Konfigurationsbeispiel für 802.1x-EAP-TLS mit binärem Zertifikatsvergleich aus AD- und NAM-Profilen

Inhalt

Einführung

In diesem Dokument wird die 802.1x-Konfiguration mit Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) und Access Control System (ACS) beschrieben, da diese einen binären Zertifikatvergleich zwischen einem vom Supplicant bereitgestellten Clientzertifikat und demselben in Microsoft Active Directory (AD) aufbewahrten Zertifikat durchführen. Das AnyConnect Network Access Manager (NAM)-Profil wird zur Anpassung verwendet. Die Konfiguration für alle Komponenten wird in diesem Dokument zusammen mit Szenarien zur Fehlerbehebung bei der Konfiguration vorgestellt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Topologie

- 802.1x-Komponente - Windows 7 mit Cisco AnyConnect Secure Mobility Client Release 3.1.01065 (NAM-Modul)
- 802.1x-Authentifizierer - 2960-Switch
- 802.1x-Authentifizierungsserver - ACS Version 5.4
- ACS integriert in Microsoft AD - Domain Controller - Windows 2008 Server

Topologiedetails

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (e0/0 - Komponente verbunden)
- Gleichstrom: 192.168.10.101
- Windows 7 - DHCP

Fluss

Auf der Windows 7-Station ist AnyConnect NAM installiert, das als Komponente für die Authentifizierung am ACS-Server mithilfe der EAP-TLS-Methode verwendet wird. Der Switch mit 802.1x fungiert als Authentifizierer. Das Benutzerzertifikat wird vom ACS verifiziert, und die Richtlinienautorisierung wendet Richtlinien an, die auf dem Common Name (CN) des Zertifikats basieren. Darüber hinaus ruft der ACS das Benutzerzertifikat von AD ab und führt einen Binärvergleich mit dem vom Supplicant bereitgestellten Zertifikat durch.

Switch-Konfiguration

Der Switch verfügt über eine Basiskonfiguration. Standardmäßig befindet sich der Port im Quarantäne-VLAN 666. Dieses VLAN hat einen eingeschränkten Zugriff. Nachdem der Benutzer autorisiert wurde, wird das Port-VLAN neu konfiguriert.

```
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
```

Zertifikatvorbereitung

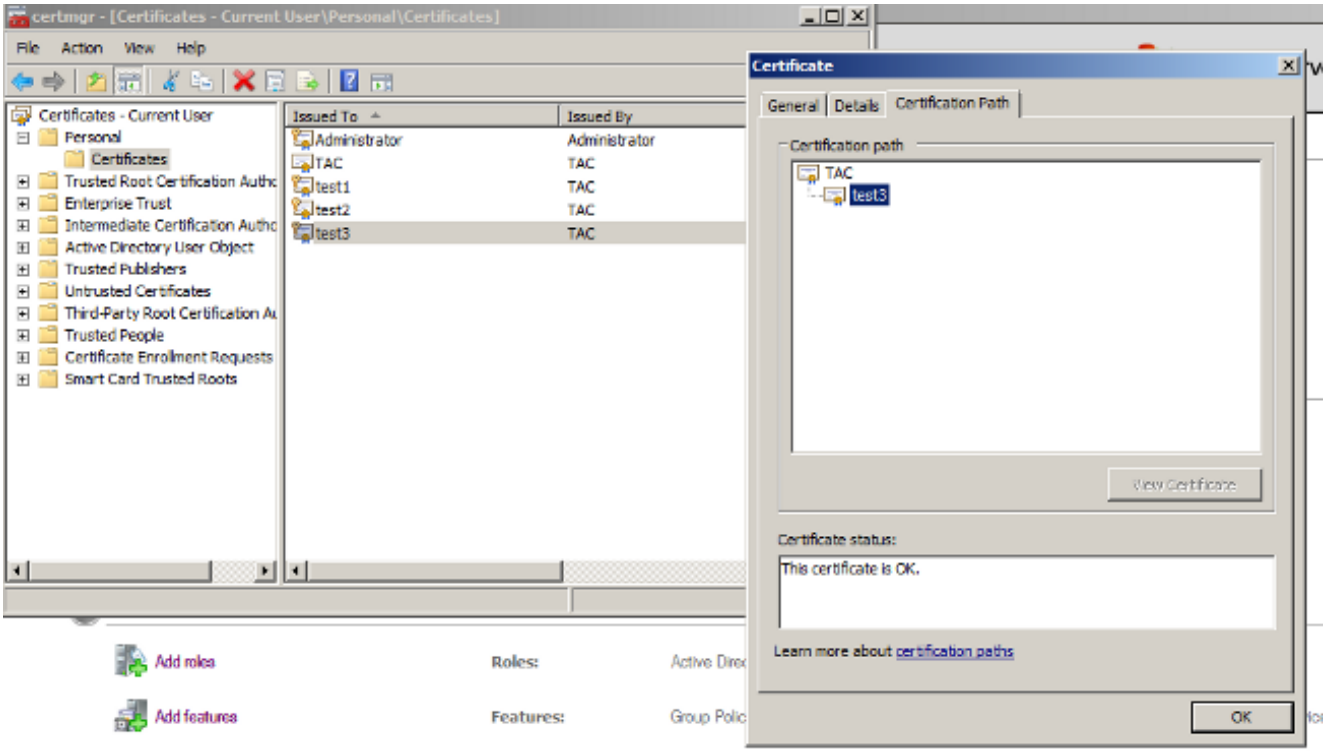
Für EAP-TLS ist sowohl für den Supplicant als auch für den Authentifizierungsserver ein Zertifikat erforderlich. Dieses Beispiel basiert auf von OpenSSL generierten Zertifikaten. Microsoft Certificate Authority (CA) kann zur Vereinfachung der Bereitstellung in Enterprise-Netzwerken eingesetzt werden.

1. Geben Sie zum Generieren der CA die folgenden Befehle ein:
   ```
   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
   ```
   Das CA-Zertifikat wird in der Datei ca.crt und der private (und ungeschützte) Schlüssel in der Datei ca.key gespeichert.
2. Erstellen Sie drei Benutzerzertifikate und ein Zertifikat für ACS, die alle von dieser Zertifizierungsstelle signiert werden: CN=Test1CN=Test2CN=Test3CN=ACS54Das Skript zum Generieren eines einzelnen Zertifikats, das von der Cisco Zertifizierungsstelle signiert wird, lautet:
   ```
   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
   ```
   Der private Schlüssel befindet sich in der Datei server.key und das Zertifikat in der Datei server.crt. Die Version pkcs12 befindet sich in der Datei server.pfx.

