Esempio di configurazione dei profili 802.1x EAP-TLS con confronto dei certificati binari da AD e NAM

Sommario

Introduzione

In questo documento viene descritta la configurazione 802.1x con EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) e ACS (Access Control System) in quanto questi eseguono un confronto binario tra un certificato client fornito dal richiedente e lo stesso certificato conservato in Microsoft Active Directory (AD). Il profilo AnyConnect Network Access Manager (NAM) viene usato per la personalizzazione. La configurazione per tutti i componenti è illustrata in questo documento, insieme a scenari per la risoluzione dei problemi relativi alla configurazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Topologia

- Supplicant 802.1x - Windows 7 con Cisco AnyConnect Secure Mobility Client release 3.1.01065 (modulo NAM)
- autenticatore 802.1x - switch 2960
- Server di autenticazione 802.1x - ACS release 5.4
- ACS integrato con Microsoft AD - Controller di dominio - Windows 2008 Server

Dettagli topologia

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

Flusso

Sulla stazione di Windows 7 è installato AnyConnect NAM, che viene usato come supplicant per autenticarsi al server ACS con il metodo EAP-TLS. Lo switch con 802.1x funge da autenticatore. Il certificato utente viene verificato da ACS e l'autorizzazione criterio applica criteri basati sul nome comune (CN) del certificato. Inoltre, il servizio ACS recupera il certificato utente da AD ed esegue un confronto binario con il certificato fornito dal richiedente.

Configurazione degli switch

Lo switch ha una configurazione di base. Per impostazione predefinita, la porta è nella VLAN 666 in quarantena. Tale VLAN ha un accesso limitato. Dopo aver autorizzato l'utente, la porta VLAN viene riconfigurata.

```
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
```

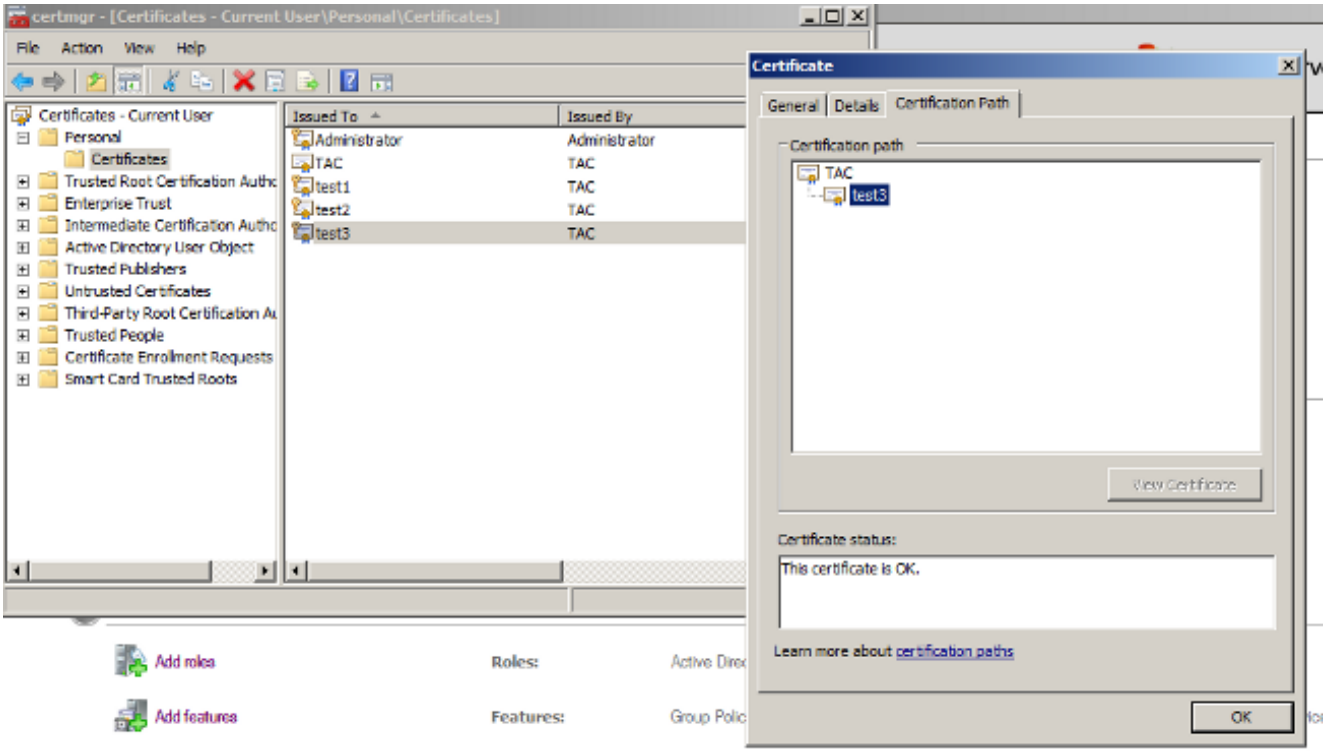
Preparazione certificato

Per EAP-TLS, è necessario un certificato sia per il richiedente che per il server di autenticazione. Questo esempio si basa sui certificati generati con OpenSSL. È possibile utilizzare Microsoft Certificate Authority (CA) per semplificare la distribuzione nelle reti aziendali.

1. Per generare la CA, immettere i seguenti comandi:
   ```
   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
   ```
   Il certificato CA viene conservato nel file ca.crt e la chiave privata (e non protetta) nel file ca.key.
2. Generare tre certificati utente e un certificato per ACS, tutti firmati da tale CA: CN=prova1CN=prova2CN=prova3CN=acs54Lo script per generare un singolo certificato firmato dalla CA di Cisco è:
   ```
   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
   ```
   La chiave privata si trova nel file server.key e il certificato nel file server.crt. La versione di pkcs12 si trova nel file server.pfx.
3. Fare doppio clic su ogni certificato (file con estensione pfx) per importarlo nel controller di dominio. Nel controller di dominio tutti e tre i certificati devono essere attendibili.

