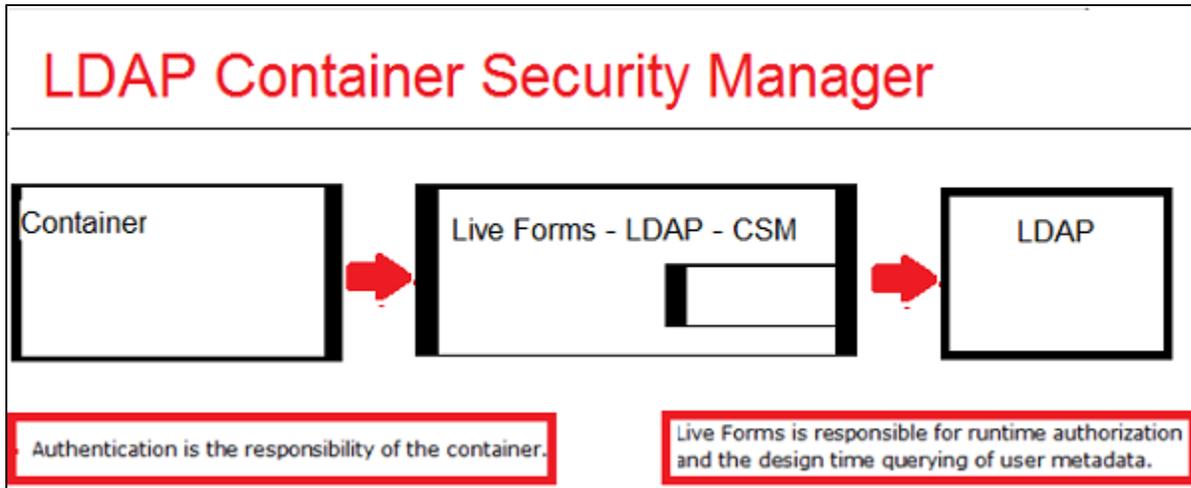


Configuring the LDAP Container Security Manager

Sometimes, Live Forms is deployed to an existing servlet container that is already handling user authentications through, for instance, LDAP. Here the authentication is the responsibility of the container, but Live Forms is still responsible for the runtime authorization and the design time querying of user metadata. The LDAP Container Security Manager reuses the existing Live Forms LDAP connector but relies on the container for user authentications.

frevvo only supports/certifies the LDAP Container Security Manager in the Apache Tomcat container. Refer to our [Supported Platforms](#) for the list of Application Servers supported/certified by frevvo.



On this page:

- [Active Directory Requirements](#)
- [Configuration Steps](#)
- [Check if the configuration is correct](#)
- [Troubleshooting](#)

Active Directory Requirements

- There must be a `frevvo.User` group in Active Directory
- All the users in your LDAP-CSM tenant must be members of this group
- The tenant admin must have the roles of `frevvo.TenantAdmin`, `frevvo.Designer` and `frevvo.User`.

- The group names for these three special roles must be **frevvo.User**, **frevvo.TenantAdmin**, and **frevvo.Designer**. Upper/lower case may be a factor for Open LDAP systems.
- [frevvo Best Practice](#) recommends that you create a user account in your Active Directory or IDP 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, download them to your desktop as a backup **BEFORE** changing the Security Manager
- frevvo only supports the LDAP Container Security Manager when Live Forms is running in the tomcat container. Refer to our [Supported Platforms](#) for the list of Application Servers supported/certified by frevvo.

Configuration Steps

1. Stop Live Forms if it is running.
2. Modify the `<frevo-home>\tomcat\conf\server.xml` file. Here is an example of the changes needed when using tomcat.
 - a. Edit this file with a text editor.
 - b. Search for `'ldap://localhost:389` - you should find this in the `org.apache.catalina.realm.JNDIRealm` section of the file.
 - c. Uncomment this section. Replace the existing code with the code shown below:

- d. Replace the connectionURL, connectionName and the connectionPassword default values with your LDAP server information.
- e. Refer to this [Apache Tomcat website](#) for detailed information about the remaining parameters.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
  connectionURL="ldap://test.windows.frevvo.com:389"
  connectionName="TEST\Administrator"
  connectionPassword="FrevvoTest00" adCompat="true" referrals="follow"

  userBase="CN=Users,DC=test,DC=windows,DC=frevvo,DC=com"
  userSearch="( & (objectClass=user) (sAMAccountName={0})) "
  userSubtree="true" userRoleName="memberOf"