3. Doppelklicken Sie auf jedes Zertifikat (PFX-Datei), um es in den Domänencontroller zu importieren. Im Domain Controller sollten alle drei Zertifikate vertrauenswürdig sein.

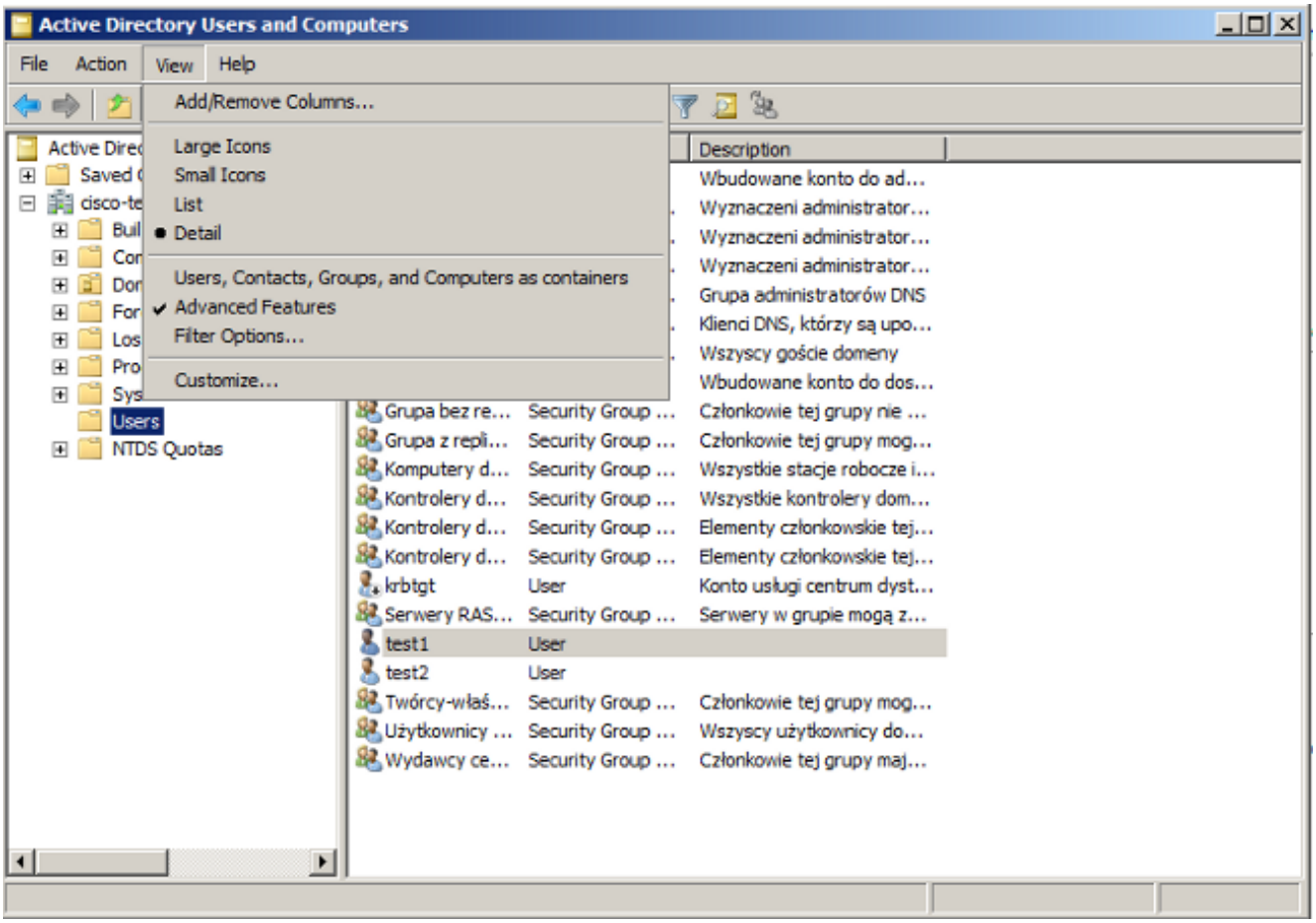


Derselbe Prozess kann in Windows 7 (Supplicant) ausgeführt werden oder mithilfe von Active Directory die Benutzerzertifikate übertragen werden.

