

What You Make Possible



Practical PKI for VPN

BRKSEC-2053

Abstract

- This intermediate level session will provide a technical overview and best practices for deploying X.509 certificates for two-factor authentication to support AnyConnect client. A number of different SSLVPN use cases including bring your own device will be introduced and explained. The recommended solutions will focus on ease of use and manageability with detailed configuration examples. Technologies used include Cisco ASA and Cisco AnyConnect Secure Mobility using both Cisco and MSFT public key solutions. By the end of the session participants should grasp the major steps in X.509 certificate deployment and be able to make informed decisions about using certificate authentication with Cisco solutions.

Agenda

- **Making the case** for Identity-based Digital Certificates
- Using best practices to **Simplify the Deployment of Certificates** for VPN
- **Best Practices Case Study** – Cisco Anyconnect SSLVPN with certificates
- **Case Study Demo**
- **Q&A**

Making the Case for Digital Certificates

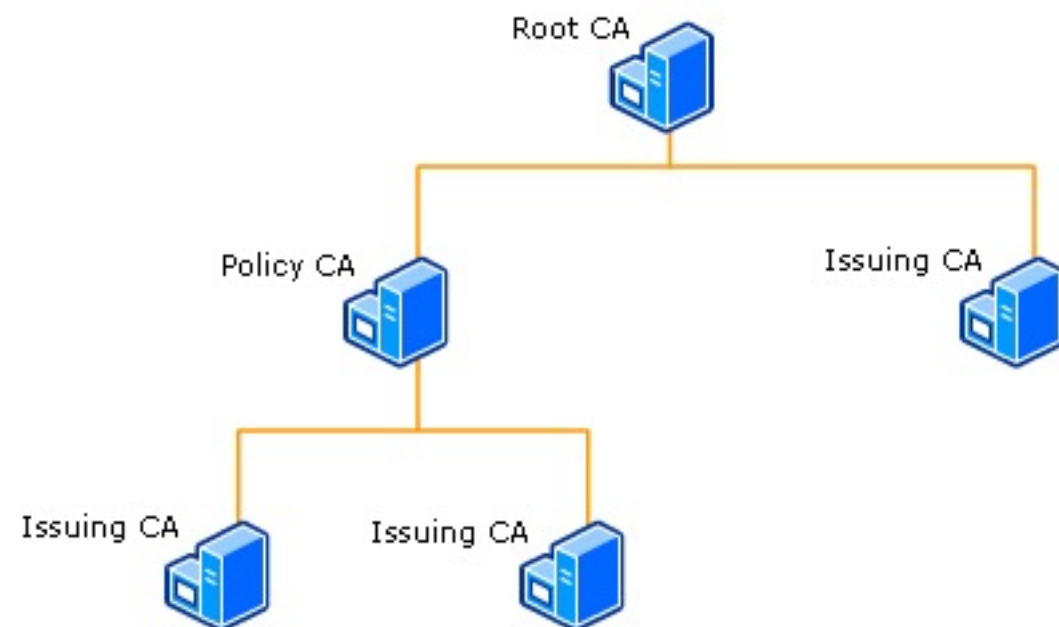
Two-factor VPN Authentication and Much More



Certificate Authority (CA)

The Source of Truth for any PKI

- Responsible for issuing, validating, renewing, revoking and logging certificates
- Establishes and verifies the identities of certificate requestors
- Configures the usage and content of certificates (templates) and issues certificates to users, computers, and services



Types of Client Digital Certificates

1. User/Identity Certificates

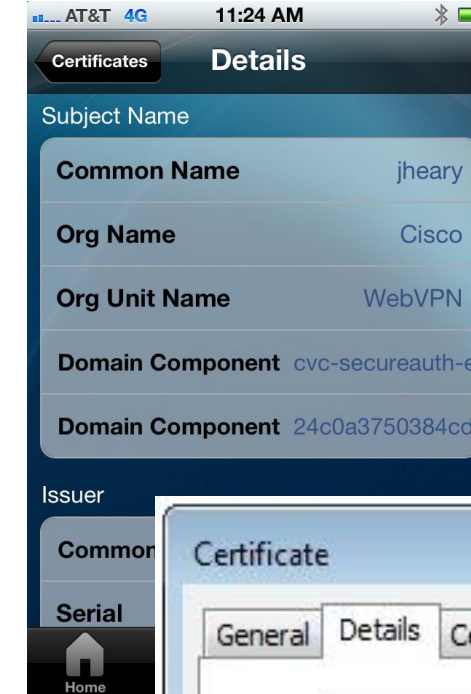
- A certificate that contains a user based attribute
- Usually in the CN or UPN field

2. Device Certificates

- A certificate that contains a device specific attribute

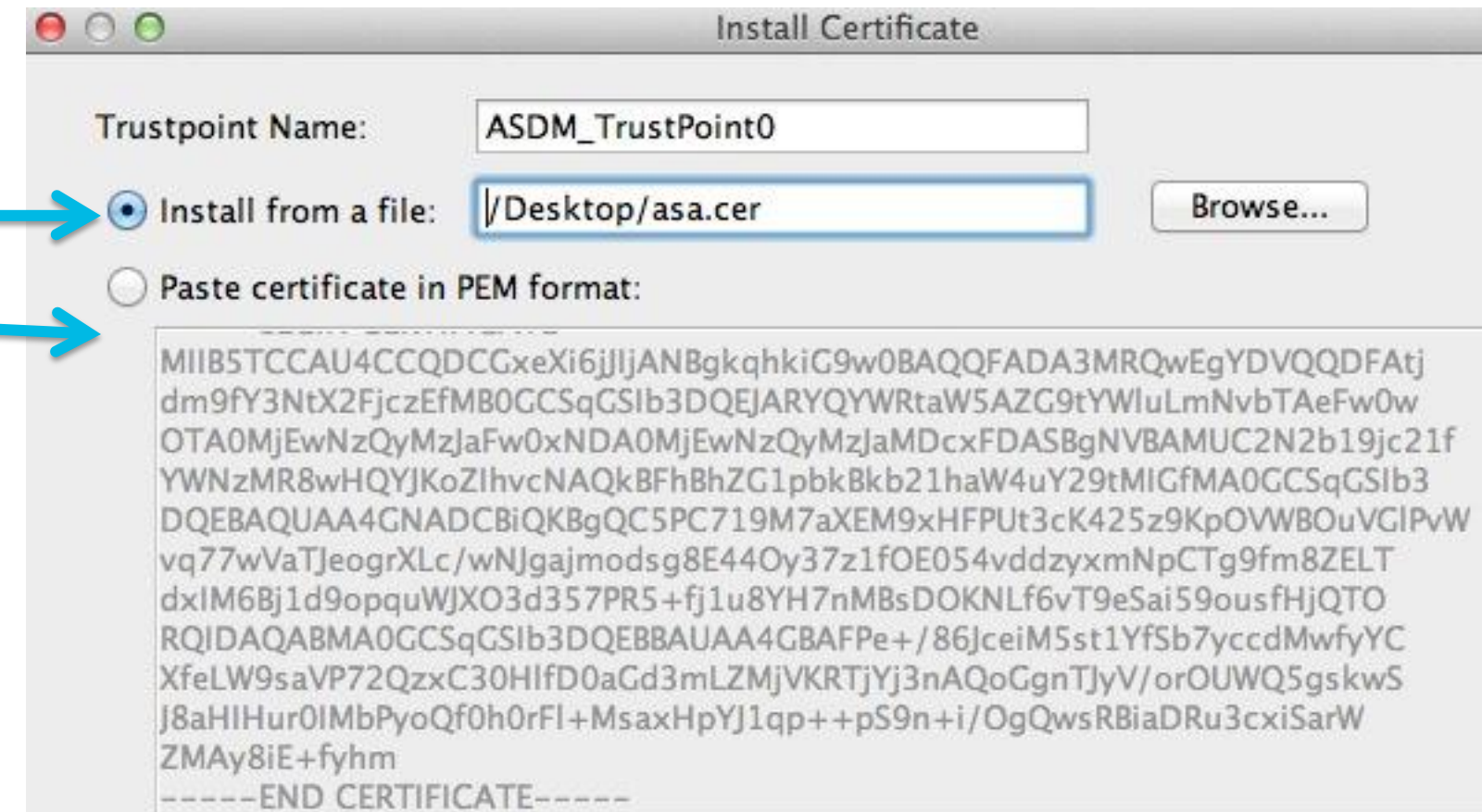
3. Hybrid (User plus Device) Certificates

- Allow for network access of specifically authorised devices used by specifically authorised users.



Certificate File Formats Demystified

- DER (.der .cer) – Distinguished Encoding Rules
 - Binary encoded single cert per file
 - Cannot copy / paste
- 😊 ■ PEM (.pem .cer .crt .key)
 - Base64 encoded txt
 - Can copy / paste
- PKCS#12 (.pfx .p12)
 - Certificate Chain usually with private keys
 - Password may be required to open
- CSR (.csr) - certificate signing request (PKCS10)
- PKCS#7 (.p7b .p7c)
 - Certificate chain without private keys
 - *Cannot import directly into ASA, need to convert

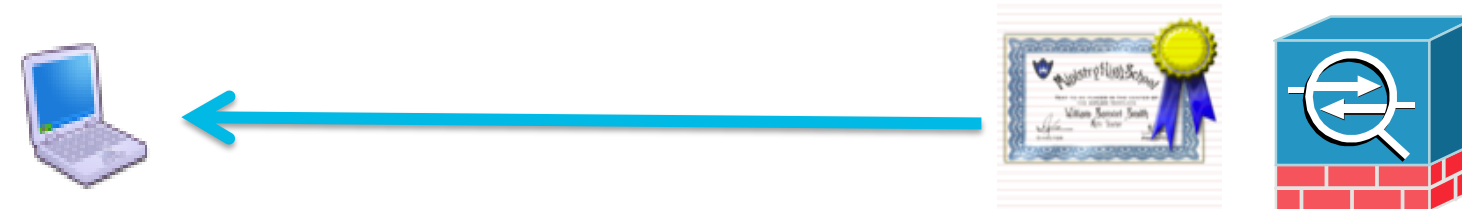


How Identity Certificates Work

VPN Use Case – Exchange of Certificates

- Connection initiated by AnyConnect or browser session to ASA Head end

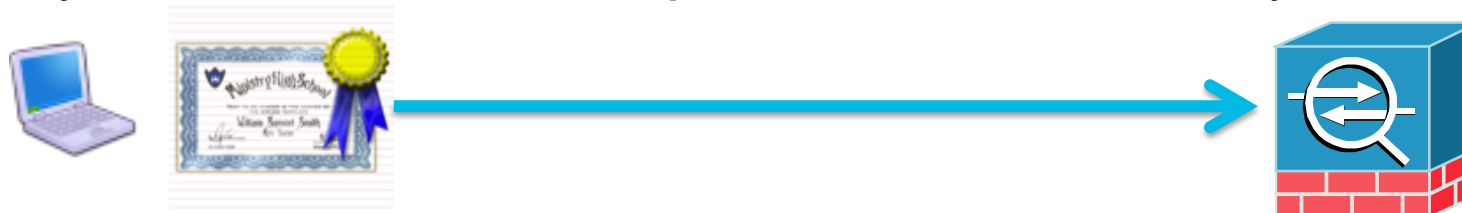
1. ASA presents its outside interface SSL Identity Certificate



2. Client validates ASA certificate



3. AnyConnect or browser provides client Identity Certificate to ASA



4. ASA validates Client certificate

- Optional: ASA requests 2nd factor username + password
- Optional: ASA evaluates certificate matching rules to set connection policy

How Identity Certificates Work

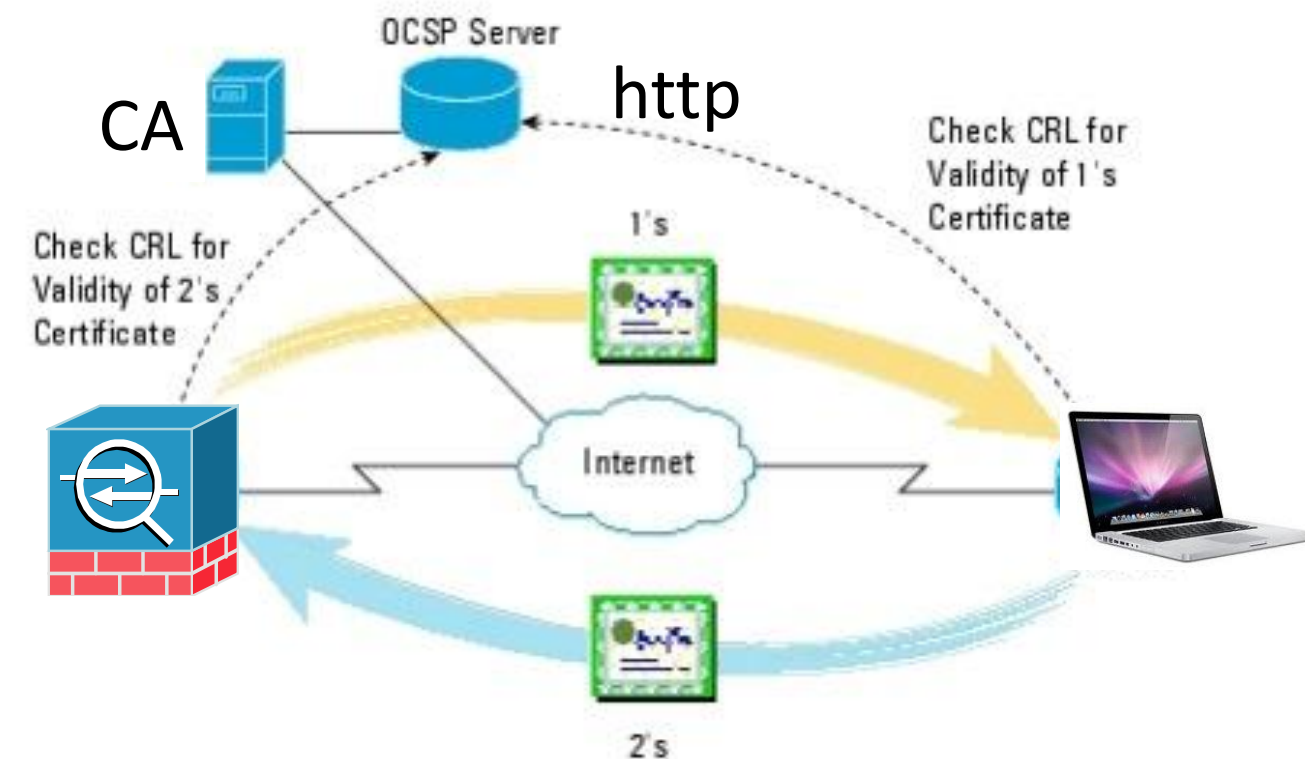
VPN Use Case – Mutual Validation of Certificates

- Certificate validation steps:
 - Has the digital certificate been **issued by a trusted CA**?
 - Is the certificate **expired**? (start + end date validity check)
 - Has the certificate been **revoked**? (OCSP or CRL check)
 - Does the **VPN URL match** the CN or SAN field in the certificate?
- Protects against Man in the Middle Attacks
 - ASA checks against a known trusted CA



Certificate Revocation Explained

- CRL (Certificate Revocation List)
 - Full list of all revoked certs
 - Periodic Updates (default 1 week!)
 - Unnecessary public exposure
- Delta CRL
- OCSP (online certificate status protocol)
 - Request/response per certificate check
 - Near real-time updates
 - OCSP Server gathers CRL's from one or many CA's
 - Nonce helps defeat replay attacks



How Identity Certificates Work

VPN Use Case – Parsing of Certificate Attributes

- ASA can parse client identity certificate fields for authorisation checks
 - Connection Profile mapping based on email domain (example)
 - VLAN / IP address assignment based on AD domain name (example)

The image shows two 'Certificate' dialog boxes and a configuration window. The left dialog shows 'Version 1 Fields Only' with fields like Version, Serial number, Signature algorithm, Issuer, Valid from, Valid to, Subject, and Public key. The right dialog shows '<All>' fields including SMIME Capabilities, Subject Key Identifier, Certificate Template Name, Authority Key Identifier, CRL Distribution Points, Authority Information Access, Enhanced Key Usage, and Subject Alternative Name. The configuration window is titled 'Configure a certificate matching rule criterion' and shows 'Rule Priority: 10' and 'Mapped to Connection Profile: DefaultWEBVPNGroup'. It has a table with columns 'Field', 'Component', 'Operator', and 'Value'.

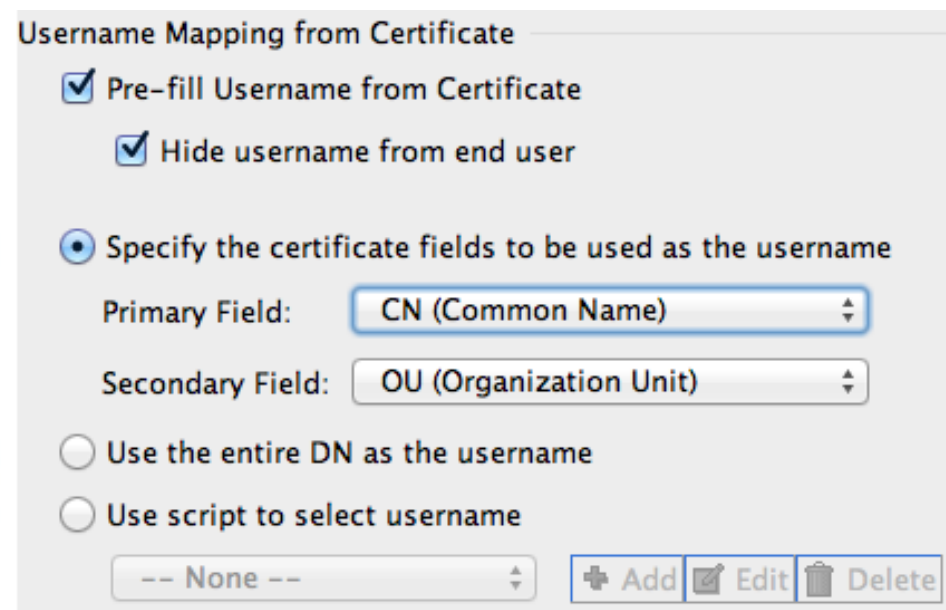
Subject (CN)
&
Subject Alternative
Name (SAN) fields

| Field | Component | Operator | Value |
|-------------------|-------------------|----------|-----------------|
| Alternative Su... | -- Whole Field -- | Contains | sfd-dc-lab.cisc |

How Identity Certificates Work

Forcing per user cert auth

- Pre-fill username adds security
- ASA can query AD (LDAP) record of user in certificate

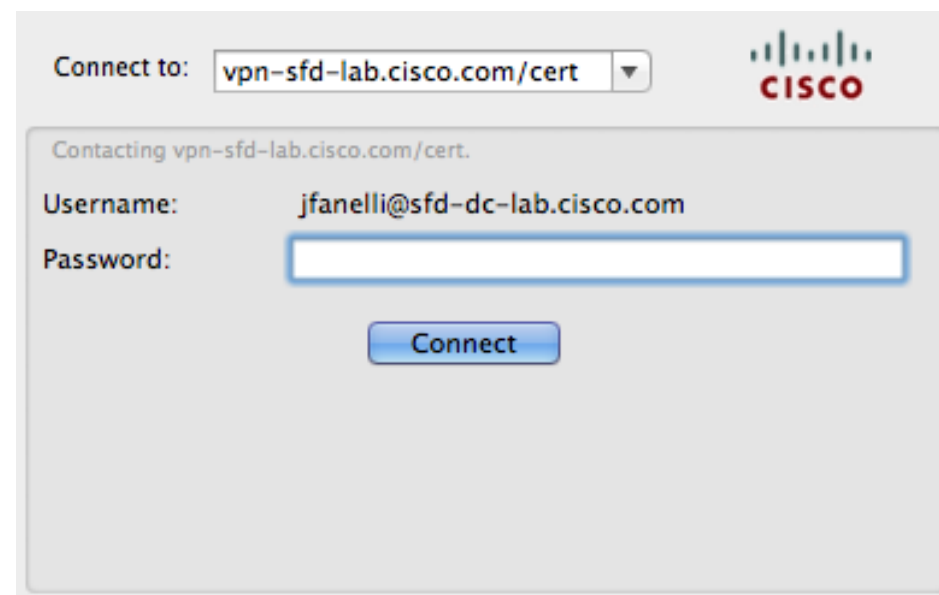



Username Mapping from Certificate

- Pre-fill Username from Certificate
- Hide username from end user
- Specify the certificate fields to be used as the username
 - Primary Field: CN (Common Name)
 - Secondary Field: OU (Organization Unit)
- Use the entire DN as the username
- Use script to select username

-- None --

ASA Pre-fill Authentication Configuration



Connect to: vpn-sfd-lab.cisco.com/cert 

Contacting vpn-sfd-lab.cisco.com/cert.

Username: jfanelli@sfd-dc-lab.cisco.com

Password:

Anyconnect with pre-filled username

Advantages of Certificates

- **Two-factor Authentication** using Identity Certs plus username/password
 - Less expensive TCO alternative to token solutions
 - Simpler end-user experience = Happier users 😊
- **Increased protection** against Phishing, MiTM and Social Engineering Attacks
- Provides a **user friendly experience** for Mobile device VPN
 - Automatic On-demand VPN connectivity
- Establish VPN security **policy per device**



Disadvantages of Certificates

VPN Use Case



- Another mouth to feed!
 - Must maintain PKI server(s) and keep highly available (backups, redundancy, updates)
- Portability and Enrolling **Multiple** Devices
 - Multiple end user devices = multiple identity certificates
 - Can't use an endpoint for VPN until it has been enrolled first
- General lack of PKI skillset in IT today
 - Steeper learning curve than deploying OTP solutions
 - Incorrect deployments can be insecure

Common x.509 Certificate Myths!



- **Hard to deploy!**

- Takes forever to setup and get right
- Hard to create a robust PKI in house, huge project
- Hard to get certificate to user / device

- **Hard to manage!**

- Takes several FTE to run this thing
- Lots of care and feeding
- Troubleshooting is a nightmare

- **Confusing end user experience!**

- Which certificate do I choose and when?
- Certificate warning pop-ups
- Tedious and confusing certificate enrollment process for each device!

- **Not true two-factor authentication!**

- Anyone on the PC can use my VPN
- Everyone has the same certificate

Common Myths Busted!



■ Hard to deploy!

- Usually a skillset issue not a technology issue
- Can be deployed in about a day using MSFT AD CA
- Complete automation for AD domain PC's

■ Hard to manage!

- Once deployed there is very little on-going maintenance or management
- Cisco ASA provides easy to understand error logs when something goes wrong

■ Confusing end user experience!

- In most cases the user will not interact with a certificate
- Even enrollment can be made completely transparent to the end-user
- Certificates = Happy Users 😊

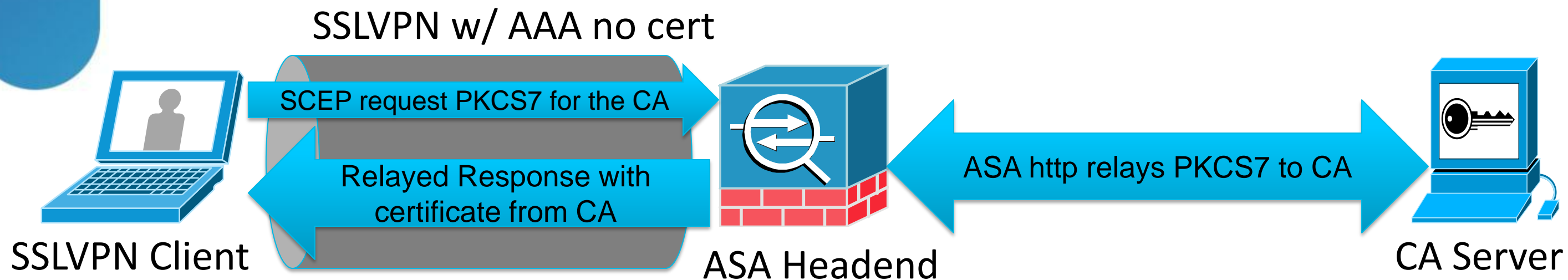
■ Not true two-factor authentication!