  roleBase="CN=Users,DC=test,DC=windows,DC=frevvo,DC=com" roleSubtree="true"
  roleName="cn" roleSearch="( & (objectClass=group) (member={0})) " />
```

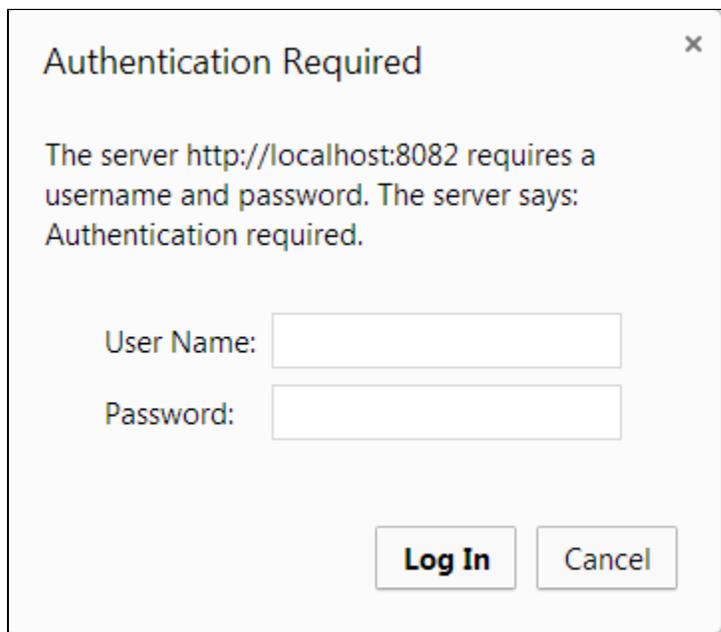
3. Start Live Forms.

5. Create a tenant with the **LDAP Container Security Manager** .

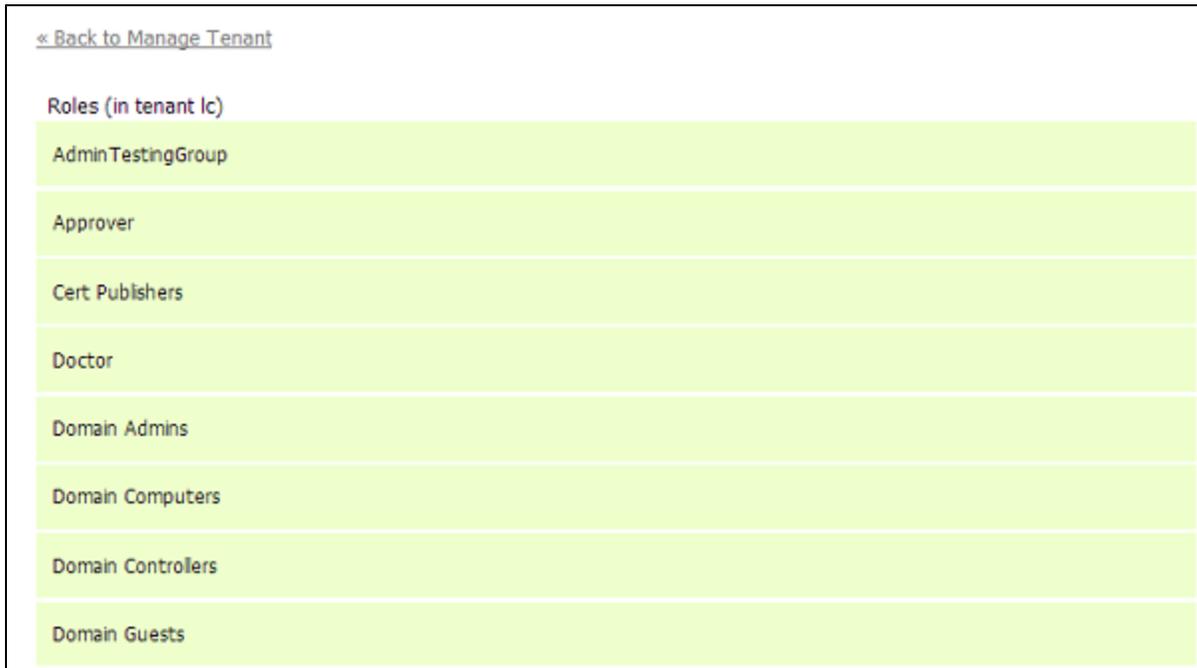
Check if the configuration is correct

Here are some quick tests to check if the LDAP Container Security Manager tenant configuration is correct:

1. Browse 'http://<IP>:<PORT>/frevvo/web/tn/<tenant id>/login'. Substitute the ip address/port of the Live Forms server and the name of your LDAPCSM tenant for the tenant id. The browser authentication light-box displays.



2. Login as the tenant admin for the LDAP-CSM tenant. This admin must have the frevvo.User role in addition to the frevvo.tenantadmin and frevvo.designer roles.
3. Click **Manage Roles**. You should see a list of groups.

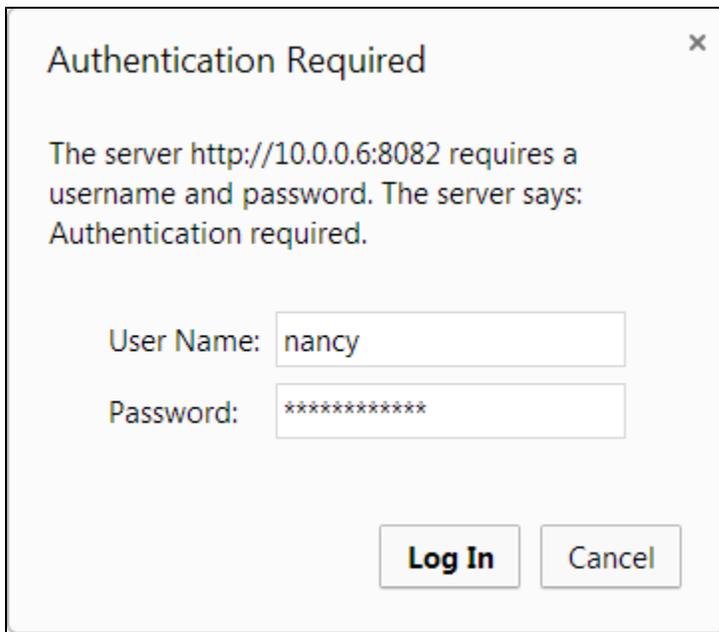


4. Click the **Back to Manage Tenant** link.
5. Click **Manage Users**.
6. Click **All**. You should see a list of LDAP users.



7. Now, click **Back To Manage Tenant**.
8. Log out from Live Forms.
9. Try to login with the user name and password of a user in the LDAP-CSM tenant. You do NOT need to

specify the LDAP-CSM tenant when logging in. For instance, if nancy is a valid LDAP user you should log in as nancy. The password would be nancy's password in LDAP. User nancy's home page will display.

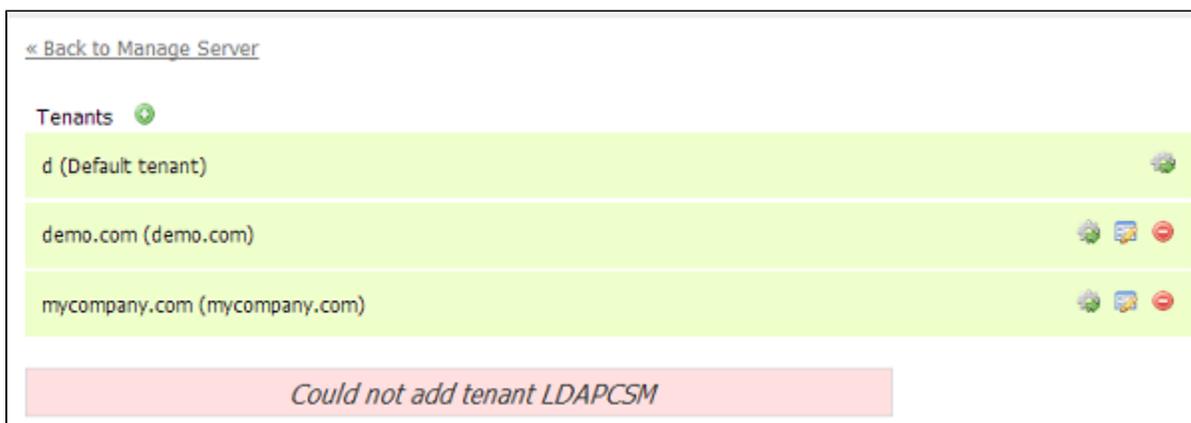