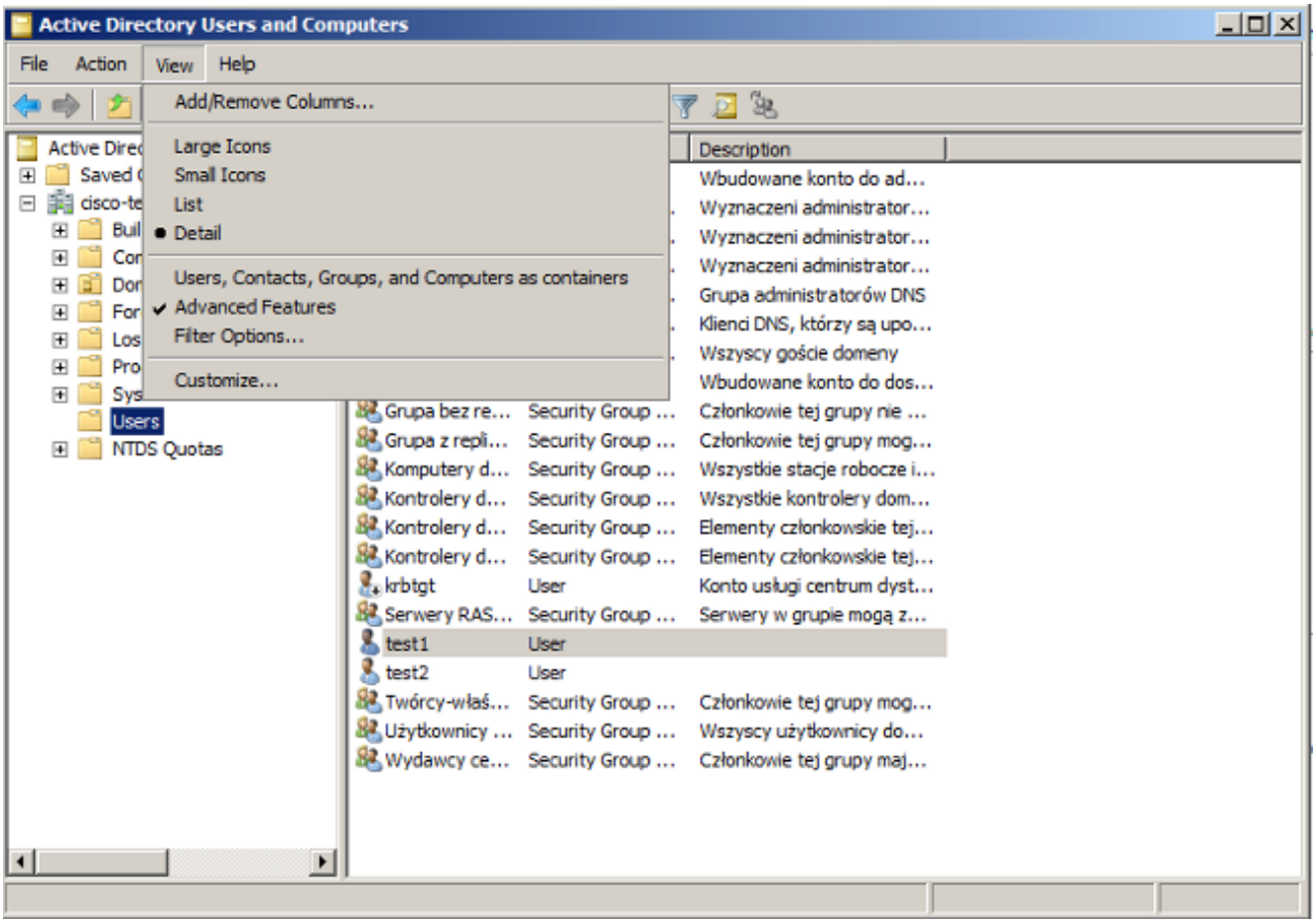


Lo stesso processo può essere seguito in Windows 7 (supplicant) o utilizzare Active Directory per eseguire il push dei certificati utente.

