Group Policy Management Editor

File   Action   View   Help

Policy ▲	Policy Setting
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Require signing
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled
Domain member: Digitally encrypt secure channel data (when possible)	Disabled
Domain member: Digitally sign secure channel data (when possible)	Disabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled

Tree (Computer Configuration):
- Policies
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)
    - Deployed Printers
    - Security Settings
      - Account Policies
      - Local Policies
        - Audit Policy
        - User Rights Assignmer
        - Security Options
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wired Network (IEEE 802.
      - Windows Firewall with Adv
      - Network List Manager Poli
      - Wireless Network (IEEE 80
      - Public Key Policies
      - Software Restriction Polici
      - Network Access Protectior
      - IP Security Policies on Act
  - Policy-based QoS
  - Administrative Templates: Policy d
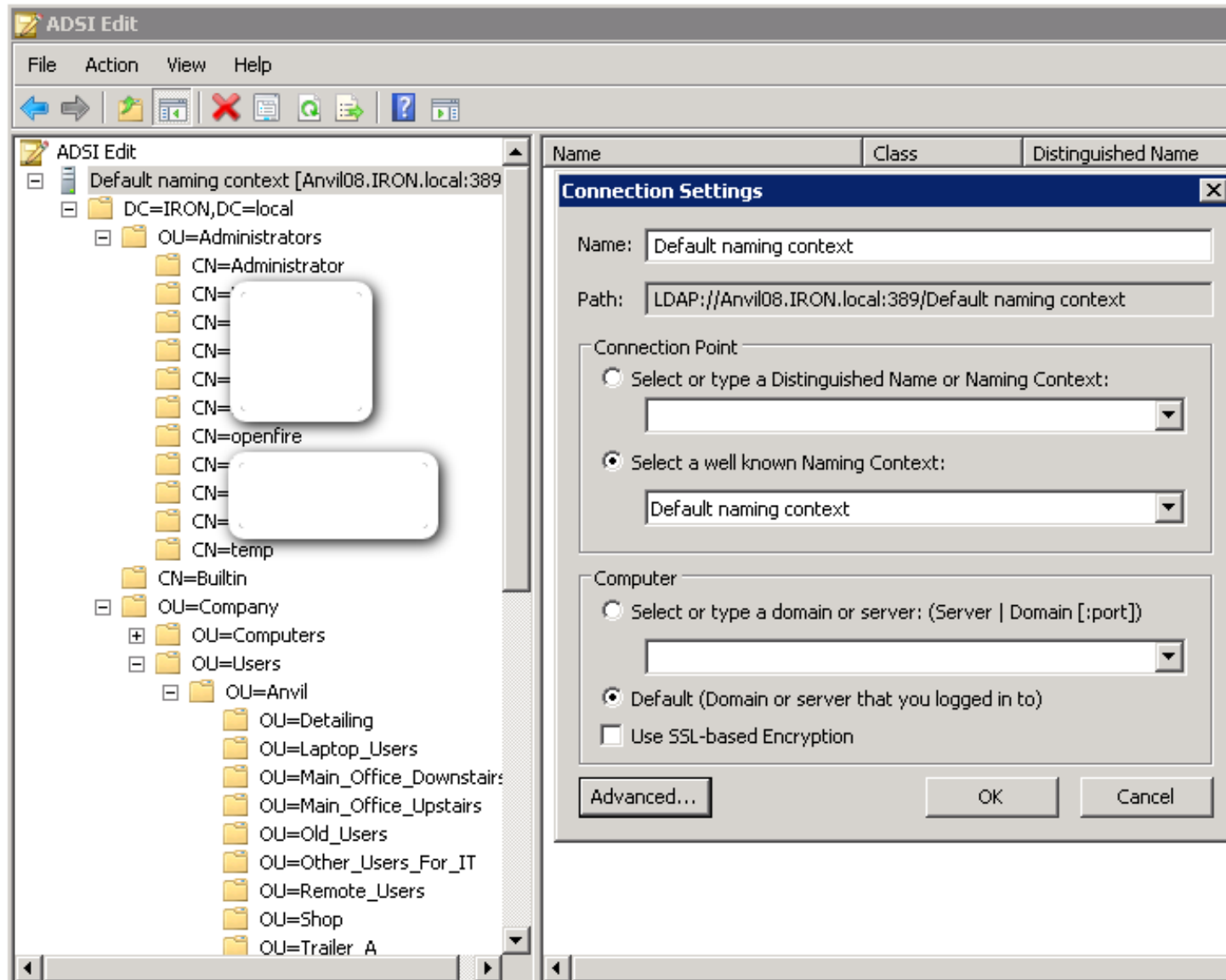- references
- Configuration
- olicies

