Configurazione e risoluzione dei problemi di ISE con l'archivio identità LDAPS esterno

Sommario

Introduzione

Questo documento descrive l'integrazione di Cisco Identity Service Engine (ISE) con il server Secure Lightweight Directory Access Protocol (LDAPS) come origine identità esterna. LDAPS consente la crittografia dei dati LDAP (incluse le credenziali utente) in transito quando viene stabilita un'associazione alla directory. LDAPS utilizza la porta TCP 636.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dell'amministrazione ISE
- Conoscenze base di Active Directory/LDAP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 2.6 Patch 7

- Microsoft Windows versione 2012 R2 con Active Directory Lightweight Directory Services installato
- PC con sistema operativo Windows 10 con supplicant nativo e certificato utente installato
- Cisco Switch C3750X con immagine 152-2.E6

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.

Premesse

Con LDAPS sono supportati i seguenti protocolli di autenticazione:

- EAP-GTC (EAP Generic Token Card)
- Protocollo PAP (Password Authentication Protocol)
- EAP-TLS (Transport Layer Security)
- PEAP-TLS (Protected EAP Transport Layer Security)

> **Nota:** EAP-MSCHAPV2 (come metodo interno di PEAP, EAP-FAST o EAP-TTLS), LEAP, CHAP e EAP-MD5 non sono supportati con l'origine identità esterna LDAPS.

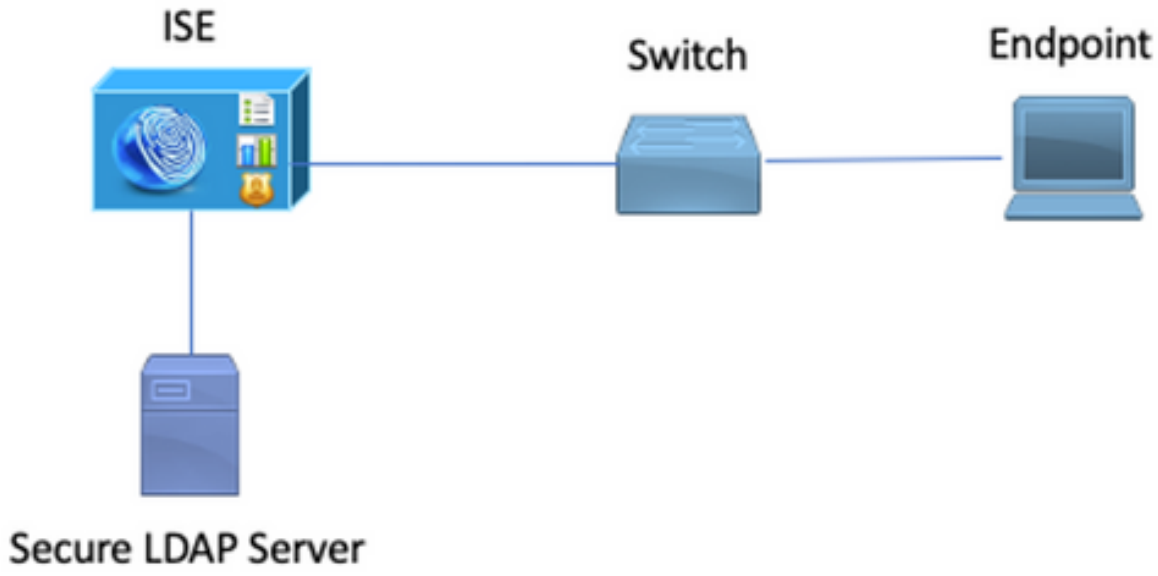
Configurazione

In questa sezione viene descritta la configurazione dei dispositivi di rete e l'integrazione dell'ISE con il server LDAPS Microsoft Active Directory (AD).

Esempio di rete

In questo esempio di configurazione, l'endpoint utilizza una connessione Ethernet con uno switch per connettersi alla LAN (Local Area Network). La porta dello switch connessa è configurata per l'autenticazione 802.1x al fine di autenticare gli utenti con ISE. Ad ISE, LDAPS è configurato come un negozio di identità esterno.

Nell'immagine è illustrata la topologia di rete utilizzata:



Configura LDAPS in Active Directory

Installa certificato di identità nel controller di dominio

Per abilitare LDAPS, installare un certificato nel controller di dominio che soddisfi i seguenti requisiti:

1. Il certificato LDAPS si trova nell'archivio dei certificati personali del controller di dominio.

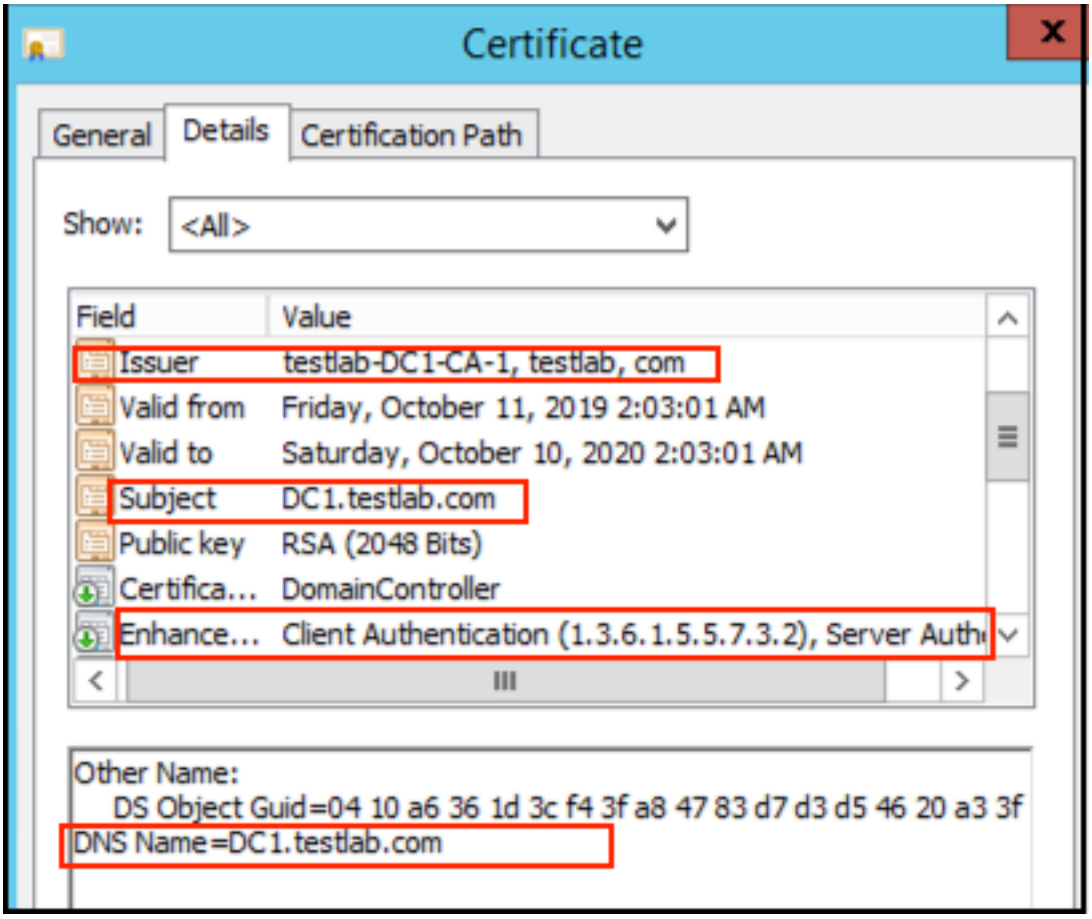
2. Una chiave privata corrispondente al certificato è presente nell'archivio del controller di dominio ed è associata correttamente al certificato.

3. L'estensione Utilizzo chiavi avanzato include l'identificatore di oggetto Autenticazione server (1.3.6.1.5.5.7.3.1) (noto anche come OID).

4. Il nome di dominio completo (FQDN) del controller di dominio (ad esempio, DC1.testlab.com) deve essere presente in uno dei seguenti attributi: Il **nome comune (CN)** nel campo Oggetto e la voce DNS nell'estensione del **nome alternativo soggetto**.

5. Il certificato deve essere rilasciato da un'Autorità di certificazione (CA) considerata attendibile dal controller di dominio e dai client LDAPS. Per una comunicazione protetta attendibile, il client e il server devono considerare attendibili la CA radice e i certificati della CA intermedia che hanno rilasciato i certificati.

6. Per generare la chiave è necessario utilizzare il provider del servizio di crittografia (CSP) Schannel.



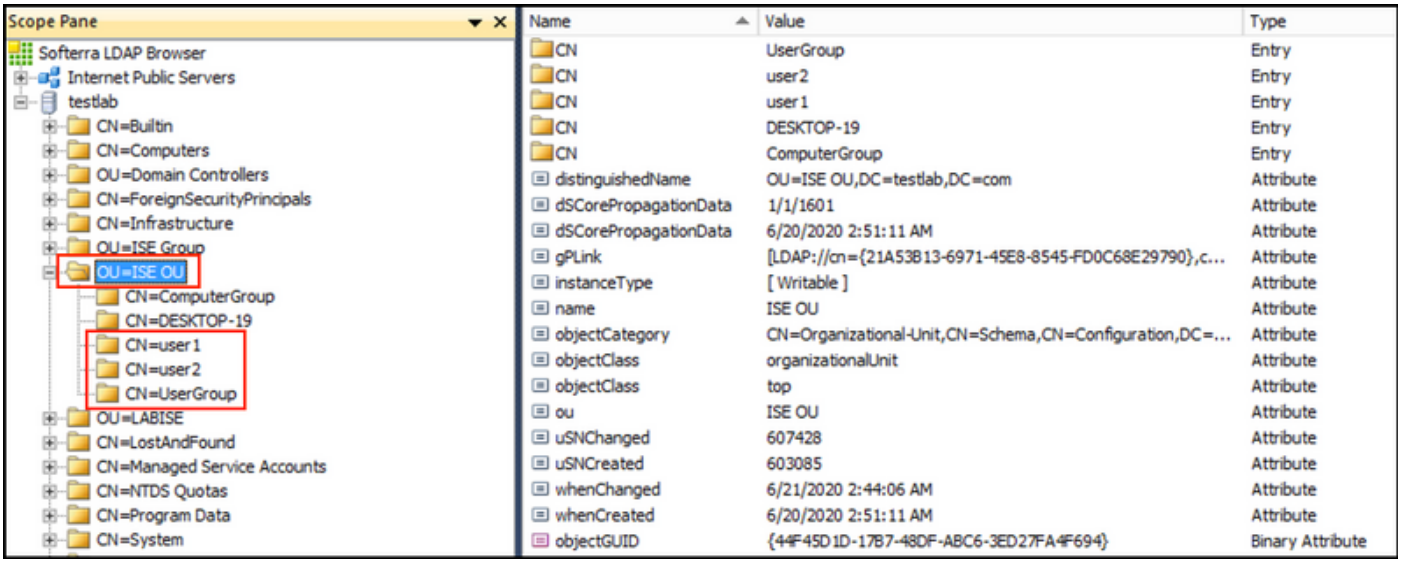
Struttura della directory di Access LDAPS

Per accedere alla directory LDAPS sul server Active Directory, utilizzare un browser LDAP. In questo laboratorio viene utilizzato Softerra LDAP Browser 4.5.