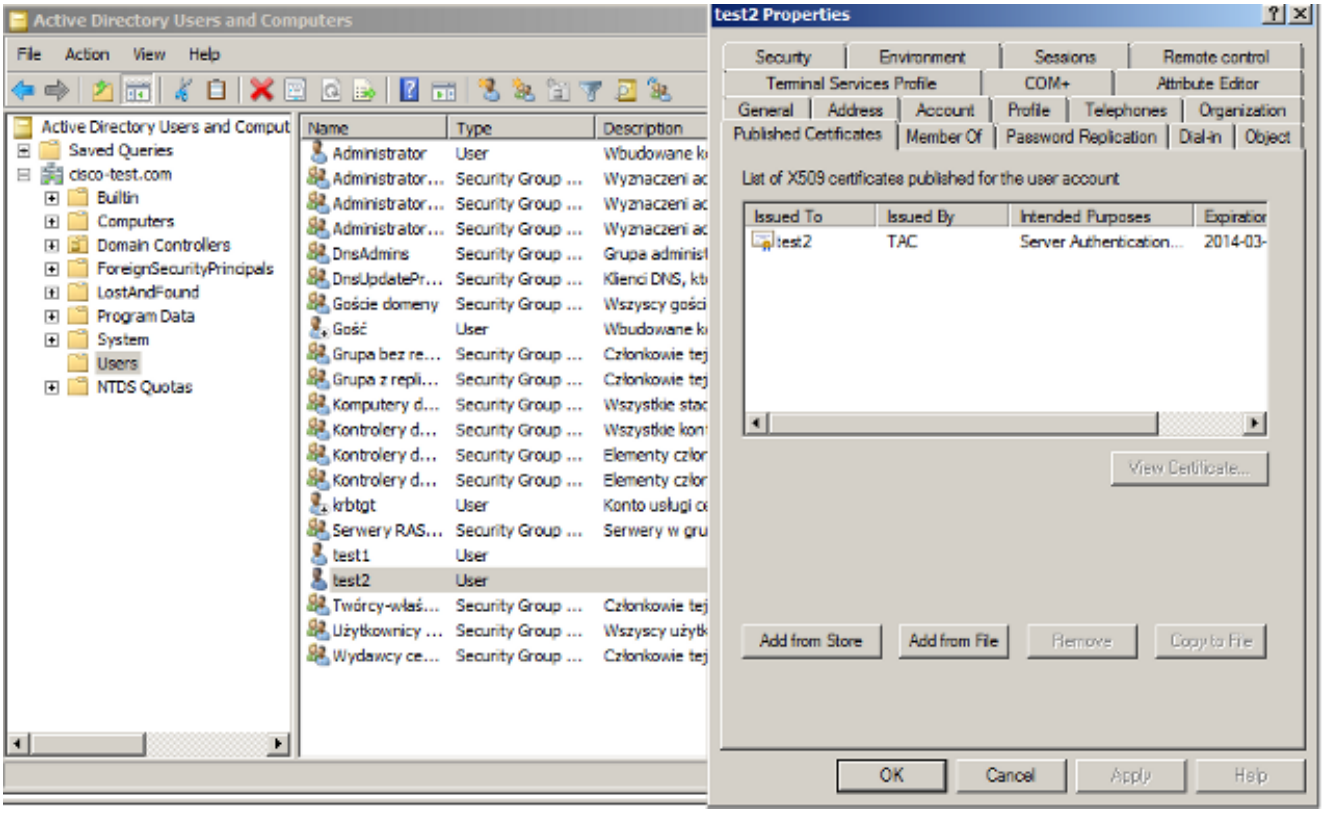
Configurazione controller di dominio

Ènecessario mappare il certificato specifico all'utente specifico in AD.

1. Da Utenti e computer di Active Directory passare alla cartella **Utenti**.
2. Scegliere **Caratteristiche avanzate** dal menu Visualizza.



3. Aggiungi questi utenti: test1test2test3**Nota:** La password non è importante.
4. Nella finestra Proprietà scegliere la scheda **Certificati pubblicati**. Scegliere il certificato specifico per il test. Ad esempio, per test1 l'utente CN è test1.**Nota:** Non utilizzare Mapping nomi (fare clic con il pulsante destro del mouse sul nome utente). Viene utilizzato per diversi servizi.



In questa fase il certificato è associato a un utente specifico in Active Directory. È possibile verificare questa condizione tramite ldapsearch:

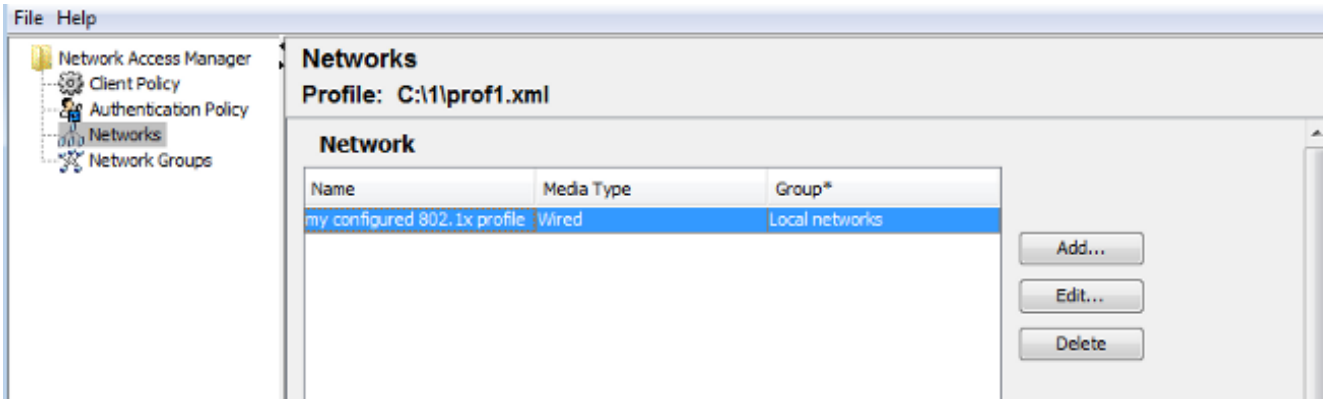
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

Di seguito sono riportati alcuni risultati di esempio per test2.

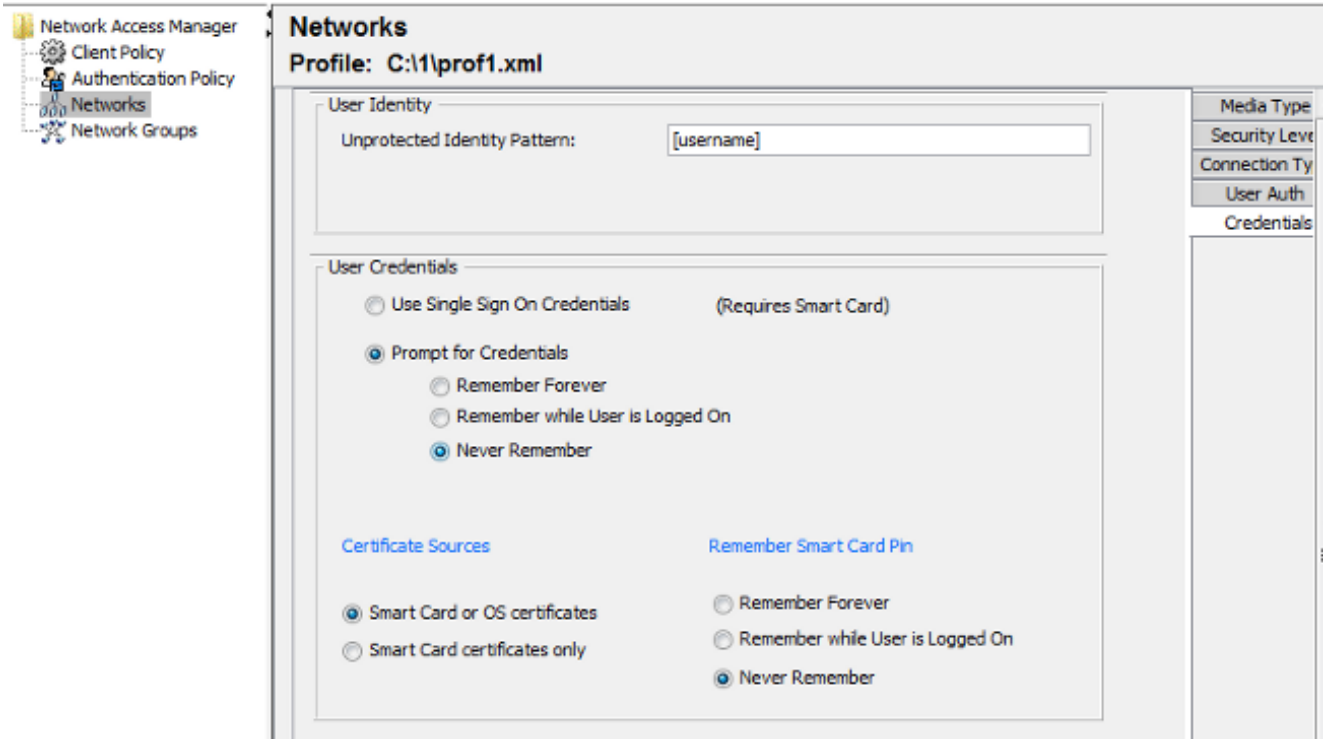
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

