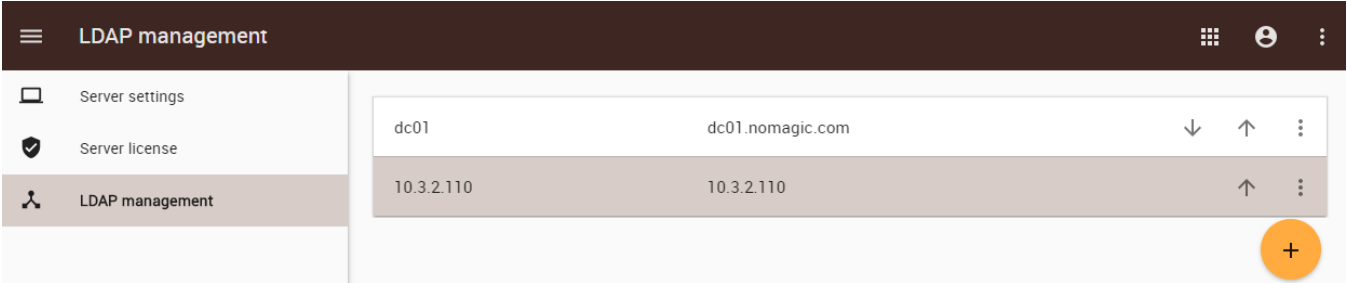


# Configuring LDAP properties

On this page

- [Create LDAP configuration pane](#)
- [Encryption protocol pane](#)
- [Authentication pane](#)

A Server Administrator can add as many LDAP servers to Teamwork Cloud (TWCloud) as needed. Depending on your permissions, you may edit a LDAP server's configuration, disable the server, or delete it. Once you have added the LDAP servers and successfully connected to them, the TWCloud Admin will store the servers on the **LDAP management** page.



The LDAP management page.

Before adding an LDAP server to TWCloud, you must configure the LDAP server's properties (such as the connection settings, server address, connection timeout, read timeout, and encryption protocol that will be used to connect to the LDAP server). Each LDAP server has its own setting properties. There are three LDAP configuration property sets that you must configure in following panes.

- [Create LDAP configuration pane](#)
- [Encryption protocol pane](#)
- [Authentication pane](#)

An [example of how to add an LDAP server to TWCloud](#) is also provided on the next page.

×

Create LDAP configuration

Configuration name \*

10.3.2.110

Server address \*

10.3.2.110

Connect timeout (ms) \*

5000

Read timeout (ms) \*

10000

☐ Anonymous bind

Username \*

CN=admin,CN=Users,DC=siemensdc,DC=local

Password \*


\*\*\*\*\*

☒ Enabled




Create LDAP configuration pane

## Create LDAP configuration pane





To start creating new LDAP configuration, click , the **Create LDAP configuration** pane opens. The table below shows the components of this pane.

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.

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 similar authentication service (10000 is the default value). This field is required.
 <b>Anonymous bind</b>	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 this check box, the Bind 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.
 <b>Enabled</b>	The option to enable a connection with the LDAP server.
	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.)

## Encryption protocol pane

The table below shows the UI components of the LDAP server Encryption properties.

Component	Description
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</b> , or <b>TLS</b> . Selecting <b>None</b> 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 either SSL or TLS is selected).
	To remove the certificate file (enabled if either SSL or TLS is selected).

## Authentication pane

You can select either one of the two authentication options available on the **Create LDAP directory** page:

- [Use User DN Template](#)
- [Retrieve User DN by using an LDAP query](#) (default)

The table below shows the UI components of the LDAP server's Authentication properties.

