

1 Configuration - Using exacqVision Version 7.2 or Higher

NOTE: The domain controller must run on Windows Server 2003 operating system or later.


NOTE: The exacqVision Server must have an Enterprise license.

To configure the directory settings, complete the following steps:

1. On the exacqVision server, download and install the exacqVision server and client software from www.exacq.com. You must be logged in with Local Administrator privileges to do this. If using a Windows server, it is recommended, but not required, to join the machine to the domain.
2. Under 'Configure System' on the 'Active Directory/LDAP tab', select the Enable Directory Service checkbox.
3. Enter the AD server's IP address in the Hostname/IP Address field.
4. Select the SSL checkbox if you want LDAP operations to use SSL.

5. a. Windows (joined to domain):
The SPN should already exist and would be in the form of 'HOST/fqdn'. (HOST/exacqserver.exacq.com)

b. Any OS, including Edge Cameras, (not joined to the domain):
You can opt to allow exacqVision to create the SPN (service principal name) by checking the "Permission to Create SPN" box. The resulting SPN displays below.



c. If you would still like to create the SPN manually on the Active Directory server itself:
Open a command prompt (right-click to run as an Administrator, if necessary) on the Active Directory server and execute the following command, substituting the name and fully qualified hostname of your exacqVision Server:

setspn -A EDVR/hostname.domain.xxx hostname (example: setspn -A EDVR/evserver.exacqsupport.local evserver)

NOTE: Type the entire command above; do NOT copy and paste it. Also, all text after the forward slash should be lower case, and "EDVR" must be upper case. The SPN must replicate to, or be entered on, all Domain Controllers.

6. Select the appropriate LDAP Schema from the drop-down list.
7. Verify the AD server's connection port. Unless you have reconfigured your AD server, the port should be 636 when using SSL, or 389 without SSL.

NOTE: It is best practice to make sure you have AD connectivity without SSL (port 389) before trying SSL (port 636).

8. Enter the LDAP Base DN, the container of all directory user accounts or groups that you want to map in the exacqVision software. For example, if the domain were exacq.test.com, the LDAP Base DN might be:

CN=Users, DC=exacq, DC=test, DC=com

9. Enter the LDAP Account name of a directory user who has access to view the records of the directory user accounts. It is recommended that you enter the Administrator user account as the LDAP Binding DN. For example, if the domain were `exacq.test.com`, the LDAP Account Name of the Administrator account would be:

`EXACQ.TEST.COM\Administrator`

NOTE: The binding DN user's password should be set to never expire. The Binding DN user must be a member of Domain Users. This user must have the ability to set Service Principal Names, otherwise, you will need to manually configure the SPN on the Domain Server for Single Sign-On to work.

10. Enter the password for the account entered in the previous step.
11. To prevent any non-directory users that have previously been created from connecting to the exacqVision server (optional), deselect Enable Local User Accounts.
12. Click Apply to connect. An indicator on the ActiveDirectory/LDAP tab displays the success or failure of the connection attempt.

2 Adding exacqVision Users from the Active Directory Database

When the exacqVision server is appropriately configured and connected to your AD server, the Users page and the Enterprise User Setup page each contain a Query LDAP button that allows you to search for users or user groups configured in AD. You can manage their exacqVision server permissions and privileges using the exacqVision Client the same way you would for a local user. On the System Information page, the Username column lists any connected AD users along with their AD origin (whether each user was mapped as an individual or part of a user group) in parentheses.

3 Connecting to exacqVision Servers

You can connect to your Enterprise exacqVision servers from the Windows exacqVision Client software in any of the following ways:

- Use a local exacqVision username and password.
- If you are already logged into Windows as a domain user, use your system login without entering a username or password. In this case, leave the username and password fields empty on the Add Systems page, select Use Single Sign-On, and click Apply.
- Use any domain user account. Enter the account name in `user@realm` format as the username (such as `test.user@exacq.com`). Use the password associated with that account. Do NOT select Use Single Sign-On with this login method.

NOTE: If you attempt to connect to an exacqVision server using your system login without first logging in to Windows through the domain, the connection will fail.