1. Stabilire una connessione al dominio sulla porta TCP 636.

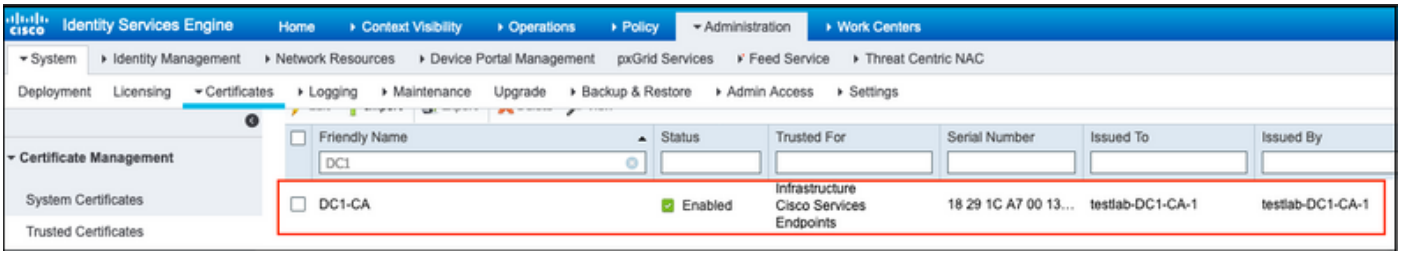
2. Per semplicità, creare un'unità organizzativa (OU) denominata **ISE OU** in Active Directory e dovrebbe avere un gruppo denominato **UserGroup**. Creare due utenti (**user1** e **user2**) e renderli membri del gruppo **UserGroup**.

> **Nota:** LDAP Identity Source su ISE è utilizzato solo per l'autenticazione dell'utente.



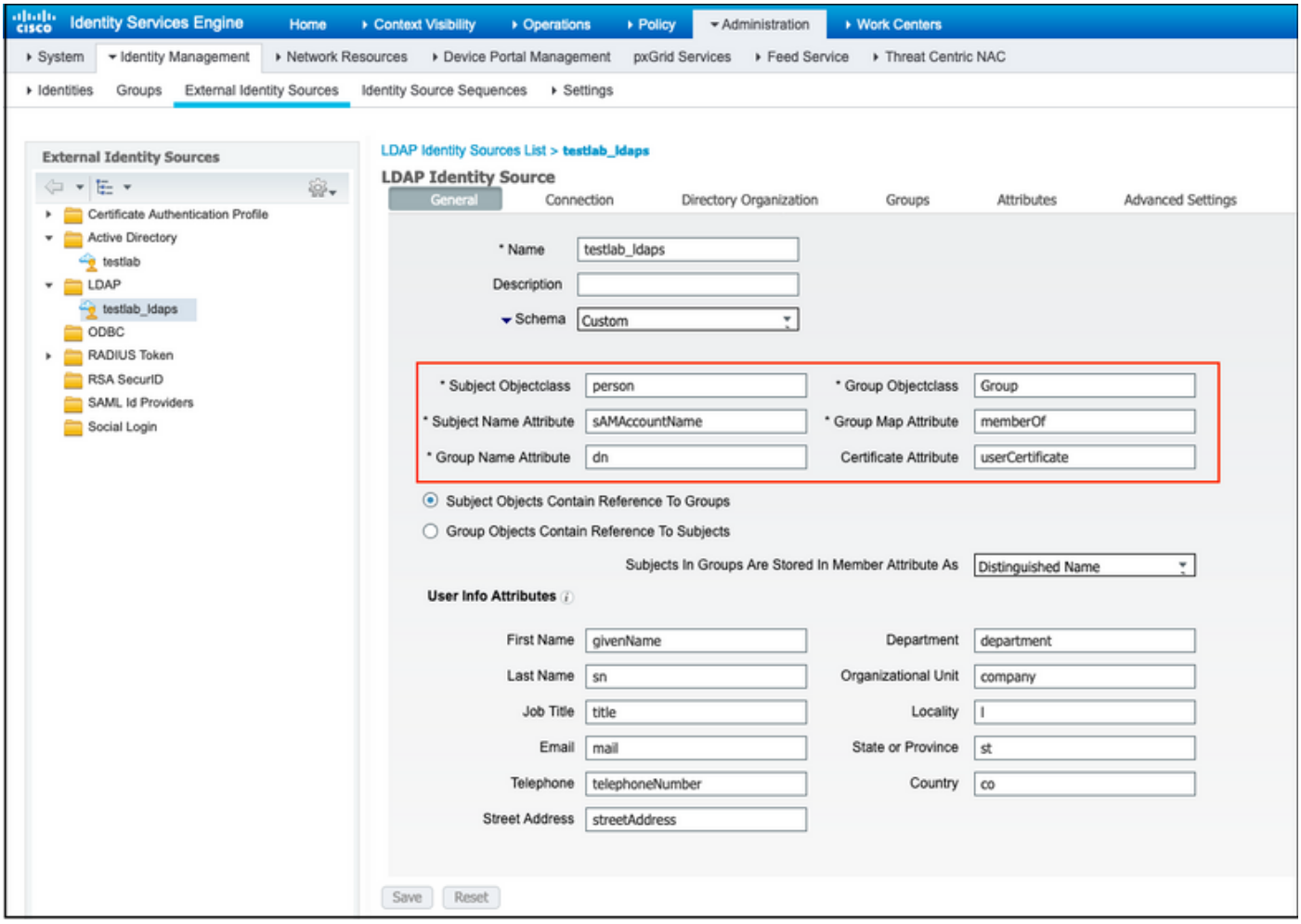
Integrazione di ISE con LDAPS Server

1. Importare il certificato CA radice del server LDAP nel certificato protetto.



2. Convalidare il certificato di amministrazione ISE e verificare che il certificato dell'autorità emittente del certificato di amministrazione ISE sia presente anche nell'archivio certificati attendibile.

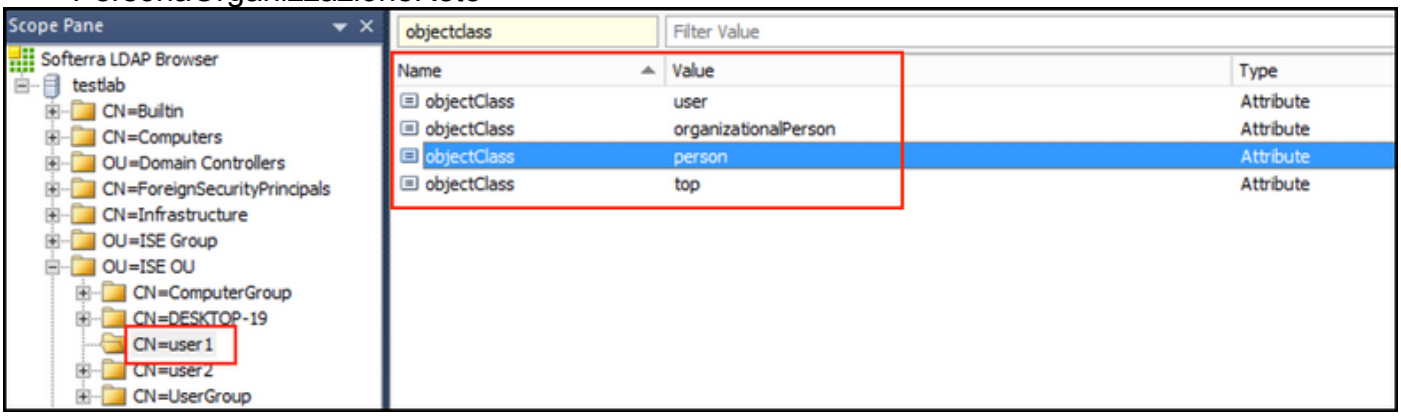
3. Per integrare il server LDAPS, utilizzare i diversi attributi LDAP della directory LDAPS. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Origini identità LDAP > Aggiungi**.



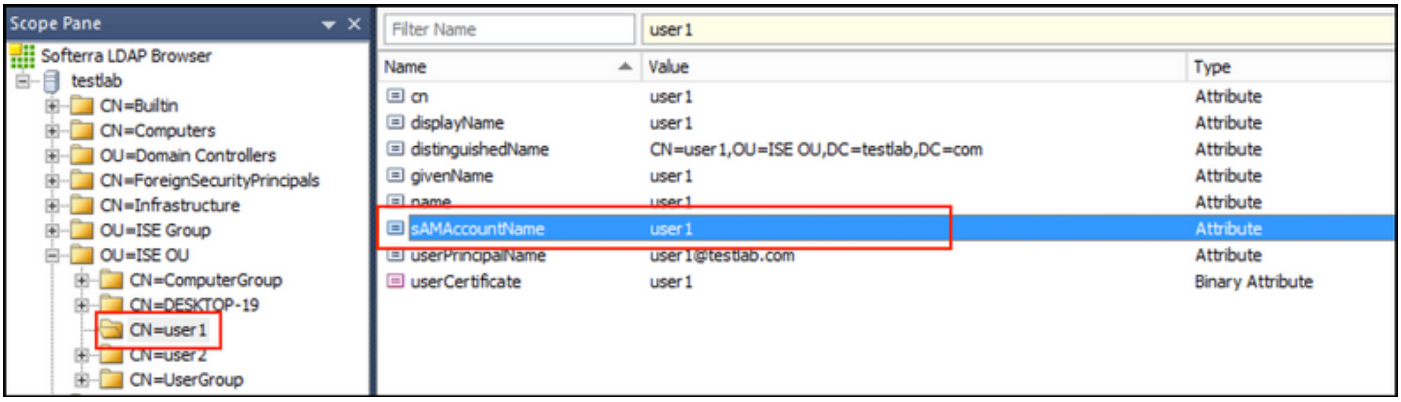
4. Configurare questi attributi dalla **scheda Generale**:

Oggetto Objectclass: Questo campo corrisponde alla classe Object degli account utente. È possibile utilizzare una delle quattro classi seguenti:

