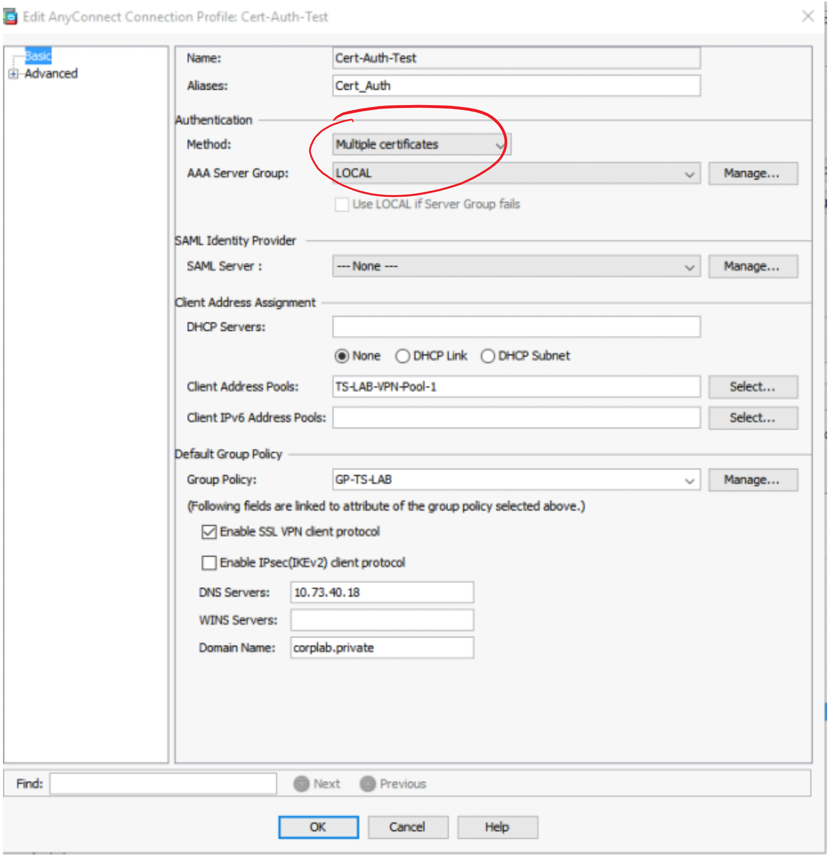
Cert Based Authentication (Multiple Certs)

09 June 2017 17:05

Applies to ASA 9.7 and 9.8 - Provided 'As-Is' with no warranty or liability.

Setup Tunnel group as normal, select method as multiple certs:



Edit AnyConnect Connection Profile: Cert-Auth-Test

Name: Cert-Auth-Test

Aliases: Cert_Auth

Authentication

Method: Multiple certificates

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: TS-LAB-VPN-Pool-1

Client IPv6 Address Pools:

Default Group Policy

Group Policy: GP-TS-LAB

(Following fields are linked to attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

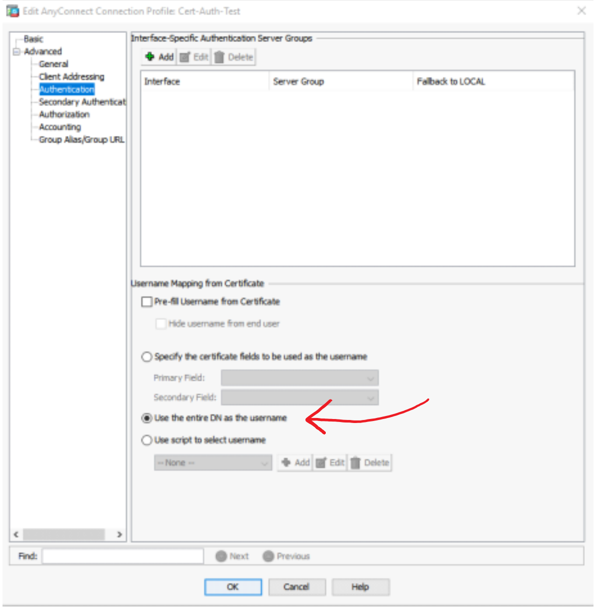
□ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.73.40.18

WINS Servers:

Domain Name: corplab.private

Set Advanced > Authentication to "use the entire DN as the username"



Edit AnyConnect Connection Profile: Cert-Auth-Test

Interface-Specific Authentication Server Groups

Interface	Server Group	Fallback to LOCAL

Username Mapping from Certificate

□ Pre-fill Username from Certificate

□ Hide username from end user

○ Specify the certificate fields to be used as the username

Primary Field:

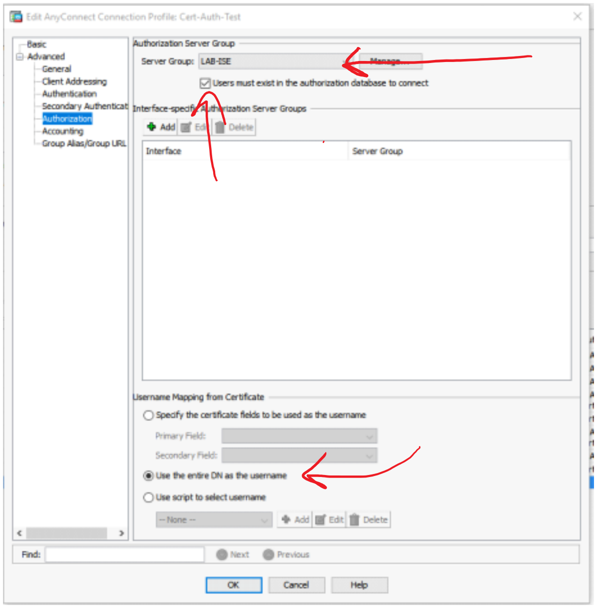
Secondary Field:

● Use the entire DN as the username

○ Use script to select username

-- None --

Set Authorization to the ISE Server Group and to use the entire DN as the username:



