Comtarsia Logon Client 2016 and SignOn Proxy 2016

Active Directory Authentication Modes

Manual

10 February 2020

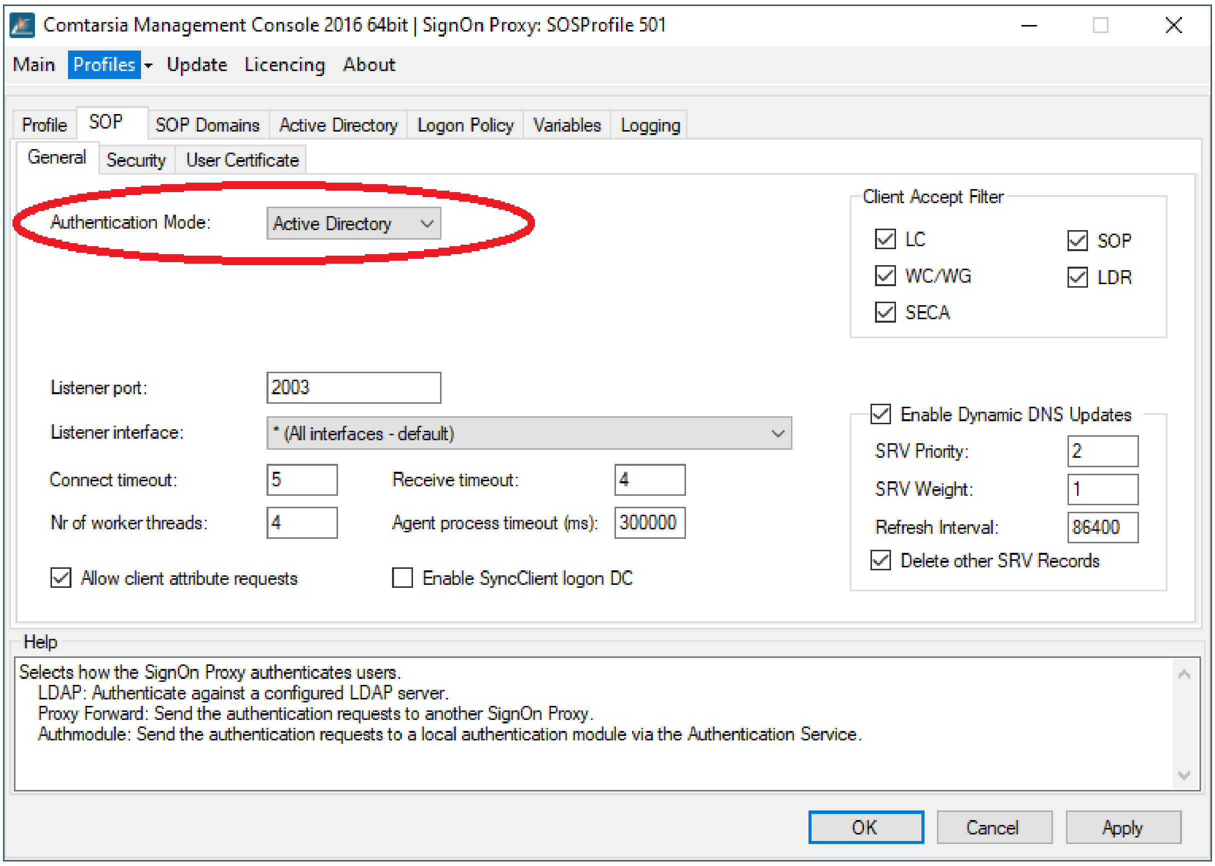
Contents

1. Active Directory authentication modes

The Comtarsia SignOn Solutions support different methods of authenticating users against an Active Directory. If the Comtarsia SignOn Proxy is used and is installed directly on a domain controller, the native Kerberos mode should be used. Otherwise, the LDAP authentication will be used for the Logon Client and the SignOn Proxy.

1.1 Active Directory native mode

This mode can be selected if the SignOn Proxy is directly installed on a domain controller. This mode has the advantage that no further configuration is necessary to authenticate the users. Just set in the management console the authentication mode to Active Directory, see Figure 1.



