

Active Directory & LDAP Best Practices

1. **Introduction**
 - a. **Benefits of Integration**
 - b. **exacqVision Server must have Enterprise license**
 - c. **Use groups on domain**
2. **exacqVision to AD/LDAP Data Flow**
3. **Configuration**
4. **Troubleshooting**

1. Introduction

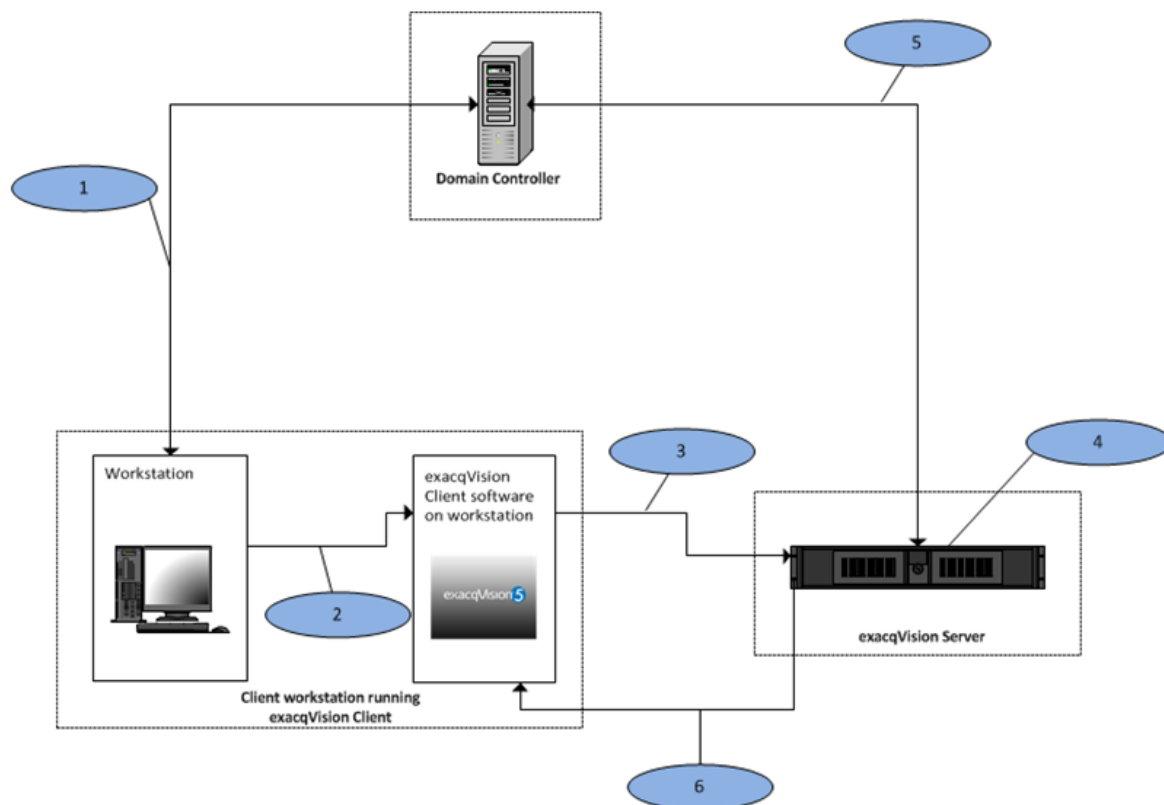
For an organization using Active Directory (AD) for user management of information technology services, integrating exacqVision into the AD infrastructure can greatly simplify continuing maintenance of user access to your video management system (VMS). On each exacqVision Server, you can assign VMS permissions to one or more AD groups. Then, as you add user accounts to those groups through standard IT user management practices, those users will automatically have access to log in to the exacqVision Servers with appropriate permissions. User management directly through exacqVision becomes a one-time configuration requiring that you join the server to the domain and assign permissions and privileges to groups, and all additional user management occurs through AD.

To provide the ongoing benefits of using group-based permissions with exacqVision Server, the server must do more than simply authenticate login credentials of a user requesting access; it must be able to browse AD groups to present them as configuration options and to determine whether a user requesting access is a member of any configured groups.

Minimum Requirements

- Your exacqVision Server must have an Enterprise license to interact with AD
- The domain controller must be running on Windows Server 2003 or later.
- To configure AD on an exacqVision Server, you must have Active Directory credentials with the following access to a minimum of the following AD parameters:
 - * objectClass (specifically "group" & "user")
 - * userPrincipalName
 - * sAMAccountName
 - * inetOrgPerson
 - * krbPrincipalName

2. exacqVision to AD/LDAP Data Flow

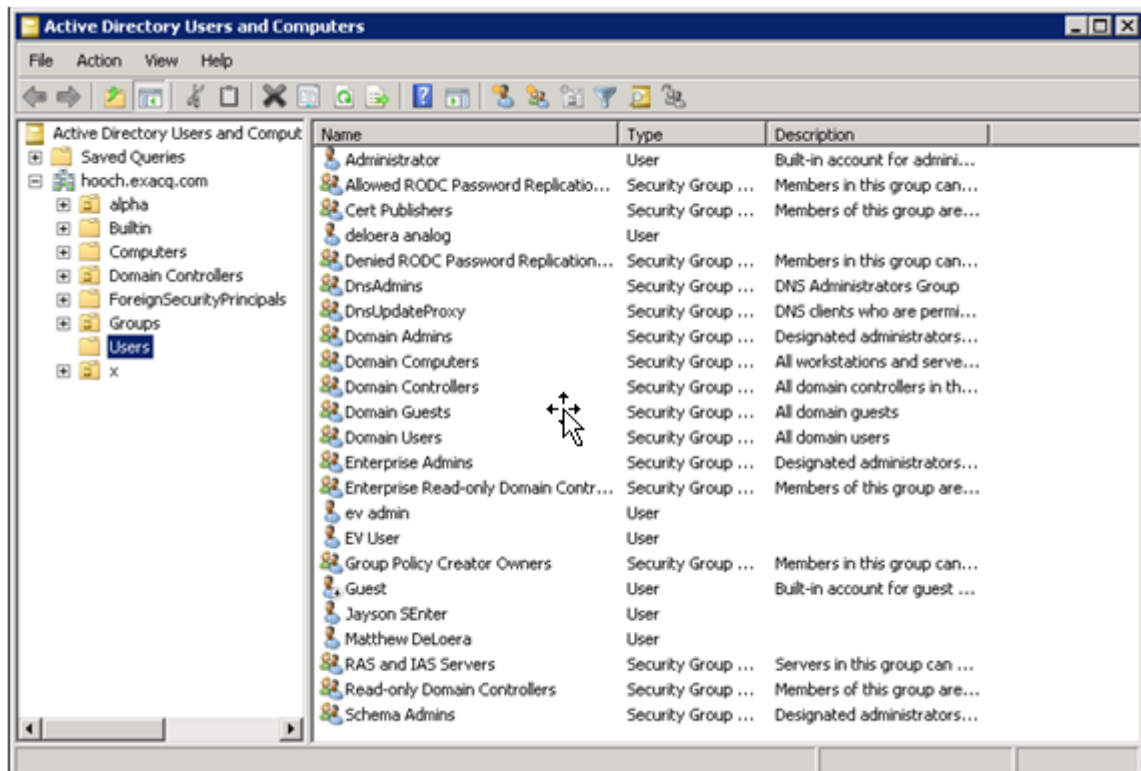


1. exacqVision Client computer joined to the domain. Optionally, you can join the exacqVision Server to the domain.
2. The Kerberos ticket (the operating system domain login credential) is passed from the client workstation operating system to exacqVision Client.
3. exacqVision Client initiates communication with the exacqVision Server and passes the Kerberos ticket.
4. The exacqVision Server validates the ticket and extracts the user information.
5. The exacqVision Server passes the user to LDAP, which looks at the group and/or user associations for the passed user credential.
6. The exacqVision Server passes the rights and privileges based on the user and groups associated with the user credential.

