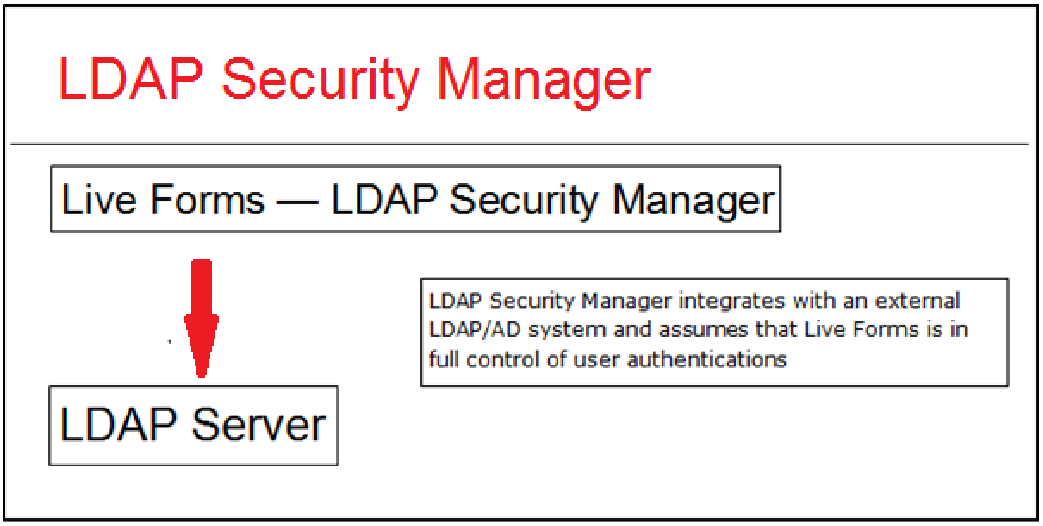
Configuring the LDAP Security Manager LDAP(s) for Cloud tenants

Connecting your frevvo Cloud tenant to your on-premise LDAP server requires some extra steps in addition to setting up the LDAP Security Manager tenant screen. Secure LDAP provides encrypted communication between Live Forms and LDAP. Refer to the Secure LDAP Configuration topic below and our blog article, LDAP in the cloud which discusses the topic in more detail.

> Safari browsers later than v5.1.7 running on Windows is no longer supported. Issues were found when using Safari with LDAP - SSO.



LDAP Security Manager integrates with an external LDAP/AD system and assumes that Live Forms is in full control of user authentications

On This Page:

Secure LDAP Configuration

Live Forms will be connecting to your LDAP server over the network. Here are two methods to secure the LDAP connection:

1. Simple authentication over SSL - To enable SSL use the **ldaps** scheme in your LDAP tenant configuration in place of **ldap** and use port 636. This is supported by older LDAP products such as AD 2000. **It is important that the hostname in the certificate matches the hostname in your ldaps url.**
2. Simple or external SASL authentication over TLS (Transport Layer Security) - To enable this method check the TLS checkbox in your

LDAP tenant configuration. TLS is used by the LDAP v3 standard in products such as AD 2003 and above. TLS uses the standard LDAP port 389.

When using either of these two methods, the recommended approach is to use a CA signed certificate. If you do not have a CA signed certificate then you can use a self-signed certificate.

> Self signed certificates are not supported for Live Forms Online. Although they are supported for Live Forms in-house, use of self-signed certificates is not recommended.

Finally you need to install your signed or self-signed certificate. You can import the certificate into a keystore that Live Forms can access and trust. Follow the instructions for your keystore. If Live Forms is installed in a tomcat server, the tomcat keystore can be used. Refer to this Apache Tomcat website for instructions .

External SASL and pooling are currently not supported. This is planned for a later release.

Configuring LDAPs for your Cloud tenant

Once your Live Forms Online cloud hosted tenant has been provisioned for production use, follow the steps below to configure your tenant to use the frevvo LDAP/Active Directory Security Manager to integrate with your company's AD server:

1. Confirm that your LDAP/AD server is running LDAPs with a third-party certification authority.
    a. It is likely your LDAP/AD server already has a CA certificate installed. But if not, this Microsoft KB article tells you how to do this: **It is important that the hostname in the certificate matches the hostname in your ldaps url.**
    b. **Your LDAP/AD server must be running LDAPs with a third-party certification authority BEFORE performing Step 4.**

