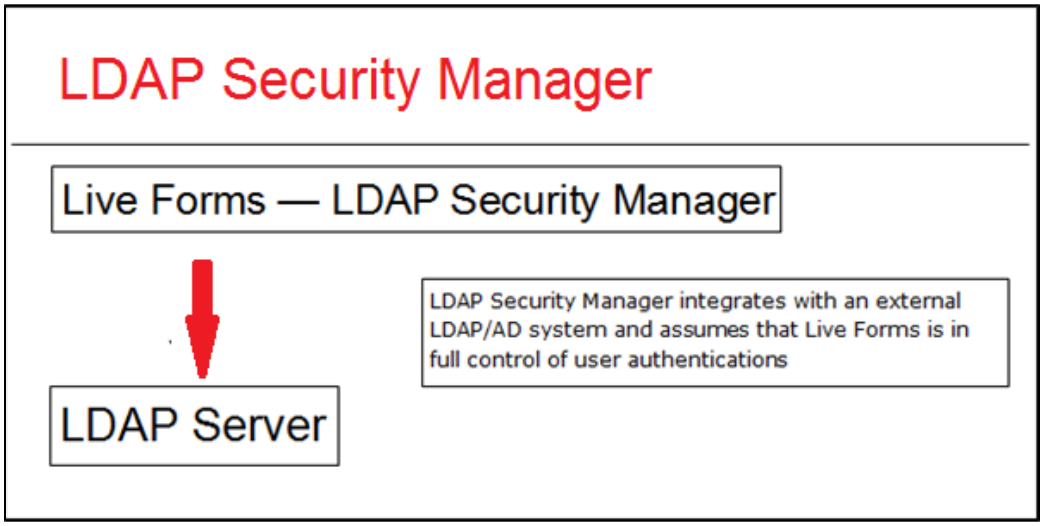
Configuring the LDAP Security Manager for In-house

Follow these instructions if you have an in-house installation of Live Forms up and running. If you have a provisioned cloud tenant and you want to configure the LDAP Security Manager, follow the instructions for Configuring the LDAP Security Manager LDAP(s) for Cloud tenants.

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



On This Page:

Prerequisite Tasks

These instructions assume that you have an in-house installation of Live Forms up and running. Refer to Configuring the LDAP Security Manager LDAP(s) for Cloud tenants if you have signed up for an LDAP tenant on the cloud server.

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 **BE FORE** 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 Li ve 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/Active Directory Security Manager** class.
3. Once you have your tenant successfully connecting with your LDAP server, review the available options regarding the authentication process.

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

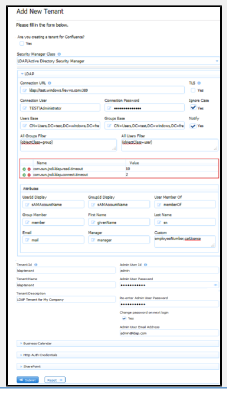
The connection to your LDAP server is configured at the tenant level.

- New Live Forms in-house customers can add an LDAP tenant and configure the LDAP parameters via the Add Tenant screen. LDAP properties can be updated at anytime via the Edit Tenant screen.
- Cloud customers must request an LDAP tenant from frevvo customer support. Cloud customers will receive a default tenant login from frevvo and then they can edit the LDAP configuration properties using the Edit Tenant screen to connect to their LDAP server.

In all cases, follow these steps to configure LDAP. These instructions assume that you have an in-house installation of Live Forms up and running or you have signed up for an LDAP tenant on the cloud server.

- **In-house customers:**
    1. Login to Live Forms as an administrator (user:admin and password:admin if you have not changed it)
    2. Click on **Manage** and then **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.
    5. Configure the new tenant - Choose **LDAP Security Manager**.from the **Security Manager Class** drop down.