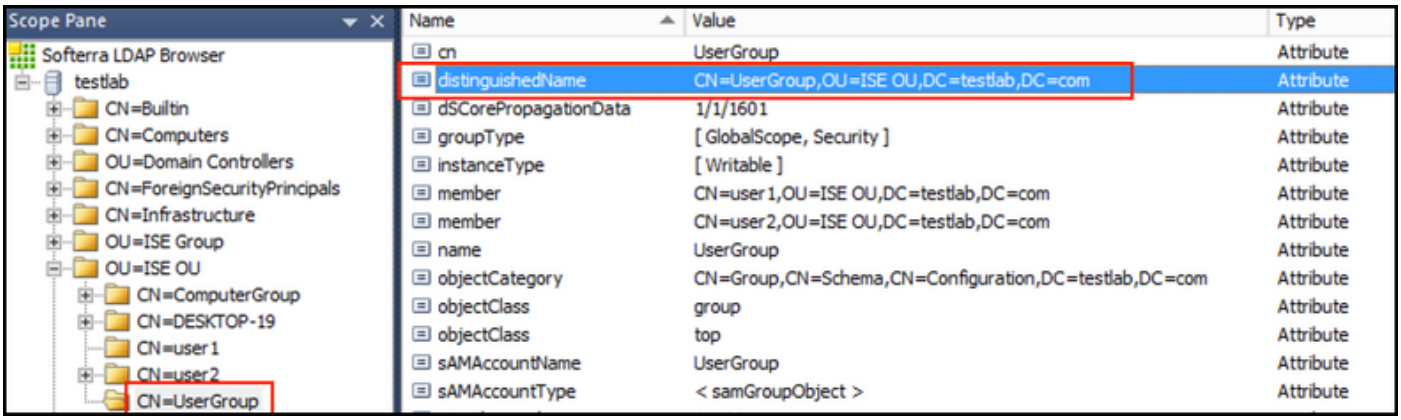
- In alto
- Persona
- PersonaOrganizzazione
- PersonaOrganizzazioneRete



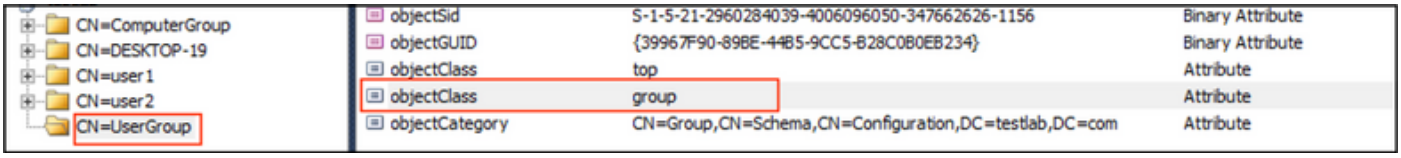
Attributo nome soggetto: questo campo è il nome dell'attributo contenente il nome utente della richiesta. Questo attributo viene recuperato da LDAPS quando ISE richiede un nome utente specifico nel database LDAP (è possibile utilizzare cn, sAMAccountName, ecc.). In questo scenario viene utilizzato il nome utente user1 sull'endpoint.



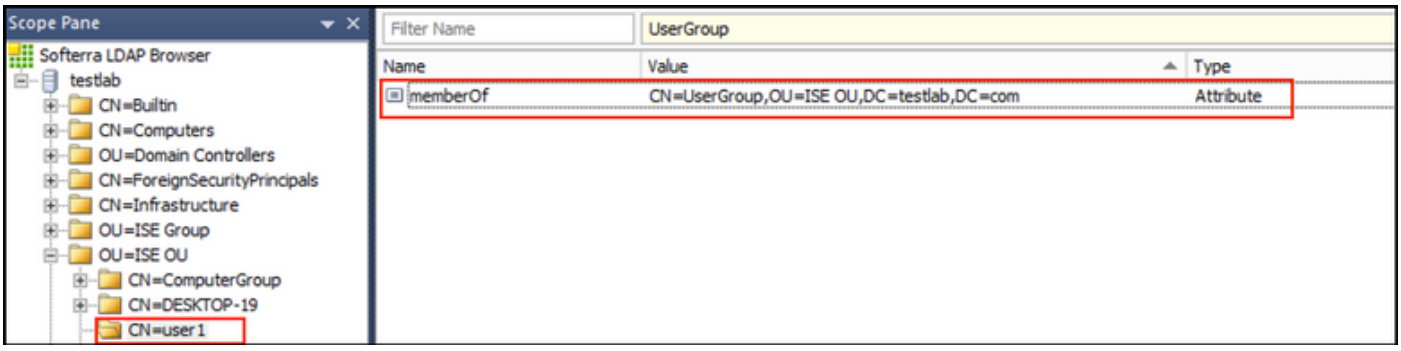
Attributo nome gruppo: Attributo che contiene il nome di un gruppo. I valori dell'**attributo Nome gruppo** nella directory LDAP devono corrispondere ai nomi dei gruppi LDAP nella pagina **Gruppi utenti**



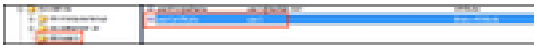
Group Objectclass: questo valore viene utilizzato nelle ricerche per specificare gli oggetti riconosciuti come gruppi.

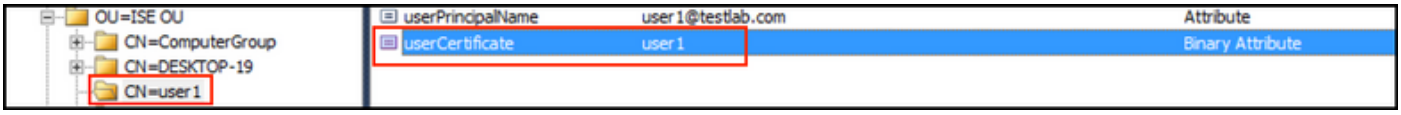


Attributo mappa gruppo: Questo attributo definisce la modalità di mapping degli utenti ai gruppi.

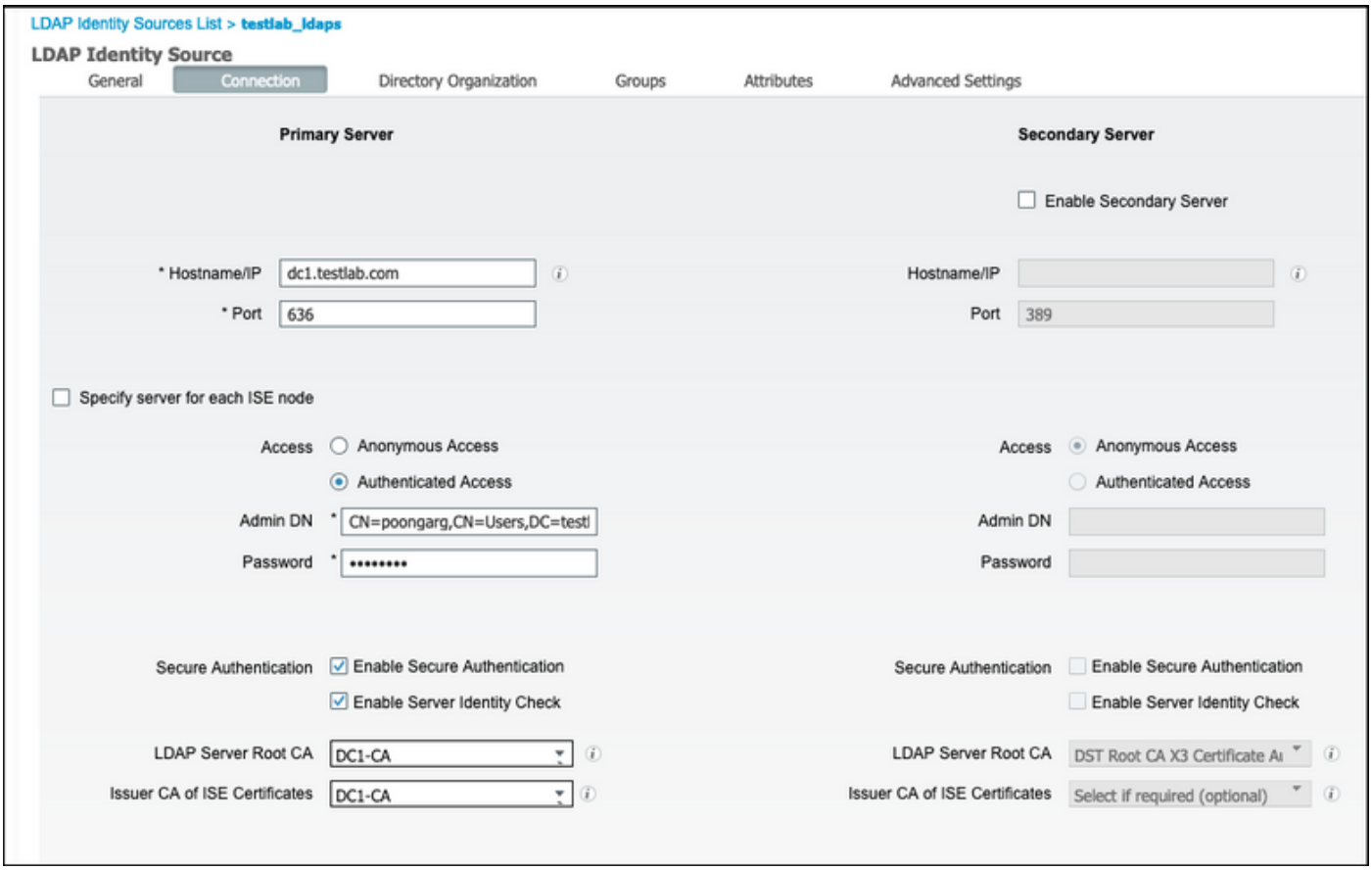


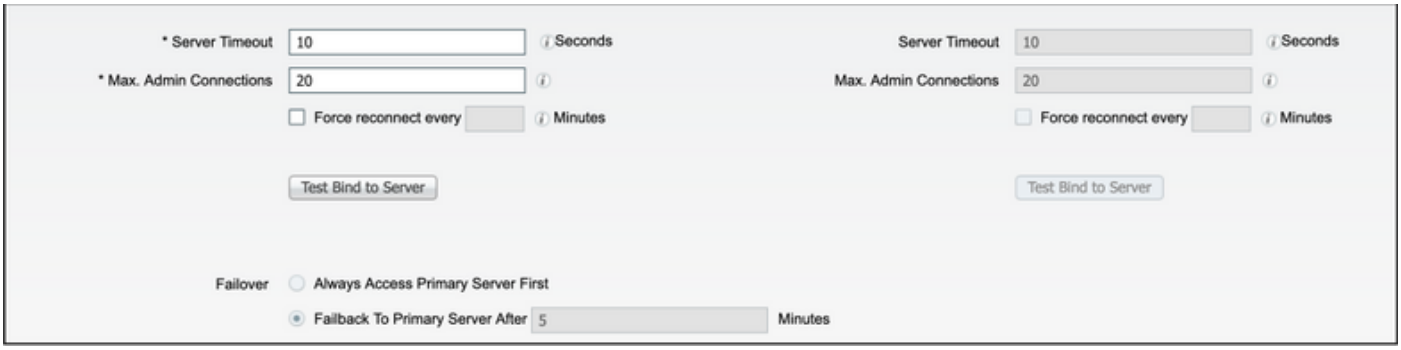
Attributo certificato: Immettere l'attributo che contiene le definizioni del certificato. Queste definizioni possono essere utilizzate facoltativamente per convalidare i certificati presentati dai client quando sono definiti come parte di un profilo di autenticazione dei certificati. In questi casi, viene eseguito un confronto binario tra il certificato client e il certificato recuperato dall'origine dell'identità LDAP.