    > Self signed certificates are not supported for Live Forms Online tenants

2. Customers that use firewall white-listing must add the frevvo cloud outgoing server **IP 54.86.85.105 (host outgoing.frevvo.com)** to the list.
3. Email your frevvo Security Manager resource. The frevvo infrastructure team will white label your server and port using the information provided.
    a. Provide frevvo with the following:
        i. **the DNS Name(s) of the machine(s) hosting your AD server AND the IP Address or range of IP Addresses (in the case where your LDAP config is fault tolerant) of the machine(s) hosting your AD server.**

4. **STOP**:
    a. Wait for a reply email from your frevvo Security Manager resource letting you know that the frevvo infrastructure team has completed the white listing of your IP(s) on port 636 (ssl) or port 389 (TLS) in our firewall and verified connectivity.
5. Once you receive this white listing confirmation email verify that you have completed:
    a. the Prerequisite Tasks listed below
    b. collected the information in the Key Information to Collect topic below
6. Go to https://app.frevvo.com
    a. Login as your tenant admin
    b. Click on **the Edit tenant** link
    c. Change the security manager to the LDAP Security Manager.

    > If you have developed applications/forms/flows in your starter/trial cloud tenant that you want to preserve, download them to your desktop as a backup **BEFORE** changing the existing Security Manager to the LDAP Security Manager.

    d. Change the LDAP properties to your company's AD server following the instructions listed below
    e. Save your tenant AD configuration settings
    f. Verify that your tenant is now connected to your company AD server

Prerequisite Tasks

Active Directory Customers using LDAP **must** ensure **frevvo.TenantAdmin and frevvo.Designer groups** are specified on your LDAP/AD server. The group names must be spelled as shown. Upper/lower case may be a factor for Open LDAP systems.

- Tenant admin users must be assigned to the **frevvo.TenantAdmin** group.
- Designer users must be assigned to the **frevvo.Designer** group.

- Contact the frevvo Customer Success team to schedule your Security Manager configuration.
- frevvo Best Practice recommends that you create a user account in your Active Directory that will house all of your deployed Production forms/flows. This user can be named anything i.e.frevvoProduction but it must be a member of the frevvo.Designer group
- If you want to preserve Applications/Forms/Flows developed in your trial/starter tenant to your desktop, perform these steps **BEFORE** changing the Security Manager. :
    1. Download the Applications/Forms/Flows that you want to preserve to your desktop as a backup. Do this for all Live Forms user accounts that have Applications/Forms/flows that you want to keep.
    2. When the backup of all Applications/Forms/flows is completed, delete the user accounts in your Default Security Manager tenant.
- There are two additional roles in Live Forms - **frevvo.Publisher** and **frevvo.ReadOnly.** These roles are optional.
    - In order to give a user the frevvo.publishers role, create the **frevvo.Publisher** group in your AD and assign users to it. Refer to the Administrator Best Practices for an explanation of this role.
    - In order to give a user the frevvo.ReadOnly role, create the **frevvo.ReadOnly** group in your AD and assign users to it. Following frevvo Best Practice eliminates the need for this role.

Configuring Live Forms and LDAP/Active Directory

Live Forms users and groups can be maintained externally in systems such as Active Directory or Open LDAP. Follow these steps to integrate Live Forms and your LDAP server:

1. Collect the key information listed below and verify the Prerequisite Tasks have been performed.
2. Create a tenant with the **LDAP Security Manager** class.

Key Information to Collect

Before configuring the LDAP/Active Directory Security Manager, you will need the following information:

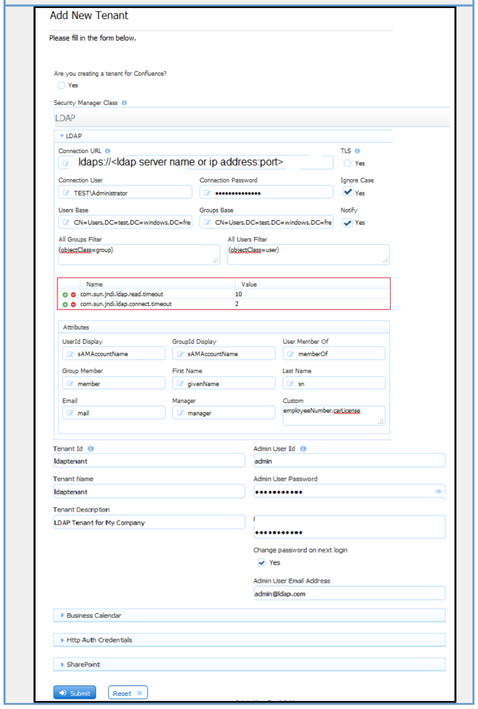
- LDAP server name or ip
- LDAP server port
- User name and password with proper permissions to access and browse LDAP.
- LDAP groups and/or users that will be considered Live Forms **designers**. These users will be able to create forms and flows in frevvo.
- LDAP groups and users that will be considered Live Forms **administrators**.
- LDAP groups and users that will be considered Live Forms **publishers**. This role gives a user the permission to go to the home page of every other tenant user.
- LDAP groups and users that will be considered **ReadOnly**.
- LDAP user and groups base filters
- LDAP all users and all groups filters
- LDAP the attribute names in your Active Directory for UserId Display, GroupId Display, User Member Of, Group Member, First Name, Last Name, Email and Manager (optional)