- Accepted by PCI, FISMA, NIST...
- Needs to be identity based certs not shared certs

SCEP and SCEP Proxy Overview

- SCEP stands for Simple Certificate Enrollment Protocol
- SCEP provides an easy and secure mechanism to deploy certificates
- SCEP is supported by MSFT CA's, IOS CA, others
- SCEP embedded into Cisco AnyConnect Client on all Platforms

SCEP Proxy hides CA Server from Client



Certificate Use Cases

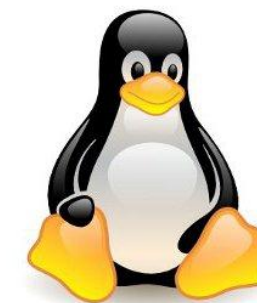
VPN is just one use case!

- User and Machine certificates are **the gift that keeps on giving**
- Quickly increase corporate security in other areas
- Deploy once, use everywhere*



AnyConnect Secure Mobility

- SSL and IPSec VPN Client
 - Certificate and two factor authentication support
- 802.1x network supplicant
 - EAP-TLS support
- Broad client device support
 - Windows, Mac, Apple iOS, Android
- Built-in SCEP support
 - Easy deployment of certificates



Cisco *live!*

Cisco Jabber for iPhone/Android

- Enterprise VoIP calling
 - “Office” like VoIP calling and directory services
- Embedded Anyconnect
 - Allows certificate based ‘embedded’ SSL VPN for seamless user experience
- Broad mobile device support
 - Apple iOS, Android
- Built-in SCEP support
 - Easy deployment of certificates



Wired and Wireless 802.1x Security

- EAP-TLS uses certificates for authentication to wireless
- Wired 802.1x uses certificates for authentication and device authorisation
- Network Admission Control (NAC) can use certificates for

device security posture check

```
if RegisteredDevice.NetworkUsesEapAuthentication EQUALS Employee  
EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS  
Radius:Calling-Station-ID AND AD1:ExternalGroups EQUALS  
cts.local/Users/Employees )
```



Many Other Use Cases for Identity Certs!

- **Secure Email** – Use identity certificate to sign and encrypt email



- **Document Signing** – Ensure Authenticity and Integrity of sensitive docs

- **Secure Login to Web Services** – Identity Certificates provide a single-sign-on experience or provide two-factor authentication

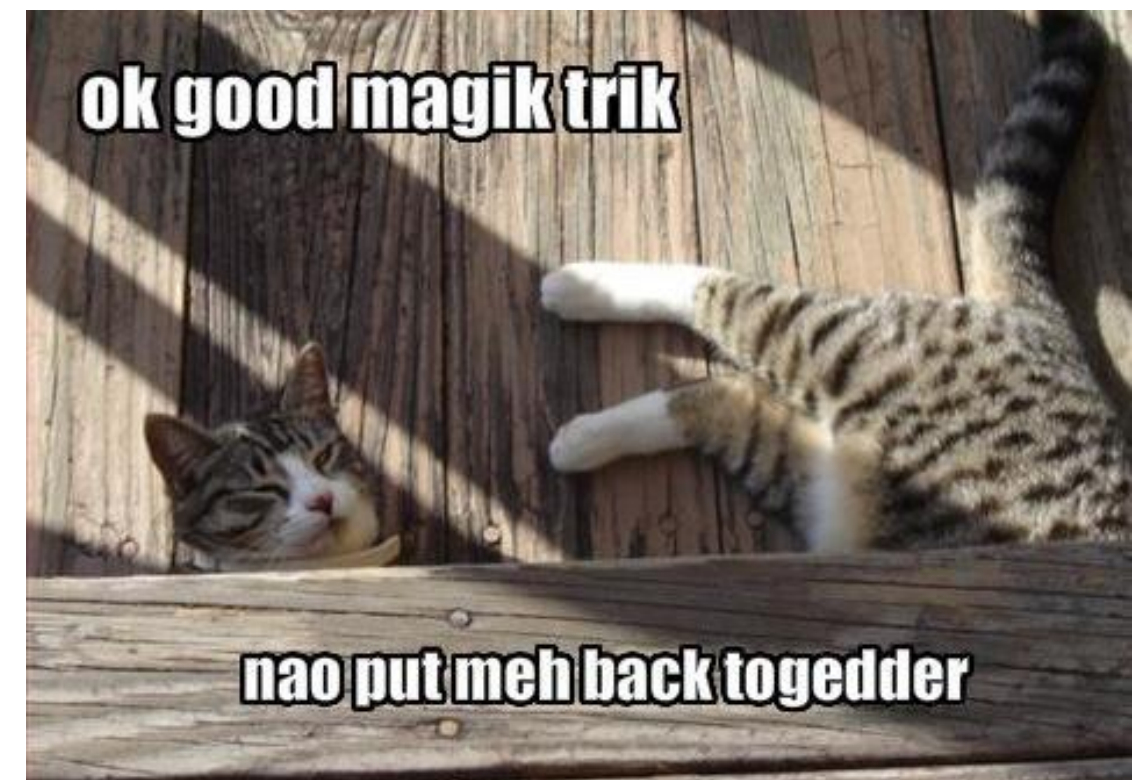


Agenda

- ✓ Making the case for Identity-based Digital Certificates
- ✧ Using best practices to **Simplify the Deployment of Certificates** for VPN
 - **Best Practices Case Study** – Cisco Anyconnect SSLVPN with certificates
 - **Case Study Demo**
 - **Q&A**

Our Two Deployment Goals

- Easy to Use
 - Minimise the interaction end users have in the whole process
- Easy to Deploy
 - Setup a CA deployment quickly and easily
 - Deploy Identity certificates quickly to end users



What Certs do we Need to Deploy?

1. One or more CA Trusted Root Certificates:

Used to establish a chain of trust for Identity Certificates

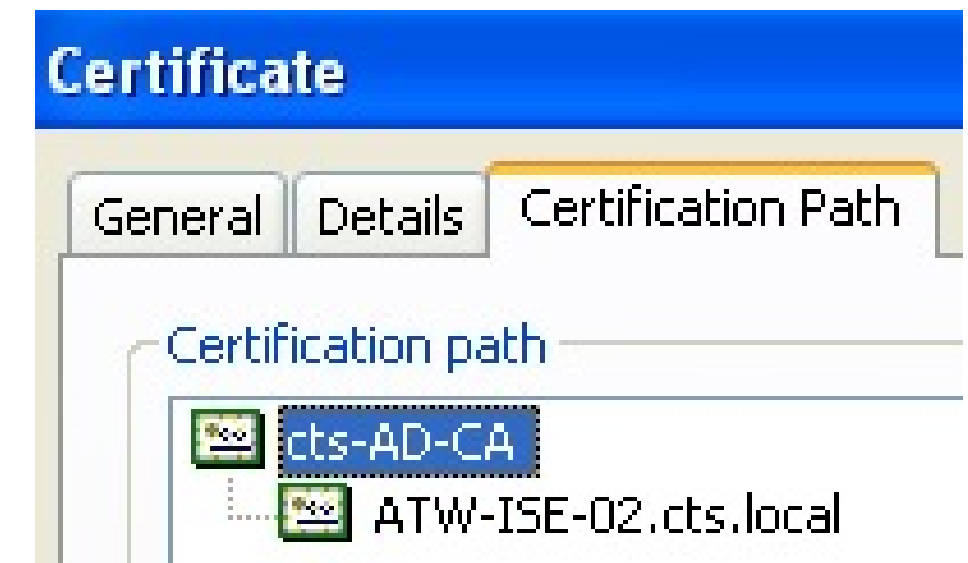
- Both sides, ASA and VPN clients, need proper certificate chains in place

1. Cisco ASA Device Identity Certificate:

- Presented to remote users to identify Cisco ASA
- Only one Device Certificate per interface allowed
- Should be signed by a *Public CA* to ease deployment

1. User Identity Certificate:

- Presented by remote users to identify themselves to the ASA
- ASA can authenticate either User or Machine certificates
- Usually signed by an *internal CA* to decrease costs and ease deployment



Certificate Deployment Considerations

Easy as 1-2-3 😊

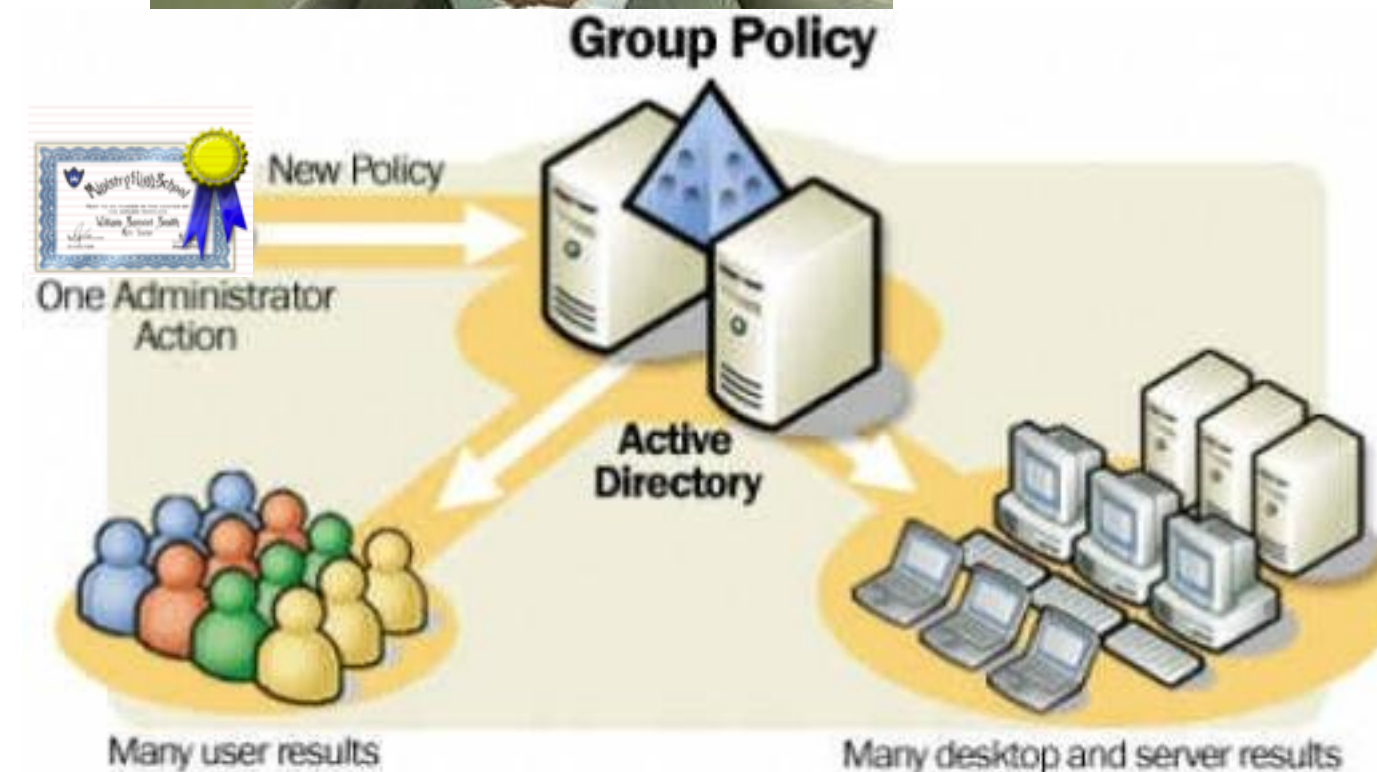
1. Choosing a Certificate Authority Solution
2. Best Practice Configuration of CA Server
3. Best practices for deploying device and user certificates on various device types

Cisco Certificate Authorities

- **Cisco IOS Router CA [*recommended for small/medium sized S2S VPNs]**
 - Well suited for Site to Site IPSEC VPN deployments
 - Supports Secure Device Provisioning (SDP) for easy router cert deployment
- **Cisco ASA CA [*recommended for small SSLVPN deployments]**
 - Remote Access AnyConnect usage only
 - Integrates basic CA operation into the ASA
- **Cisco Identity Services Engine (ISE)**
[*recommended for provisioning wired/wireless non-AD PCs and mobile devices]
 - Provides Certificate and Client Provisioning
 - Not a CA!... It is a SCEP Proxy

Microsoft Certificate Authority

- **Active Directory Certificate Services**
 - Built into Windows Server OS (Save\$)
 - Windows Server 2008 R2 Enterprise is recommended
- **Automatic Certificate Enrollment!!!**
 - AD Group Policy cert push to domain computers
 - Fully Active Directory Integrated
 - SCEP support for easy deployment to mobile / non-AD



Microsoft 2008 R2 Editions

| Components | Web edition | Standard edition | Enterprise edition | Datacenter edition |
|---|-------------|------------------|--------------------|--------------------|
| CA | No | Yes | Yes | Yes |
| Network Device Enrollment Service | No | No | Yes | Yes |
| Online Responder service | No | No | Yes | Yes |
| CA Web Enrollment | No | Yes | Yes | Yes |
| Certificate Enrollment Web Service | No | Yes | Yes | Yes |
| Certificate Enrollment Policy Web Service | No | Yes | Yes | Yes |

| AD CS features | Web edition | Standard edition | Enterprise edition | Datacenter edition |
|--|-------------|------------------|--------------------|--------------------|
| Customizable version 2 and version 3 certificate templates | No | Yes | Yes | Yes |
| Key archival | No | Yes | Yes | Yes |
| Role separation | No | No | Yes | Yes |
| Certificate manager restrictions | No | No | Yes | Yes |
| Delegated enrollment agent restrictions | No | No | Yes | Yes |
| Certificate enrollment across forest boundaries | No | No | Yes | Yes |

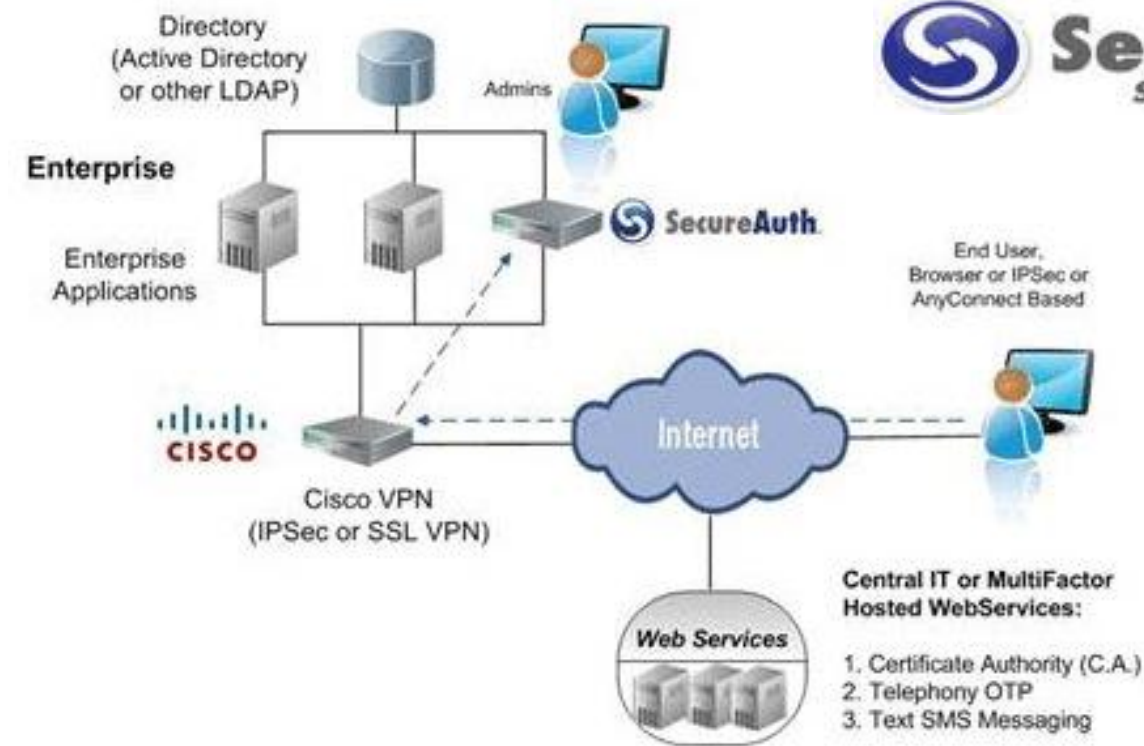
Other Certificate Authorities

- On Premise

- Appliance based
- Broad feature support
- Windows & Non-Windows focus

- Hosted

- Cloud based SaaS offering
- Less care and feeding
- Usually more expensive



Entrust[®]

RSA
SECURITY[®]

Cisco *live!*

Certificate Authority Recommendations

If Mostly AD Domain Joined Computers:

- Microsoft Windows 2008 R2 Enterprise Certificate Authority
 - Low cost, most Windows Server customers already own this
 - User and Machine certificates can be auto deployed using Group Policy
 - SCEP and Web enrollment support for mobile / non domain devices

Mostly non-domain joined computers and non-windows devices

- MSFT or 3rd party on premise or cloud service
 - Tightly integrated with Cisco ASA
 - Streamlined enrollment process

Best Practice Configuration of CA Servers

VPN Use Case



Cisco ASA Certificate Authority

Configuration Best Practices for Small Businesses

- Considerations with using ASA CA
 - Small deployments only <50
 - No support for High Availability (LB or FO)
 - Cannot be subordinate CA, only root
 - Web enrollment via email invitation only
 - OTP is only enrollment validation method
 - Does not support CSR files only copy/paste
 - No SCEP support



From: asa-ca@cisco.com
Subject: Reminder: Certificate Enrollment Invitation
Date: April 3, 2012 9:05:30 PM EDT
To: jfanelli@cisco.com

You have been granted access to enroll for a certificate.

The credentials below can be used to obtain your certificate.

Username: jfanelli
One-time Password: 7036DE559A8E6CF6
Enrollment is allowed until: 22:04:40 EDT Wed Apr 4 2012

NOTE: The one-time password is also used as the passphrase to unlock the certificate file.

Please visit the following site to obtain your certificate:

<https://asa-ca.sfd-dc-lab.cisco.com/+CSCOCA+/enroll.html>

You may be asked to verify the fingerprint/thumbprint of the CA certificate during installation of the certificates. The fingerprint/thumbprint should be:

MD5: 5D1334D5 561B1179 EF2FFBB3 2C67A5D7
SHA1: DCA06E7A FDF448A6 7485ABE6 2A2E9436 214D27D5

Cisco ASA CA Configuration

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server

Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, click the **Configure** button.

Create Certificate Authority Server

Enable Disable

Passphrase:

Issuer Name:

CA Server Key Size:

Client Key Size:

CA Certificate Lifetime: days

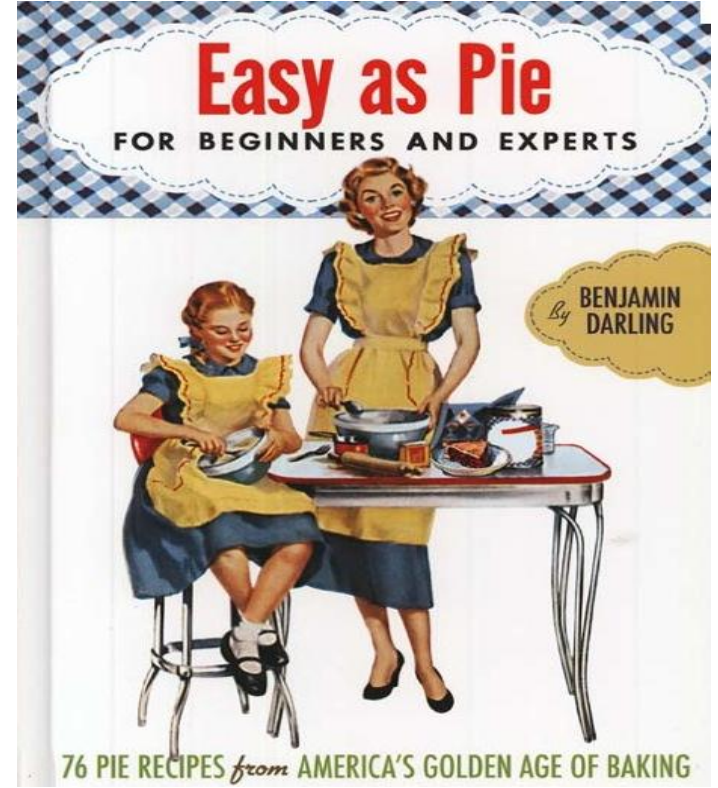
Client Certificate Lifetime: days

SMTP Server & Email Settings

Server Name/IP Address:

From Address:

Subject:



- Minimum configuration steps:**
1. Passphrase to secure CA key files
 2. Email server settings to notify users of enrollment

ASA CA Operations and User Enrollment

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

| Username | Email | Subject Name | Enrollment Status | Certificate Holder |
|----------|-------------|----------------------|-------------------|--------------------|
| jfanelli | jefanell... | CN=cisco\jefanell... | allowed | no |

Add User

Username: jfanelli

Email: jefanell@cisco.com

DN String: CN=cisco\jefanell,OU=Borderless Security Team,O=Cisc

enrollment

Help Cancel Add User

Add Edit Delete Allow Enrollment Email OTP View/Re-generate OT

Mozilla Firefox

cisco.com https://asa-ca.sfd-dc-lab.cisco.com/+CSCOCA+/login.html

https://asa-ca...CA+/login.html

ASA - Local Certificate Authority

CISCO

ASA - Local Certificate Authority

Username

One-time Password

Submit Reset

NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

1) Add a New User and Email OTP

2) User Obtains Certificate from:

<https://<asa-webvpn-interface>/+CSCOCA+/enroll.html>

3) User logs on to SSLVPN

Cisco ASA SSLVPN Connection Log

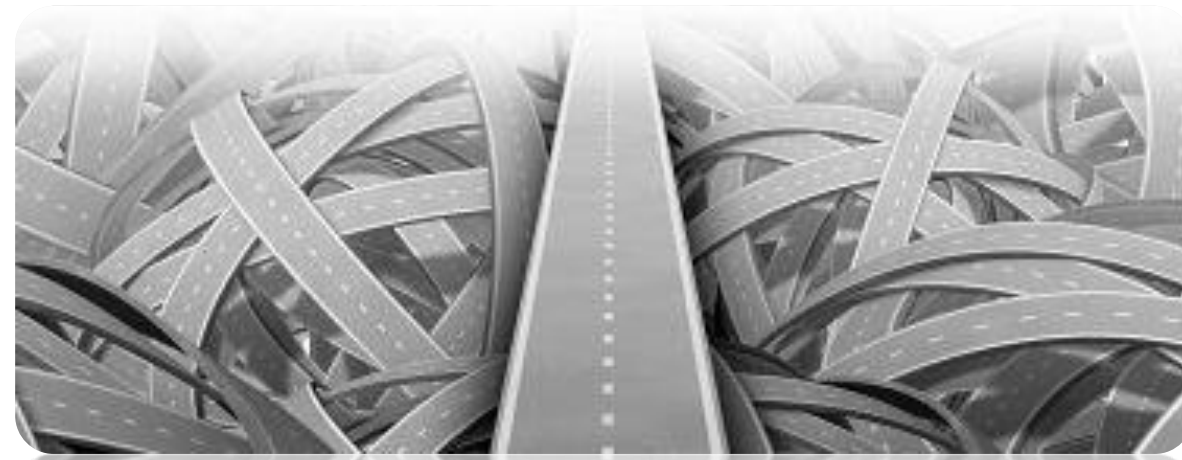
Successful certificate authentication should show:

- Certificate validation showing Cert username
- Certificate chain validation with CRL check
- Tunnel Group Certificate Matching Rule (optional)
- DAP rule matches + IP address assignment

```
Description
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> UDP SVC connection established without compression
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> First UDP SVC connection established for SVC session.
DAP: User cisco\jefanell, Addr 166.147.96.128, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> Address <192.168.52.1> assigned to session
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> TCP SVC connection established without compression
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> First TCP SVC connection established for SVC session.
TunnelGroup <AC_Split_Profile> GroupPolicy <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> No IPv6 address available for SVC connection
IPAA: Local pool request succeeded for tunnel-group 'AC_Split_Profile'
IPAA: Client assigned 192.168.52.1 from local pool
Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> WebVPN session started.

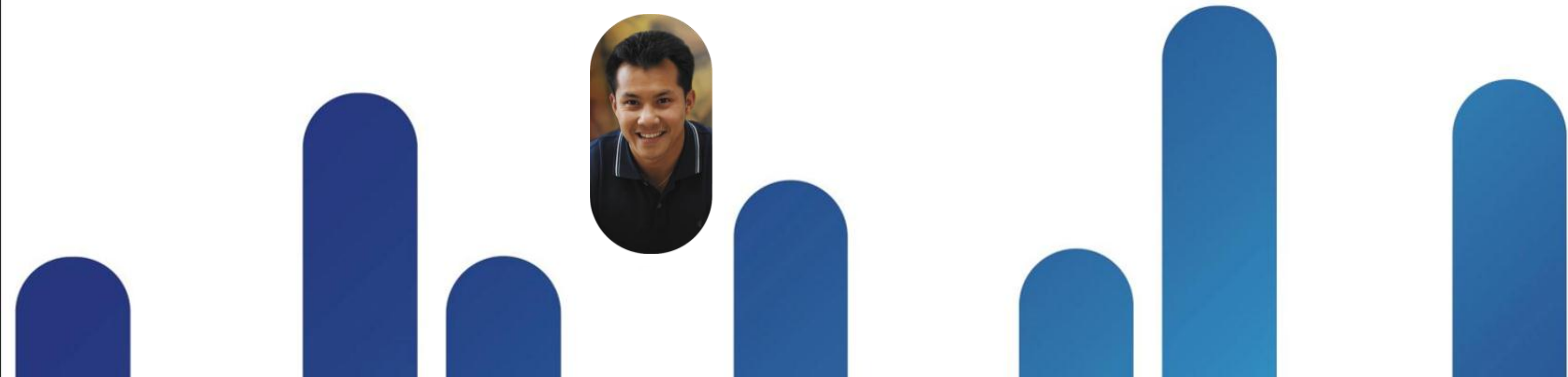
Group <DfltGrpPolicy> User <cisco\jefanell> IP <166.147.96.128> Authentication: successful, Session Type: WebVPN.
Tunnel group search using certificate maps failed for peer certificate: serial number: 02, subject name: cn=cisco\jefanell,ou=Borderless Security Team,...
AAA retrieved default group policy (Split_Policy) for user = cisco\jefanell

Tunnel group search using certificate maps failed for peer certificate: serial number: 02, subject name: cn=cisco\jefanell,ou=Borderless Security Team,...
Certificate chain was successfully validated with revocation status check.
Certificate was successfully validated. serial number: 02, subject name: cn=cisco\jefanell,ou=Borderless Security Team,o=Cisco,c=US,st=MI,ea=jefan...
```



Configuring Microsoft CA

Best Practices!