I am using Windows Server 2008 in this example I also have Windows Server 2003 on the same network for our Exchange.
Okay I enabled the LDAP in the Group Policy. I have tried both None & Required signing neither work.
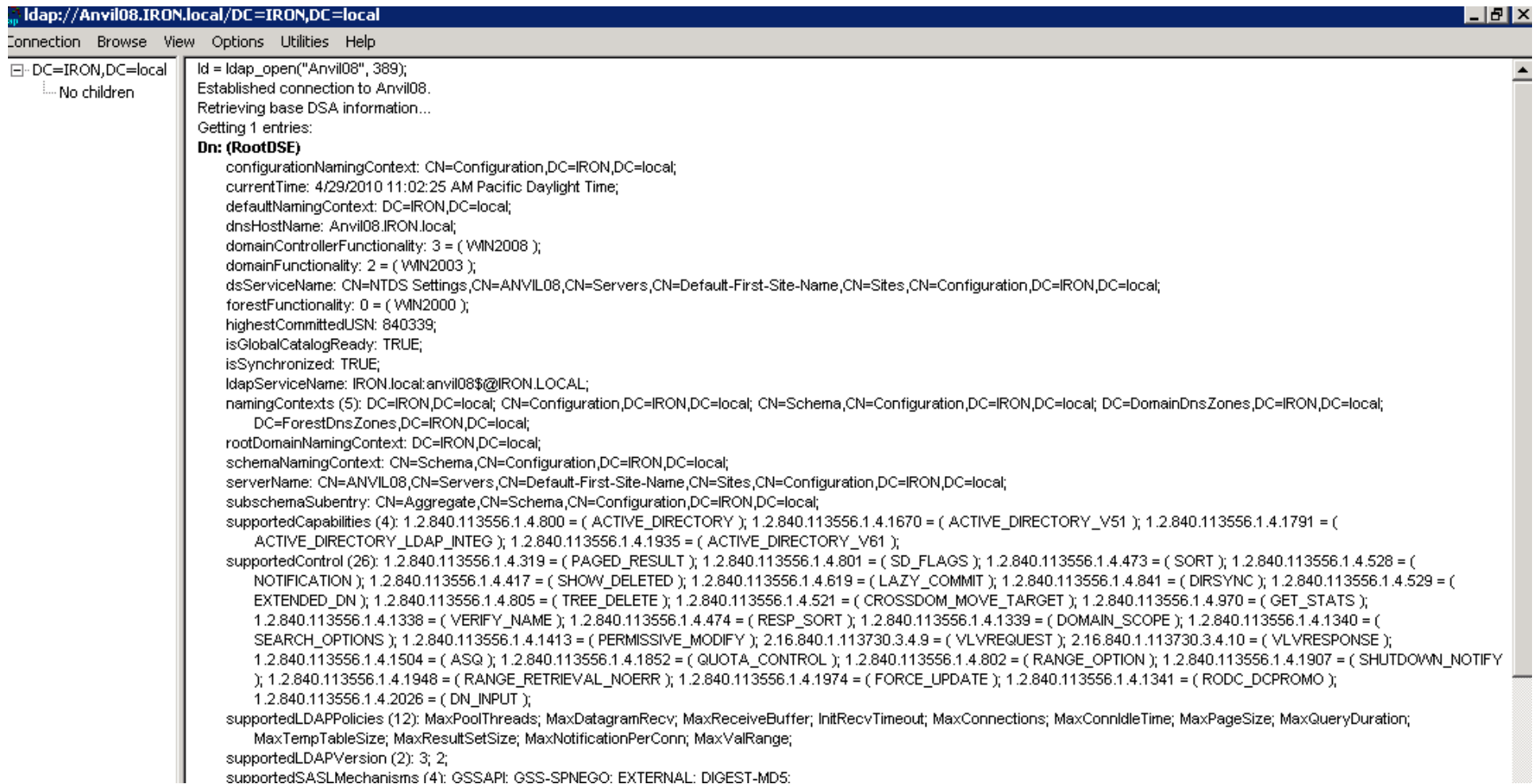
On the server I opened adsiedit.msc and connected using the credentials below and was able to establish a connection

