AD および NAM プロファイルのバイナリ証明書比較を行う 802.1x EAP-TLS のコンフィギュレーション例

内容

概要

このドキュメントでは、サプリカントにより提供されるクライアント証明書および Microsoft Active Directory（AD）で保持された同じ証明書のバイナリ証明書比較を行う、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）および Access Control System（ACS）での 802.1x コンフィギュレーションについて説明します。 AnyConnect Network Access Manager（NAM）プロファイルは、カスタマイズに使用されます。このドキュメントでは、すべてのコンポーネントのコンフィギュレーション、およびコンフィギュレーションをトラブルシューティングする状況について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

トポロジ

- 802.1x サプリカント：Cisco AnyConnect Secure Mobility Client Release 3.1.01065（NAM モジュール）を使用した Windows 7
- 802.1x オーセンティケータ：2960 スイッチ
- 802.1x 認証サーバ：ACS リリース 5.4
- Microsoft AD 統合 ACS：ドメイン コントローラ：Windows 2008 Server

トポロジの詳細

- ACS：192.168.10.152
- 2960：192.168.10.10（e0/0：サプリカント接続）
- DC - 192.168.10.101
- Windows 7：DHCP

フロー

Windows 7 ステーションには、EAP-TLS メソッドで ACS サーバを認証するサプリカントとして使用される、AnyConnect NAM がインストールされています。802.1x にスイッチは、オーセンティケータとして機能します。ユーザ証明書は、ACS により検証されます。ポリシー認証は、証明書の Common Name（CN）に基づいたポリシーを適用します。また、ACS は、AD からユーザ証明書をフェッチし、サプリカントにより提供される証明書とのバイナリ比較を行います。

スイッチの設定

スイッチには、基本コンフィギュレーションがあります。デフォルトでは、ポートは隔離VLAN 666にあります。このVLANにはアクセスが制限されています。ユーザが承認されると、ポート VLAN が再設定されます。

```
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
```

証明書の準備

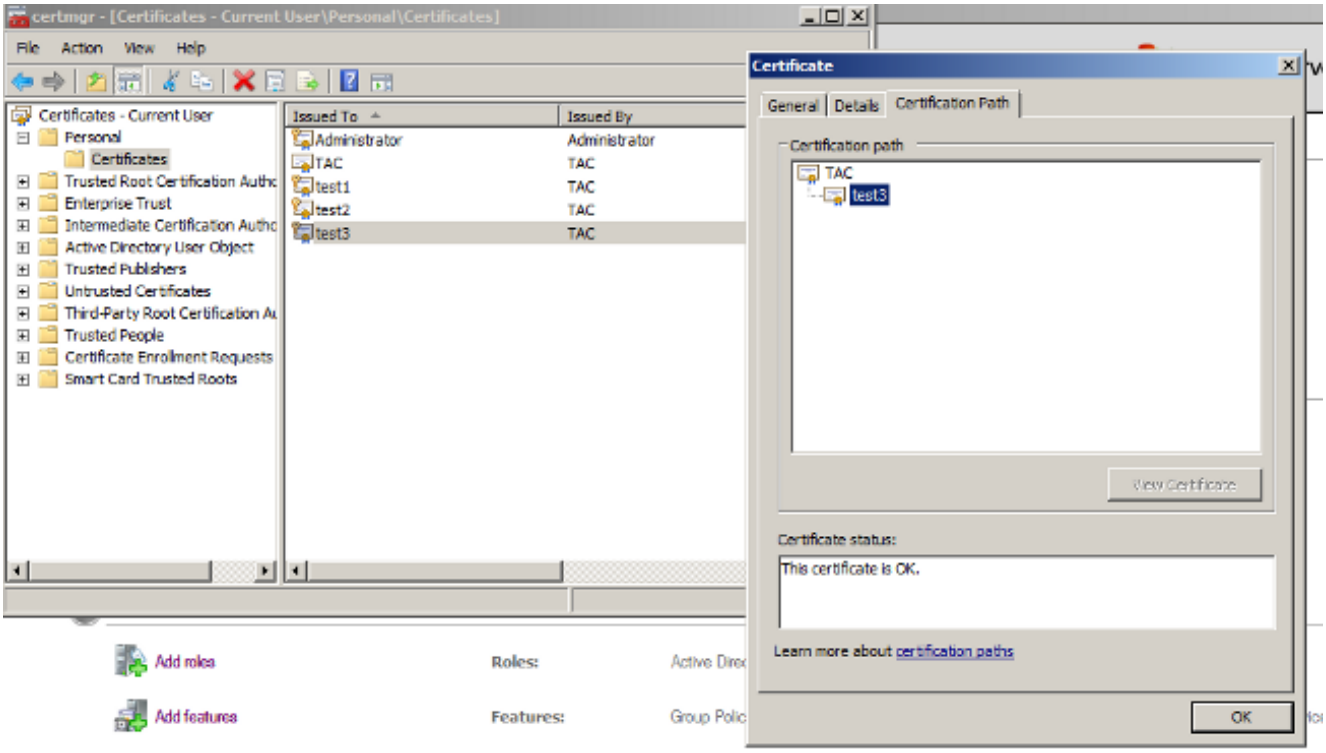
EAP-TLS では、証明書は、サプリカントおよび認証サーバの両方で必要です。この例は、OpenSSL により生成された証明書に基づいています。Microsoft 認証局（CA）は、企業ネットワークでの導入を簡素化できます。

1. CA を生成するには、次のコマンドを入力します。
   ```
   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
   ```
   CA 証明書は、ca.crt ファイルに保存されます。秘密（保護されない）キーは、ca.key ファイルに保存されます。
2. 次の 3 つのユーザ証明書および ACS の証明書を生成します。これらはすべて CA により署名されます。 CN=test1CN=test2CN=test3CN=acs54次に、Cisco の CA により署名された 1 つの証明書の生成スクリプトを示します。
   ```
   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
   ```
   秘密キーは server.key ファイルに保存され、証明書は server.crt ファイルに保存されます。pkcs12 バージョンは、server.pfx ファイルに保存されます。
3. 各証明書（.pfx ファイル）をダブルクリックして、ドメイン コントローラにインポートします。ドメイン コントローラで、3 つすべての証明書は、信頼できる証明書でなければなりま

