PIX/ASA 8.x: CAC – SmartCards Authentication for Cisco VPN Client

Document ID: 107237

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

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 and DAP
  Active Directory Setup
  ASA Configuration
  Scenario 2 : Active Directory Enforcement with 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 Misconfigured Cisco Attribute Mapping
  Troubleshooting DAP
    Example 1: Allowed Connection with DAP
    Example 2: Denied Connection with DAP
  Troubleshooting Certificate Authority / OCSP
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, LDAP attribute maps, and Dynamic Access Polices (DAP).

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 8.0(x) and later
- Cisco Adaptive Security Device Manager (ASDM) Version 6.x for ASA 8.x
- 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, or Dynamic Access Policy (DAP) checks. DoD mandates OCSP checking, but the tunnel works without the OCSP configured.
- The ASA image required is at least 8.0.2 and ASDM 6.0.2.
- 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:

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:** User has to have 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**
We will use this option later on the configuration to add other AD/LDAP object for authorization.

k. Click OK.

6. Click OK.

Manage Certificates

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:

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**

![Add Key Pair](image)

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 Root CA Certificates

Follow these instructions:

2. Choose Install from File and browse to the certificate.
3. Choose Install Certificate.

**Figure 4: Install Root Certificate**

![Install Root Certificate](image)
4. This message appears. 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: Install Root Certificate
Enroll ASA and Install Identity Certificate

Follow these instructions:

2. Choose Add a new identity 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 choose Select Attribute.
5. In the Certificate Subject DN window, enter the information of the device. See Figure 8 for an example.

**Figure 8: Edit DN**
6. Click **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 on **Browse** 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, go to Remote Access VPN > Certificate Management > ID Certificate > Install. See Figure 11.

**Figure 11: Import Identity Certificate**

11. In the Install certificate window, browse to the ID certificate and choose Install Certificate. See Figure 12 for an example.

**Figure 12: Install Identity Certificate**
Note: It is recommended to export the ID certificate trustpoint 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. For more information, refer to Exporting and Importing Trustpoints.

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.

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 13.

Figure 13: Add IP Pool

4. Click OK.
5. Go to Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.
6. Choose the appropriate IP address assignment method. This guide uses the internal address pools. See
Create Tunnel Group and Group Policy

Note: Before you create a tunnel group and group policy, go to Remote Access VPN > Network (Client) Access > IPSec Connection Profiles and make sure that the Allow Access box is checked for the Outside interface in the Enable interfaces for IPSec access.

Group Policy

Note: If you do not want to create a new policy, you can use the default built in 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 15.

Figure 15: Add Internal Group Policy
a. In the General tab, choose the **IPsec in the Tunneling Protocols** option unless you use other protocols such as SSL.
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 Servers section, uncheck the **Inherit** check box in the Default Domain and enter the appropriate domain name.
d. In the General tab, uncheck 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 set to **Inherit** and make the appropriate change.
e. All other configuration tabs 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 **Remote Access VPN > Network (Client) Access > IPsec Connection Profile > Add**. See Figure 16.

**Figure 16: Add Connection Profile**
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 Profile window, choose the ID certificate installed previously for peer authentication.
5. Leave the authentication set to LOCAL.
6. In the Profile window, choose the group policy created in the previous step.

Note: ASDM automatically configures local as the option for authentication even though certificates are used. In order to resolve this, set the IKE Authentication mode to disable. If you do not disable this, a username and password prompt appear when you try to connect. See figure 17.

Figure 17: Add Connection Profile

7. Click the Advanced tab > Authorization. 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. In the Authorization settings, choose UPN as the attribute to use. See Figure 18.

Figure 18: UPN Configuration
8. Click **OK**.

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

### Configure IKE/ISAKMP Parameters

Follow these instructions:

1. Go to **Remote Access VPN > Network (Client) Access > Advanced > IPSec**.
2. Ensure that the outside interface has IKE enabled on the IKE Parameters tab. If not, highlight the outside interface, click **Enable**, and leave everything else in default.
3. Go to **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 19 for an example.
5. Click **OK**.