I did not select simple bind and it connected it will not connect with simple bind checked, I also tried the account openfire which I setup for Open Fire only.
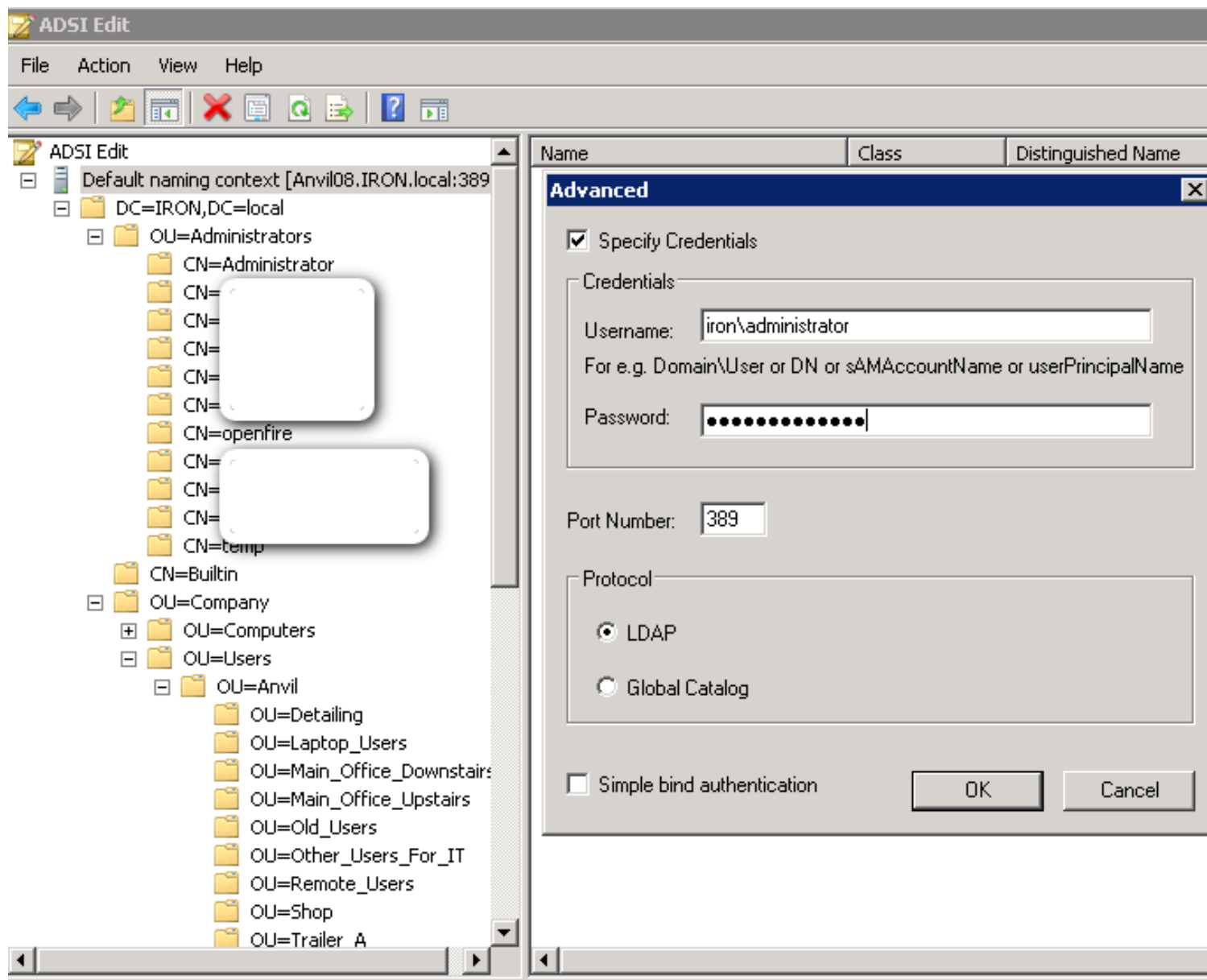
Then I opened ldp.exe and tested that connection and it worked fine. It did not work with the SSL connection on port 636

```
ldap://Anvil08.IRON.local/DC=IRON,DC=local                                    _ | 5 | X
Connection  Browse  View  Options  Utilities  Help
⊟ DC=IRON,DC=local      Id = ldap_open("Anvil08", 389);
    └ No children       Established connection to Anvil08.
                        Retrieving base DSA information...
                        Getting 1 entries:
                        Dn: (RootDSE)
                            configurationNamingContext: CN=Configuration,DC=IRON,DC=local;
                            currentTime: 4/29/2010 11:02:25 AM Pacific Daylight Time;
                            defaultNamingContext: DC=IRON,DC=local;
                            dnsHostName: Anvil08.IRON.local;
                            domainControllerFunctionality: 3 = ( WIN2008 );
                            domainFunctionality: 2 = ( WIN2003 );
                            dsServiceName: CN=NTDS Settings,CN=ANVIL08,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=IRON,DC=local;
                            forestFunctionality: 0 = ( WIN2000 );
                            highestCommittedUSN: 840339;
                            isGlobalCatalogReady: TRUE;
                            isSynchronized: TRUE;
                            ldapServiceName: IRON.local:anvil08$@IRON.LOCAL;
                            namingContexts (5): DC=IRON,DC=local; CN=Configuration,DC=IRON,DC=local; CN=Schema,CN=Configuration,DC=IRON,DC=local; DC=DomainDnsZones,DC=IRON,DC=local;
                                DC=ForestDnsZones,DC=IRON,DC=local;
                            rootDomainNamingContext: DC=IRON,DC=local;
                            schemaNamingContext: CN=Schema,CN=Configuration,DC=IRON,DC=local;
                            serverName: CN=ANVIL08,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=IRON,DC=local;
                            subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=IRON,DC=local;
                            supportedCapabilities (4): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
                                ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 );
                            supportedControl (26): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = ( SORT ); 1.2.840.113556.1.4.528 = (
                                NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = ( LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC ); 1.2.840.113556.1.4.529 = (
                                EXTENDED_DN ); 1.2.840.113556.1.4.805 = ( TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
                                1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = ( DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = (
                                SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE );
                                1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY
                                ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO );
                                1.2.840.113556.1.4.2026 = ( DN_INPUT );
                            supportedLDAPPolicies (12): MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize; MaxQueryDuration;
                                MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxValRange;
                            supportedLDAPVersion (2): 3; 2;
                            supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
```