Add New Tenant Screen



Edit Existing Tenant Screen

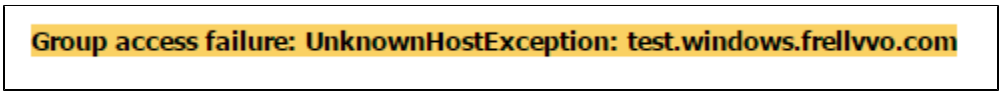
a. Enter your LDAP Configuration Properties and Sample Configurations. Alternatively, you can start off from one of the sample configurations and provide only the key information listed above. See below for information on the TLS checkbox.

> 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.

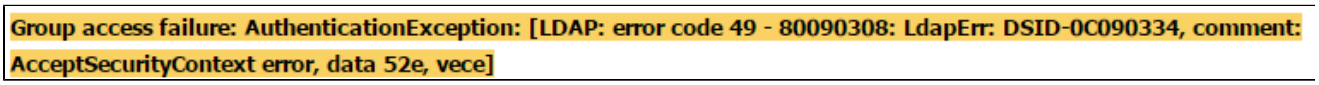
b. If you are creating a new tenant:
   i. Enter a tenant id, a tenant name and description.
   ii. The **Max Concurrent Users** is the maximum allowed by your license or less.
   iii. Specify the User ID, password and email address of a user that will have the tenant admin permission. This user id is the built-in admin and can be used to access tenant administrative functions if you cannot log in as an authenticated LDAP tenant admin.
      1. The tenant admin id, password and email fields are required. The Change password on next login is optional. It is checked by default.
   iv. 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:



Here is another example if the connection password is not correct



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

Check if the configuration is correct

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

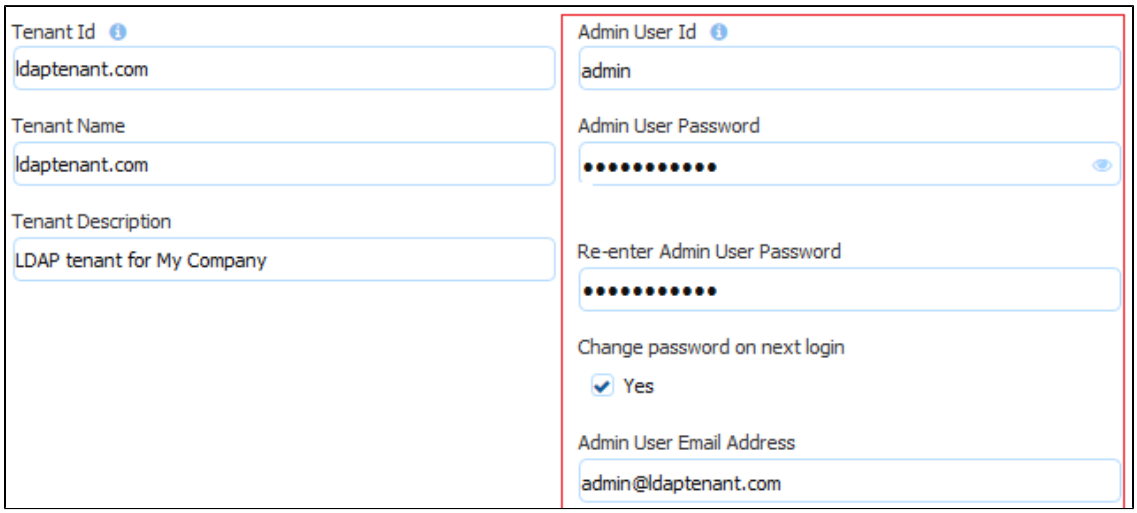
1. Login as the Live Forms tenant admin for the LDAP tenant.
2. Click on the **Manage Users** link.
3. Click **All**. You should see a list of LDAP users which were assigned one of these Live Forms roles on the LDAP server: frevvo.TenantAdmin, frevvo.Designer, frevvo.Publisher, frevvo.ReadOnly
4. Now, 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 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.

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 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.