5. Per configurare la connessione LDAPS, passare alla scheda **Connessione**:





6. Eseguire **dsquery** sul controller di dominio per ottenere il DN del nome utente da utilizzare per effettuare una connessione al server LDAP:

PS **C:\Users\Administrator> dsquery user -name poongarg**
"CN=poongarg,CN=Users,DC=testlab,DC=com"

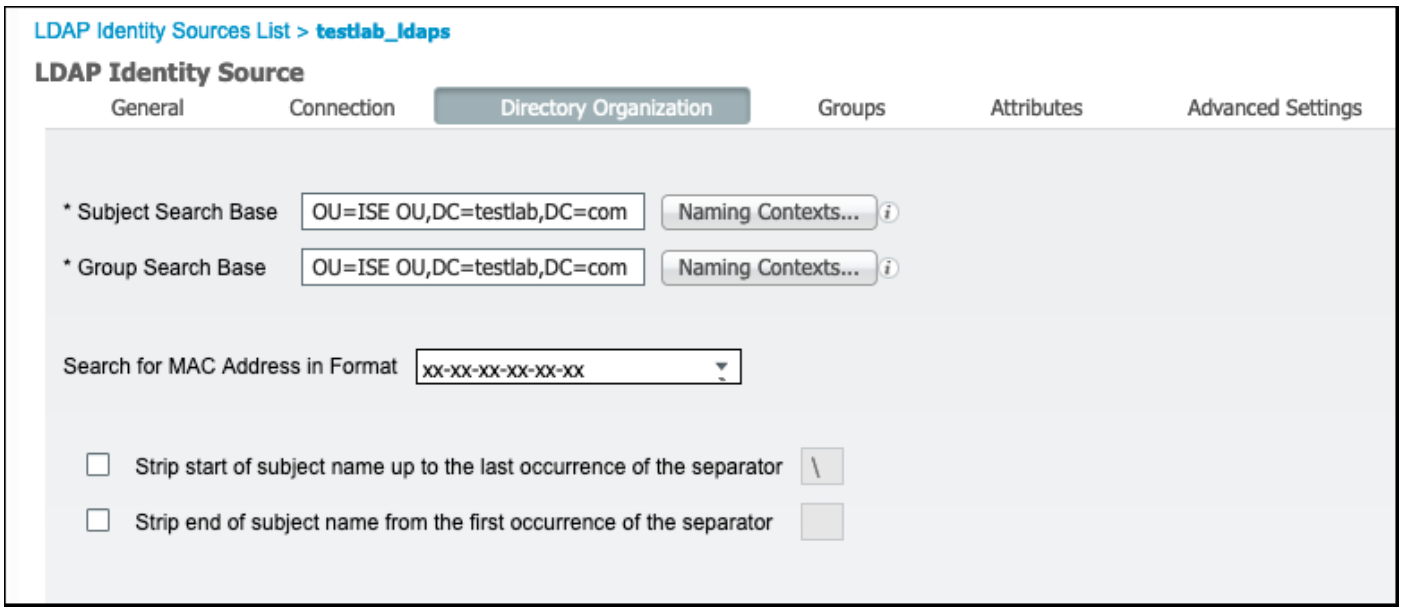
Passaggio 1. SImpostare l'indirizzo IP o il nome host corretto del server LDAP, definire la porta LDAPS (TCP 636) e il DN di amministrazione per stabilire una connessione con il server LDAP tramite SSL.

Passaggio 2. Abilitare l'opzione Autenticazione sicura e Controllo identità server.

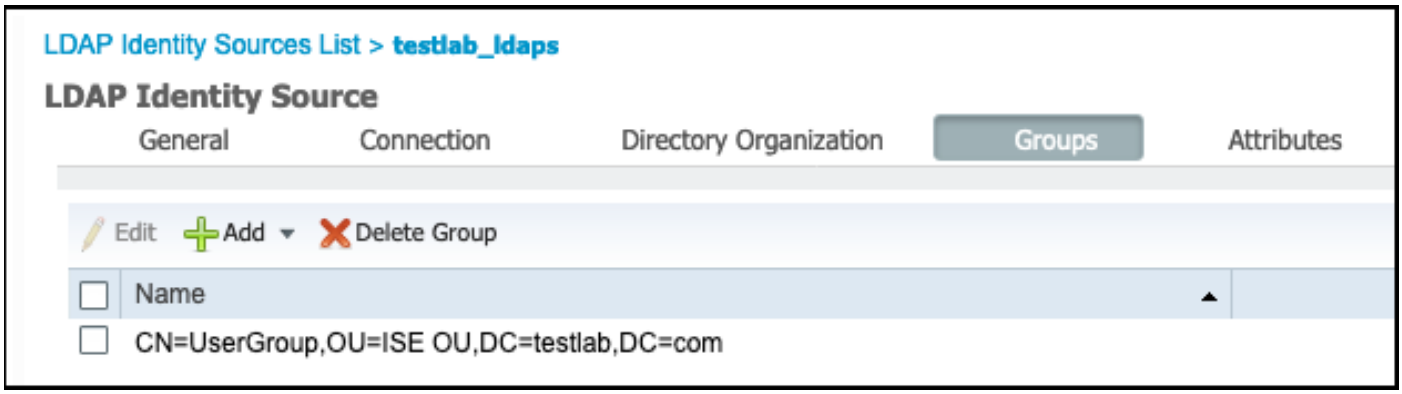
Passaggio 3. Dal menu a discesa, selezionare il certificato **CA radice del server LDAP** e il certificato **ISE admin** CA **emittente** (abbiamo utilizzato l'autorità di certificazione, installata sullo stesso server LDAP anche per rilasciare il certificato ISE admin),

Passaggio 4. Selezionare il **test di associazione al server.** A questo punto, gli argomenti o i gruppi non vengono recuperati perché le basi di ricerca non sono ancora configurate.

7. In **Organizzazione directory** scheda, configurare la Base di ricerca soggetto/gruppo. È il **punto** di **join** per ISE al LDAP. Ora è possibile recuperare solo gli oggetti e i gruppi figli del punto di giunzione. In questo scenario, l'oggetto e il gruppo vengono recuperati dall'**unità organizzativa OU=ISE**



8. In **Gruppi**, fare clic su **Aggiungi** per importare i gruppi dal server LDAP sull'ISE e recuperare i gruppi, come mostrato in questa immagine.



Configurazione dello switch

Configurare lo switch per l'autenticazione 802.1x. Il PC Windows è collegato a switchport Gig2/0/47

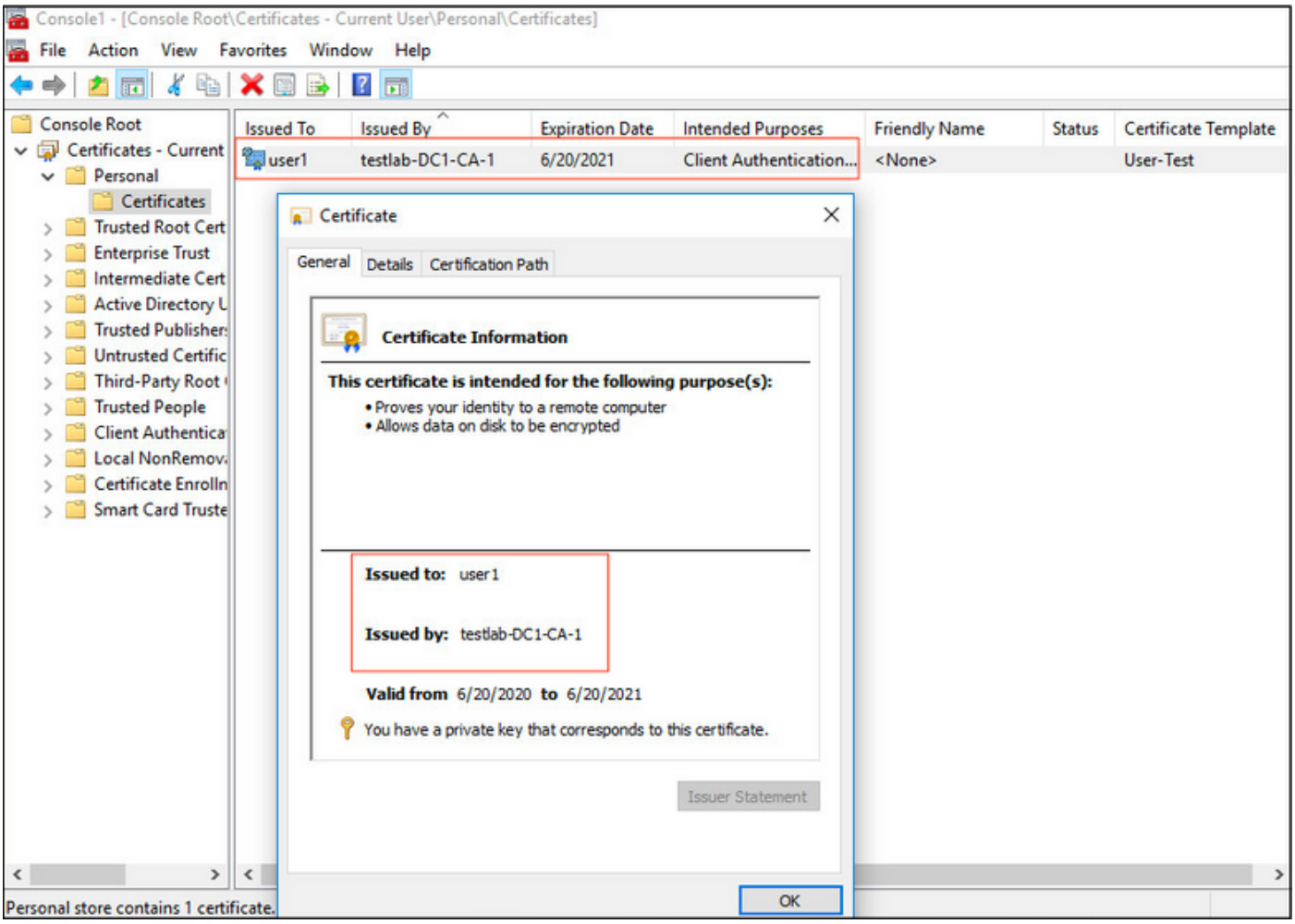
```
aaa new-model radius server ISE address ipv4 x.x.x.x auth-port 1812 acct-port 1813 key xxxxxx
aaa group server radius ISE_SERVERS server name ISE ! aaa server radius dynamic-author client
x.x.x.x server-key xxxxxx ! aaa authentication dot1x default group ISE_SERVERS local aaa
authorization network default group ISE_SERVERS aaa accounting dot1x default start-stop group
```

```
ISE_SERVERS ! dot1x system-auth-control ip device tracking ! radius-server attribute 6 on-for-login-auth radius-server attribute 8 include-in-access-req ! ! interface GigabitEthernet2/0/47 switchport access vlan xx switchport mode access authentication port-control auto dot1x pae authenticator
```

