802.1x EAP−TLS with Binary Certificate Comparison from AD and NAM Profiles Configuration Example

Document ID: 116018

Contributed by Michal Garcarz, Cisco TAC Engineer.
Apr 09, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used
- Conventions

Configure
- Topology
- Topology Details
- Flow
- Switch Configuration
  - Certificate Preparation
- Domain Controller Configuration
- Supplicant Configuration
- ACS Configuration

Verify
Troubleshoot
- Invalid Time Settings on ACS
- No Certificate Configured and Binded on AD DC
- NAM Profile Customization

Related Information

Introduction

This document describes the 802.1x configuration with Extensible Authentication Protocol−Transport Layer Security (EAP−TLS) and Access Control System (ACS) as they perform a binary certificate comparison between a client certificate provided by the supplicant and the same certificate kept in Microsoft Active Directory (AD). The AnyConnect Network Access Manager (NAM) Profile is used for customization. The configuration for all components is presented in this document, along with scenarios to troubleshoot the configuration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

Topology

- 802.1x supplicant − Windows 7 with Cisco AnyConnect Secure Mobility Client Release 3.1.01065 (NAM module)
- 802.1x authenticator − 2960 switch
- 802.1x authentication server − ACS Release 5.4
- ACS integrated with Microsoft AD − Domain Controller − Windows 2008 Server

Topology Details

- ACS − 192.168.10.152
- 2960 − 192.168.10.10 (e0/0 − supplicant connected)
- DC − 192.168.10.101
- Windows 7 − DHCP

Flow

The Windows 7 station has AnyConnect NAM installed, which is used as a supplicant to authenticate to the ACS server with the EAP−TLS method. The switch with 802.1x acts as the authenticator. The user certificate is verified by the ACS and the policy authorization applies policies based on the Common Name (CN) from the certificate. Additionally, the ACS fetches the user certificate from AD and performs a binary comparison with the certificate provided by the supplicant.

Switch Configuration

The switch has a basic configuration. By default, the port is in quarantine VLAN 666. That VLAN has a restricted access. After the user is authorized, the port VLAN is reconfigured.

```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system−auth−control

interface Ethernet0/0
  switchport access vlan 666
  switchport mode access
  ip device tracking maximum 10
  duplex auto
  authentication event fail action next−method
  authentication order dot1x mab
```

```
  authentication port-control auto
  dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco
```

Certificate Preparation

For EAP−TLS, a certificate is required for both the supplicant and the authentication server. This example is based on OpenSSL generated certificates. Microsoft Certificate Authority (CA) can be used to simplify deployment in Enterprise networks.

1. In order to generate the CA, enter these commands:

   ```
   openssl genrsa -des3 -out ca.key 1024
   openssl req -new -key ca.key -out ca.csr
   cp ca.key ca.key.org
   openssl rsa -in ca.key.org -out ca.key
   openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
   ```

   The CA certificate is kept in the ca.crt file and the private (and unprotected) key in the ca.key file.
2. Generate three user certificates and a certificate for ACS, all signed by that CA:
   - CN=test1
   - CN=test2
   - CN=test3
   - CN=acs54

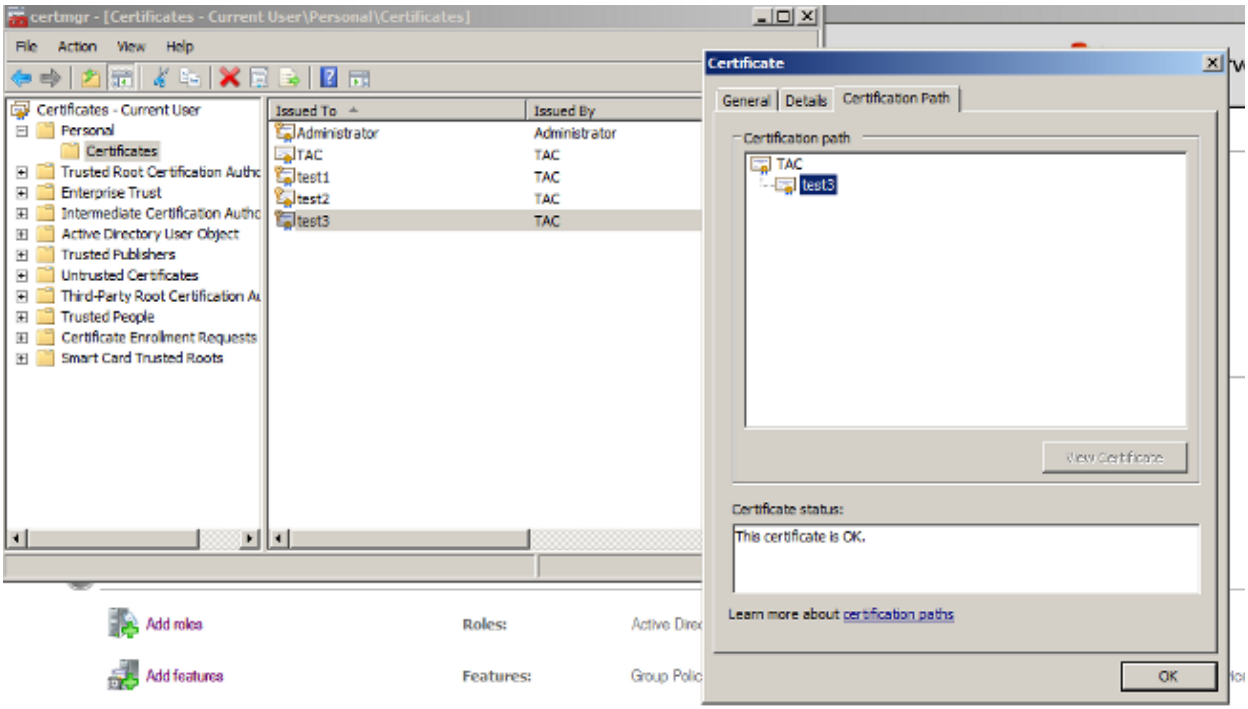
   The script to generate a single certificate signed by Cisco's CA is:

   ```
   openssl genrsa -des3 -out server.key 1024
   openssl req -new -key server.key -out server.csr

   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key

   openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
       -out server.crt -days 365
   openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
       -certfile ca.crt
   ```

   The private key is in the server.key file and the certificate is in the server.crt file. The pkcs12 version is in the server.pfx file.
3. Double−click each certificate (.pfx file) to import it to the Domain Controller. In the Domain Controller, all three certificates should be trusted.