**Figure 19: Add IKE/ISAKMP Policy**
**Note:** You can add multiple IKE/ISAKMP policies if needed.

6. Go to **Remote Access VPN > Network (Client) Access > Advanced > IPSec > Certificate to Connection Profile Maps > Policy**. See Figure 20.

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 **Remote Access VPN > Network (Client) Access > Advanced > IPSec > Certificate to Connection Profile Maps > Rules**.

9. Click **Add** on the top table.

### Figure 20: 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 21.
   
   d. Click **OK**.

### Figure 21: Add Certificate Matching Rule

11. Click **Add** on the bottom table.

12. In the Add Certificate Matching Rule Criterion window, follow these instructions:

### Figure 22: Certificate Matching Rule Criterion
Configure IPSec Parameters

Follow these instructions:

2. Click Add.
3. In the Create IPSec Rule window, in the Basic tab, follow these instructions: See Figure 23.

   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 any.
8. Click OK.
9. Click Apply.

Figure 23: 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 **Remote Access VPN > Certificate Management > CA Certificates**.
2. Choose a CA to configure to use OCSP when you highlight it in the table.
3. Click **Edit**.
4. Ensure that the **Check certificate for revocation** is checked.
5. In the Revocation Methods section, add **OCSP**. See Figure 24.

**Figure 24: OCSP Revocation Check**

6. Ensure that the **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 follow these procedures.

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

2. In order to choose a CA to configure, use OCSP to 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 25.

**Figure 25: 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 26.
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 26: 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 and DAP

Starting in 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. 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, etc.


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

![Active Directory Management Console](image)

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

![User Properties](image)
7. Click **OK**.

**ASA Configuration**

Follow these instructions:

1. In ASDM, go to **Remote Access VPN > AAA Setup > 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.

![Image of Edit LDAP Attributes Map Value window]

j. Click **OK**.
k. Click **OK**.
l. Click **APPLY**.
m. Configuration looks like Figure A5.

**Figure A5: LDAP Attribute Map Configuration**
4. Go to Remote Access VPN > 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
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=ggsgseclab,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=ggsgseclab,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=ggsgseclab,DC=org = 20

For the DENY condition, map

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

Note: In a future release, there will be 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 Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Click Add.
3. In the Add LDAP Attribute Map window, follow these instructions: See Figure A3.
   a. Enter a name in the Name text box.
   b. 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.
   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=ggsgseclab,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=ggsgseclab,DC=org 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 A9.

**Figure A9: LDAP Attribute Map**

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.
Scenario 3: Dynamic Access Policies for Multiple memberOf Attributes

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

- Use an existent group or create a new group (or multiple groups) 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.

ASA Configuration

Follow these instructions:

2. Click Add.
3. In the Add Dynamic Access Policy, follow these instructions:
   a. Enter a name in the Name text box.
   b. In the Priority section, enter 1 (or a number greater than 0).
   c. In the Selection Criteria, click Add.
   d. In the Add AAA Attribute, choose LDAP.
   e. In the Attribute ID section, enter memberOf.
   f. In the Value section, choose =, and enter the AD group name. Repeat this step for each group that you want to reference. See figure A10.

   Figure A10: AAA Attribute Map

   ![Add AAA Attribute Map](image)

   g. Choose OK.
   h. In the Access Policy Attributes section, choose Continue. See Figure A11.

   Figure A11: Add Dynamic Policy
5. Choose the Default Access Policy, and choose Edit.
6. The default action must be set to Terminate. See Figure A12.