My firewall is off, also for our AV.
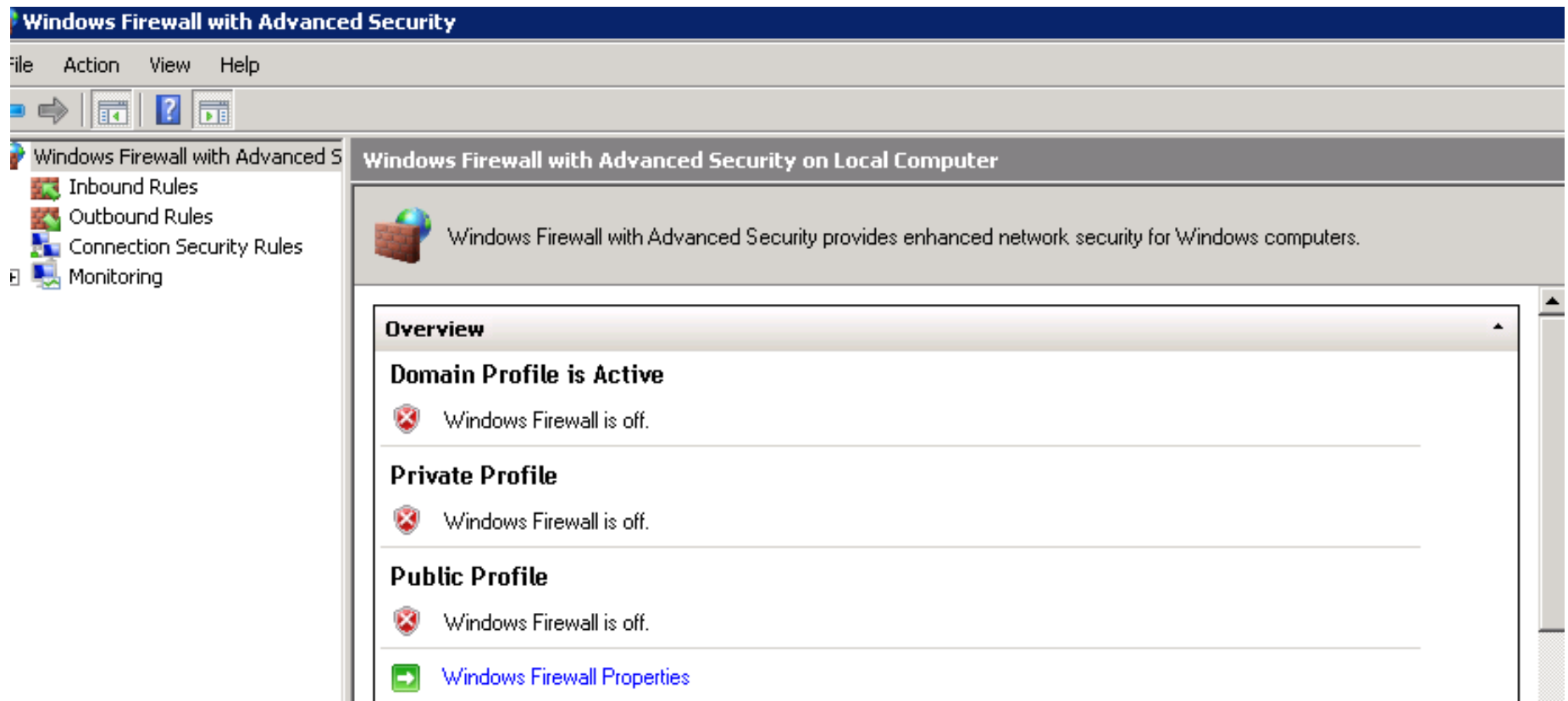
I get this error every time I try to connect with the following info below.