Create/Edit a tenant with the LDAP/Active Directory Security Manager

The connection to your LDAP server is configured at the tenant level.

1. Login to your Live Forms as the tenant admin
2. Click on **Manage Tenants**
3. You will see a page where the current tenants are listed. If this is a new installation you will only see the default tenant **d**
4. Click on the
   ⊕
   plus icon to add a new tenant or click the **Edit Tenant** link to edit an existing one.
5. Configure the tenant for the LDAP Security Manager:
    a. Choose **LDAP Security Manager**.from the **Security Manager Class** drop down.

Add New Tenant Screen



Add New Tenant

Please fill in the form below.

Are you creating a tenant for Confluence?
□ Yes

Security Manager Class
LDAP

LDAP

Connection URL: ldaps://<ldap server name or ip address:port>
TLS: □ Yes

Connection User: TEST\Administrator
Connection Password: •••••••••••••••
Ignore Case: ☑ Yes

Users Base: CN=Users,DC=test,DC=windows,DC=fre
Groups Base: CN=Users,DC=test,DC=windows,DC=fre
Notify: ☑ Yes

All Groups Filter: (objectClass=group)
All Users Filter: (objectClass=user)

Name	Value
com.sun.jndi.ldap.read.timeout	10
com.sun.jndi.ldap.connect.timeout	2

Attributes

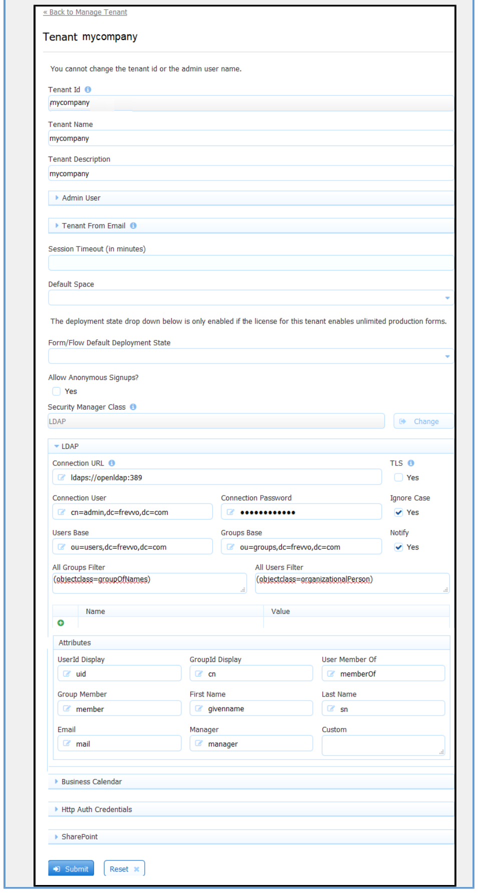
UserId Display: sAMAccountName
GroupId Display: sAMAccountName
User Member Of: memberOf
Group Member: member
First Name: givenName
Last Name: sn
Email: mail
Manager: manager
Custom: employeeNumber,carLicense

Tenant Id: ldaptenant
Admin User Id: admin
Tenant Name: ldaptenant
Admin User Password: •••••••••••
Tenant Description: LDAP Tenant for My Company
•••••••••••

Change password on next login
☑ Yes

Admin User Email Address: admin@ldap.com

Edit Existing Tenant Screen



« Back to Manage Tenant

Tenant mycompany

You cannot change the tenant id or the admin user name.

Tenant Id: mycompany
Tenant Name: mycompany
Tenant Description: mycompany

Session Timeout (in minutes):

Default Space:

The deployment state drop down below is only enabled if the license for this tenant enables unlimited production forms.