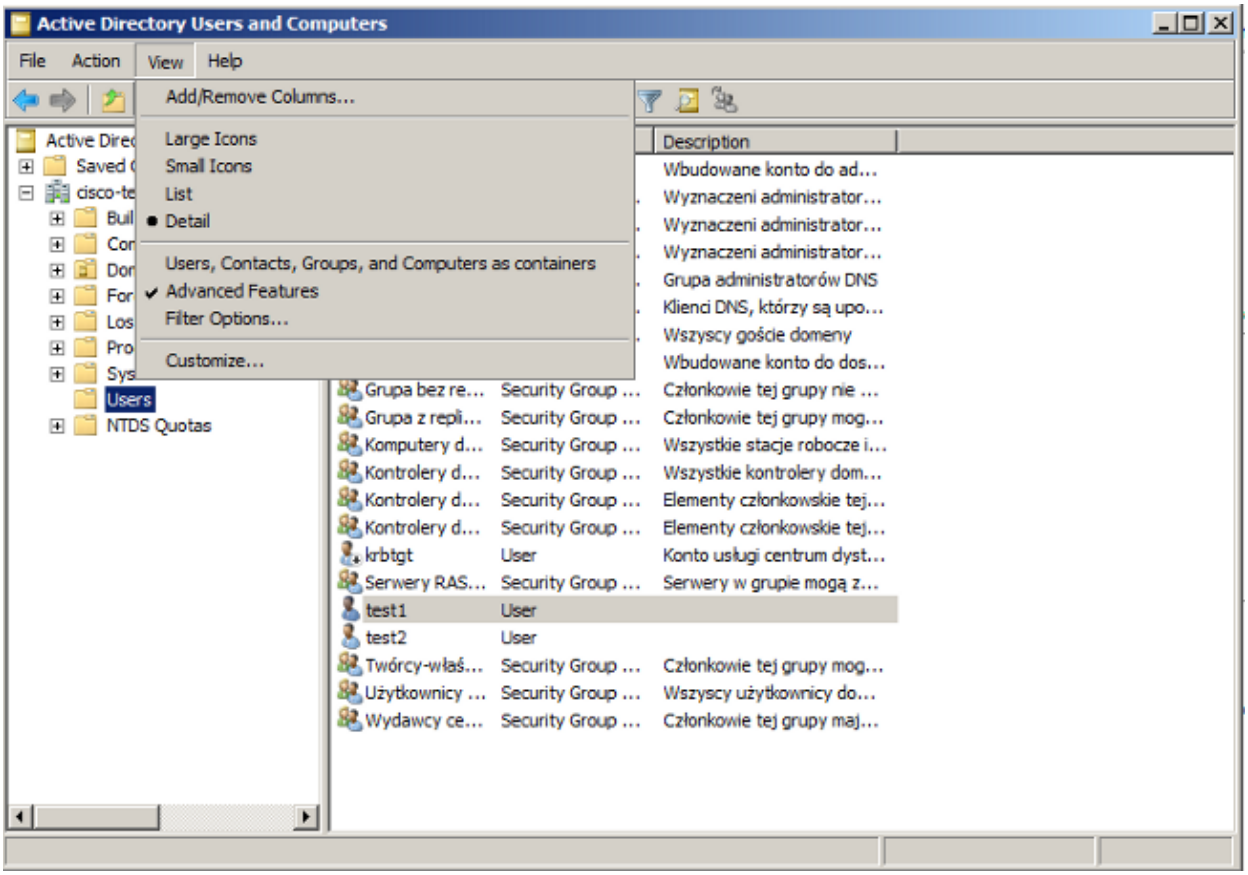


The same process can be followed in Windows 7 (supplicant) or use Active Directory to push the user certificates.

Domain Controller Configuration

It is necessary to map the specific certificate to the specific user in AD.

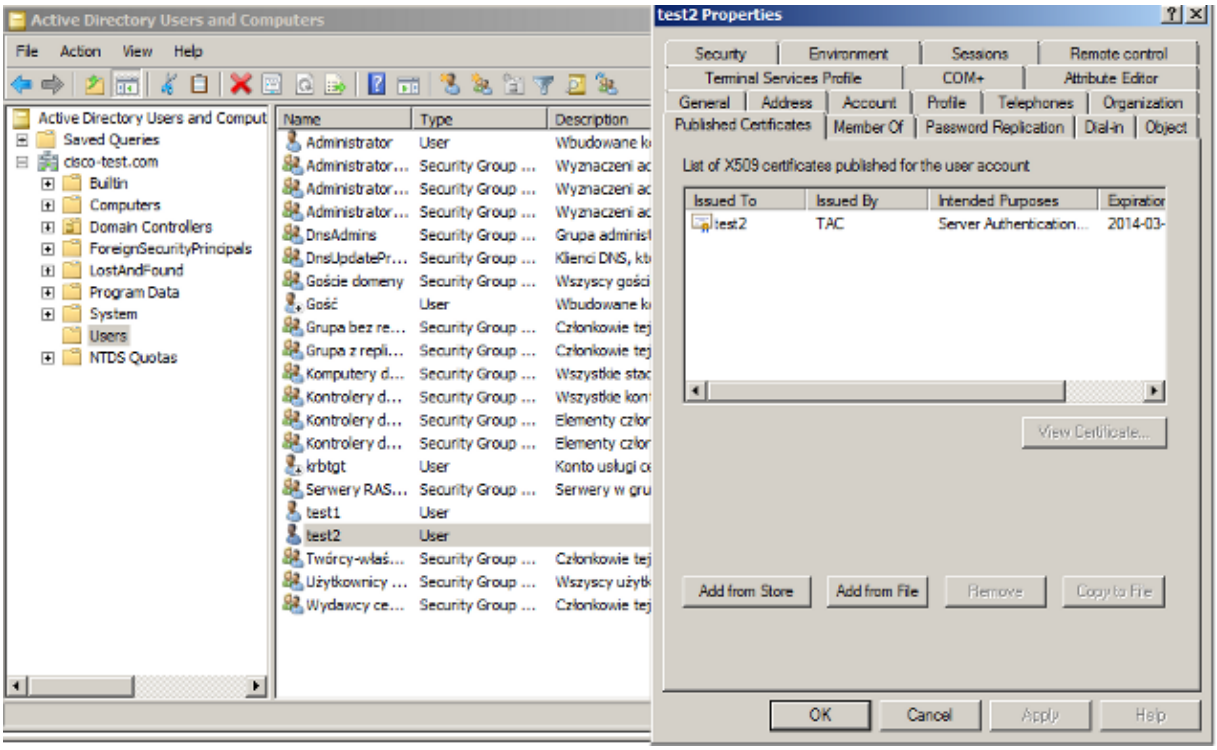
1. From Active Directory Users and Computers, navigate to the ***Users*** folder.
2. From the View menu, choose ***Advanced Features***.