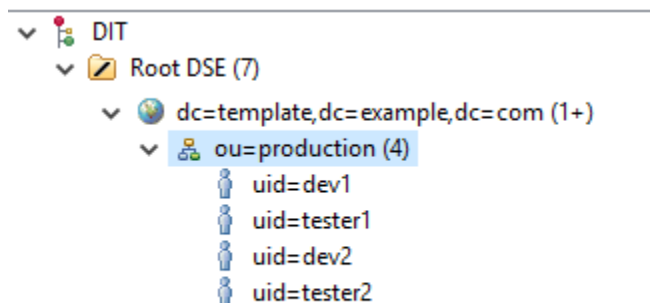
Component	Description
Search base	The authentication methods. It defines the location in the directory from which the LDAP search begins.

Authenticate using	<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	The LDAP query for retrieving the DN of a user, such as ( <b>uid={0}</b> ).

## Using the User DN Template authentication option

### When to use the User DN Template authentication option

The **DN Template** authentication will replace **{0}** with a username in TWCloud to create a full DN for authentication. Only the users in the specified search base can log in. The users above the **Search Base** and the users in a sub-level are unable to log in. For example, if we set up the LDAP server as follows.



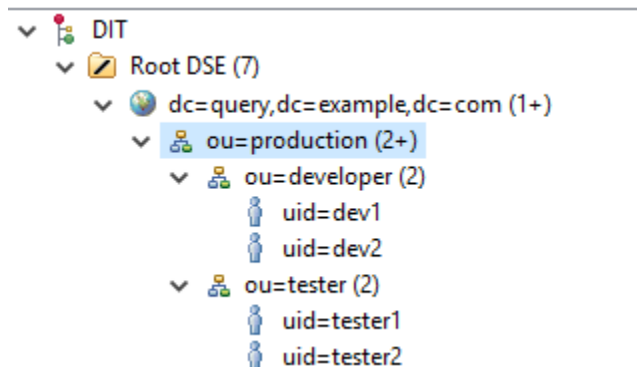
If we configure the TWCloud LDAP configuration page as follows.

- Search Base to "*ou=production,dc=template,dc=example,dc=com*"
- User DN to "*uid={0}*"

We allow the users in production to log into TWCloud.

### When to not use the User DN Template authentication option

The following is an example of Query Authentication (you cannot use **DN template** authentication for this case).



In this example, you have to choose which unit can log into TWCloud.

- If you set the search base to **ou=production,dc=template,dc=example,dc=com**, no user can log in.
- If you set the search base to **ou=developer,ou=production,dc=template,dc=example,dc=com**, only developer users can log in. Tester users will be unable to log in.

## Retrieving User DN by using an LDAP query

To allow all users under the specified search base to log in, you have to change the authentication method to **Retrieve User DN by using an LDAP query** instead.

### Finding the User DN on Linux

You can use the **ldapsearch** command on Linux to identify which attribute should be used in the **User DN** box.

```
ldapsearch -h <host> -p <port> -b "<your_searchbase>" -x -D "<your_systemuser>" -w <your_systempassword>
"(objectclass=*)"
```

#### Example

```
ldapsearch -h localhost -p 389 -b "dc=example,dc=com" -x -D "cn=admin,ou=system" -w "secret" "(objectclass=*)"
```

Then, take a look at the **dn** or **distinguishedName** attribute. The first attribute is the attribute that should be used in **User DN** for the LDAP configuration.

#### Example result

```
# firstname, People, example.com dn: cn=firstname surname, dc=example,dc=com
objectClass: top
objectClass: user
objectClass: organizationalPerson
objectClass: person
samaccountname: firstname
sn: surname
cn: firstname surname
distinguishedName: cn=firstname surname, dc=example,dc=com
```

In this result, **DN** starts with the **cn** attribute. So, you should enter **cn={0}** as the **User DN** when configuring the LDAP server.

### Finding the User DN on Windows (Active Directory)

To find your User DN on Windows (Active Directory)

- Run the following query in command prompt (from any server on your domain) to find the User Base DN.

```
dsquery user -name <any known username>
```

The following is an example of the result.