To connect with your exacqVision client software from a Linux machine attached to your domain:

- Open a terminal and type the **kinit** command before using Single Sign-On. For example: `kinit user@DOMAIN`
- You cannot sign in by typing your UPN name at the **Use credentials entered below:** prompt.

4 Troubleshooting

LDAP Not Connecting

On the Domain Controller, add and confirm rules for TCP/UDP ports 389 (standard clear text LDAP) and 636 (standard SSL LDAP).

✓ Active Directory Domain Controller - LDAP (TCP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - LDAP (UDP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - LDAP for Global Catalog (TCP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - NetBIOS name resolution (UDP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - Secure LDAP (TCP-In)	Active Directory Domain Services	All
✓ Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-In)	Active Directory Domain Services	All

Re-imaging or Replacing System (Including Virtual Machines)

1. Use a different hostname and IP (recommended).
2. If using the same hostname and IP, make sure all instances and references of this hostname, IP, and SPN have been removed from the DC.
3. Rejoin to the domain and import the exacqVision configuration file to restore settings and preferences

Client-Side Kerberos Errors

- Either the binding DN account does not have permission to set the SPN or you did not manually run the setspn command on all DCs, or it has not replicated to all DCs. If you entered the SPN manually, you can check on each DC by opening a command prompt on the DC and typing **setspn -l hostname** (the hostname of the exacqVision server). If your machine was on the domain, use **setspn -l fqdn**. If your machine was not on the domain use **setspn -l mac_address or serial**

You should have something like this:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -l ewinserver
Registered ServicePrincipalNames for CN=EUWINSERVER,OU=T3 Cor
ort,DC=local:
EDUR/ewinserver.exacqsupport.local
TERMSRU/ewinserver.exacqsupport.local
RestrictedKrbHost/ewinserver.exacqsupport.local
HOST/ewinserver.exacqsupport.local
TERMSRU/EUWINSERVER
RestrictedKrbHost/EUWINSERVER
HOST/EUWINSERVER
```

Name Resolution Issues

You should be able to ping and resolve the exacqVision server from the client computer. If connecting using a hostname, DNS must be resolvable. In Command Prompt on the client computer, type **ping exacqhostname.domain.xxx**.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\hstovall>ping ewwinserver

Pinging ewwinserver.exacqsupport.local [2002:198c:a9bc::198c:a9bc]
of data:
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms

Ping statistics for 2002:198c:a9bc::198c:a9bc:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If it is still not resolving:

- Check DNS PTR records. Make sure the hostname and IP address are correct.
- Delete and add back the DNS record for the exacqVision server, if needed.
- Verify that you can resolve any FQDNs.
- Try logging in using your UPN name instead of Single Sign-On (Windows clients only). UPN=user@domain.xxx. If successful with the UPN name, restart the client computer and try Single Sign-On again.
- Verify that ports are open for 636 (secure LDAP) or 389 (LDAP).
- In Linux, check whether **kinit** returns an error stating it cannot find or connect to the KDC server. Ping your KDC server's FQDN (usually your DC). If you cannot ping the KDC, this is a DNS issue. You can resolve by making sure you have set a valid internal DNS server via exacqVision Client, or by adding your KDC server to your HOSTS file.

```
GNU nano 2.2.2      File: /etc/hosts
127.0.0.1          exacqshostname.domain.xxx localhost
127.0.1.1          exacqshostname.domain.xxx exacqshostname
xxx.xxx.xxx.xxx   yourKDCserver.domain.xxx yourKDCserver
```

Server-Side Kerberos Errors

- The exacqVision server log could contain the following error:

```
StreamPI Error SSPI error: SEC_E_TIME_SKEW
```

This means the clocks on the client and server computers do not match. The exacqVision server time can be no more than five minutes off the DC's time.

- Make sure the User and Group OU/Container are nested under the Base DN (see discussion earlier in this document).
- Can you ping all your DC FQDNs and resolve them from the client and server?
- You may have entered your Service Principle Name (SPN) incorrectly. You can verify the SPN from a command prompt on the DC, enter **setspn -I hostname** (the hostname or the exacqVision server). If your machine was on the domain, use **setspn -I fqdn**. If your machine was not on the domain use **setspn -I serial** (where serial is the exacqVision Serial number, or mac_address for a 3rd party server).