3. Configuration

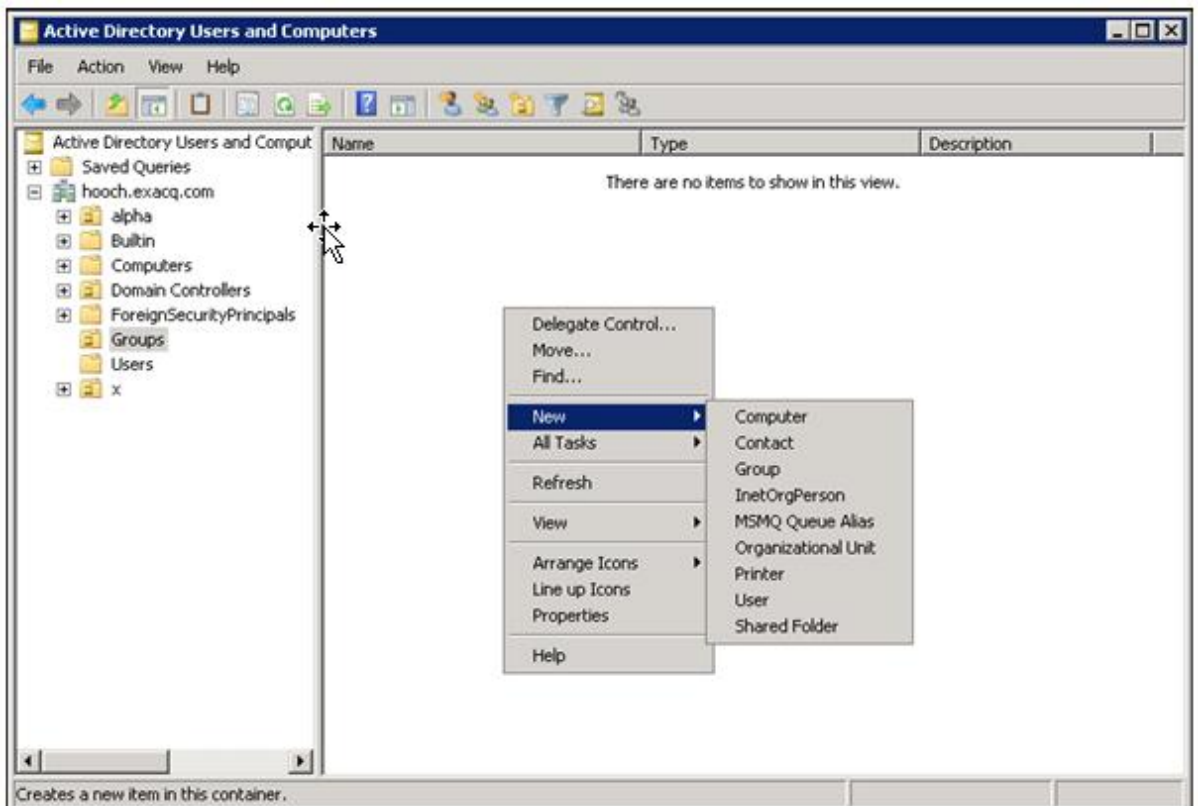
exacqVision Support Portal

1. Log in to your domain controller and expand the tree.



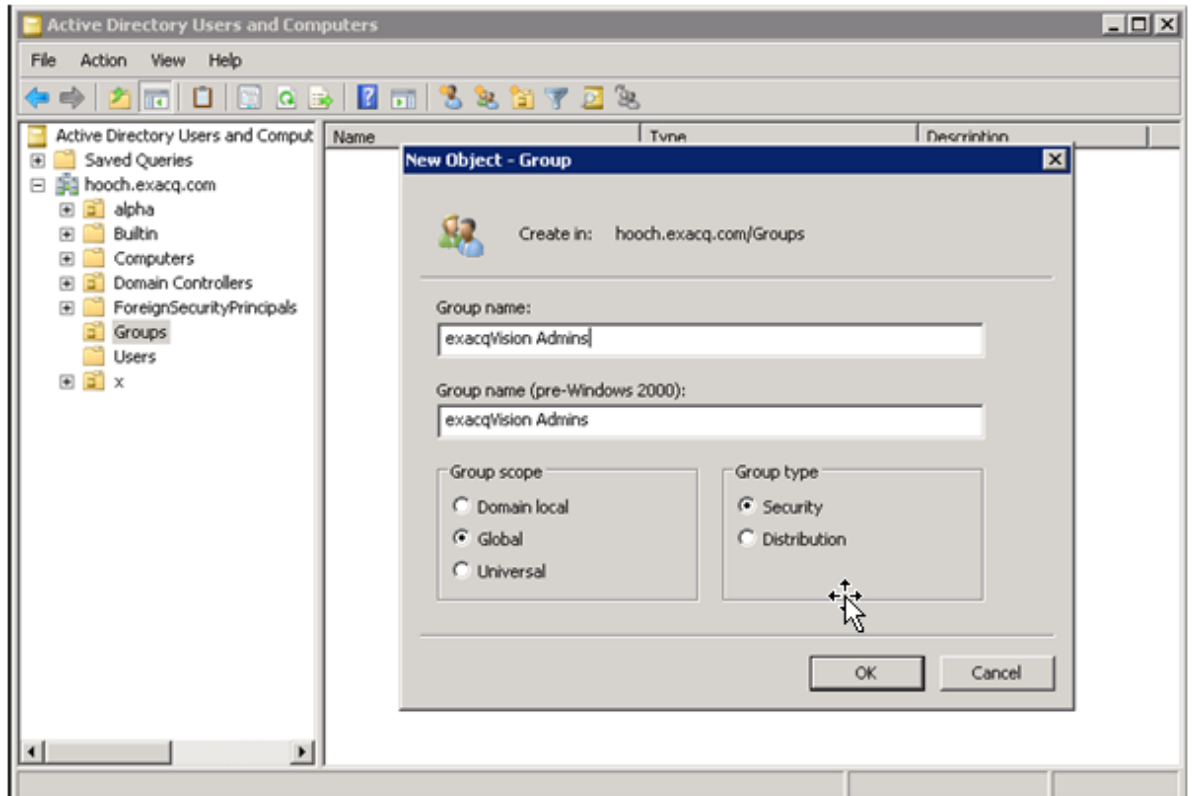
2. Create a new group that specifies privileges in the name nested under your desired Base DN.