せん。

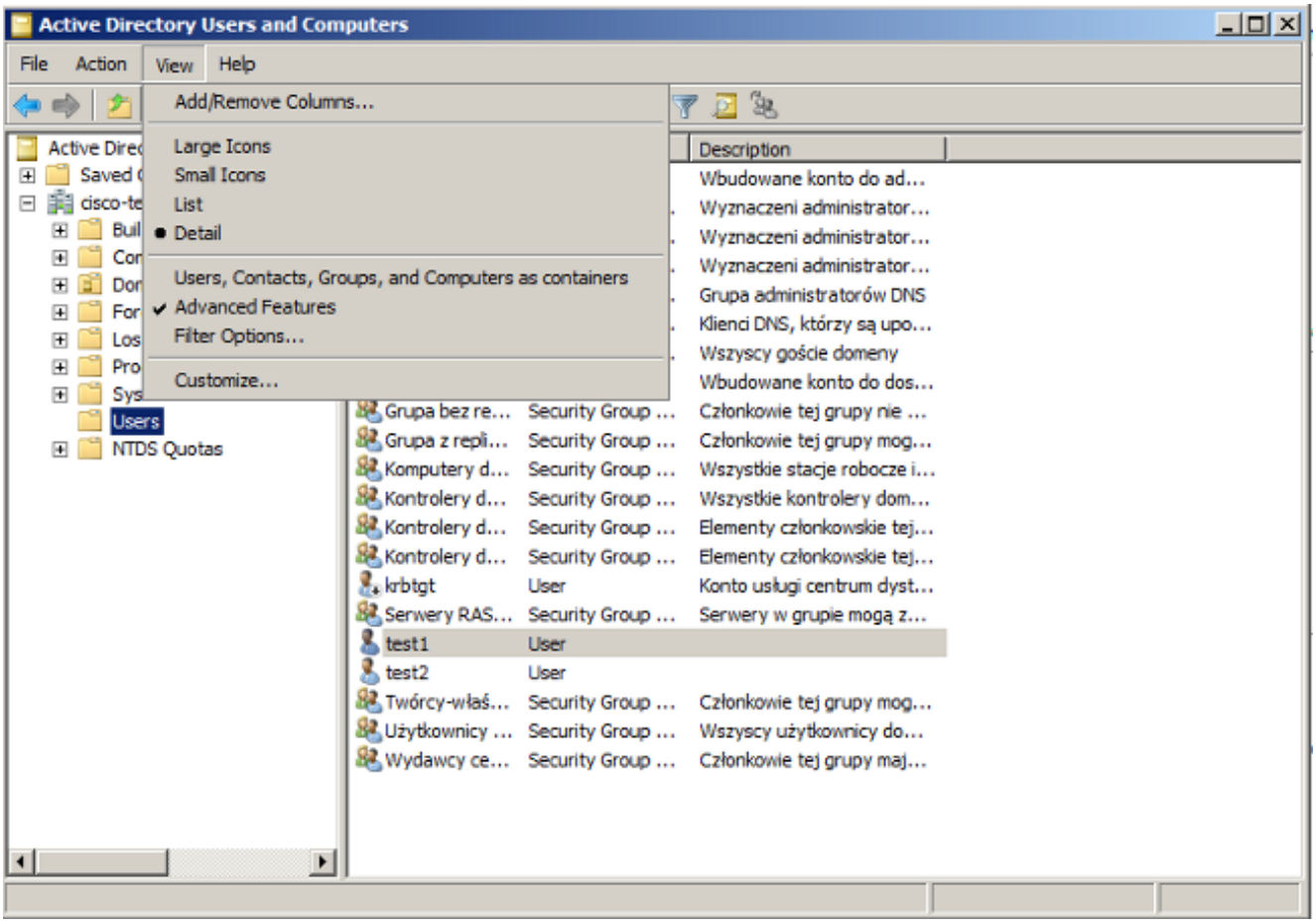


同じプロセスが、Windows 7（サプリカント）で実行されるか、Active Directory によりユーザ証明書にプッシュされます。

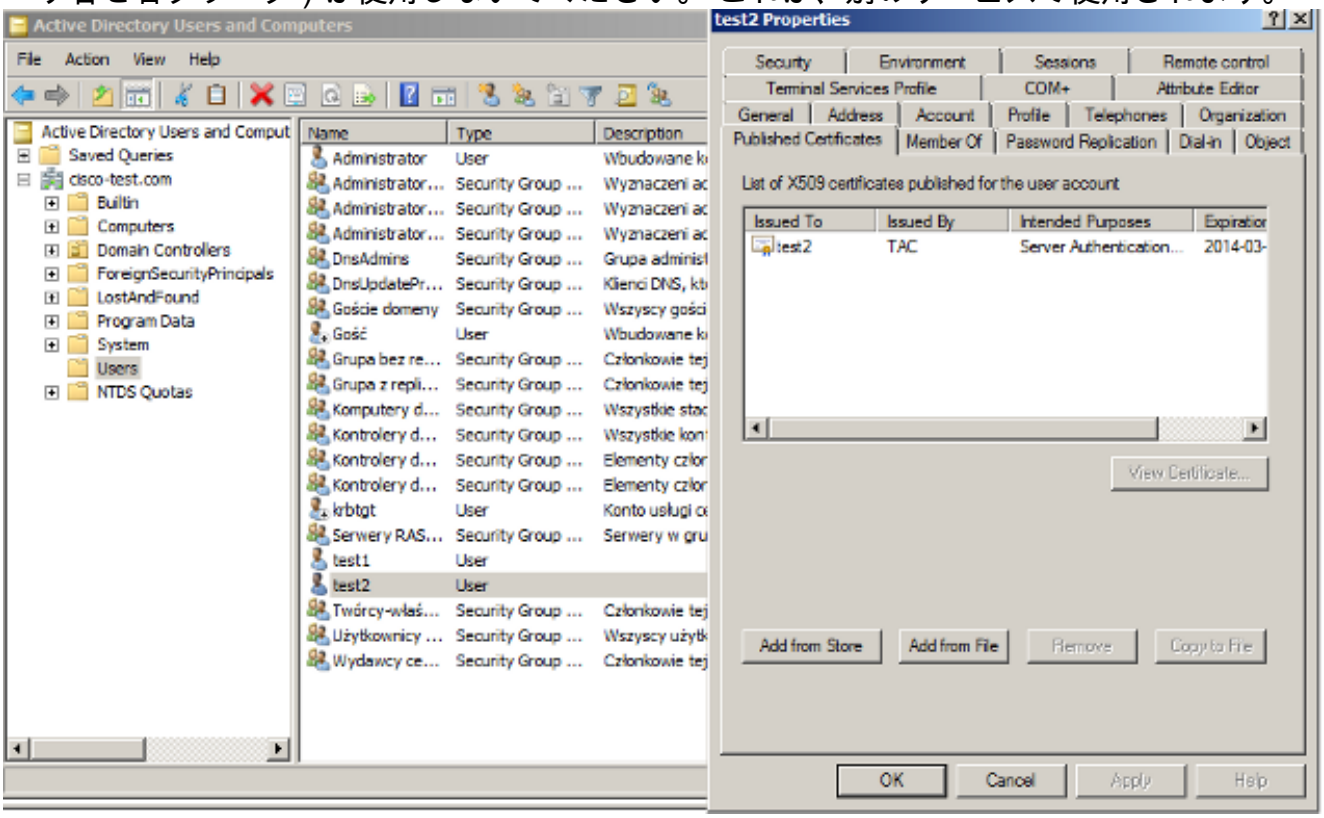
ドメイン コントローラのコンフィギュレーション

特定の証明書を AD の特定のユーザにマッピングする必要があります。

1. Active Directory ユーザおよびコンピュータから、[Users] フォルダに移動します。
2. [View] メニューから、[Advanced Features] を選択します。



3. 次のユーザを追加します。 test1test2test3**注：**パスワードは重要ではありません。
