

# LDAP Configuration Guide

Publication date: 11/8/2017

[www.xcalar.com](http://www.xcalar.com)

# Table of Contents

<b>About this guide</b> .....	<b>3</b>
<b>Configuring LDAP</b> .....	<b>4</b>
Before you start .....	5
Configuring and starting a new LDAP connection .....	6
<b>Adding users</b> .....	<b>10</b>
<b>Adding users to the LDAP administrators group</b> .....	<b>15</b>
<b>Creating additional Xcalar admin users</b> .....	<b>17</b>
<b>Removing users</b> .....	<b>18</b>
<b>Copyright and trademark information</b> .....	<b>20</b>

## About this guide

This guide is intended for the Xcalar administrator who has used the Xcalar Wizard to install Xcalar.

If you use the Lightweight Directory Access Protocol (LDAP) server deployed by Xcalar, follow the instructions in this guide to perform these tasks:

- Configure the LDAP server so that you can manage user accounts on it.
- Create user accounts on the LDAP server so that users can log in to Xcalar.
- Add users to the LDAP administrators group if you want multiple users to have administrator privileges on the LDAP server.
- Create additional Xcalar administrator accounts if you (or other users) want to log in to Xcalar with administrator privileges by using a login name other than admin.

## Configuring LDAP

You must configure the LDAP server before you can create and manage user accounts on it. (If you choose to use LDAP for user authentication, Xcalar users must have accounts on the LDAP server.) This section describes how to configure the LDAP server deployed by Xcalar on your Xcalar cluster.

This section assumes that you have successfully completed these tasks:

- Installing the OpenLDAP server on the first node (node 0) by using the Xcalar Wizard.
- Downloading and installing the latest version of Apache Directory Studio, which is an LDAP directory client, on a computer that can access node 0 of the Xcalar cluster. Apache Directory Studio is available at this website:

<https://directory.apache.org/studio/downloads.html>

**NOTE:** The screenshots in this document are from a Windows-based computer. The exact screens depend on the operating system of your computer running Apache Directory Studio.

## Before you start

Gather the following information:

- Fully qualified domain name (FQDN) or IP address of node 0 of the cluster. This information is used by Apache Directory Studio.

If you want to access node 0 through a private host name or address, you can find the name or address by entering the following commands on node 0:

```
cd /mnt/xcalar/config  
head -n1 privHosts.txt
```

- Password entered in Step 4 of the Xcalar Wizard.
- Domain name entered in Step 4 of the Xcalar Wizard.

The following screenshot shows Step 4 of the Xcalar Wizard, in which the password and domain name are entered:

## Configuring and starting a new LDAP connection

Follow these steps to configure and start a new LDAP connection:

1. Start Apache Directory Studio.
2. In the top menu, select clicking **LDAP > New Connection...** The **New LDAP Connection** window is displayed.
3. Enter the value for each field in the window as described in the following table:

Field	Value
Connection name	Any name to help you identify this connection
Hostname	Either: <ul style="list-style-type: none"> <li>• FQDN or IP address of node 0</li> <li>• private host name or IP address of node 0</li> </ul>
Port	389 (default)
Encryption method	Use StartTLS extension (recommended)
Provider	Apache Directory LDAP Client API

**IMPORTANT:** Do not click the check box for **Read-Only**.

The following screenshot shows the **Network Parameter** section of the **New LDAP Connection** window with sample configuration information.

4. Click **Next**.
5. Provide authentication information required for starting the connection to the LDAP server. Enter the value for each field as described in the following table:

Field	Value
Authentication method	Simple Authentication

Field	Value
Bind DN or user	<p>The value depends on how you set up your domain name in Step 4 of the Xcalar Wizard:</p> <ul style="list-style-type: none"><li>• If the domain name is in the form of <code>companyname.com</code>, enter the following information in this field: <code>cn=admin,dc=companyname,dc=com</code></li><li>• If the domain name is in the form of <code>word1.word2.word3.word4</code>, enter the following information in this field: <code>cn=admin,dc=word1,dc=word2,dc=word3,dc=word4</code></li></ul>
Bind password	The password entered in Step 4 of the Xcalar Wizard

The following screenshot shows the **Authentication** section of the **New LDAP Connection** window with sample configuration information.