exacqVision Support Portal

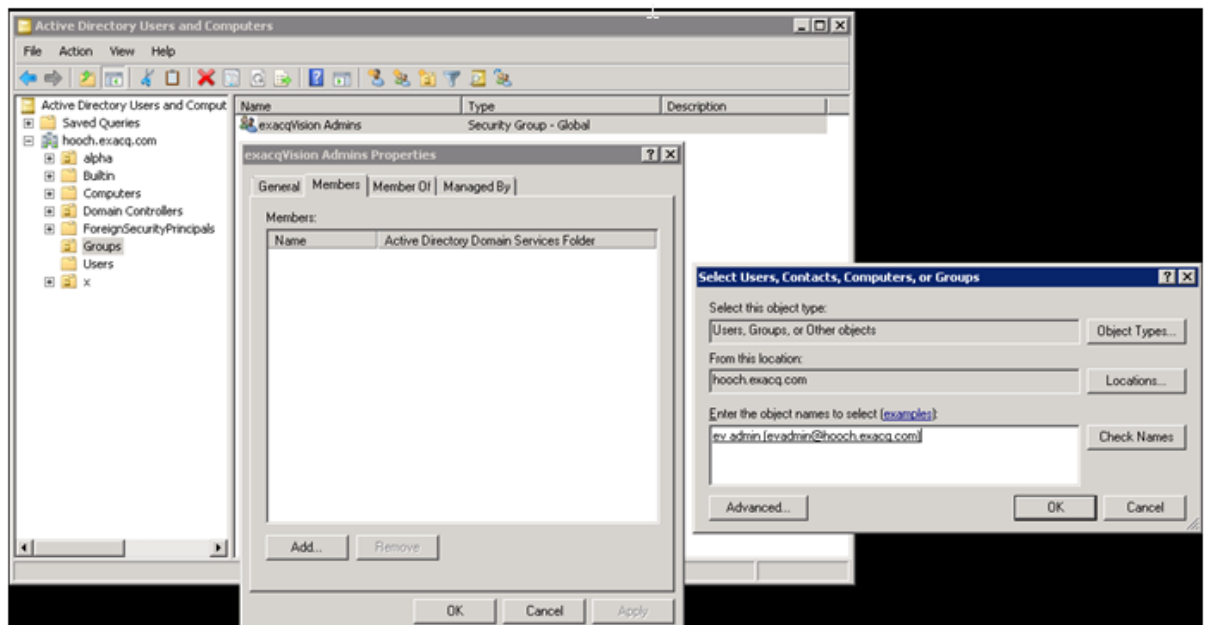


exacqVision Support Portal

3. Give that Group a Name. This example creates an exacqVision Admin Group.

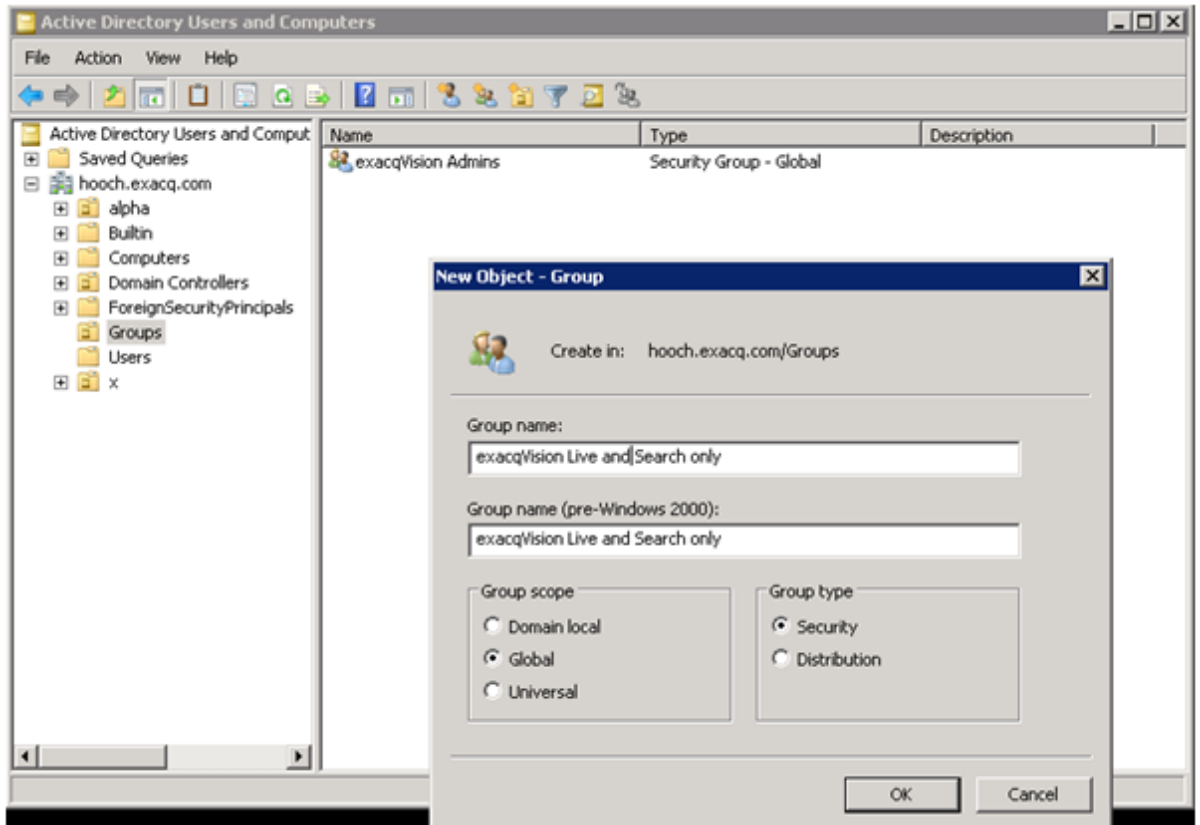


4. Add domain users to the new group.



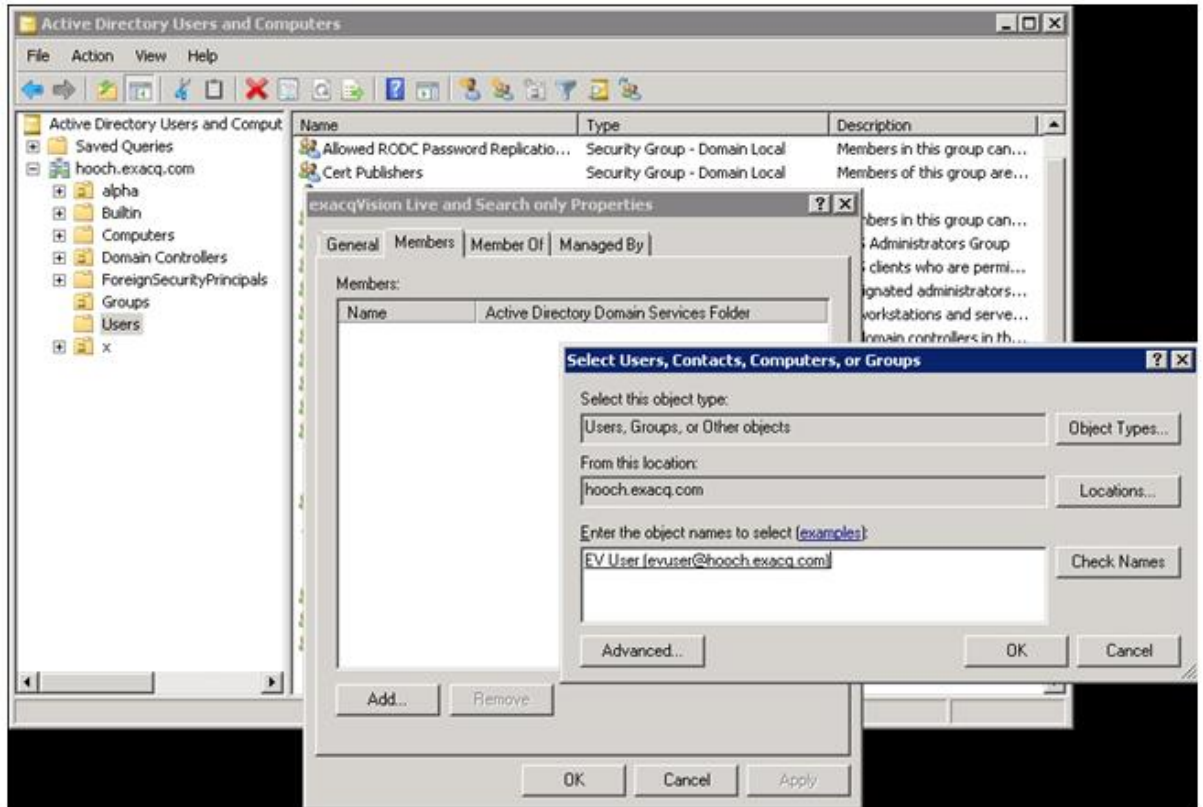
exacqVision Support Portal

5. Create additional groups. This example will create a Live and Search Only group.



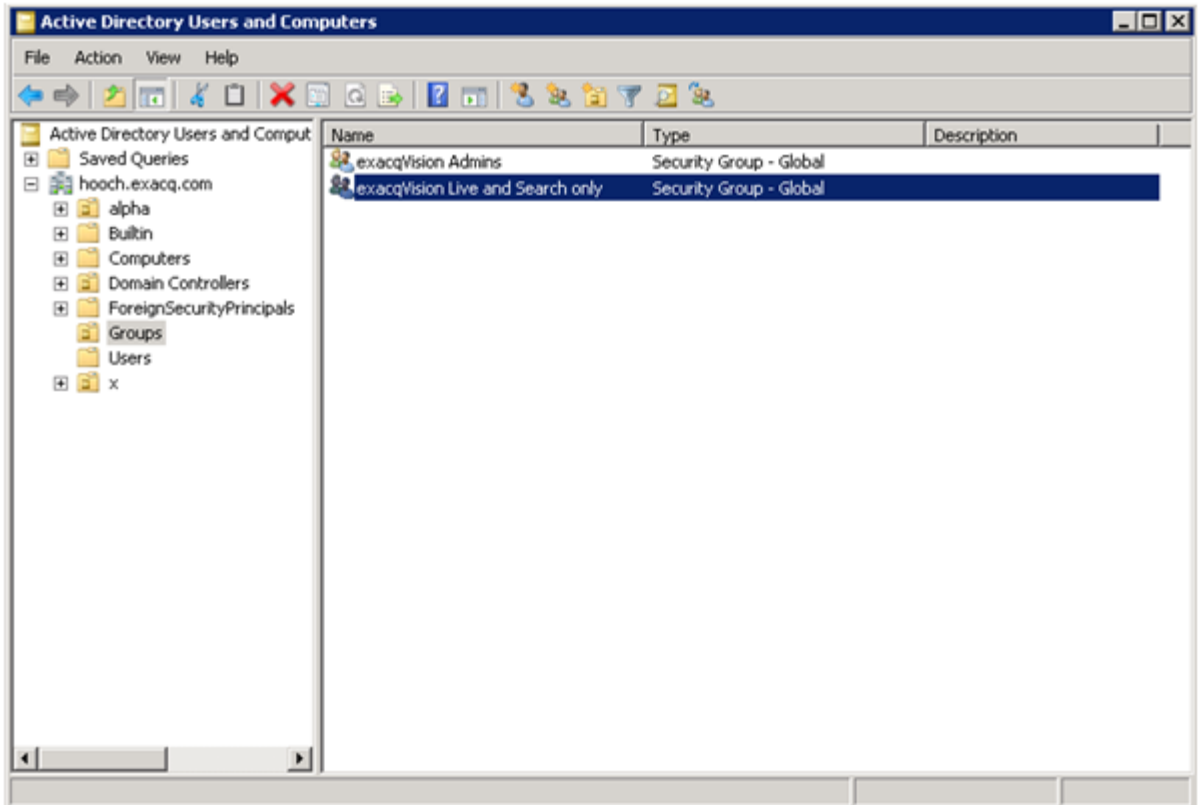
exacqVision Support Portal

6. Add domain users to the group.



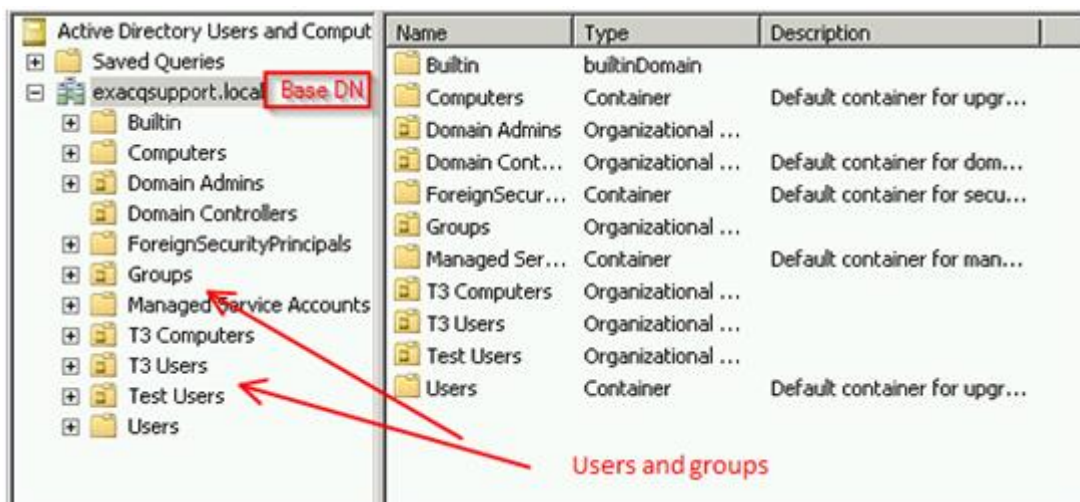