Form/Flow Default Deployment State:

Allow Anonymous Signups?
□ Yes

Security Manager Class: LDAP

LDAP

Connection URL: ldaps://openldap:389
TLS: □ Yes

Connection User: cn=admin,dc=frevvo,dc=com
Connection Password: •••••••••••••
Ignore Case: ☑ Yes

Users Base: ou=users,dc=frevvo,dc=com
Groups Base: ou=groups,dc=frevvo,dc=com
Notify: ☑ Yes

All Groups Filter: (objectclass=groupOfNames)
All Users Filter: (objectclass=organizationalPerson)

Name	Value

Attributes

UserId Display: uid
GroupId Display: cn
User Member Of: memberOf
Group Member: member
First Name: givenname
Last Name: sn
Email: mail
Manager: manager
Custom:

a. Enter your LDAP Configuration Properties. Alternatively, you can start off from one of the sample configurations and provide only the key information listed above. See above for information on the TLS checkbox.

The Name/value table highlighted in the image allows you to configure up to 10 additional LDAP properties. See this Oracle website for a complete list of all available LDAP properties. For example, you can configure Live Forms to ignore or follow referrals.

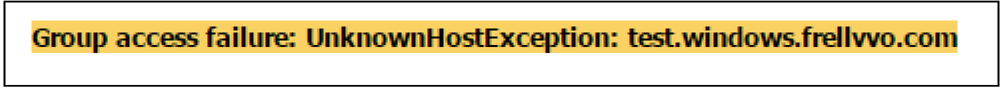
Setting the java.naming.referral property to a value of "ignore" in the Name/Value table configures Live Forms to ignore referrals. Consult your LDAP Administrator for the details.

b. If you are creating a new tenant:
   i. Enter a tenant id, a tenant name and description.
   ii. The **Max Concurrent Users** is the maximum allowed by your license or less.
   iii. Specify the LDAP User ID that will have the tenant admin permission. If editing an existing tenant, verify that the tenant admin user id is the LDAP user id for the tenant admin.
c. Click Submit. You will see your new tenant in the tenant list if the connection to your LDAP server is successful.

The **Ignore Case** and **Notify** checkboxes are checked by default. It is recommended that you leave them checked. Refer to Mixed or Upper case User Names topic for an explanation of the Ignore Case option.

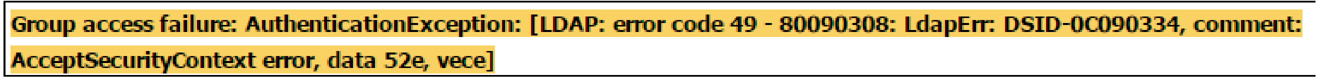
The **Notify** checkbox determines whether the task notification emails setup in Live Forms flows are sent or not.

Clicking the submit button tests the connection. Any errors are displayed at the top of the form. Here is an example of an error when there is a typo in the LDAP server name:



Group access failure: UnknownHostException: test.windows.frellvvo.com

Here is another example if the connection password is not correct



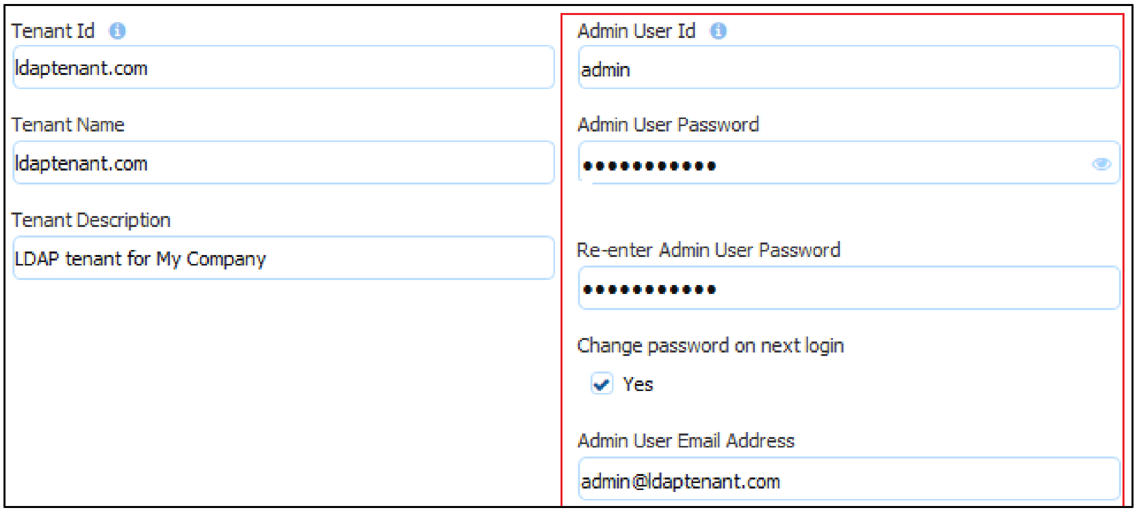
Group access failure: AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 52e, vece]

Refer to FAQ - Live Forms and LDAP for more troubleshooting information.

