XPression Maps

LDAP and XPression Maps

Lightweight directory access protocol (LDAP) is an open and cross-platform protocol that will help secure and authenticate the XPression Maps HTML5 application's user information (user names, passwords, email addresses, account IDs, etc.)

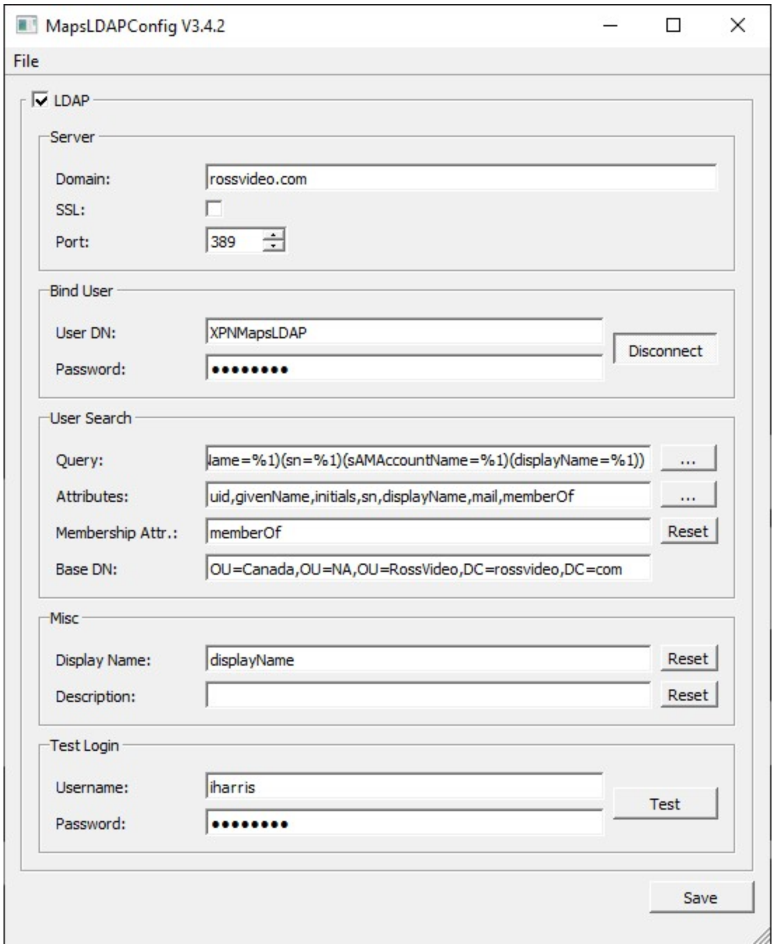
★Before you start configuring LDAP, consult with your IT department to get the information designated with the ★ symbol.

To access and enable the Maps LDAP configuration file:

1. Navigate to the **MapsLDAPConfig.exe** file on your computer.

   Typically this file is located in **C:\XPressionMapsGateway\bin64\MapsLDAPConfig.exe.**

2. Double-click the **MapsLDAPConfig.exe** file to open the configuration dialog.



MapsLDAPConfig V3.4.2

File

☑ LDAP

Server

Domain: rossvideo.com

SSL: □

Port: 389

Bind User

User DN: XPNMapsLDAP

Password: ••••••••

User Search

Query: lame=%1)(sn=%1)(sAMAccountName=%1)(displayName=%1))

Attributes: uid,givenName,initials,sn,displayName,mail,memberOf

Membership Attr.: memberOf

Base DN: OU=Canada,OU=NA,OU=RossVideo,DC=rossvideo,DC=com

Misc

Display Name: displayName

Description:

Test Login

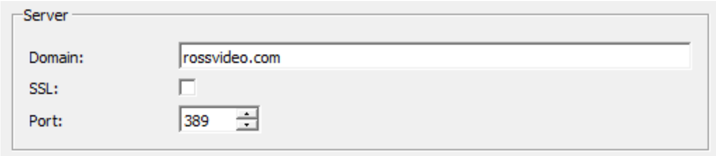
Username: iharris

Password: ••••••••

MapsLDAP Configuration File

To configure the LDAP server parameters:

1. In the **Server** section, in the **Domain** field, enter the domain name that is appended to all users in your company, e.g., rossvideo.com.



Server

Domain: rossvideo.com

SSL: □

Port: 389

Server Properties

2. If you are using the **Secure Sockets Layer** (SSL) protocol, select the **SSL** checkbox and in the **Port** field, enter **636**.

   OR

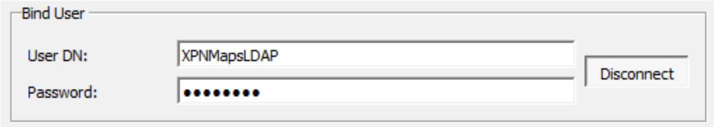
   If you are not using the **SSL** protocol, leave the **SSL** checkbox clear and in the **Port** field, enter **389**.

   ★These are the standard LDAP ports. A different port may be used if necessary. Consult with your IT department.