Windows 2008 R2 Certificate Services

On a AD plus IIS server...

- Add administrator or SCEP_User to IIS_IUSRS group
- Add AD-CS Role plus Role Services to your Domain Controller

Server Manager

The screenshot shows the Windows Server Manager interface for Active Directory Certificate Services (AD CS). The 'Role Status' section indicates that all system services are running and there are no messages or events. The 'Role Services' section shows that four services are installed: Certification Authority, Certification Authority Web Enrollment, Online Responder, and Network Device Enrollment Service. The other two services, Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service, are not installed. A red circle highlights the installed services table.

Active Directory Certificate Services AD CS Help

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications

Role Status Go to Active Directory Certificate Services

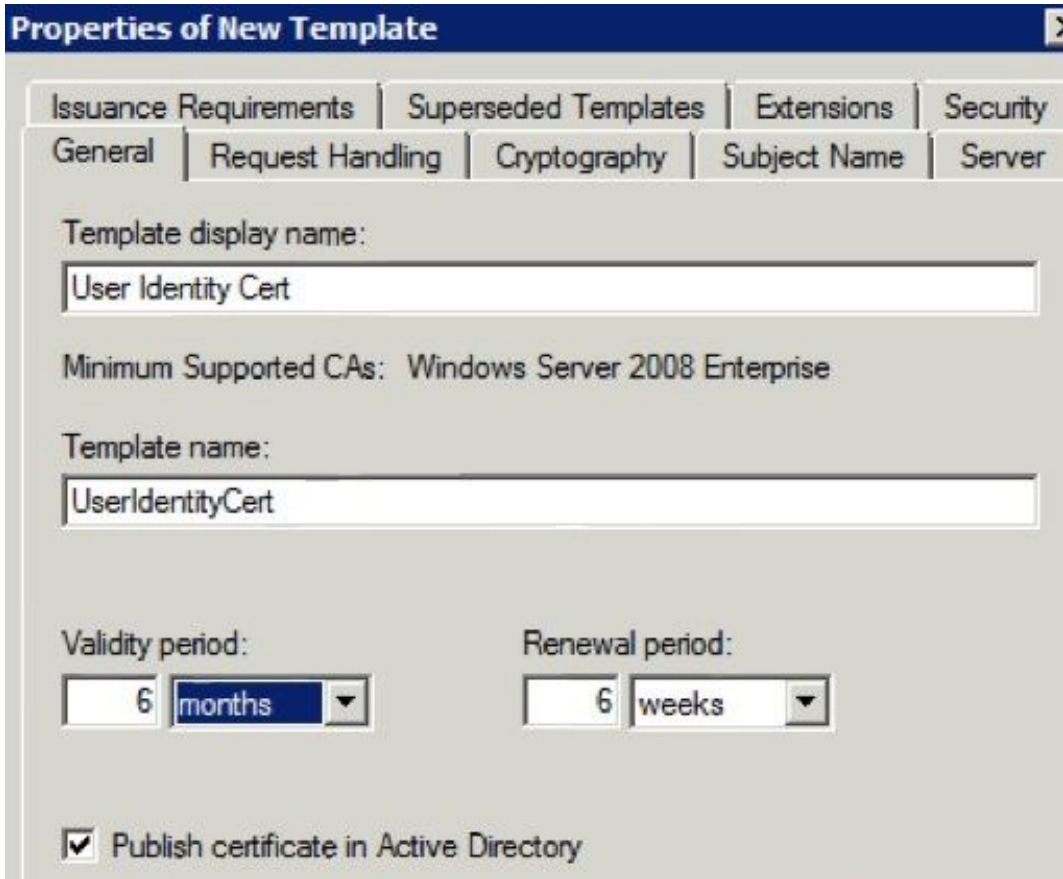
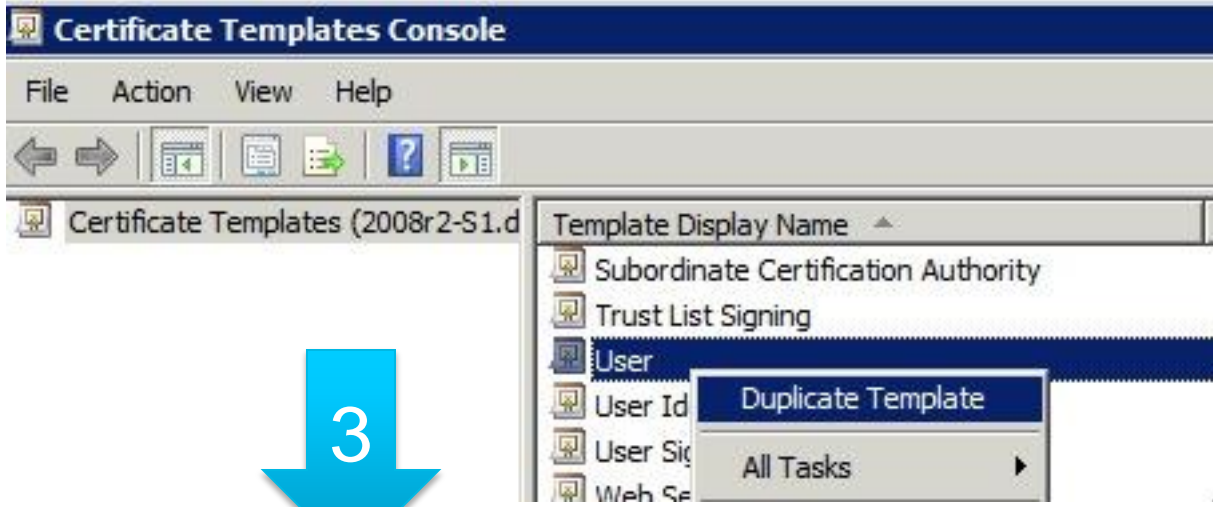
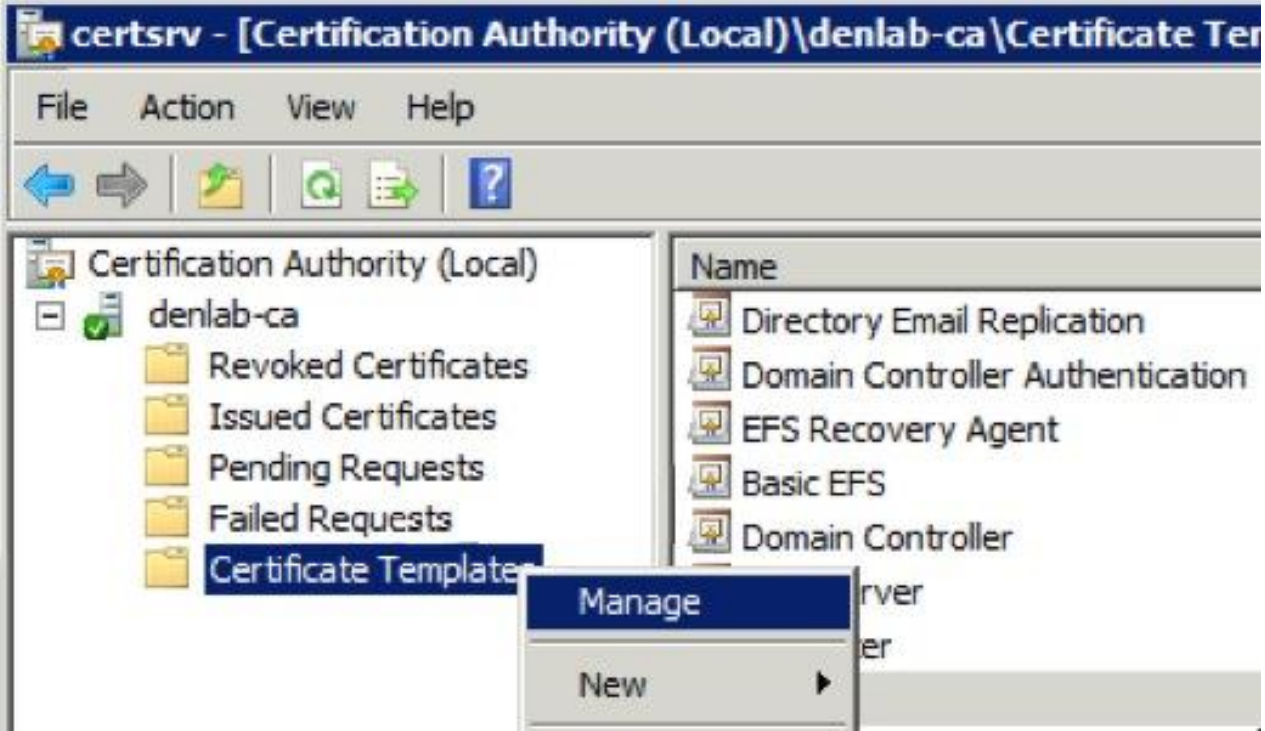
Messages: None
System Services: All Running
Events: None in the last 24 hours
Best Practices Analyzer: 1 noncompliant; 0 excluded; 7 compliant Last Scan: 4/15/2012 1:05:09 PM

Role Services: 4 installed Add Role Services
Remove Role Services

| Role Service | Status |
|---|---------------|
| Certification Authority | Installed |
| Certification Authority Web Enrollment | Installed |
| Online Responder | Installed |
| Network Device Enrollment Service | Installed |
| Certificate Enrollment Web Service | Not installed |
| Certificate Enrollment Policy Web Service | Not installed |

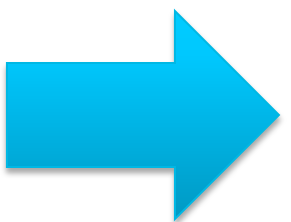
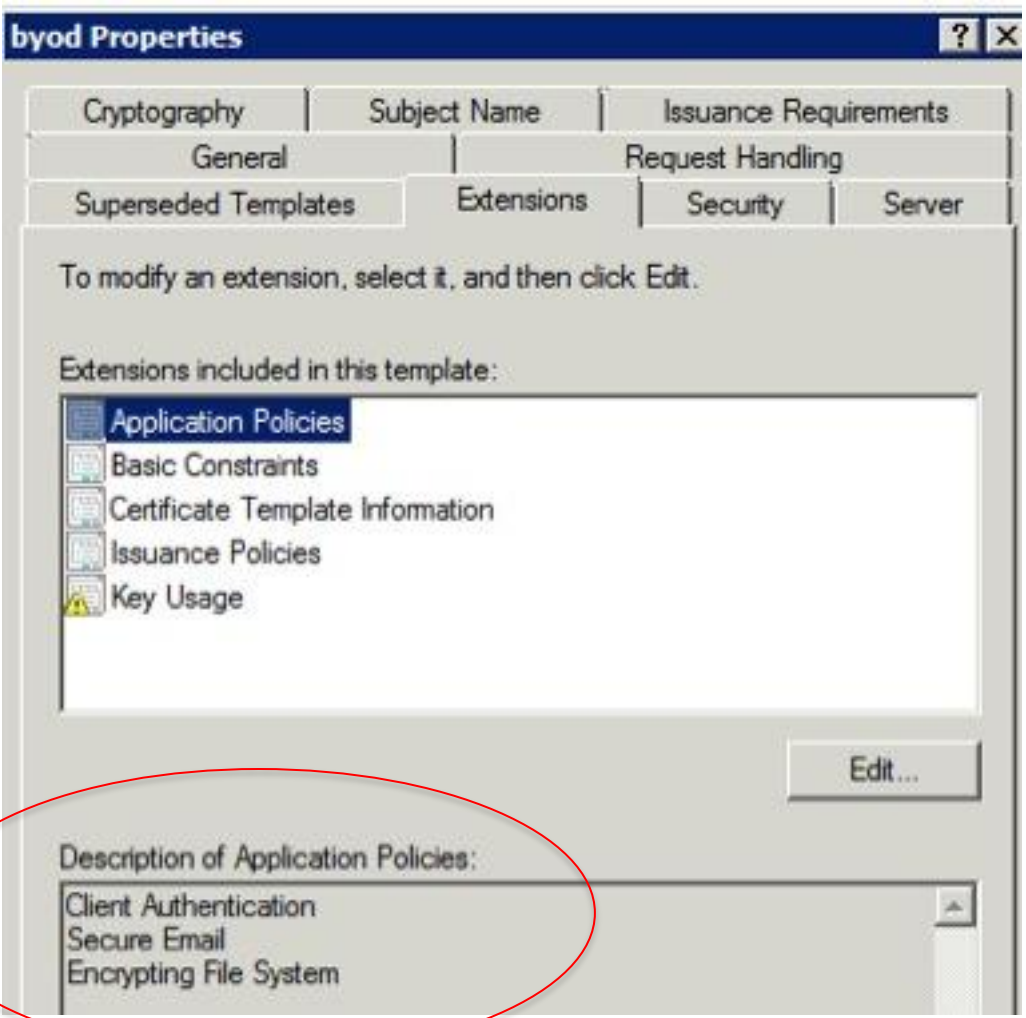
Create Your Certificate Template

1. Open MMC > Certificates Snap-in

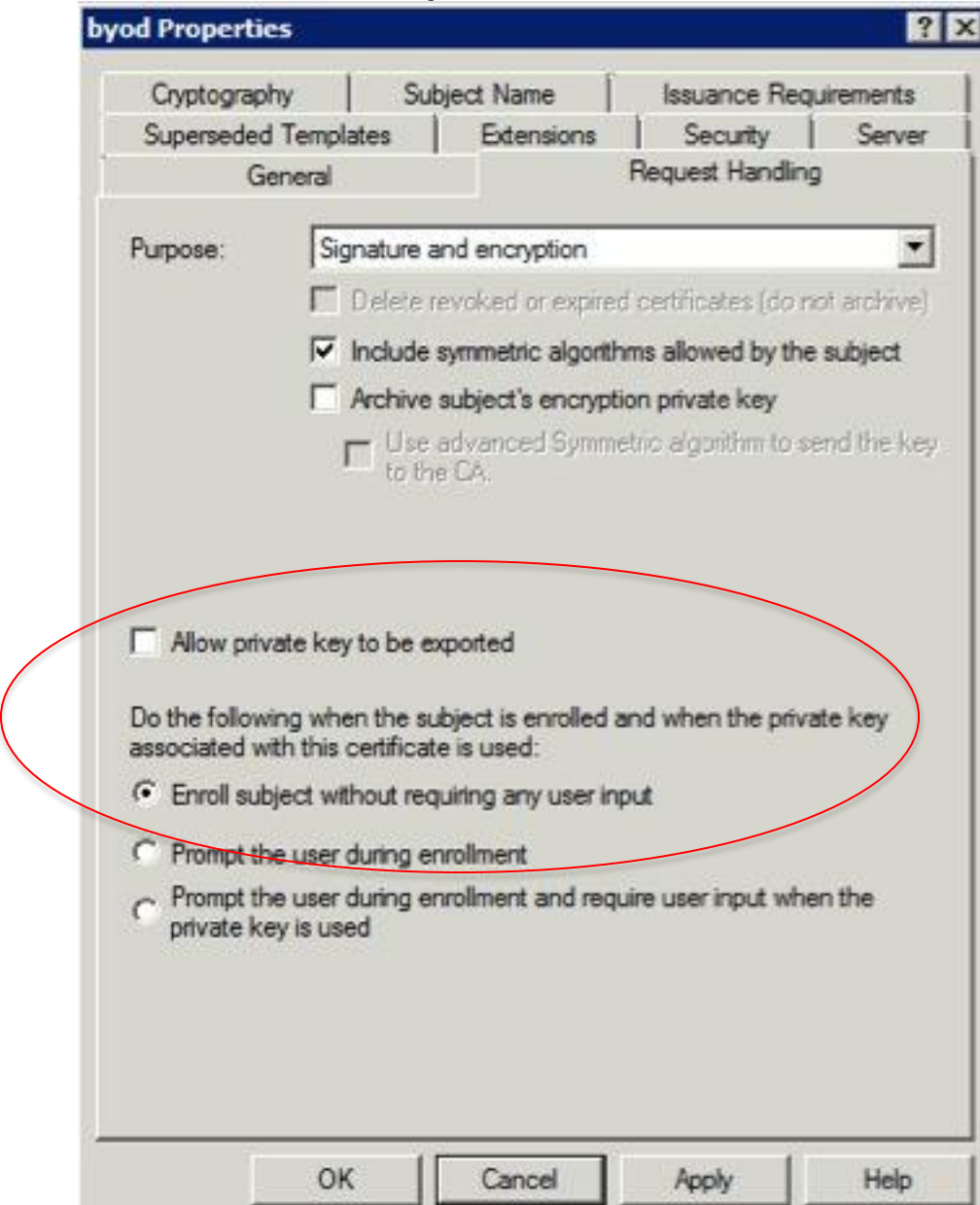


Certificate Template Changes

Check Extensions/App Policies

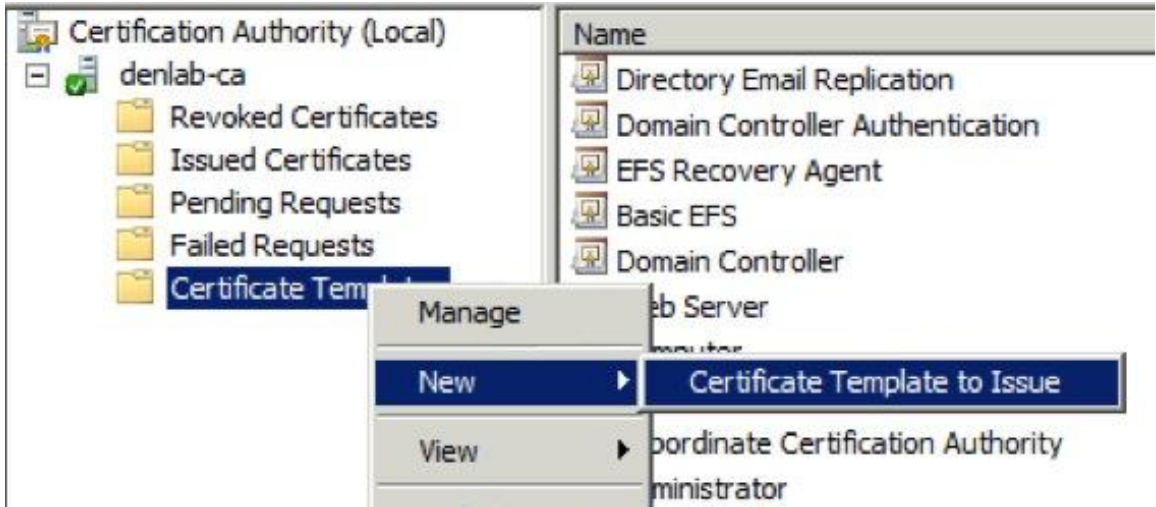
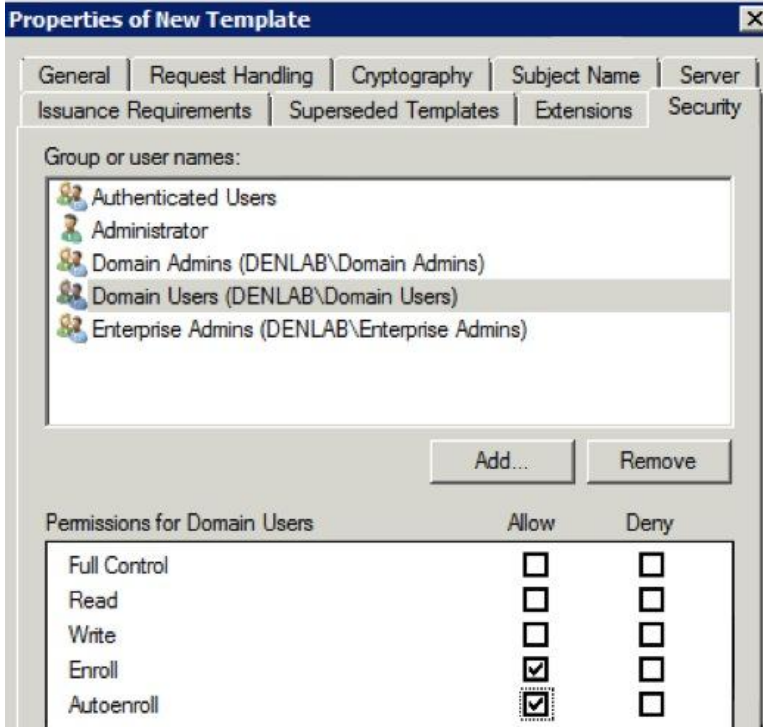
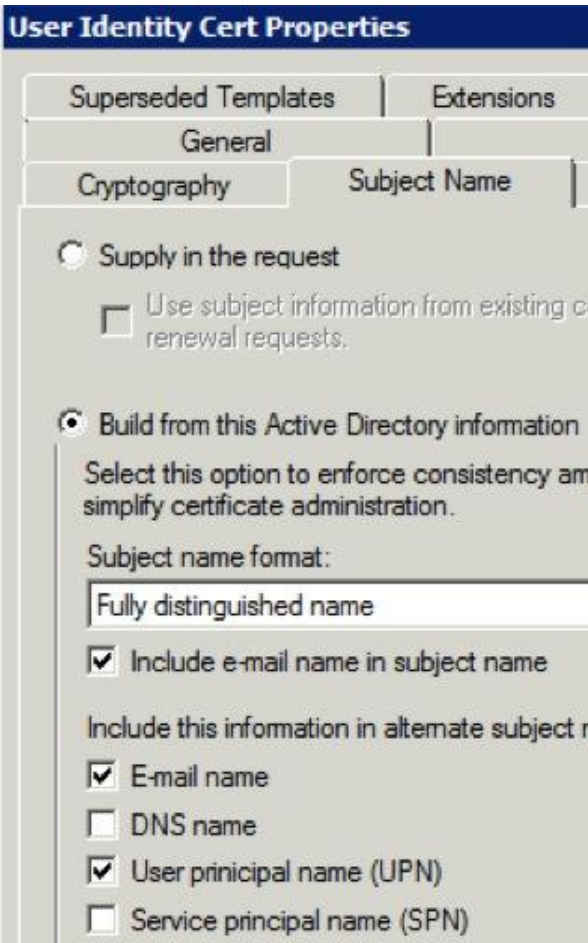


Disable Export of Certs



Certificate Template Final Steps

- Select the subject criteria
- Must have email populated in accounts for Auto-enroll
- Publish Template!