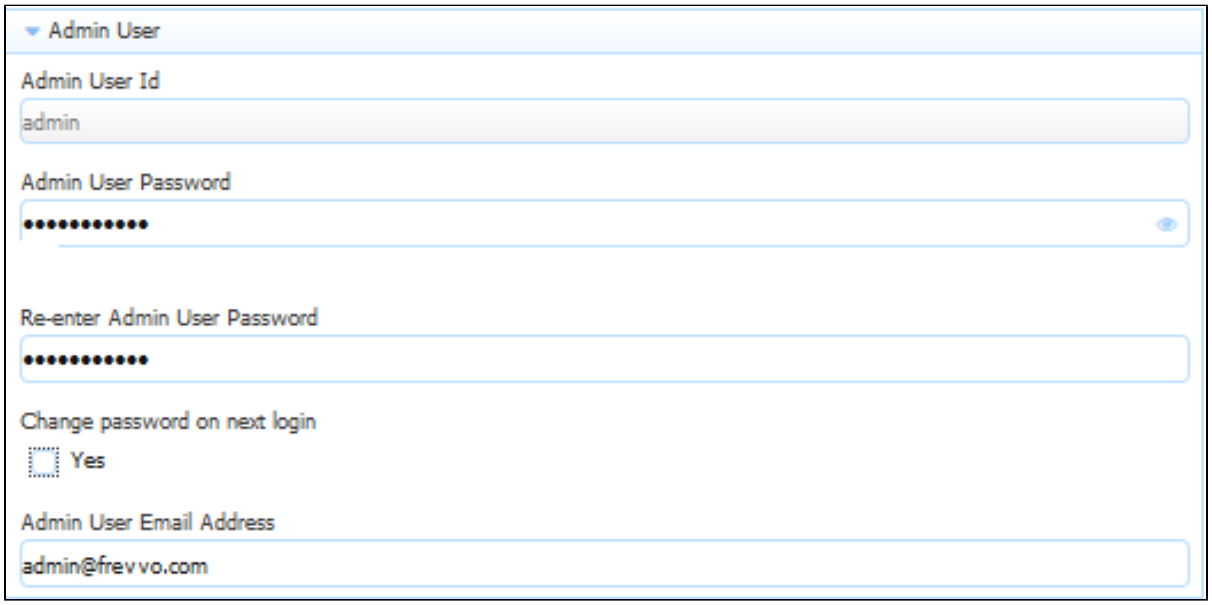


Browse this URL to login as the built-in admin: **<base_URL>/frevvo/web/admin/login**. When specified, Live Forms will prepend the base URL to the URLs in your Form/Document Actions. The <base_URL> is typically http(s)://<your servername>:<port>.

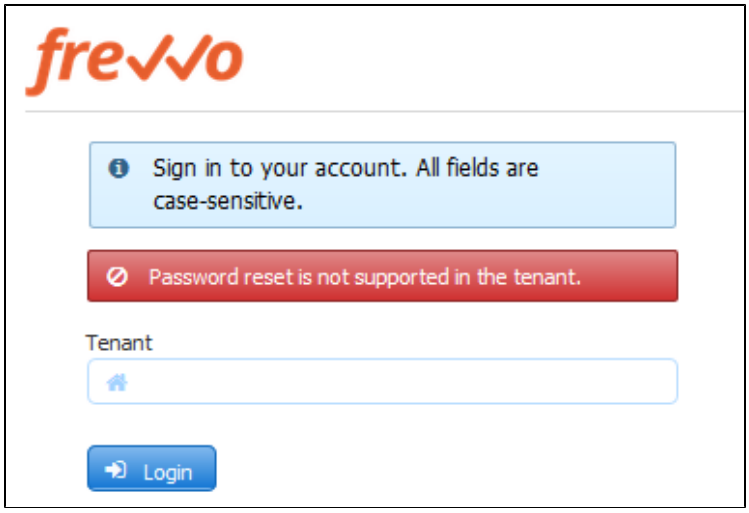
- You must use the admin specific URL - **<base-url>/frevvo/web/admin/login** - to login as the built-in admin.
- Non admin users can also login using the admin specific URL.

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 :

- Login 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.