Authentication Mode: Active Directory

Listener port: 2003

Listener interface: * (All interfaces - default)

Connect timeout: 5

Receive timeout: 4

Nr of worker threads: 4

Agent process timeout (ms): 300000

☑ Allow client attribute requests

□ Enable SyncClient logon DC

☑ LC ☑ SOP

☑ WC/WG ☑ LDR

☑ SECA

☑ Enable Dynamic DNS Updates

SRV Priority: 2

SRV Weight: 1

Refresh Interval: 86400

☑ Delete other SRV Records

Selects how the SignOn Proxy authenticates users.
LDAP: Authenticate against a configured LDAP server.
Proxy Forward: Send the authentication requests to another SignOn Proxy.
Authmodule: Send the authentication requests to a local authentication module via the Authentication Service.

Figure 1: The Comtarsia Management Console for the SignOn Proxy showing the AD authentication mode

1.2 LDAP mode

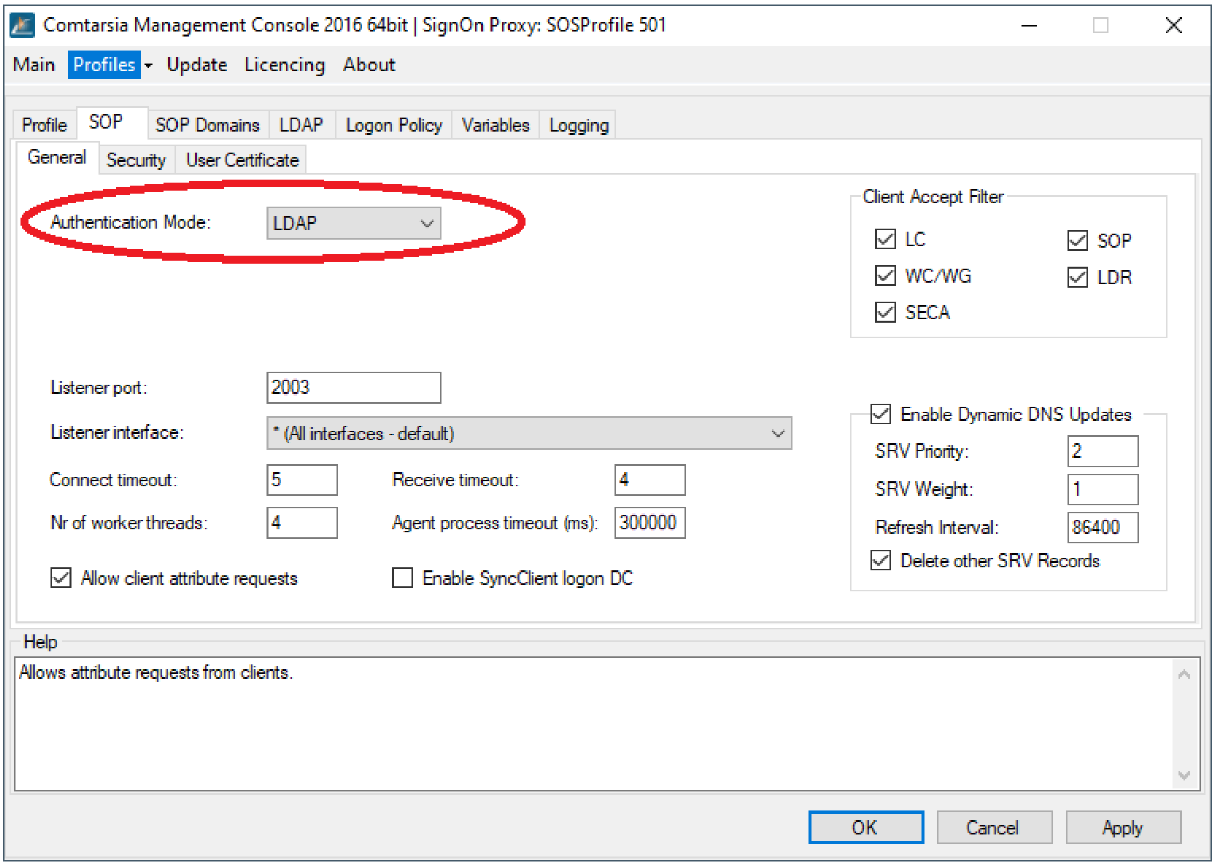
The Active Directory LDAP server supports user bind requests in three different formats; using the full user DN, using the user principal name (UPN) and using the samaccountname (SAN). Details about these three different naming attributes can also be found in this Microsoft document [2]. Further information about binding with the different naming attributes can be found in [3].