Authorization Server Group

Server Group: LAB-ISE

☑ Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

Username Mapping from Certificate

○ Specify the certificate fields to be used as the username

Primary Field:

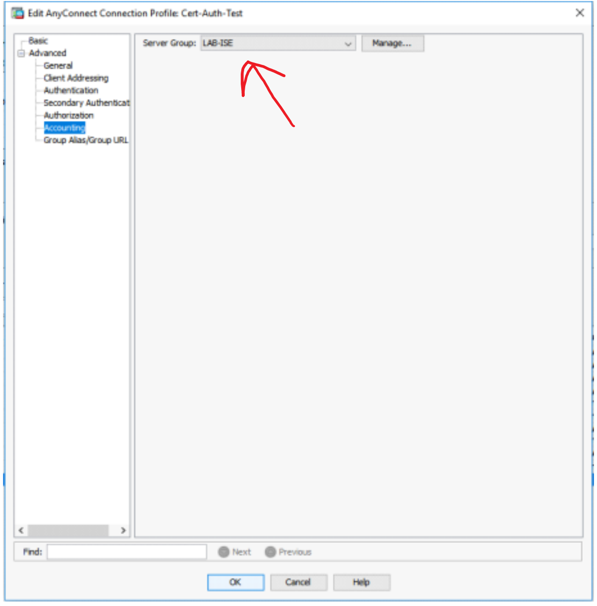
Secondary Field:

● Use the entire DN as the username

○ Use script to select username

-- None --

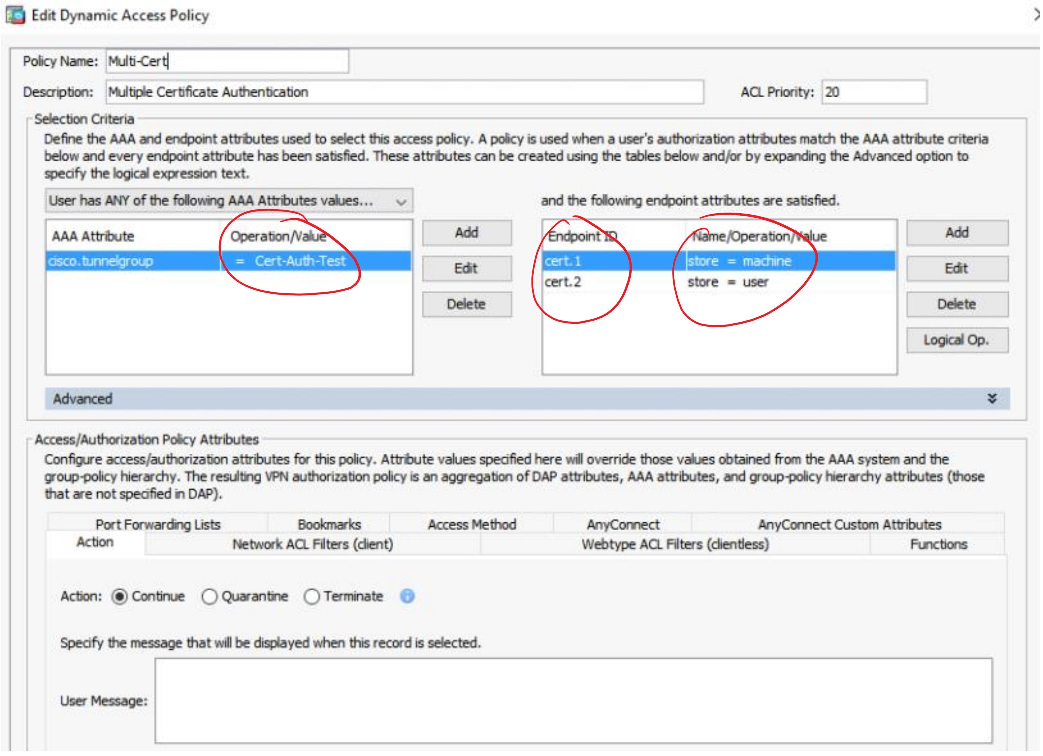
Set accounting to the ISE Server Group:



Server Group: LAB-ISE

If desired set a group alias / URL to make life easier, or you can setup certificate to group matching rules - I prefer the URL setting (at this time!)

Add a DAP policy:



Edit Dynamic Access Policy

Policy Name: Multi-Cert

Description: Multiple Certificate Authentication

ACL Priority: 20

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
cisco.tunnelgroup	= Cert-Auth-Test

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
cert.1	store = machine
cert.2	store = user

Access/Authorization Policy Attributes

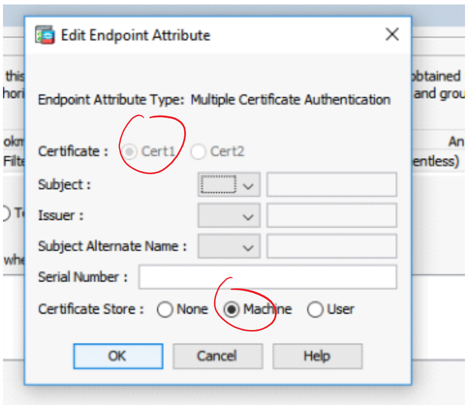
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists
Bookmarks
Access Method
AnyConnect
AnyConnect Custom Attributes
Action
Network ACL Filters (client)
Webtype ACL Filters (clientless)
Functions

Action: ● Continue ○ Quarantine ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message:



Edit Endpoint Attribute

Endpoint Attribute Type: Multiple Certificate Authentication

Certificate : ● Cert1 ○ Cert2

Subject :

Issuer :