Configurazione supplicant

1. Installare questo editor di profili, anyconnect-profileeditor-win-3.1.00495-k9.exe.
2. Aprire l'Editor profili di Network Access Manager e configurare il profilo specifico.
3. Creare una rete cablata specifica.



In questa fase è molto importante offrire all'utente la possibilità di utilizzare il certificato per ogni autenticazione. Non memorizzare nella cache tale scelta. Utilizzare inoltre 'username' come ID non protetto. È importante ricordare che non si tratta dello stesso ID utilizzato da ACS per eseguire una query su AD per il certificato. L'ID verrà configurato in ACS.



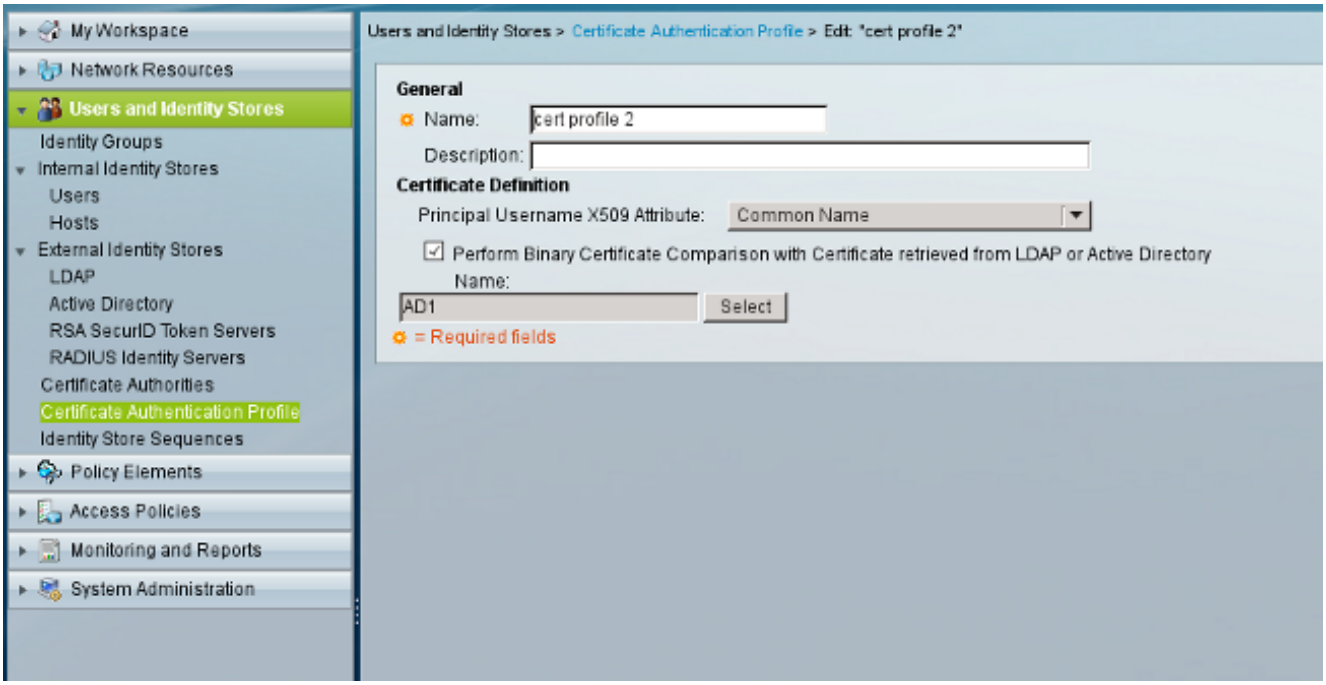
4. Salvare il file con estensione xml come c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Riavviare il servizio Cisco AnyConnect NAM.

Nell'esempio è illustrata una distribuzione manuale del profilo. AD potrebbe essere utilizzato per distribuire il file per tutti gli utenti. Inoltre, se integrata con le VPN, l'ASA può essere utilizzata per effettuare il provisioning del profilo.