3. Add these users:
   - ♦ test1
   - ♦ test2
   - ♦ test3

   Note: The password is not important.
4. From the Properties window, choose the ***Published Certificates*** tab. Choose the specific certificate for the test. For example, for test1 the user CN is test1.

   Note: Do not use Name Mapping (right−click on username). It is used for different services.



At this stage, the certificate is binded to a specific user in AD. This can be verified with the use of ldapsearch:

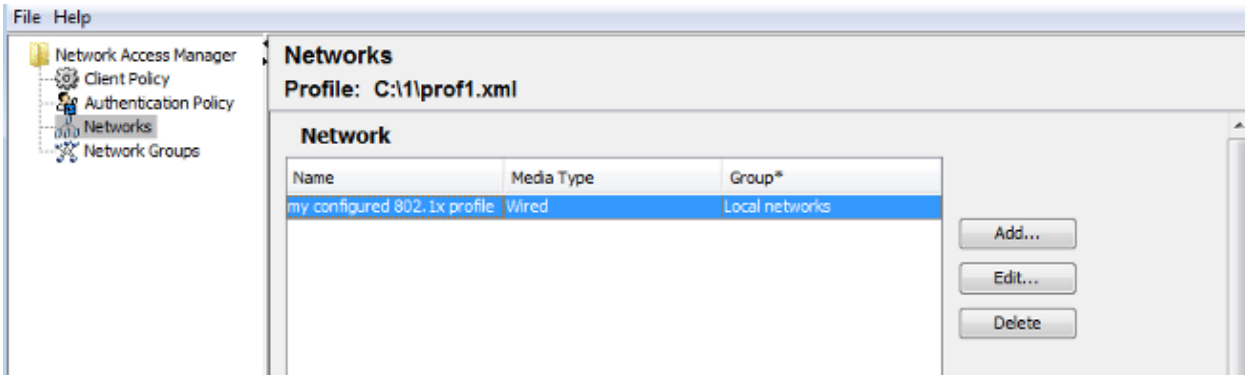
```
ldapsearch −h 192.168.10.101 −D "CN=Administrator,CN=Users,DC=cisco−test,DC=com" −w
   Adminpass −b "DC=cisco−test,DC=com"
```

Example results for test2 are as follows:

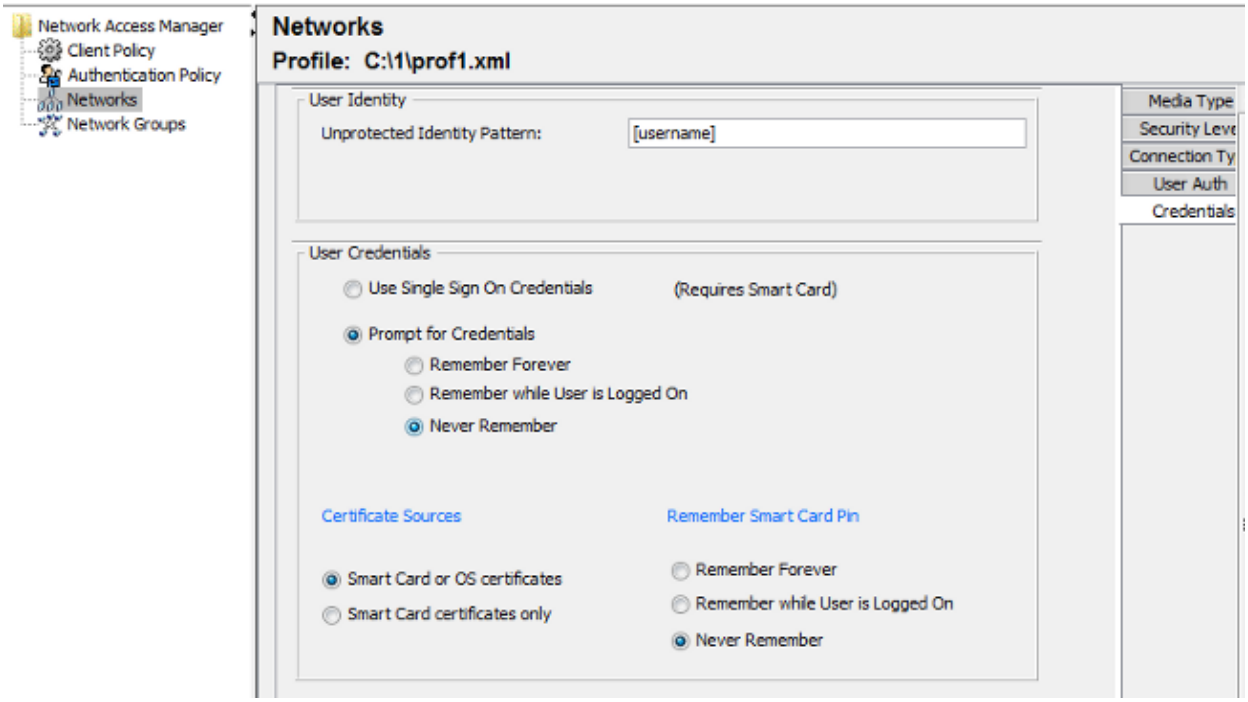
```
# test2, Users, cisco−test.com
dn: CN=test2,CN=Users,DC=cisco−test,DC=com
..................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF
oxCzAJBgNVBAYTAlBMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN
jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA
QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n
PulwF4nkcnu1xO/B7x+LpcjxjhQ==
```

Supplicant Configuration

1. Install this profile editor, anyconnect−profileeditor−win−3.1.00495−k9.exe.
2. Open the Network Access Manager Profile Editor and configure the specific profile.
3. Create a specific wired network.



