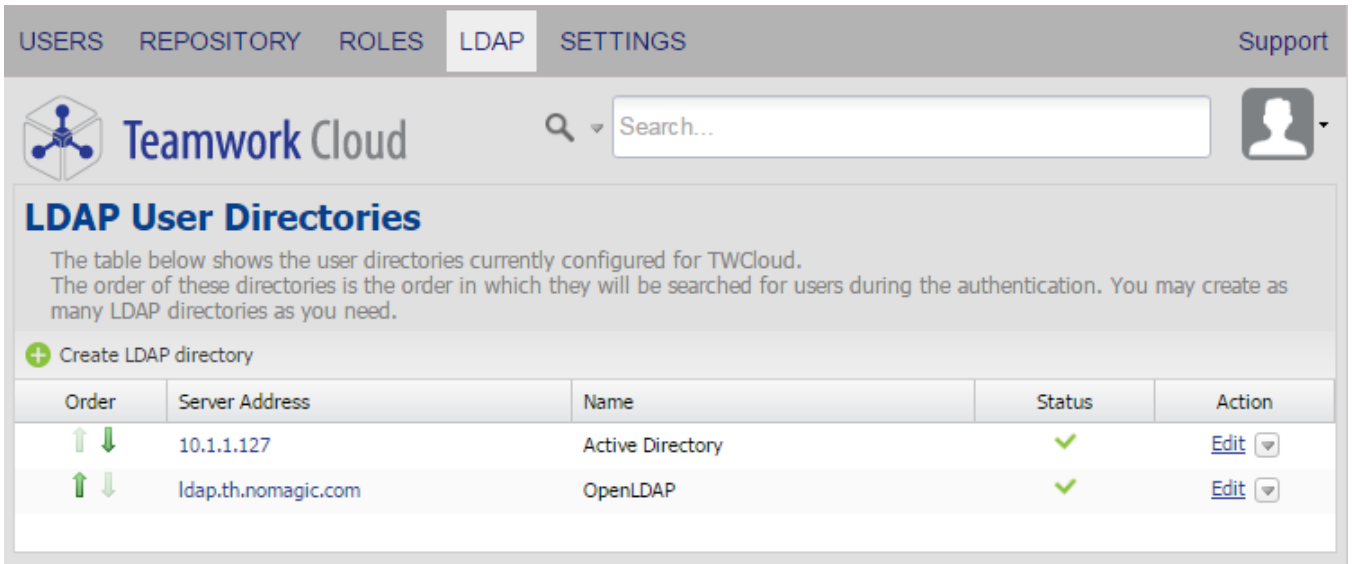
Configuring LDAP properties

On this page

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

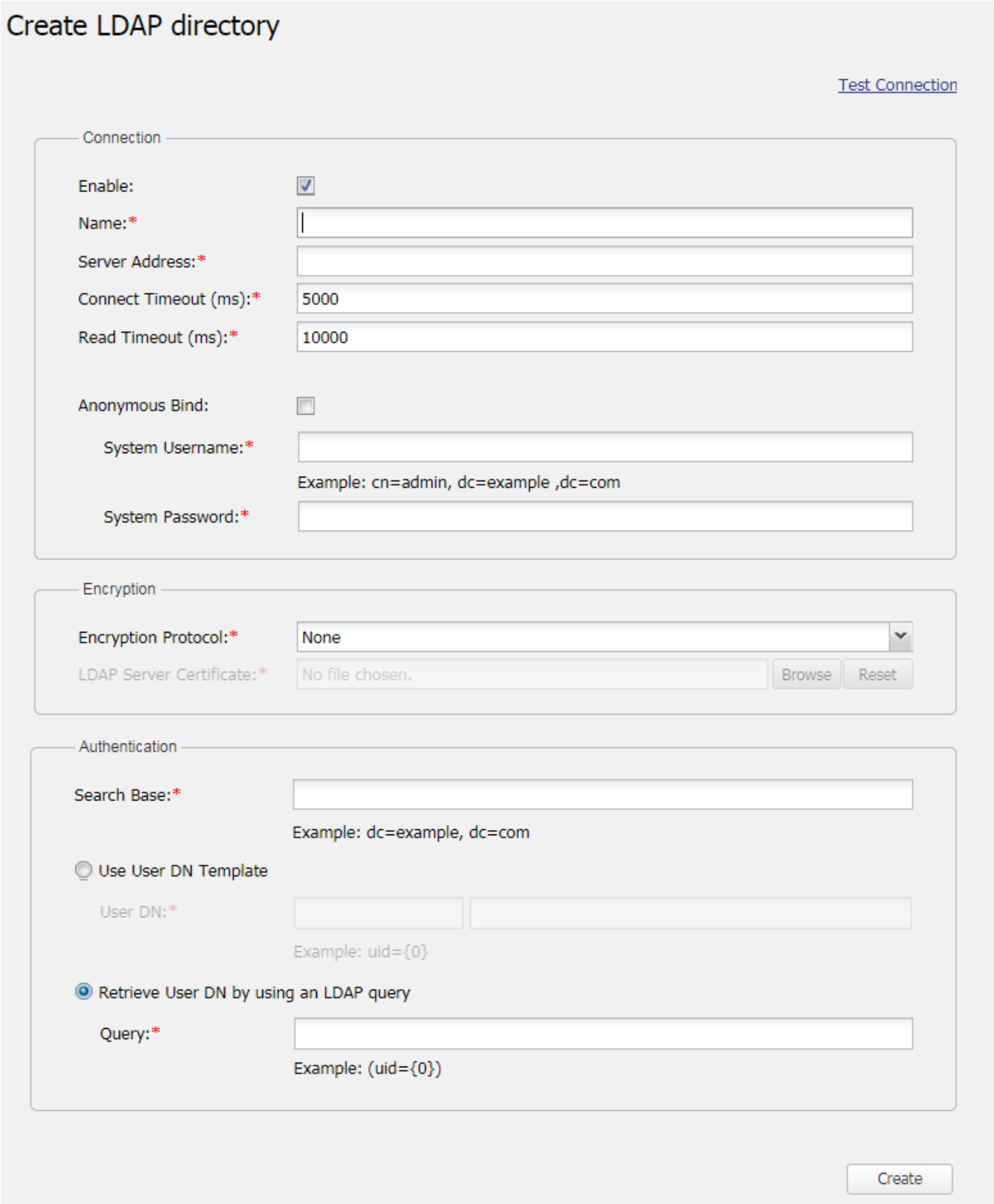


The LDAP User Directories page.

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 as follows.

- Connection
- Encryption
- Authentication

An example of how to add an LDAP server to TWCloud is also provided on the next page.



The LDAP server directory settings.

Connection

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

UI Component		Description
Test Connection		To test a connection to the specified LDAP server using the current configuration, system username, and password.
Connection	Enable: ☑	The option to enable a connection with the LDAP server.
	Name	To enter the connection name of the LDAP server. A duplicate name is allowed.
	Server Address	To enter the server IP address/hostname and the server port. 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. The port number is optional. If you do not specify the port number, the port number **389** will be used for non-encryption protocol and **636** will be used for SSL protocol.
	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.
	Anonymous Bind: ☐	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.
	System Username	The DN of a user to connect to the LDAP server and perform queries.
	System Password	The system password to connect to the LDAP server and perform queries.
Create		To create or save changes to the LDAP server's configuration properties. The function of this button is the same as that of the **Save** button on the **Edit LDAP Configuration** page.

Encryption

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

UI component		Description
Encryption	Encryption Protocol	The SSL and TLS are data encryption and authentication for a secure connection with the server. You can select **None**, **SSL**, or **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 TWAdmin and LDAP server.
	Browse	To select a certificate file (enabled if either SSL or TLS is selected).
	Reset	To clear the certificate file (enabled if either SSL or TLS is selected).