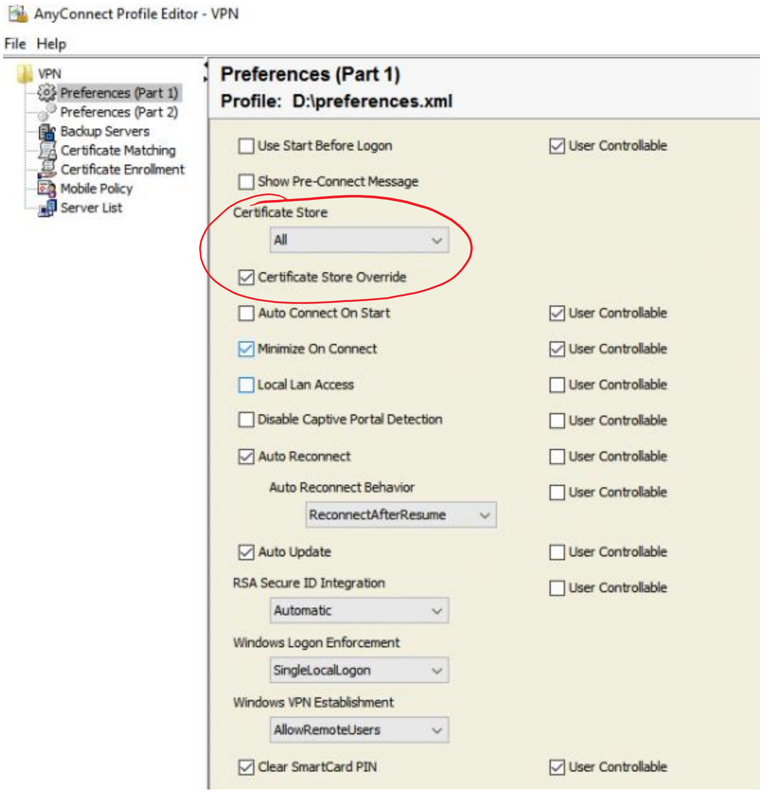
Subject Alternate Name :

Serial Number :

Certificate Store : ○ None ● Machine ○ User

Cert1 for machine and then add Cert2 for user to force the lookup of the stores.

Create an AnyConnect Profile Policy that allows access to the machine certificate store, this is done with the Certificate Store Override selection, but ensure that the store is set to "all" to ensure that we can retrieve both the user and the machine certificates, else Certificate Auth will fail. Import this to your client with the normal settings. I've added an entry to the server list to account for my peer details.



Preferences (Part 1)

Profile: D:\preferences.xml

□ Use Start Before Logon ☑ User Controllable

□ Show Pre-Connect Message

Certificate Store: All

☑ Certificate Store Override

□ Auto Connect On Start ☑ User Controllable

☑ Minimize On Connect ☑ User Controllable

□ Local Lan Access □ User Controllable

□ Disable Captive Portal Detection □ User Controllable

☑ Auto Reconnect □ User Controllable

Auto Reconnect Behavior: ReconnectAfterResume □ User Controllable

☑ Auto Update □ User Controllable

RSA Secure ID Integration: Automatic □ User Controllable

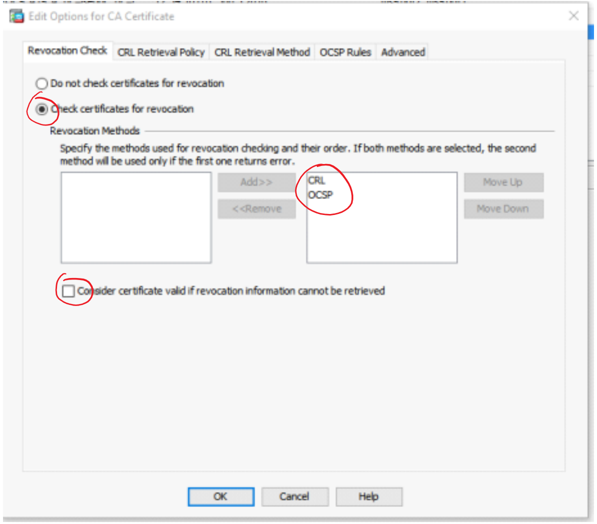
Windows Logon Enforcement: SingleLocalLogon

Windows VPN Establishment: AllowRemoteUsers

☑ Clear SmartCard PIN ☑ User Controllable

AAA Services are only used for Authorization, so ensure that you're able to receive the CRL lists for the CA (they may need configuring). You will need to import the Root CA from your AD CA to the ASA if you have not already done so, this becomes a trust-point on the ASA to allow validation of the presented certificates.

Device Management > Certificate Management > Trusted Root from your AD



○ Do not check certificates for revocation

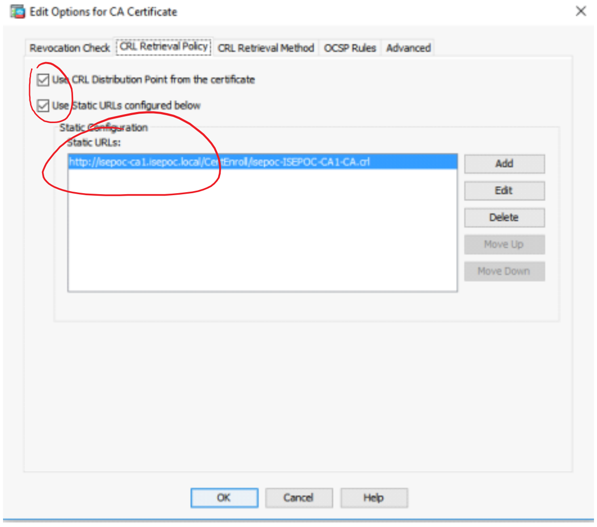
● Check certificates for revocation

Revocation Methods

Specify the methods used for revocation checking and their order. If both methods are selected, the second method will be used only if the first one returns error.