7. Now you have multiple groups to query in the exacqVision Client. This allows you to assign permissions to users based on their Directory Group.

exacqVision Support Portal



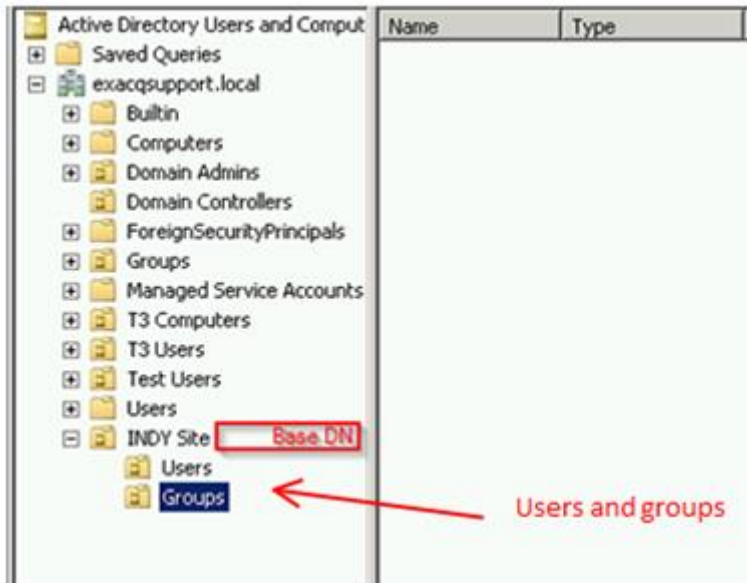
NOTE: Check with the system administrator for the correct LDAP Base DN for your situation. User and Group OUs/containers must be below (nested under) the Base DN, not equal to or above the Base DN. Binding will succeed, but users will not be able to log in.

Good:

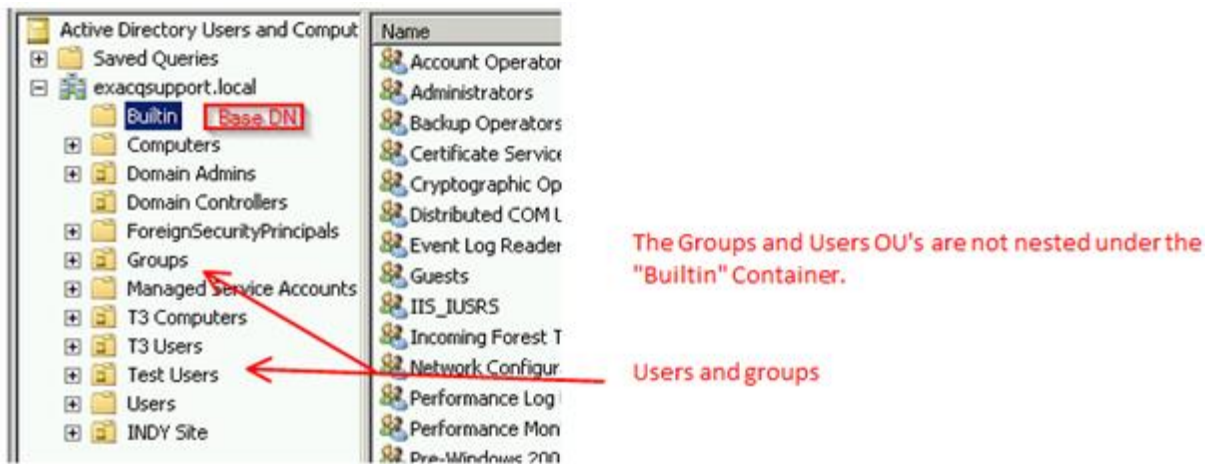


Better:

exacqVision Support Portal



Bad:

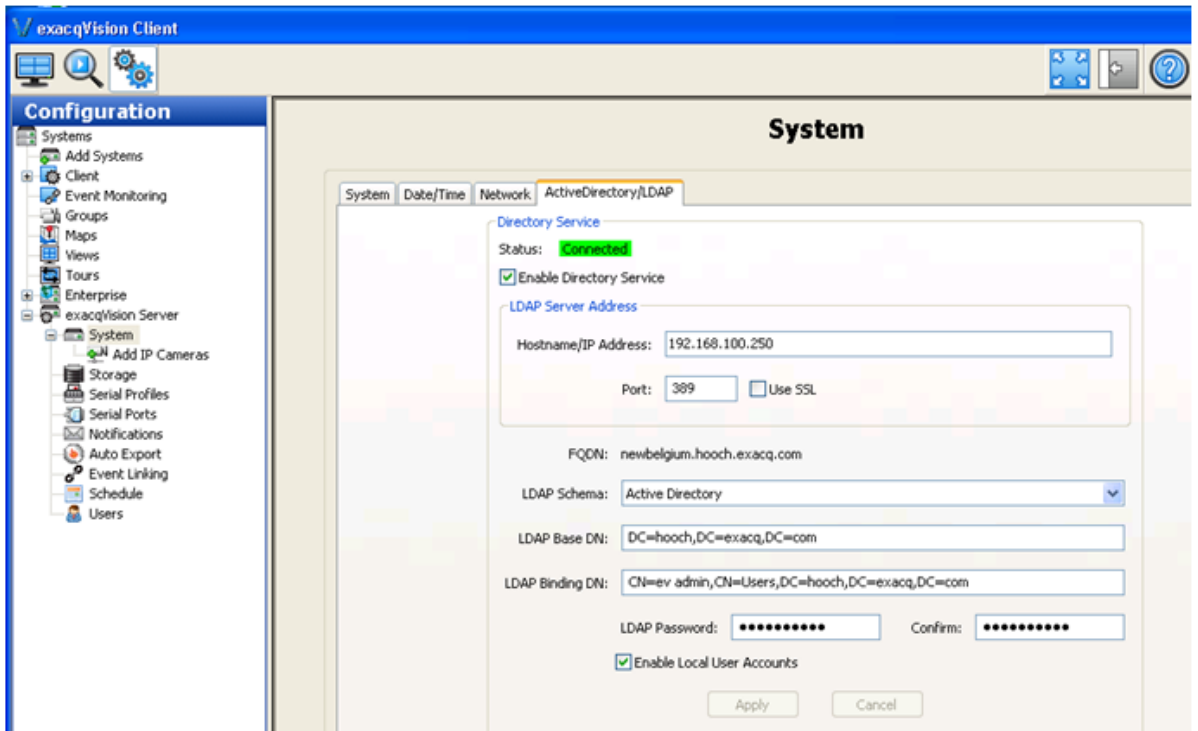


8. Log in to the client workstation with an exacqVision user account.



exacqVision Support Portal

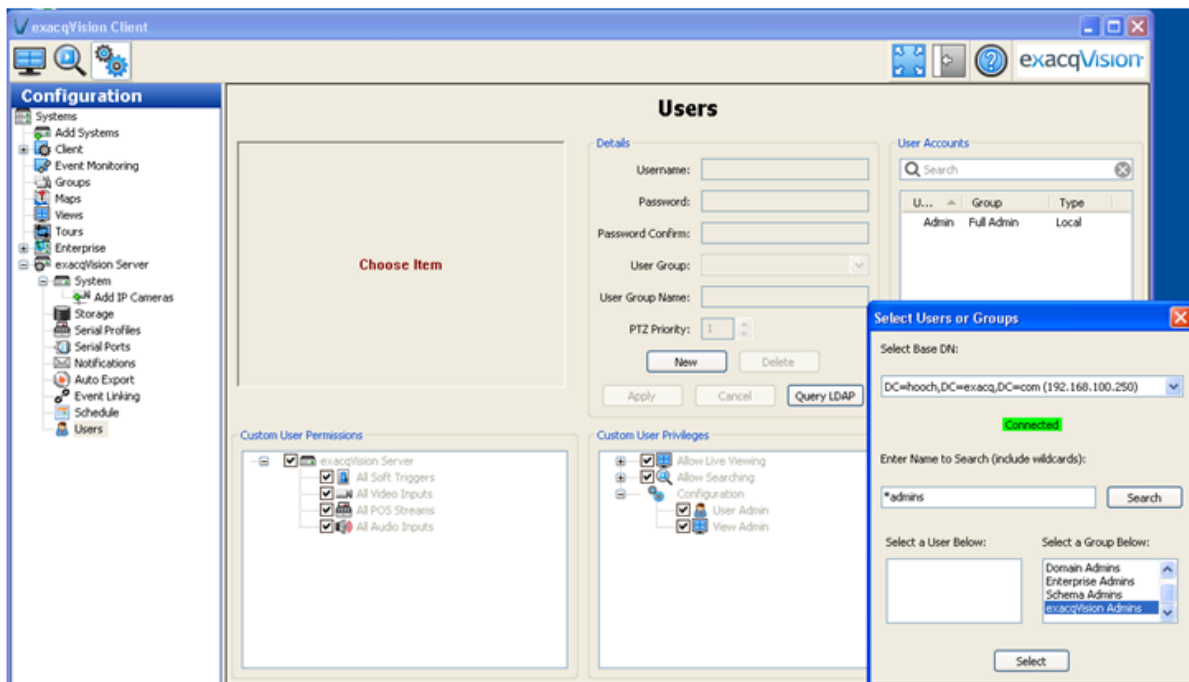
- Open the exacqVision Client and select the System tab on the Config (Setup) page. Enter the Base DN and Binding DN for the directory.
NOTE: Make sure the Base DN is at least one level above the Group container you will be querying.



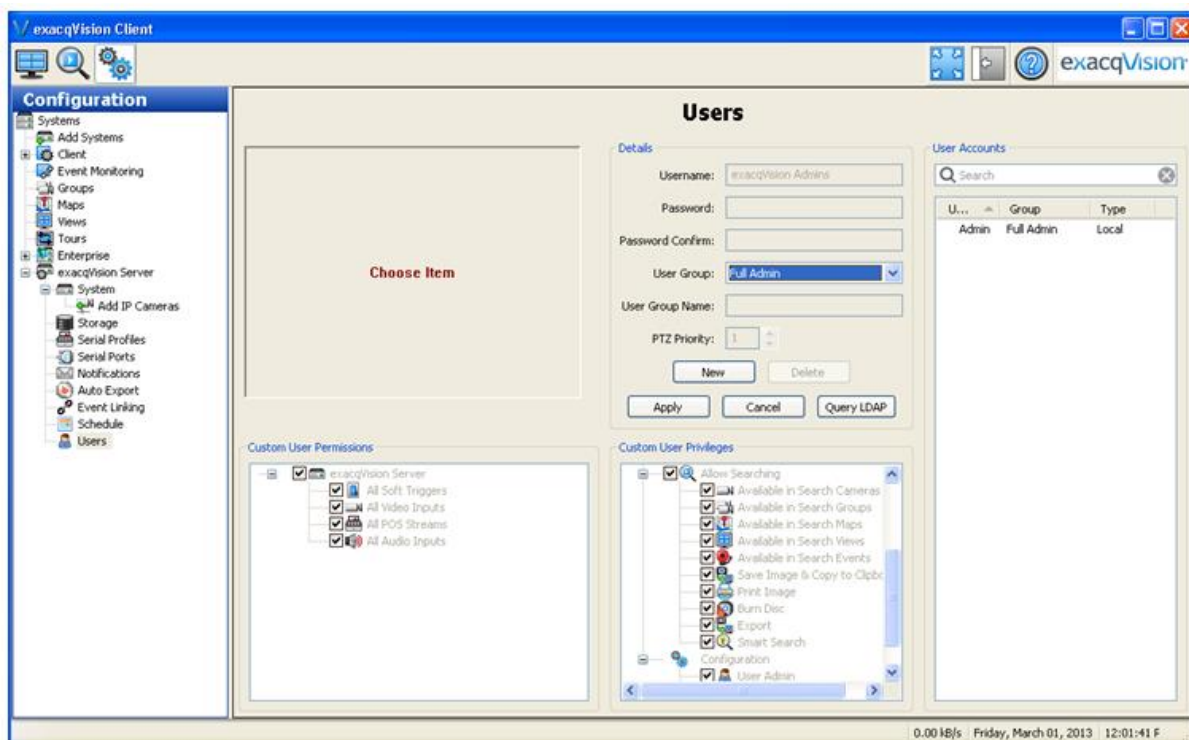
The status should now be Connected.