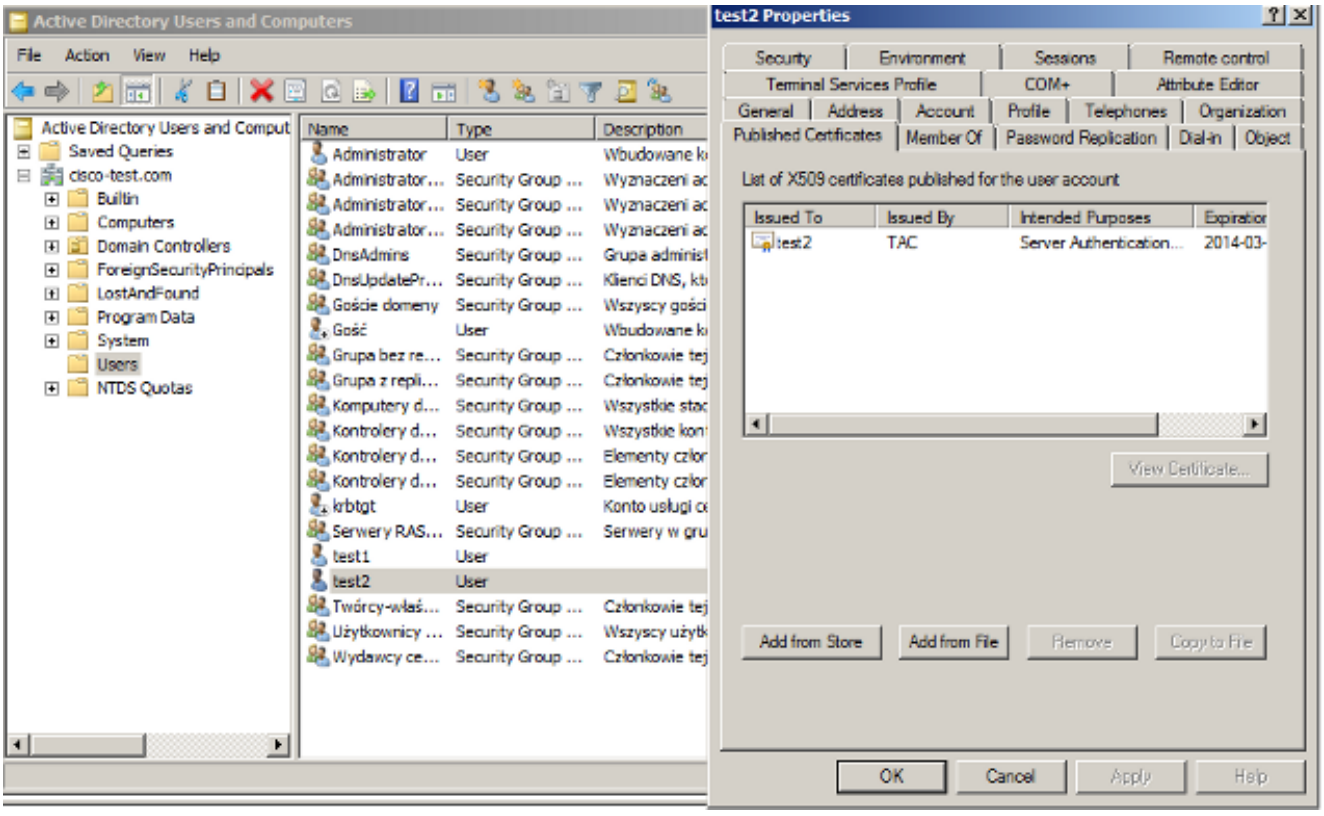
Domänencontrollerkonfiguration

Das spezifische Zertifikat muss dem jeweiligen Benutzer in AD zugeordnet werden.

1. Navigieren Sie von Active Directory-Benutzern und -Computern zum Ordner **Benutzer**.
2. Wählen Sie im Menü Ansicht die Option **Erweiterte Funktionen aus**.



3. Fügen Sie diese Benutzer hinzu: Test1Test2Test3**Hinweis**: Das Kennwort ist nicht wichtig.
4. Wählen Sie im Eigenschaftenfenster die Registerkarte **Veröffentlichte Zertifikate aus**. Wählen Sie das spezifische Zertifikat für den Test aus. Für Test1 ist die Benutzer-CN beispielsweise test1.**Hinweis**: Verwenden Sie keine Namenszuordnung (klicken Sie mit der rechten Maustaste auf den Benutzernamen). Es wird für verschiedene Services verwendet.



In dieser Phase wird das Zertifikat an einen bestimmten Benutzer in AD gebunden. Dies kann

mithilfe von ldapsearch überprüft werden:

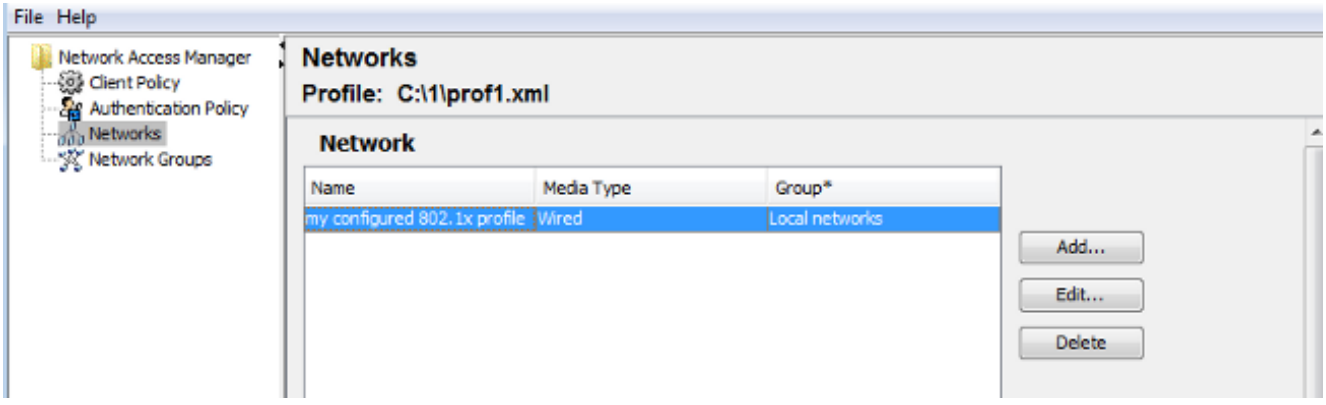
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

Die Beispielergebnisse für Test2 sind wie folgt:

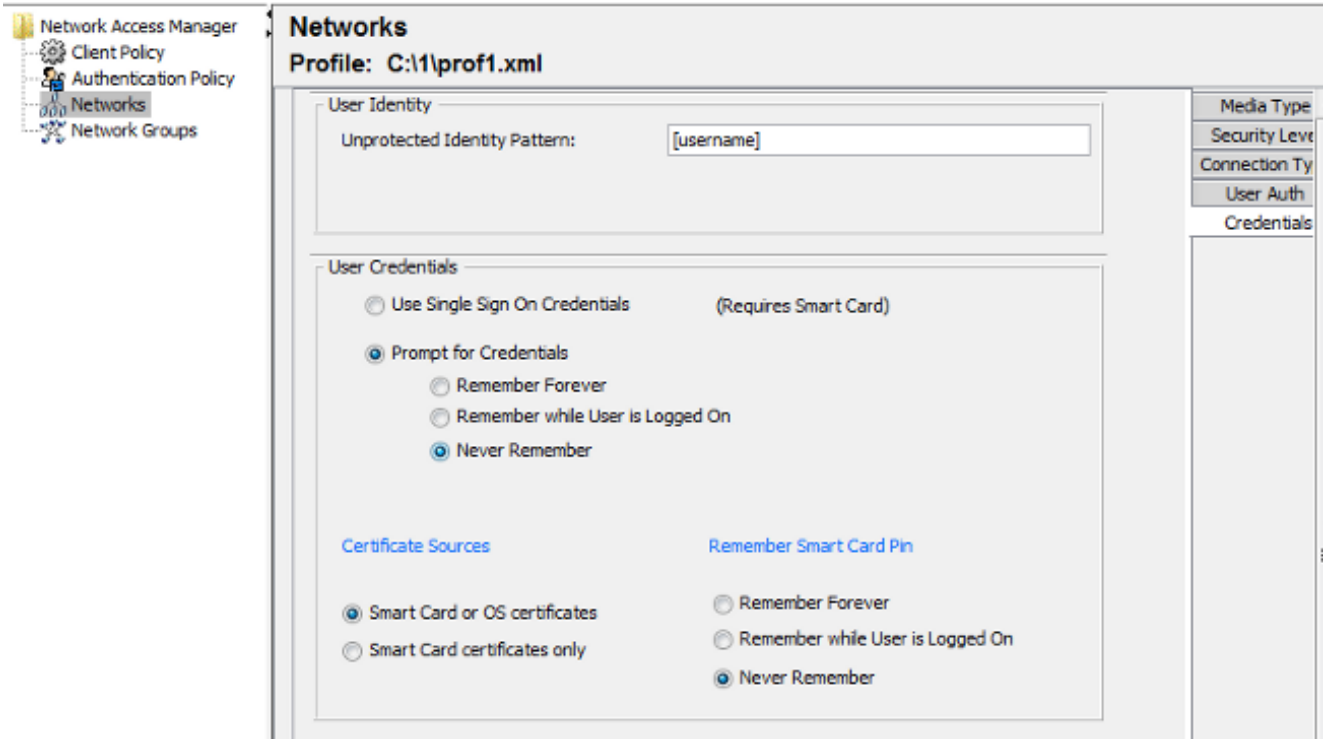
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