All three formats can be used to perform a simple authentication, while UPN and SAN can also be used to authenticate using the NTLM or Negotiate authentication methods.

In addition to this, the connection to the Active Directory LDAP server can be optionally encrypted using SSL/TLS. The use of SSL/TLS is mandatory if the users should be able to change their passwords over LDAP. The usage of SSL/TLS gets enabled automatically on the Active Directory LDAP server after an appropriate certificate for the server is installed. The easiest way to accomplish this is to add the Certificate Services for the domain using the Server Manager “Add roles and features” and then select “Active Directory Certificate Services”. Afterwards, a certificate for the Active Directory can be requested and will be automatically issued and installed.

Microsoft plans to release an update for the Active Directory LDAP server to disallow simple authentication requests over non SSL/TLS connections in March 2020. Details can be found in [1].

Figure 2 shows how to select the LDAP authentication mode in the Comtarsia Management Console.



Authentication Mode: LDAP

Client Accept Filter
☑ LC ☑ SOP
☑ WC/WG ☑ LDR
☑ SECA

Listener port: 2003

Listener interface: * (All interfaces - default)

Connect timeout: 5 Receive timeout: 4

Nr of worker threads: 4 Agent process timeout (ms): 300000

☑ Allow client attribute requests ☐ Enable SyncClient logon DC

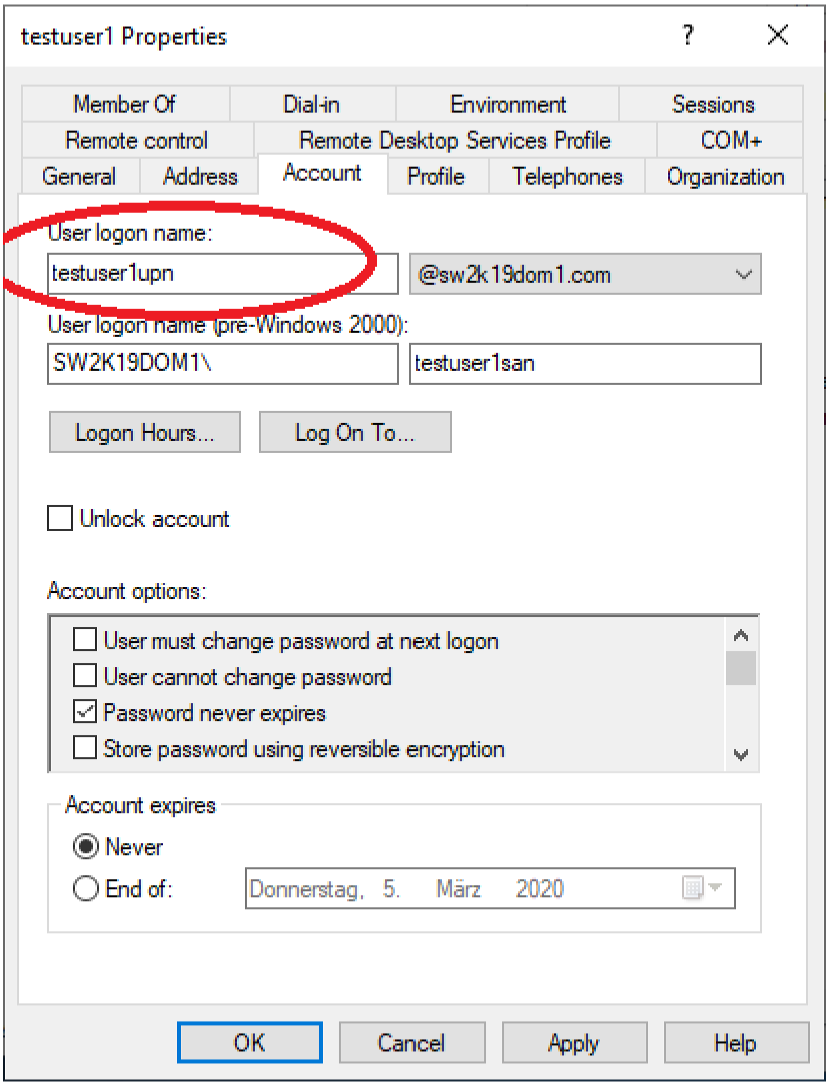
☑ Enable Dynamic DNS Updates
SRV Priority: 2
SRV Weight: 1
Refresh Interval: 86400
☑ Delete other SRV Records

Help
Allows attribute requests from clients.

