

## 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

Administrator bind

Username

cn=admin,dc=example,dc=com

Password

\*\*\*\*\*

Enabled

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

Authentication

Search base

dc=example, dc=com

Authenticate using

LDAP query

Query


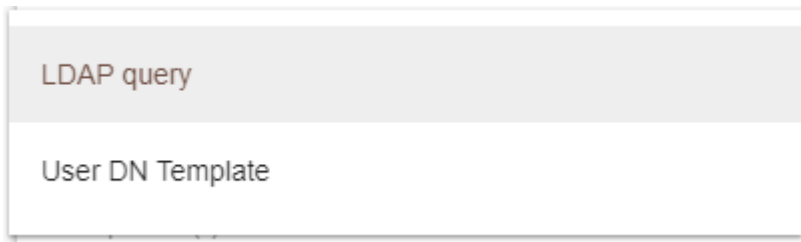

uid={0}


Encryption

Encryption protocol

None

The table below shows the components of **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.
Anonymous bind/Administrator bind	<p>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.</p> <p>If you select <b>Anonymous bind</b>, the Username and Password are not required and the system username and password will be disabled.</p>
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.
	To save the LDAP server's configuration properties. The function of this button is the same as that of the <b>Save</b> button on the <b>Edit LDAP Configuration</b> page.
<b>Specific for authentication data</b>	
Search base	The authentication methods. It defines the location in the directory from which the LDAP search begins.
	<p><b>LDAP query</b> - To search for users by LDAP query. This is the default option.</p> <p><b>User DN Template</b> - The button to search for users by User DN.</p>
User DN	To store a template for mapping user authentication with LDAP servers using the LDAP distinguished names.
Query	<p>An LDAP query for searching, retrieving and importing the DN of a user, e.g., <b>(uid={0})</b>.</p> <div>  <b>Note</b> </div>
<b>Specific for encryption data</b>	

Encryption Protocol	The SSL and TLS are data encryption and authentication for a secure connection with the server. You can select <b>None</b> , <b>SSL/TLS</b> . Selecting <b>None</b> indicates you do not need to use an encryption protocol.	
LDAP server certificate	• If you want to use other attributes, you need to The option to select a certificate file. The LDAP Server Certificate is pointed from the <b>User Group attribute</b> parameter in the <b>application.conf</b> . TWCloud configuration file as shown below and restart the	
	To select a certificate file (enabled if SSL/TLS is selected).	
	To remove selected	<pre>esi.ldap {     ...     usergroup.attribute = cn     ... }</pre>

## 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**

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. See the Authentication section in [Configuring LDAP properties](#) to configure the authentication method using **User DN Template**.

## Configuring encryption data

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 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. [rfc2254.txt](#).