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:

1. Create a Yellowfin User (or specify an existing user) within the LDAP directory to allow Yellowfin to connect and search for Users and Groups.
2. Create a 'Yellowfin User' Group within the LDAP directory (or specify one) which will be used to determine which users will have access to Yellowfin.
3. Ensure network connectivity between the Yellowfin server and the LDAP server.
4. Define the default Yellowfin Role for LDAP users.

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.

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
Encryption	The encryption method implemented by the LDAP server. (None, TLS, SSL)
LDAP Base Distinguishing Name (DN)	The LDAP node that all users and groups are contained within.
LDAP (Yellowfin User) Group	LDAP Group Name that identifies which users can log into Yellowfin. This group exists in the LDAP directory, not Yellowfin. Only members of this group will be able to login to Yellowfin.
LDAP Bind User	This is an LDAP User that the Yellowfin application uses to connect to the LDAP directory for search access, it must have rights to search the LDAP directory.
LDAP Bind Password	The LDAP Password required for the Yellowfin application to connect to the LDAP directory, associated with the LDAP Bind User defined above.

LDAP Search Attribute	This is a unique User Name field that LDAP users will login to Yellowfin with.
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 maps to a Yellowfin Role to be assigned to the user instead of the Default Role. See RoleCode in OrgRole table.
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. (LDAP Authentication First, Internal Authentication First)

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	cn=Administrator,cn=Users,dc=i4,dc=local
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 cn=Administrator, cn=Users, dc=i4, dc=local bound to the LDAP server with the password defined.
- 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