Supplicant-Konfiguration

1. Installieren Sie diesen Profil-Editor anyconnect-profile editor-win-3.1.00495-k9.exe.
2. Öffnen Sie den Network Access Manager Profile Editor, und konfigurieren Sie das spezifische Profil.
3. Erstellen Sie ein bestimmtes kabelgebundenes Netzwerk.



In diesem Stadium ist es sehr wichtig, dem Benutzer die Möglichkeit zu geben, das Zertifikat bei jeder Authentifizierung zu verwenden. Diese Auswahl nicht zwischenspeichern. Verwenden Sie auch den 'username' als ungeschützte ID. Es ist wichtig zu beachten, dass es sich nicht um dieselbe ID handelt, die von ACS verwendet wird, um AD für das Zertifikat abzufragen. Diese ID wird im ACS
konfiguriert.

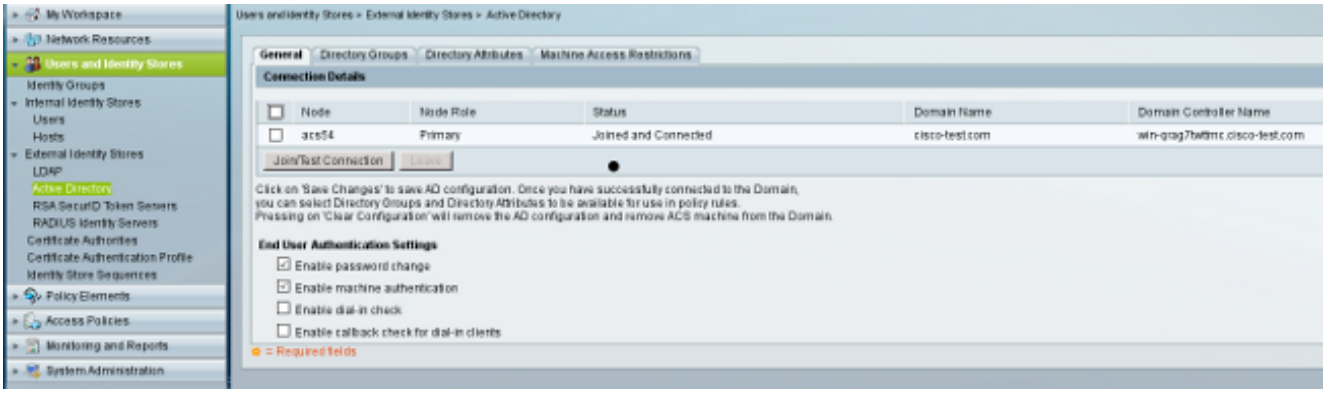


4. Speichern Sie die XML-Datei als c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Starten Sie den Cisco AnyConnect NAM-Dienst neu.

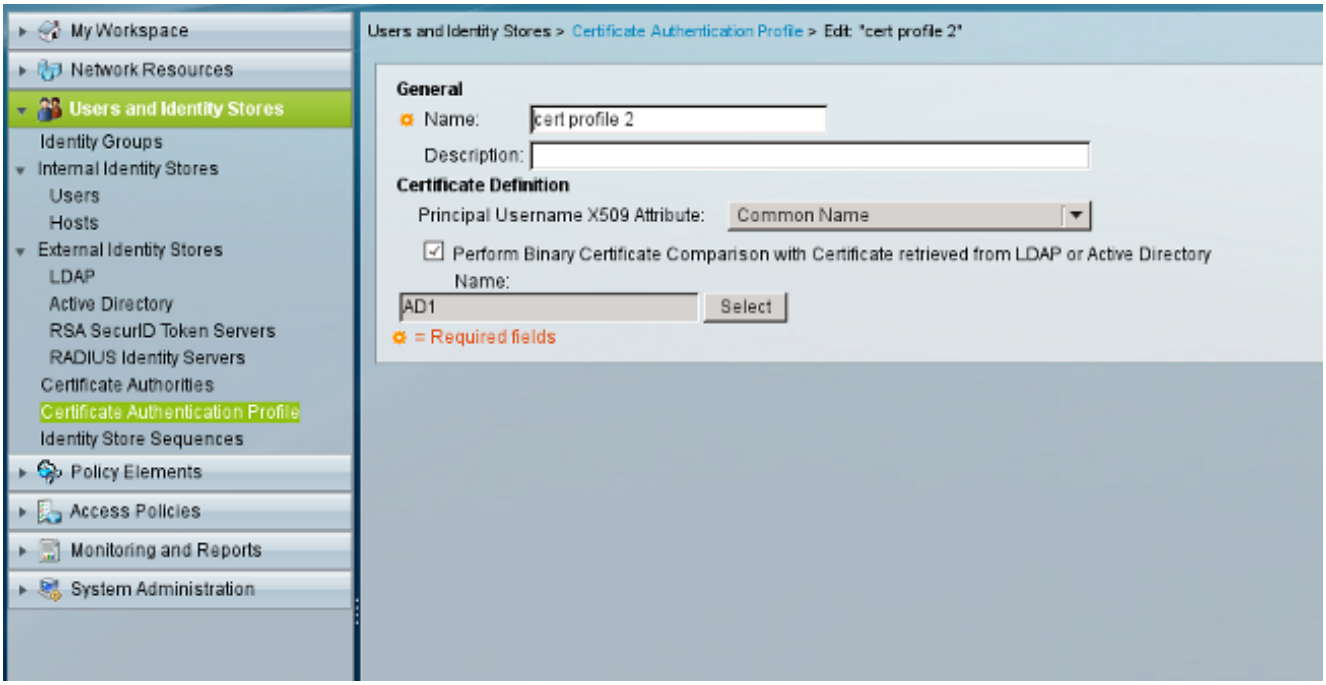
Dieses Beispiel zeigte eine manuelle Profilbereitstellung. AD könnte verwendet werden, um diese Datei für alle Benutzer bereitzustellen. Bei der Integration in VPNs kann das Profil auch mithilfe der ASA bereitgestellt werden.