Figure 2: The Comtarsia Management Console for the SignOn Proxy showing the LDAP authentication mode

1.2.1 Using the user principal name (UPN) for authentication

The screenshot in Figure 2 shows an Active Directory user object with the user principal name field highlighted.



testuser1 Properties

User logon name: testuser1upn @sw2k19dom1.com

User logon name (pre-Windows 2000): SW2K19DOM1\ testuser1san

□ Unlock account

Account options:

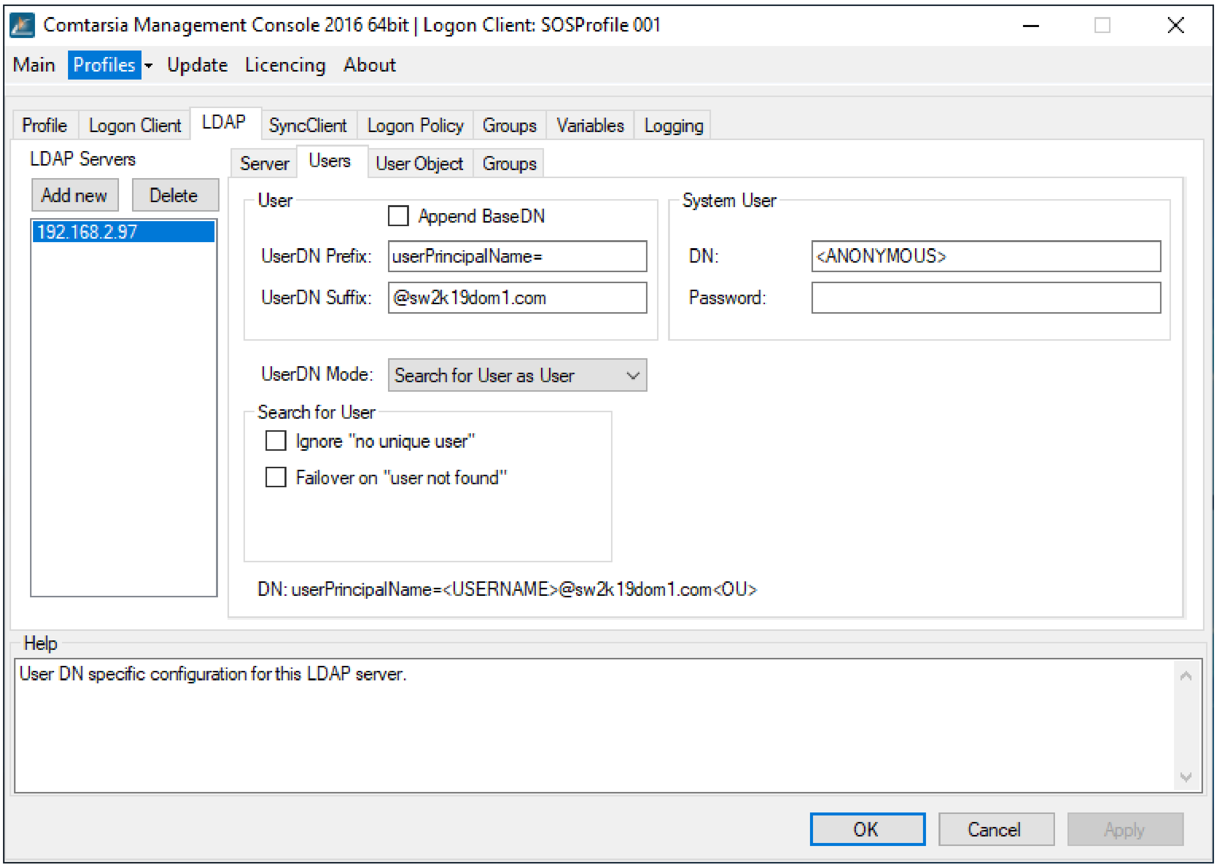
- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Donnerstag, 5. März 2020