The image shows a dialog box titled "Authentication Required" with a close button (X) in the top right corner. The text inside the dialog box reads: "The server http://10.0.0.6:8082 requires a username and password. The server says: Authentication required." Below the text are two input fields: "User Name:" with the value "nancy" and "Password:" with the value "*****". At the bottom of the dialog box are two buttons: "Log In" and "Cancel".

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.

Troubleshooting

If the tenant admin user does not exist or it does not have the required roles, this error will display with the name of the tenant you are trying to add:



The screenshot shows a web interface for managing tenants. At the top left, there is a link: "[« Back to Manage Server](#)". Below this is a section titled "Tenants" with a green plus icon. There are three rows of tenant information, each in a light green box:

- Row 1: "d (Default tenant)" with a green plus icon on the right.
- Row 2: "demo.com (demo.com)" with a green plus icon, a blue gear icon, and a red minus icon on the right.
- Row 3: "mycompany.com (mycompany.com)" with a green plus icon, a blue gear icon, and a red minus icon on the right.

At the bottom of the screenshot, there is a red error message box that says: "Could not add tenant LDAPCSM".

This error message can be seen in the <frevvo-home>\tomcat\logs\frevvo.log file if the LDAP-CSM tenant cannot be created.

```
Application error processing /frevvo/web/tn?edit=true javax.servlet.ServletException:
javax.servlet.ServletException: Tenant admin user 111 does not exist!
or
Tenant admin user 111 must have roles: [frevvo.TenantAdmin,frevvo.Designer] if the
tenant admin exists but does not have the correct roles.
```