Authentication

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)

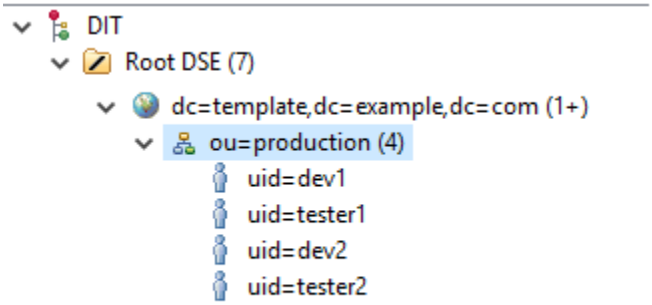
The table below shows the UI components of the LDAP server's Authentication properties.

UI component		Description
Authentication	Search Base	The authentication methods. It defines the location in the directory from which the LDAP search begins.
	Use User DN Template	The button 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.
	Retrieve User DN by using an LDAP query	To search for users by LDAP query. This is the default option.
	Query	The LDAP query for retrieving the DN of a user, such as **(uid={0})**.

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.



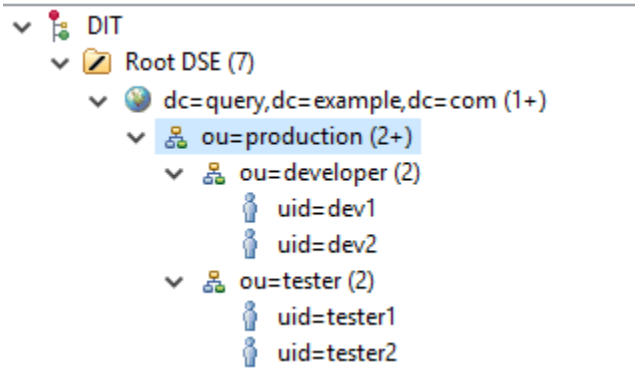
If we configure the TWCloud LDAP configuration page as follows.

- 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.

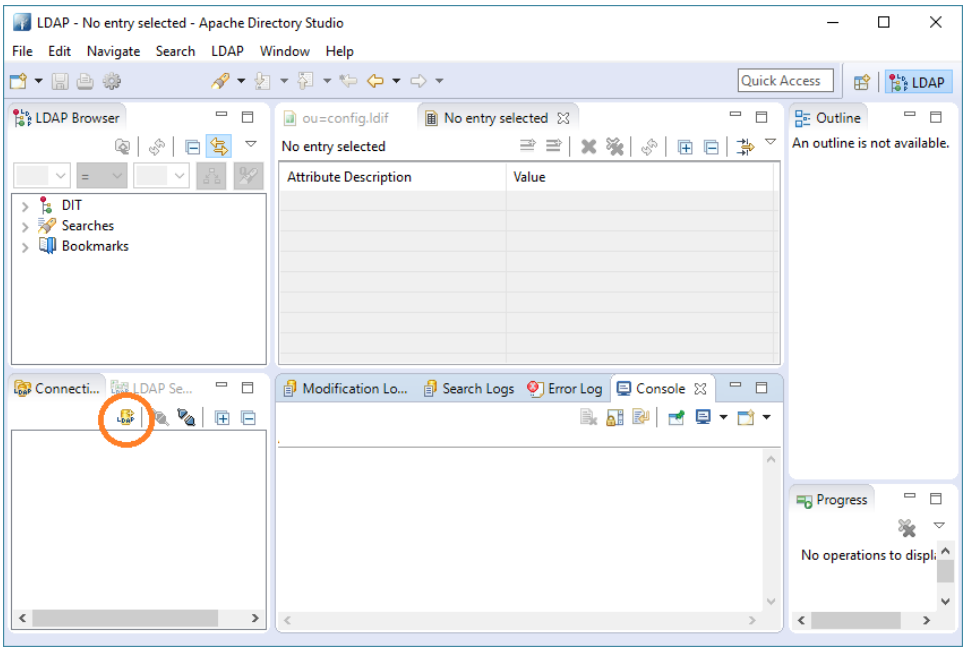
```
CN= firstname surname,CN=Users,DC=example,DC=com
```