At this stage it is very important is to give the user the choice to use the certificate at each authentication. Do not cache that choice. Also, use the 'username' as the unprotected id. It is important to remember that it is not the same id which is used by ACS to query AD for the certificate. That id will be configured in ACS.



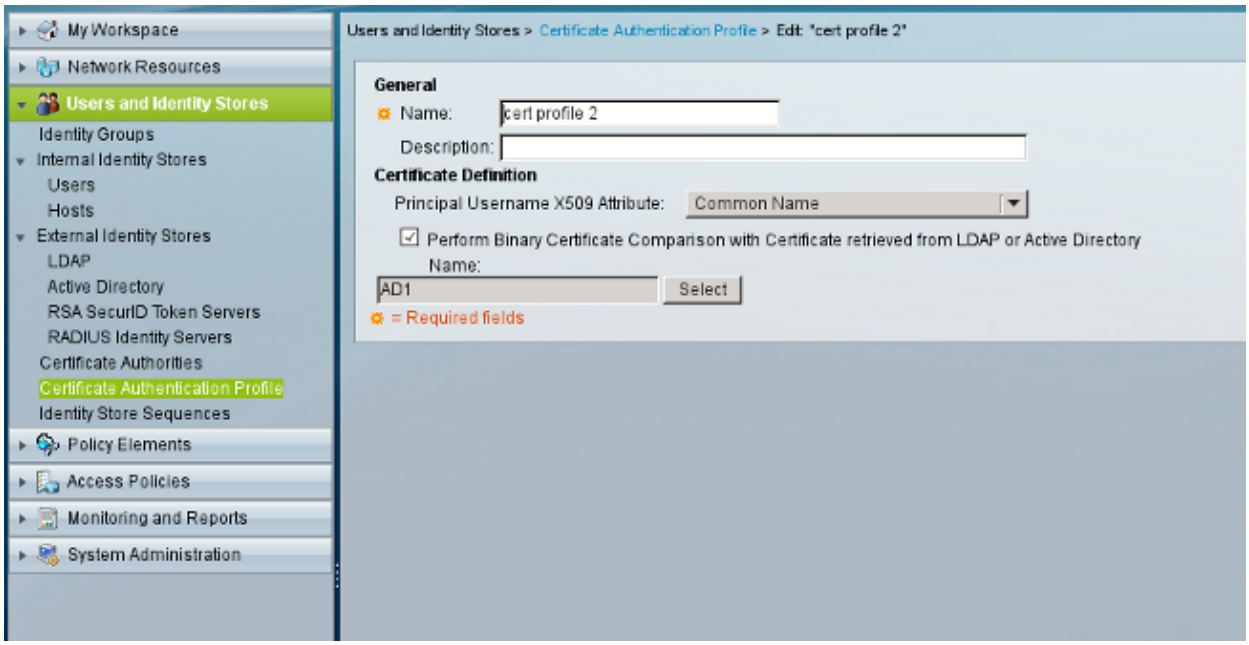
4. Save the .xml file as c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Restart the Cisco AnyConnect NAM service.

This example showed a manual profile deployment. AD could be used to deploy that file for all users. Also, ASA could be used to provision the profile when integrated with VPNs.