**New LDAP Connection**

Please select an authentication method and input authentication data.

**Authentication**

Authentication Method: Simple Authentication

Authentication Parameter

Bind DN or user: cn=admin,dc=mycompany,dc=com

Bind password: ●●●●●●●●

Save password

Check Authentication

▶ SASL Settings

▶ Kerberos Settings

< Back   Next >   Finish   Cancel

6. Click the check box for **Save password**.
7. Click **Check Authentication** to verify that the credentials are correct.

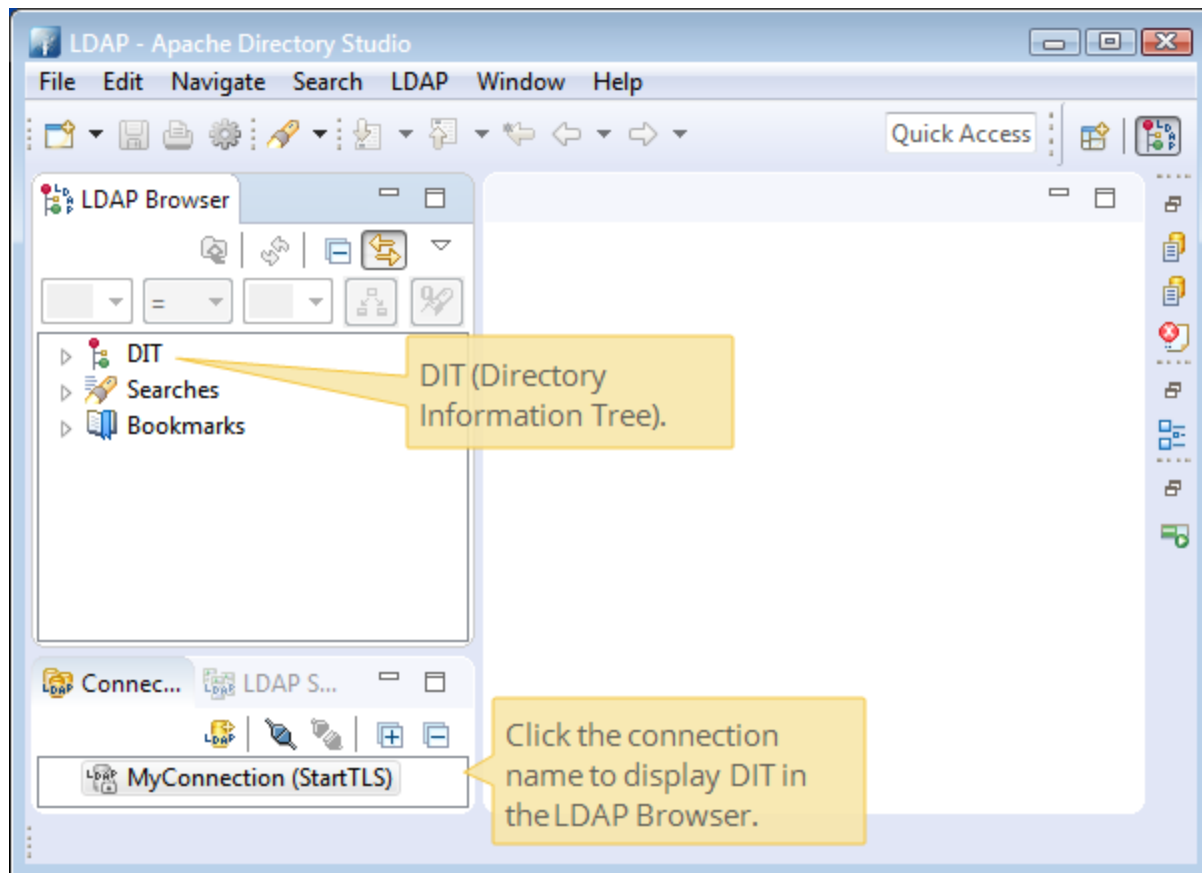
If you use TLS for encryption, a window may appear, prompting you to accept an SSL certificate. Accept the certificate either for this session or permanently. If authentication is not successful, verify the hostname of node 0, the ability to access to port 389 on node 0, the Bind DN, and the password.