CRL
OCSP

□ Consider certificate valid if revocation information cannot be retrieved



Edit Options for CA Certificate

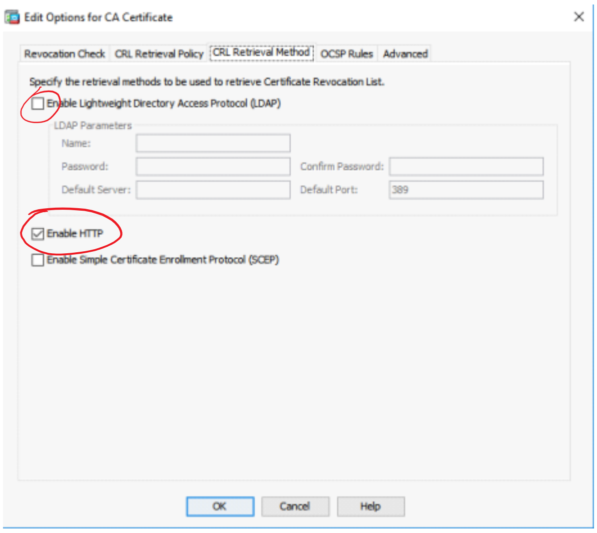
☑ Use CRL Distribution Point from the certificate

☑ Use Static URLs configured below

Static Configuration

Static URLs:

http://isepoc-ca1.isepoc.local/CertEnroll/isepoc-ISEPOC-CA1-CA.crl



Edit Options for CA Certificate

Specify the retrieval methods to be used to retrieve Certificate Revocation List.

□ Enable Lightweight Directory Access Protocol (LDAP)

LDAP Parameters

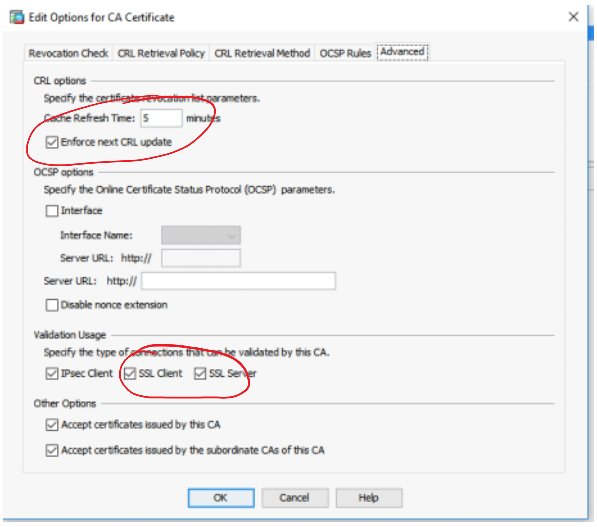
Name:

Password: Confirm Password:

Default Server: Default Port: 389

☑ Enable HTTP

□ Enable Simple Certificate Enrollment Protocol (SCEP)



Edit Options for CA Certificate

CRL options

Specify the certificate revocation list parameters.

Cache Refresh Time: 5 minutes

☑ Enforce next CRL update

OCSP options

Specify the Online Certificate Status Protocol (OCSP) parameters.

□ Interface

Interface Name:

Server URL: http://

Server URL: http://

□ Disable nonce extension

Validation Usage

Specify the type of connections that can be validated by this CA.

☑ IPsec Client ☑ SSL Client ☑ SSL Server

Other Options

☑ Accept certificates issued by this CA

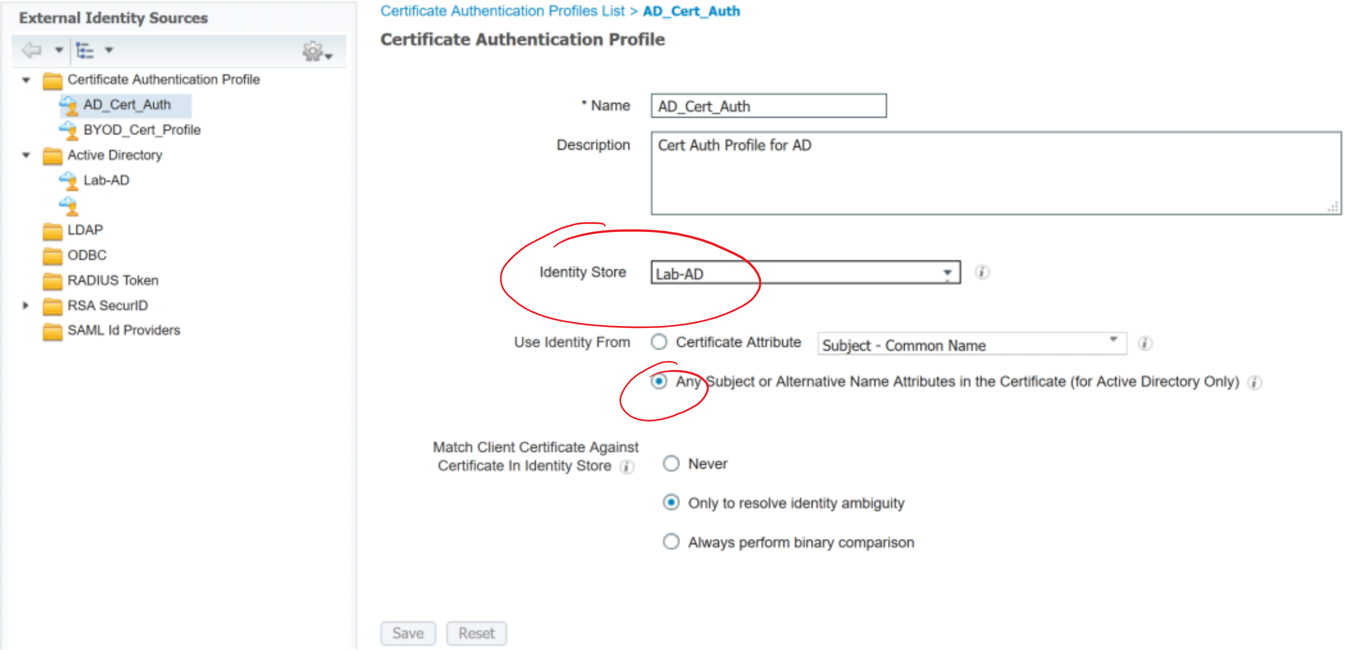
☑ Accept certificates issued by the subordinate CAs of this CA

Configure an appropriate policy on ISE to Authenticate and Authorize the user. We're not authenticating the machine. The Multi-Auth takes care of that aspect, the two certificates (Machine and User) need to be present to allow this to occur. The CRL's account for the Certificate's being accepted and that the laptop isn't lost / stolen.