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

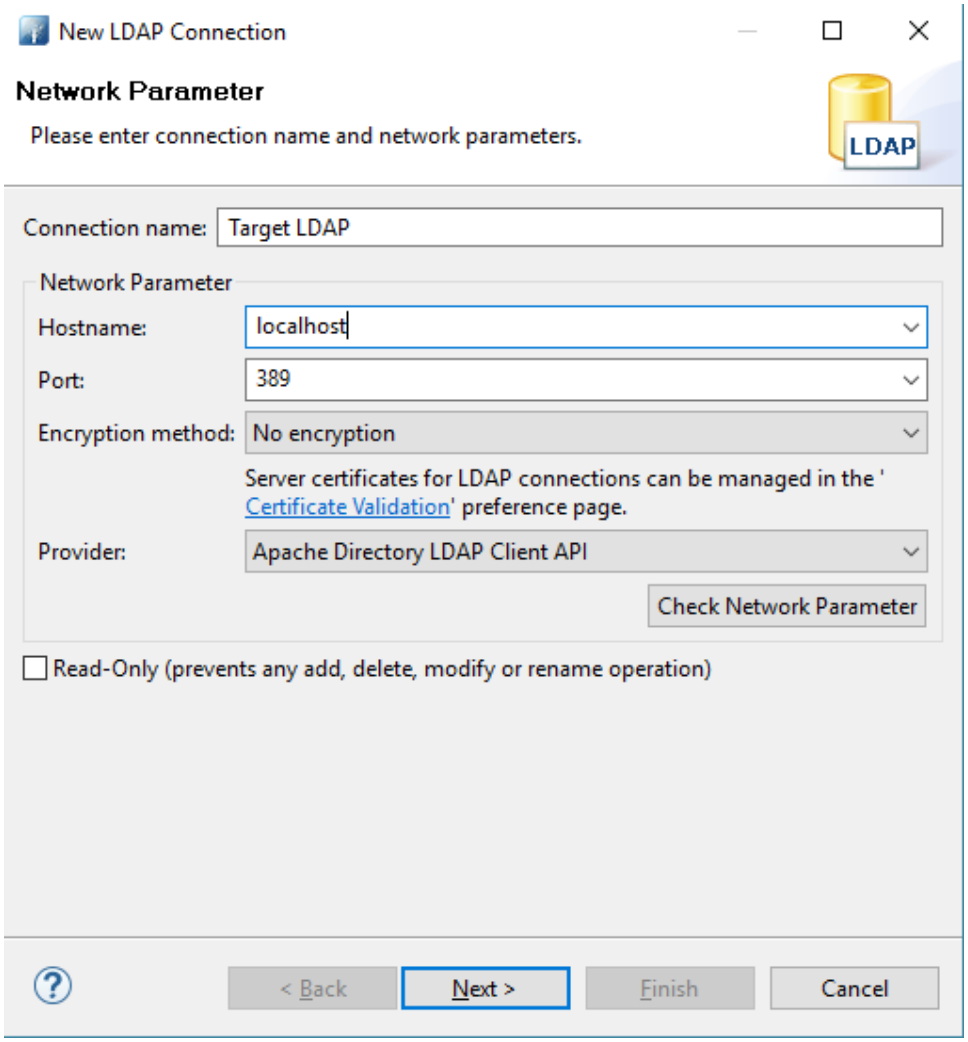
Finding the User DN using Apache Directory Studio