- To map each group created on the domain to an exacqVision user, select Users from the configuration tree and click Query LDAP. This will allow us to assign exacqVision permissions to all domain users in each group.

exacqVision Support Portal

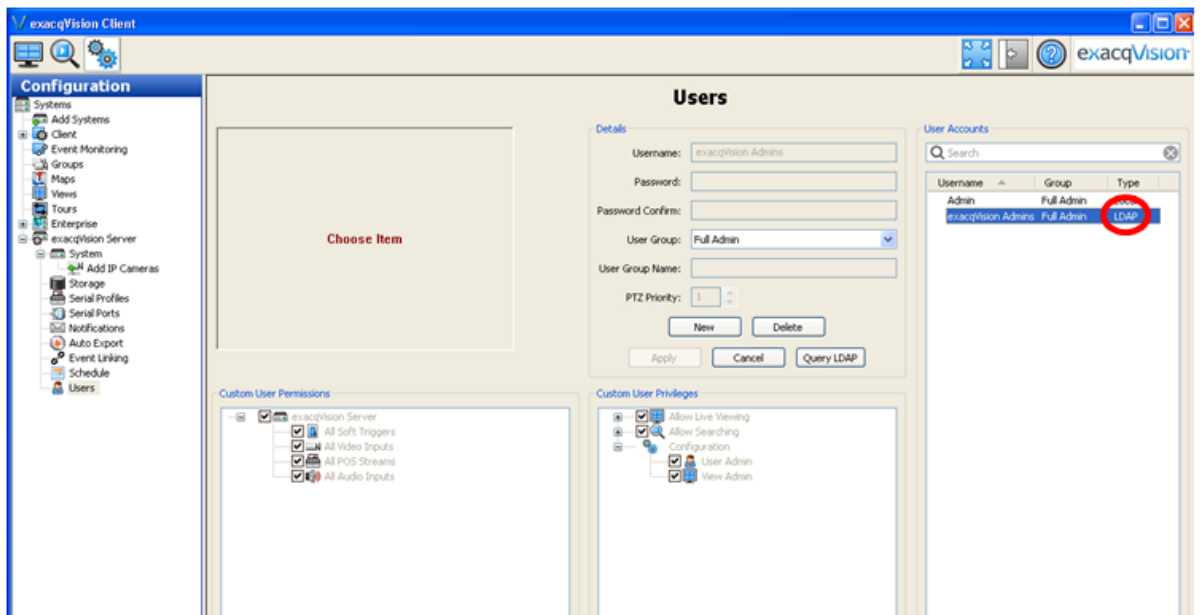


11. Select the group returned by the query and assign permissions to that group. This example gives full admin rights to the exacqVision Admins group.