The ISE Policy can be used to authorize and return ACL's based on the AD group of the user, but also - critically check if the account is valid within AD - so it's not disabled / expired.

Authentication options:

Firstly create a Certificate Profile for Active Directory:



Certificate Authentication Profiles List > **AD_Cert_Auth**

Certificate Authentication Profile

* Name: AD_Cert_Auth

Description: Cert Auth Profile for AD

Identity Store: Lab-AD

Use Identity From: ○ Certificate Attribute — Subject - Common Name

● Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store

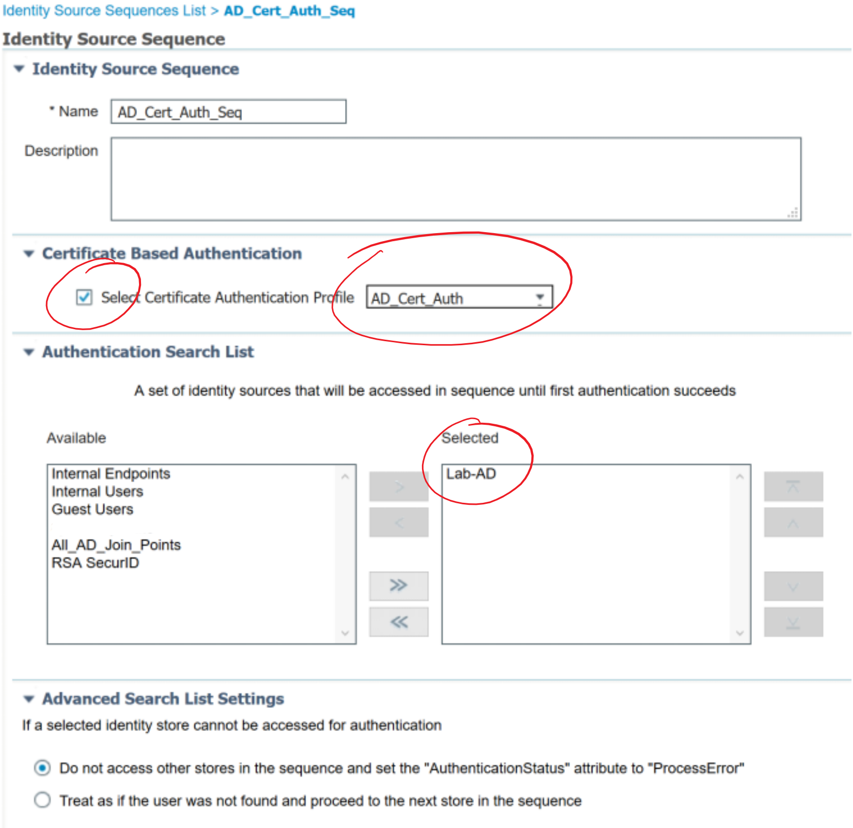
○ Never

● Only to resolve identity ambiguity

○ Always perform binary comparison

Screen clipping taken: 12/06/2017 14:12

Then create a sequence for it:



Identity Source Sequences List > **AD_Cert_Auth_Seq**

Identity Source Sequence

Identity Source Sequence

* Name: AD_Cert_Auth_Seq

Description:

Certificate Based Authentication

☑ Select Certificate Authentication Profile: AD_Cert_Auth

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints Internal Users Guest Users All_AD_Join_Points RSA SecurID	Lab-AD

Advanced Search List Settings

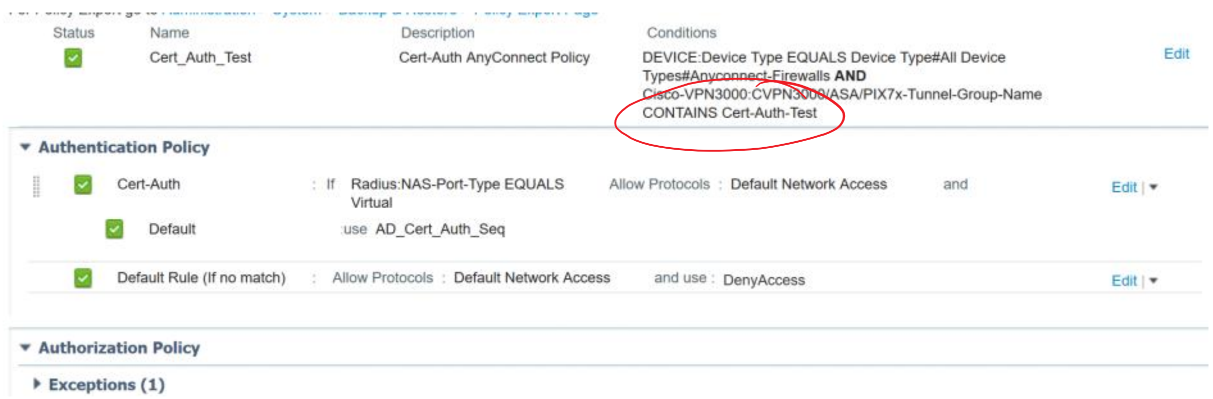
If a selected identity store cannot be accessed for authentication

● Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

○ Treat as if the user was not found and proceed to the next store in the sequence

Screen clipping taken: 12/06/2017 14:12

Setup a new policy set (if you use them, and if not - you should think about it, because it not only makes things so much easier to read, and also because it significantly limited the scope of human error. If I make a mistake in this policy, then it only breaks this one, not the whole system).
Here I match on Tunnel Group name.