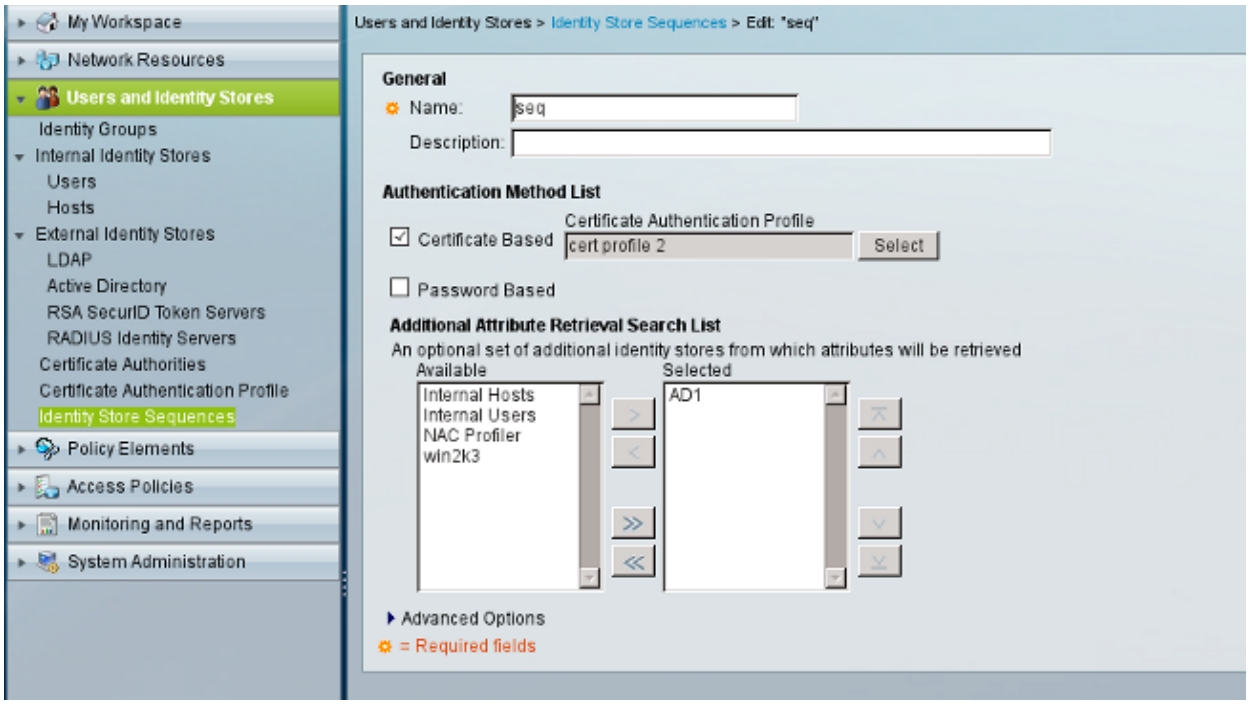
ACS Configuration

1. Join the AD domain.

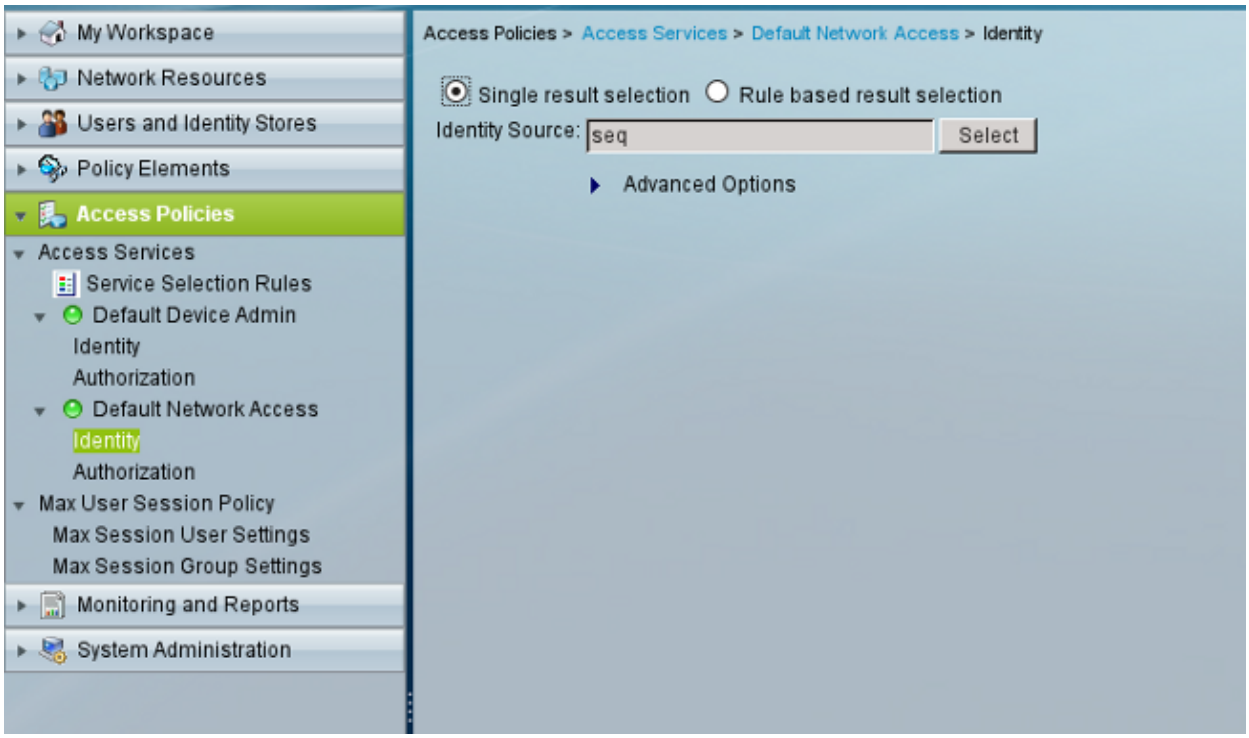
ACS matches AD usernames witht the use of the CN field from the certificate received from the supplicant (in this case it is test1, test2, or test3). Binary comparison is also enabled. This forces ACS to obtain the user certificate from AD and compare it with the same certificate received by the supplicant. If it does not match, authentication fails.



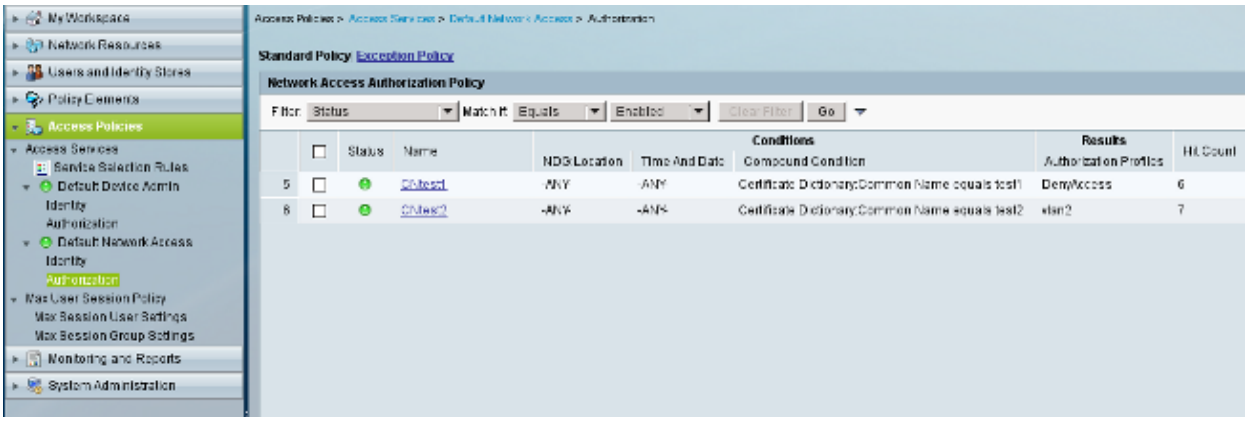
2. Configure the Identity Store Sequences, which uses AD for certificate−based authentication along with the certificate profile.