Figure 3: An Active Directory user object with the UPN highlighted

To use the UPN to authenticate the users in the Comtarsia Logon Client/SignOn Proxy, set the following configuration in the Management Console:



192.168.2.97

User

□ Append BaseDN

UserDN Prefix: userPrincipalName=

UserDN Suffix: @sw2k19dom1.com

System User

DN: <ANONYMOUS>

Password:

UserDN Mode: Search for User as User

Search for User

□ Ignore "no unique user"

□ Failover on "user not found"

DN: userPrincipalName=<USERNAME>@sw2k19dom1.com<OU>

Help

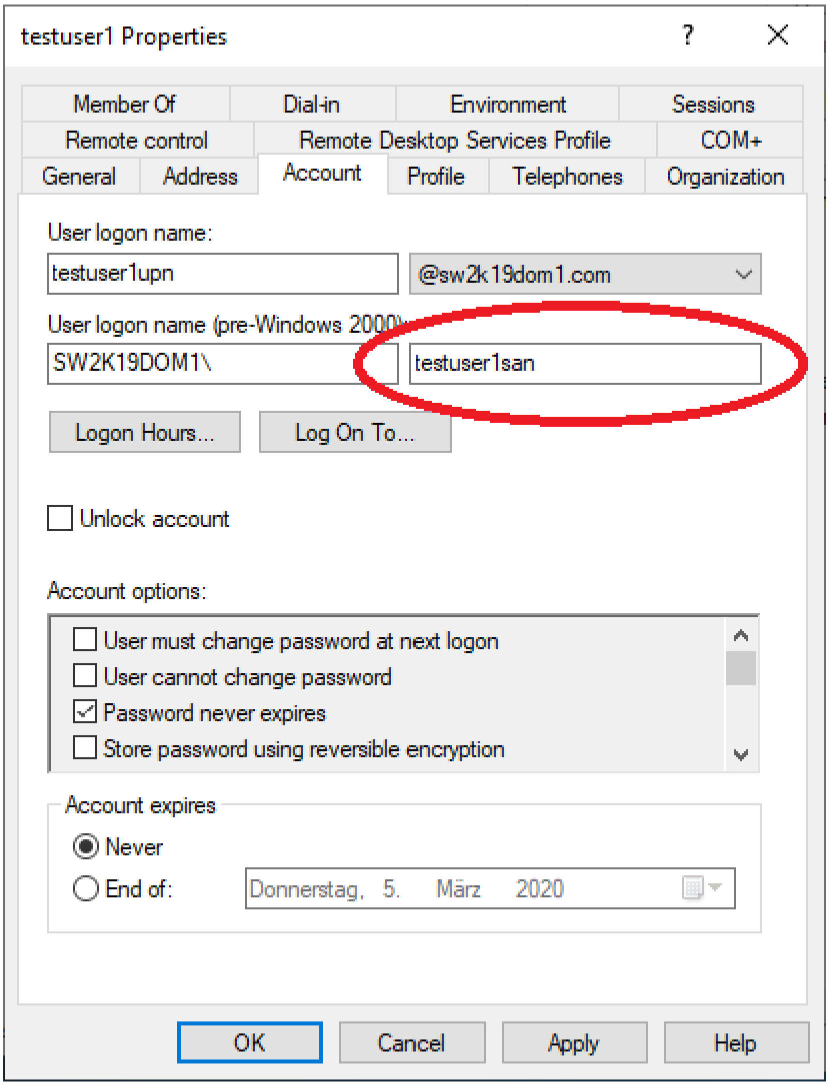
User DN specific configuration for this LDAP server.

Figure 4: The Comtarsia Management Console showing the LDAP\Users tab for UPN logon

The value UserDN Suffix must be set to the actual used value from the Active Directory.

1.2.2 Using the pre-Windows 2000 logon name (samaccountname) for authentication

The screenshot in Figure 4 shows an Active Directory user object with the pre-Windows 200 logon name (samaccountname in LDAP) field highlighted.