LDAP(s) Built-in Admin

A Tenant admin can login directly to Live Forms or login with a user id who has been given tenant admin permissions in your Active Directory.

When you create a new tenant you are prompted to set up a tenant admin user id, password and email address. This tenant admin does not authenticate via your LDAP IDP. It only exists in Live Forms. If you experience an issue with your LDAP configuration such that you can't login as an Active Directory authenticated user, use this account to login to your tenant as a tenant admin in order to fix your configuration issue. The built-in admin is able to access the Live Forms tenant admin functions if your LDAP Server should become inaccessible. Only one built-in tenant admin account is supported.



Tenant Id: ldaptenant.com
Tenant Name: ldaptenant.com
Tenant Description: LDAP tenant for My Company

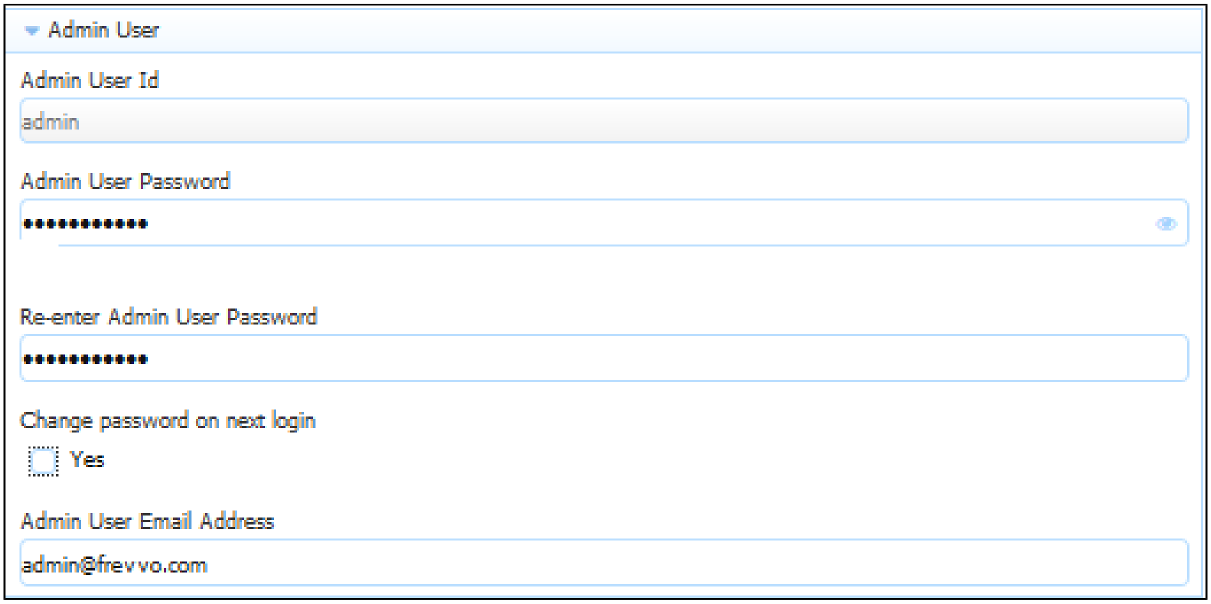
Admin User Id: admin
Admin User Password: ••••••••••••
Re-enter Admin User Password: ••••••••••••
Change password on next login: ☑ Yes
Admin User Email Address: admin@ldaptenant.com

Browse this URL to login as the built-in admin: <base_URL>/frevvo/web/admin/login. When specified, Live Forms will prepend the base URL to the URLs in your Form/Document Actions. The <base_URL> is typically http(s)://<your servername>:<port>. For cloud customers the <base> is always https://app.frevvo.com.

- You must use the admin specific URL - <base-url>/frevvo/web/admin/login - to login as the built-in admin.
- Non admin users can also login using the admin specific URL.

If your tenant originally used the Default Security Manager and then you changed to the LDAP Security Manager, this tenant admin account has already been setup. If you have forgotten the password, you can change it by :

- Logging as your authenticated LDAP tenant admin. Click the Edit Tenant link. The Admin User information is displayed .
- If logging in as the authenticated LDAP tenant admin is not possible, browse this admin specific URL - <base-url>/frevvo/web/admin/login. Enter the built-in admin userid. Click Forgot Password? Once you have changed the password, browse the admin specific URL again and login with the tenant admin user id and the new password. If you need to change the password again, or make changes to your tenant, click the Edit Tenant link. The built-in admin password can be changed on this screen.