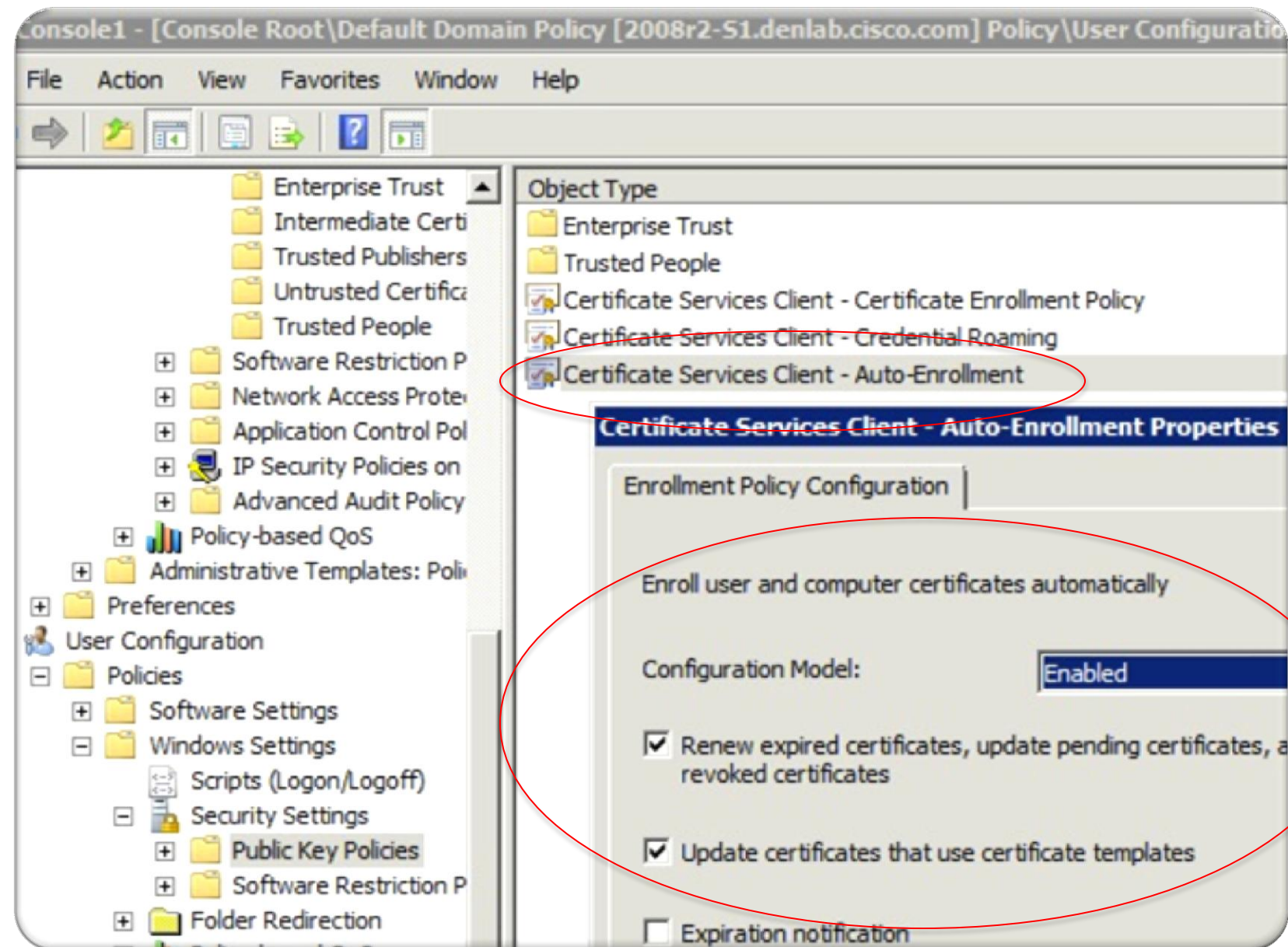
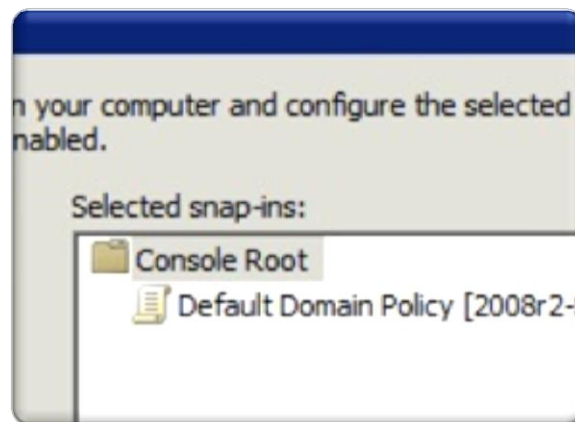


Enable GPO Auto-enrollment User Certs

1-Step Deployment!!! Who says certs are hard?

- Enable Auto-enrollment in the MMC>Default Domain Policy > User Configuration

- Done! 

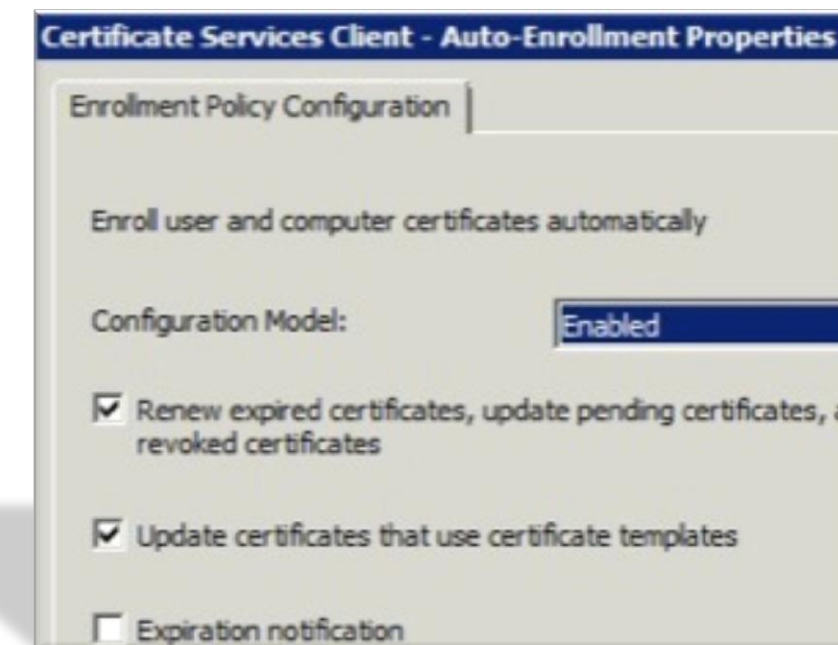
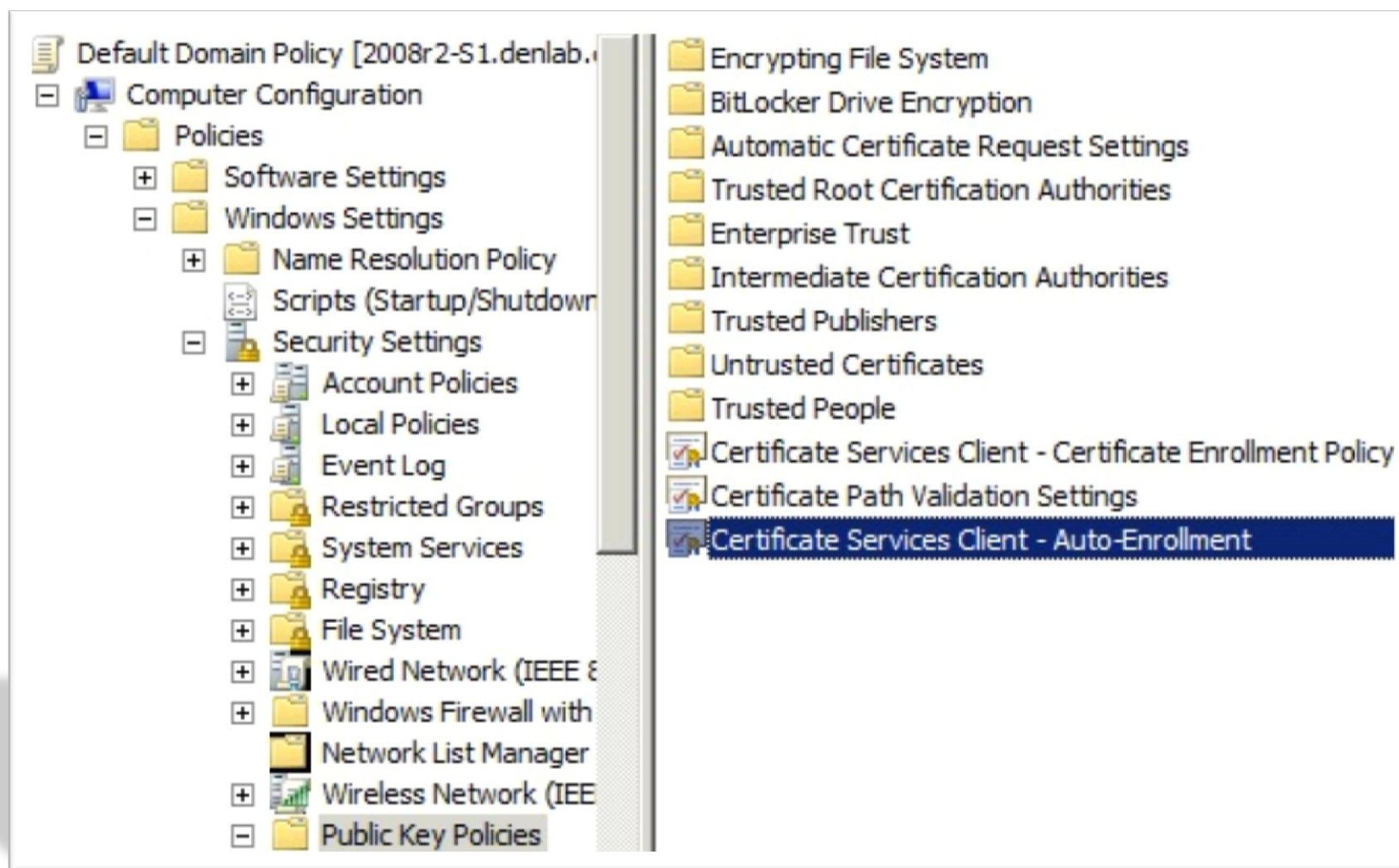


-Users get certs as soon as GPO refreshes on their PC
-By Default this is ~90 minutes max

Enable GPO Auto-enrollment Computer Certs

Yep still a 1-step deployment. Bang!

- Enable Auto-enrollment in the Default Domain Policy > Computer Configuration



```
C:\Users\jheary.DENLAB>gpupdate /force
Updating Policy...

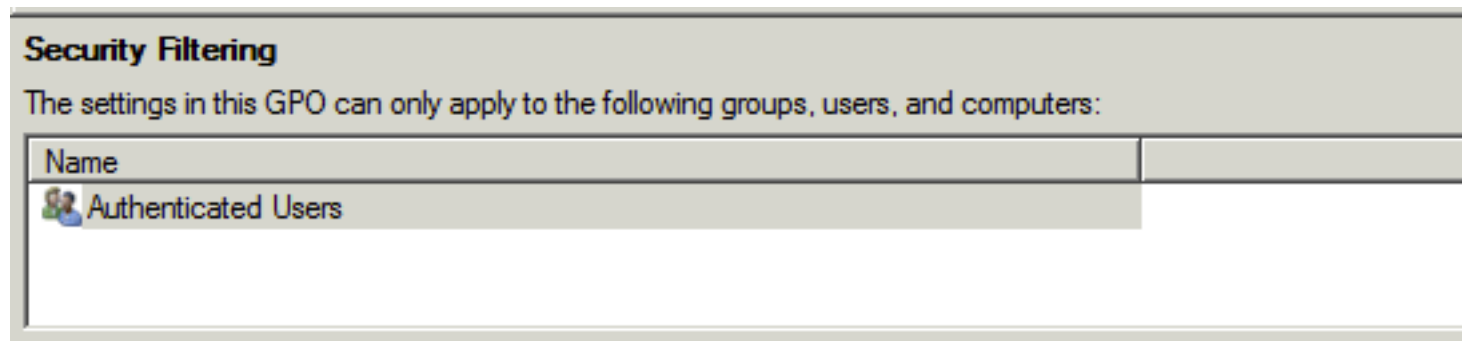
User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\Users\jheary.DENLAB>
```

GPO Authorisation

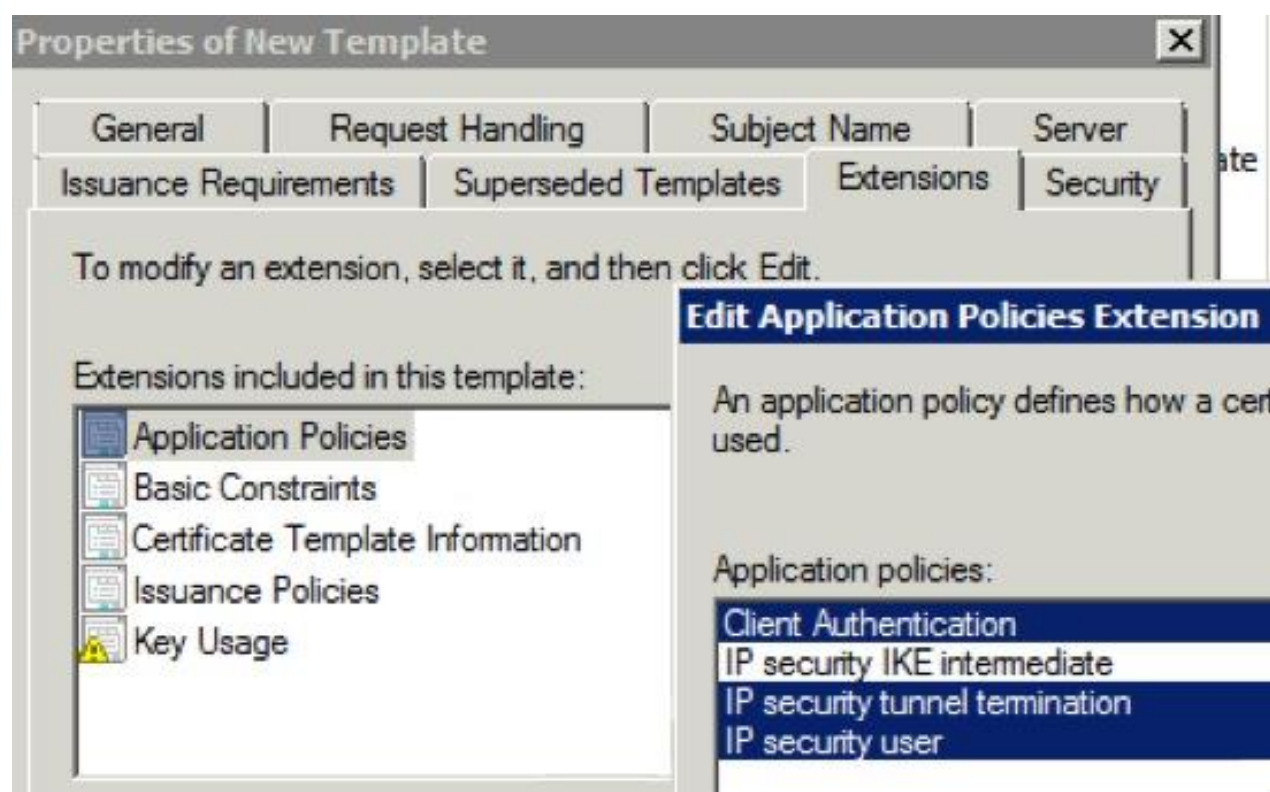
Just in case

Verify GPO policies allow certificates to be used for authentication



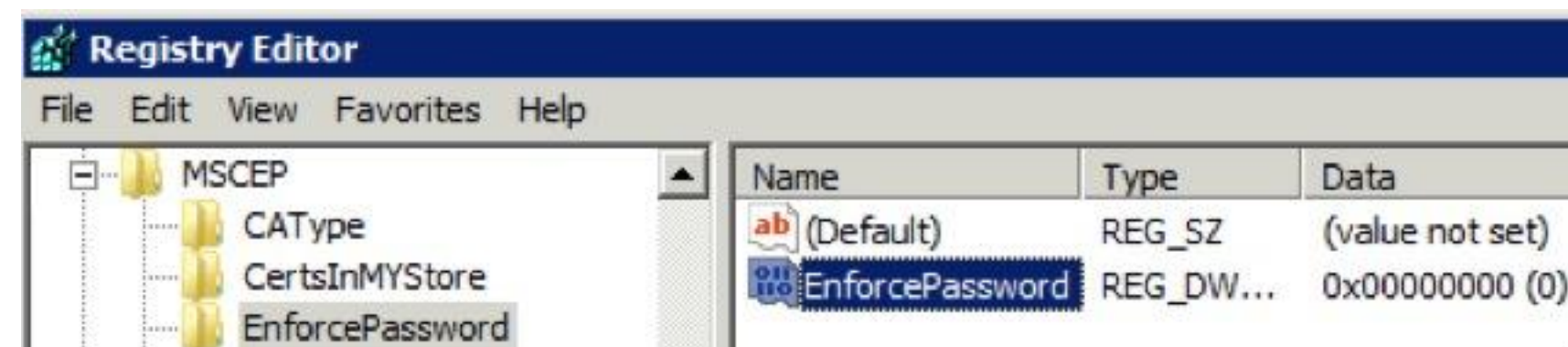
Enable SCEP for non-AD joined Hosts

1. Clone the IPSECIntermediateOffline Template
2. Change Application Policies
3. Issue Certificate Template



4. Open Regedit
5. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP
5. Change GeneralPurposeTemplate to match the new clone
6. Optional: Disable Force OTP for SCEP
7. Reboot CA Server

| Name | Type | Data |
|------------------------|--------|--------------------------|
| (Default) | REG_SZ | (value not set) |
| EncryptionTemplate | REG_SZ | IPSECIntermediateOffline |
| GeneralPurposeTemplate | REG_SZ | SCEPCert |
| SignatureTemplate | REG_SZ | IPSECIntermediateOffline |



ASA CA Cert SCEP Enrollment

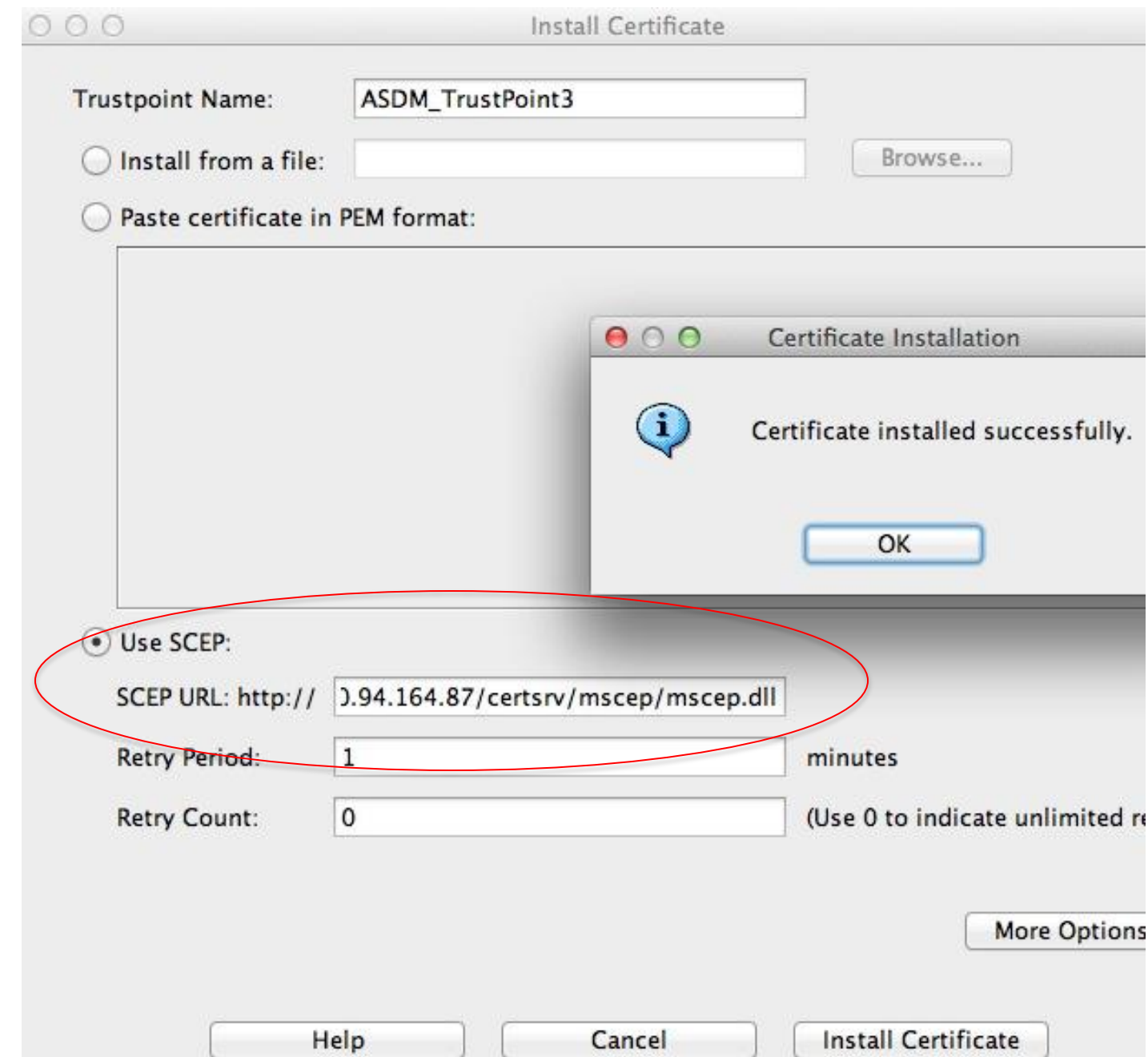
Adds CA Server Certificate chain to ASA

Default CA SCEP URL:

HTTP://<CA Server>/certserv/mscep/mscep.dll

Configuration > Remote Access VPN > Certificate Management > CA Certificates

| Issued To | Issued By | Expiry Date |
|--|---------------------------------------|--------------------------|
| HomeFW.appledreams.com | cn=HomeFW.appledreams.com | 14:00:20 MDT Sep 1 2013 |
| denlab-ca | cn=denlab-ca, dc=denlab, dc=cisc... | 20:46:19 MDT Apr 11 2017 |
| VeriSign Class 3 Secure Server CA - G3 | cn=VeriSign Class 3 Public Primary... | 16:59:59 MST Feb 7 2020 |



ASA Identity Cert SCEP Enrollment

Example

Go to Remote Access VPN > Certificate Management > Identity Certificates

The 'Add Identity Certificate' dialog box is shown. The 'Trustpoint Name' is 'ASDM_TrustPoint2'. The 'Add a new identity certificate' radio button is selected. The 'Key Pair' dropdown is set to 'denlab-ASA'. The 'Certificate Subject DN' is 'CN=denlab-asa'. The 'Advanced...' button is circled in red. At the bottom are 'Help', 'Cancel', and 'Add Certificate' buttons.

The 'Advanced Options' dialog box is shown with the 'Certificate Parameters' tab selected. The 'Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.' message is at the top. The 'FQDN' is 'denlab-asa.denlab.cisco.com', 'E-mail' is empty, and 'IP Address' is '10.20.246.5'. The 'Include serial number of the device' checkbox is checked.

The 'Advanced Options' dialog box is shown with the 'Enrollment Mode' tab selected. The 'Request from a CA' radio button is selected. The 'Enrollment URL (SCEP)' is 'http://10.94.164.87/certsrv/mscep/mscep.dll'. The 'Retry Period' is '1' minutes and the 'Retry Count' is '2'.