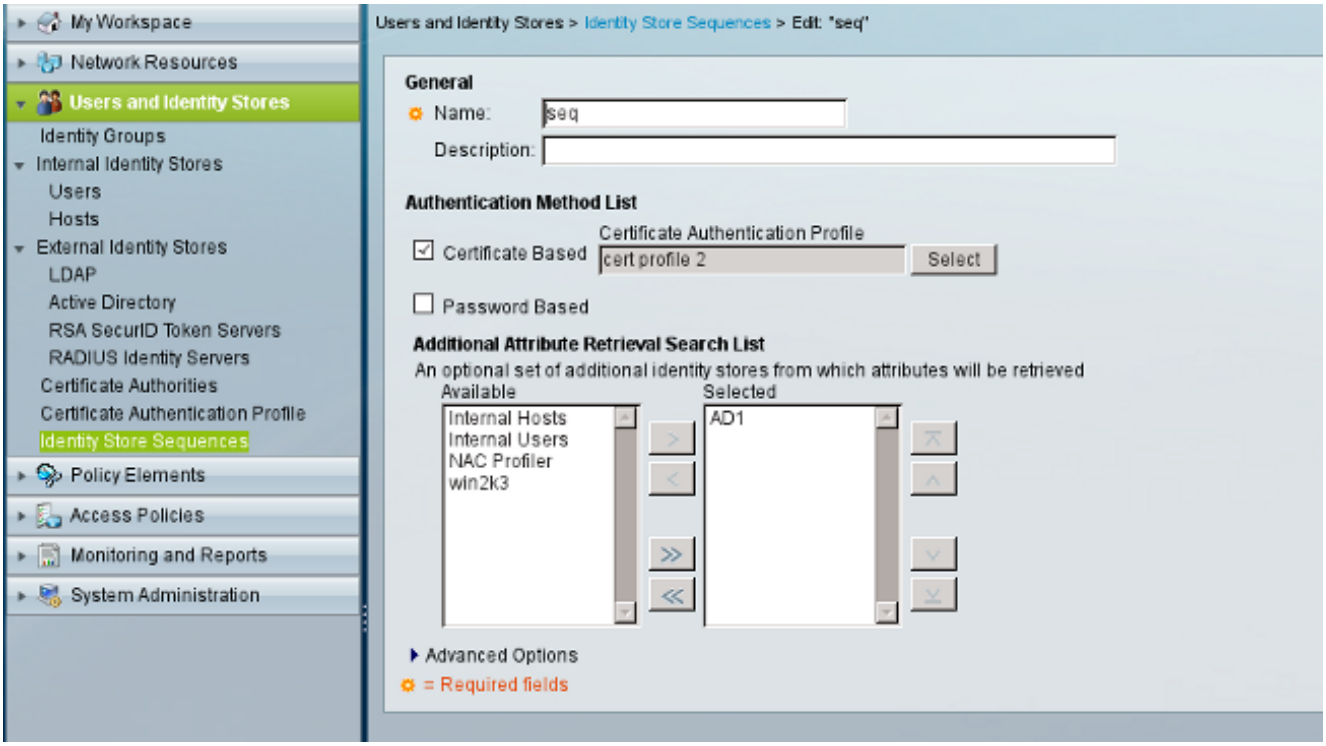
Configurazione ACS

1. Aggiungere il computer al dominio Active Directory.

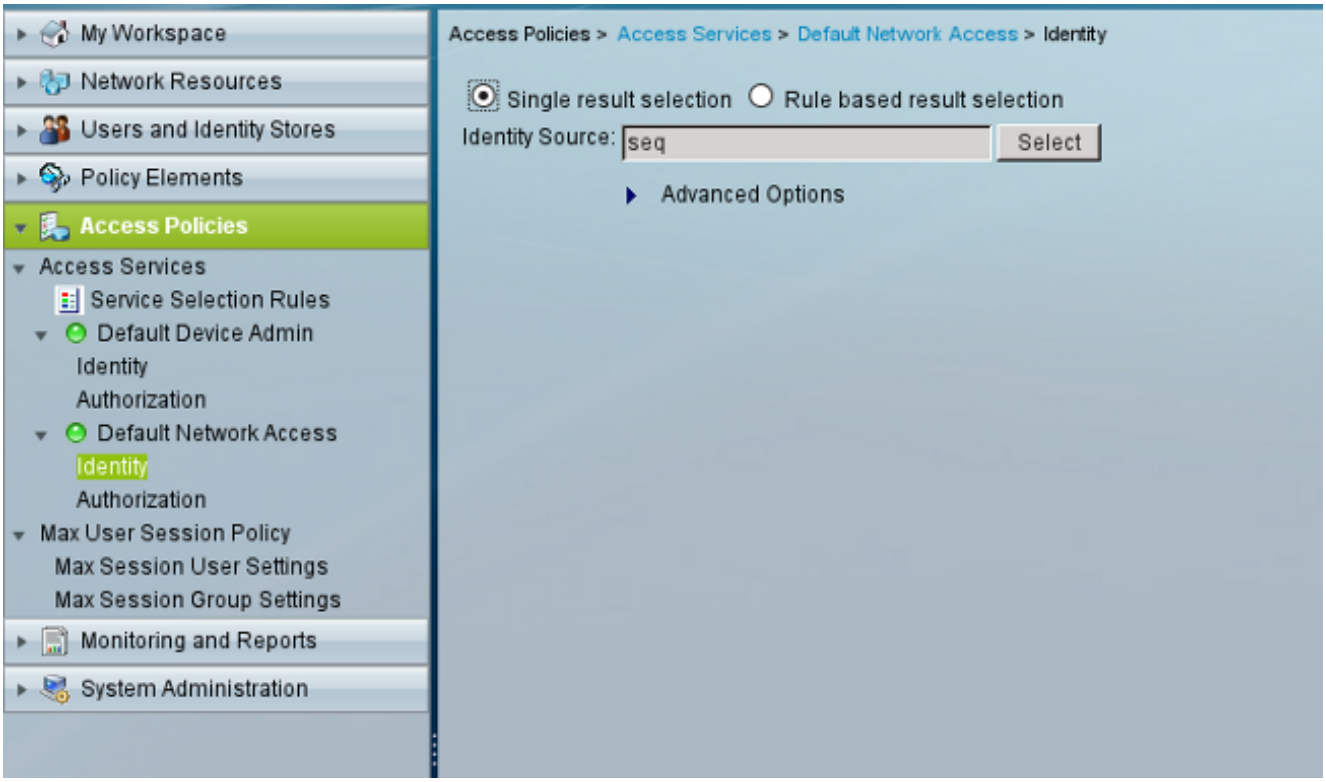
ACS confronta i nomi utente AD con l'utilizzo del campo CN del certificato ricevuto dal richiedente (in questo caso test1, test2 o test3). È inoltre abilitato il confronto binario. In questo modo ACS ottiene il certificato utente da AD e lo confronta con lo stesso certificato ricevuto dal richiedente. Se non corrisponde, l'autenticazione non riesce.



