

Adding and configuring LDAP server


On this page:

- [Adding LDAP server](#)
- [Configuring encryption data](#)

As an example of the process of adding and connecting to the LDAP server, the connection timeout is defined in milliseconds (ms) and specifies the period of response waiting time from the LDAP server.

Adding LDAP server

To add an LDAP server

1. Go to **Setting** application > **LDAP management** page.
2. In the right bottom corner of the page click . The **Create LDAP configuration** page opens.
3. Enter all required data and click the **Save** button.

Create LDAP configuration

Configuration name

Server address

Port

389

Connect timeout (ms)

5000

Read timeout (ms)

10000

Bind as

Administrator

Username

cn=admin, dc=example ,dc=com

Password

LDAP status

Enabled

When disabled, users within this LDAP will be unable to sign in

Authentication

Search base

dc=example, dc=com

Authenticate using

LDAP query

Users query

uid={0}

User groups query

uid={0}

Encryption




Encryption protocol

None

Adding and configuring a new LDAP server.

The table below describes the components of the **Create LDAP configuration** page.

UI Component	Description
Configuration name	Enter the connection name of the LDAP server. A duplicate name is allowed.

Server address	Enter the server IP address/hostname. This is a mandatory field and is editable once created. You will get an error message if you enter a duplicate server IP address or hostname.
Port	If you need to change the default port number.
Connect timeout (ms)	The maximum amount of time in milliseconds for the system to system to successfully authenticate a single server (5000 is the default value). If authentication fails, the system will query the next server in the queue. This field is required.
Read timeout (ms)	The maximum amount of time in milliseconds for the system to system to successfully query User DN before requiring a similar authentication service (10000 is the default value). This field is required.
Bind as	A mode of bind specifying whether a user connects to the LDAP server with a specific username or anonymously for finding the Distinguished Name (DN) of a user corresponding to the user trying to log into the TWCloud system. If you select Anonymous , the Username and Password are not required and the system username and password will be disabled.
Username	The DN of a user to connect to the LDAP server and perform queries.
Password	The system password to connect to the LDAP server and perform queries.
Enabled /Disabled	The option to enable a connection with the LDAP server. When disabled users within LDAP will not be able to sign in.
	Click to save the LDAP server configuration properties. The function of this button is the same as that of the Save button on the Edit LDAP Configuration page.
Specific for authentication data	
Search base	The authentication methods. It defines the location in the directory from which the LDAP search begins.
Authenticate using	Select LDAP query to search for users by LDAP query. This is the default option. Select User DN Template to search for users by User DN.
User DN	To store a template for mapping user authentication with LDAP servers using the LDAP distinguished names.
Users query	An LDAP query for searching, retrieving, and importing users, e.g., (&(cn={0})(objectClass=user)) . Note that Users query and User groups query must be different. Both queries work only in the Search base scope.
User groups query	An LDAP query for searching, retrieving, and importing user groups, e.g., (&(cn={0})(objectClass=group)) . Note that Users query and User groups query must be different. Both queries work only in the Search base scope.
Specific for encryption data	
Encryption Protocol	The SSL and TLS are data encryption and authentication for a secure connection with the server. You can select None , SSL/TLS . Selecting None indicates you do not need to use an encryption protocol.
LDAP server certificate	The option to select a certificate file. The LDAP Server Certificate file is exported from the LDAP server to make a secure connection between the TWCloud Admin and LDAP server. Only files with the following extensions may be uploaded: crt, pem.
	To select a certificate file (enabled if SSL/TLS is selected).
	To remove the certificate file (enabled if either SSL/TLS is selected).

Authentication data

The **LDAP query** authentication method is selected by default. The Active Directory LDAP attribute name and value should be set to **(sAMAccountName={0})**. Besides **sAMAccountName**, you can use any attribute name, but it must be followed with **"={0}"**. The authentication information group should look like the following figure.

All LDAP users necessary to connect to Teamwork Cloud reside in **CN=Users**. The **Search Base** of this kind of LDAP server should be **CN=Users, DC=example,DC=com**. The pattern for the **Search Base** is **{Parent_Of_LDAP_Users},{Grand_Parent_Of_LDAP_Users},...{n}**.



Note

Configuring encryption data

Only users that are under the **Search Base** will be able to log in using the **User DN Template** authentication method. Other users in another subtree will be unable to log in. The LDAP server connection is secured with SSL/TLS protocol (LDAPS) at default port number 636. The Encryption Protocol must be SSL/TLS, and the LDAP server certificate file must be selected.

If the LDAP server is **OpenLDAP** or **ApacheDS**, the default attribute name is **uid**. If the LDAP server is set for **LDAP query**, the LDAP query for querying a user DN should be entered into the **Query** box. Click the following link for more information about the LDAP query <https://www.ietf.org/rfc/rfc2254.txt>.