How can I enable LDAP for Autoform DM?

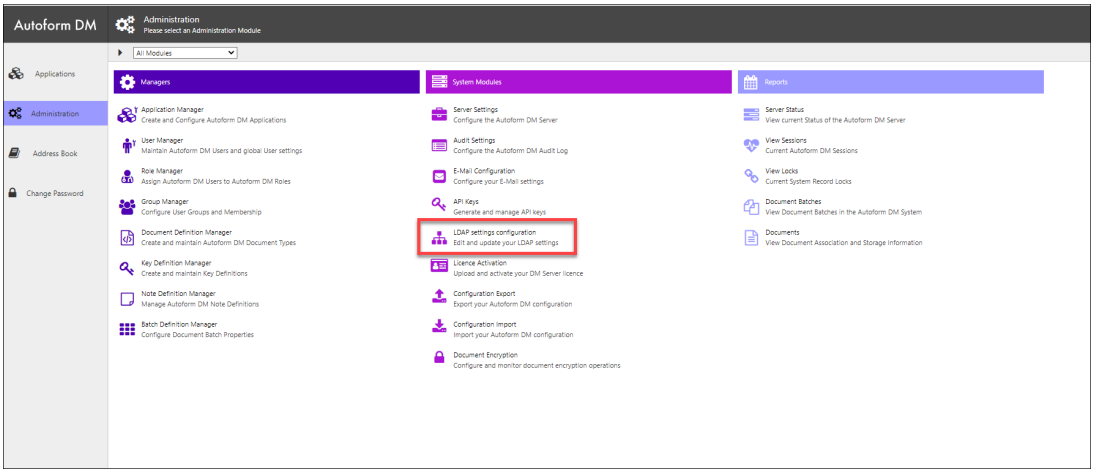
Ross Glover - 2024-06-21 - Comments (0) - Autoform DM FAQs

Autoform DM

DM can be configured to use the Windows Active Directory to obtain user login credentials and even allocate group access. Once LDAP is set up correctly, all user management can be done externally from DM, and as a result, users can use their Windows login to access DM as long they are in the relevant active directory groups.

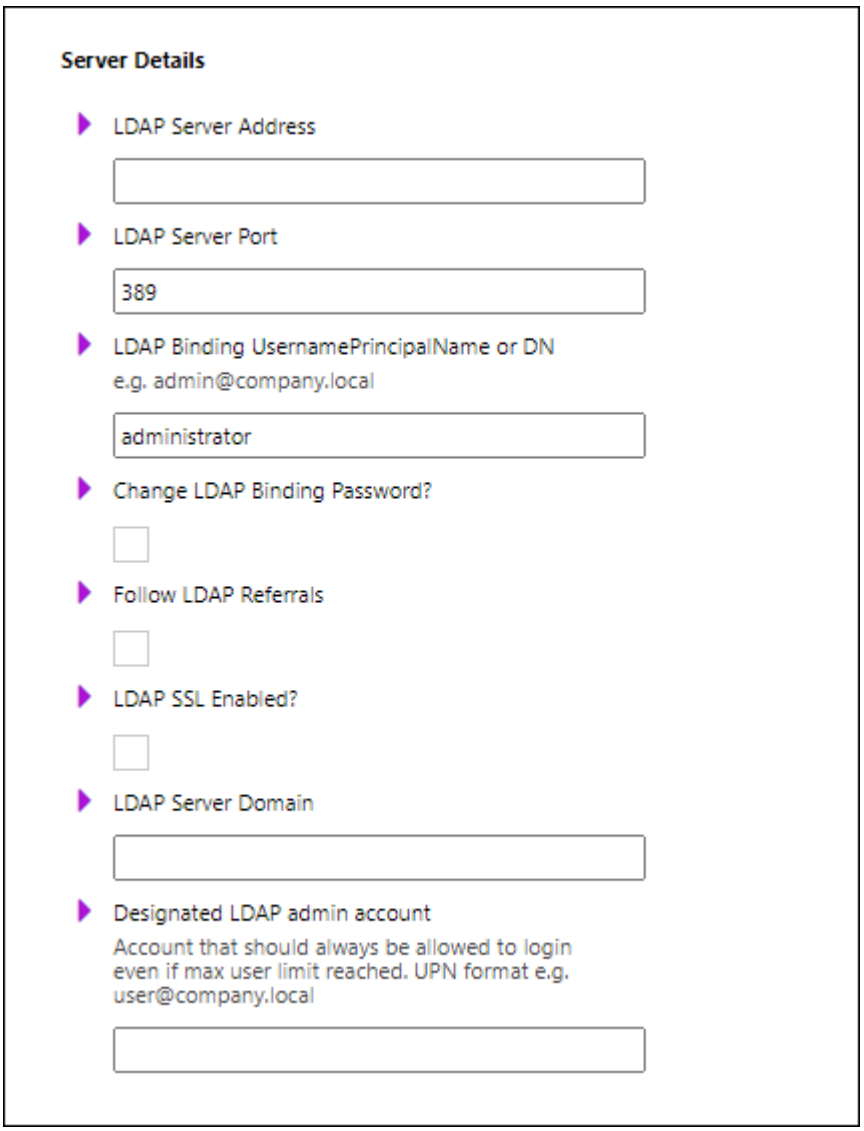
Depending on your DM version some of the options may appear differently. Most of the settings will be for whoever manages the Windows Active Directory to specify.