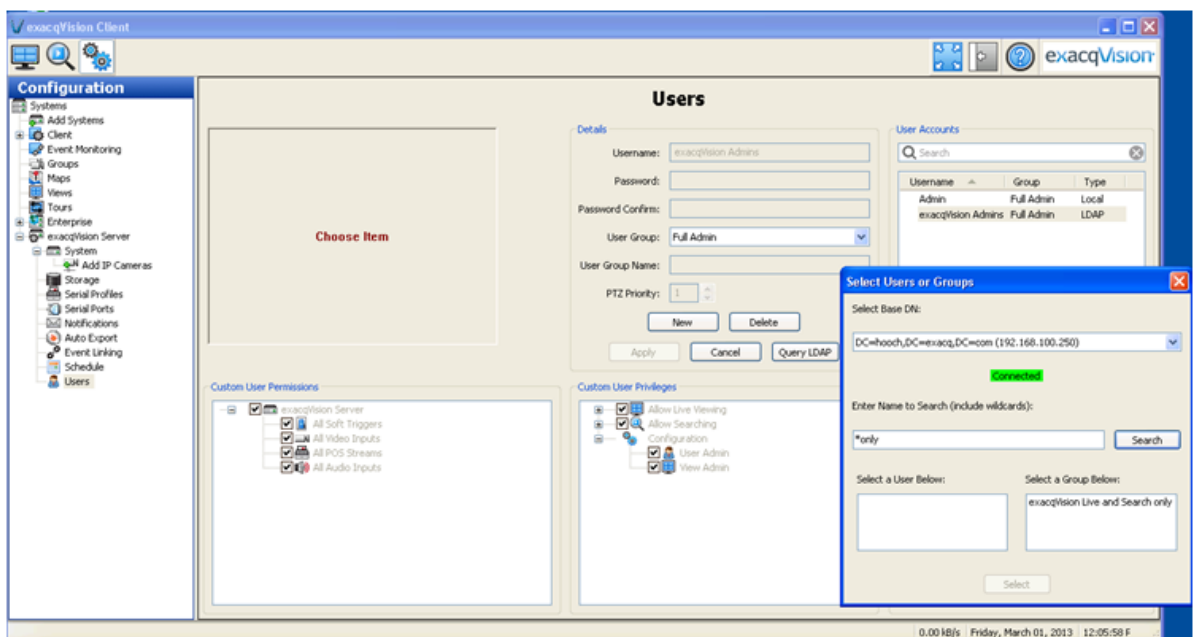


12. Click Apply. The group and all its domain users now have permissions, and the type is specified as LDAP.

exacqVision Support Portal

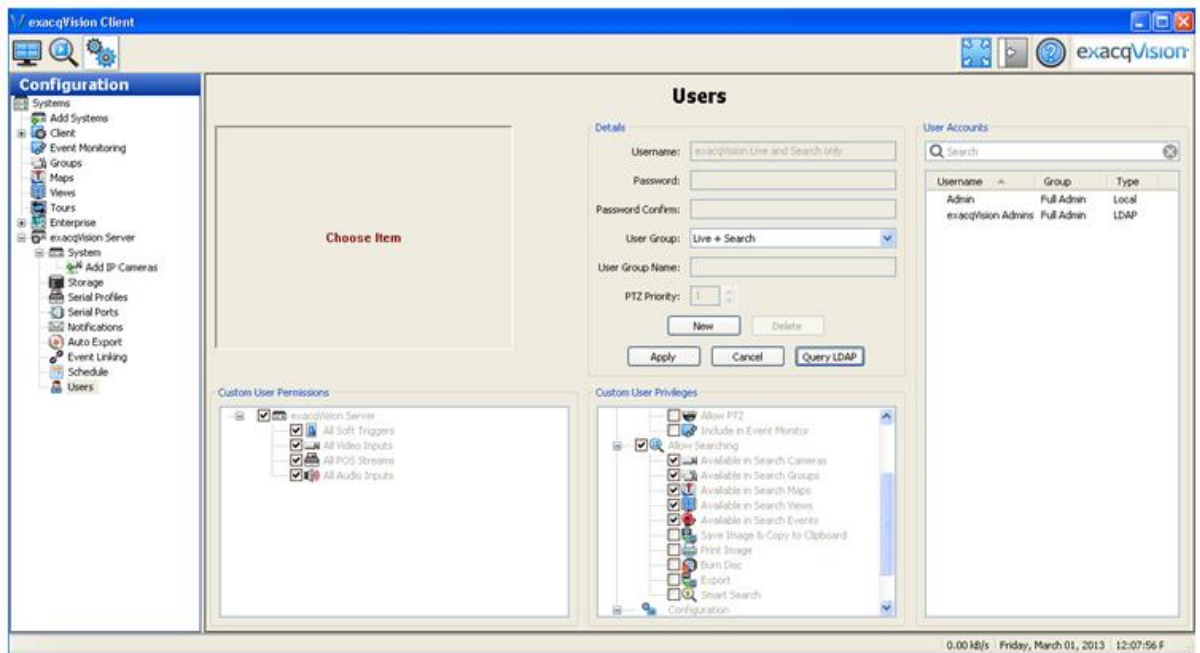


13. On the Users page, click Query LDAP and search for the next group that was created.

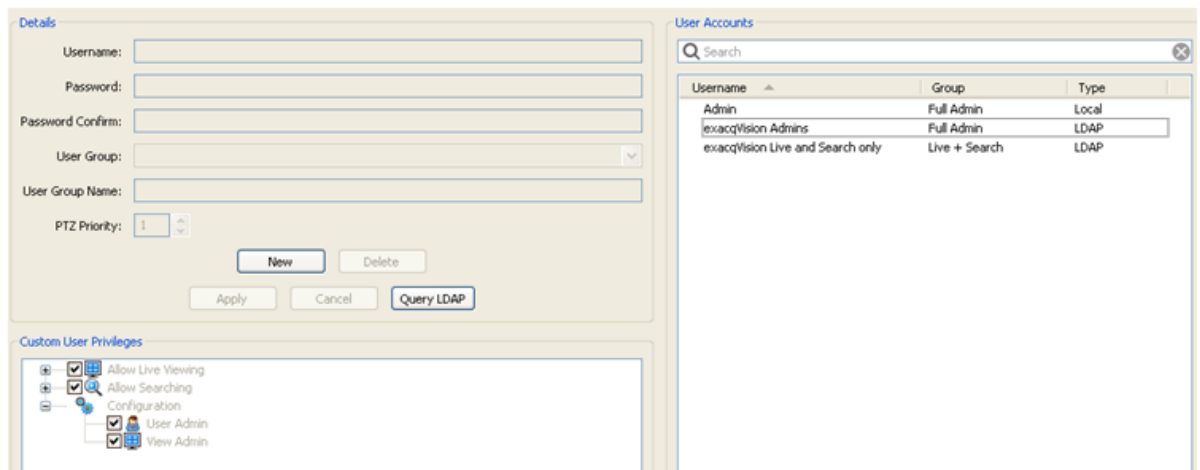


14. Add permissions for this specific group. This example selects the Live + Search permission for the Live and Search Only group.

exacqVision Support Portal

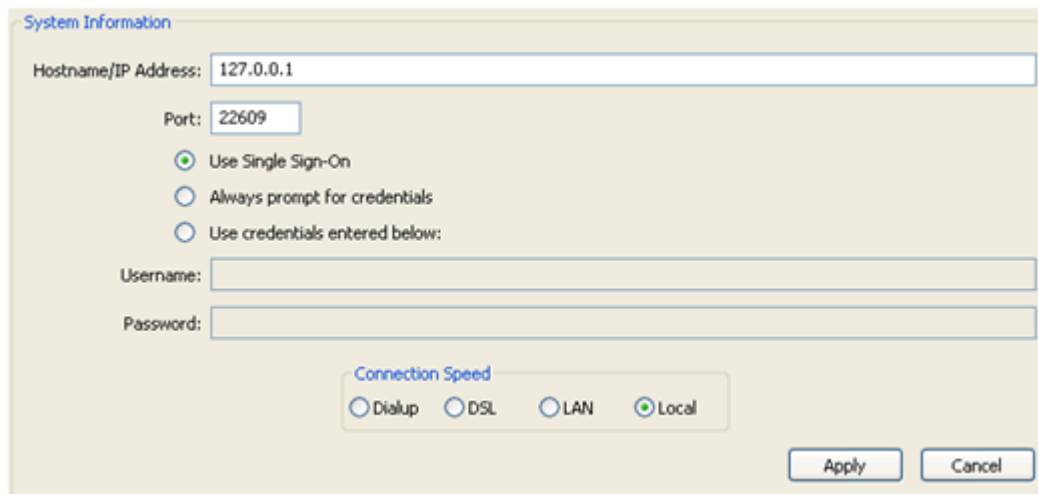


15. Now both groups are mapped on the exacqVision Server with the appropriate permission levels.



16. On the Add System page, select Use Single Sign-On so that exacqVision Client will pass the client computer's login credentials to the server for validation when it starts.

exacqVision Support Portal

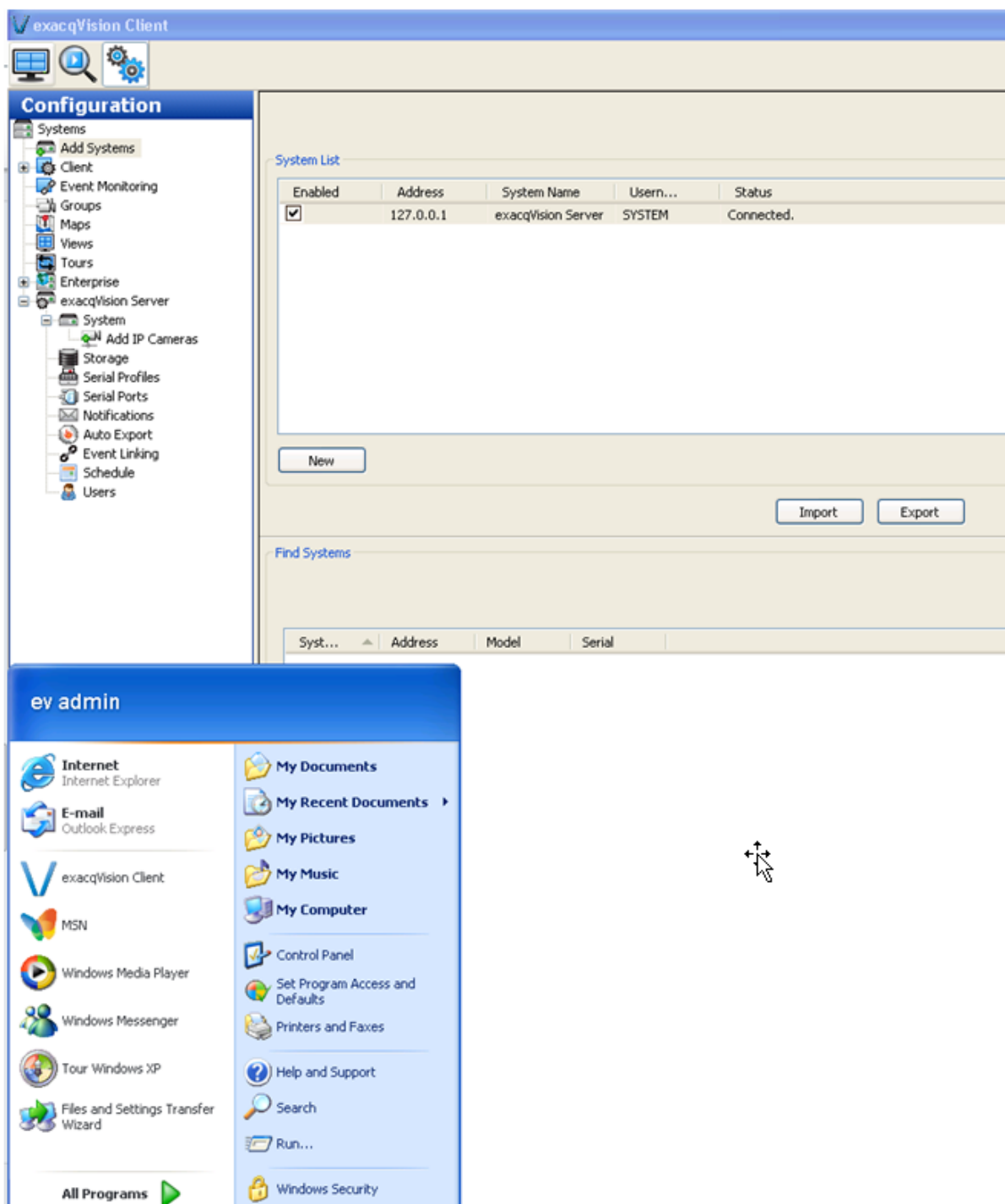


The screenshot shows a 'System Information' dialog box with the following fields and options:

- Hostname/IP Address: 127.0.0.1
- Port: 22609
- Use Single Sign-On (selected)
- Always prompt for credentials
- Use credentials entered below:
- Username: [empty field]
- Password: [empty field]
- Connection Speed:
 - Dialup
 - DSL
 - LAN
 - Local (selected)
- Buttons: Apply, Cancel

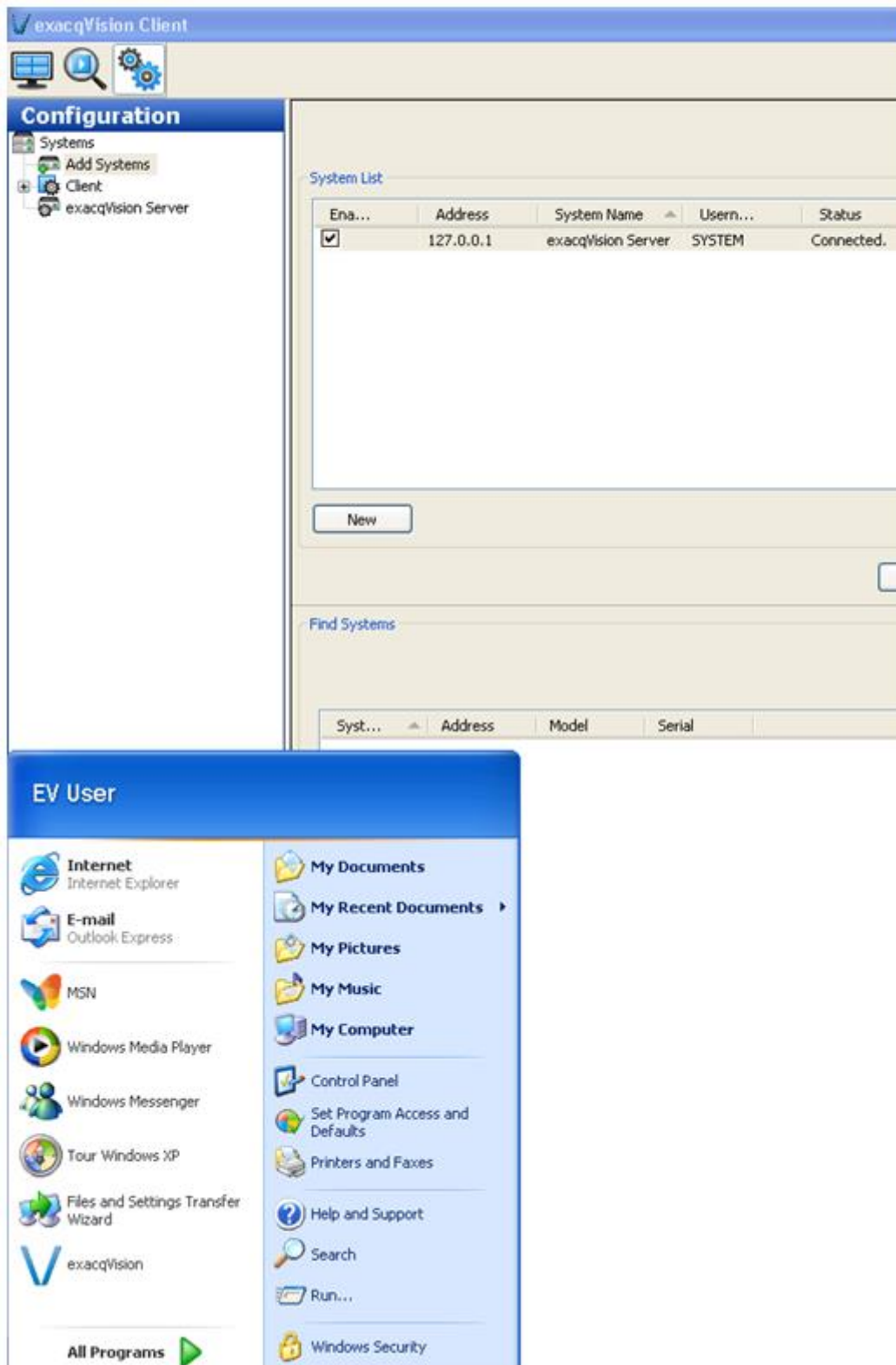
17. Because you are logged in to the Client workstation with an exacqVision Admin user account, the system will automatically log in to the server with these credentials.

exacqVision Support Portal



18. Now you can log out of the Client Workstation with admin credentials and log in as a Live and Search Only user. Notice that the account does not have any of the server configuration options available when logged in to the Admin group account.

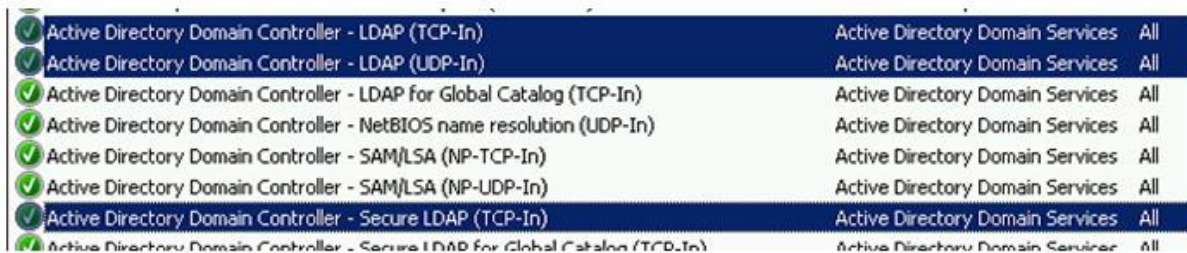
exacqVision Support Portal



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

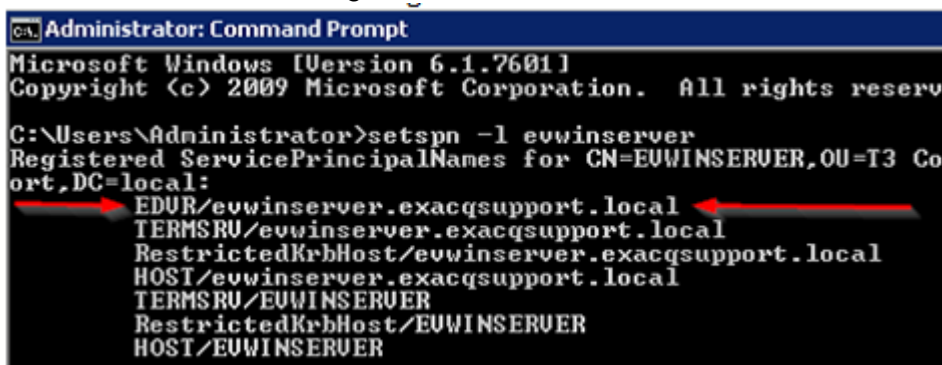
Re-imaging or Replacing System (Including Virtual Machines)

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. 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 serial` (where serial is the exacqVision Serial number, or mac_address for a 3rd party server).

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 Con
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

Created On: 11th February 2021

KB Number: KB-00284-284-210211

exacqVision Support Portal

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\bstovall>ping ewinserver

Pinging ewinserver.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:

1.
 1. Check DNS PTR records. Make sure the hostname and IP address are correct.
 2. Delete and add back the DNS record for the exacqVision server, if needed.
 3. Verify that you can resolve any FQDNs.
 4. 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.
 5. Verify that ports are open for 636 (secure LDAP) or 389 (LDAP).
 6. 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

1. The exacqVision server log could contain the following error:

StreamPI_____Error_____SSPIerror: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.

2. Make sure the User and Group OU/Container are nested under the Base DN (see discussion earlier in this document).
3. Can you ping all your DC FQDNs and resolve them from the client and server?
4. You may have entered your Service Principle Name (SPN) incorrectly. You can verify the SPN from a command prompt on the DC, enter `setspn -l hostname` (the hostname or 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 serial` (where *serial* is the exacqVision Serial number, or `mac_address` for a 3rd party server).