LDAP Authentication

Overview

top

Yellowfin has two methods of authentication configurable from the Admin Console; Yellowfin Authentication, or LDAP Authentication. Yellowfin Authentication means that the user's credentials (user ID and password) are stored in Yellowfin and checked to authenticate a user logging into the system. LDAP Authentication means that Yellowfin references an external directory (LDAP) or database to perform the authentication - a user will enter their user ID and password (or this will be passed by Single Sign On) and Yellowfin will authenticate these details with those in the LDAP directory.

Using LDAP means that Yellowfin access can be controlled externally, and organisation-wide, simply and quickly. Users can use their existing intranet password for Yellowfin, and reports can be given access restrictions which include or exclude users in specific LDAP groups. In addition, removal/lockout of the user in the LDAP directly will automatically flow through to Yellowfin, as Yellowfin has to authenticate via the directory for every login request, minimising the manual effort of mananaging users.

LDAP Preparation

top

Prior to setting up the LDAP parameters in Yellowfin, the following will have to be completed:

- Creating a user group folder in the Active Directory.
- Enabling the LDAP authentication setting on your Yellowfin instance.
- Ensure network connectivity between the Yellowfin server and the LDAP server.
- Define the default Yellowfin Role for LDAP users.

Set up in the Active Directory

1. Ensure that you have set up a domain on your domain controller.
2. Create a folder within that domain and add users and groups that you want to allow access to Yellowfin.

Defining the Default Role

For Yellowfin to provision users automatically it has to assign a role to them. This role is defined as a Yellowfin 'Default' Role. In the Roles page, define one Role as the Default.

1. Navigate to Administration > General > Role Management
2. Select the Role you wish to make Default
3. Tick the Default Role box and Save

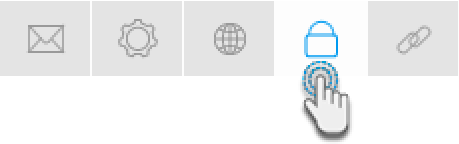
Note: if no role is set as default the users will not be provisioned correctly into Yellowfin and the process will fail.

Enable LDAP Authentication

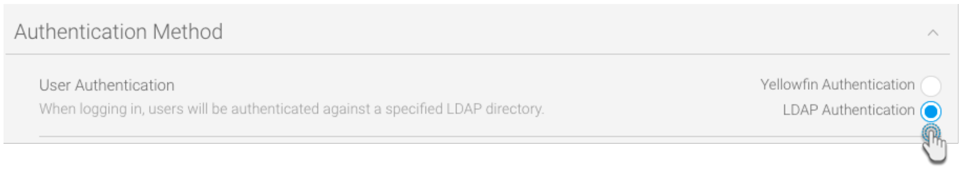
You will need to make sure that your instance of Yellowfin has the LDAP authentication functionality enabled.

1. In Yellowfin, navigate to the Configuration page. (Left side menu > Administration > Configuration)

2. Click on the Authentication icon.



3. Expand Authentication Method and select the LDAP option.



Authentication Method

User Authentication

When logging in, users will be authenticated against a specified LDAP directory.

○ Yellowfin Authentication

● LDAP Authentication

4. This will reveal an LDAP section. Provide configuration details in this section. There are explained below in detail.
5. Once the configuration details are provided, click on Test to validate the connection.
6. You can save the validated connection by clicking on the Save button on the top-right of the screen.

Yellowfin LDAP Configuration

top

To provision users from the LDAP directory and to use LDAP Authentication the required attributes must be defined on the Configuration page. The attributes required by Yellowfin include:

Property	**Description**
LDAP Host	LDAP server hostname or IP address.
LDAP Port	TCP/IP port that the LDAP server is listening on. Set this to 389 for normal LDAP connections, or 636 for encrypted connections (that is, if no custom changes have been to the LDAP configuration).
Encryption	The encryption method implemented by the LDAP server. (Options include: None, TLS, SSL) This determines whether or not the LDAP connection would need to be encrypted.
LDAP Base Distinguishing Name (DN)	The LDAP node that all users and groups are contained within. All your users might not be contained within a single group, so set the base domain here. Yellowfin will start searching for the LDAP directory from here.
LDAP (Yellowfin User) Group	LDAP Group Name that identifies which users have access to Yellowfin. This group exists in the LDAP directory, not Yellowfin. Only members of this group will be able to log in to Yellowfin. You can grant access to multiple LDAP groups, by using the '|' character as a separator. For e.g: LDAP_Consumers | LDAP_Writers
LDAP Bind User	The username of the user with the rights to search the LDAP directory. The format of this username should either be in NETBIOS or full domain. For example: admin@Yellowfin.bi or YELLOWFIN\admin **Note:** It is not recommended to use an admin user.
LDAP Bind Password	The LDAP password required for the Yellowfin application to connect to the LDAP directory; it authenticates the LDAP Bind User defined above. You must click 'Update Password" before testing your settings.
LDAP Search Attribute	This is a unique User Name field that LDAP users will log in to Yellowfin with. You can find the LDAP attributes by opening the property box of an LDAP object and clicking on the 'Attribute Editor' tab. You can set most of these attributes to a value of your choice. The attribute name is what you will provide in the LDAP Search Attribute field.
LDAP First Name Attribute	This maps to the First Name attribute of the user within the LDAP directory. This is so Yellowfin can match the user to a name and create an internal user account.
LDAP Surname Attribute	This maps to the surname attribute of the user within the LDAP directory. This is so that Yellowfin can match the user to a name and create an internal user account.
LDAP Email Attribute	This maps to the email address attribute of the user within the LDAP directory. This is so that Yellowfin can match the user to an email address for broadcast reports.
LDAP Role Attribute	This is an alternative method of mapping a Yellowfin Role to an LDAP user instead of the default role. By default, users brought in via LDAP will have the 'Consumer & Collaborator' role. But this sets a user's role in Yellowfin in accordance to their LDAP directory prior to their login. See RoleCode in OrgRole table.

	Note that Role Attribute is an attribute of the user’s LDAP record. For example, in the LDAP directory, the user might be assigned an attribute called ‘YellowfinRole’ that contains the name of a Yellowfin role; the user will then be assigned this role upon logging into Yellowfin.
LDAP Group Filtering Criteria	Criteria used to filter a list of LDAP groups. Only groups returned in the filtered list will be passed to Yellowfin.
Ordering	This order in which internal authentication is performed. Options include: LDAP Authentication First (default) or Internal Authentication First. This setting is important as it determines how Yellowfin will authenticate a user attempting to log in.
LDAP group role mapping	This toggle enables functionality to associate LDAP groups with Yellowfin roles. Note that once enabled, it’s required that every LDAP user should only have one associated role. See *here* for a detailed process.

Once defined, Yellowfin will automatically provision users as they attempt to login to Yellowfin for the first time.

Note: if the users in LDAP exceed the number of licences purchased, any new users will not be provisioned into the system.

Example

Setting	Parameter
LDAP Host	192.168.4.241
LDAP Port	389
LDAP Base DN	cn=Users,dc=i4,dc=local
LDAP Group	CN=Yellowfin Users,CN=Users, CD=i4,CD=local
LDAP Bind User	admin@Yellowfin.bi or YELLOWFIN\admin
LDAP Bind Password	*********
LDAP Search Attribute	employeeID
LDAP First Name Attribute	givenName
LDAP Surname Attribute	lastName
LDAP Email Attribute	userPrincipleName
LDAP Role Attribute	Writer
Ordering	LDAP Authentication First

Description:

- Connect to LDAP host 192.168.4.241 on port 389
- Users will be searched from cn=Users, dc=i4, and dc=local
- Users will be allowed to access Yellowfin if they are a member of cn=Yellowfin Users, cn=Users, dc=i4, or dc=local
- The user search will be conducted with user 'admin', who will get authenticated based on the bind password provided.
- The user will use employeeID as their login ID and Yellowfin will load their given name, surname, and email from the LDAP directory attributes givenName, lastName, and userPrincipleName respectively.

Note: if a user is not found in the LDAP directory, it will look for the username as a standard Yellowfin user.

Yellowfin Security & LDAP

top

Once LDAP Authentication is enabled, the Group Management screens will include a new group option called **LDAP**. This will source groups from the LDAP directory for use as normal Yellowfin Groups. Yellowfin Groups can also be created based on a variety of sources including mixtures of LDAP and Yellowfin groups, where LDAP groups can be either included or excluded in the new group.

1. Open the **Add LDAP Group** drop down
2. A list of LDAP groups will be displayed. Select the group to be used to create members for the Yellowfin Group
3. Click **Add** to add the LDAP Group members into the Yellowfin Group

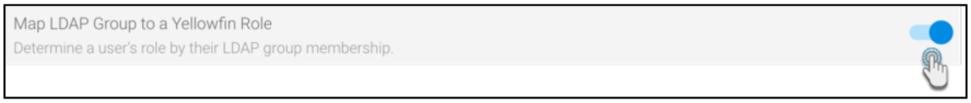
top

Role Based on LDAP Groups

The Yellowfin application allows for a user’s role to be dynamically determined by their group membership in a list of associated LDAP groups. This means that user’s roles are defined centrally in the LDAP Server, rather than within Yellowfin itself. Yellowfin will determine the correct role for an LDAP user each time they login.