Navigate to the **LDAP Settings Configuration** from the **Administration** screen.



Server Details

This initial section is for providing DM with the information for the Active Directory.



LDAP Server Address: This will be the name or IP of the server which holds all the Active Directory settings.

We recommend defining the Domain instead of a specific Domain Controller if there are multiple DCs controlling the same Domain. So if one DC goes down then the other DC takes the role and DM remains connected.

LDAP Server Port: The port of the Active Directory Server.

LDAP Binding Username: Administrative username with full access to LDAP tree being searched.

Change LDAP Binding Password?: For changing the binding user's password.

Follow LDAP Referrals: Check for whether to use AD referring or not.

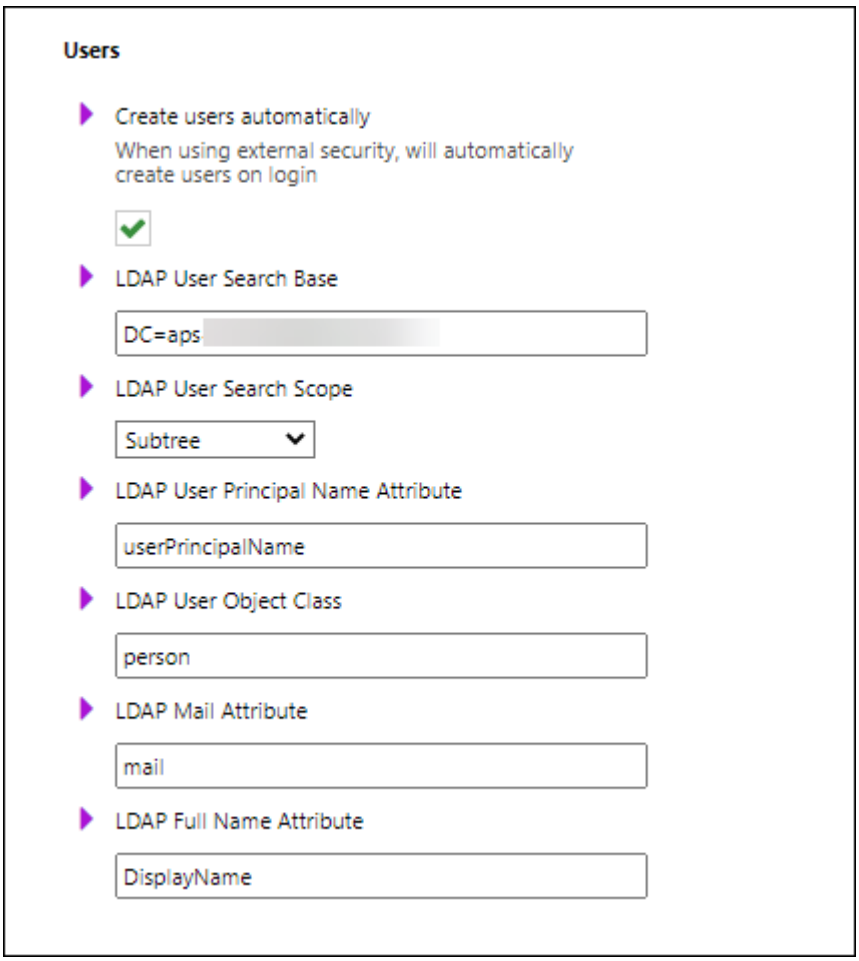
LDAP SSL Enabled: Secure LDAP communication with.