ACS-Konfiguration

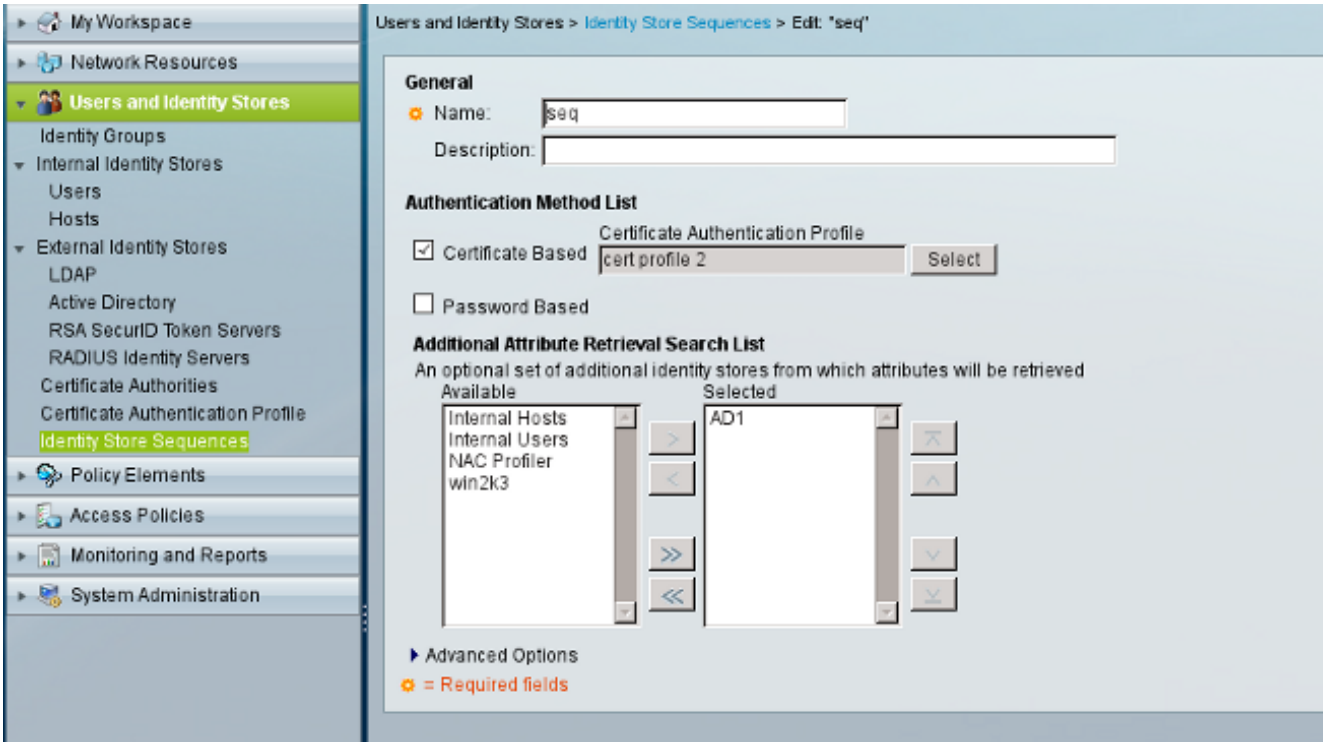
1. Treten Sie der AD-Domäne
   bei.



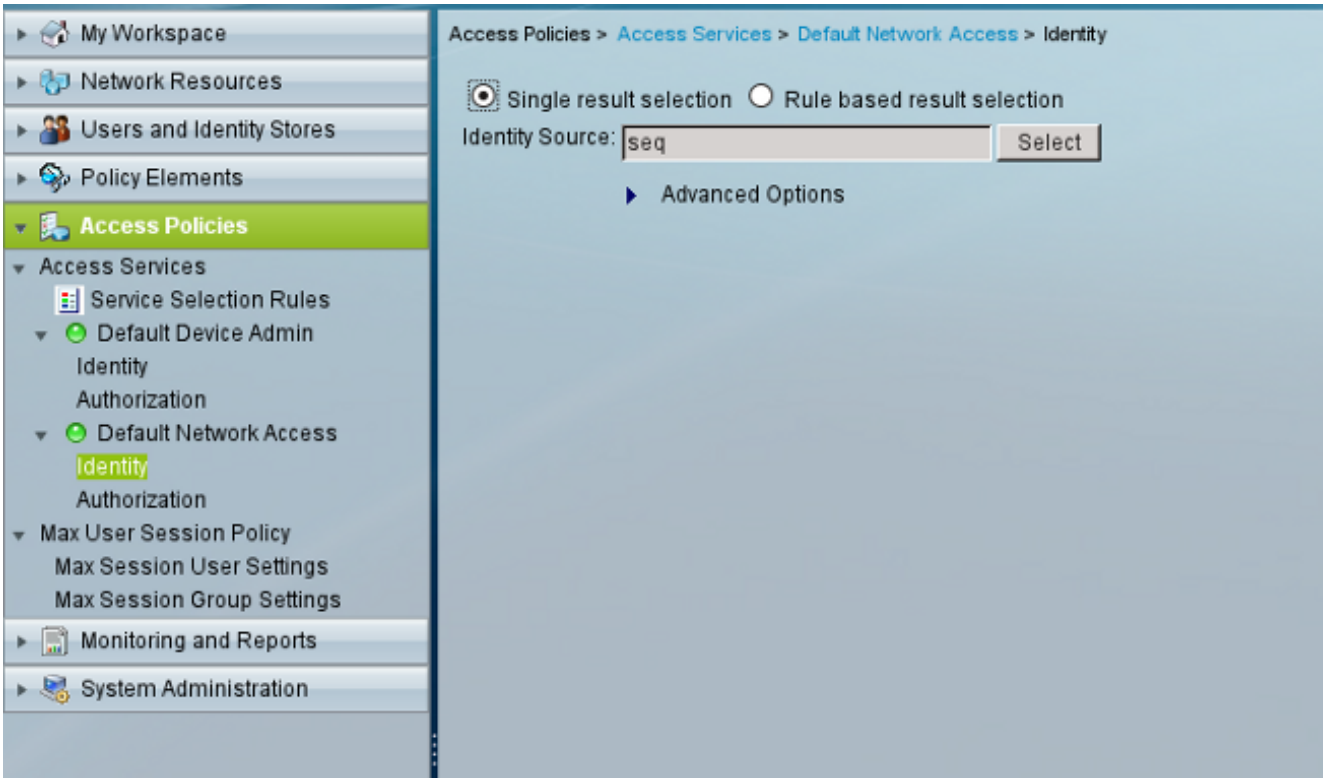
   ACS ordnet AD-Benutzernamen der Verwendung des CN-Felds aus dem Zertifikat zu, das vom Supplicant empfangen wurde (in diesem Fall Test1, test2 oder test3). Der Binärvergleich ist ebenfalls aktiviert. Dadurch wird ACS gezwungen, das Benutzerzertifikat von AD zu erhalten und es mit dem gleichen Zertifikat zu vergleichen, das der Supplicant erhalten hat. Wenn sie nicht übereinstimmt, schlägt die Authentifizierung
   fehl.