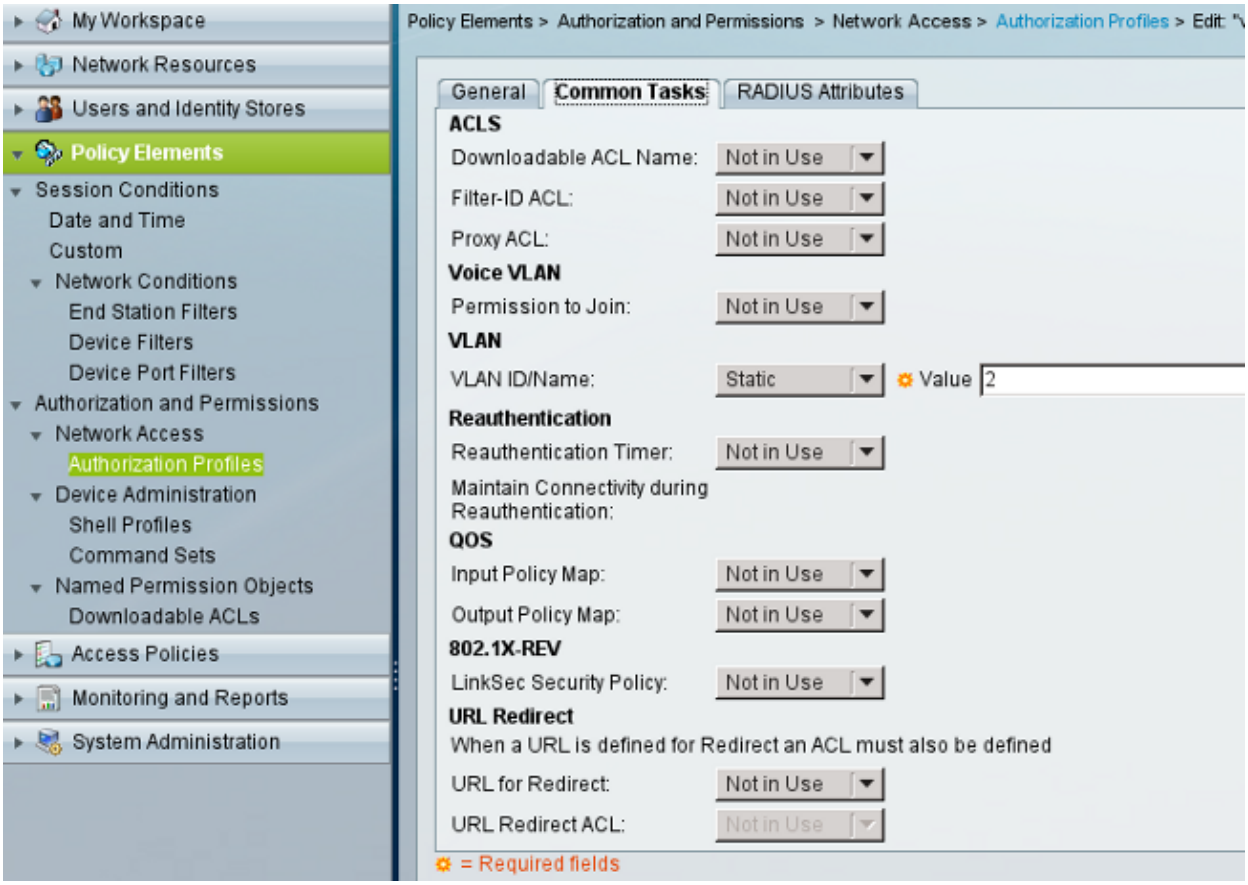
This is used as the Identity Source in the RADIUS Identity policy.



3. Configure two authorization policies. The first policy is used for test1 and it denies access to that user. The second policy is used for test 2 and it allows access with the VLAN2 profile.

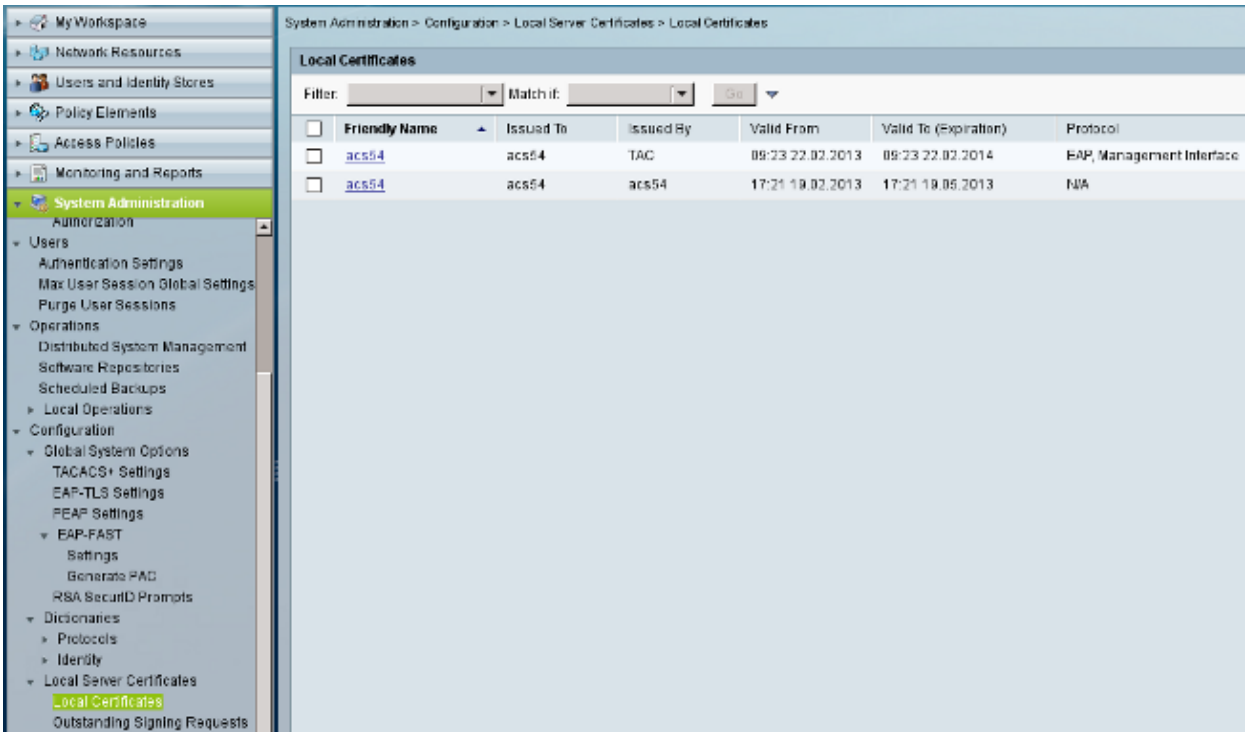


VLAN2 is the authorization profile which returns RADIUS attributes that bind the user to VLAN2 on the switch.