Admin User

Admin User Id

admin

Admin User Password

••••••••••••

Re-enter Admin User Password

••••••••••••

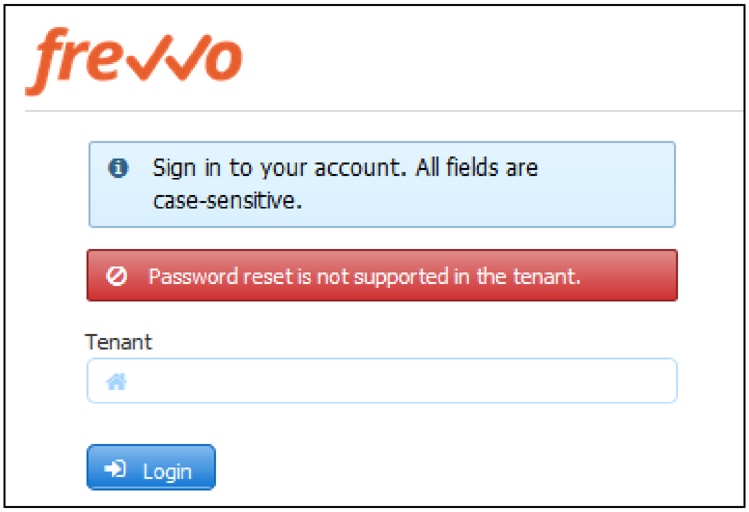
Change password on next login

□ Yes

Admin User Email Address

admin@frevvo.com

This error message displays if any other user clicks on the Forgot Password? link after browsing the admin specific URL:



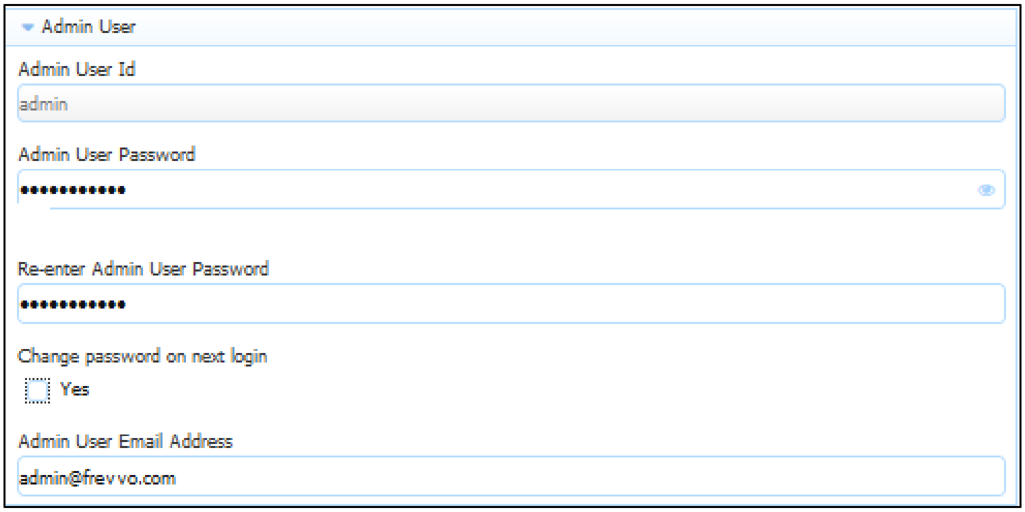
Sign in to your account. All fields are case-sensitive.

Password reset is not supported in the tenant.

Tenant

What if you do not remember the userid of your original tenant admin? Follow these steps:

1. Login as your authenticated LDAP tenant admin. Click the Edit Tenant link. The Admin User information is displayed.



Admin User

Admin User Id

admin

Admin User Password

•••••••••••

Re-enter Admin User Password

•••••••••••

Change password on next login

☐ Yes

Admin User Email Address

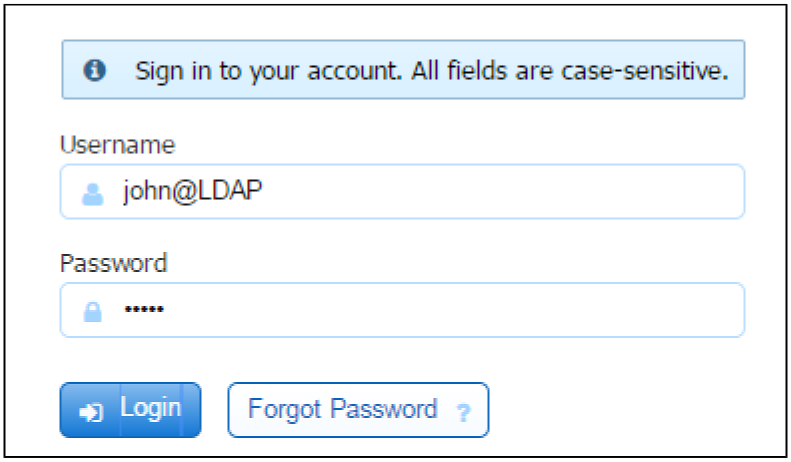
admin@frevvo.com

2. If logging in as the authenticated LDAP tenant admin is not possible, the frevvo (Cloud customers) and in-house superuser can see the built-in admin tenant userid from the Edit Tenant page.

Check if the configuration is correct

Here are some quick tests to check if the LDAP configuration is correct:

1. Login as the Live Forms tenant admin for the LDAP tenant.
2. Click on the **Manage Users** link.
3. Click **All**. You should see a list of LDAP users which were assigned one of these Live Forms roles on the LDAP server: frevvo.TenantAdmin, frevvo.Designer, frevvo.Publisher, frevvo.ReadOnly
4. Now, click **Back To Manage Tenant**.
5. Click **Manage Roles**. You should see a list of groups from your LDAP server.
6. Log out from Live Forms (you should be currently logged in as the tenantadmin)
7. Try to login with the user name and password of a designer user in LDAP. You need to specify the proper tenant when logging in. For instance, if **john** is a valid LDAP user and the name of the LDAP tenant is MYLDAP, you should log in as john@MYLDAP. The password would be john's password in LDAP. Verify that the Application Home Page displays.



Sign in to your account. All fields are case-sensitive.

Username

john@LDAP

Password

•••••

8. Log out from Live Forms
9. Try to login with the user name and password of a non-designer user in LDAP. Verify that the user's Task List displays.

Since you are using LDAP to define Live Forms users and roles (i.e., groups), you do not see an *Add User* icon or *Add Role* icon on the Manage Users or Manage Roles pages.

LDAP Configuration Properties and Sample Configurations

These are the properties used to configure the LDAP/Active Directory security manager. The properties in bold are required.

Property	Description	Active Directory Sample Configuration	OpenLDAP Sample Configuration

Connection URL	ldap server url	In-house ldap://[your server]:[port, typically the default is 389] Cloud - SSL installed on your LDAP server ldaps://[your server]:[port, typically the default is 636]	In-house ldap://[your server]:[port, typically the default is 389] Cloud -SSL installed on your LDAP server ldaps://[your server]:[port, typically the default is 636]
Connection User	User to connect to LDAP. This user must have the proper permissions to read and run queries in the ldap server. If using Active Directory, it is common to specify the domain. Ex: an entry of TEST\Administrator refers to the user Administrator in the TEST domain.	[user name]	`cn=admin,dc=test,dc=frevvo,dc=com`
Connection Password	Password for the Connection user.	[user password]	[user password]
Users Base	Searches for users will start from the ldap node specified by this property.I If the value is empty the searches will start from the root domain.	CN=Users,DC=test,DC=windows,DC=frevvo,DC=com	DC=test,DC=frevvo,DC=com
Groups Base	Searches for the groups will start from the ldap node specified by this property. If the value is empty, searches will start from the root domain	CN=Users,DC=test,DC=windows,DC=frevvo,DC=com	DC=test,DC=frevvo,DC=com
UserId Display	User attribute that will be visible in frevvo. This is what will be displayed in the list of users a tenant admin sees and has to be unique in the server. Another restriction is that the values for the attribute configured here cannot have spaces. For instance, don't configure CN as the value since it can contain spaces in most systems.	sAMAccountName	uid

GroupId Display	Group attribute that will be visible in frevvo. This is, for instance, what will be displayed in the list of groups a tenant admin sees or the groups used in workflows. This attribute has to be unique in the server.	sAMAccountName	entryDN
Notify checkbox	Notifications are emails sent by frevvo to workflows participants. If checked, notifications will be sent.	Check the Notifications checkbox	Check the Notifications checkbox
All Groups Filter	The expected value is an LDAP filter expression. The expression should return the groups that will have access to frevvo forms and workflows.	(objectClass=group)	(| (objectClass=groupOfUniqueNames)(objectClass=organizationalRo
All Users Filter	The expected value is an LDAP filter expression. The expression should return the users that will have access to frevvo forms and work flows.	(objectClass=user)	(objectClass=person)
User Member Of	Attribute on a user object storing the groups the user is a member of.	memberOf	" "
Group Member	Attribute on a group object storing the users that are a member of this group.	member	uniqueMember
First Name	Name of the user "first name" attribute	givenName	cn
Last Name	Name of the user "last name" attribute.	sn	sn
Email	Name of the user "email" attribute in the LDAP server. This value can be used in a rule is used in email notifications	mail	mail