To associate LDAP groups with Yellowfin roles, follow the steps below:

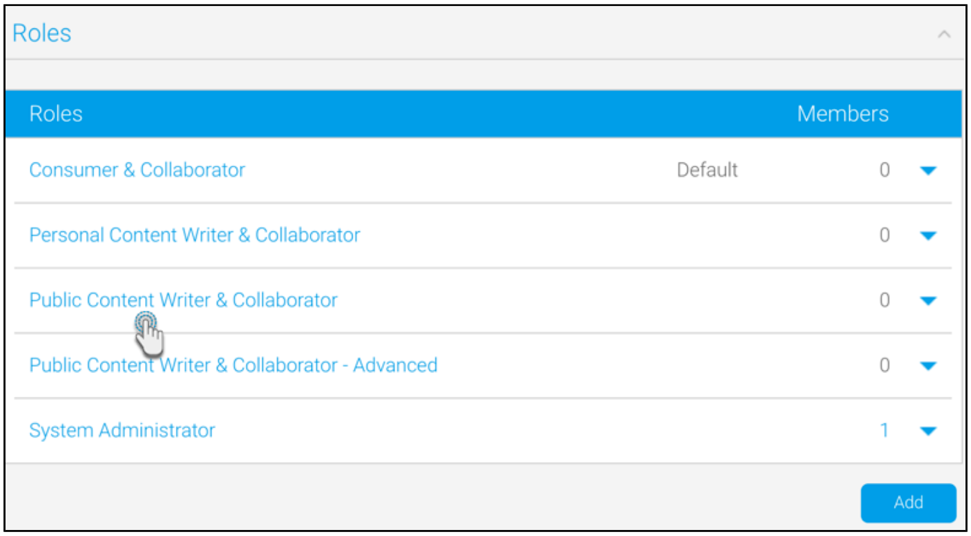
1. First, enable this functionality from the LDAP configuration page. Navigate to Administration > Configuration > Authentication page, and expand the LDAP Configuration tab (ensure that LDAP is selected as the chosen method of authentication)
2. From this list of configurations, enable the **Map LDAP Group to a Yellowfin Role** toggle.



Map LDAP Group to a Yellowfin Role

Determine a user's role by their LDAP group membership.

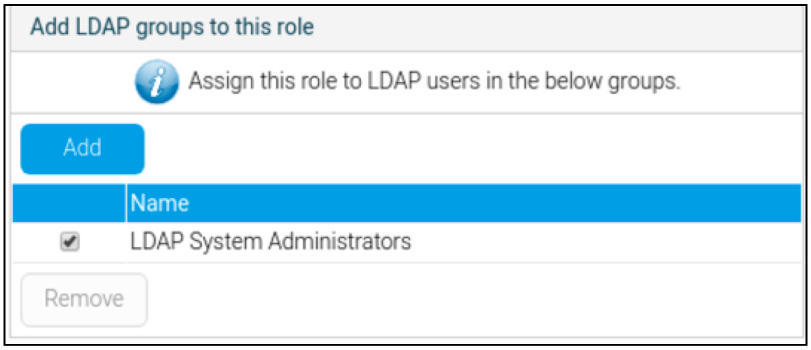
3. Save the changes.
4. Navigate to the Admin Console, and from the Roles tab, select a role to associate LDAP groups with.



Roles

Roles		Members	
Consumer & Collaborator	Default	0	▼
Personal Content Writer & Collaborator		0	▼
Public Content Writer & Collaborator		0	▼
Public Content Writer & Collaborator - Advanced		0	▼
System Administrator		1	▼

5. At the Role page, scroll to the panel titled ‘Add LDAP groups to this role’ (this only appears if the LDAP group role mapping functionality is enabled).
6. Add an LDAP group to associate to the selected role.



Add LDAP groups to this role

Assign this role to LDAP users in the below groups.

	Name
☑	LDAP System Administrators

7. Save the settings on the role page.
8. Users of this LDAP group will now inherit all the role permissions defined directly here upon logging into Yellowfin.

Notes:

- If the LDAP Group Role Mapping functionality is disabled from configuration, Yellowfin will continue to use the saved role for new Yellowfin user sessions.
- Each time a login is successful, the user’s role will be updated in the Yellowfin repository. In the event that a returning user is found to be a member of multiple role-associated groups, or a member of none, Yellowfin will use the last updated role for that user’s session.

- If a new LDAP user (logging into Yellowfin for the first time) is not a member of any role-associated groups, or is a member of more than one LDAP groups, access will not be given to the user.
- If a user is given a role explicitly within Yellowfin's interface, this will be overridden if the user logs in and is a member of valid role-associated LDAP group. If the user is not a member of any role-associated LDAP groups, then they will retain the role explicitly given to them.

top