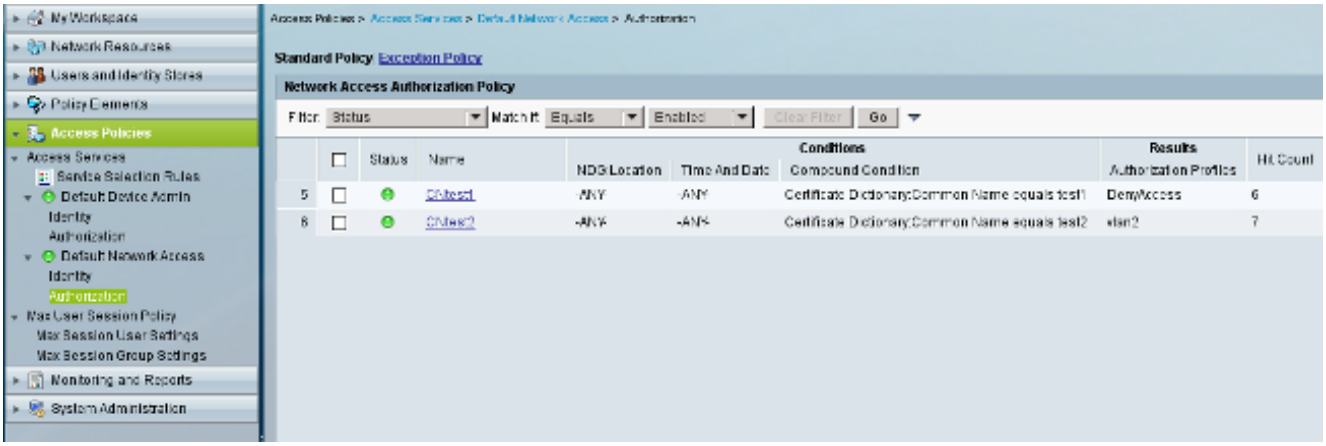
2. Configurare le sequenze dell'archivio identità, che utilizza AD per l'autenticazione basata su certificati insieme al profilo del certificato.



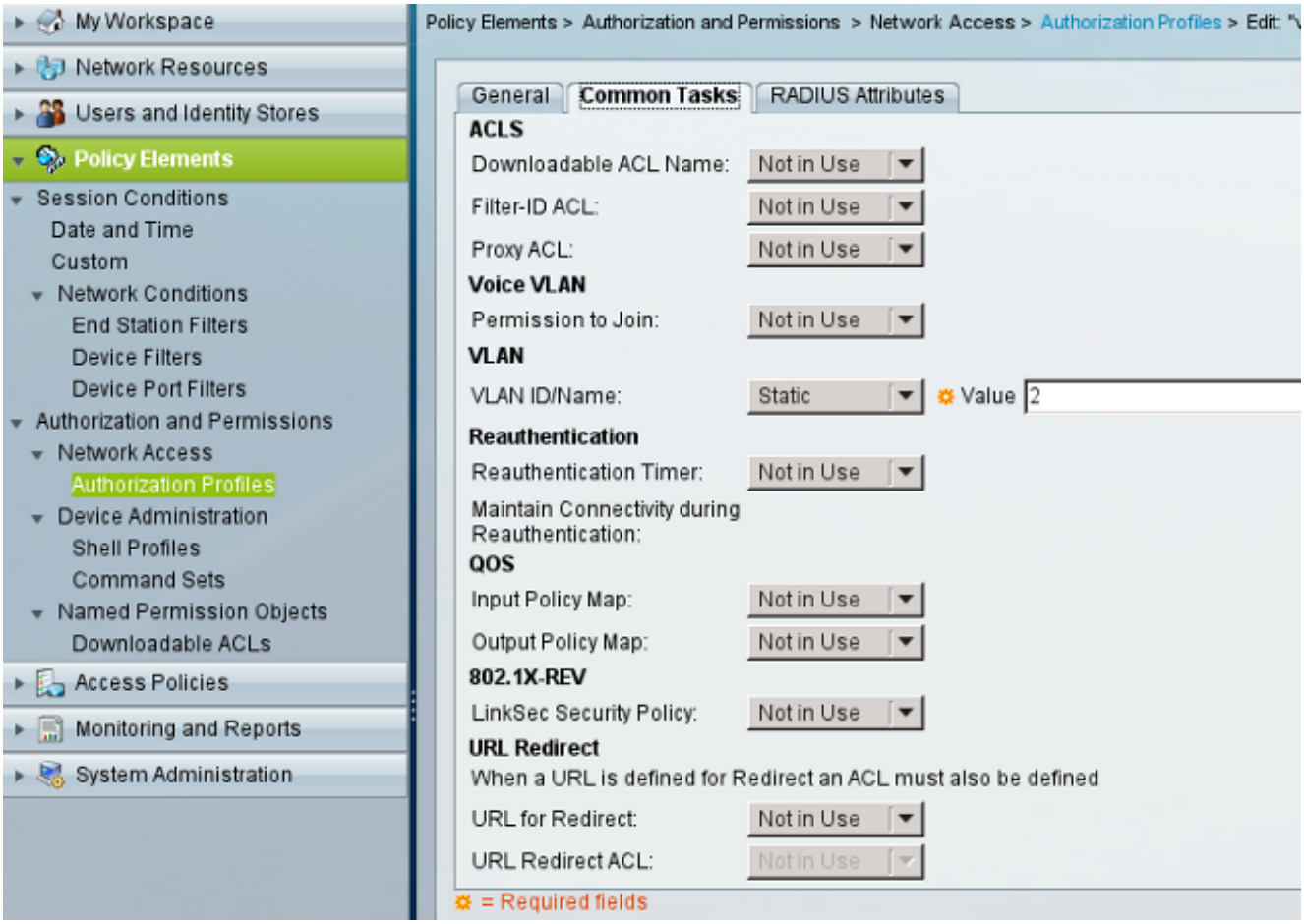
Utilizzato come origine identità nei criteri di identità RADIUS.