Test: Connection Settings

Status: Error

Error connecting to the LDAP server. Ensure that the directory server is running at the specified host name and port and that a firewall is not blocking access to the server.

Profile Settings: Connection Settings

1. Connection Settings	2. User Mapping	3. Group Mapping

Step 1 of 3: Connection Settings

Configure connection settings for your LDAP directory below. All fields are required; if you need additional information about a field, hover your mouse over the corresponding help icon.

LDAP Server

Server Type: Active Directory ⌄ ⑦

Host: Anvil08.IRON.local   Port: 389 ⑦

Base DN: OU=Administrators,DC=IRON,DC=local ⑦

Authentication:

Administrator DN: IRON\openfire ⑦

Password: ••••••• ⑦

▶ Advanced Settings

Test Settings   Save & Continue

Step 1 of 3: Connection Settings

Configure connection settings for your LDAP directory below. All fields are required; if you need additional information about a field, hover your mouse over the corresponding help icon.

LDAP Server

Server Type: `Active Directory` ▼ ⑦

Host: `Anvil08.IRON.local`   Port: `389` ⑦

Base DN: `OU=Administrators,DC=IRON,DC=local` ⑦

Authentication:

Administrator DN: `CN=openfire,OU=Administrators,DC=IRON,DC=local` ⑦

Password: `••••••` ⑦

▶ Advanced Settings

Test Settings   **Save & Continue**

Step 1 of 3: Connection Settings

Configure connection settings for your LDAP directory below. All fields are required; if you need additional information about a field, hover your mouse over the corresponding help icon.

LDAP Server

Server Type: Active Directory ▼ ⑦

Host: Anvil08.IRON.local   Port: 389 ⑦

Base DN: OU=Administrators,DC=IRON,DC=local ⑦

Authentication:
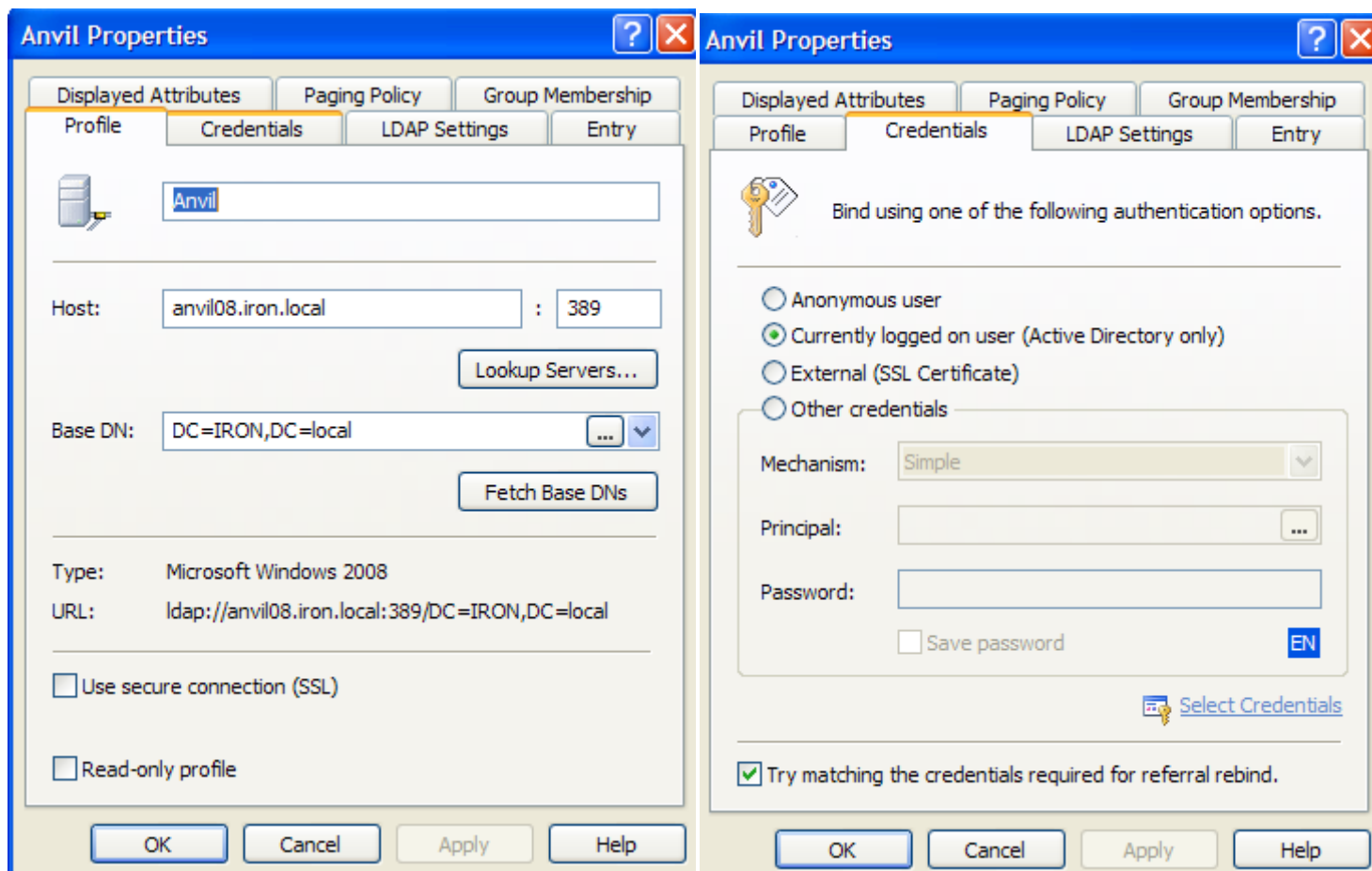
Administrator DN: openfire@iron.local ⑦