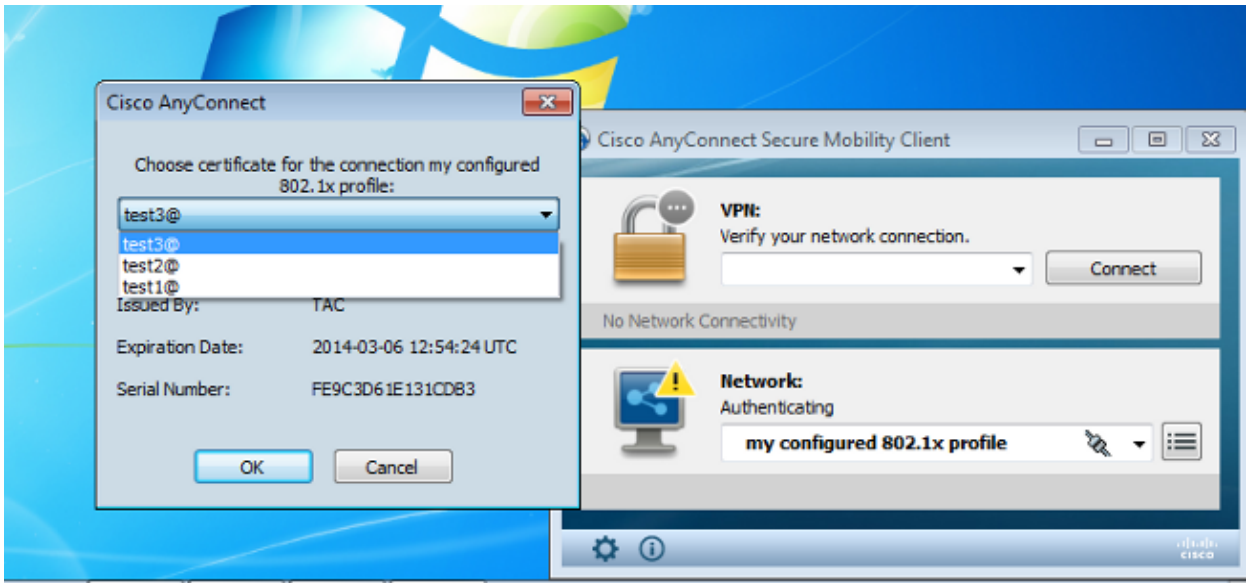
4. Install the CA certificate on ACS.

5. Generate and install the certificate (for Extensible Authentication Protocol usage) signed by Cisco's CA for ACS.



Verify

It is good practice to disable native 802.1x service on the Windows 7 supplicant since AnyConnect NAM is used. With the configured profile, the client is allowed to select a specific certificate.



When the test2 certificate is used, the switch receives a success response along with the RADIUS attributes.

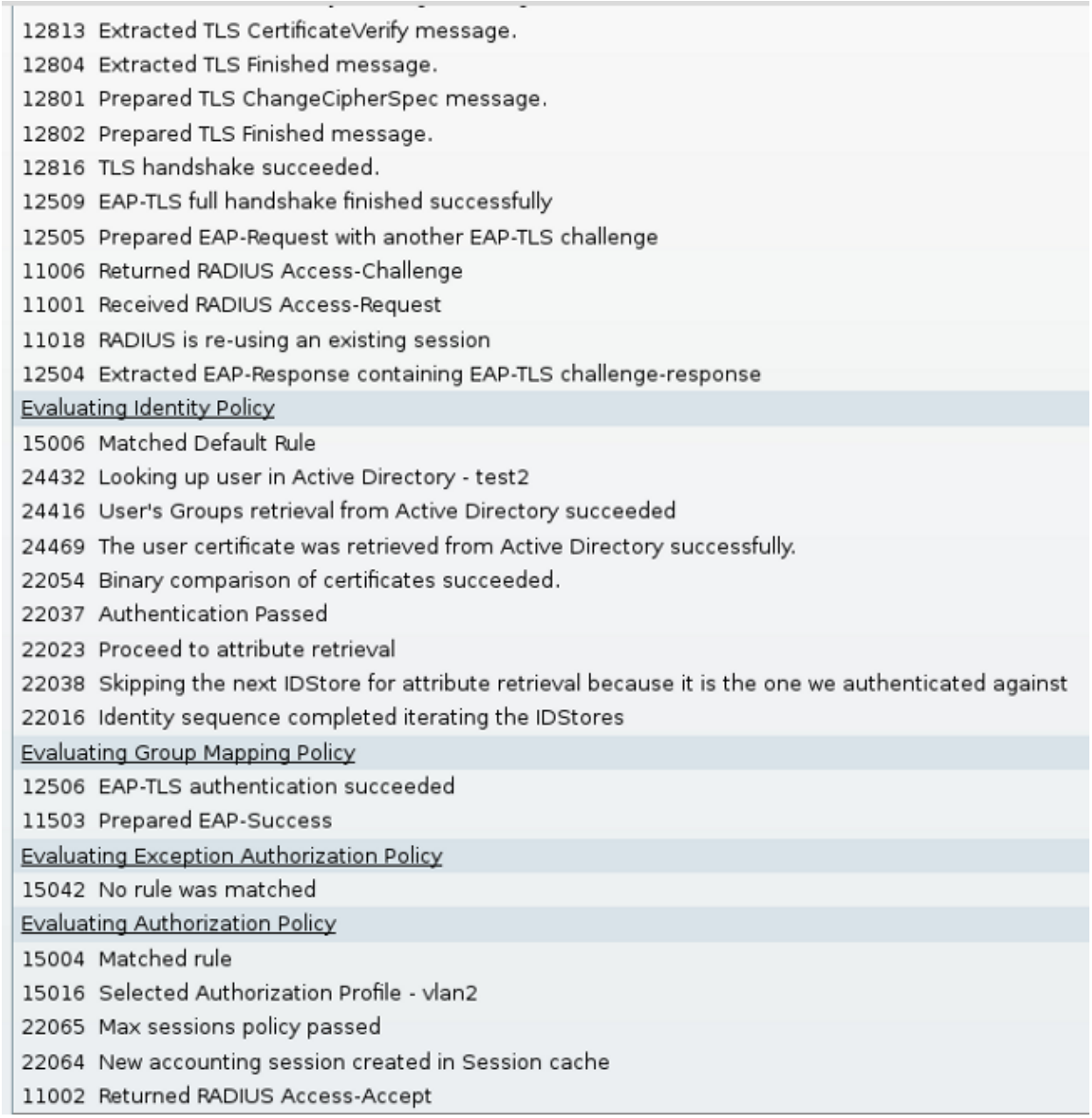
```
00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client
    (0800.277f.5f64) on Interface Et0/0
00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
    for client (0800.277f.5f64) on Interface Et0/0
switch#
00:02:51: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64|
        AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X|
        EVENT=APPLY

switch#show authentication sessions interface e0/0
            Interface:  Ethernet0/0
            MAC Address:  0800.277f.5f64
            IP Address:  Unknown
            User-Name:  test2
            Status:  Authz Success
            Domain:  DATA
            Oper host mode:  single-host
            Oper control dir:  both
            Authorized By:  Authentication Server
            Vlan Policy:  2
            Session timeout:  N/A
            Idle timeout:  N/A
            Common Session ID:  C0A80A0A00000001000215F0
            Acct Session ID:  0x00000005
            Handle:  0xE8000002

Runnable methods list:
       Method   State
       dot1x    Authc Succes
```