To configure the Bind User parameters:

1. In the **User DN** field, enter the name of the administrative account which will be responsible for retrieving information from the LDAP server.

   This is a **Read-Only** account.



Bind User

User DN: XPNMapsLDAP

Password: ••••••••

Bind User Properties

2. In the **Password** field, enter the password for this account.

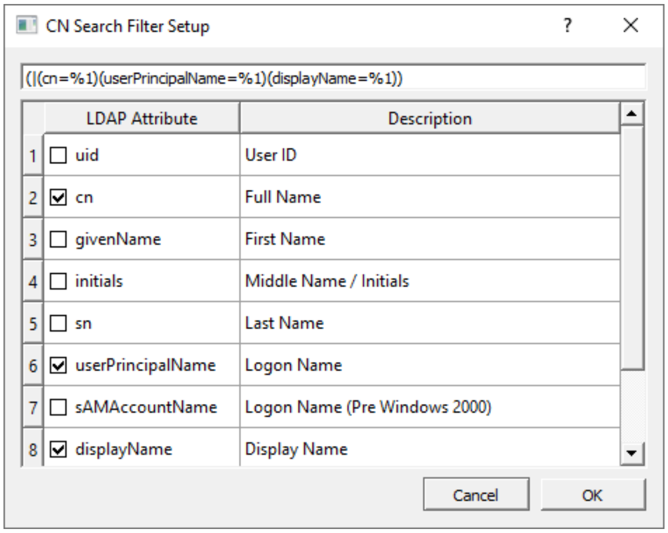
   ★Ask your IT department for the name of the administrative account and the password.

3. Then select **Connect**.

   If the **Bind User** credentials are correct, you will see a message at the bottom of the window, saying "**BindUser Connected**!"

To configure the User Search parameters:

1. Select the **Browse** button to the right of the **Query** field to open the **CN Search Filter Setup** dialog.



CN Search Filter Setup

(|(cn=%1)(userPrincipalName=%1)(displayName=%1))

	LDAP Attribute	Description
1	☐ uid	User ID
2	☑ cn	Full Name
3	☐ givenName	First Name
4	☐ initials	Middle Name / Initials
5	☐ sn	Last Name
6	☑ userPrincipalName	Logon Name
7	☐ sAMAccountName	Logon Name (Pre Windows 2000)
8	☑ displayName	Display Name

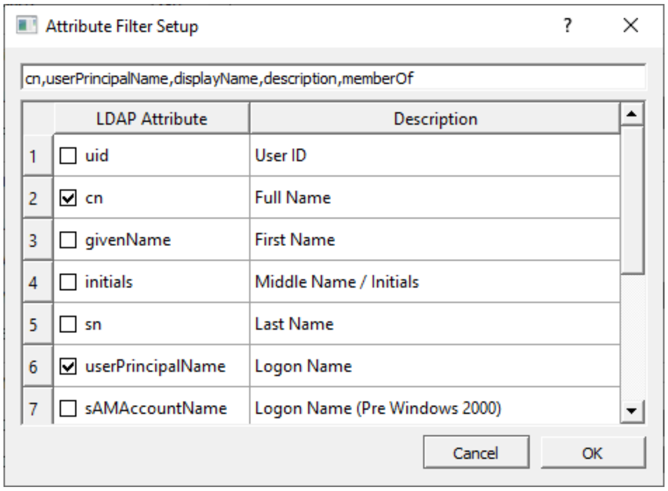
CN Search Filter Setup

2. Select the user identification attributes to use when searching for a specific HTML5 plugin user and then select **OK**.

   e.g., cn (Full Name), userPrincipalName, displayName

   ★Consult with your IT department to determine which attributes should be used.

3. Select the **Browse** button to the right of the **Attributes** field to open the **Attribute Filter Setup** dialog.



Attribute Filter Setup

cn,userPrincipalName,displayName,description,memberOf

	LDAP Attribute	Description
1	☐ uid	User ID
2	☑ cn	Full Name
3	☐ givenName	First Name
4	☐ initials	Middle Name / Initials
5	☐ sn	Last Name
6	☑ userPrincipalName	Logon Name
7	☐ sAMAccountName	Logon Name (Pre Windows 2000)

Attribute Filter Setup

4. Select the user attributes you want to see in the results and then select **OK**.

   These should only include the attributes selected in the **CN Search Filter Setup**, and in the **Display Name** and **Description** fields.

5. In the **Membership Attr** field, enter the group membership attribute used by your company (e.g., memberOf).

   ★Consult with your IT department to determine what attribute to use.

   ★This attribute must be one of the attributes selected in the **Attributes** field.

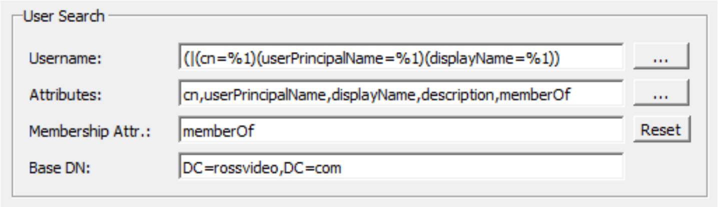
   Selecting the **Reset** button restores the field to its default value.

