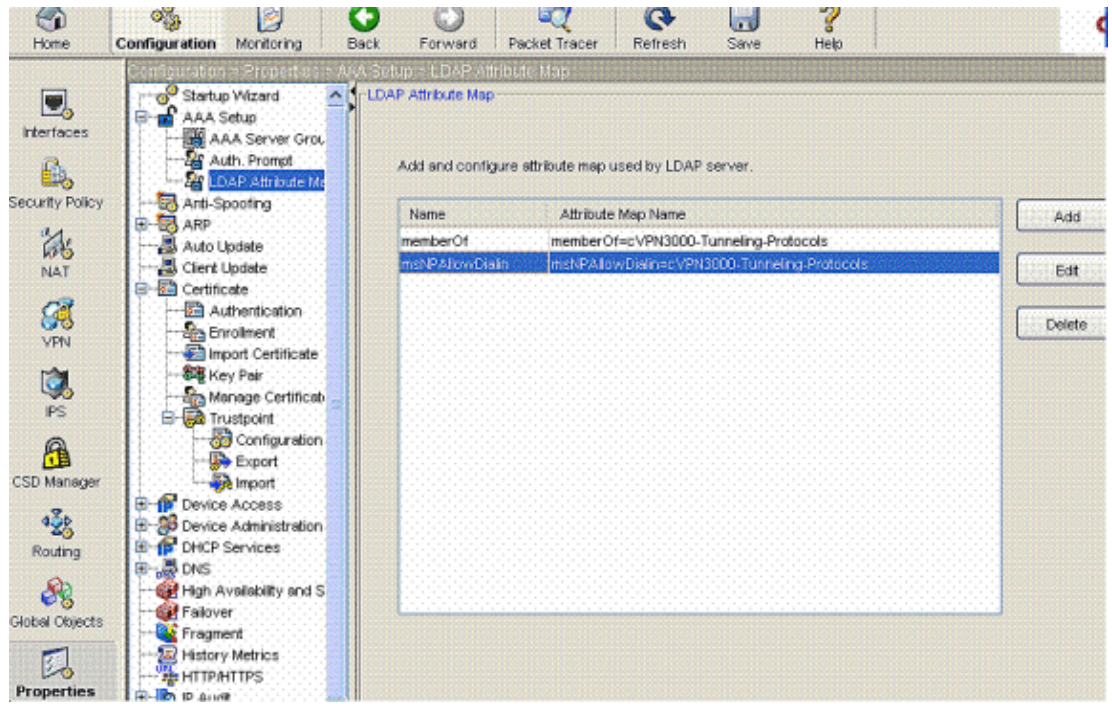
5. Right-click the Users folder and choose **New > Group**.
6. Enter a Group Name, for example: ASAUsers.
7. Click **OK**.
8. Click the **Users** folder, and then double-click the group that you just created.
9. Click the **Members** tab, and then click **Add**.
10. Type the name of the user you want to add, and then click **OK**.

ASA Configuration

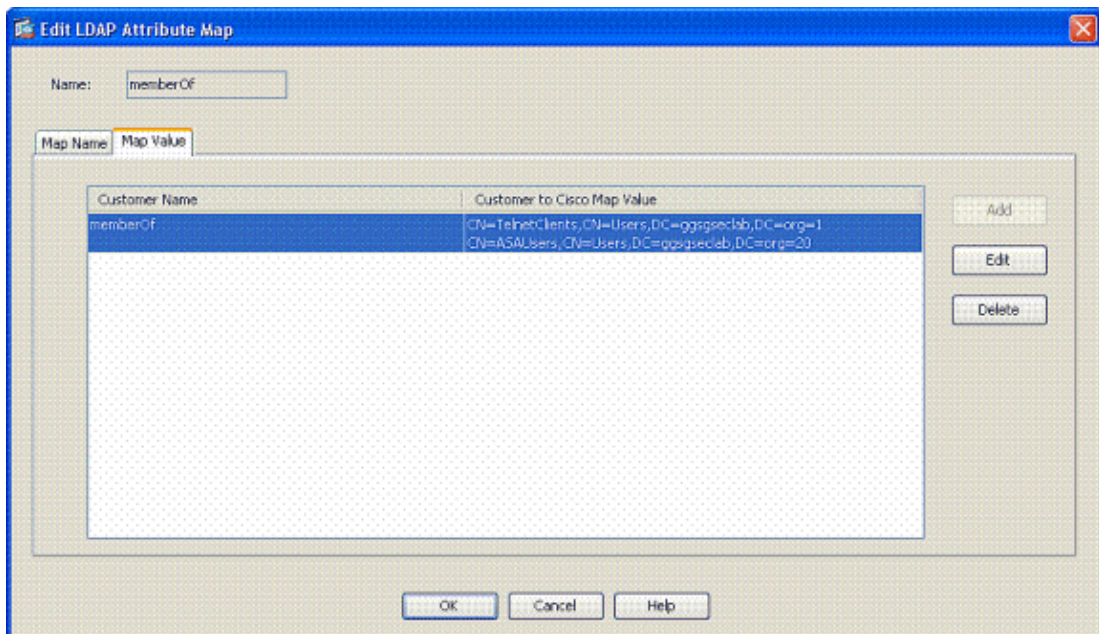
Follow these instructions:

1. In ASDM, go to **Configuration > Properties > AAA > LDAP Attribute Map**.
2. Click **Add**.
3. In the Add LDAP Attribute Map window, follow these instructions: See Figure A9.
 - a. Enter a name in the Name text box.
 - b. In the Map Name tab, type **memberOf** in the Customer Name text box c.
 - c. In the Map Name tab, choose **Tunneling-Protocols** in the drop-down option in the Cisco Name.
 - d. Click **Add**.
 - e. Click the **Map Value** tab.
 - f. Click **Add**.
 - g. 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.
 - h. Click **Add**.
 - i. 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 A9.
 - j. Click **OK**.
 - k. Click **OK**.
 - l. Click **Apply**.
 - m. The configuration looks like Figure A9.

Figure A9: LDAP Attribute Map



4. Go to **Configuration > Properties > AAA Setup > AAA Server Groups**.
5. Click the server group that you want to edit. In the Servers of 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 button.
7. Click **OK**.

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

Appendix B ASA CLI Configuration

ASA 5510
<code>ciscoasa#show running-config</code>

```

ASA Version 7.2(2)10
!
hostname lab-asa
domain-name lab.army.mil
names
dns-guard
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.18.120.224 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa722-10-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name lab.army.mil
-----ACL's-----
access-list out extended permit ip any any
-----VPN Pool-----
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
-----
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
asdm image disk0:/asdm522-54.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 -----
ldap attribute-map memberOf
map-name memberOf cVPN3000-Tunneling-Protocols
map-value memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org 20
map-value memberOf CN=TelnetClinets,CN=Users,DC=gsgseclab,DC=org 1
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin cVPN3000-Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
-----LDAP Server-----
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=gsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=gsgseclab,DC=org
-----VPN Policy-----
group-policy CAC-USERS internal
group-policy CAC-USERS attributes
vpn-tunnel-protocol IPSec
address-pools value CAC-USERS
-----
!
-----IPsec-----

```

```
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
    ESP-DES-SHA ESP-3DES-MD5 ESP-AES-192-SHA ESP-AES-256-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

-----CA Trustpoints-----

```
crypto ca trustpoint CA-13-JITC
revocation-check ocs
enrollment terminal
fqdn none
subject-name CN=lab-asa,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override
    ocs trustpoint DISA-OCSP 10 url http://ocs.disa.mil
crl configure
no enforcenextupdate
crypto ca trustpoint Class3Root
revocation-check ocs
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override
    ocs trustpoint DISA-OCSP 10 url http://ocs.disa.mil
crl configure
no enforcenextupdate
crypto ca trustpoint DoD-CA2
revocation-check ocs
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override
    ocs trustpoint DISA-OCSP 10 url http://ocs.disa.mil
crl configure
no enforcenextupdate
crypto ca trustpoint DISA-OCSP
enrollment terminal
keypair DoD-1024
crl configure
no enforcenextupdate
```

-----Certificate Map-----

```
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
```

-----CA Certificates (Partial Cert is Shown)-----

```
crypto ca certificate chain CA-13-JITC
certificate 311d
308203fd 30820366 a0030201 02020231 1d300d06 092a8648 86f70d01 01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101 05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f
crypto ca certificate chain Class3Root
certificate ca 04
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101 05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f
crypto ca certificate chain DoD-CA2
certificate ca 05
```

```

30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101 05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53 2e20476f
c3ad60a4
crypto ca certificate chain DISA-OCSP
certificate ca 00
30820219 30820182 a0030201 02020100 300d0609 2a864886 f70d0101 05050030
3a310b30 09060355 04061302 7573310d 300b0603 55040a13 0441726d 79310d30
-----ISAKMP-----
crypto isakmp enable outside
crypto isakmp policy 10
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp nat-traversal 20
-----VPN Group/Tunnel Policy-----
tunnel-group CAC-USERS type ipsec-ra
tunnel-group CAC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy CAC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group CAC-USERS ipsec-attributes
trust-point CA-13-JITC
isakmp ikev1-user-authentication none
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
tunnel-group-map DefaultCertificateMap 10 CAC-USERS
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
!
service-policy global_policy global
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

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

Note: The tunneling group is configured to allow ONLY IPsec connection. The member grouping/assignment in LDAP is mapped to the value of 4, which is IPsec. This mapping is what gives it an ALLOW condition. For a deny condition, that value is 1 for PPTP.