4. [Properties] ウィンドウから、[Published Certificates] タブを選択します。テスト用の証明書を選択します。たとえば、test1 の場合、ユーザ CN は test1 です。**注：**名前マッピング（ユーザ名を右クリック）は使用しないでください。 これは、別のサービスで使用されます。



この段階では、証明書は、AD の特定のユーザにバインドされます。これは、ldapsearch で検証できます。

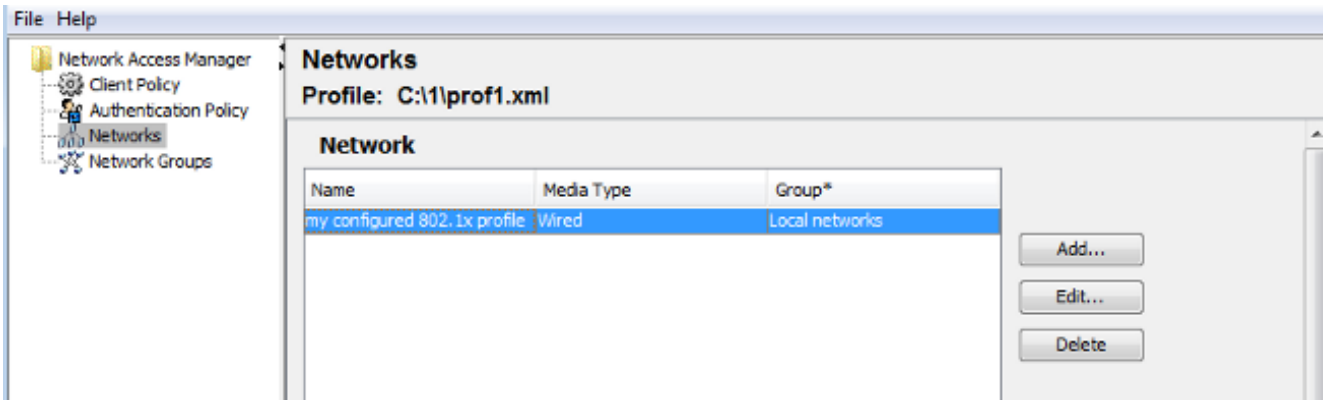
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

次に、test2 の結果の例を示します。

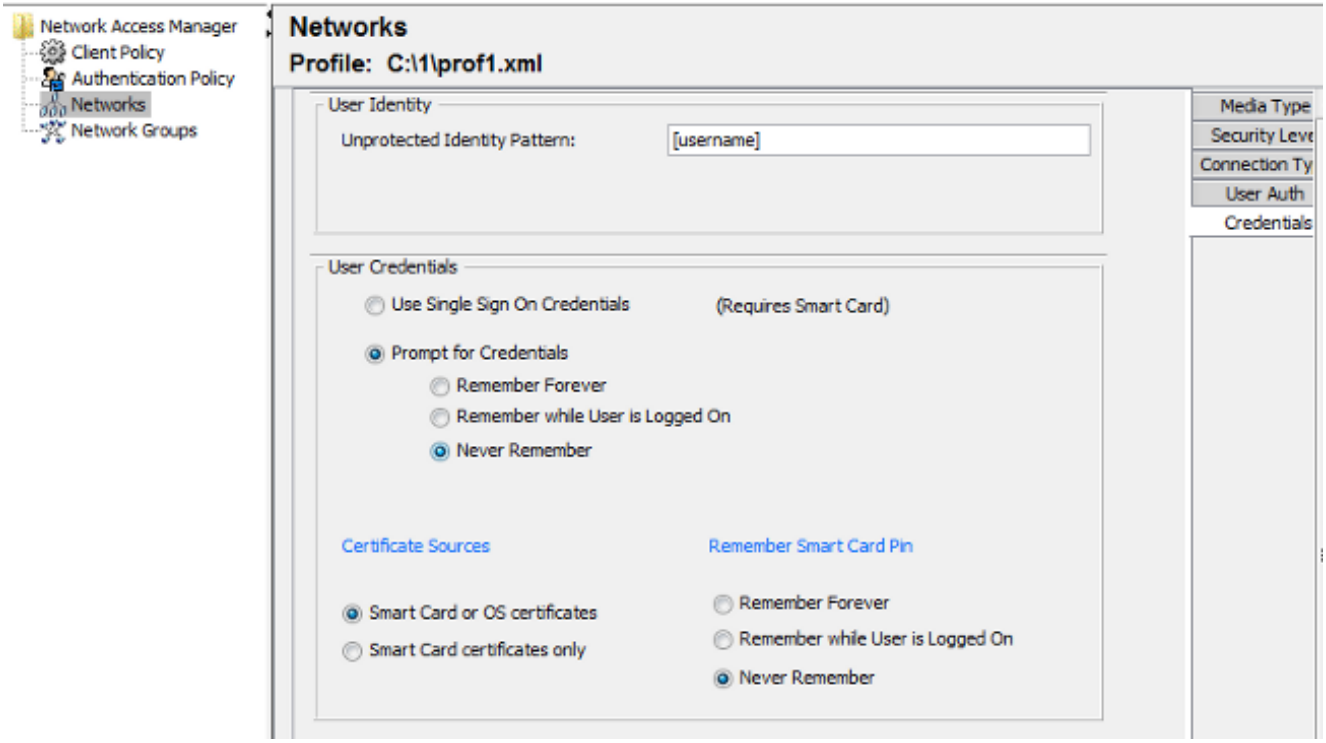
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