8. Click **Finish** to open a connection to the LDAP server. After the connection is established, you can add user accounts on the LDAP server as described in [Adding users](#).

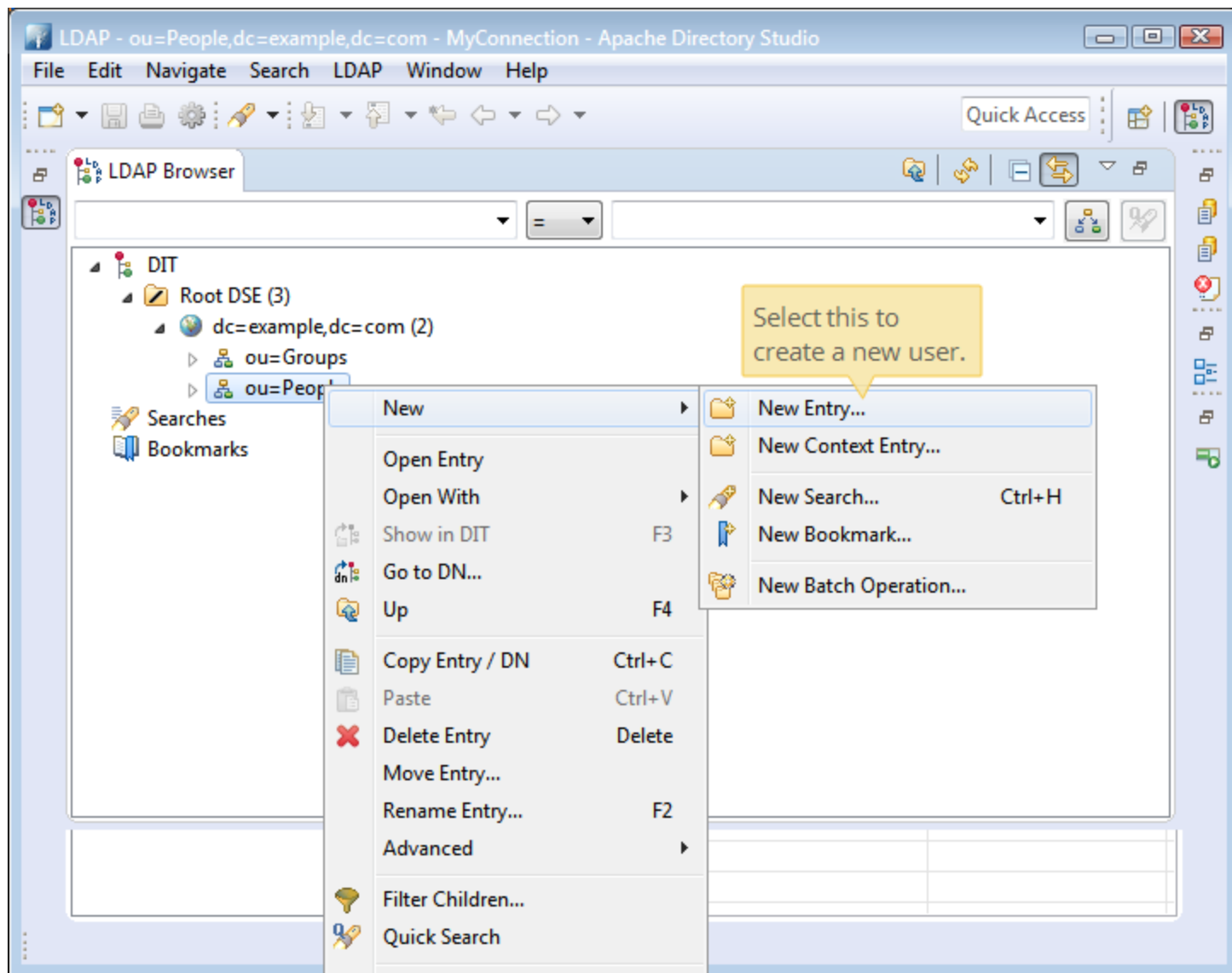
## Adding users

Follow these steps for adding each user:

1. In the **LDAP Browser** pane, locate **DIT** (Directory Information Tree) for your connection. If it is not displayed, click the connection name as shown in the following screenshot:



2. under **DIT** (Directory Information Tree), right click the **ou=People** entry to create a new entry for the organization unit, as shown in the following screenshot:



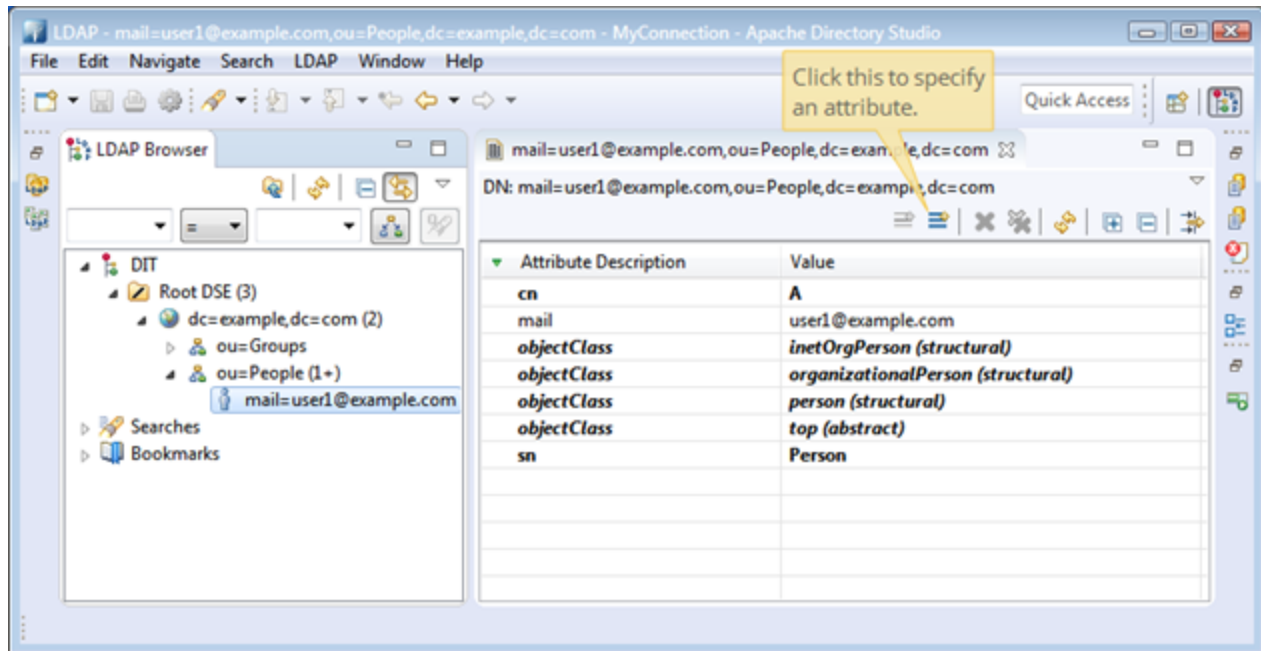
The **New Entry** wizard is started.

3. Select **Create entry from scratch**. Then click **Next**.
4. In the **Object Classes** dialog box, click **InetOrgPerson** in the list of available object classes and click **Add** to select it. Then click **Next**.
5. In the **Distinguished Name** dialog box, select **mail** for the **RDN** field and then the email address. This email address is the user name for the Xcalar login.

The following screenshot illustrates how to enter the information for a user whose user name is user1@example.com.