Password: ••••••• ⑦

▶ Advanced Settings

Test Settings   Save & Continue

Then I opened Softerra LDAP Administrator 2010 and created this profile with these credentials and was able to connect just fine.

File Edit View Favorites Server Entry Schema Reports Tools Window Help

New ▾   (objectClass=*)

Scope Pane ▾ ⊞ ✕

Find what: ▾ Search in: Names, Descriptions

Name	Value	Type
objectClass	top	Attribute
objectClass	person	Attribute
objectClass	organizationalPerson	Attribute
objectClass	user	Attribute
cn	openfire	Attribute
description	Account for LDAP for OpenFire and Spark IM System	Attribute
givenName	openfire	Attribute
distinguishedName	CN=openfire,OU=Administrators,DC=IRON,DC=local	Attribute
instanceType	[Writable]	Attribute
whenCreated	4/28/2010 6:55:12 PM	Attribute
whenChanged	4/29/2010 5:35:19 PM	Attribute
displayName	openfire	Attribute
uSNCreated	820049	Attribute
memberOf	CN=Account Operators,CN=Builtin,DC=IRON,DC=local	Attribute
uSNChanged	840010	Attribute
name	openfire	Attribute
userAccountControl	[NormalAccount, NoPasswordExpiration]	Attribute
badPwdCount	0	Attribute
codePage	0	Attribute
countryCode	0	Attribute
badPasswordTime	unspecified	Attribute
lastLogoff	unspecified	Attribute
lastLogon	4/29/2010 5:26:39 PM	Attribute

Scope Pane tree:
- Softerra LDAP Administrator
  - Internet Public Servers
  - Intranet Private Servers
    - Anvil
      - OU=Administrators
        - CN=Administrator
        - CN=
        - CN=
        - CN=
        - CN=
        - CN=
        - CN=openfire
        - CN=
        - CN=
        - CN=
        - CN=temp
      - CN=Builtin
      - OU=Company
      - CN=Computers
      - CN=defaultMigrationContain
      - OU=Domain Controllers
      - CN=ForeignSecurityPrincipals
      - CN=Infrastructure
      - CN=LostAndFound
      - OU=Microsoft Exchange Sec
      - CN=Microsoft Exchange Sys

But when I use other credentials and use simple and the correct login info it will not connect.

Anvil Properties ? ✕

| Displayed Attributes | Paging Policy | Group Membership |

| Profile | Credentials | LDAP Settings | Entry |

Credentials Validation Error ✕

⚠ Can't validate credentials. Strong authentication is required. Would you like to proceed?

[Yes] [No] [Cancel]

⦿ Other credentials

Mechanism: Simple ▼

Principal: CN=openfire,OU=Administrators,DC=IF [...]

Password: *******

☐ Save password EN

🔑 Select Credentials

☑ Try matching the credentials required for referral rebind.

[OK] [Cancel] [Apply] [Help]