How to Verify or Revoke a Certificate

- See what certs have been issued
- Revoke Certificates when required
- *CRL Validity is 1 week + 10% by default on 2008R2 CA
- OCSP updates can be near real-time

The screenshot shows the Certification Authority console for 'denlab-ca'. The main pane displays a table of issued certificates. A context menu is open over the selected certificate (Request ID 13), with the 'Revoke Certificate' option highlighted.

| Request ID | Requester Name | Binary Certificate | Certificate Template | Serial Number |
|------------|-------------------------|---------------------|--------------------------|-----------------|
| 2 | DENLAB\2008R2-S1\$ | -----BEGIN CERTI... | Domain Controller (...) | 61147f1e000... |
| 7 | DENLAB\jheary | -----BEGIN CERTI... | User Identity Cert (...) | 18d47d77000... |
| 9 | DENLAB\Administrator | -----BEGIN CERTI... | Exchange Enrollmen... | 19fef9dc0000... |
| 10 | DENLAB\Administrator | -----BEGIN CERTI... | CEP Encryption (CE... | 19fefbd0000... |
| 11 | DENLAB\2008R2-S1\$ | -----BEGIN CERTI... | Directory Email Repli... | 1a0f8e7d000... |
| 12 | DENLAB\2008R2-S1\$ | -----BEGIN CERTI... | Domain Controller A... | 1a0f9013000... |
| 13 | DENLAB\WIN-EKL9A7DEVDR6 | -----BEGIN CERTI... | Computer Identity C... | 1a36de33000... |

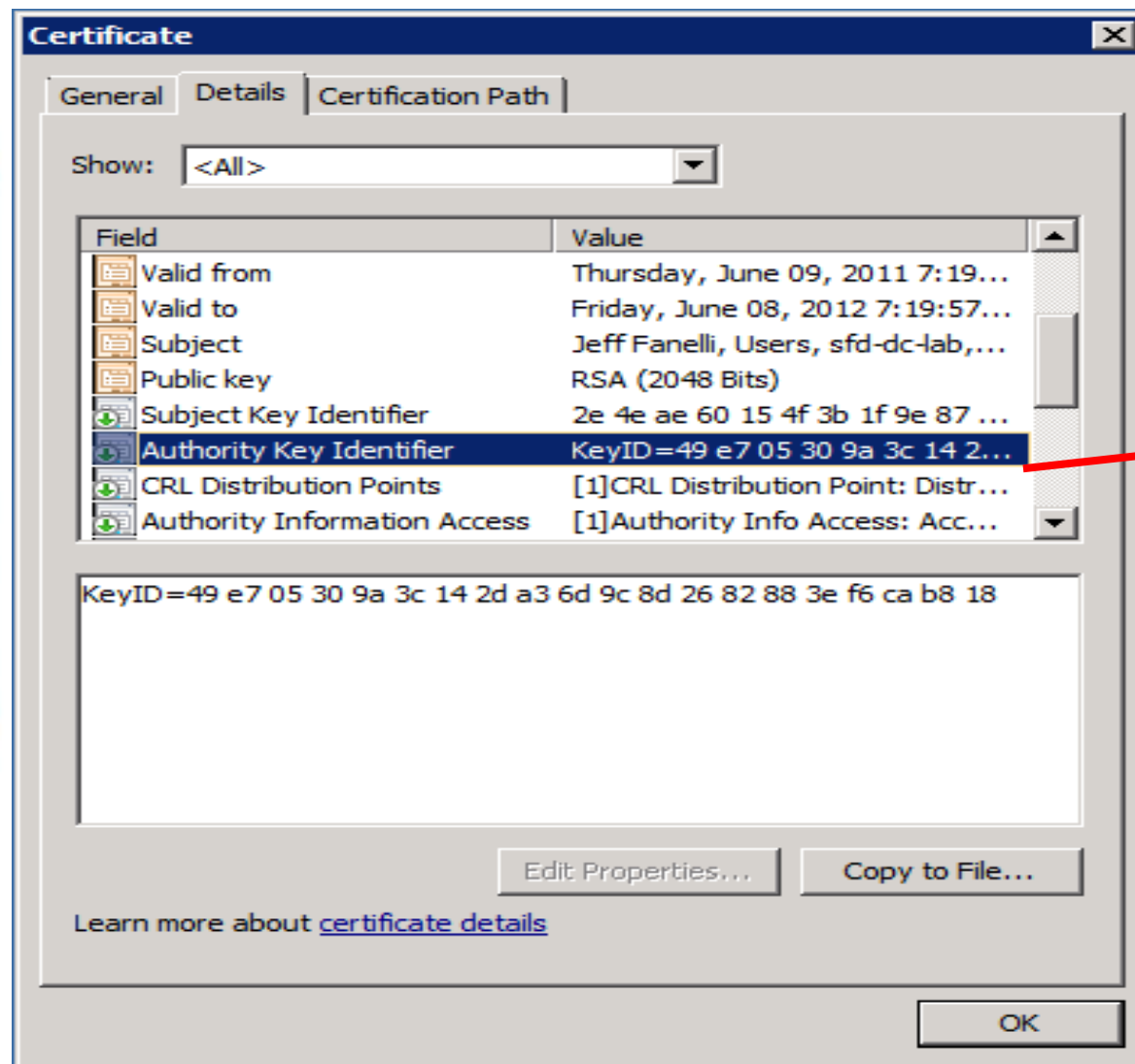
Certificate Based AnyConnect SSLVPN Monitoring and Troubleshooting



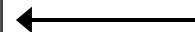
Certificate Troubleshooting

Chain of certificates may be incomplete

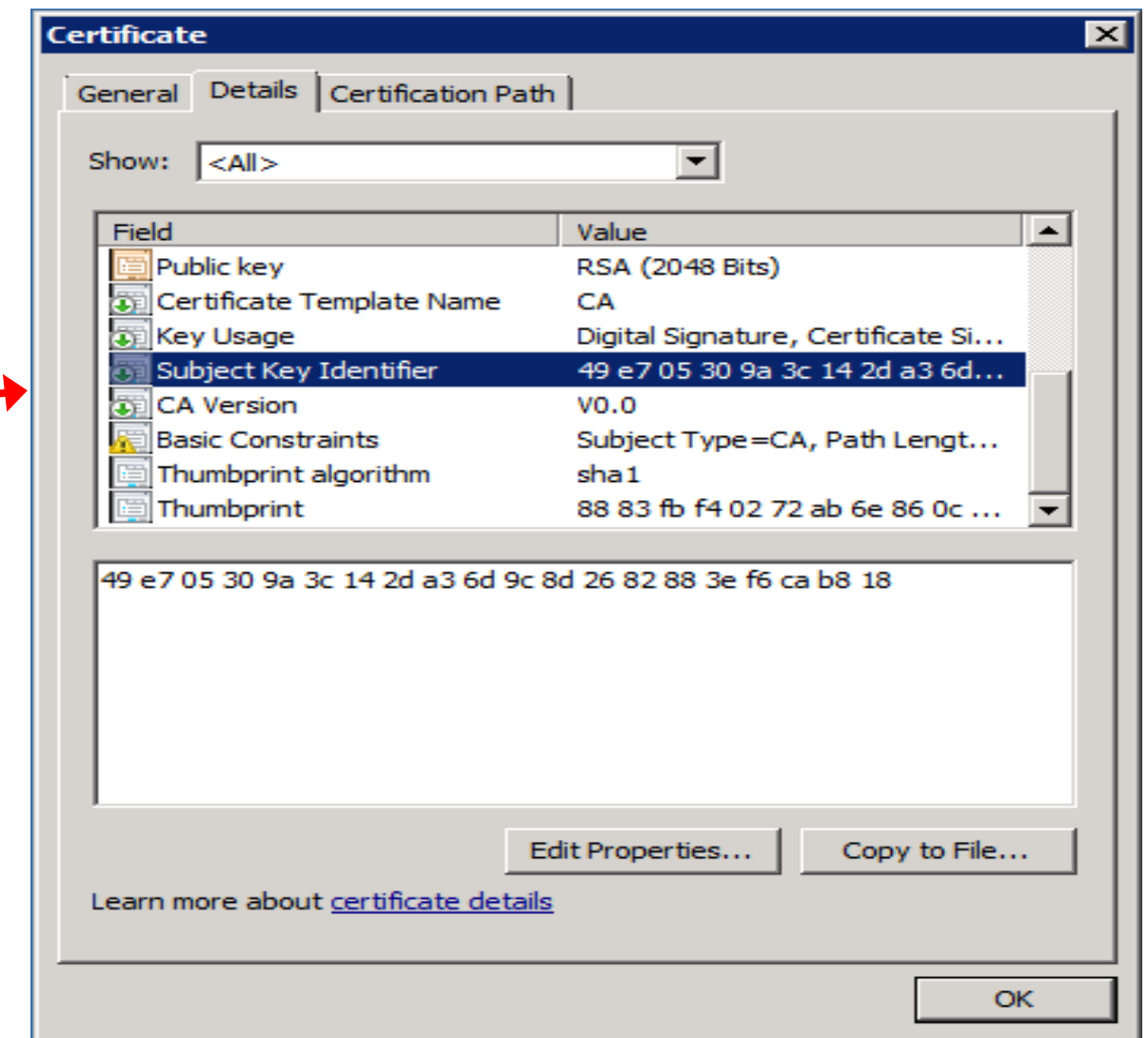
-Match Authority Key Identifier field to CA Root Cert(s)



User Cert



CA Root Cert



MSFT CA Troubleshooting

Server Manager, Event Viewer and Certificate Services are FULL of info

Server Manager (2008R2-S1)

- Roles
 - Active Directory Certificate
 - Active Directory Domain Se
 - DHCP Server
 - DNS Server
 - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to create certification authorities and relate

Description:
Creates, manages, and removes X.509 certificates for applications such as S/MIME and SSL. If this serv...
is disabled, any services that explicitly depend on it will fail to start.

Best Practices Analyzer: 2 noncompliant; 0 excluded; 6 compliant Last Scan: 4/13/2012 7:14:52

Noncompliant (2) | Excluded (0) | Compliant (6) | All (8)

| Severity | Title | Category |
|----------|--|---------------|
| Warning | Computer autoenrollment group policy is not enabled | Configuration |
| Warning | CA database and log files should not be stored on the system drive | Configuration |

Event Viewer (Local)

- Custom Views
 - Server Roles
 - Active Directory Certific
 - Active Directory Domair
 - DHCP Server
 - DNS Server
 - Web Server (IIS)
 - Administrative Events
- Windows Logs

Active Directory Certificate Services

Number of events: 13

Number of events: 13

| Level | Date and Time | Source | Event ID |
|-------------|---------------|------------------------|----------|
| Information | 4/13/2012 ... | CertificationAuthority | 26 |
| Information | 4/13/2012 ... | CertificationAuthority | 38 |
| Information | 4/13/2012 ... | CertificationAuthority | 26 |
| Information | 4/13/2012 ... | CertificationAuthority | 38 |
| Warning | 4/13/2012 ... | CertificationAuthority | 53 |

Certification Authority (Local)

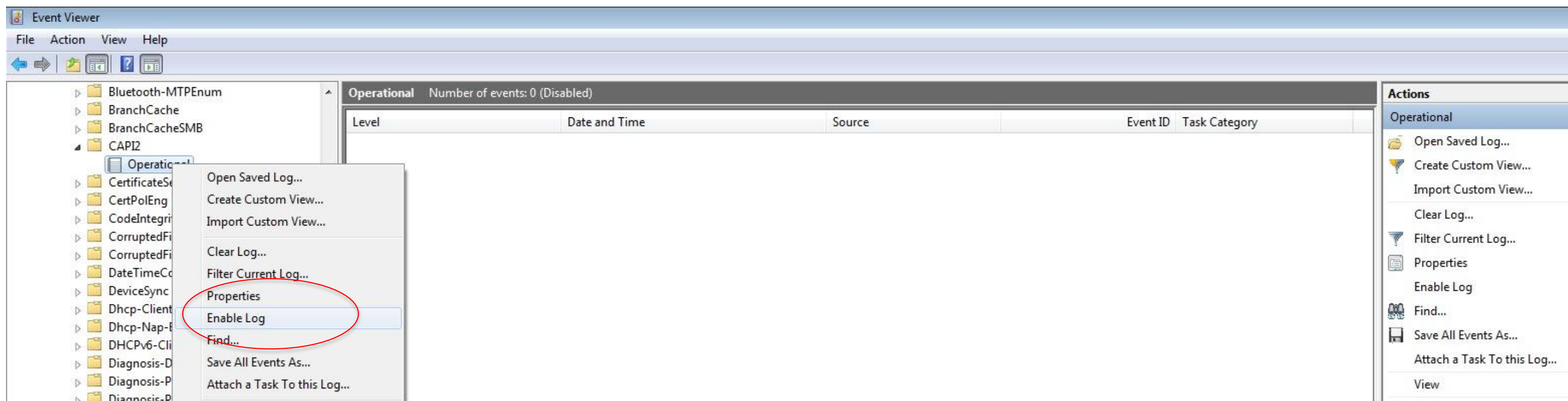
- denlab-ca
 - Revoked Certificates
 - Issued Certificates
 - Pending Requests
 - Failed Requests

| Request ID | Bin... | Request Status Code | Request Disposition Message |
|------------|--------|---|-----------------------------|
| 3 | ---- | The EMail name is unavailable and cannot be added to the Subject... | Denied by Policy Module |
| 4 | ---- | The EMail name is unavailable and cannot be added to the Subject... | Denied by Policy Module |



Microsoft CA Event Viewer

- Works on Vista/Win7 or CA Server 2008
- For more detailed logs turn on CryptoAPI 2.0 Diagnostics logging
 1. In the Event Viewer, navigate to **Application Logs > Microsoft> Windows> CryptoAPI 2.0 or CAPI2** for the CryptoAPI 2.0 channel
 2. Right-click, Enable Log



Event Monitoring- Cisco CSM 4.2

Views

+ New Edit Delete

Predefined Views

- All Device Events
- Firewall Traffic Eve
- Firewall Denied Eve
- AAA Events
- NAT Events
- Botnet Events
- IPSec VPN Events
- SSL VPN Events**
- Failover Events
- All IPS Events
- IPS Priority Alerts
- IPS Alert Events
- IPS Status Events
- IPS Error Events

My Views

Event Monitoring

SSL VPN Events x

View Settings

Search within results: last 1 week All Events (Default) Save Start Stop Clear 20,000

| Receive Ti... | Event Name | VPN User | VPN Group | Action | Description | Device | Severity |
|------------------|---------------------------|-------------------------------|---------------------|-------------|---------------------------|--------------|----------|
| 4/11/12 1:45:... | WebVPN SVC connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | | Group <AC_SSL_Split... | asa.sfd-d... | Inform |
| 4/11/12 1:45:... | WebVPN Session Termin... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | terminated | Group <AC_SSL_Split... | asa.sfd-d... | Inform |
| 4/11/12 1:45:... | WebVPN SVC connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | closing | Group <AC_SSL_Split... | asa.sfd-d... | Notific |
| 4/11/12 1:45:... | WebVPN SVC Message | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | | Group <AC_SSL_Split... | asa.sfd-d... | Notific |
| 4/11/12 1:45:... | WebVPN SVC connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | | Group <AC_SSL_Split... | asa.sfd-d... | Inform |
| 4/11/12 1:45:... | SSL Session terminated | | | | SSL session with clien... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | WebVPN SVC connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | established | Group <AC_SSL_Split... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | WebVPN SVC Connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | established | Group <AC_SSL_Split... | asa.sfd-d... | Notific |
| 4/11/12 1:44:... | SSLHandshake completed | | | | Device completed SSL... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | SSL Client session resume | | | | SSL client outside:jef... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | SSL handshake Started | | | | Starting SSL handsha... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | WebVPN address assigned | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | | Group <AC_SSL_Split... | asa.sfd-d... | Warni |
| 4/11/12 1:44:... | WebVPN SVC connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | established | Group <AC_SSL_Split... | asa.sfd-d... | Inform |
| 4/11/12 1:44:... | WebVPN SVC Connection... | jfanelli@sfd-dc-lab.cisco.com | AC_SSL_Split_Policy | established | Group <AC_SSL_Split... | asa.sfd-d... | Notific |

Event Details

| | | | | | |
|---------------|--------------------------|------------|---------------------------|-------------|---|
| Receive Time | 4/11/12 1:45:04 AM | Event Name | WebVPN Session Terminated | VPN User | jfanelli@sfd-dc-lab.cisco.com |
| VPN Group | AC_SSL_Split_Policy | Action | terminated | Description | Group <AC_SSL_Split_Policy> User <jfanelli@sfd-dc-lab.cisco.com> IP <jfanell-net> WebVPN session terminated: User Requested. |
| Device | asa.sfd-dc-lab.cisco.com | Severity | Informational | | |
| Event Type ID | 716002 | | | | |

Reporting- Cisco ACS 5 and CSM 4.2

User > User Authentication Summary

User : johender
 Protocol : RADIUS
 Time Range : March 13, 2012 - April 11, 2012 (Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on April 12, 2012 11:33:00 PM EDT

Authentications
 12 Passed Authentication(s)
 1 Failed Authentication(s)
 13 Total

Sessions
 Active Sessions

Most Recent Authentication
 Time: April 10, 2012 3:52:06.296 PM
 RADIUS Status: Authentication succeeded
 NAS Failure:
 MAC/IP Address: 10.117.66.72
 Network Device: vpn-sfd-lab : 192.168.64.1 :
 Access Service: Default Network Access
 Authorization Profiles: Permit Access
 CTS Security Group:
 Authentication Method: MSCHAPV2

Authentications By Day

| Day | Pass | Fail | Total | Fail % | Avg Response Time (ms) | Peak Re |
|----------------|------|------|-------|--------|------------------------|---------|
| April 10, 2012 | 1 | 1 | 2 | 50.00 | 650.00 | 820 |
| April 3, 2012 | 1 | 0 | 1 | 0.00 | 12.00 | 12 |
| March 28, 2012 | 1 | 0 | 1 | 0.00 | 12.00 | 12 |
| March 26, 2012 | 1 | 0 | 1 | 0.00 | 24.00 | 24 |
| March 20, 2012 | 1 | 0 | 1 | 0.00 | 9.00 | 9 |
| March 15, 2012 | 1 | 0 | 1 | 0.00 | 12.00 | 12 |
| March 14, 2012 | 5 | 0 | 5 | 0.00 | 13.00 | 20 |
| March 13, 2012 | 1 | 0 | 1 | 0.00 | 23.00 | 23 |

Authentications By Failure Reason

| Failure Reason | Total |
|---|-------|
| 24407 User authentication against Active Directory failed since user is required to change his password | 1 |

User Report

User Report - Settings Create Schedule Edit Save As Save Reset

Generate Report Print Export Chart Type: Pie

Duration : Mar 1, 2012 12:00:00 AM - Apr 1, 2012 12:00:00 AM

Generated on Apr 12, 2012 11:54:48 PM

| Username | Duration | Bandwidth (MB) | Throughput (kbps) |
|-----------------|-------------------|----------------|-------------------|
| swasko | 5days 14h:44m:33s | 45.63 | 0.75 |
| johender | 2days 14h:38m:42s | 81.27 | 2.88 |
| chadrich | 0days 20h:51m:39s | 9.78 | 1.04 |
| dark_steven | 0days 20h:09m:14s | 84.64 | 9.33 |
| jfanelli | 0days 02h:32m:28s | 0.53 | 0.47 |
| bob.christenson | 0days 01h:12m:47s | 4.18 | 7.66 |

Reporting- ACS 5

AAA Protocol > RADIUS Authentication

Network Device Name : vpn-sfd-lab

Access Service : Default Network Access

Authentication Status : Pass or Fail

Date : March 13, 2012 - April 11, 2012 ([Last 30 Minutes](#) | [Last Hour](#) | [Last 12 Hours](#) | [Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#))

Generated on April 12, 2012 11:43:09 PM EDT

✓=Pass ✗=Fail 🔍=Click for details 🖱️=Mouse over item for additional information

| ACS View Timestamp | ACS Timestamp | RADIUS Status | NAS Failure | Details | Username | MAC/IP Address | Access Service | Authentication Method | Network Device | Failure Reason |
|---------------------------|---------------------------|---------------|-------------|---------|--------------------------|----------------|--|-----------------------|-----------------------------|---|
| Apr 11,12 7:22:11.686 PM | Apr 11,12 7:22:11.610 PM | ✓ | | | jfanelli | 70.91.233.132 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | |
| Apr 11,12 2:49:15.573 PM | Apr 11,12 2:49:15.490 PM | ✓ | | | jfanelli | 10.130.2.55 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | |
| Apr 11,12 1:39:12.876 AM | Apr 11,12 1:39:12.793 AM | ✓ | | | jfanelli | 70.91.233.132 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | |
| Apr 11,12 1:39:05.336 AM | Apr 11,12 1:39:05.266 AM | ✗ | | | jfanelli | 70.91.233.132 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | 24408 User authentication against Active Directory failed since user has entered the wrong password |
| Apr 10,12 3:52:06.296 PM | Apr 10,12 3:52:06.233 PM | ✓ | | | johender | 10.117.66.72 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | |
| Apr 10,12 3:51:31.960 PM | Apr 10,12 3:51:31.883 PM | ✗ | | | johender | 10.117.66.72 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | 24407 User authentication against Active Directory failed since user is required to change his password |
| Apr 10,12 12:21:48.003 PM | Apr 10,12 12:21:47.930 PM | ✗ | | | navegupt | 10.20.219.217 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | 24408 User authentication against Active Directory failed since user has entered the wrong password |
| Apr 10,12 12:21:38.546 PM | Apr 10,12 12:21:38.470 PM | ✗ | | | navegupt | 10.20.219.217 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | 24408 User authentication against Active Directory failed since user has entered the wrong password |
| Apr 10,12 12:21:28.693 PM | Apr 10,12 12:21:28.620 PM | ✗ | | | navegupt | 10.20.219.217 | Default Network Access | MSCHAPV2 | vpn-sfd-lab | 24409 User authentication against Active Directory failed since the user account is disabled |

Agenda

- ✓ Making the case for Identity-based Digital Certificates
- ✓ Using best practices to **Simplify the Deployment of Certificates** for VPN
- ✧ **Best Practices Case Study** – Cisco Anyconnect SSLVPN with certificates
 - Case Study Demo
 - Q&A

Case Study Certificate Authentication for AnyConnect



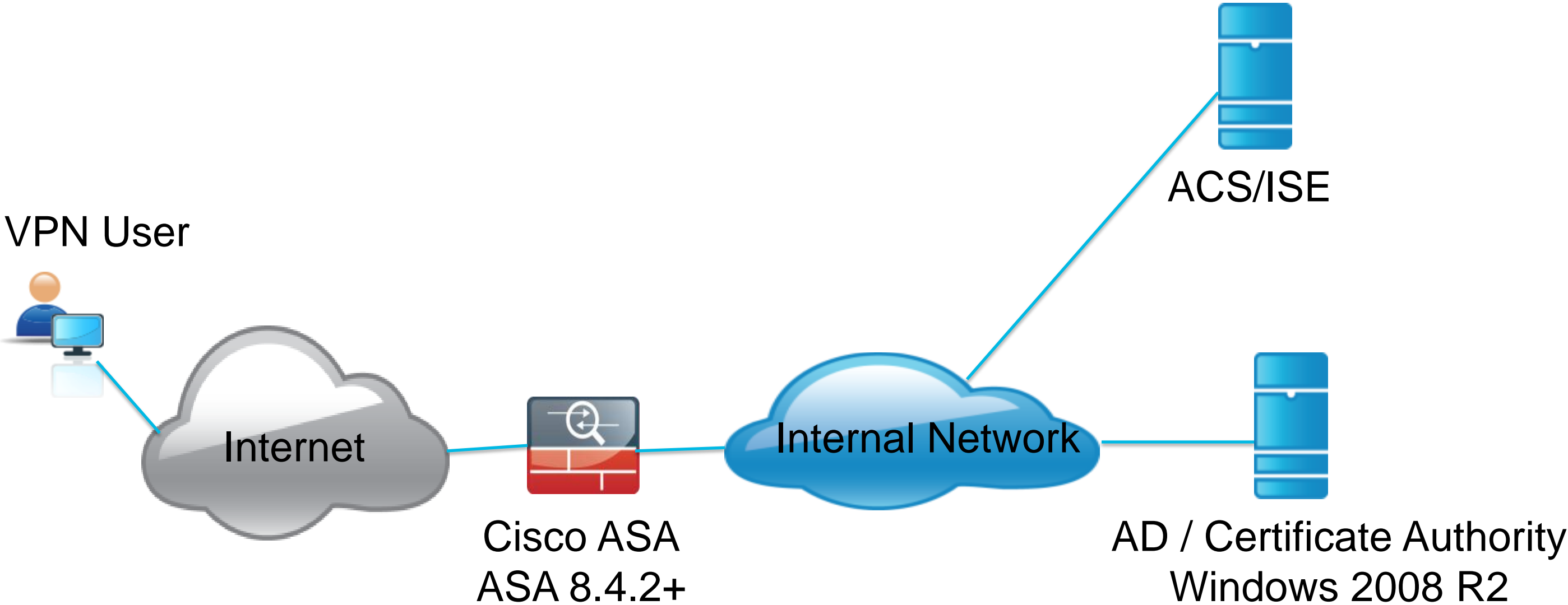
Assumptions

You have setup an AnyConnect SSLVPN either manually or through the ASDM SSLVPN Wizard