サプリカントのコンフィギュレーション

1. このプロファイル エディタ、anyconnect-profileeditor-win-3.1.00495-k9.exe をインストールします。
2. Network Access Manager Profile Editor を開き、特定のプロファイルを設定します。
3. 特定の有線ネットワークを作成します。



この段階で、各認証で証明書を使用する選択肢をユーザに与えることは非常に重要です。この選択はキャッシュされません。また、保護されていないIDとして「username」を使用します。ACSが証明書のADを照会するために使用するIDと同じではないことに注意してください。この ID は、ACS で設定されます。



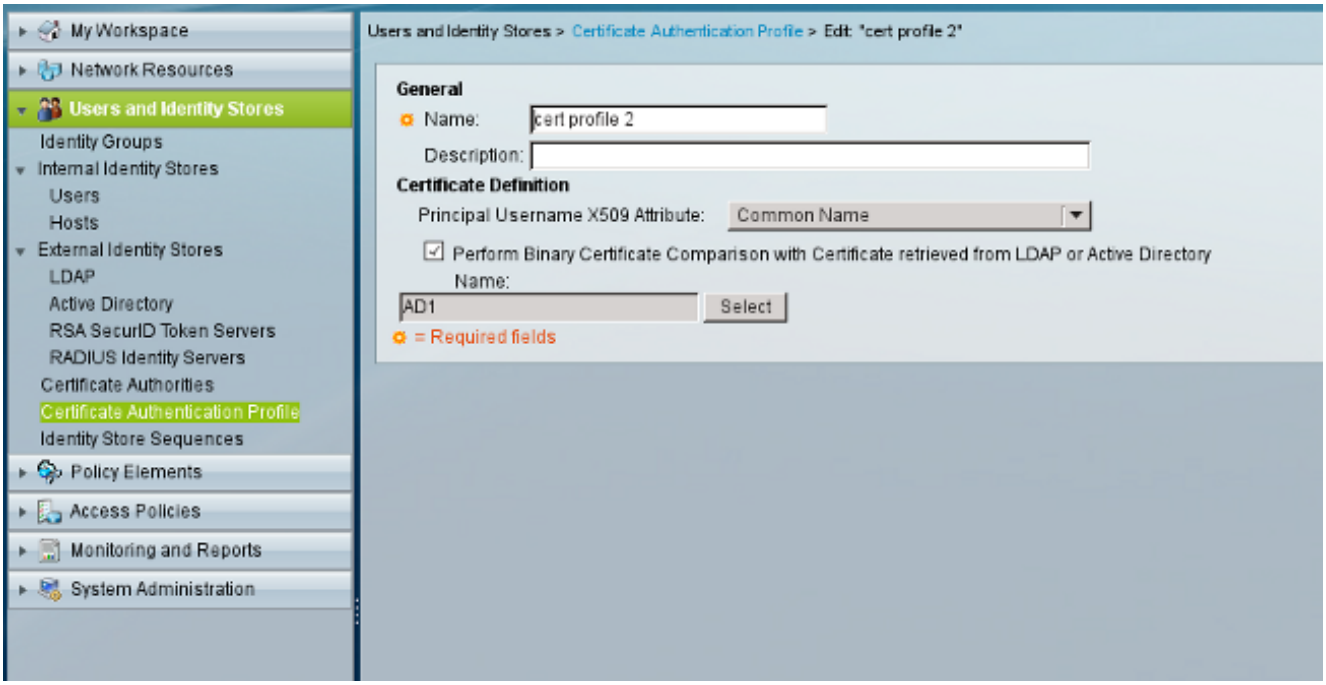
4. .xml ファイルを c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml として保存します。
5. Cisco AnyConnect NAM サービスを再起動します。

この例では、手動によるプロファイル導入を示します。AD を使用して、このファイルをすべてのユーザに導入できます。また、VPN と統合される場合、ASA を使用してプロファイルをプロビジョニングできます。