6. In the **Base DN** field, enter the **Base Distinguished Name** of your LDAP directory.

   The **Base Distinguished Name** (also known as the search base) identifies the root LDAP node in the directory, from which user searches are initiated.

   e.g., DC=companyname, DC=com (where "**DC**" stands for "**Domain Component**") and OU=Canada and OU=IT (where "**OU**" stands for "**Organizational Unit**")

   ★Ask your IT department for this information.



User Search

Username: (|(cn=%1)(userPrincipalName=%1)(displayName=%1))

Attributes: cn,userPrincipalName,displayName,description,memberOf

Membership Attr.: memberOf

Base DN: DC=rossvideo,DC=com

Base DN Properties

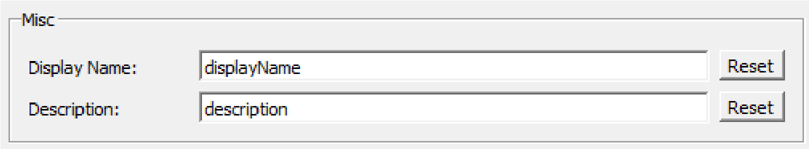
To configure the Miscellaneous section:

1. In the **Display Name** field, enter the attribute you want to see displayed when the user logs in to the application.

   e.g., displayname, givenName, mail

   ★This attribute must be one of the attributes selected in the **Attributes** field.

   Selecting the **Reset** button restores the field to its default value.



Misc

Display Name: displayName

Description: description

Misc Properties

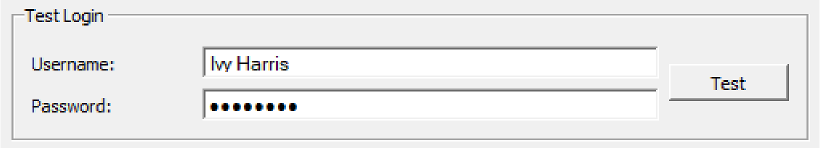
2. The **Description** field is optional and doesn't impact any function.

   Selecting the **Reset** button restores the field to its default value.

To configure the Test Login section:

1. In the **Username** field, enter your username, as defined in the **Username** attributes in the **User Search** section.

   e.g., If you selected **(givenName=%1)** in the **Username** attributes, you would enter your full name here.

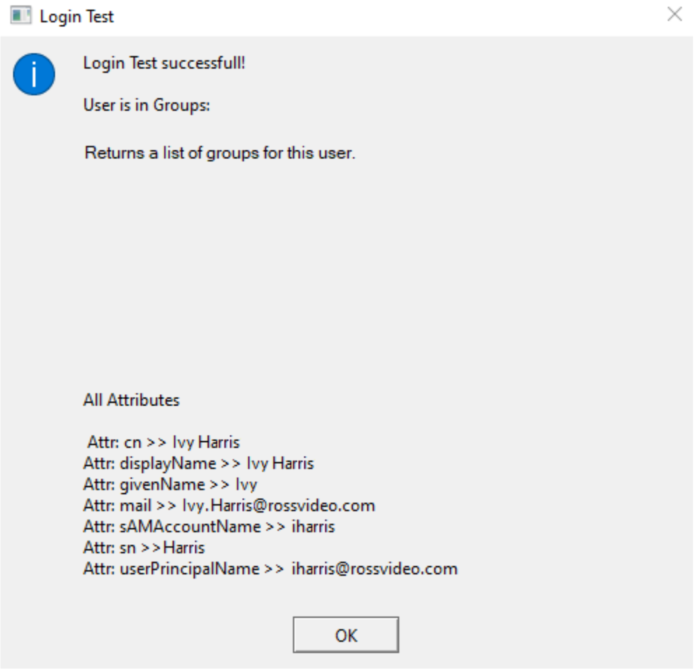
   Username: Ivy Harris

   Password: ••••••••

   Test Login Properties

2. In the **Password** field, enter your usual company login password.
3. Select the **Test** button to check that the credentials you entered work.

   If you have everything configured correctly, you will get a **Results** window indicating that the Login Test was successful and returning all the data you requested in the **Attributes** field.

   Login Test successfull!

   User is in Groups:

   Returns a list of groups for this user.

   All Attributes

   ```
    Attr: cn >> Ivy Harris
   Attr: displayName >> Ivy Harris
   Attr: givenName >> Ivy
   Attr: mail >> Ivy.Harris@rossvideo.com
   Attr: sAMAccountName >> iharris
   Attr: sn >>Harris
   Attr: userPrincipalName >> iharris@rossvideo.com
   ```

   Successful Login Results

   If you have configured something incorrectly, you will get a **Login Test Failed** message. Review your configuration to make sure it is correct and re-test.

4. When you have achieved a successful login test, select **Save** and close the Maps LDAP Configuration file.