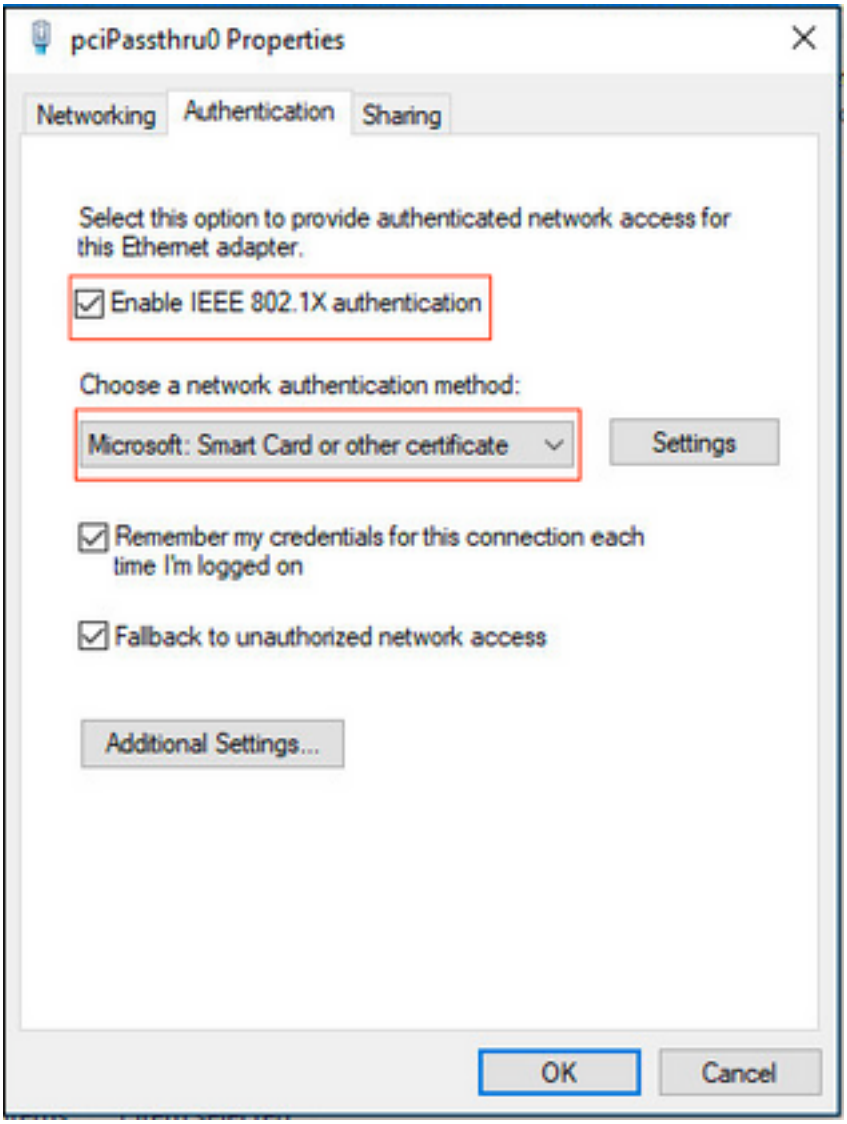
Configurazione dell'endpoint

Viene utilizzato Windows Native Supplicant e viene utilizzato uno dei protocolli EAP supportati da LDAP, EAP-TLS per l'autenticazione e l'autorizzazione degli utenti.

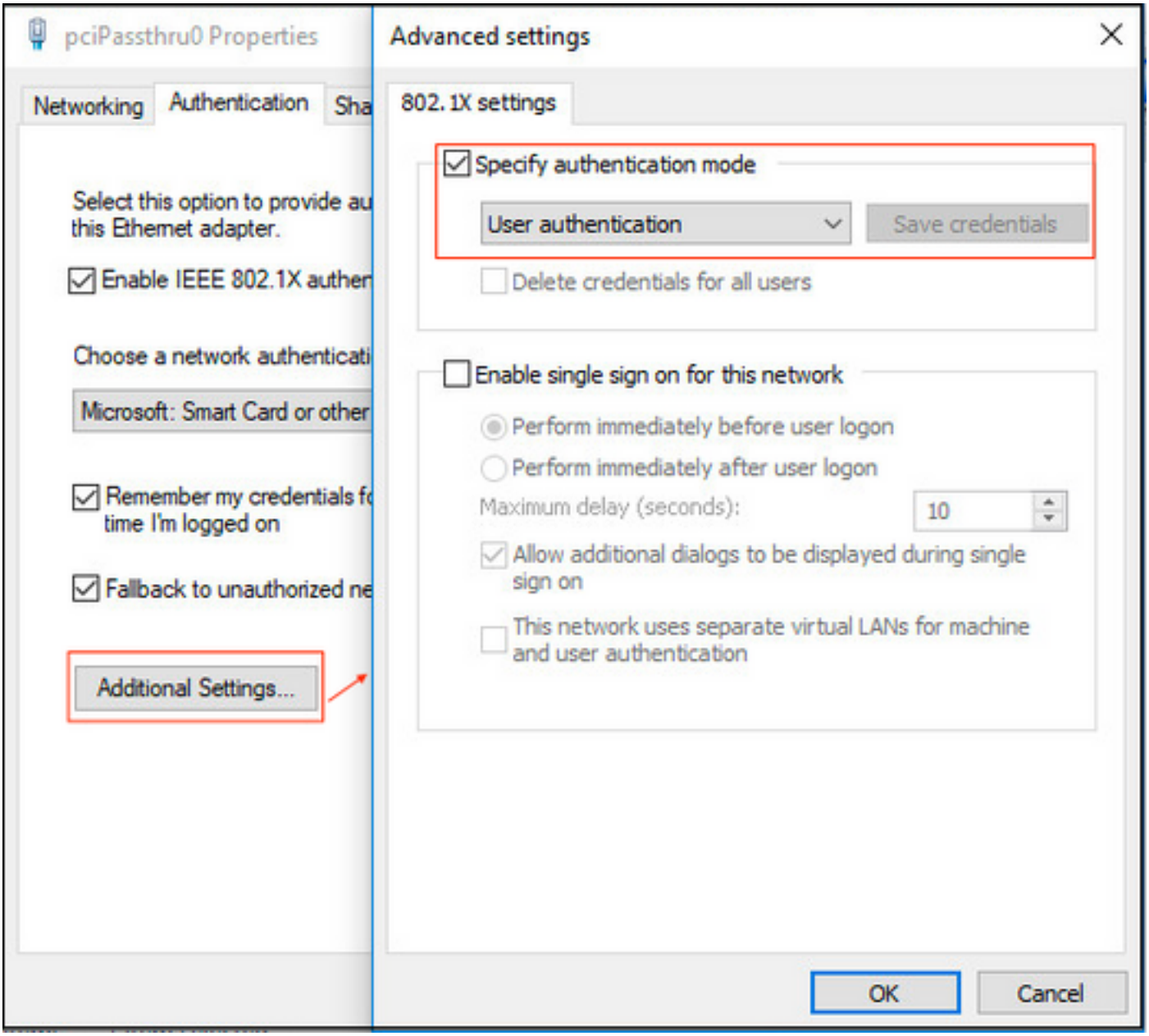
1. Verificare che il PC disponga del certificato utente (per l'utente 1) e abbia lo scopo designato come Autenticazione client e che la catena di certificati dell'autorità di certificazione principale attendibile sia presente nel PC.



2. Abilitare l'autenticazione Dot1x e selezionare il metodo di autenticazione come **Microsoft:Smart Card o altro certificato** per l'autenticazione EAP-TLS.