For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions	
✓	Cert_Auth_Test	Cert-Auth AnyConnect Policy	DEVICE:Device Type EQUALS Device Type#All Device Types#Anyconnect-Firewalls **AND** Cisco-VPN3000:CVPN3000/ASA/PIX7x-Tunnel-Group-Name CONTAINS Cert-Auth-Test	Edit

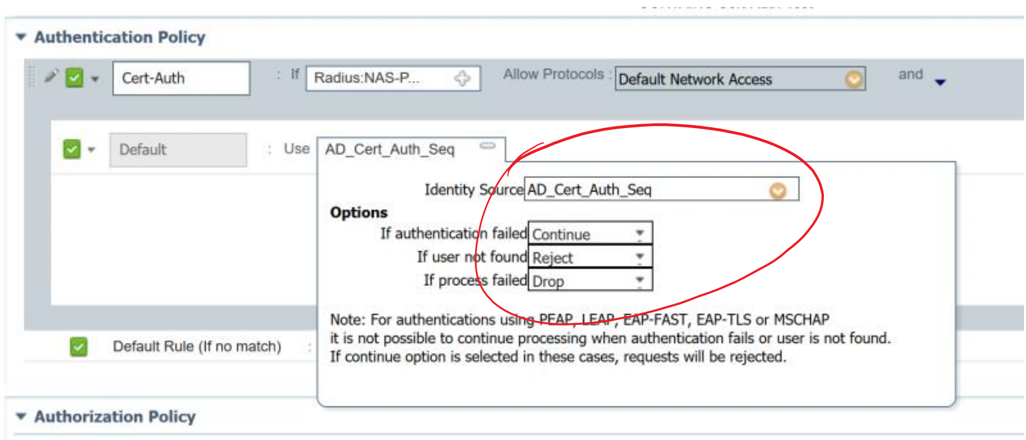
Authentication Policy

- ✓ Cert-Auth : If Radius:NAS-Port-Type EQUALS Virtual Allow Protocols : Default Network Access and Edit |
  - ✓ Default use AD_Cert_Auth_Seq
- ✓ Default Rule (If no match) : Allow Protocols : Default Network Access and use : DenyAccess Edit |

Authorization Policy

Exceptions (1)

Screen clipping taken: 12/06/2017 14:09



Authentication Policy

✓ Cert-Auth : If Radius:NAS-P... Allow Protocols : Default Network Access and

✓ Default : Use AD_Cert_Auth_Seq

Identity Source AD_Cert_Auth_Seq

Options

If authentication failed Continue

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or MSCHAP
it is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.

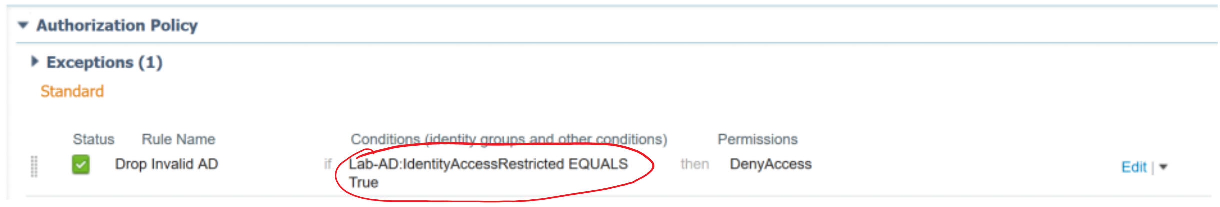
✓ Default Rule (If no match)

Authorization Policy

Screen clipping taken: 12/06/2017 14:11

Next we add AuthZ options:

Authorization Options:



Authorization Policy

Exceptions (1)

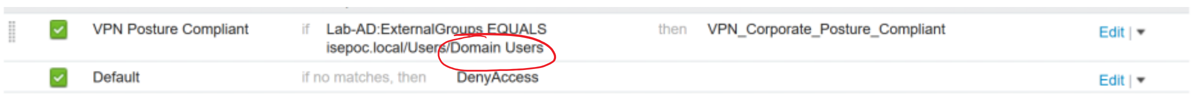
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Drop Invalid AD	if	Lab-AD:IdentityAccessRestricted EQUALS True	then	DenyAccess	Edit

Screen clipping taken: 12/06/2017 14:15

Here we've added a check for the AD if IdentityAccessRestricted = True (basically is the account disabled / expired). If it is, then Deny Access. That allows us to disable an account in AD and instantly deny VPN access while we wait for the CRL's to catch up.

Then write your policy based on what you want:

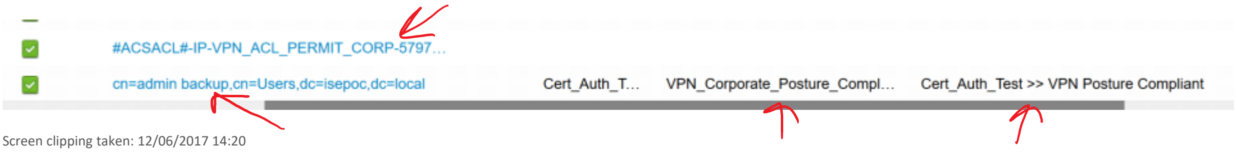


Status	Rule Name		Conditions		Permissions	
✓	VPN Posture Compliant	if	Lab-AD:ExternalGroups EQUALS isepoc.local/Users/Domain Users	then	VPN_Corporate_Posture_Compliant	Edit
✓	Default		if no matches, then		DenyAccess	Edit

Screen clipping taken: 12/06/2017 14:17

In this one we're basically saying if you are in domain users, then give VPN access. But if you want to do different levels of access based on user group, you can do this above and apply different ACL results on this attribute.