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@l.0.....&...d....coml.0.....&...d...
[78] userCertificate: value = 0..'0...../..t.....50...*.
H.....0@l.0.....&...d....coml.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=gsgseclab,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 Misconfigured Cisco Attribute Mapping

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

Note that the mapping for both attributes matches the same value, which is incorrect.

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....com1.0.....
&...d...
[82] userCertificate: value =

```

```
0...'0...../..t.....50...*.H.....0@1.0.....&....,d....com1.0.....
&....,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 "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 (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop

```

Troubleshooting Certificate Authority / OSCP

- debug crypto ca 3
- In the configuration mode, logging class ca console (or buffer) debugging

The examples below show a successful certificate validation with the OSCP 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 misconfigured certificate group matching policy.

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

Figure C3: OSCP debugging Successful Certificate Validation

```

CRYPTO_PKI: Attempting to find tunnel group for cert with serial number:
2FB5FC7400000000035,
subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=com, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,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=ggsgseclab,dc=org,
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence # 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 CRYPTO_PKI:Certificate validated.
serial number: 2FB5FC74000000000035, subject name: cn=Ethan Hunt,ou=MIL,
dc=gsgseclab,dc=org.
CRYPTO_PKI: Certificate validated
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: looking for cert in handle=2467668, digest=

```

Figure C4: Output of a failed certificate group matching policy

Figure C4: Output of a Failed Certificate Group Matching Policy

```

CRYPTO_PKI: Attempting to find tunnel group for cert with 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 FAILED.
Peer cert field: = cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org,
map rule: subject-name eq "".
CRYPTO_PKI: Peer cert could not be authorized with map: DefaultCertificateMap.
No Tunnel Group Match for peer certificate.
Unable to locate tunnel group map

```

Figure C5: Output of a Revoked Certificate