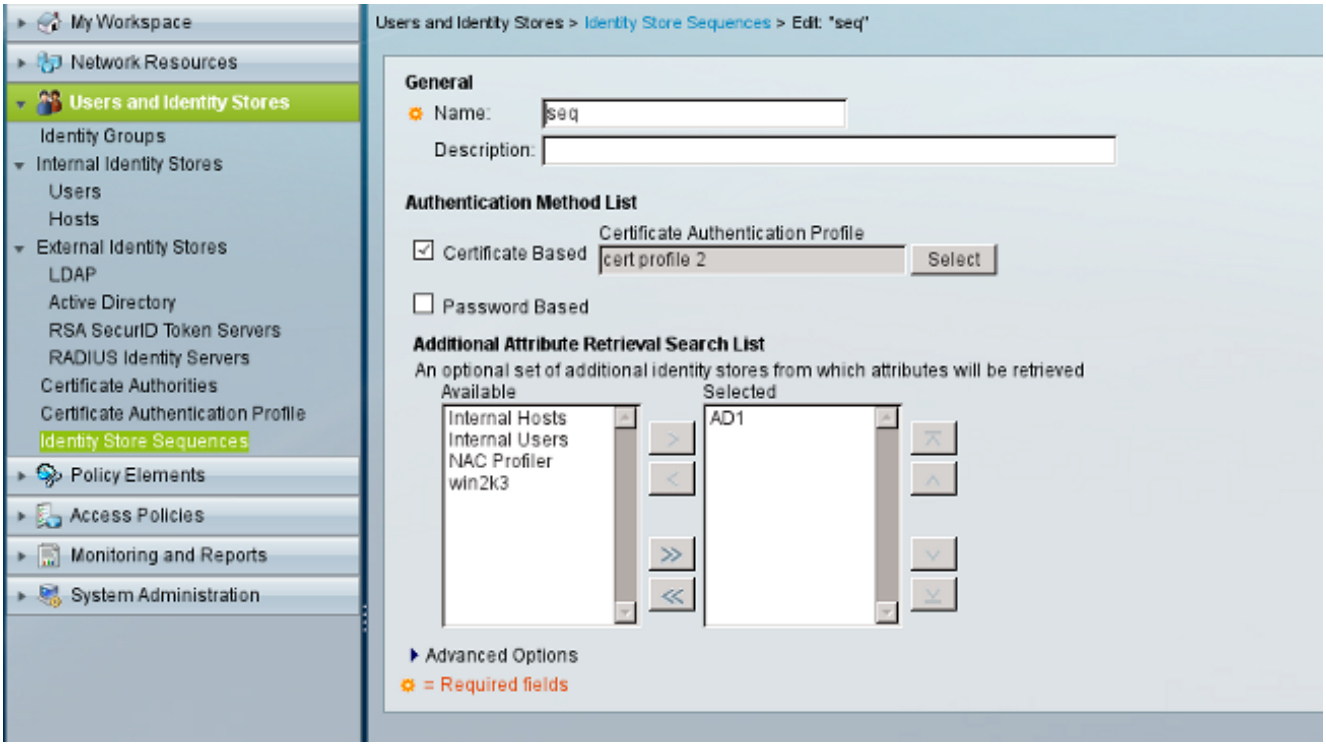
ACS 設定

1. AD ドメインに参加します。

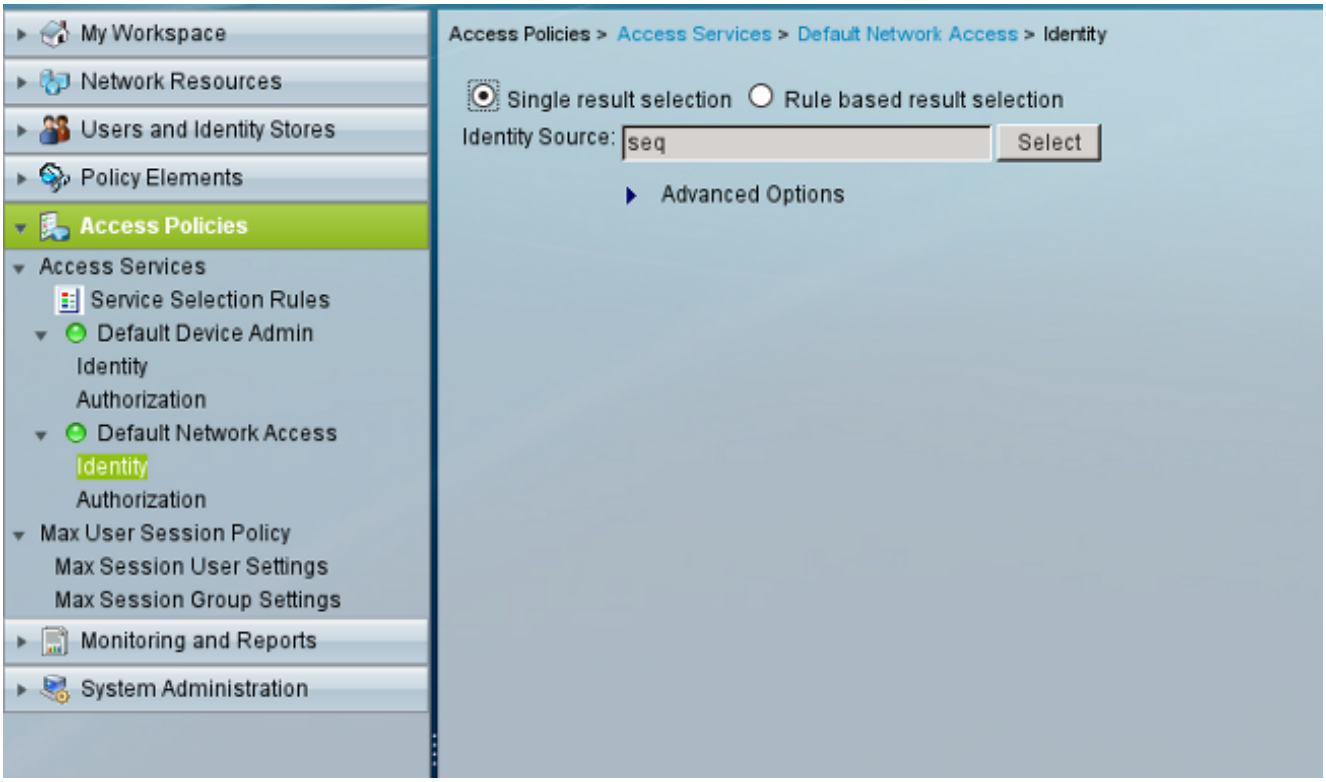
ACS は、サプリカントから受信した証明書の CN フィールドを使用して、AD ユーザ名をマッチングします（この例では、test1、test2 または test3 です）。 バイナリ比較もイネーブルにされます。これにより、ACS は、AD からユーザ証明書を取得して、サプリカントにより受信した同じ証明書と比較します。これが一致しない場合、認証は失敗します。