What does this look like in ISE logs:

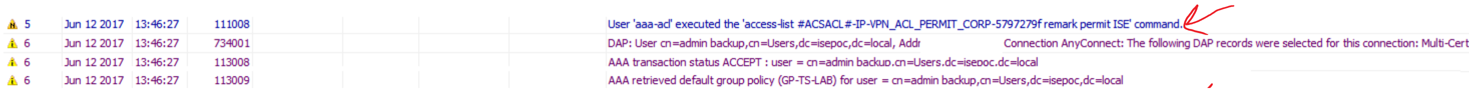


✓	#ACSACL#-IP-VPN_ACL_PERMIT_CORP-5797...			
✓	cn=admin backup,cn=Users,dc=isepoc,dc=local	Cert_Auth_T...	VPN_Corporate_Posture_Compl...	Cert_Auth_Test >> VPN Posture Compliant

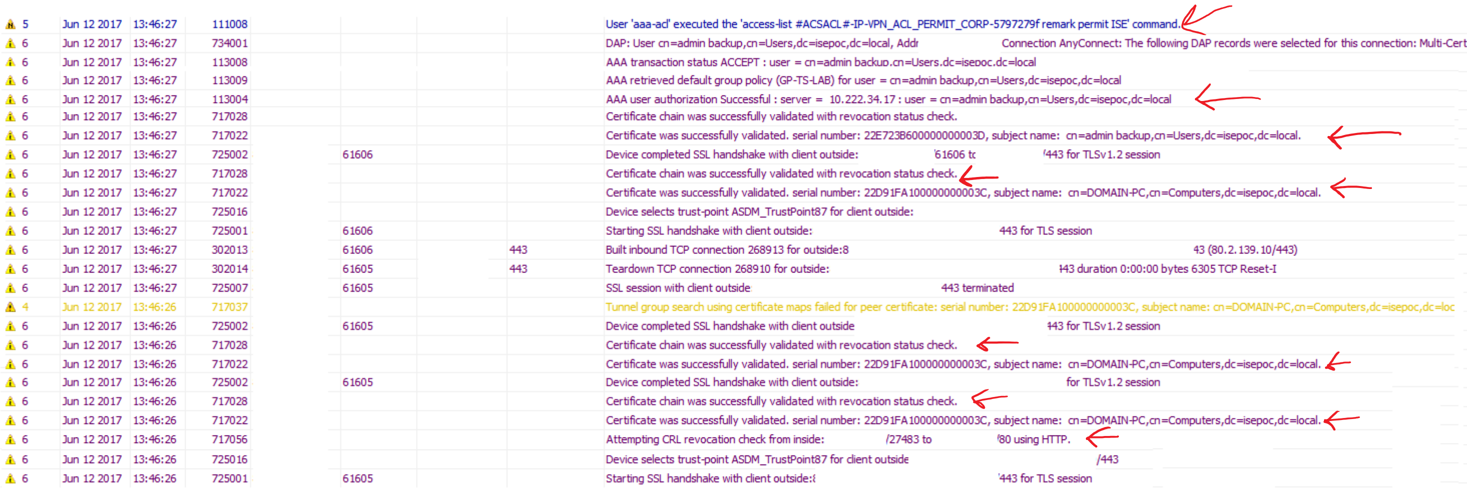
Screen clipping taken: 12/06/2017 14:20

Here we see that my user (admin backup - I know, I know, it was a convenient test account - "Bad Kev!") has triggered the right policy elements and above it, the ACL has been sent to the ASA

ASA Log:



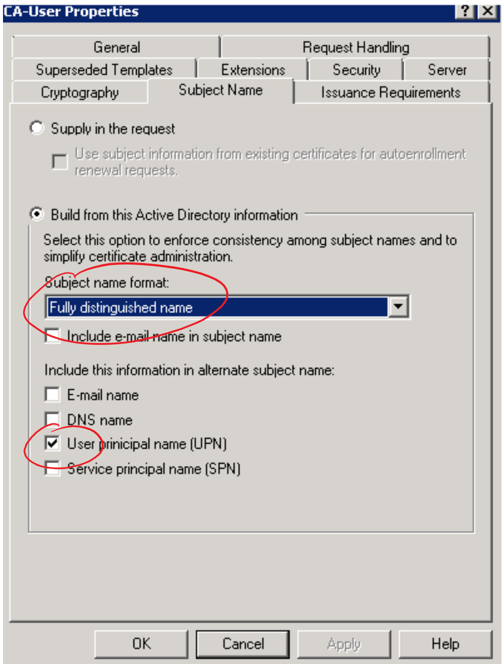
```
5  Jun 12 2017  13:46:27  111008   User 'aaa-acl' executed the 'access-list #ACSACL#-IP-VPN_ACL_PERMIT_CORP-5797279f remark permit ISE' command.
6  Jun 12 2017  13:46:27  734001   DAP: User cn=admin backup,cn=Users,dc=isepoc,dc=local, Addr          Connection AnyConnect: The following DAP records were selected for this connection: Multi-Cert
6  Jun 12 2017  13:46:27  113008   AAA transaction status ACCEPT : user = cn=admin backup,cn=Users,dc=isepoc,dc=local
6  Jun 12 2017  13:46:27  113009   AAA retrieved default group policy (GP-TS-LAB) for user = cn=admin backup,cn=Users,dc=isepoc,dc=local
```



```
5  Jun 12 2017  13:46:27  111008                      User 'aaa-acl' executed the 'access-list #ACSACL#-IP-VPN_ACL_PERMIT_CORP-5797279f remark permit ISE' command.
6  Jun 12 2017  13:46:27  734001                      DAP: User cn=admin backup,cn=Users,dc=isepoc,dc=local, Addr          Connection AnyConnect: The following DAP records were selected for this connection: Multi-Cert
6  Jun 12 2017  13:46:27  113008                      AAA transaction status ACCEPT : user = cn=admin backup.cn=Users.dc=isepoc.dc=local
6  Jun 12 2017  13:46:27  113009                      AAA retrieved default group policy (GP-TS-LAB) for user = cn=admin backup,cn=Users,dc=isepoc,dc=local
6  Jun 12 2017  13:46:27  113004                      AAA user authorization Successful : server =  10.222.34.17 : user = cn=admin backup,cn=Users,dc=isepoc,dc=local
6  Jun 12 2017  13:46:27  717028                      Certificate chain was successfully validated with revocation status check.
6  Jun 12 2017  13:46:27  717022                      Certificate was successfully validated. serial number: 22E723B600000000003D, subject name:  cn=admin backup,cn=Users,dc=isepoc,dc=local.
6  Jun 12 2017  13:46:27  725002   61606              Device completed SSL handshake with client outside:          '61606 tc          '443 for TLSv1.2 session
6  Jun 12 2017  13:46:27  717028                      Certificate chain was successfully validated with revocation status check.
6  Jun 12 2017  13:46:27  717022                      Certificate was successfully validated. serial number: 22D91FA100000000003C, subject name:  cn=DOMAIN-PC,cn=Computers,dc=isepoc,dc=local.
6  Jun 12 2017  13:46:27  725016                      Device selects trust-point ASDM_TrustPoint87 for client outside:
6  Jun 12 2017  13:46:27  725001   61606              Starting SSL handshake with client outside:                              443 for TLS session
6  Jun 12 2017  13:46:27  302013   61606      443     Built inbound TCP connection 268913 for outside:8                                                     43 (80.2.139.10/443)
6  Jun 12 2017  13:46:27  302014   61605      443     Teardown TCP connection 268910 for outside:                                   443 duration 0:00:00 bytes 6305 TCP Reset-I
6  Jun 12 2017  13:46:27  725007   61605              SSL session with client outside                        443 terminated
4  Jun 12 2017  13:46:26  717037                      Tunnel group search using certificate maps failed for peer certificate: serial number: 22D91FA100000000003C, subject name: cn=DOMAIN-PC,cn=Computers,dc=isepoc,dc=loc
6  Jun 12 2017  13:46:26  725002   61605              Device completed SSL handshake with client outside                          443 for TLSv1.2 session
6  Jun 12 2017  13:46:26  717028                      Certificate chain was successfully validated with revocation status check.
6  Jun 12 2017  13:46:26  717022                      Certificate was successfully validated. serial number: 22D91FA100000000003C, subject name:  cn=DOMAIN-PC,cn=Computers,dc=isepoc,dc=local.
6  Jun 12 2017  13:46:26  725002   61605              Device completed SSL handshake with client outside:                            for TLSv1.2 session
6  Jun 12 2017  13:46:26  717028                      Certificate chain was successfully validated with revocation status check.
6  Jun 12 2017  13:46:26  717022                      Certificate was successfully validated. serial number: 22D91FA100000000003C, subject name:  cn=DOMAIN-PC,cn=Computers,dc=isepoc,dc=local.
6  Jun 12 2017  13:46:26  717056                      Attempting CRL revocation check from inside:        /27483 to         '80 using HTTP.
6  Jun 12 2017  13:46:26  725016                      Device selects trust-point ASDM_TrustPoint87 for client outside                      /443
6  Jun 12 2017  13:46:26  725001   61605              Starting SSL handshake with client outside:8                              '443 for TLS session
```

Tweaks to the CA:

These are tweaks I've made, keeping in mind that my domain isn't production and your millage may vary:
User Certificate Template:



CA-User Properties

? ✕
General | Request Handling
Superseded Templates | Extensions | Security | Server
Cryptography | Subject Name | Issuance Requirements

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

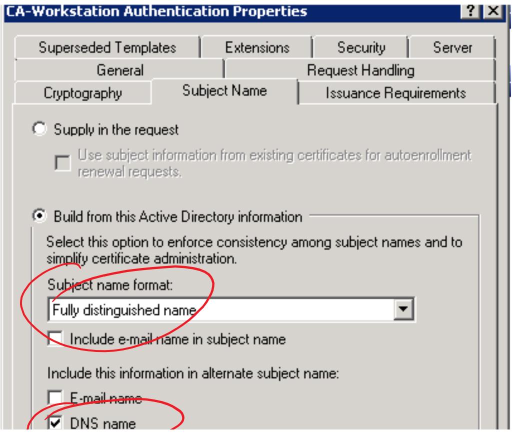
□ DNS name

☑ User prinicipal name (UPN)

□ Service principal name (SPN)

Screen clipping taken: 12/06/2017 14:25

Setting to Fully Distinguished Name for the user cert. Note I don't have email address, because my lab setup has no requirement.



CA-Workstation Authentication Properties

? ✕
Superseded Templates | Extensions | Security | Server
General | Request Handling
Cryptography | Subject Name | Issuance Requirements

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

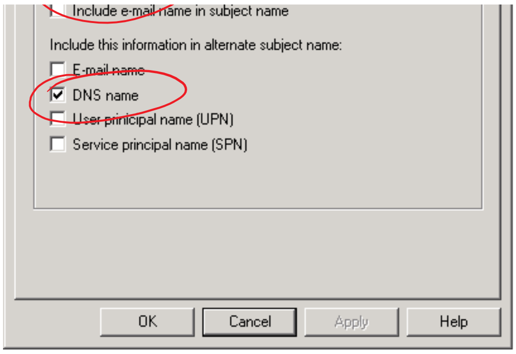
Fully distinguished name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

☑ DNS name



□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

☑ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Screen clipping taken: 12/06/2017 14:26

Similar setup for the machine certificate.

Reference Information:

Setting up a MS CA:
User Side Certificates - https://technet.microsoft.com/en-us/library/cc770857(v=ws.10).aspx
Machine Side Certificates - https://technet.microsoft.com/en-us/library/cc731242(v=ws.10).aspx
CRL Server - https://blogs.technet.microsoft.com/nexthop/2012/12/17/updated-creating-a-certificate-revocation-list-distribution-point-for-your-internal-certification-authority/

Great Cisco Live guides: BRKSEC-3053 (Cisco Live Berlin 2016 - Ned Zaldivar (Practical PKI for Remote Access VPN with ISE).