Figure A12: Edit Dynamic Policy

7. Click OK.

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

Appendix B  ASA CLI Configuration
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

---------IPsec---------
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des 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 SYSTEM_DEFAULT_CRYPTO_MAP 1 set transform-set ESP-AES-128-SHA
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128

crypto map outside_map interface outside

---------CA Trustpoints---------
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
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 ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types

crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types

crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp 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 6d65e74 310c300a 06035504 0b130344 6f44310c 300a0603
  55040b13
  03504b49 311b3019 06035504 03131244 6f44204a 49544320 52666f74
```

```
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 6e6d65e74 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 6d65e74 310c300a 06035504 0b130344 6f44310c 300a0603
  55040b13
  f766e045 f15ddb43 9549d1e9 a0eaa614 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 6d65e74 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
  6e6d65e74 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
  1303504b
  49311630 14060355 0403130d 446f4420 52666f74 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 6d65e74 310c300a 06035504 0b130344 6f44310c 300a0603
  55040b13
  03504b49 311c301a 06035504 03131344 6f442043 4c153535 20332052
  6f6f7420
```

---ISAKMP---
```
crypto isakmp enable outside
crypto isakmp policy 10
authentication rsa-sig
encryption 3des
```
hash sha
group 2
lifetime 86400

!  
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
!
----------------------------------------VPN Group/Tunnel Policy----------------------------------------
group-policy CAC-USERS internal
group-policy CAC-USERS attributes
vpn-tunnel-protocol IPSec
default-domain none
address-pools value CAC-USERS
tunnel-group CAC-USERS type remote-access
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 ASDM_TrustPoint1
isakmp ikev1-user-authentication none
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

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 that 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.

---

```
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
Psw: 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=ggsgseclab,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....com1.0.....&...,d...
[78] userCertificate: value = 0.'0........../..t.....50...*.
H........0@1.0.....&...,d....com1.0.....&...,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
```
callback_aaa_task: status = 1, msg = AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
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"
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**

```plaintext
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
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
Pass: 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=ggsgseclab,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
```
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_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_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_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_NextFunction: `i_fsm_state = IFSM_TUNN_GRP_POLICY`, `auth_status = ACCEPT`
AAA_NextFunction: `authen svr = <none>`, `author svr = AD-LDAP`, `user 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 DAP

- **debug dap errors** displays DAP errors
- **debug dap trace** displays DAP function trace

Example 1: Allowed Connection with DAP

The example below shows the output of **debug dap errors** and **debug dap trace** within a successful connection with scenario 3 shown in Appendix A. Notice the multiple memberOf attributes. The user can belong to both _ASAUsers or VPNUsers or ANY one of the groups dependent upon the ASA configuration.

```
# debug dap errors
dump dap errors enabled at level 1
# debug dap trace
dump 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
```

Figure C3: debug DAP
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.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID = ...
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 = 12827349546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
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=ggsgseclab,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=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] = "20070626163734.02";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] = "20070718151143.02";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] = "VPNUsers";
**Example 2: Denied Connection with DAP**

The example below shows the output of `debug dap errors` and `debug dap trace` within an unsuccessful connection with scenario 3 shown in Appendix A.

```bash
# 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, 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: C8EEFA10d.
```
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 = 12827349546718750
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=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
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=ggsgseclab,DC=org";
Troubleshooting Certificate Authority / OCSP

- 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 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 misconfigured certificate group matching policy.

Figure C5 shows the debug output of a user with a revoked certificate.
Figure C3: OCSP Debugging Successful Certificate Validation

CRYPTO_PKI: Attempting to find tunnel group for cert with serial number: 2FB5FC740000000000035,
subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=com, issuer_name: cn=ggsgseclab,dc=ggsgseclab,dc=org.
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: 2FB5FC740000000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name: cn=ggsgseclab, dc=ggsgseclab,dc=org.
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.
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match CRYPTO_PKI:Certificate validated.
serial number: 2FB5FC740000000000035, subject name: cn=Ethan Hunt,ou=MIL, dc=ggsgseclab,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: 2FB5FC740000000000035, subject name: cn=Ethan Hunt,ou=MIL,dc=ggsgseclab, dc=org, issuer_name: cn=ggsgseclab,dc=ggsgseclab,dc=org.
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=ggsgseclab,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,ted ccha=inl als eibtrhaer tin,validid cor =noct
osauthori,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=ggsgseclab,dc=org, issuer_name: cn=ggsgseclab,dc=ggsgseclab,dc=org.
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.
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: 2FB5FC740000000000035, subject name: cn=Ethan Hunt,ou=MIL,
dc=ggsgseclab,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 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
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

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