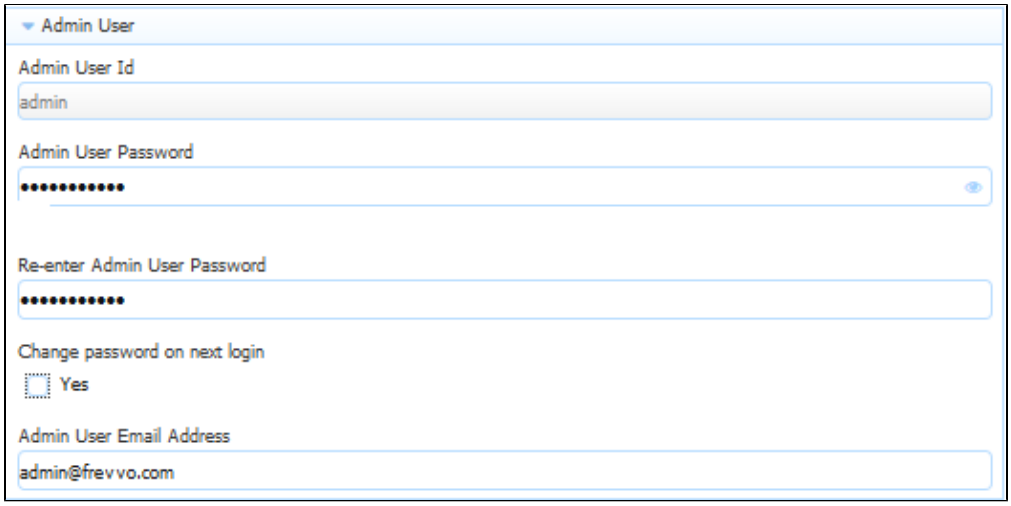


This error message displays if any other user clicks on the Forgot Password? link after browsing the admin specific URL:



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 .
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.



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.

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 f 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

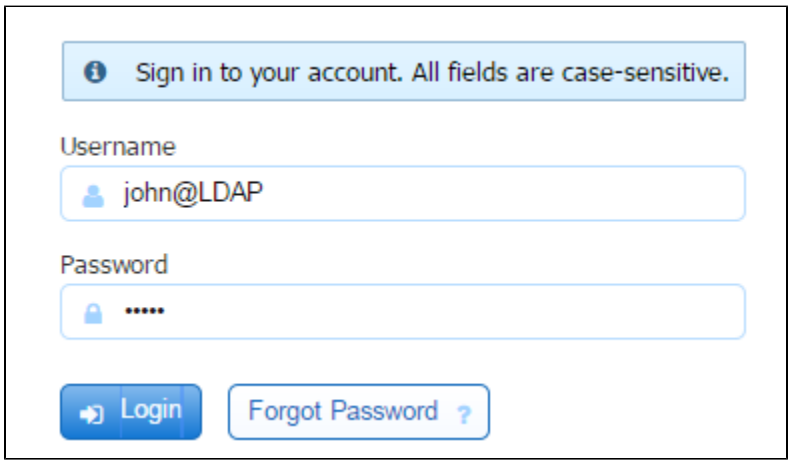
Options for Authentication

Once you have your tenant successfully connecting with your LDAP server, there are two options available regarding the authentication process.

- Options 1: Users can login using the Live Forms login page and Live Forms will delegate authentication back to the LDAP/Active Directory server. See the example below. There is nothing more to do if you choose this option.
- Options 2: You can implement Single Sign On with IIS. See the details below.

Option 1 - Live Forms login page authenticating against LDAP

This is the case where the user will authenticate through the Live Forms's login page but delegate authentication to LDAP. Lets assume that your tenant named 'LDAP' was successfully configured to connect to your LDAP server and there is a user 'john' in your LDAP server. You can now login directly via Live Forms's login page:



The password provided in the login page is the user's password in LDAP. A very important point to note is that the user name, "john" in the example above, needs to match the value for the LDAP entry attribute configured in the property **UserID Display** field on the Edit Tenant screen. For instance, for Active Directory, the value of this property is normally **sAMAccountName**. That means Live Forms will try to find an entry in LDAP that has sAMAccountName=john.