3. Configurare due criteri di autorizzazione. Il primo criterio viene utilizzato per test1 e nega l'accesso all'utente. Il secondo criterio viene utilizzato per il test 2 e consente l'accesso con il profilo
VLAN2.

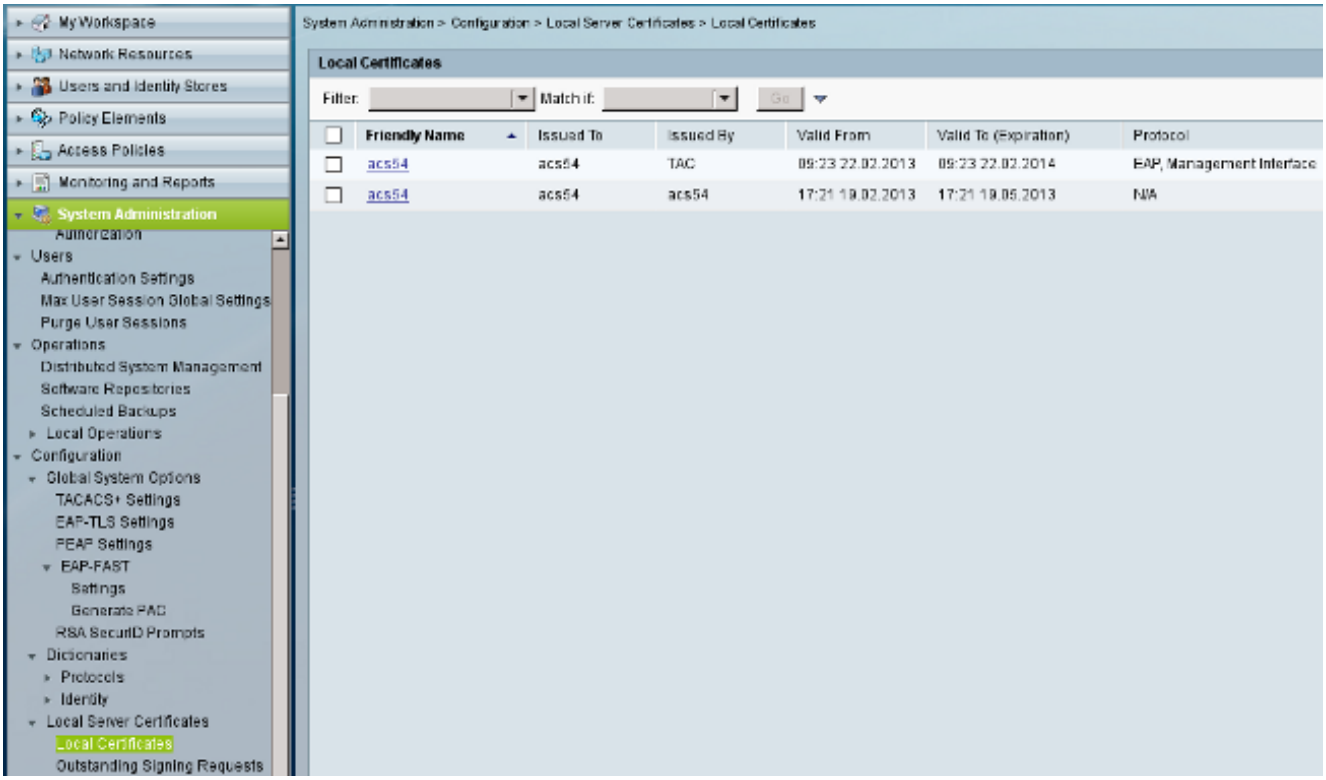


VLAN2 è il profilo di autorizzazione che restituisce gli attributi RADIUS che associano l'utente alla VLAN2 sullo
switch.



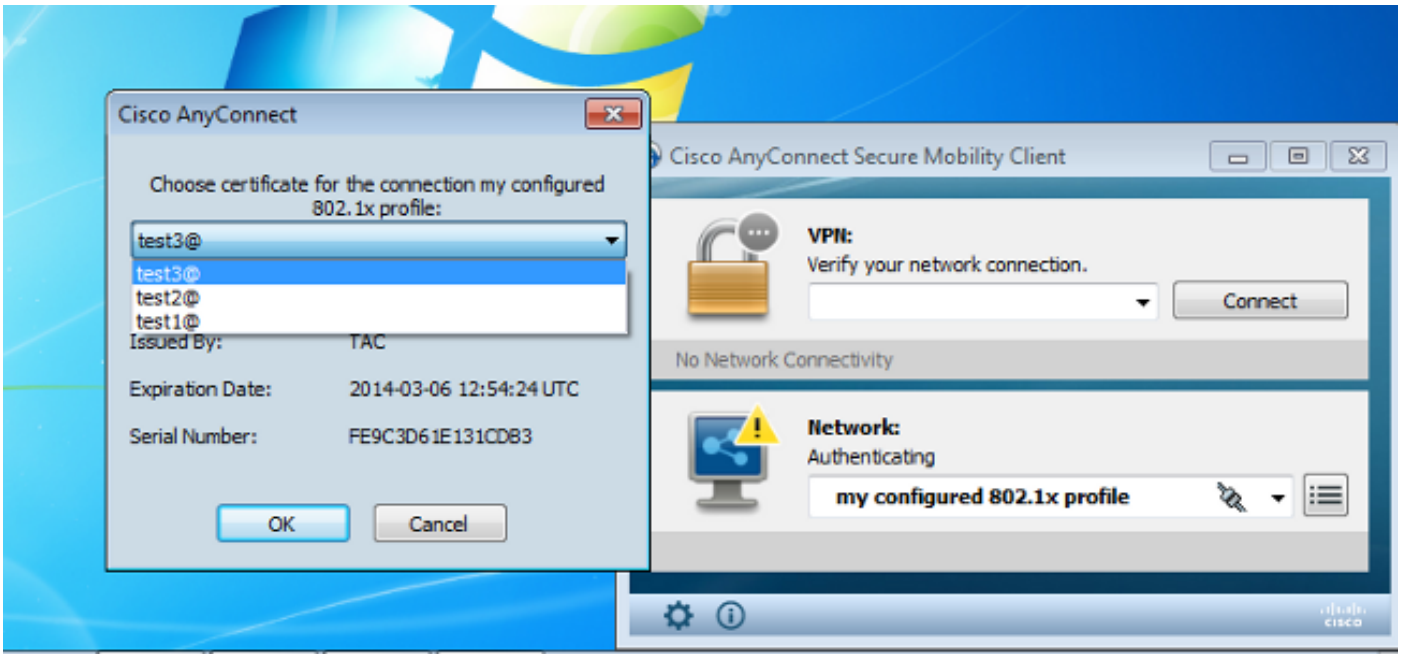
4. Installare il certificato CA su ACS.