The screenshot shows the 'New Entry' dialog box. The title bar reads 'New Entry'. Below the title bar, there is a section titled 'Distinguished Name' with a folder icon. The text below this section says 'Please select the parent of the new entry and enter the RDN.' The 'Parent' field is a dropdown menu showing 'ou=People,dc=example,dc=com' with a 'Browse...' button to its right. The 'RDN' field is a dropdown menu showing 'mail' followed by an equals sign and a text box containing 'user1@example.com'. There are '+' and '-' buttons to the right of the text box. The 'DN Preview' field shows the resulting distinguished name: 'mail=user1@example.com,ou=People,dc=example,dc=com'. At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

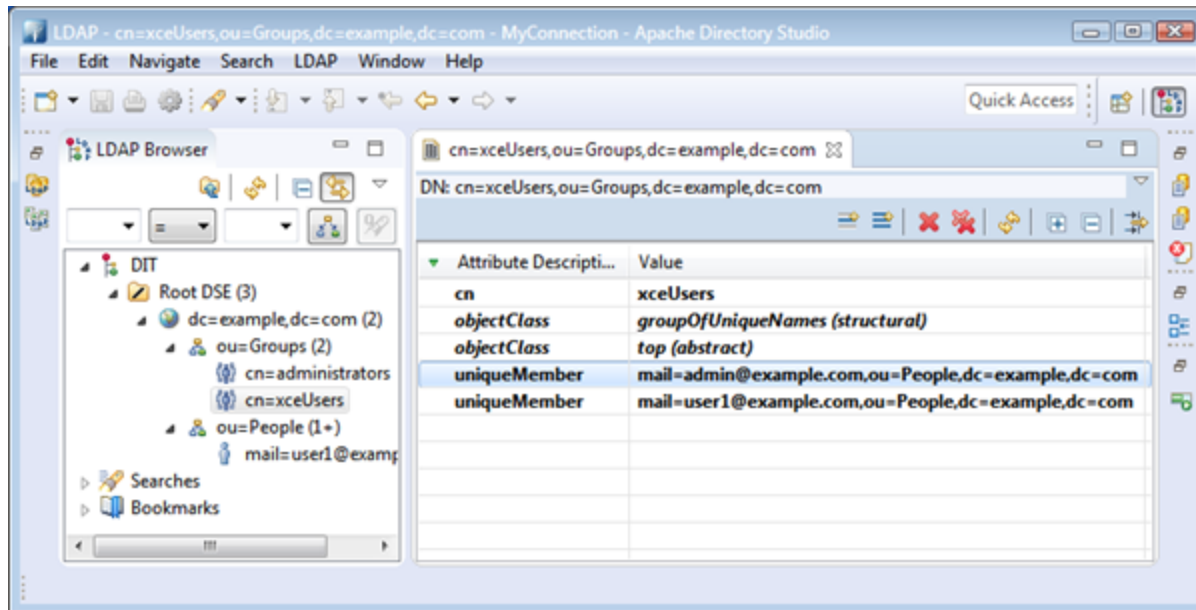
6. (Optional) Copy the information in the **DN Preview** field to your computer's clipboard so that you can paste the information later in this procedure.
7. Click **Next**.
8. In the **Attribute** dialog box, type the user's first name in the **cn** field and the user's last name in the **sn** field. Then click **Finish**. The user account is created.
9. To create a user password, add a new attribute, as shown in the following screenshot:



10. In the **Attribute Type** dialog box, select **userPassword** from the drop-down menu. Then click **Finish**.
11. In the **Password Editor**, enter and confirm the new password.
12. Select **SSHA** as the hash method. Then click **OK**. A password is now created for the user account.
13. Follow these steps to add the user's distinguished name (DN) to the group named xceUsers:
  - a. Under **ou=Groups**, click **cn=xceUsers**.
  - b. Right click in an existing **uniqueMember** entry the **Attribute Description** column and then select **New Value**.
  - c. In the new **uniqueMember** entry, paste or type the user's DN. For example, type the following DN:
 

```
mail=user1@example.com,ou=People,dc=example,dc=com
```
  - d. Press Enter.

The following screenshot illustrates the result of adding a user to xceUser.