And you understand the basics of:

- Connection Profiles/Tunnel Group
- Group Policy
- Dynamic Access Policy
- Cisco Secure Desktop/Host scan

Case Study Architecture



Configuration Steps Overview

ASA AnyConnect SSLVPN

Modify your Connection Profiles

Create Client Profiles

Modify Group Policy

Create Dynamic Access Policy (DAP) rules

MSFT CA

- Create Certificate Template(s)
- Enable GPO to roll certificates to domain users/devices
- Enable NDES/SCEP Services on Windows Server

Best Practice Essentials

- ✦ **Delivery** – How do I put a certificate on Computers & Mobile Devices?
- ❑ **AAA** – Security of Device/User, Has Certificate been moved?
- ❑ **Validation** – What is required to check the Certificate?
- ❑ **Management** – Certificate, Dynamic Access Policies, and LDAP

Recommended Delivery Methods

SCEP

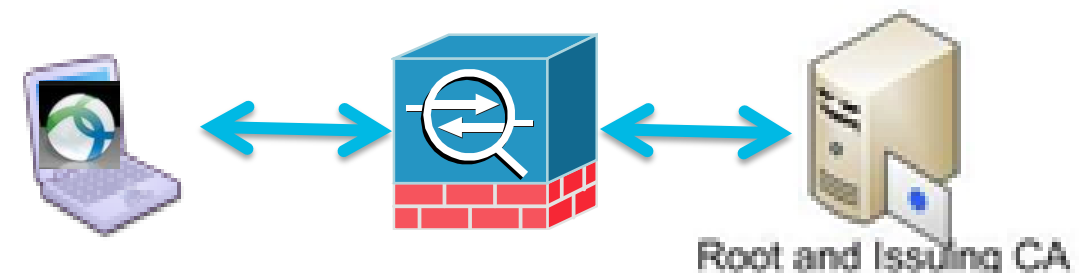
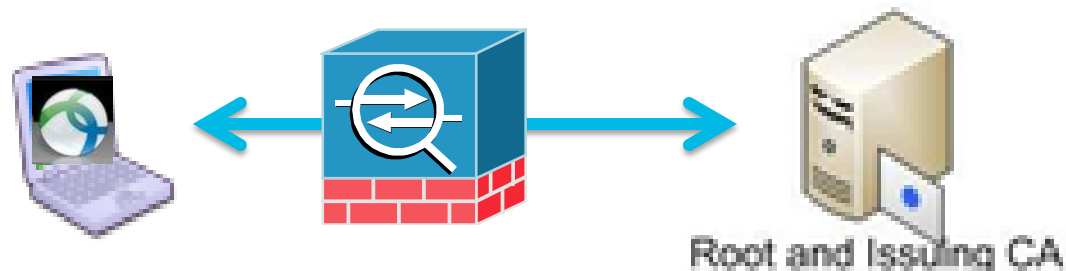
- Controlled via Client
- Needs to use Pull Down List
- Direct communication with CA
- Needs Multiple Conn. Profiles

SCEP Proxy

- Controlled via Headend
- Does not need Pull Down List
- ASA communicates with CA
- Can use Single Connection Profile

Caveats

- Requires Premium AC License
- Requires ASA 8.4(1)+

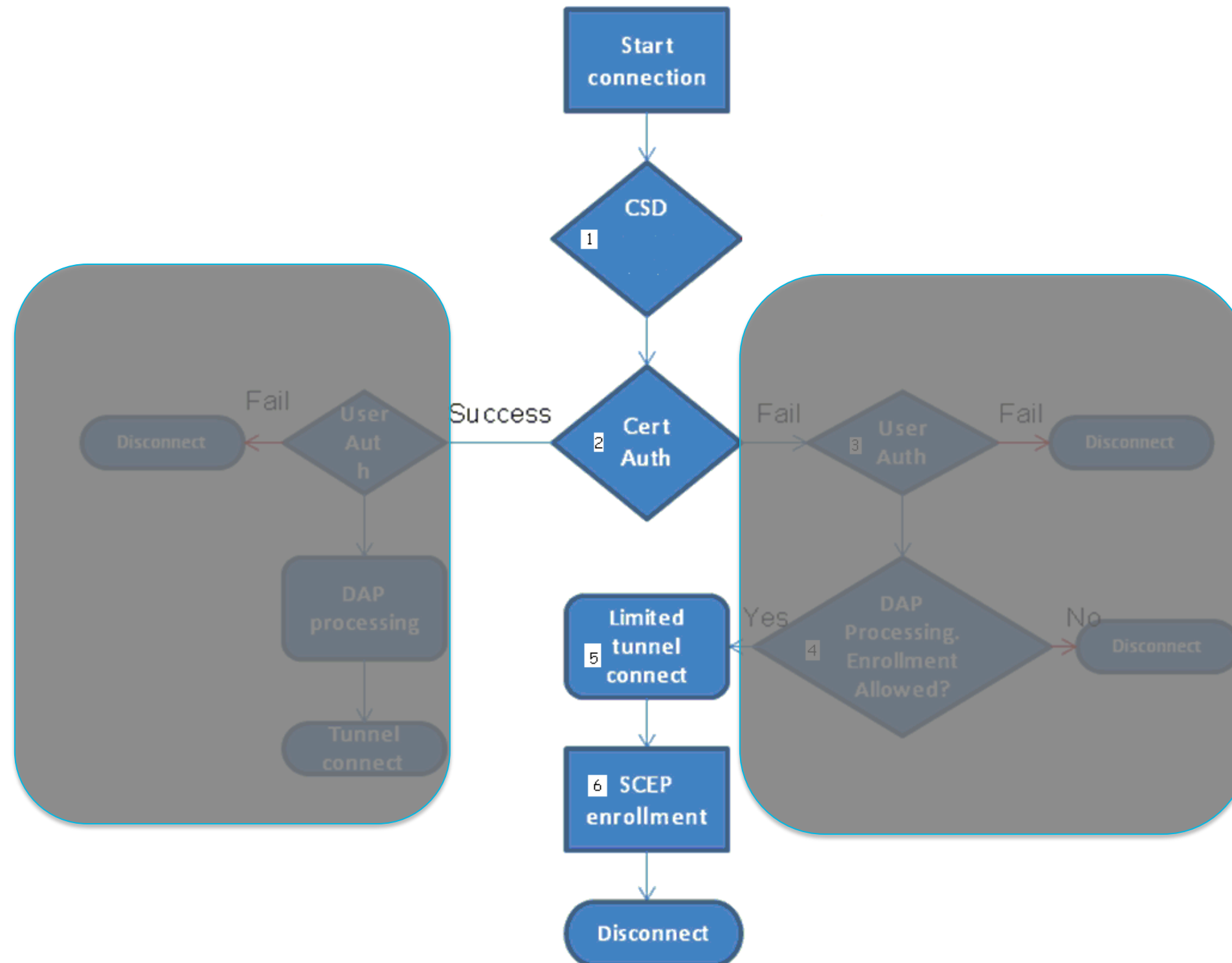


GPO

- Supported for Domain joined devices only
- ***Easiest way to roll out certificates

ASA SCEP Proxy Connection Flow

AnyConnect handles with and without Certificate



SCEP Delivery

Connection Profiles

| Aliases | Authentication Method |
|------------|------------------------------------|
| secmob | Certificate |
| GetCert | AAA(securemobility) |
| scep_proxy | AAA(securemobility) Certificate |

SCEP

Two Connection Profiles

- **GetCert** – Leverage AAA for enrollment
- **Secmob** – Certificate Authentication for tunnel

SCEP Proxy -

Windows/Mac/Linux/iOS/Android

One Connection profile

- **Scep_proxy** - profile handles enrollment and authentication

*Enable SCEP enrollment for this profile

Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile

Delivery

Group Policy Change for SCEP Proxy

The screenshot shows a configuration page titled "Add Internal Group Policy". The fields are as follows:

| | |
|----------------------|--|
| Name: | <input type="text" value="secmob"/> |
| Banner: | <input checked="" type="checkbox"/> Inherit <input type="text"/> |
| SCEP forwarding URL: | <input type="checkbox"/> Inherit <input type="text" value="http://ca.securemobility.net/certsrv/mscep/mscep.dll"/> |
| Address Pools: | <input checked="" type="checkbox"/> Inherit <input type="text"/> |
| IPv6 Address Pools: | <input checked="" type="checkbox"/> Inherit <input type="text"/> |

- Without this feature:
 - a device with a certificate will authenticate
 - a device without a certificate will not be able to enroll

Delivery

AnyConnect SCEP Configuration

Client Profile

- Requires CA URL
- Automatic SCEP Host – Certificate Enrollment Group
- %USER% as CN and/or Email used for User Authorisation

Profile: getcert

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Certificate Enrollment

Certificate Enrollment

Certificate Expiration Threshold (days)

Automatic SCEP Host

CA URL

Prompt For Challenge Password

CA Thumbprint

Certificate Contents:

| | | | |
|------------------|--|---|--------------------------------------|
| Name (CN) | <input type="text" value="%USER%"/> | Qualifier (GEN) | <input type="text"/> |
| Department (OU) | <input type="text" value="Mobility"/> | Qualifier (DN) | <input type="text"/> |
| Company (O) | <input type="text" value="Cisco Systems"/> | City (L) | <input type="text" value="Houston"/> |
| State (ST) | <input type="text" value="TX"/> | Title (T) | <input type="text"/> |
| State (SP) | <input type="text"/> | CA Domain | <input type="text"/> |
| Country (C) | <input type="text" value="USA"/> | Key Size | <input type="text" value="2048"/> |
| Email (EA) | <input type="text" value="%USER%@securem"/> | <input type="checkbox"/> Display Get Certificate Button | |
| Domain (DC) | <input type="text" value="securemobility.ne"/> | | |
| SurName (SN) | <input type="text"/> | | |
| GivenName (GN) | <input type="text"/> | | |
| UnstructName (N) | <input type="text"/> | | |
| Initials (I) | <input type="text"/> | | |

Delivery

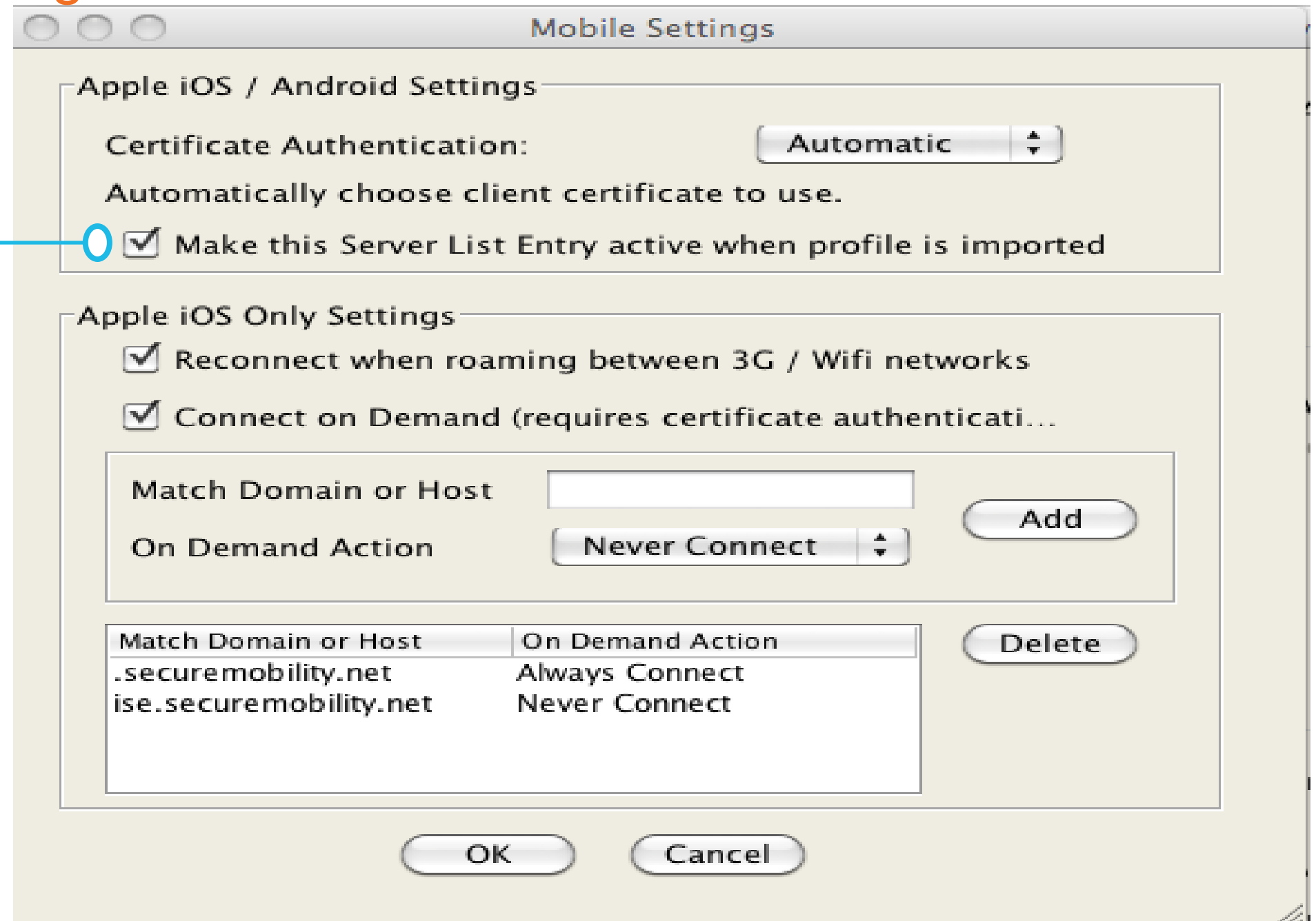
Mobile Device Specific Configuration

Mobile Settings

Connect on Demand requires Certificate Authentication

Activate on import needed for device to automatically select imported profile.

On Demand Domain list



Delivery

Device Based Certificates

Client Profile

- %MACHINEID% used to input in certificate request [optional]
- Notice %USER% is not in CN to enforce Device/Certificate Pair
- Dynamic Access Policy will be used to verify device/certificate pair

Certificate Contents:

| | | | |
|-----------------|---|---|-----------------------------------|
| Name (CN) | <input type="text" value="%MACHINEID%"/> | Qualifier (GEN) | <input type="text"/> |
| Department (OU) | <input type="text"/> | Qualifier (DN) | <input type="text"/> |
| Company (O) | <input type="text"/> | City (L) | <input type="text"/> |
| State (ST) | <input type="text"/> | Title (T) | <input type="text"/> |
| State (SP) | <input type="text"/> | CA Domain | <input type="text"/> |
| Country (C) | <input type="text"/> | Key Size | <input type="text" value="2048"/> |
| Email (EA) | <input type="text" value="%USER%@securen"/> | <input type="checkbox"/> Display Get Certificate Button | |
| Domain (DC) | <input type="text"/> | | |
| SurName (SN) | <input type="text"/> | | |
| GivenName (GN) | <input type="text" value="%USER%"/> | | |

Delivery

Using Microsoft CA with GPO and SCEP/NDES

SCEP configuration for CA

Easiest way to deploy Certificates via Group Policy

Role Services: 4 installed

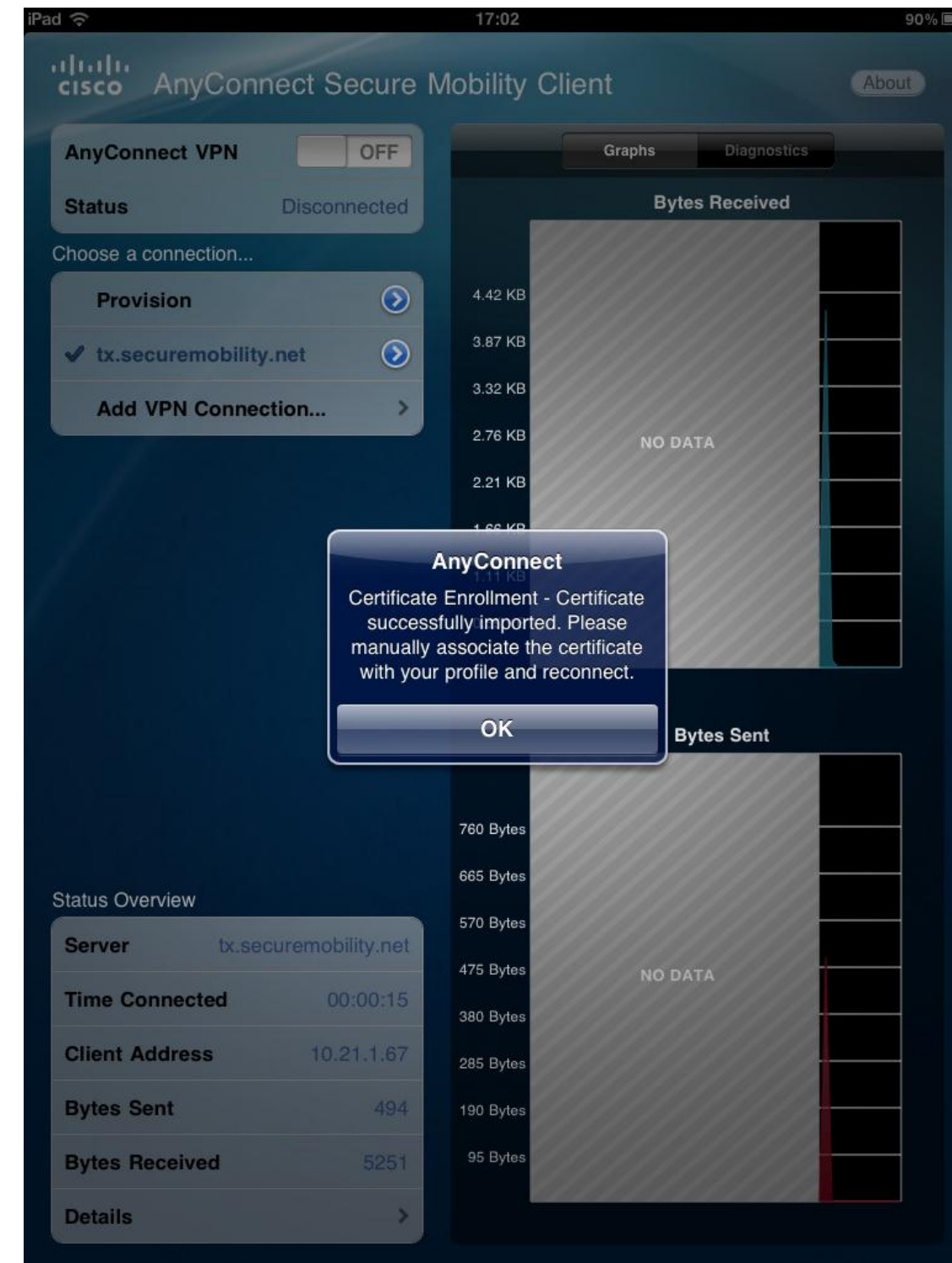
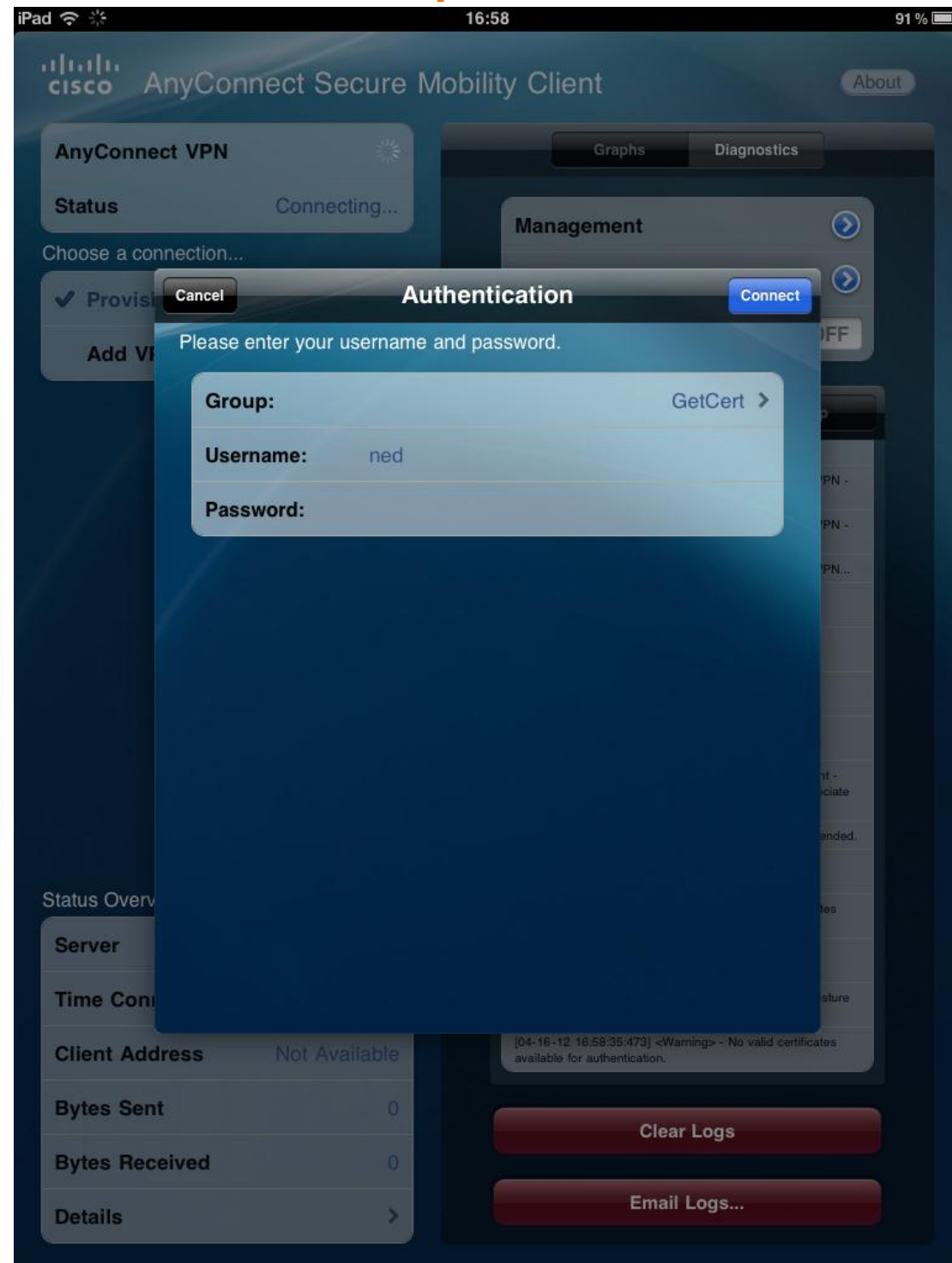
| Role Service | Status |
|---|---------------|
| Certification Authority | Installed |
| Certification Authority Web Enrollment | Installed |
| Online Responder | Installed |
| Network Device Enrollment Service | Installed |
| Certificate Enrollment Web Service | Not installed |
| Certificate Enrollment Policy Web Service | Not installed |

The screenshot shows the Group Policy Management Editor interface. The left pane displays the tree structure under 'Computer Configuration' > 'Policies'. The right pane shows the 'Object Type' list, with 'Certificate Services Client - Auto-Enrollment' selected. A dialog box titled 'Certificate Services Client - Auto-Enrollment Properties' is open, showing the 'Enrollment Policy Configuration' tab. The 'Enroll user and computer certificates automatically' checkbox is checked. The 'Configuration Model' is set to 'Enabled'. The 'Renew expired certificates, update pending certificates, and remove revoked certificates' checkbox is checked. The 'Update certificates that use certificate templates' checkbox is checked. The 'Expiration notification' checkbox is unchecked. The 'Show expiry notifications when the percentage of remaining certificate lifetime is' is set to 10%.