User logon name:

testuser1upn @sw2k19dom1.com

User logon name (pre-Windows 2000):

SW2K19DOM1\ testuser1san

□ Unlock account

Account options:

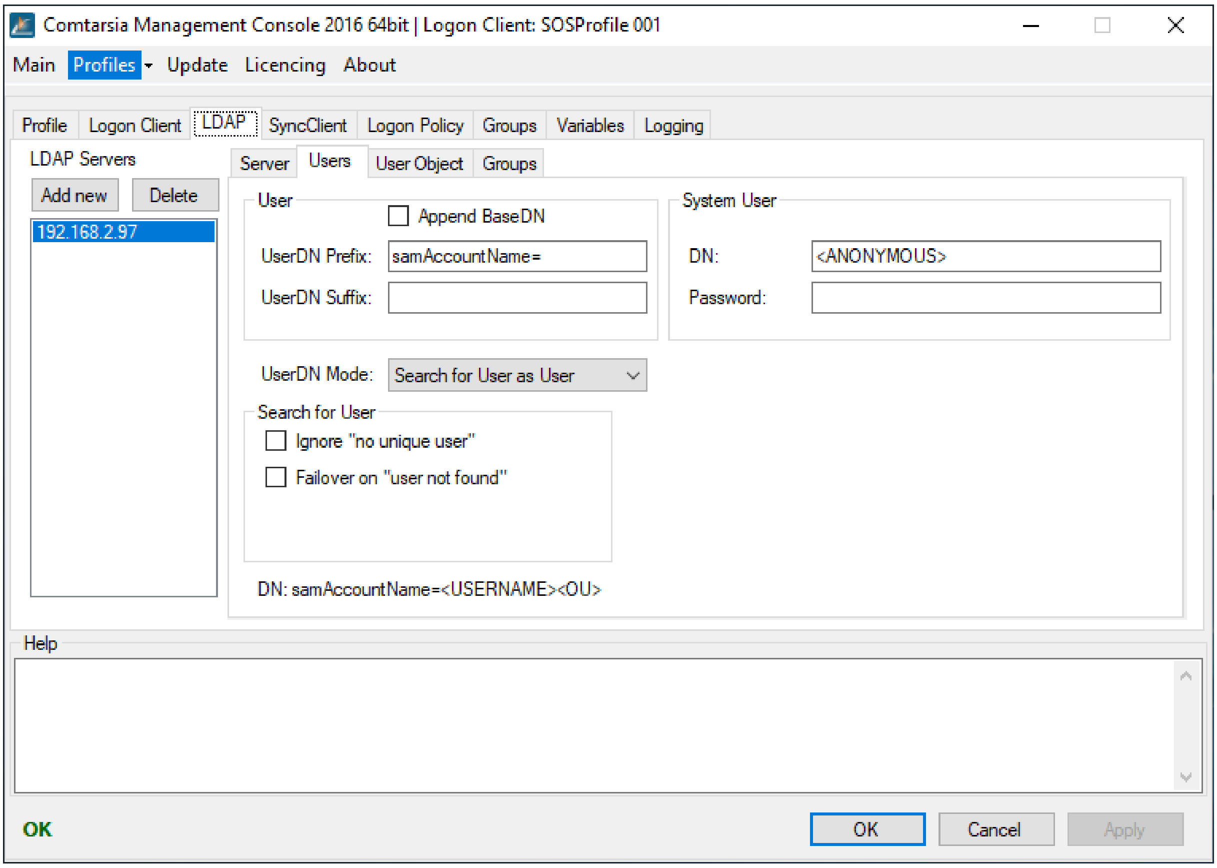
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Donnerstag, 5. März 2020

Figure 5: An Active Directory user object with the samaccountname highlighted

To use the samaccountname to authenticate the users in the Comtarsia Logon Client/SignOn Proxy, set the following configuration in the Management Console:



Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001

LDAP Servers: 192.168.2.97

User

□ Append BaseDN

UserDN Prefix: samAccountName=

UserDN Suffix:

System User

DN: <ANONYMOUS>

Password:

UserDN Mode: Search for User as User

Search for User

□ Ignore "no unique user"

□ Failover on "user not found"

DN: samAccountName=<USERNAME><OU>

OK

Figure 6: The Comtarsia Management Console showing the LDAP\Users tab for samaccountname logon

2. References

[1] https://signon.comtarsia.com/main/en/Update-b26

[2] https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties

[3] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/6a5891b8-928e-4b75-a4a5-0e3b77eaca52