SSLLDAP Server Domain: The name of the domain Autoform DM/AD is installed on.

Designated LDAP admin account: Account to bypass license limitations for emergency access.

Users Details

This section is for providing the Active Directory settings for users.



Create users automatically: Automatically create users when logging into Autoform DM.

LDAP User Search Base: Specifies the tree location of the usernames in Active Directory for example CN=Users,DC=mydomain,DC=local.

LDAP User Search Scope: Number of levels to search for users beyond the User Search Base.

LDAP Username Attribute: The field within Active Directory that holds the login name (UID attribute) for the user selected. Over the version of *6.919 (included)* only UPN can be used (SamAccountName can't be used anymore).

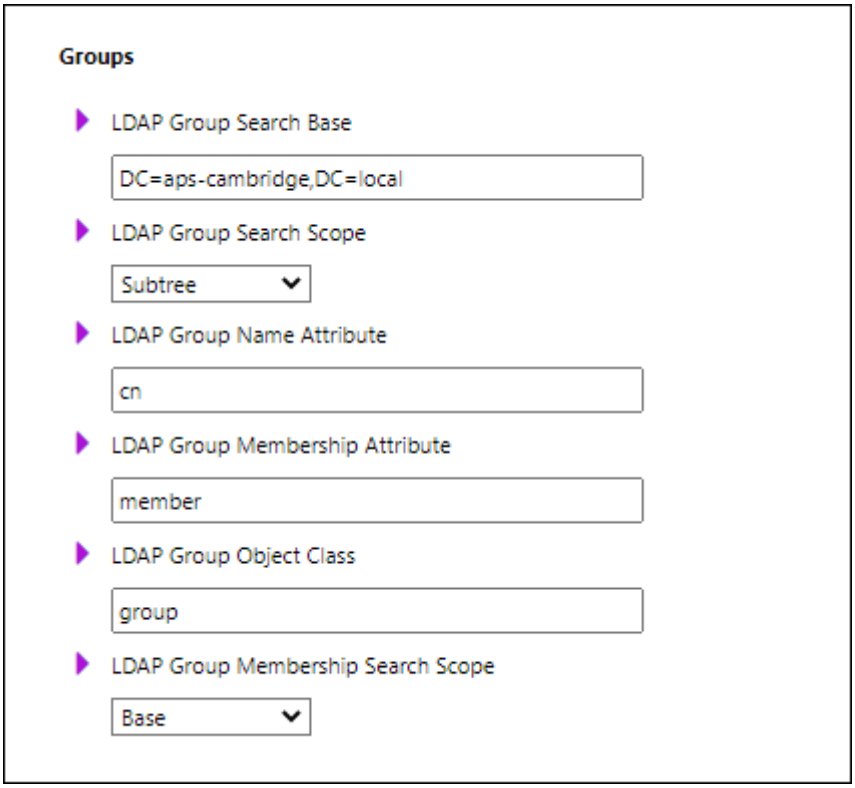
LDAP User Object Class: Used to limit results to users and not computer names etc, enter class name of a person. If this is not the default, change as appropriate.

LDAP Mail Attribute: The field that contains the email address of the user in Active.

LDAP Full Name Attribute: LDAP field that contains the full name of the user.

Group Details

This section is for providing the Active Directory settings for Groups.



LDAP Group Search Base: Specifies the tree location of the group names in Active Directory for example CN=Groups,DC=mydomain,DC=local.

LDAP Group Search Scope: Levels to search for groups beyond the Group Search Base.

LDAP Group Name Attribute: The field within Active Directory that holds the group name.