## Adding users to the LDAP administrators group

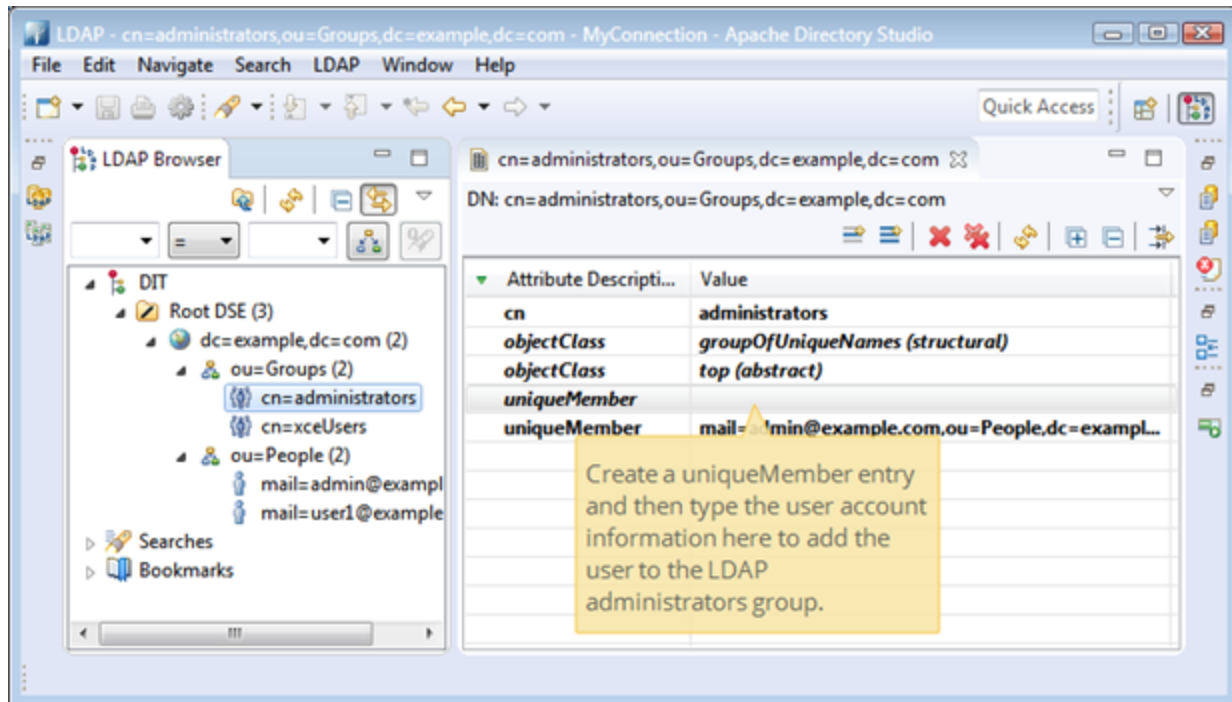
The admin account created by the Xcalar Wizard on the LDAP server has LDAP administrator privileges. The LDAP administrator can perform administrative tasks such as adding or removing user accounts.

If you want another user to have LDAP administrator privileges, add the user to the administrators group. The user must already have an account on the LDAP server.

Follow these steps in Apache Directory Studio when connected to the LDAP server:

1. In the **LDAP Browser** pane, click the **cn=administrators** entry under **ou=Groups**.
2. In the **Attribute Description** column, follow one of these steps:
  - If there is a **uniqueMember** entry with no value, right click **uniqueMember** and select **Edit Value**.
  - If there is not an empty **uniqueMember** entry (that is, if there is not a **uniqueMember** entry with no value), right click an existing **uniqueMember** entry and select **New Value**.

The following screenshot shows how to edit the **uniqueMember** entry. It is an example in which you create a **uniqueMember** entry because currently there is not an empty entry.



3. In the **Value** column for **uniqueMember**, enter the full DN of the user who will become an LDAP administrator as in this example:

`mail=user1@example.com,ou=People,dc=example,dc=com`

Press Enter.

The user whose DN is specified in the **uniqueMember** entry is an LDAP administrator. This user has write permission to modify the LDAP directory schema, using Apache Directory Studio.