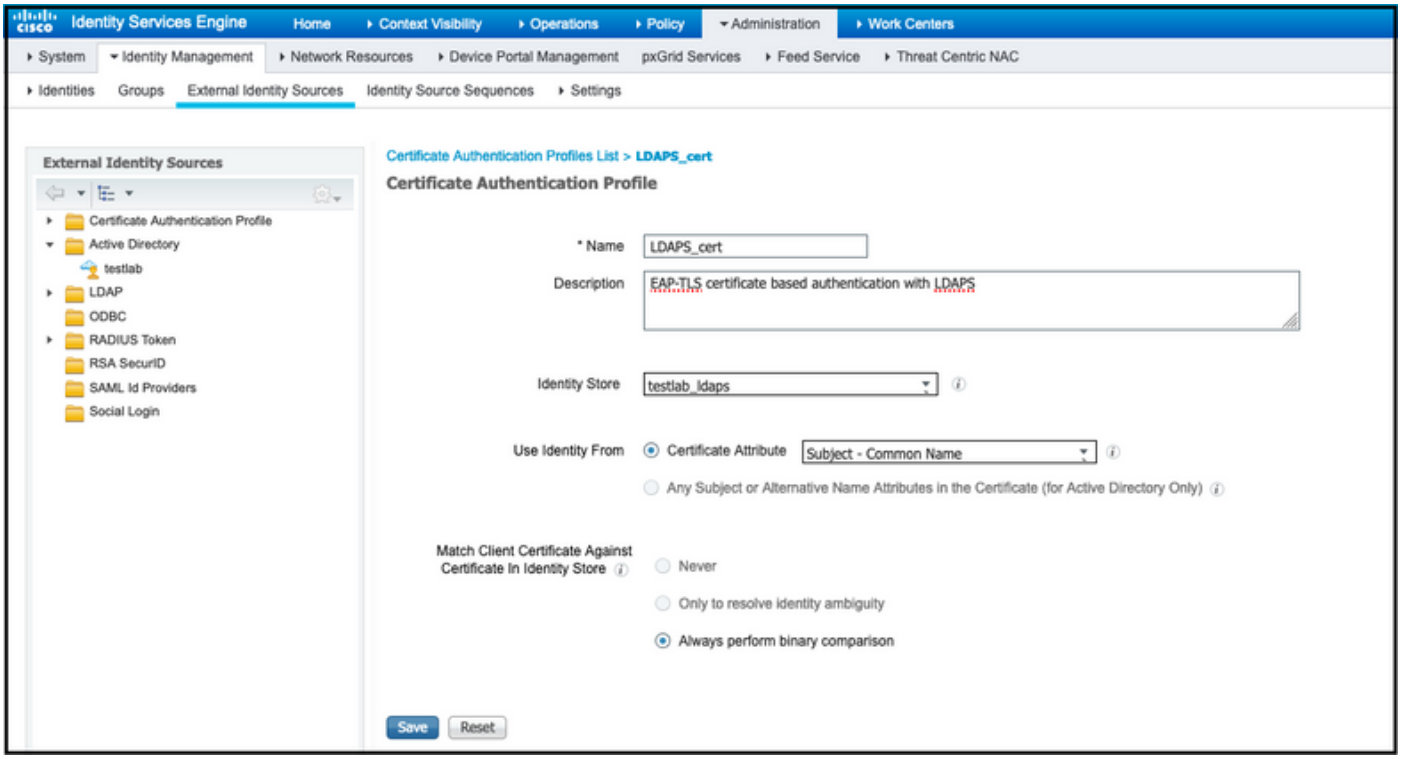


3. Fare clic su **Impostazioni aggiuntive**, si apre una finestra, selezionare la casella con **specifica modalità di autenticazione** e scegliere **Autenticazione utente**, come mostrato in questa immagine.

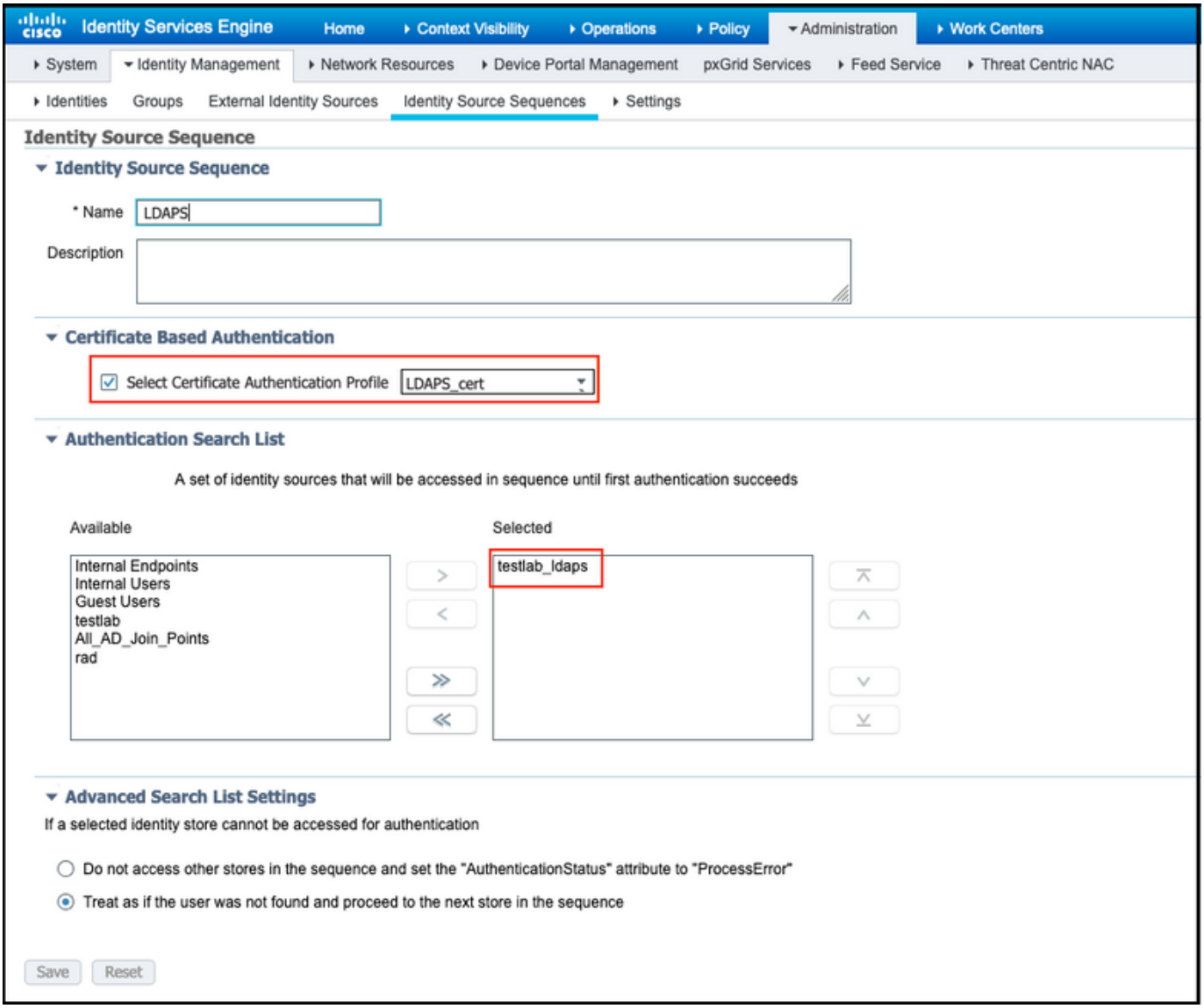


Configura Policy Set su ISE

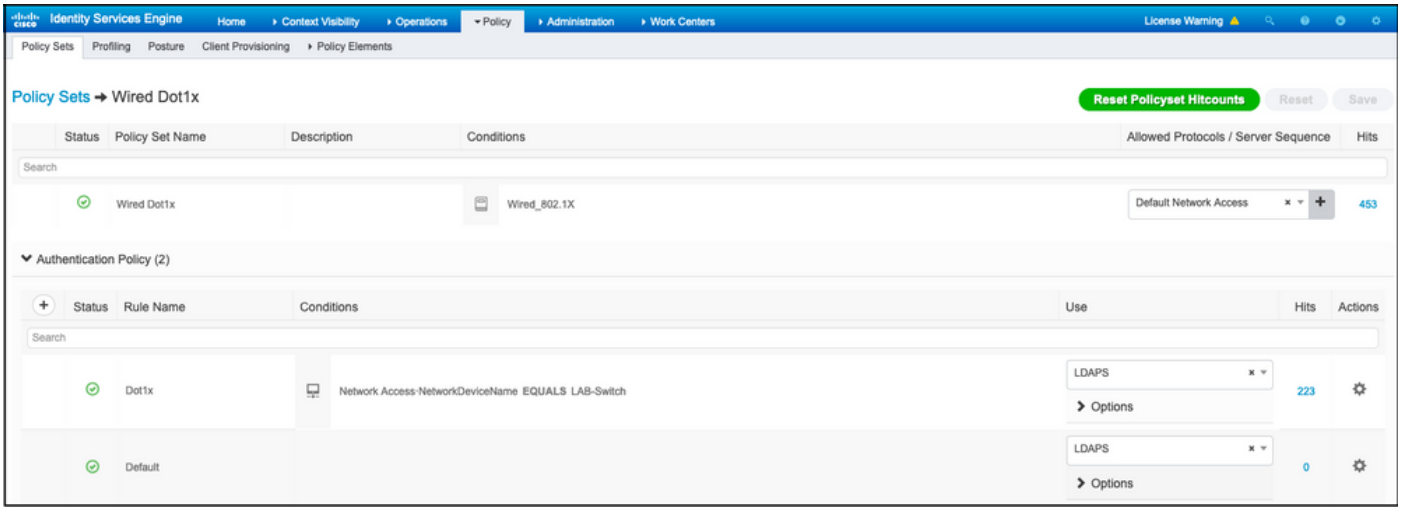
Poiché viene utilizzato il protocollo EAP-TLS, prima della configurazione di Policy Set è necessario configurare Certificate Authentication Profile e utilizzare Identity Source Sequence nel criterio di autenticazione in un secondo momento.