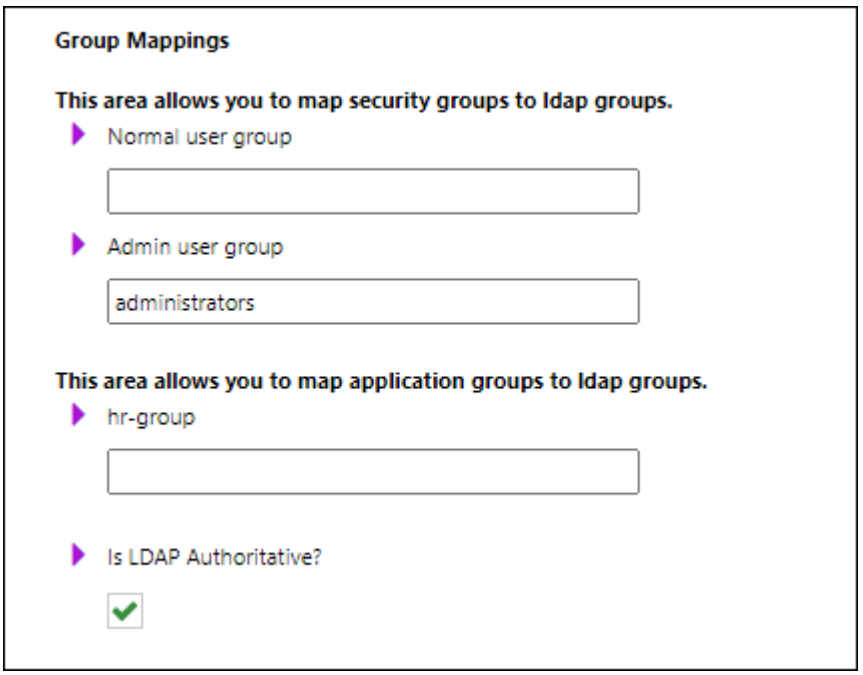
LDAP Group Membership Attribute: The field within AD that holds the member list of a group.

LDAP Group Object Class: Name of the group object class.

LDAP Group Membership Attribute Search Scope: Levels to search for group members beyond the base.

Group Mappings

This section is for mapping the groups within DM to groups within Active.



Normal User Group: Name of the user group in Active Directory that will contain users of DM.

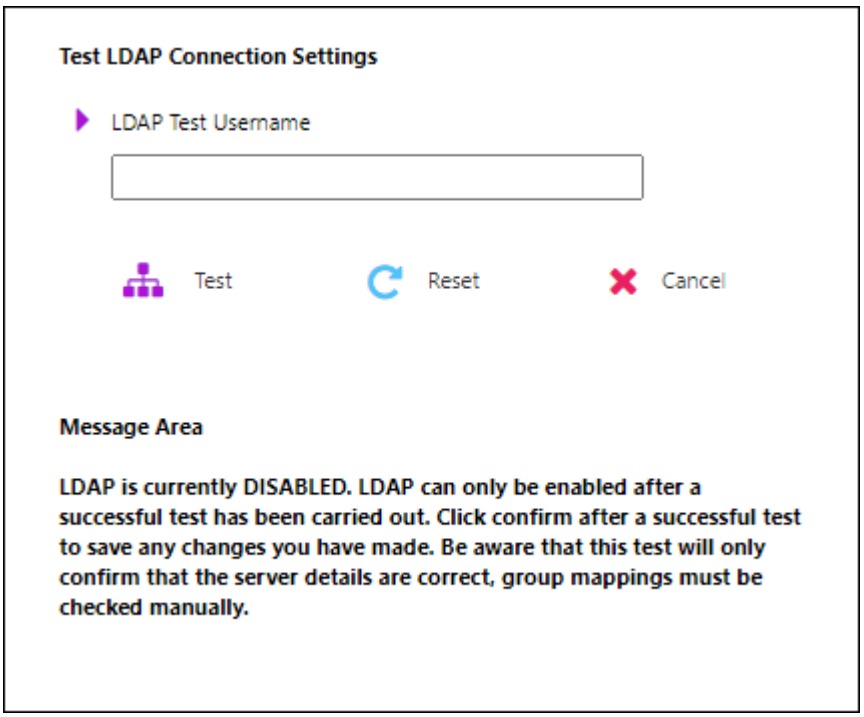
Admin User Group: Name of the user group is AD that will contain DM administrators.

LDAP Groups: It will then list any groups you have in DM and you can map these to groups in AD.

Is LDAP Authoritative? Designates whether DM will always rely on AD to get group/application access permissions or if it will still allow access to be set manually within DM.

Test LDAP Connection Settings

Before Saving any LDAP setting you must perform a successful test. To do this put a username in the box that exists in the Active Directory and press **test**. It will then display the results. If successful it will display the groups that the user belongs to and allow the option to enable LDAP. Select this to complete your LDAP configuration.