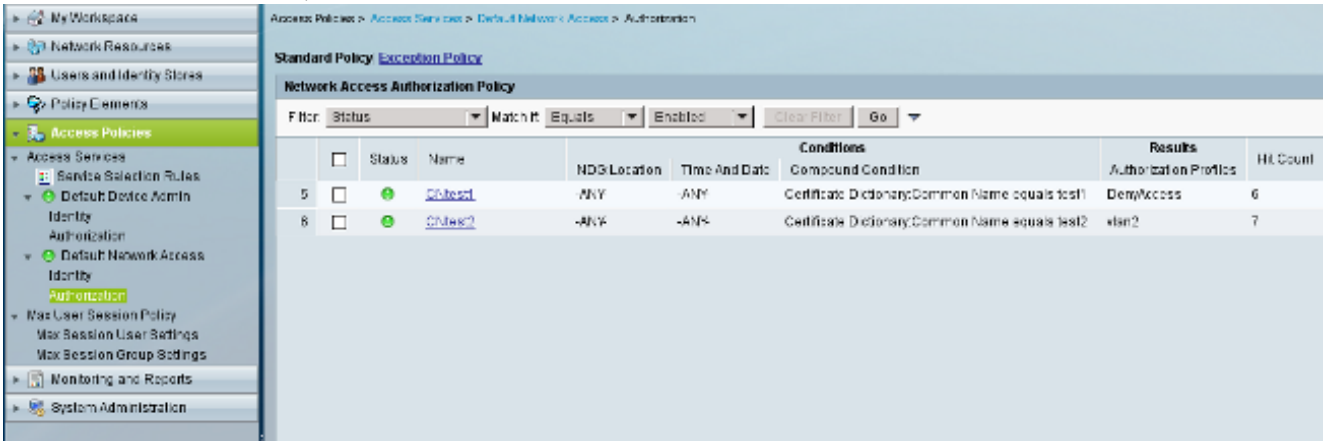
2. Identity Store Sequence を設定します。これは、証明書ベースの認証および証明書プロファイルで AD を使用します。



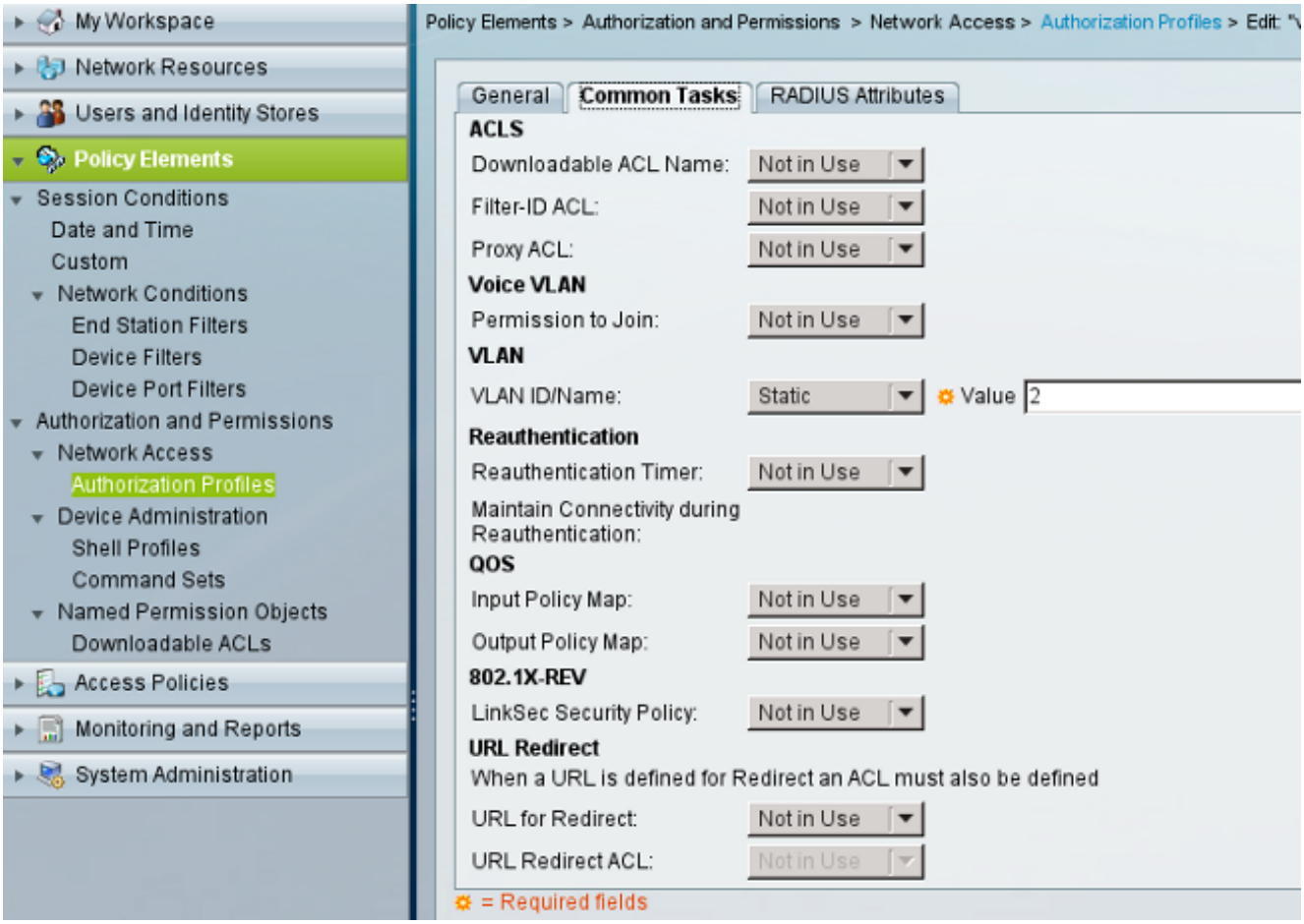
これは、RADIUS Identity ポリシーの Identity Source として使用されます。



3. 2 つの認証ポリシーを設定します。最初のポリシーは、test1 に使用され、そのユーザのアクセスを拒否します。もう一方のポリシーは、test 2 に使用され、VLAN2 プロファイルでのアクセスを許可します。