Manager	Attribute on a user object storing the DN of the user’s manager. This value can be retrieved in a rule. It can also be used in flow navigation using the subject.reports.to data available in Live Forms.	manager	manager
Ignore Case checkbox	If checked, Live Forms ignores the case stored in LDAP systems. This is primarily for the purpose of determining roles.	Check the Ignore Case checkbox	Check the Ignore Case checkbox
Custom	This is a a comma separated list of attribute names to be retrieved from the LDAP Server.	Ex: carLicense,employeeNumber	Ex: carLicense,employeeNumber
TLS	This enables simple authentication over TLS. If checked, a trusted certificate for the LDAP server is required. Refer to the secure the connection topic for details.	Check if you are using TLS to secure the connection.	Check if you are using TLS to secure the connection

Mixed or Uppercase User Names

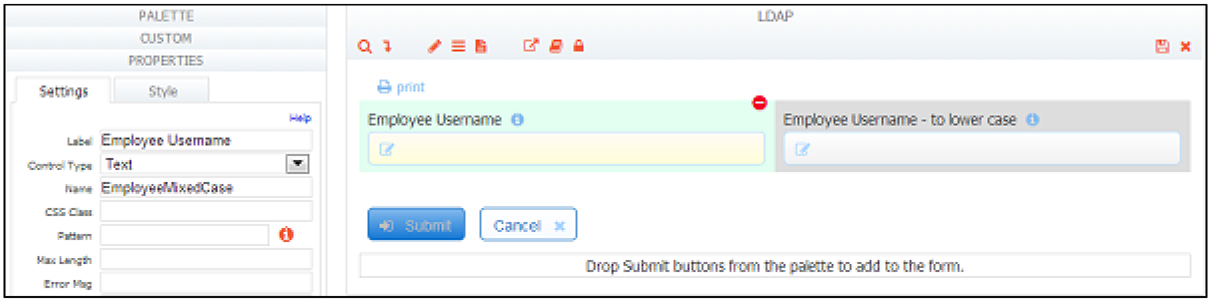
Live Forms user names are case sensitive; the user name *johndoe*" is not the same as *JohnDoe*. Several LDAP systems are case insensitive. Thus the two user names would resolve to the same LDAP account but to different Live Forms user accounts.

To avoid case issues follow these steps described in more detail below:

- Check the Ignore Case checkbox on the LDAP Configuration screen
- Convert control values to lower case if they are used in workflow routing to a specific user.

The first issue occurs when the user logs in. For instance, John Stevens LDAP account is **JStevens** but he logs in as **jstevens**, he will be recognized by case insensitive LDAP and thus granted access but will not be recognized as a designer or as a tenant admin by Live Forms. To solve this, check the Ignore Case checkbox on the LDAP Configuration screen. To prevent issues you could always login to Live Forms using lower case **jstevens**. LDAP will grant access as it is case insensitive and Live Forms will know that you may have the designer or admin special permission. However users can forget to do this. Setting Ignore Case in your LDAP security configuration will solve this.

The second problem is in directing tasks to Live Forms users if your LDAP user names are mixed case. One solution is to use hidden controls on your forms with rules to convert the case of user names to lower case. The example below shows two text controls on a form, one visible, *EmployeeMixedCase*, and the other hidden, *Employee*.



Label Employee Username
Control Type Text
Name EmployeeMixedCase
CSS Class
Pattern
Max Length
Error Msg

Drop Submit buttons from the palette to add to the form.

A user types a name (regardless of case) into the EmployeeMixedCase control. The hidden Employee control has a business rule that takes the value of the visible control and converts it to lowercase.

```
Employee.value = EmployeeMixedCase.value.toLowerCase();
```

The form or workflow routing can then use {*Employee*} rather than the control that may be mixed case.

> Changing the case of LDAP userids in Active Directory can cause undesired results. Use caution.

Referrals

LDAP administrators can configure Live Forms to ignore or follow referrals by entering the LDAP property name and value in the table provided on the Add Tenant (on-premise) or Edit Tenant (cloud) screens.