To find the User DN using Apache Directory Studio

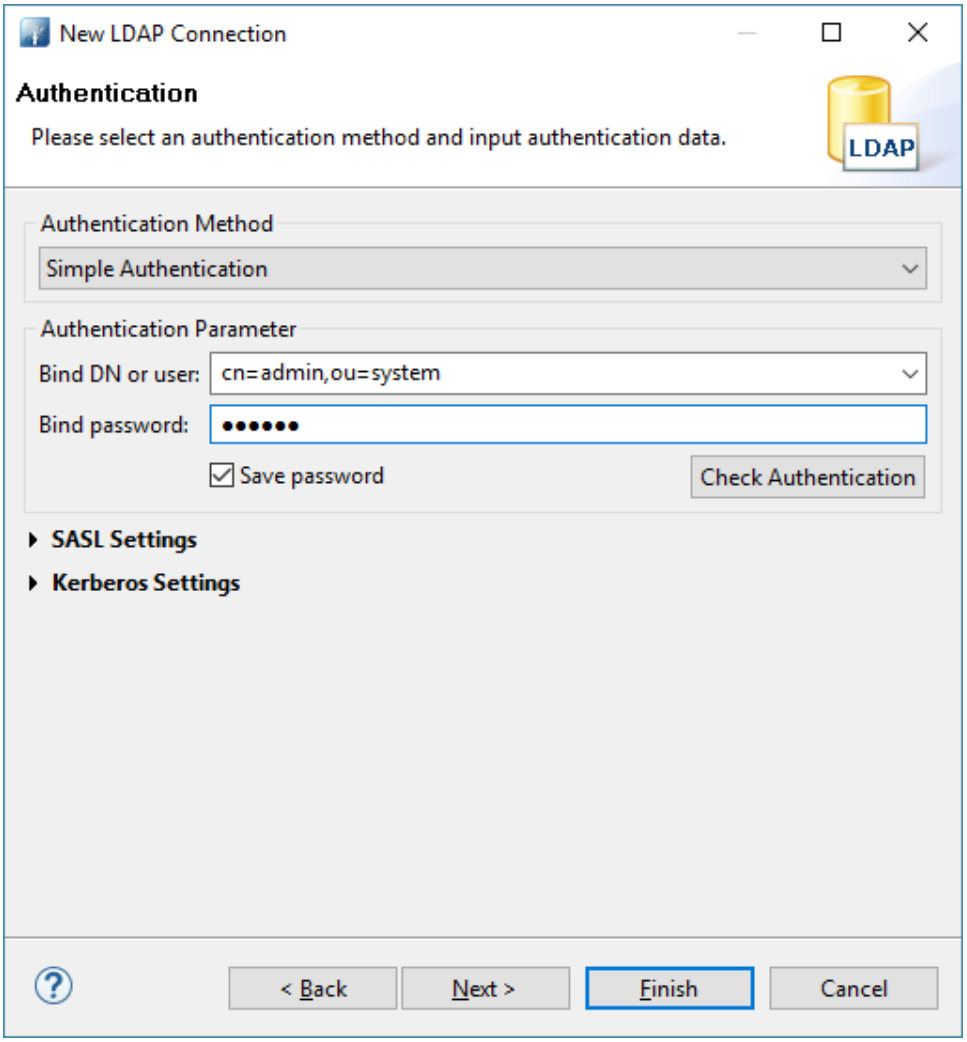
1. Download Apache Directory Studio at http://directory.apache.org/studio/.
2. Open Apache Directory Studio.
3. Select **New Connection** to create a new LDAP connection.



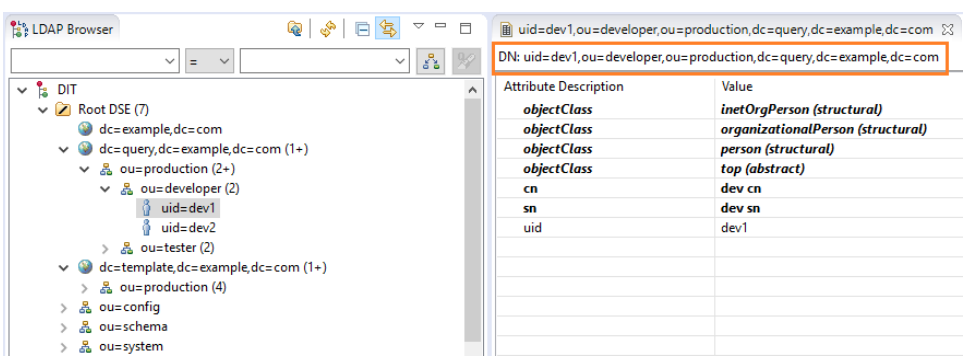
4. Enter the hostname and the port of your LDAP server.



5. Enter your Bind DN and Bind password.



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



Related pages

- LDAP setup for Active Directory and open LDAP
- LDAP TLS setup