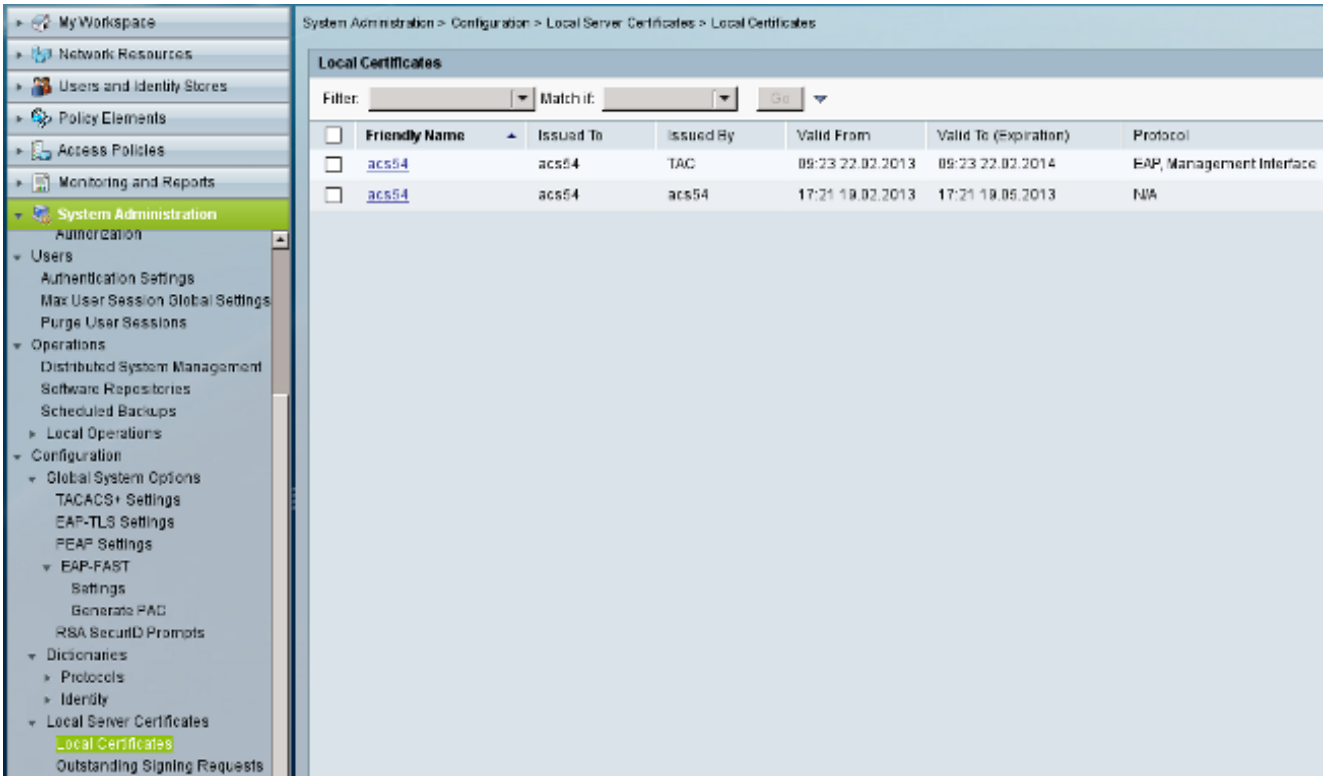


VLAN2 は、ユーザとスイッチの VLAN2 をバインドする RADIUS 属性を返す認証プロファイルです。



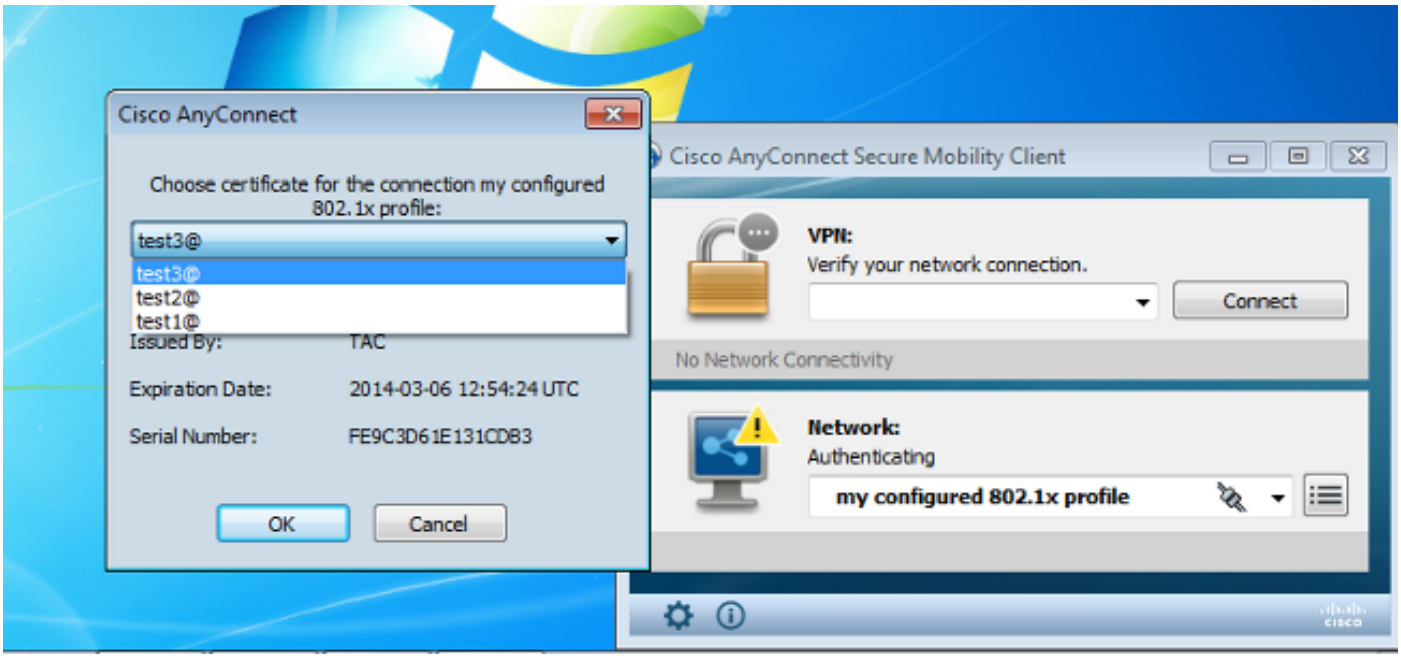
4. ACS に CA 証明書をインストールします。

5. ACS の Cisco の CA により署名される証明書（拡張認証プロトコルで使用）を生成およびインストールします。



確認

AnyConnect NAM が使用されるまで、Windows 7 サプリカントでネイティブ 802.1x サービスをディセーブルにすることをお勧めします。設定済みプロファイルにより、クライアントは特定の証明書の選択が許可されます。



test2 証明書が使用される場合、スイッチは、成功応答と RADIUS 属性を受信します。

```
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
```