Delivery

End-user Experience

*Activate on import is available on mobile devices.
No need to MANUALLY select the profile



Best Practice Essentials

- ✓ **Delivery** – How do I put a certificate on Computers & Mobile Devices?
- ✧ **AAA** – Security of Device/User, Has Certificate been moved?
- **Validation** – What is required to check the Certificate?
- **Management** – Certificate, Dynamic Access Policies, and LDAP

Authentication Authorisation Accounting (AAA)

Case Study Security Requirements:

- Two-Factor** Authentication (cert, username/pwd)
- Prevent sharing** of certificates by multiple users
- Check **user exists in AD** before allowing VPN
- Use AD **group membership** as criteria for allowing SSLVPN
- Check if the PC is **joined to the AD domain**
- Severely limit net access during certificate SCEP enrollment
- Verify Device certificate is on correct device

AAA – Two Factor Authentication

Two factor – Best practice for Non-Mobile. Notice both AAA and Certificate is selected.

The screenshot shows the configuration interface for AAA Two Factor Authentication. The 'Name' field is set to 'secmob' and the 'Aliases' field is also 'secmob'. Under the 'Authentication' section, the 'Method' is set to 'Both', which is circled in red. The 'AAA Server Group' is set to 'securemobility' and there is a 'Manage...' button next to it. A checkbox for 'Use LOCAL if Server Group fails' is present and unchecked.

Pre-Fill Username – Used to verify certificate to User

The screenshot shows the 'Username Mapping from Certificate' configuration. The 'Pre-fill Username from Certificate' checkbox is checked. The 'Specify the certificate fields to be used as the username' radio button is selected. The 'Primary Field' is set to 'CN (Common Name)' and the 'Secondary Field' is set to 'OU (Organization Unit)'. There are also options for 'Use the entire DN as the username' and 'Use script to select username'. At the bottom, there are 'Add', 'Edit', and 'Delete' buttons.

The screenshot shows the Cisco AnyConnect login dialog for 'STBU Alpha - SJC'. It prompts the user to 'Please enter your username and password.' The 'Group' is set to '3.Cert_Plus_CEC' and the 'Username' is 'jheary'. The 'Password' field is empty. There are 'Cancel' and 'OK' buttons at the bottom.

AAA

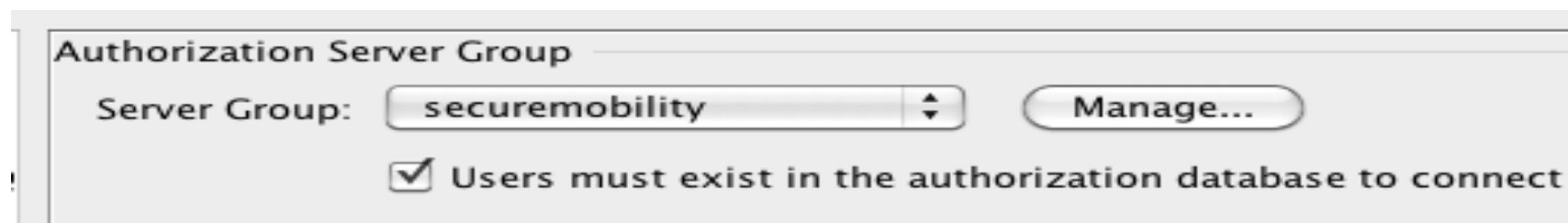
Check if user is authorised for connection

Scenario: Need to deny a user access when using Certificate only Auth

IT process: 1) IT revokes cert, validity period is 24hrs.

2) IT disables user's AD account, takes effect immediately.

User valid? - Verifies User is in AAA database



Authorization Server Group

Server Group:

Users must exist in the authorization database to connect

Pre-fill username from certificate for authorisation



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

AAA

Optional Common Authorisation checks

DAP for checking User
AD group membership

Add AAA Attribute

AAA Attribute Type: LDAP

Attribute ID: memberOf

Value: = VPN_Allowed_Users

Get AD Groups

Help Cancel OK

DAP for checking Machine is
Domain joined

Edit Endpoint Attribute

Endpoint Attribute Type: Registry

Exists Does not exist

Endpoint ID: Reg-Domain
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain

Value: string = amer.cisco.com

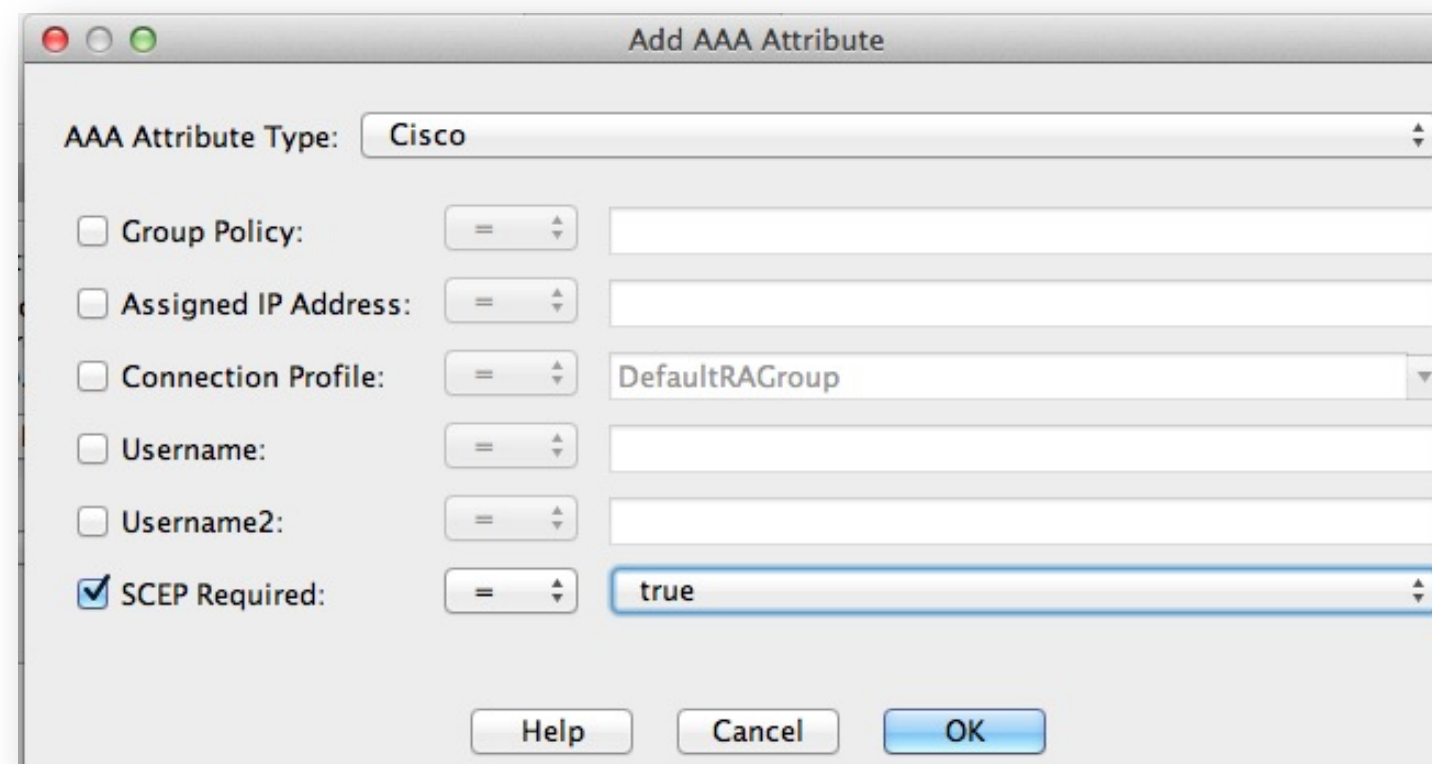
Caseless

OK Cancel Help

AAA

Restrict Devices During SCEP Certificate Enrollment

Scep.required is a new field that is populated true when you fail certificate authentication and the connection profile is set for SCEP Proxy



The screenshot shows a dialog box titled "Add AAA Attribute". The "AAA Attribute Type" is set to "Cisco". There are several attributes listed, each with a checkbox and a value field:

- Group Policy: = []
- Assigned IP Address: = []
- Connection Profile: = [DefaultRAGroup]
- Username: = []
- Username2: = []
- SCEP Required: = [true]

Buttons at the bottom: Help, Cancel, OK.

Leverage this field in a DAP rule to further control security of enrollment

AAA

Security During SCEP Certificate Enrollment

- Apply Network ACL to limit access to SCEP/CA Server during enrollment
- ACL “Required” for SCEP but not SCEP Proxy

| SCEP_Enrollment | | | | | | |
|-----------------|-------------------------------------|-----|-----------|----------|-----------|--------|
| 1 | <input checked="" type="checkbox"/> | any | CA_Server | TCP http | TCP https | Permit |

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).

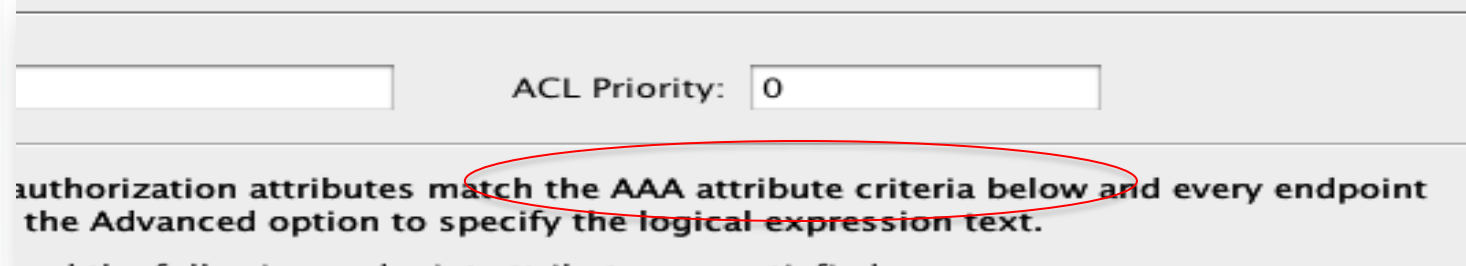
| Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions | Port Forwarding Lists | Bookmarks | Access Method |
|--------|---|--|---------------------------------------|-----------------------|-----------|---------------|
| | Network ACL (only all-permit and all-deny entries allowed) SCEP_Enrollment | | | | | |
| | <input type="button" value="Manage..."/> | <input type="button" value="Add>>"/> | <input type="button" value="Delete"/> | | | |

Network ACLs
SCEP_Enrollment

AAA

Device ID Awareness in ASA

| | |
|--------------|------------------------|
| Windows BIOS | Serial Number |
| Mac | Device Serial Number |
| Linux | Device Serial Number |
| Apple iOS | UDID |
| Android | IMEI (GSM), ESN (CDMA) |



With Android and iOS devices other attributes are available

AAA

Device Certificate is on Correct Device

- Endpoint.certificate.user["0"].subject_cn
- Endpoint.device.id is copied from anyconnect
- If NE, then certificate has been moved.**

Policy Name: Certificate_has_been_moved

Description: Because device.id is NE to certifice.subject_cn (for scep proxy) ACL Pri

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 A below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advan the logical expression text.

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

| AAA Attribute | Operation/Value |
|--------------------|-----------------|
| cisco.sceprequired | = false |
| cisco.username | = ned |

and the following endpoint attributes are satisfied.

| Endpoint ID | Name/Operation/Value |
|-------------|----------------------|
| anyconnect | platform = linux |
| anyconnect | platform = mac-intel |
| anyconnect | platform = win |

Advanced

AND OR

Logical Expressions:

EVAL(endpoint.device.id, "NE", endpoint.certificate.user["0"].subject_cn, "caseless")

Access/Authorization Policy Attributes

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

| Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions | Port Forwarding Lists | Bookmarks |
|--------|------------------------------|----------------------------------|-----------|-----------------------|-----------|
|--------|------------------------------|----------------------------------|-----------|-----------------------|-----------|

Action: Continue Quarantine Terminate

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

User Message: Your certificate has been moved to another device, please enroll each device

Best Practice Essentials

- ✓ **Delivery** – How do I put a certificate on Computers & Mobile Devices?
- ✓ **AAA** – Security of Device/User, Has Certificate been moved?
- ✧ **Validation** – What is required to check the Certificate?
- **Management** – Certificate, Dynamic Access Policies, and LDAP

Validation

Online Certificate Status Protocol (OCSP) / Certificate Revocation List (CRL)

- OCSP is a best practice for large deployments or immediate revocation
- CRL as a backup or for smaller deployments

Revocation Check

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.

Consider certificate valid if revocation information cannot be retrieved

OCSP Rules

CRL options
Specify the certificate revocation list parameters.

Cache Refresh Time: minutes
 Enforce next CRL update

OCSP options
Specify the Online Certificate Status Protocol (OCSP) parameters.

Server URL:
 Disable nonce extension

Validation Policy
Specify the type of client connections that can be validated by this CA.
 SSL IPsec SSL and IPsec

Other Options
 Accept certificates issued by this CA
 Accept certificates issued by the subordinate CAs of this CA

CRL Retrieval Method

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:

Enable HTTP
 Enable Simple Certificate Enrollment Protocol (SCEP)

Best Practice Essentials

- ✓ **Delivery** – How do I put a certificate on Computers & Mobile Devices?
- ✓ **AAA** – Security of Device/User, Has Certificate been moved?
- ✓ **Validation** – What is required to check the Certificate?
- ✦ **Management** – Certificate, Dynamic Access Policies, and LDAP

Management

CA Server – Windows 2008

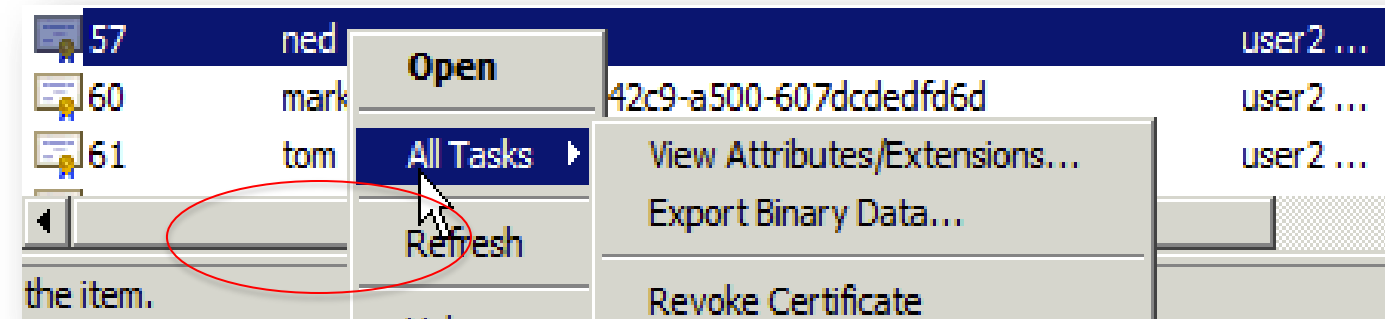
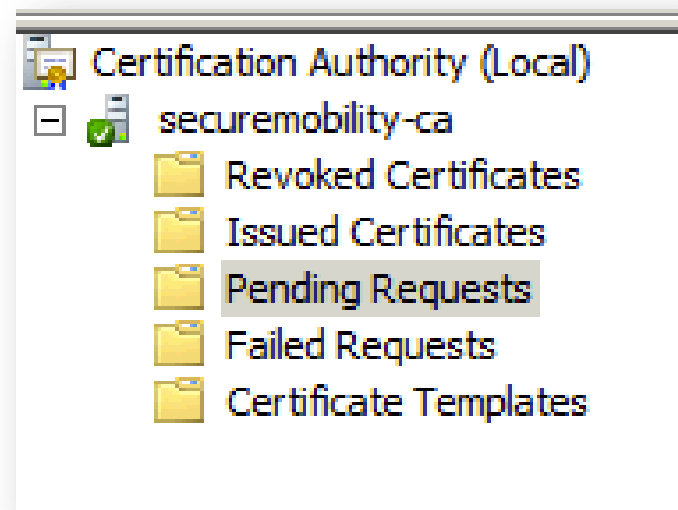
ASDM Syslog Tool

- debug dap
- debug ldap

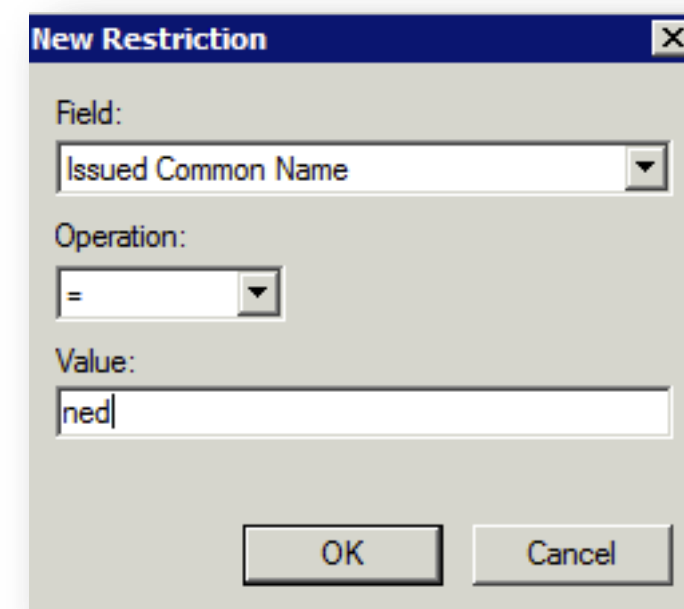
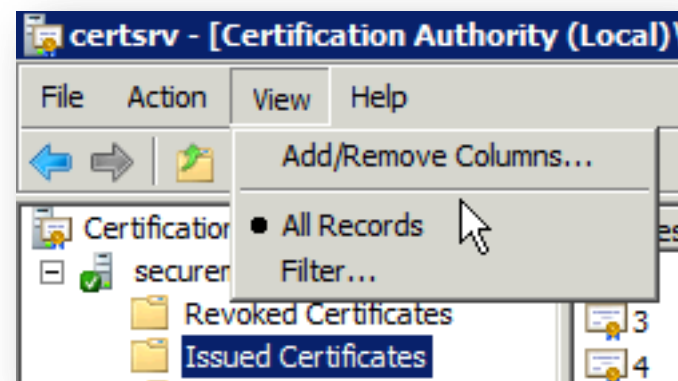
Management

CA Server MMC snap-in

- Verify/Revoke/Pending Requests



- To find a Certificate use Filter on CN



Management

Certificate Validation in Syslog

Certification validation

- Fields in the certificate can be used for comparison to CA

Certificate chain was successfully validated with revocation status check.

Certificate was successfully validated. serial number: 1B8C47AD00000000014F, subject name: ea=ned@securemobility.net,cn=ned,ou=Mobility,o=Cisco Systems,l=Houston,st=TX,dc=securemobility.net.

Certificate was successfully validated. Certificate is resident and trusted, serial number: 5B1D32BB283BE68F498E89AAA6EDDBB3, subject name: cn=securemobility-ca,dc=securemobility,dc=net.

Management

ASA Certificate Debugging

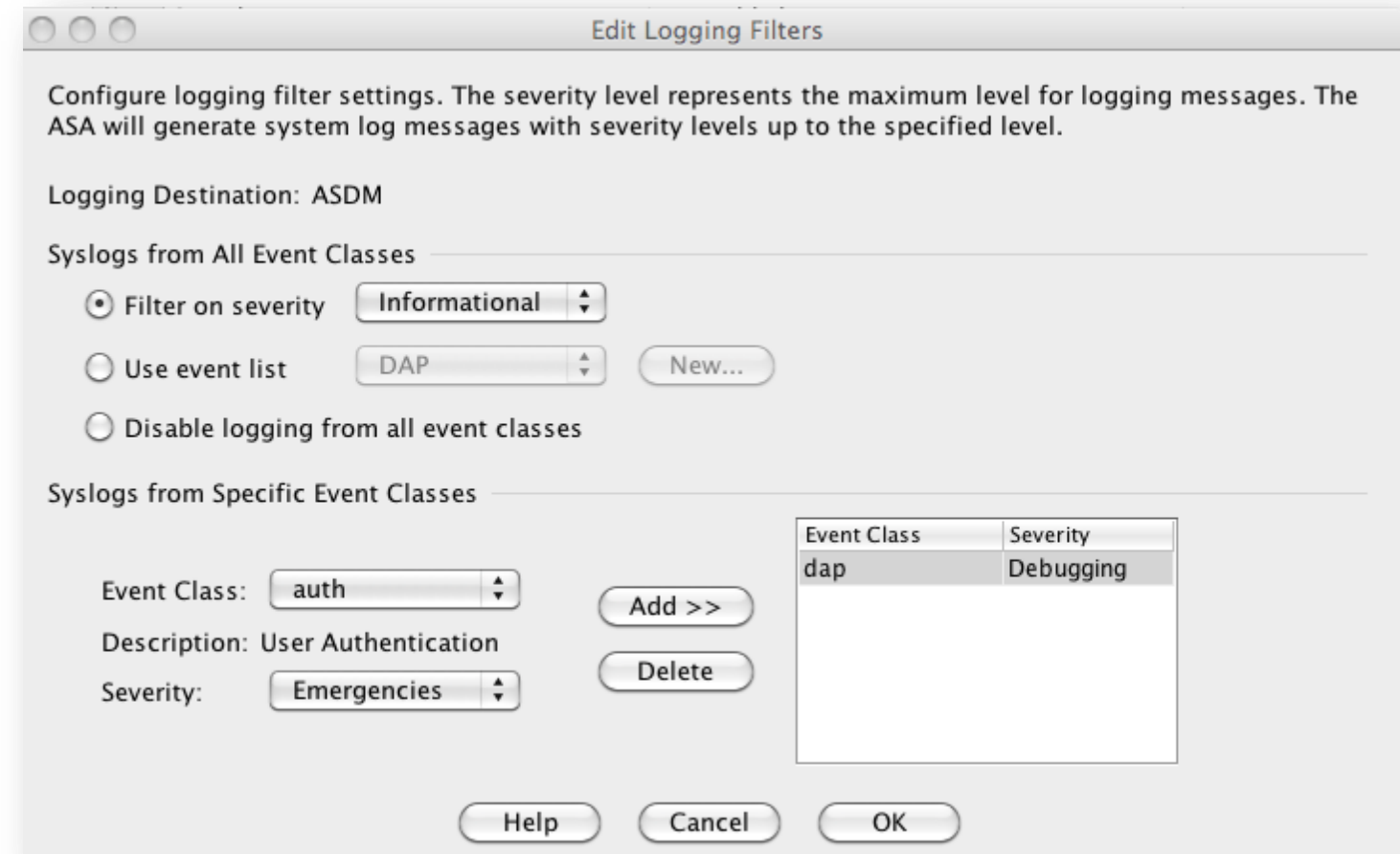
CLI Debug Commands:

- logging class ca console debug
- debug crypto ca 3
- debug crypto ca transaction 3
- debug crypto ca message 3
- debug crypto ca scep-proxy 1

Management

Debug DAP

- CLI: debug dap [trace | error]
- Define logging filter for DAP debugging to show up in ASDM syslog tool



Example output of DAP in ASDM

| | | | | | | |
|---|-----------|----------|--------|--|--|--|
| 6 | Apr 11... | 10:16:24 | 734001 | | | DAP: User ned, Addr 76.31.28.1, Connection AnyConnect: The following DAP records were selected for this connection: Certificate_has_been_moved |
| 7 | Apr 11... | 10:16:24 | 734003 | | | DAP: User ned, Addr 76.31.28.1: Session Attribute endpoint.anyconnect.deviceuniqueid="c35e4d9c320c08a5d0ea15c1eaf6d8130e743cb5" |
| 7 | Apr 11... | 10:16:24 | 734003 | | | DAP: User ned, Addr 76.31.28.1: Session Attribute endpoint.anyconnect.devicetype="iPad1,1" |
| 7 | Apr 11... | 10:16:24 | 734003 | | | DAP: User ned, Addr 76.31.28.1: Session Attribute endpoint.anyconnect.platformversion="4.2.1" |
| 7 | Apr 11... | 10:16:24 | 734003 | | | DAP: User ned, Addr 76.31.28.1: Session Attribute endpoint.anyconnect.platform="apple-ios" |
| 7 | Apr 11... | 10:16:24 | 734003 | | | DAP: User ned, Addr 76.31.28.1: Session Attribute endpoint.anyconnect.clientversion="2.5.5112" |