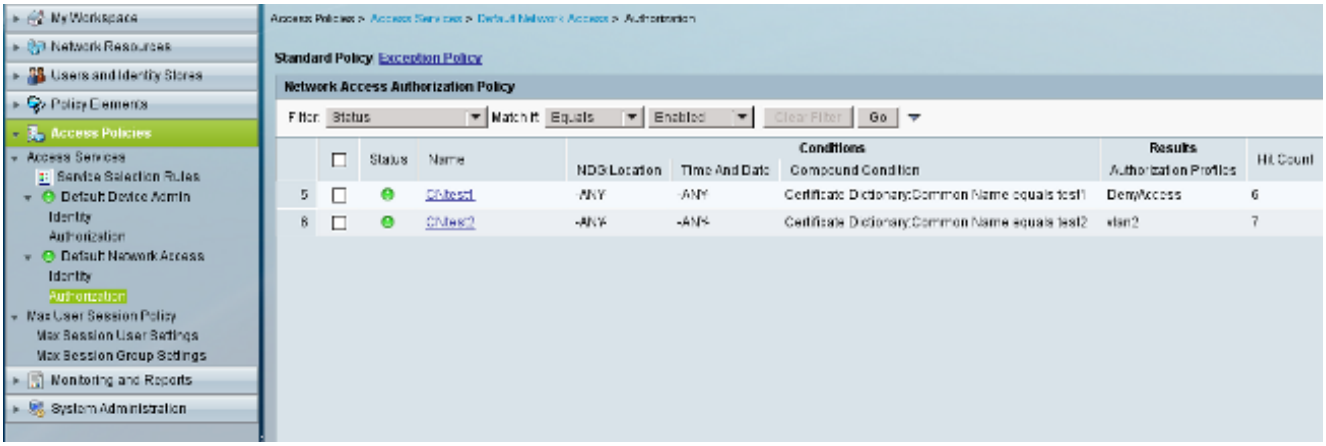
2. Konfigurieren Sie die Identity Store-Sequenzen, die AD für die zertifikatsbasierte Authentifizierung zusammen mit dem Zertifikatprofil verwenden.



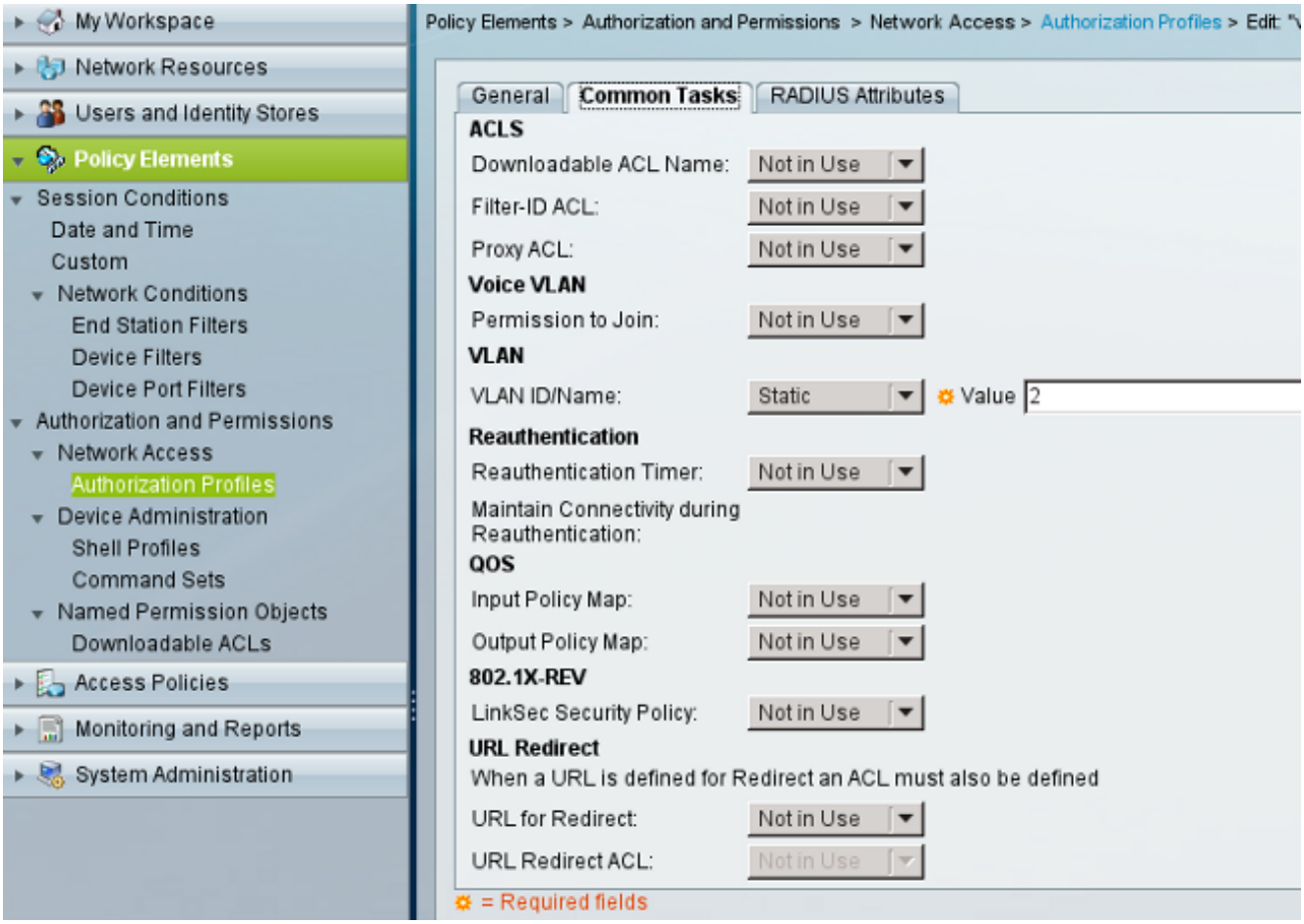
Dies wird als Identitätsquelle in der RADIUS-Identitätsrichtlinie verwendet.