VLAN 2 は割り当てられます。 他の RADIUS 属性を ACS の認証プロファイルに追加できます（Advanced Access Control List または再認証タイマーなど）。

次に、ACS のログを示します。

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
24469 The user certificate was retrieved from Active Directory successfully.
22054 Binary comparison of certificates succeeded.
22037 Authentication Passed
22023 Proceed to attribute retrieval
22038 Skipping the next IDStore for attribute retrieval because it is the one we authenticated against
22016 Identity sequence completed iterating the IDStores
Evaluating Group Mapping Policy
12506 EAP-TLS authentication succeeded
11503 Prepared EAP-Success
Evaluating Exception Authorization Policy
15042 No rule was matched
Evaluating Authorization Policy
15004 Matched rule
15016 Selected Authorization Profile - vlan2
22065 Max sessions policy passed
22064 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

トラブルシュート

ACS での無効な時間設定

発生する可能性のあるエラー：ACS Active Directory の内部エラー

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.

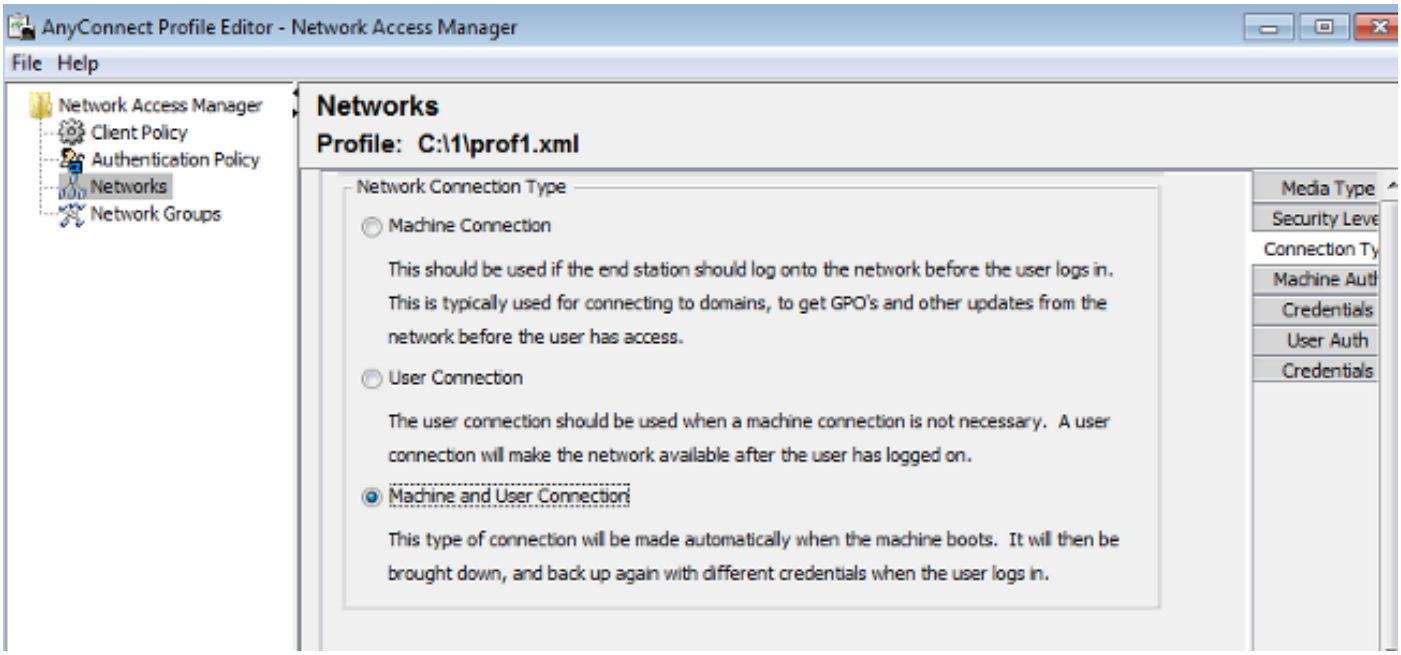
証明書が AD DC で設定およびバインドされない

発生する可能性のあるエラー：Active Directory からユーザ証明書を受信できませんでした。

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 プロファイルのカスタマイズ

企業ネットワークでは、マシンとユーザの両方の証明書を使用して認証を行うことをお勧めします。このような場合、制限付き VLAN のスイッチでオープン 802.1x モードを使用することをお勧めします。802.1x でマシンを再起動する場合、最初の認証セッションが開始し、AD マシン証明書を使用して認証が行われます。次に、ユーザが証明書を提供し、ドメインにログインすると、ユーザ証明書で次の認証セッションが開始されます。ユーザは、正しい（信頼できる）VLAN に接続され、フル ネットワーク アクセスが提供されます。これは、Identity Services Engine（ISE）で統合されます。



[Machine Authentication] および [User Authentication] タブから個別の認証を設定できます。

オープン 802.1x モードがスイッチで許容されない場合、ログオン機能がクライアント ポリシーで設定される前に、802.1x モードを使用できます。

関連情報

- Cisco Secure Access Control System 5.3 ユーザ ガイド
- Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 3.0
- AnyConnect セキュア モビリティ クライアント 3.0:Windows 上での Network Access Manager& Profile Editor
- テクニカル サポートとドキュメント – Cisco Systems