Option 2 - Single Sign On with IIS

In this scenario, a user authenticates to his windows account and tries to use Live Forms. Since the user is already authenticated to the network, Live Forms will recognize his credentials and automatically forward the user to his Live Forms account, if he is a designer, or allow the user to use a form/flow if those resources are available to the tenant.

The basic deployment is IIS fronting Live Forms and the authentication is done against LDAP. For that to work you need to:

1. Install Live Forms
2. Configure Live Forms to work with IIS
3. Configure Windows Authentication
    a. Configure Windows Authentication on IIS7
    b. Configure Windows Authentication on IIS6
4. In IIS, Make sure that **Anonymous Authentication** or **Basic Authentication** is NOT configured in the Web Application (Default Web) that will be used to proxy requests to Live Forms.

Please also refer to the force auth property for forms and flows. Force auth lets you override SSO for an individual form or flow.

> If you are using LDAP and SSO, and you want to embed the Live Forms in your website, refer to Embedding the Task List for important information.

Once all is configured and running it is possible to test these scenarios:

Signing in from within the network

In this case, the Live Forms server and the Active Directory server are running on the same network. The user is already authenticated to the windows network and points the browser to:

```
http://[server]/frevvo/web/tn/[LDAP tenant]/login
```

Substitute **LDAP tenant** above with the tenant name you configured with the LDAP Security Manager. The ***server*** variable should be the ip address of the machine where IIS is installed .

The user will automatically authenticate to Live Forms. It is crucial that the LDAP user is known to Live Forms, in other words, the user should be one of the entries retrieved by the LDAP expression configured in the **All Users Filter** on the LDAP configuration screen.

Signing in from outside the network

In this case, the Live Forms server and the Active Directory server are running on different networks. The user is trying to hit the URL below from outside the network.

```
http://[server]/frevvo/web/tn/[LDAP tenant]/login
```

Substitute **LDAP tenant** above with the tenant name you configured with the LDAP Security Manager and the ***server*** variable with the ip address of the machine where IIS is installed.

Since the user is not authenticated in the windows Network, he will be prompted by the browser for credentials. IIS will authenticate the user in the network and forward the request to Live Forms. The user will be automatically redirected to his initial page without having to re-enter his credentials.

Single sign-on Browser Configuration

If you are still being prompted for Windows authentication after SSO is configured, the security settings for your browser may be too high. Configure your browser to authenticate using the "system logon credentials" (Kerberos authentication mechanism) by adding the frevvo server to the browser's trusted sites.

Follow these steps for the specified browsers:

Configuring Internet Explorer

If you are using either the **IisLoginModule or NtlmLoginModule** option, your Internet Explorer users may want to modify their browser settings. By default, Internet Explorer will only allow automatic login for sites in its *Intranet zone*. For sites not included in the specified Intranet Zones, a windows dialog box will popup requesting login information. This popup can be avoided by having your users modify their Intranet Zone settings as described below.

IE will recognize a site as being in its Intranet zone in one of two ways.

1. The name of the server that you are accessing does not have a dot in the name. For example, http://frevvoserver/.
2. The site is configured as an Intranet site for IE.

To configure the Intranet sites for IE,

1. Open IE and select "Tools > Internet Options...".
2. Select the "Security" tab, click on the "Local intranet" icon, and then click on the "Sites..."
3. Click the **Advanced** button. Type the full name of the frevvo server, including protocol, in the first field. For example: http://frevvoserver.com
    a. If you are using SSL, then replace "http" with "https".
4. Click the "Add" button.
5. Click the "Close" and "OK" buttons to back out. Now IE should recognize the server as being part of its Intranet zone.

Configuring Firefox

If you are using either the **IisLoginModule** or **NtlmLoginModule** option, your Firefox users may want to modify their browser settings. By default, Firefox will prevent automatic login. Browsing the frevvo SSO URL will cause a windows dialog box to popup requesting login information. This popup can be avoided by having your users modify their Firefox settings as described below.