3. Konfigurieren Sie zwei Autorisierungsrichtlinien. Die erste Richtlinie wird für test1 verwendet und verweigert diesem Benutzer den Zugriff. Die zweite Richtlinie wird für Test 2 verwendet und ermöglicht den Zugriff mit dem VLAN2-
Profil.

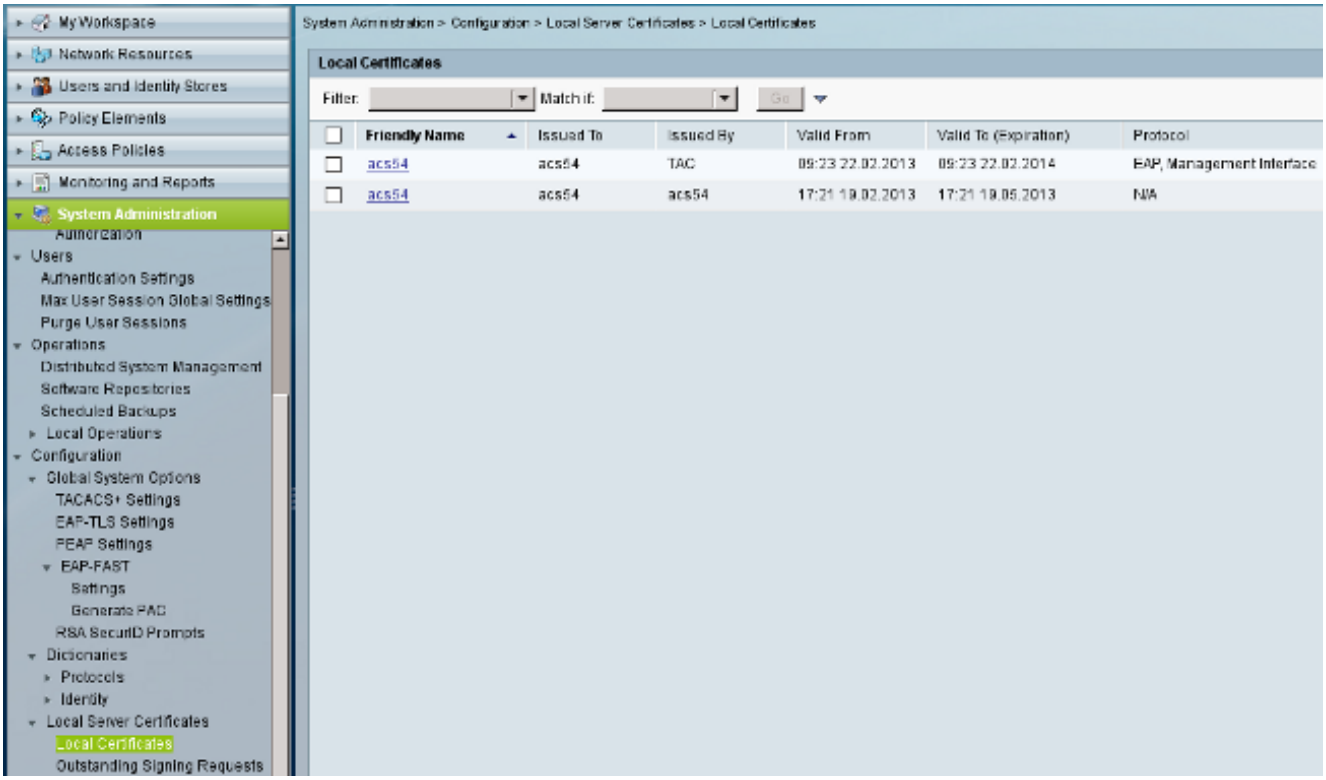


VLAN2 ist das Autorisierungsprofil, das RADIUS-Attribute zurückgibt, die den Benutzer an VLAN2 auf dem Switch
binden.



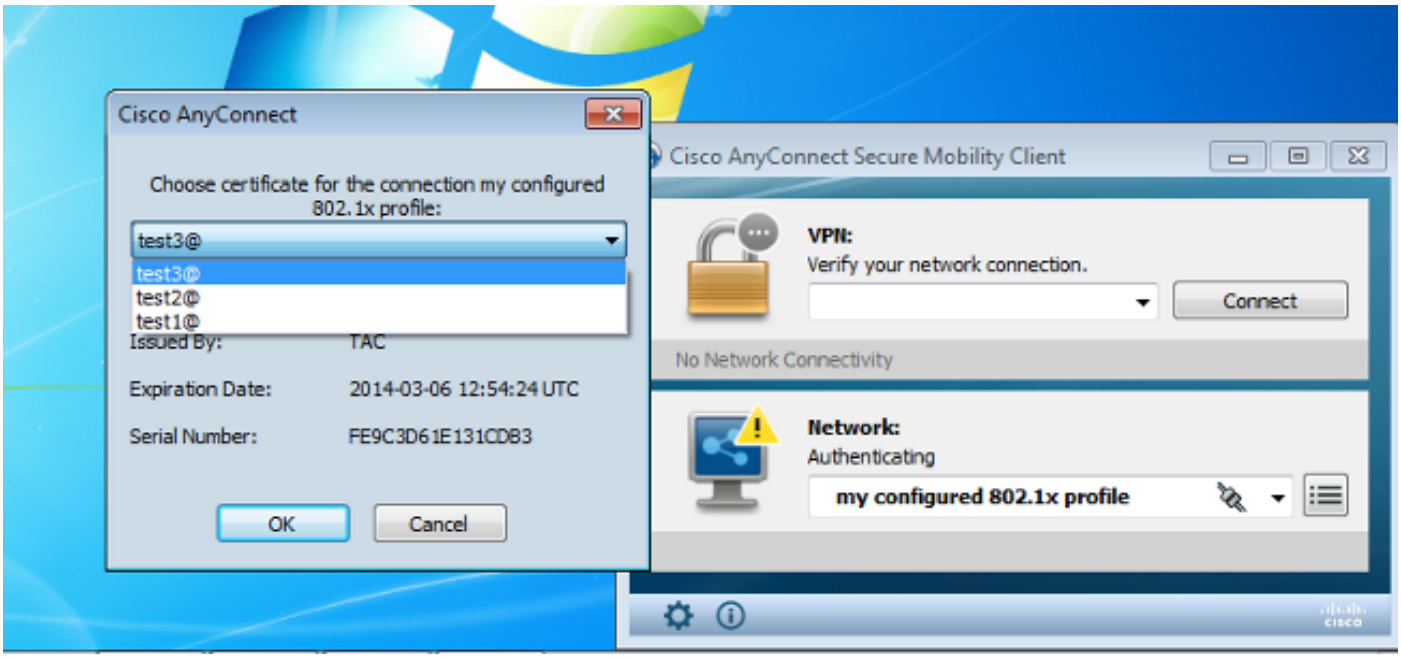
4. Installieren Sie das Zertifizierungsstellenzertifikat auf dem ACS.