5. Generare e installare il certificato (per l'utilizzo del protocollo Extensible Authentication Protocol) firmato dalla CA di Cisco per ACS.



Verifica

Èbuona norma disabilitare il servizio 802.1x nativo sul supplicant Windows 7 poiché viene utilizzato AnyConnect NAM. Con il profilo configurato, il client può selezionare un certificato specifico.



Quando si utilizza il certificato test2, lo switch riceve una risposta di esito positivo insieme agli attributi RADIUS.

```
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
```

Notare che la VLAN 2 è stata assegnata. È possibile aggiungere altri attributi RADIUS a tale profilo di autorizzazione in ACS (ad esempio, Advanced Access Control List o timer di riautorizzazione).

I log su ACS sono i seguenti:

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

Risoluzione dei problemi

Impostazioni di ora non valide in ACS

Errore possibile - errore interno 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.

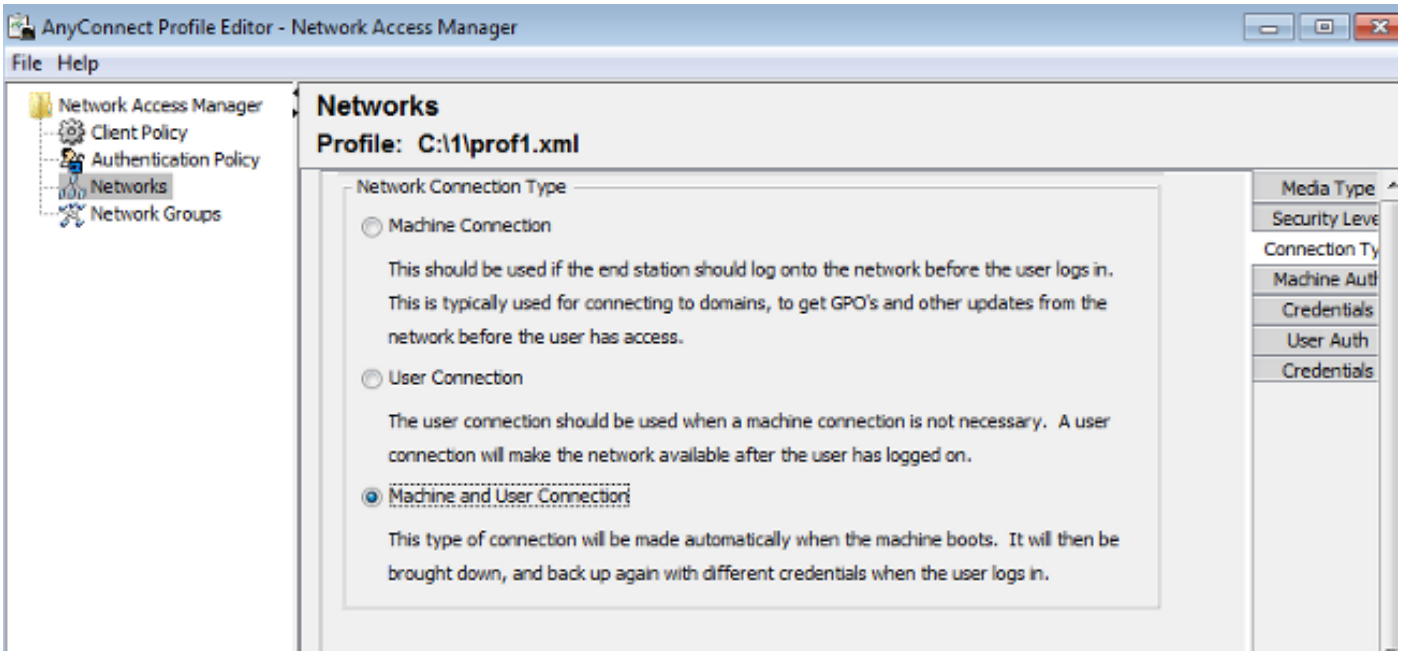
Nessun certificato configurato e associato al controller di dominio Active Directory

Errore possibile - impossibile recuperare il certificato utente da 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

Personalizzazione del profilo NAM

Nelle reti aziendali, si consiglia di eseguire l'autenticazione con l'utilizzo di certificati sia del computer che dell'utente. In questo scenario, si consiglia di utilizzare la modalità 802.1x aperta sullo switch con VLAN limitata. Al riavvio del computer per 802.1x, la prima sessione di autenticazione viene avviata e autenticata con il certificato del computer AD. Quindi, dopo che l'utente ha fornito le credenziali e ha effettuato l'accesso al dominio, viene avviata la seconda sessione di autenticazione con il certificato utente. L'utente utilizza la VLAN corretta (attendibile) con accesso completo alla rete. Si integra perfettamente con Identity Services Engine (ISE).



Èquindi possibile configurare autenticazioni separate dalle schede Autenticazione computer e

Autenticazione utente.

Se la modalità 802.1x aperta non è accettabile sullo switch, è possibile utilizzare la modalità 802.1x prima che la funzionalità di accesso sia configurata nella policy del client.

Informazioni correlate

- Guida per l'utente di Cisco Secure Access Control System 5.3
- Guida dell'amministratore di Cisco AnyConnect Secure Mobility Client, versione 3.0
- AnyConnect Secure Mobility Client 3.0: Network Access Manager ed Editor di profili su Windows
- Documentazione e supporto tecnico – Cisco Systems