Management

Debug LDAP

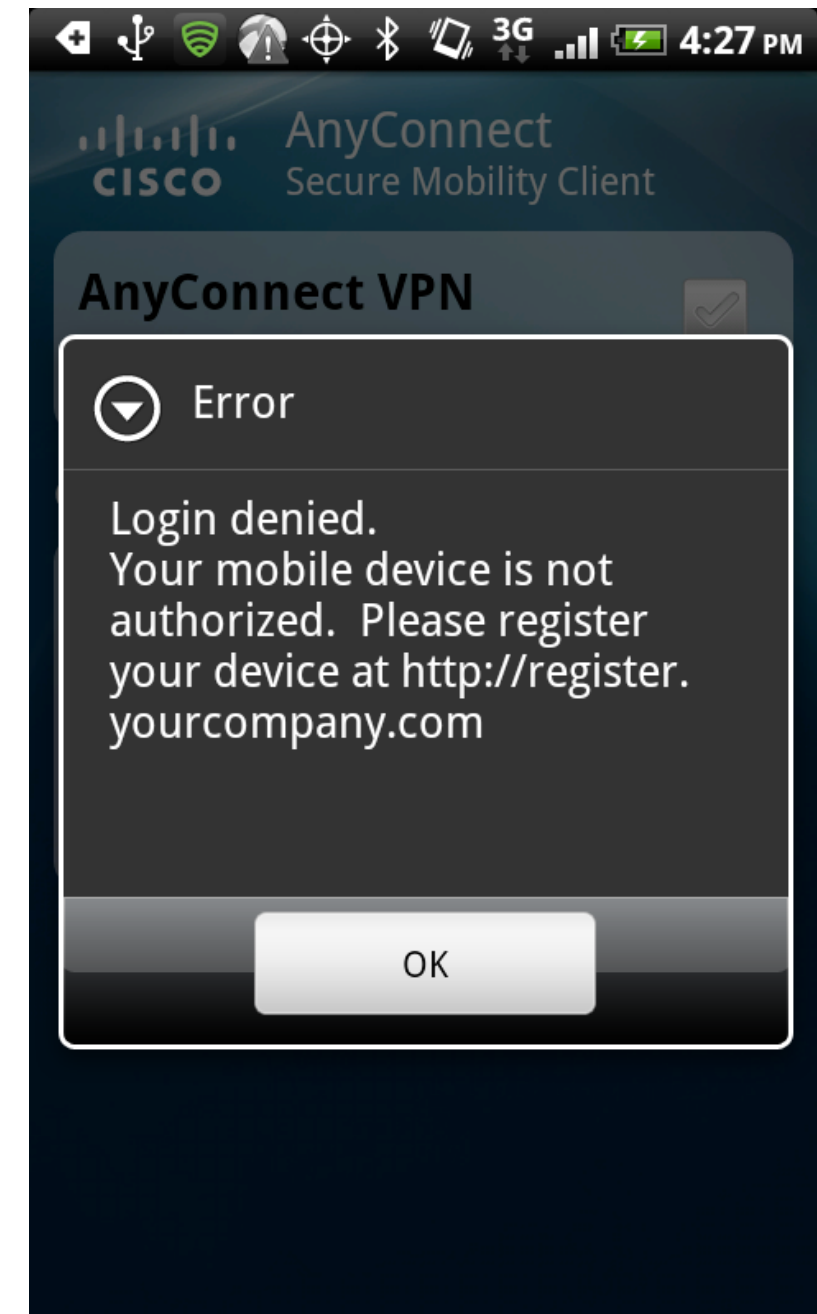
- Since DAP included LDAP lookup, all the LDAP attributes are displayed
- Especially useful when configuring authorisation rules against LDAP database

```
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.memberOf.4 = Enterprise Admins
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.memberOf.3 = Domain Admins
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.memberOf.2 = SecureMobilityGroup
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.memberOf.1 = IronPort-Operator
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.uSNCreated = 89829
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.displayName = Ned Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.whenChanged = 20120403191759.0Z
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.whenCreated = 20110922152048.0Z
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.instanceType = 4
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.distinguishedName = CN=Ned Zaldivar,OU=CSE,DC=securemobility,DC=net
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.givenName = Ned
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.description = CSE
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.sn = Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.cn = Ned Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa ldap.objectClass.4 = user
```

Management

Device Not Authorised

deviceuniqueid NE ldap.extensionAttribute1



DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.cisco.grouppolicy = getcert

DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchShadowProxyAddresses.2 = SMTP:ned@securemobility.net

DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchShadowProxyAddresses.1 = smtp:ned@securemobility.org

DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchRecipientTypeDetails = 1

DAP: User ned, Addr 97.194.113.0: Connection terminated by the following DAP records: Mobile_Device_Authorization

Case Study DEMO/VIDEO



In summary...

- Certificates excel at 2-factor auth or mobile platforms auth
- Certificates are easy to use
- Certificates can be made easy to deploy
- Certificates are the gift that keeps on giving

Additional Information Sources

Cisco Resources

- http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b25dc1.shtml
- http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008073b12b.shtml
- www.cisco.com/go/vpn
- www.cisco.com/go/anyconnect
- www.cisco.com/go/asa

Microsoft CA Server

- <http://technet.microsoft.com/en-us/library/cc770357>
- <http://technet.microsoft.com/en-us/library/cc753778>
- <http://technet.microsoft.com/en-us/library/cc753828>
- <http://technet.microsoft.com/en-us/library/cc732625>

Final Thoughts

- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
 - Facebook: <https://www.facebook.com/ciscoliveus>
 - Twitter: <https://twitter.com/#!/CiscoLive>
 - LinkedIn Group: <http://linkd.in/CiscoLI>

Q & A



Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.ww



Extras



What Is a Certificate?

- Each client sends its public key and Identity information to a third party
- That third party digitally “signs” the clients public key with its private key, binding it with identity information; this is a certificate
- The trusted third party is called a certificate authority

AAA

Optional: Device is present in LDAP

- MDM use case
- Aaa.ldap.extensionAttribute1
- Endpoint.
anyconnect.deviceuniqueid
- **If NE, then device is not authorised**

Policy Name: Mobile_Device_Authorization
Description: Device Authorization matching pre-registered ID in AD

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 below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced logical expression text.

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

| AAA Attribute | Operation/Value |
|---------------|-----------------|
|---------------|-----------------|

and the following endpoint attributes are satisfied.

| Endpoint ID | Name/Operation/Value |
|-------------|----------------------|
| anyconnect | platform = android |
| anyconnect | platform = apple-ios |

Advanced
 AND OR
Logical Expressions:
EVAL(endpoint.anyconnect.deviceuniqueid, "NE", aaa["ldap"]["extensionAttribute1"], "caseless")

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

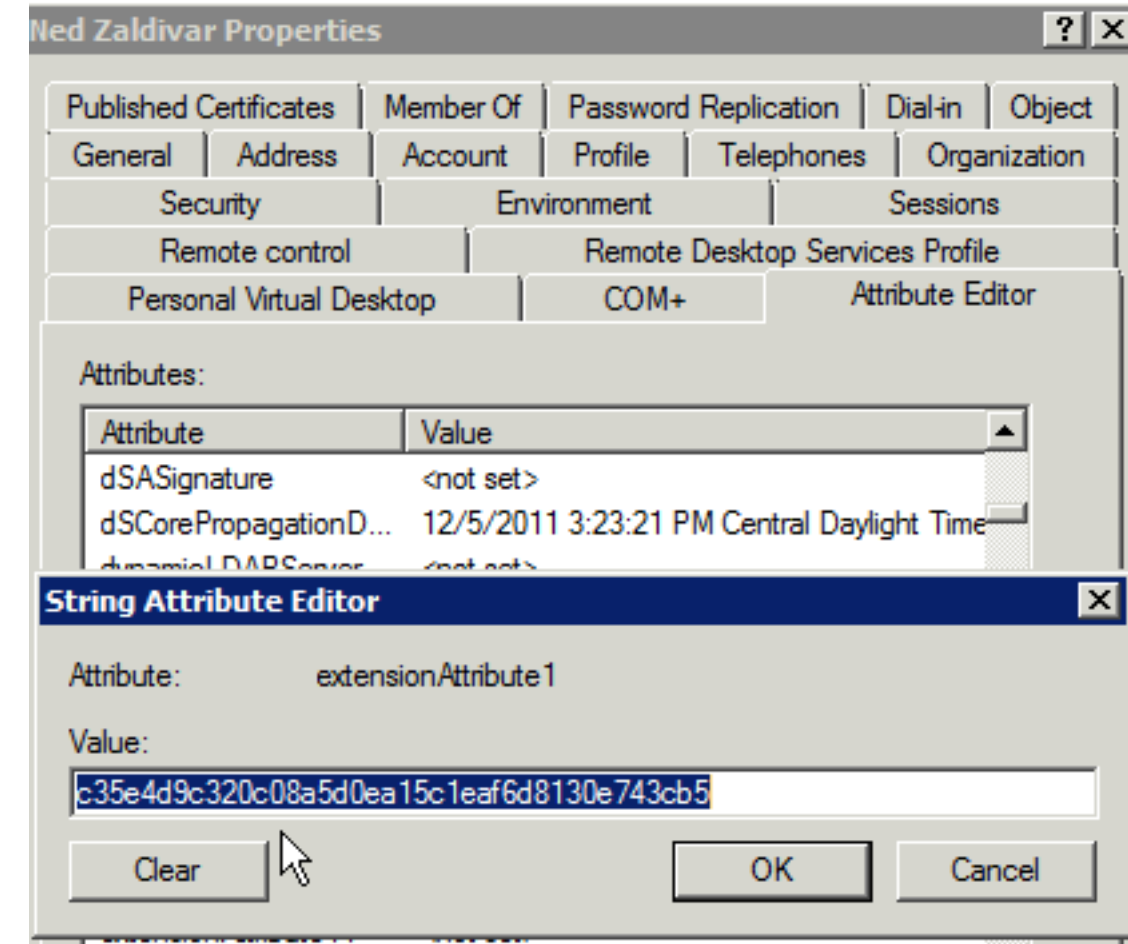
Action: Continue Quarantine Terminate

Specify the message that will be displayed when this record is selected.
User Message: Your mobile device is not authorized. Please register your device at <http://register.yourcompany.com>

AAA

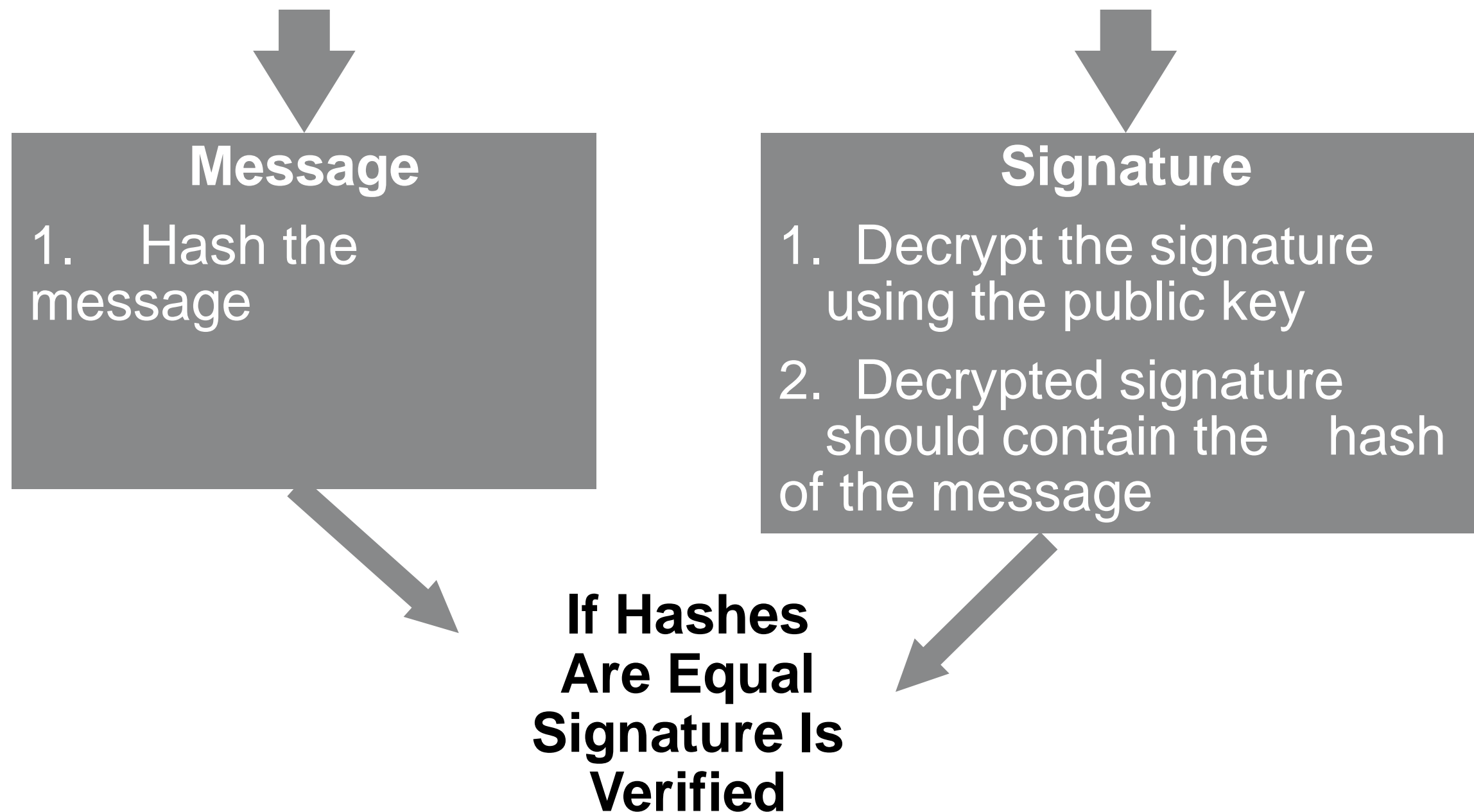
Optional: Device / AD Authorisation for Mobile

- Input Device ID into extensionAttribute1
- If multiple devices, leverage extensionAttribute#
- Device ID can be retrieved from syslog or require pre-registration of mobile devices.
- **Pre-registration is a best practice** because it lets you set standards for your IT to support.



Signature Verification Steps

- Separate the message from the signature



Certificate Authorities

Additional Information

Microsoft CA server

<http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspix>

IOS CA server

http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_brief0900aecd802b6403.html

ASA CA server (limited to SSL client certificates only)

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/cert_cfg.html#wp1067517

How to Export Local ASA CA Cert

Steps:

1. Copy ASA certificate chain (i.e. LOCAL-CA-SERVER.p12) to any PC with OpenSSL
2. “openssl pkcs12 -in LOCAL-CA-SERVER.p12 -out asa-ca.pem -nodes -nokeys”
3. Import asa-ca.pem to ‘other’ ASA’s via ASDM or CLI
4. Manually add CRL URL to ‘other’ ASA

**** Note private keys do not need to be moved ****

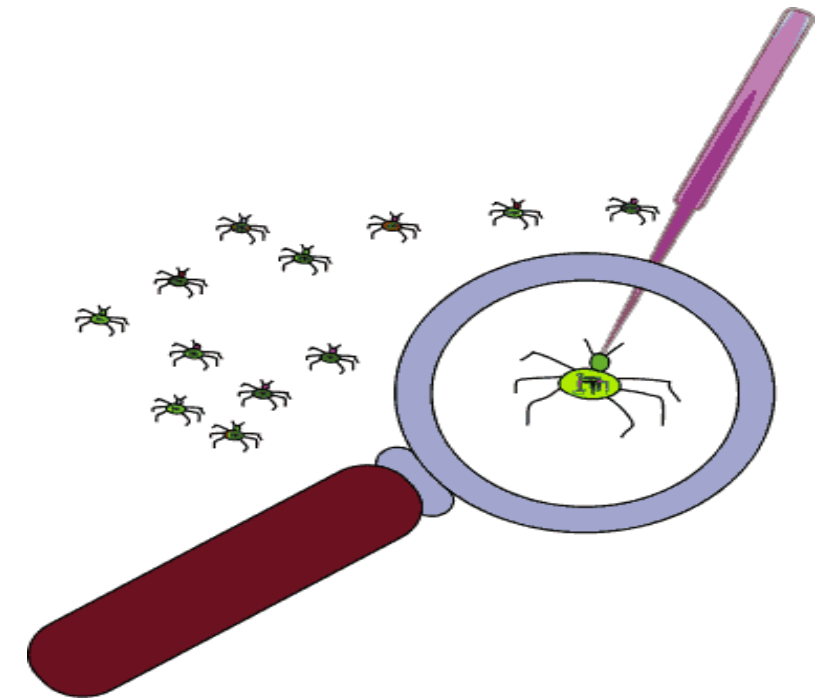
Example of Advanced LUA using Certificate Checks

```
assert(function()  
  for k,v in pairs(endpoint.certificate.user) do  
    if (EVAL(v.md5_hash, "EQ", aaa.Idap.physicalDeliveryOfficeName, "string")) and  
      (EVAL(endpoint.certificate.user.issuer_cn, "EQ", "Luis Jorge")) and  
      (EVAL (EVAL(endpoint.device.id, "EQ", endpoint.certificate.user.subject_e, "string")) )  
  then  
    return true  
  end  
end  
return false  
end)()
```

ASA Certificate Troubleshooting

Enable the following debugs when having issues with installing certificates or experiencing problems establishing IPsec/SSL VPN sessions.

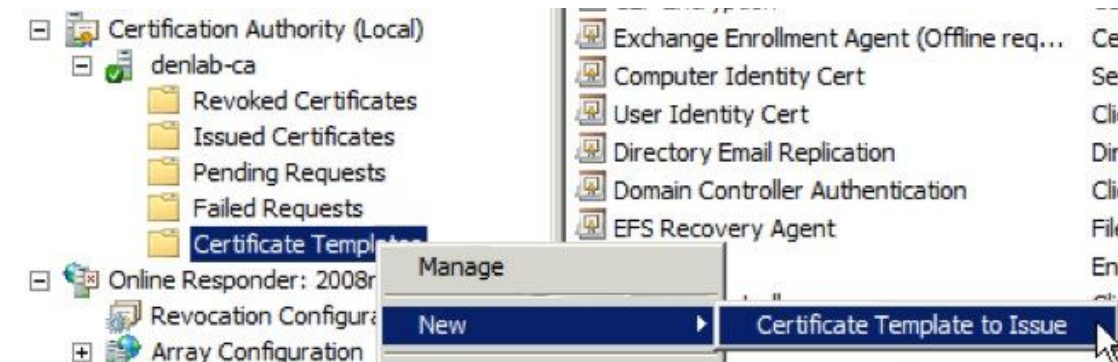
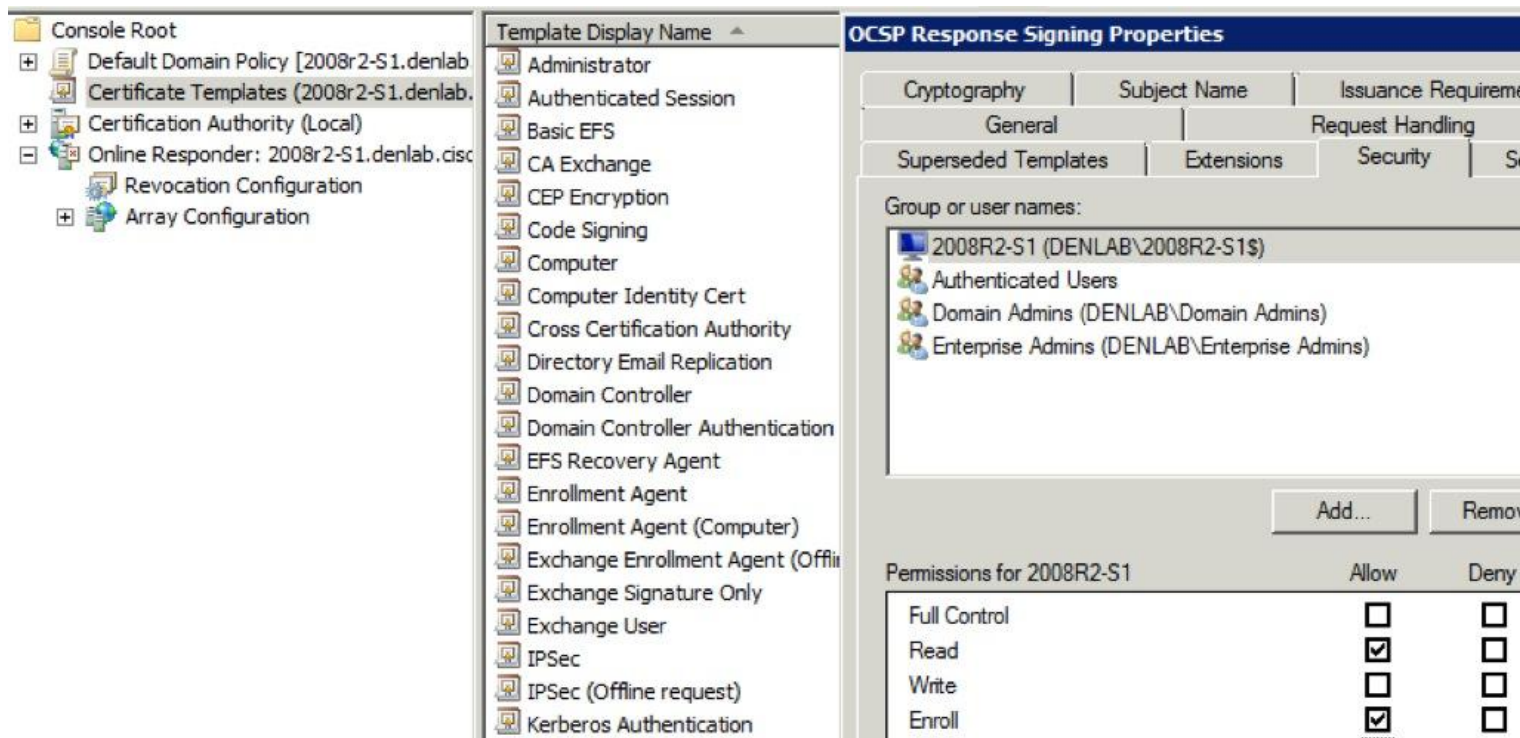
- Logging enable
- Logging class ca console debug
- Debug crypto ca 3
- Debug crypto ca transaction 3
- Debug crypto ca message 3



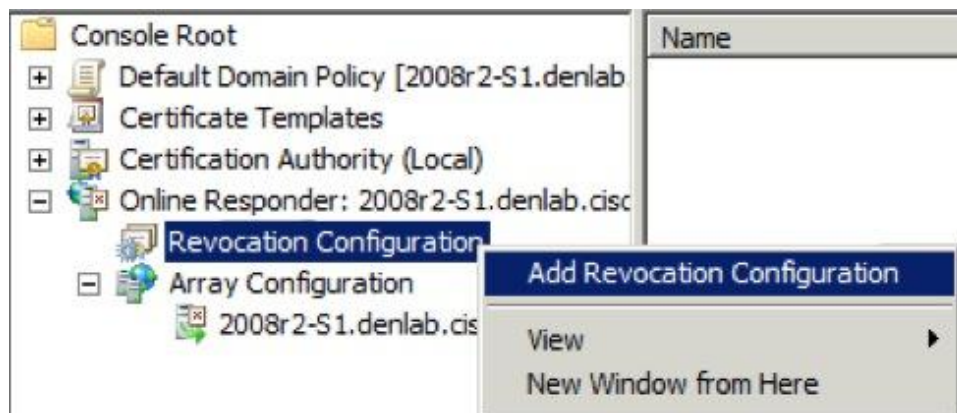
Note: elevating the level to say 5 or 10 may be useful in some cases where more detail is required.

Turn on OCSP

1. OCSP template - Add Enroll Permission to CA Computer account



2. Add Revocation Configuration from Online Responder Snap-in



OCSP Success

The screenshot shows the Windows Certificate Management console. The left pane displays a tree view with the following structure:

- Console Root
 - Default Domain Policy [2008r2-S1.denlab]
 - Certificate Templates (2008r2-S1.denlab)
 - Certification Authority (Local)
 - denlab-ca
 - Revoked Certificates
 - Issued Certificates
 - Pending Requests
 - Failed Requests
 - Certificate Templates
 - Online Responder: 2008r2-S1.denlab.cisc
 - Revocation Configuration
 - Array Configuration

The right pane displays the **Online Responder Configuration** snap-in. It includes an icon of a server rack and the following text:

Online Responder Configuration
Use this snap-in to configure and manage one or more certificate revocation responders.


Overview

The Online Responder Management snap-in helps you configure and manage online certificate s certification authorities.
Use this tool to:

- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that n select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative act
[For more information, see Verifying that a revocation configuration is functioning properly.](#)

| | |
|---|---------|
|  denlab-ocsp | Working |
|---|---------|