5. Generieren und Installieren des Zertifikats (für die Verwendung des Extensible Authentication Protocol), das von der Cisco CA für ACS signiert wurde.



Überprüfen

Es empfiehlt sich, den nativen 802.1x-Dienst auf der Windows 7-Komponente zu deaktivieren, da AnyConnect NAM verwendet wird. Mit dem konfigurierten Profil kann der Client ein bestimmtes Zertifikat auswählen.



Wenn das Test2-Zertifikat verwendet wird, erhält der Switch zusammen mit den RADIUS-Attributen eine Erfolgsantwort.

```
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
```

Beachten Sie, dass VLAN 2 zugewiesen wurde. Es ist möglich, diesem Autorisierungsprofil auf ACS weitere RADIUS-Attribute hinzuzufügen (z. B. eine erweiterte Zugriffskontrollliste oder Timer für die erneute Autorisierung).

Die Protokolle für den ACS sind wie folgt:

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

Fehlerbehebung

Ungültige Zeiteinstellungen für ACS

Möglicher Fehler - interner Fehler 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.

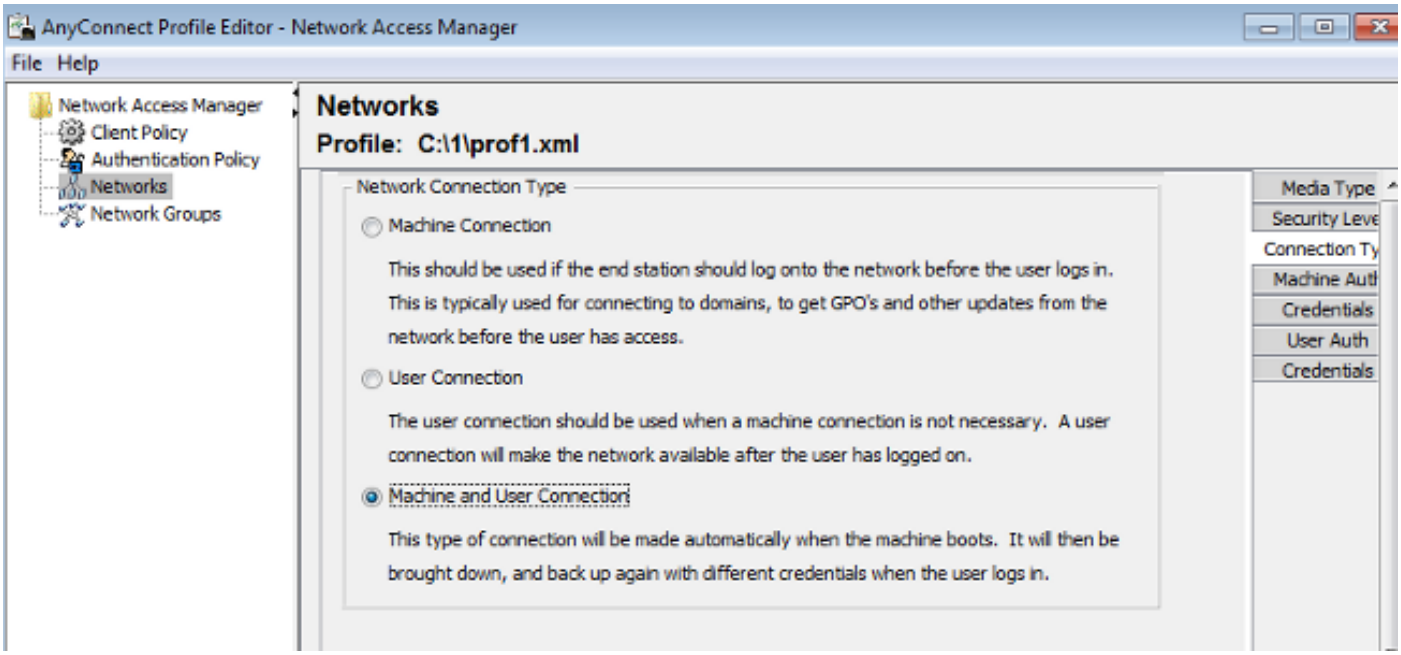
Kein Zertifikat konfiguriert und auf AD DC gebunden

Möglicher Fehler - Abruf des Benutzerzertifikats von Active Directory fehlgeschlagen

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

Anpassung des NAM-Profils

In Enterprise-Netzwerken wird empfohlen, die Authentifizierung mithilfe von Computer- und Benutzerzertifikaten vorzunehmen.In einem solchen Szenario wird empfohlen, den offenen 802.1x-Modus auf dem Switch mit eingeschränktem VLAN zu verwenden. Beim Neustart des Computers für 802.1x wird die erste Authentifizierungssitzung initiiert und mithilfe des Zertifikats des AD-Systems authentifiziert. Nachdem der Benutzer Anmeldeinformationen bereitgestellt und sich bei der Domäne angemeldet hat, wird die zweite Authentifizierungssitzung mit dem Benutzerzertifikat initiiert. Der Benutzer wird in das richtige (vertrauenswürdige) VLAN mit vollständigem Netzwerkzugriff gesetzt. Sie ist nahtlos in die Identity Services Engine (ISE) integriert.



Anschließend können separate Authentifizierungen von den Registerkarten "Machine Authentication" (Computerauthentifizierung) und "User Authentication" (Benutzerauthentifizierung) konfiguriert werden.

Wenn der offene 802.1x-Modus auf dem Switch nicht akzeptiert werden kann, kann der 802.1x-Modus verwendet werden, bevor die Anmeldungsfunktion in der Client-Richtlinie konfiguriert wird.

Zugehörige Informationen

- Benutzerhandbuch zum Cisco Secure Access Control System 5.3
- Administratorhandbuch für Cisco AnyConnect Secure Mobility Client, Version 3.0
- AnyConnect Secure Mobility Client 3.0: Network Access Manager und Profile Editor unter Windows
- Technischer Support und Dokumentation - Cisco Systems