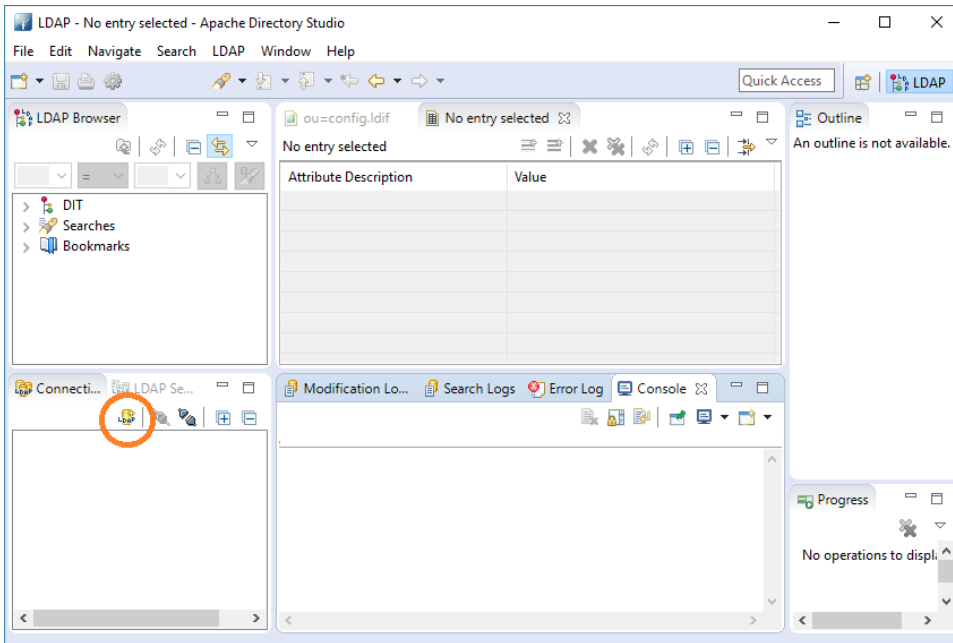
```
CN= firstname surname,CN=Users,DC=example,DC=com
```

So, the **User DN** should be **CN={0}** and the **Search Base** is **CN=Users,DC=example,DC=com**

### Finding the User DN using Apache Directory Studio

To find the User DN using Apache Directory Studio

1. Download Apache Directory Studio at <http://directory.apache.org/studio/>.
2. Open Apache Directory Studio.
3. Select **New Connection** to create a new LDAP connection.



4. Enter the hostname and the port of your LDAP server.

New LDAP Connection


—

□

×

Network Parameter

Please enter connection name and network parameters.



Connection name: Target LDAP

Network Parameter

Hostname: localhost

Port: 389


Encryption method: No encryption

Server certificates for LDAP connections can be managed in the '[Certificate Validation](#)' preference page.

Provider: Apache Directory LDAP Client API

Check Network Parameter

☐ Read-Only (prevents any add, delete, modify or rename operation)



< Back

Next >

Finish

Cancel

5. Enter your Bind DN and Bind password.

New LDAP Connection

Authentication

Please select an authentication method and input authentication data.

LDAP

Authentication Method

Simple Authentication

Authentication Parameter

Bind DN or user: cn=admin,ou=system

Bind password:

☒ Save password

Check Authentication

SASL Settings

Kerberos Settings

?

< Back

Next >

Finish

Cancel

- Double-click the created connection to connect to the LDAP server.
- In the LDAP Browser treeview, expand to your user account.
- Double-click the user account to see the details. The DN will appear on the right-hand side under the tab name.

LDAP Browser

uid=dev1,ou=developer,ou=production,dc=query,dc=example,dc=com

DN: uid=dev1,ou=developer,ou=production,dc=query,dc=example,dc=com

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	top (abstract)
cn	dev cn
sn	dev sn
uid	dev1

DIT

Root DSE (7)

dc=example,dc=com

dc=query,dc=example,dc=com (1+)

ou=production (2+)

ou=developer (2)

uid=dev1

uid=dev2

ou=tester (2)

dc=template,dc=example,dc=com (1+)

ou=production (4)

ou=config

ou=schema

ou=system

#### Related pages

Unknown macro: 'list-children'