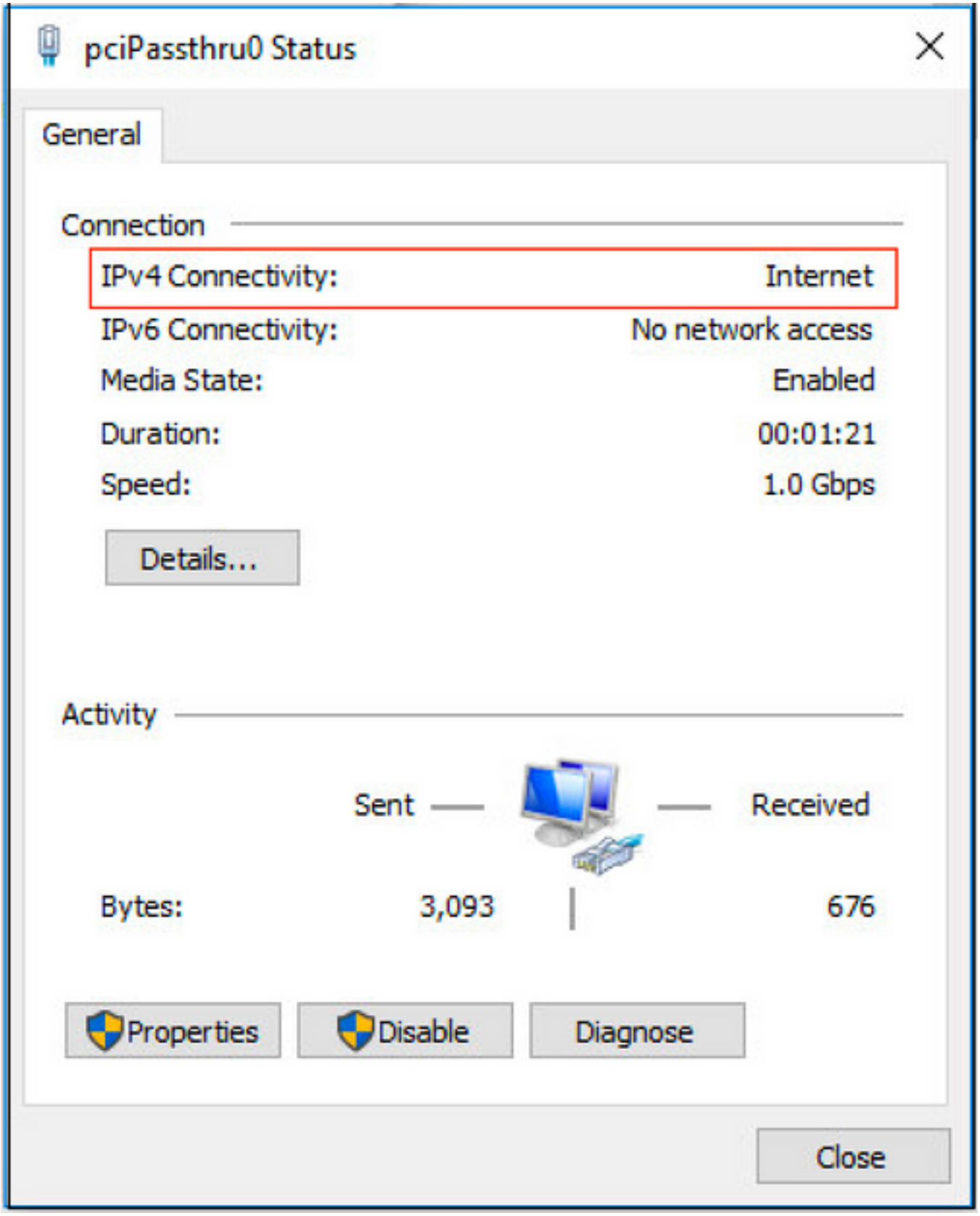
Fare riferimento al profilo di autenticazione del certificato nella sequenza Origine identità e definire l'origine identità esterna LDAPS nell'elenco di ricerca autenticazione:



Configurare ora il criterio impostato per l'autenticazione Dot1x per reti cablate:



Dopo questa configurazione, l'endpoint deve essere autenticato tramite il protocollo EAP-TLS sull'origine dell'identità LDAPS.

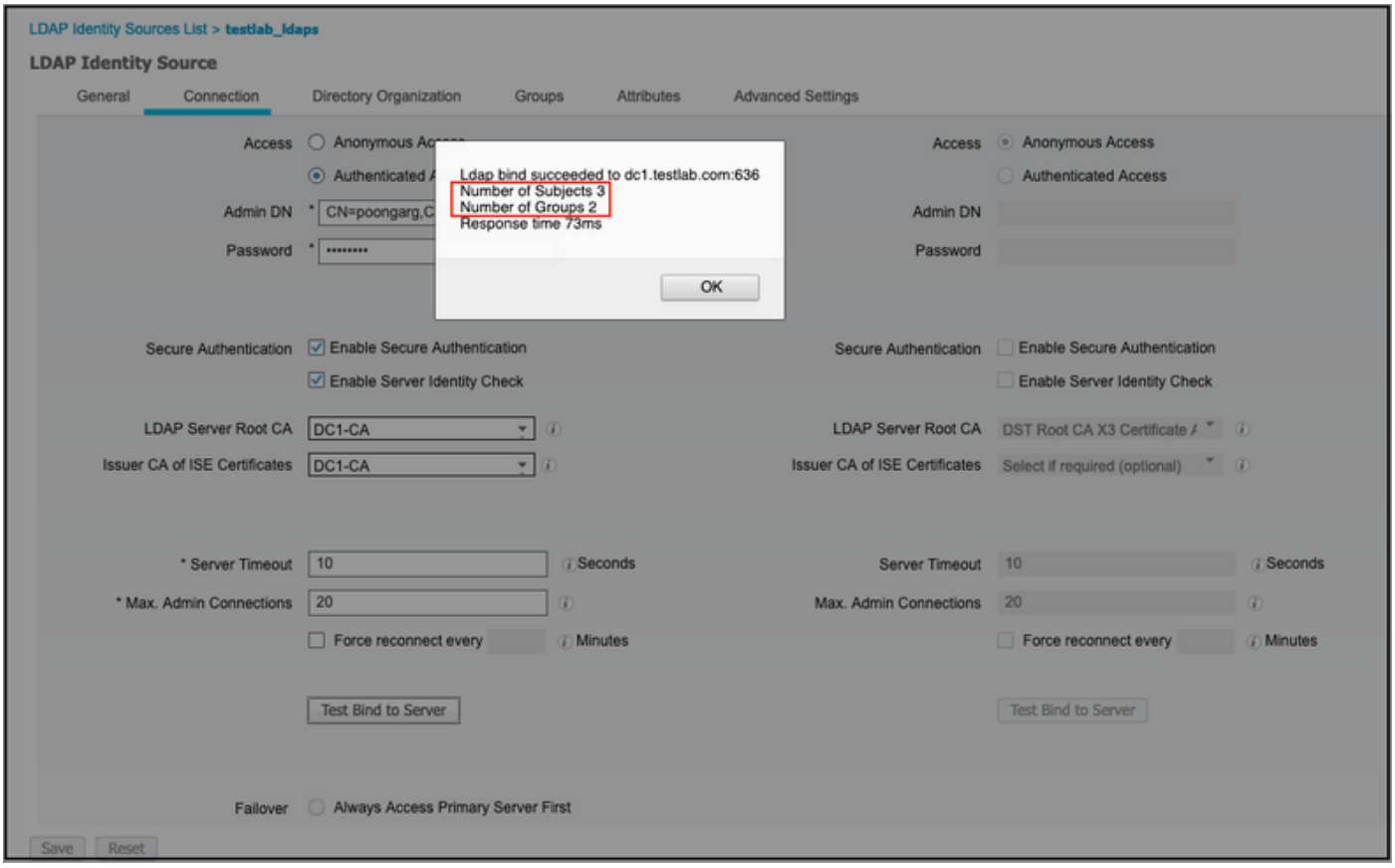


Verifica

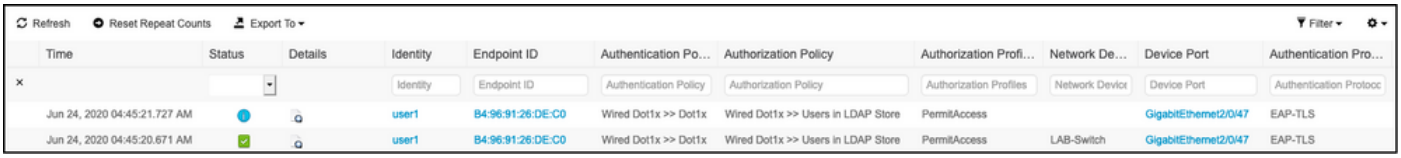
1. Controllare la sessione di autenticazione sulla porta dello switch collegata al PC:

```
SW1#sh auth sessions int g2/0/47 de
            Interface:  GigabitEthernet2/0/47
          MAC Address:  b496.9126.dec0
         IPv6 Address:  Unknown
         IPv4 Address:  10.106.38.165
            User-Name:  user1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  43s
    Common Session ID:  0A6A263900000130798C66612
      Acct Session ID:  0x00001224
               Handle:  0x6800002E
       Current Policy:  POLICY_Gi2/0/47

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
       Method           State

       dot1x            Authc Success
```

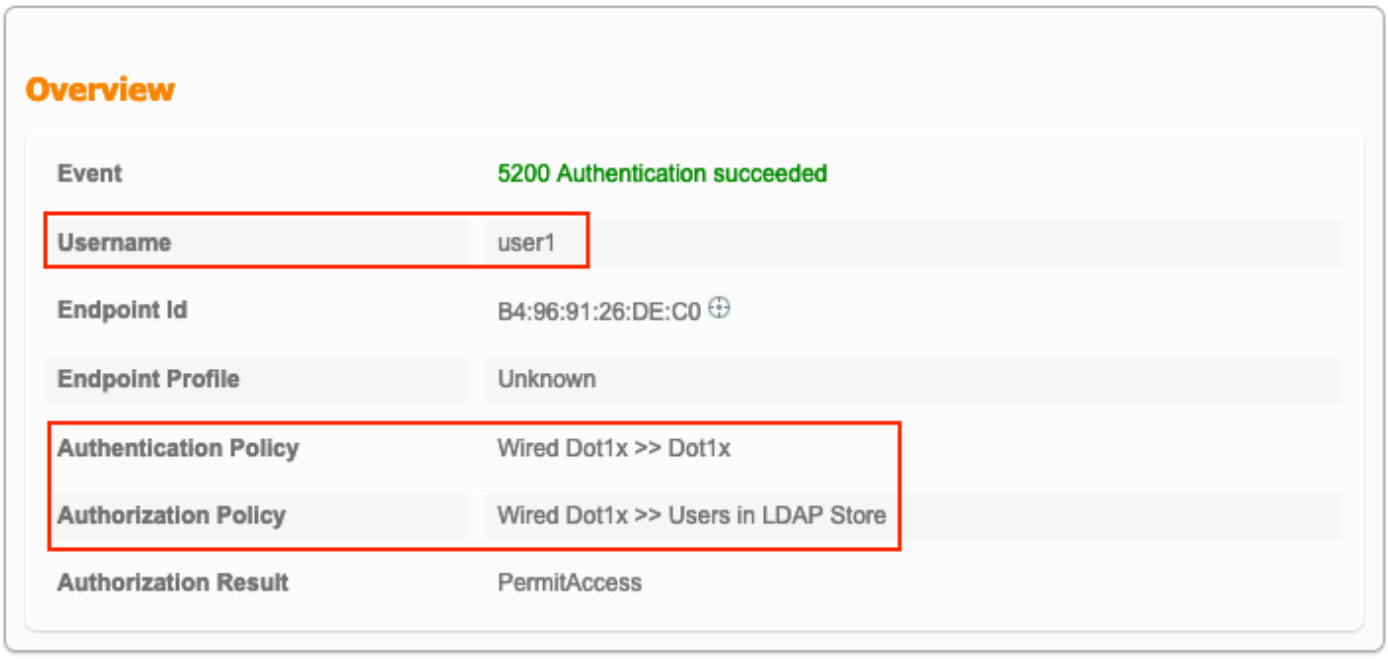
2. Per verificare le configurazioni LDAPS e ISE, è possibile recuperare gli oggetti e i gruppi con una connessione di prova al server:



3. Verificare il report di autenticazione utente:

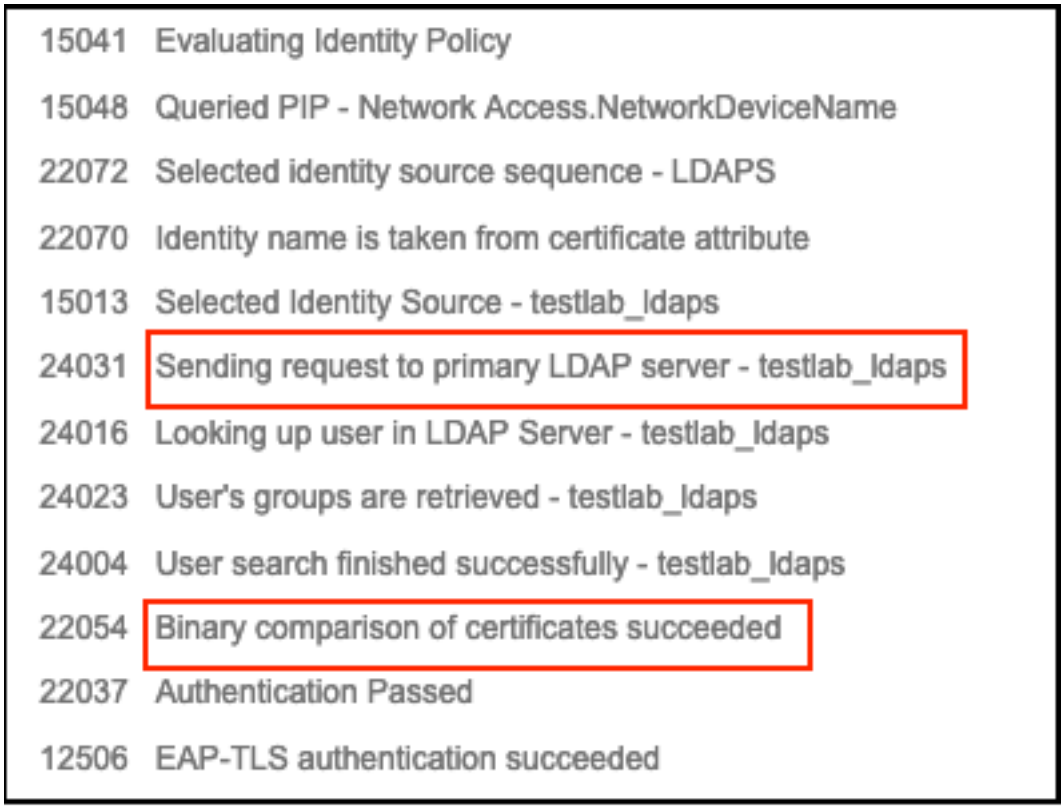


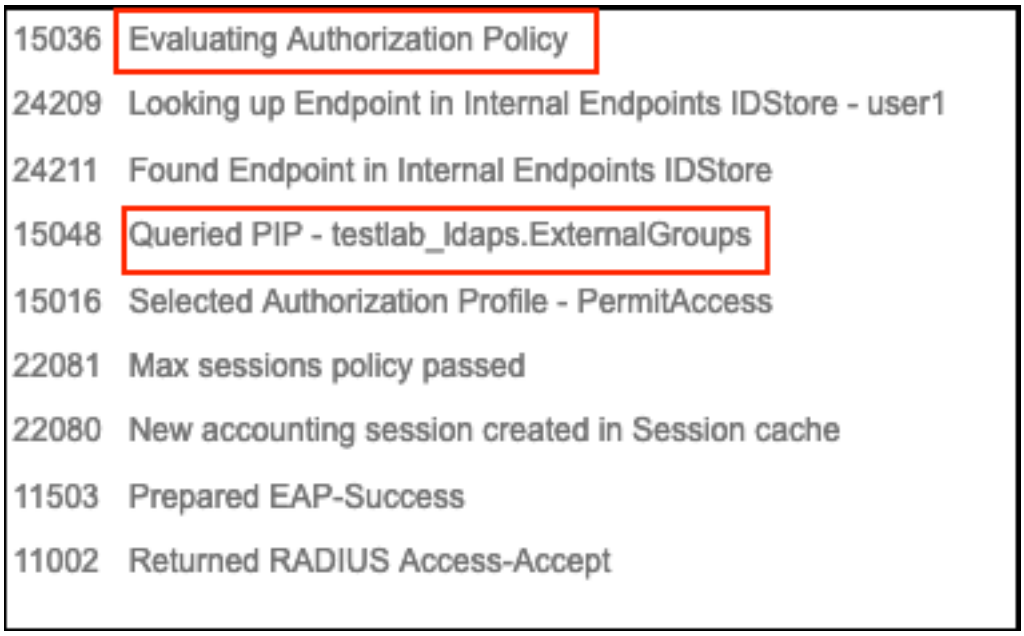
4. Verificare il report di autenticazione dettagliato per l'endpoint:



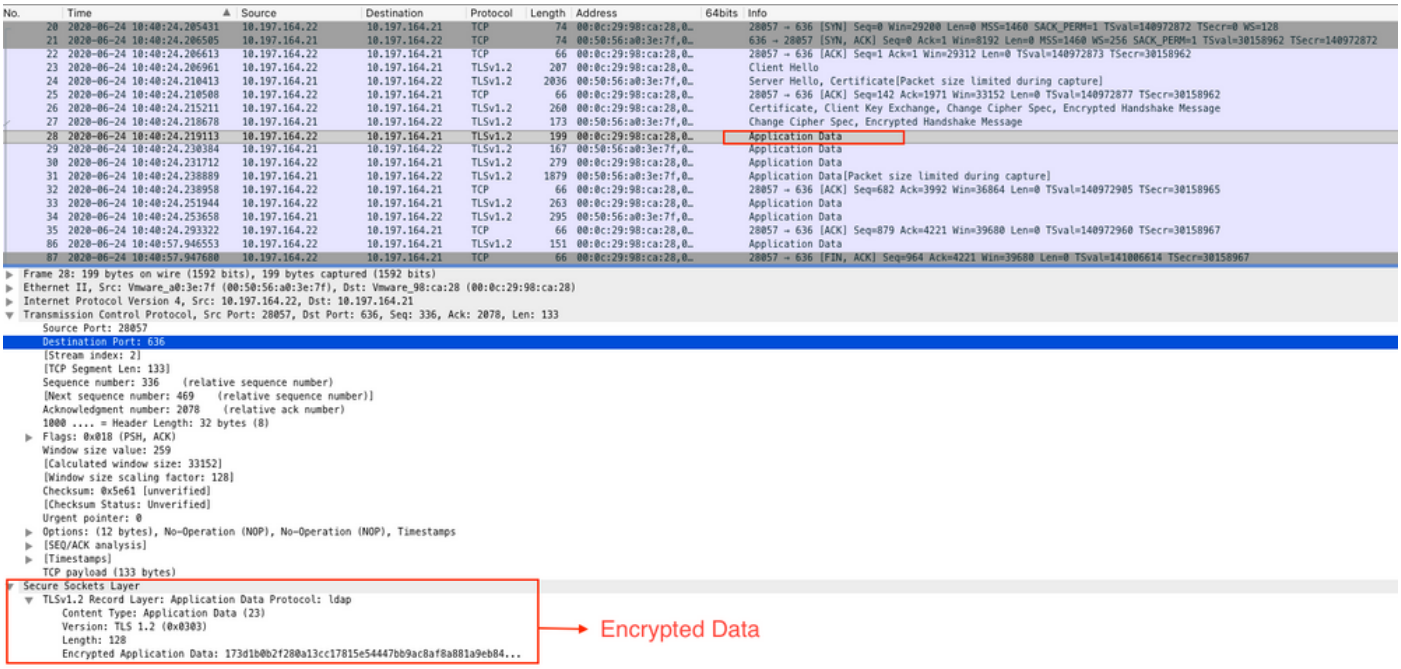
Authentication Details

Source Timestamp	2020-06-24 04:40:52.124
Received Timestamp	2020-06-24 04:40:52.124
Policy Server	ISE26-1
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	B4:96:91:26:DE:C0
Calling Station Id	B4-96-91-26-DE-C0
Endpoint Profile	Unknown
IPv4 Address	10.106.38.165
Authentication Identity Store	testlab_ldaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch





5. Verificare che i dati siano crittografati tra il server ISE e il server LDAPS effettuando l'acquisizione dei pacchetti sull'ISE verso il server LDAPS:



Risoluzione dei problemi

In questa sezione vengono descritti alcuni errori comuni che si sono verificati con questa configurazione e viene spiegato come risolverli:

- Nel report di autenticazione potrebbe essere visualizzato il seguente messaggio di errore:

`Authentication method is not supported by any applicable identity store`

Questo messaggio di errore indica che il metodo selezionato non è supportato da LDAP. Verificare che il **protocollo di autenticazione** nello stesso report mostri uno dei metodi supportati (EAP-GTC, EAP-TLS o PEAP-TLS).

- Test del binding al server terminato con un errore.

Nella maggior parte dei casi ciò è dovuto a un errore di controllo della convalida del certificato del server LDAPS. Per risolvere questi tipi di problemi, acquisire un pacchetto su ISE e abilitare tutti e tre i componenti runtime e port-jni a livello di debug, ricreare il problema e controllare il file **port-server.log**.

L'acquisizione pacchetti è in conflitto con un certificato non valido e il server di porta mostra:

```
04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error
message = SSL alert: code=0x22A=554 ; source=local ; type=fatal ; message="Server certificate
identity verification failed: host IP didnt match SAN IP.s3_clnt.c:1290
```

> **Nota:** Il nome host nella pagina LDAP deve essere configurato con il nome soggetto del certificato (o uno qualsiasi dei nomi soggetto alternativi). Pertanto, a meno che non sia presente nel soggetto o nella SAN, il certificato con l'indirizzo IP nell'elenco SAN non funziona.

3. Nel report di autenticazione è possibile notare che il soggetto non è stato trovato nell'archivio identità. Ciò significa che il nome utente del report non corrisponde all'**Attributo nome soggetto** per alcun utente nel database LDAP. In questo scenario, il valore è stato impostato su

sAMAccountName per questo attributo, il che significa che ISE cerca i valori sAMAccountName per l'utente LDAP quando tenta di trovare una corrispondenza.

4. I soggetti e i gruppi potrebbero non essere recuperati correttamente durante un test di **binding al server**. La causa più probabile è una configurazione errata delle basi di ricerca. Tenere presente che la gerarchia LDAP deve essere specificata dalla foglia alla radice e da dc (può essere costituita da più parole).

Informazioni correlate

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-configure-ise-00.html#anc9
- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html