```

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=. CMertifiIcLa,teted 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 # 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
```

Troubleshooting IPSEC

- **debug crypto isakmp** displays IKE/ISAKMP negotiation phase
- **debug crypto ipsec** displays IPsec negotiation phase
- **debug crypto engine** displays IPsec messages
- **debug crypto ca messages** displays PKI messages
- **debug crypto ca transactions** displays PKI transactions

Appendix D Verify LDAP Objects in MS

In Microsoft server 2003 CD, there are additional tools that can be installed 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

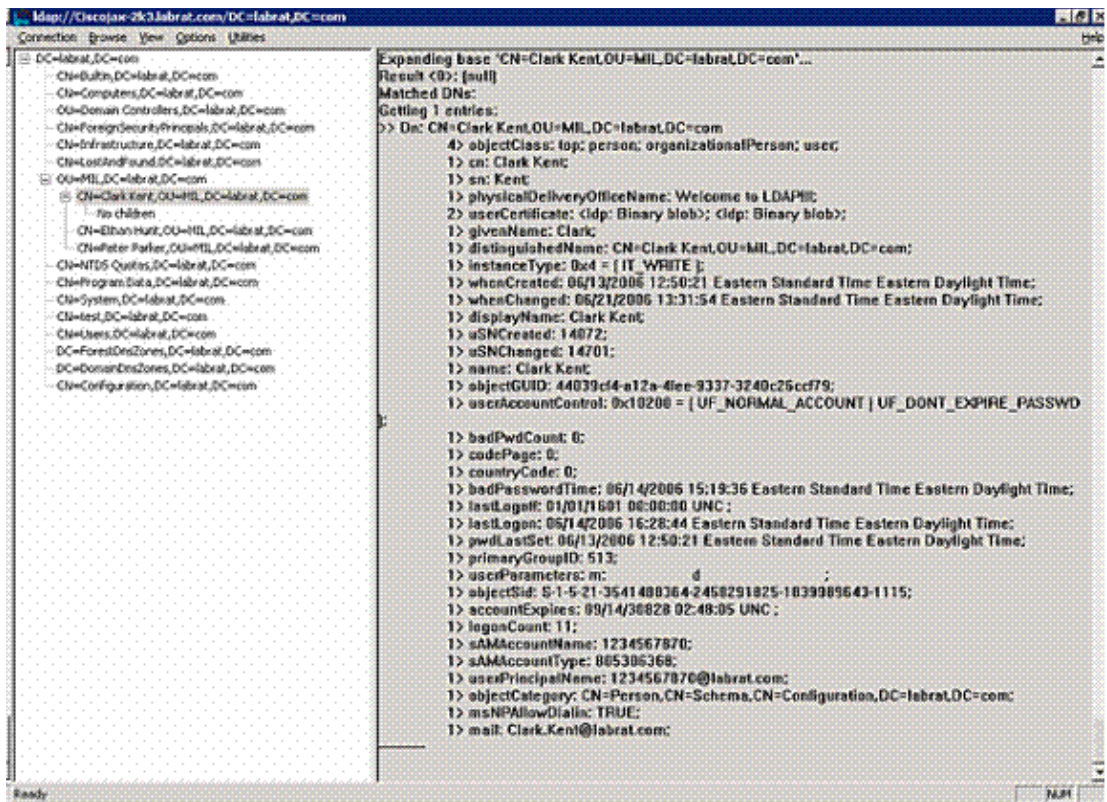
Follow these instructions:

1. After installation, go to **Start > Run**.
2. Type **ldp** and then click **OK**. This starts the LDAP viewer.
3. Click **Connection > Connect**.
4. Enter the server name, and then click **OK**.
5. Click **Connection > Bind**.
6. Enter a username and password.

Note: You need administrator rights.

7. Click **OK**.
8. View LDAP objects. See Figure D1.

Figure D1: LDAP Viewer

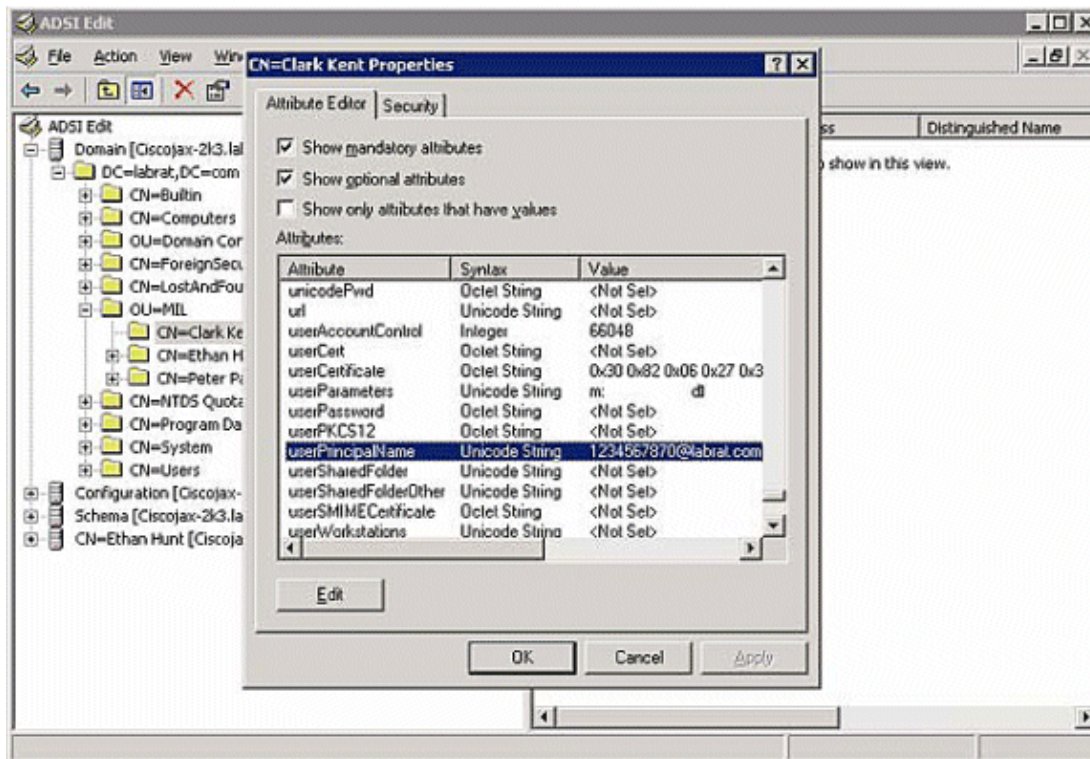


Active Directory Services Interface Editor

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

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

Figure D2: ADSI Edit



Related Information

- [Certificates & CRLs Specified by X.509 and RFC 3280](#)
- [Public Key Infrastructure Introduction](#)
- [OCSP Specified by RFC 2560](#)
- [Lightweight OCSP Profiled by Draft Standard](#)
- [SSL / TLS Specified by RFC 2246](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 02, 2008

Document ID: 107273