1. In the Firefox address bar type **about:config**. This will display all settings for Firefox.
2. In the filter box type **ntlm** and hit the enter key. This will narrow the display items to those pertaining to NTLM authentication.
3. Double click on the key entry **network.automatic-ntlm-auth.trusted.uris**. This is a comma separated list of trusted servers for which automatic NTLM authentication is enabled.
4. In the edit box displayed, enter the name of the server you are accessing. For example, http://frevvoserver.com/.
    a. If you are using SSL, replace http with https.
5. Click the OK button. Firefox should now enable automatic NTLM authentication with the frevvo server.

Configuring Chrome

To configure chrome you need to start the application with following parameter: auth-server-whitelist - <Allowed fully qualified domain name>.

For example: In Windows,

1. Click the **Start** button, **All Programs**, **Accessories**, and then click **Run**.
2. In the **Open** box, type following and click Ok:
    - chrome --auth-server-whitelist="*frevvoserver.com"

Configuring Safari

No additional configuration is needed.

Configure frevvo.internal.baseurl in frevvo.xml for LDAP SSO

This parameter is needed in frevvo.xml for various activities like accessing the ACL page, publishing templates, resetting tasks etc when using LDAP SSO. Let's say you have a browser signed in via SSO to machine m1 (port 80). IIS is running on m1 (port 80) redirecting /frevvo/web to frevvo running on m2:8082. The browser submits a form to m1, IIS redirects to m2:8082. The doc action is a frevvo:// URI which gets resolved to http://m1/frevvo/... Live Forms POSTs to this URI but m1 rejects the POST since it is not authenticated.

To avoid situations such as these, set frevvo.internal.baseurl to the actual host:port of the Live Forms server. Follow these steps:

- edit <frevvo-home>/tomcat/conf/catalina/localhost/frevvo.xml
- Add the parameter shown below with your information: Save the changes to the file.

```
Parameter name="frevvo.internal.baseurl" value="http:// <ip of the m/c where frevvo
server is hosted>:<port>" override="false"/>
```

Upload and Video Control Behavior

If your system is configured for LDAP SSO, the upload and video controls exhibit the following behaviors:

- The "uploading...." snake image displays continuously when uploading an image to an upload control in a form, accessed from a space, on a mobile device.
- The video control will ask for credentials again in use/design mode if you are using the FireFox browser. In IE9, you will see the message: " The Web-page wants to run the following add-on: 'Windows Media Player' from 'Microsoft Corporation'. What's the risk?" Enter your credentials or run the add-on to proceed.

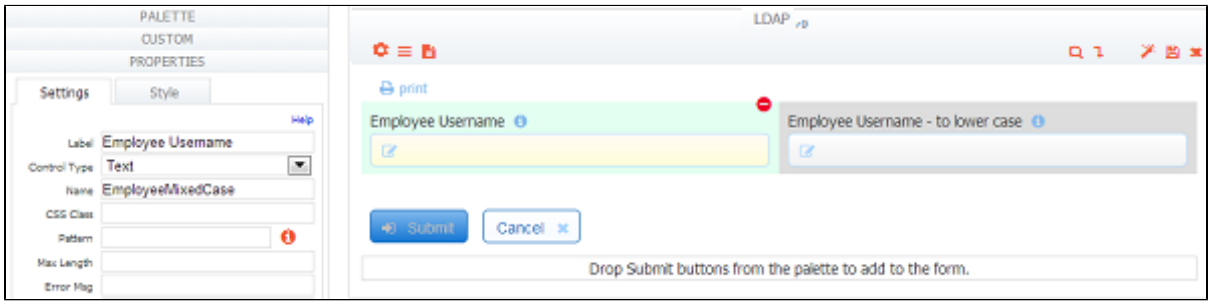
To workaround this issue, configure IIS so that it does not require re-authentication for every single request.

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*.



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.