LDAPS

Some users may wish to implement LDAPS which is also something we support. The initial configuration is to set up as the LDAP configuration as above. Next, you need to import a root certificate from the LDAP Server Certificate Store into the JDK Certificate Store. The DM JDK is found in the DM installation folder ie: *C:\Program Files\Formpipe Software\Autoform DM\Server_x.x.x\jdkx.x.x_xx.*

Now follow these steps:

1. Launch the Command Prompt as an Administrator and navigate to the 'bin' folder within the 'jdk' folder mentioned above.

2. Run the following command:

Command:

```
keytool.exe -import -file  -alias DOMAINNAME -keystore
..\lib\security\cacerts
```

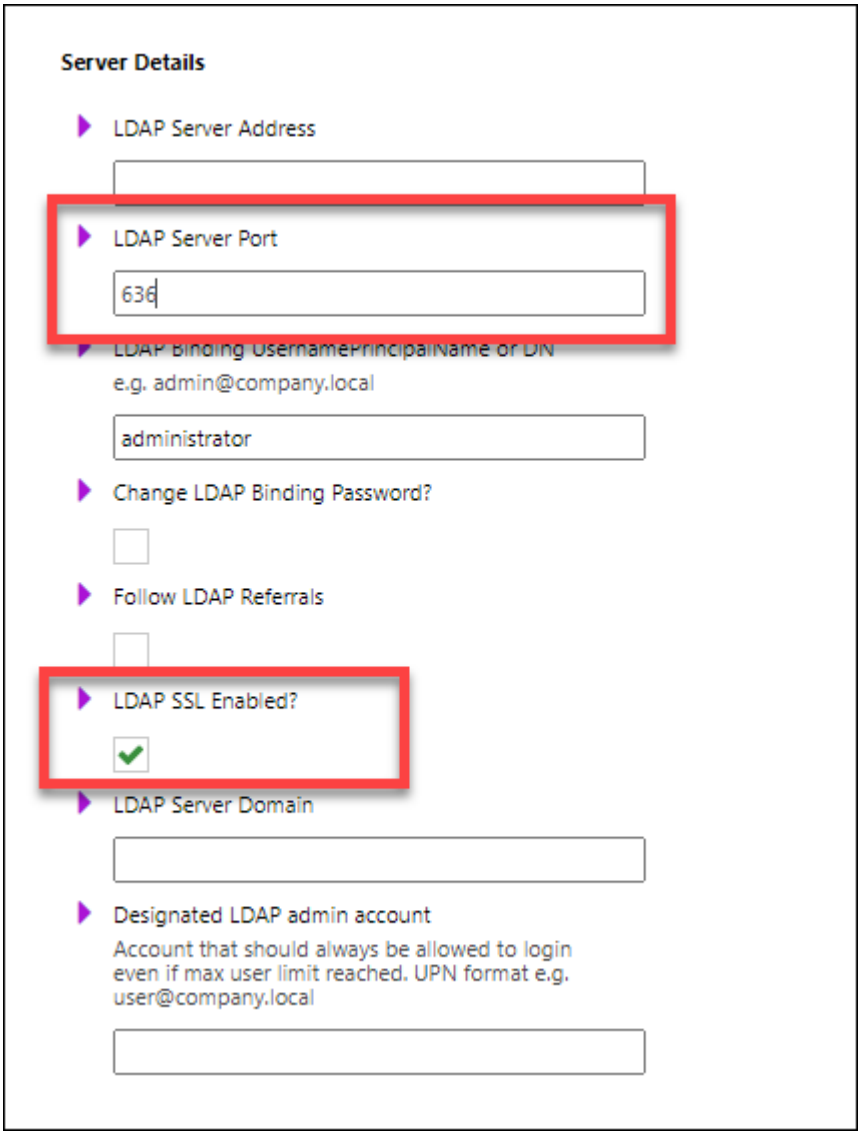
3. When you run this command you will be prompted for the Java cacerts password. By default this is 'changeit'.

4. Restart Autoform DM.

5. Once DM is back up, log in and navigate to the LDAP configuration screen.

6. Disable LDAP so that the configuration is revealed.

7. Change the **LDAP Server Port** to 636 and select the **LDAP SSL Enabled** checkbox.



8. As with standard LDAP, you need to perform a successful test before you can enable LDAPS.