Note that VLAN 2 has been assigned. It is possible to add other RADIUS attributes to that authorization profile on ACS (such as Advanced Access Control List or reauthorization timers).

The logs on ACS are as follows:



Troubleshoot

Invalid Time Settings on ACS

Possible error − internal error in ACS Active Directory

12504 Extracted EAP-Response containing EAP-TLS challenge-response
12571 ACS will continue to CRL verification if it is configured for specific CA
12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test1
24416 User's Groups retrieval from Active Directory succeeded
24463 Internal error in the ACS Active Directory
22059 The advanced option that is configured for process failure is used.
22062 The 'Drop' advanced option is configured in case of a failed authentication request.

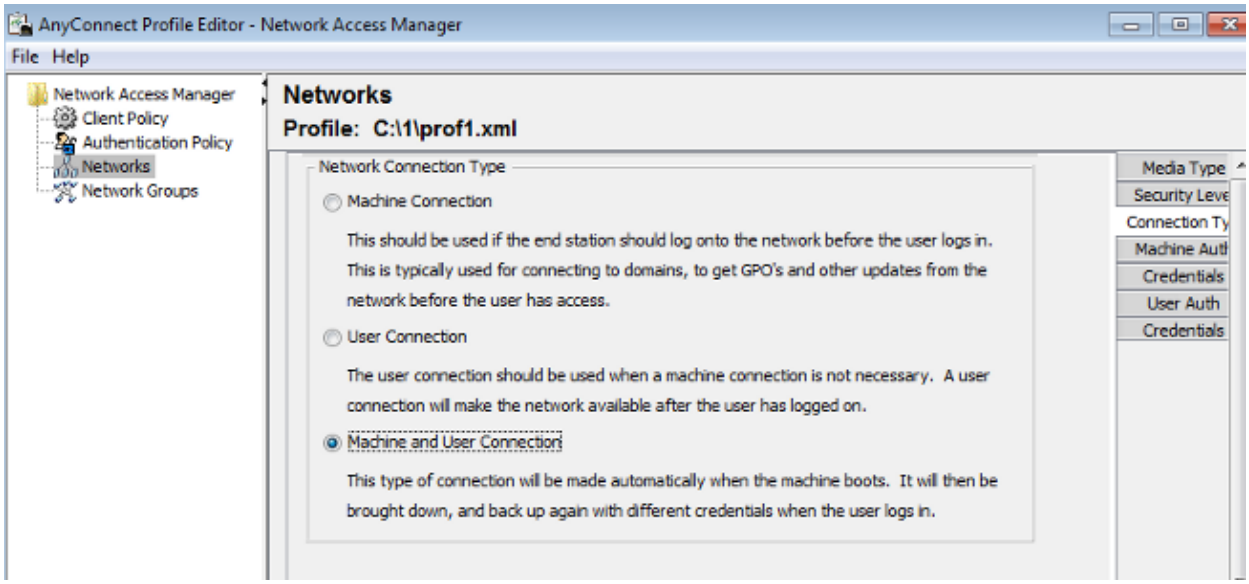
No Certificate Configured and Binded on AD DC

Possible error − failed to retrieve the user certificate from Active Directory

12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test2
24416 User's Groups retrieval from Active Directory succeeded
24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
24468 Failed to retrieve the user certificate from Active Directory.
22049 Binary comparison of certificates failed
22057 The advanced option that is configured for a failed authentication request is used.
22061 The 'Reject' advanced option is configured in case of a failed authentication request.
12507 EAP-TLS authentication failed
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject

NAM Profile Customization

In Enterprise networks, is it advised to authenticate with the use of both machine and user certificates.In such a scenario, it is advised to use open 802.1x mode on the switch with restricted VLAN. Upon the machine reboot for 802.1x, the first authentication session is initiated and authenticated with the use of the AD machine certificate. Then, after the user provides credentials and logs on to the domain, the second authentication session is initiated with the user certificate. The user is put in the correct (trusted) VLAN with full network access. It is integrated nicely on Identity Services Engine (ISE).



Then, it is possible to configure separate authentications from the Machine Authentication and User Authentication tabs.

If open 802.1x mode is not acceptable on the switch, it is possible to use the 802.1x mode before the log on feature is configured in the Client Policy.

Related Information

- User Guide for the Cisco Secure Access Control System 5.3
- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0
- AnyConnect Secure Mobility Client 3.0: Network Access Manager & Profile Editor on Windows
- Technical Support & Documentation − Cisco Systems

Updated: Apr 09, 2013 Document ID: 116018