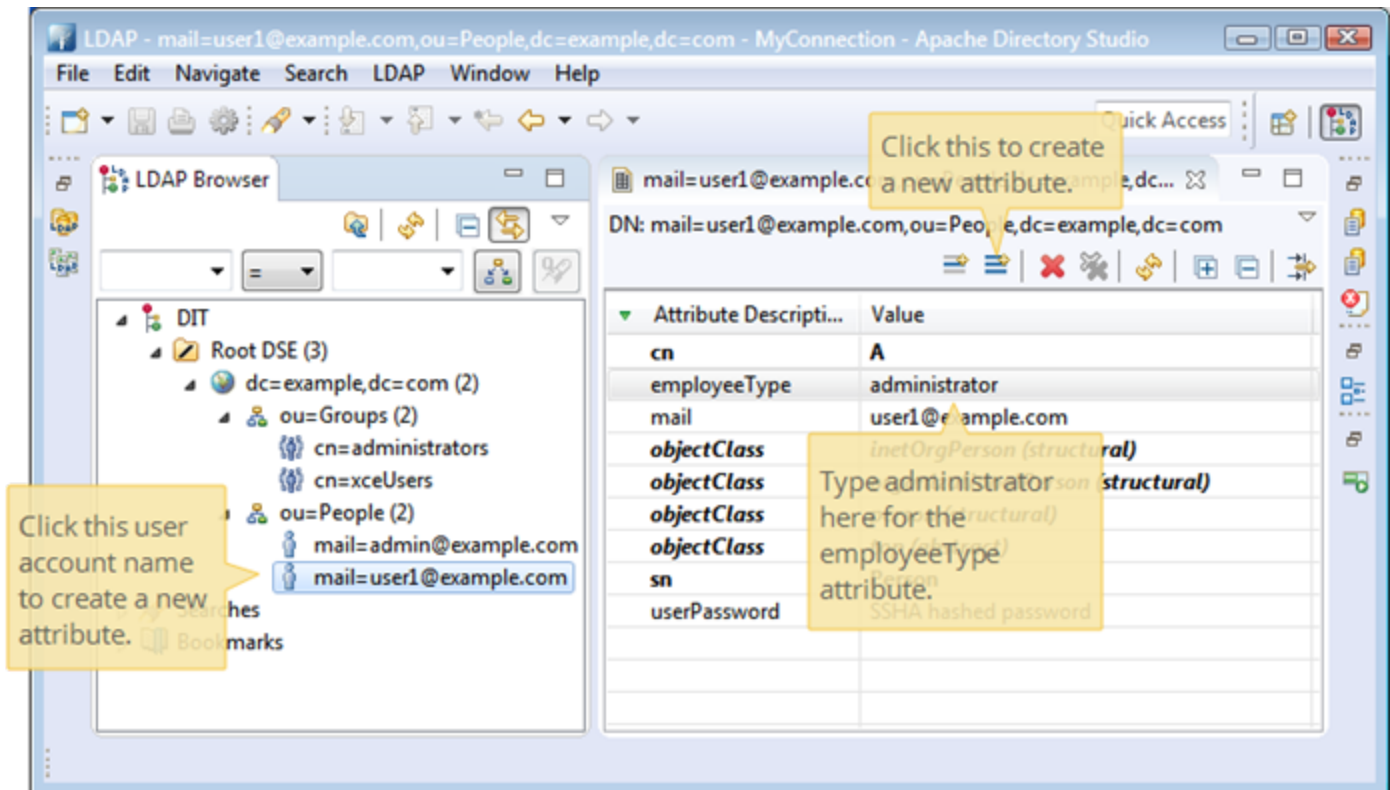
## Creating additional Xcalar admin users

The Xcalar Wizard creates an admin account for logging in to Xcalar. If you want another user to have Xcalar administrator privileges, follow these steps:

1. In the **LDAP Browser** pane, click the user's DN listed under **ou=People**.
2. In the **Attribute Description** column, right click and select **New Attribute...**
3. In the **New Attribute** dialog box, select **employeeType** as the attribute type.
4. Click **Finish**.
5. In the **Value** field for **employeeType**, type **administrator**.
6. Press Enter.

Now the user can log in to Xcalar as a Xcalar administrator.

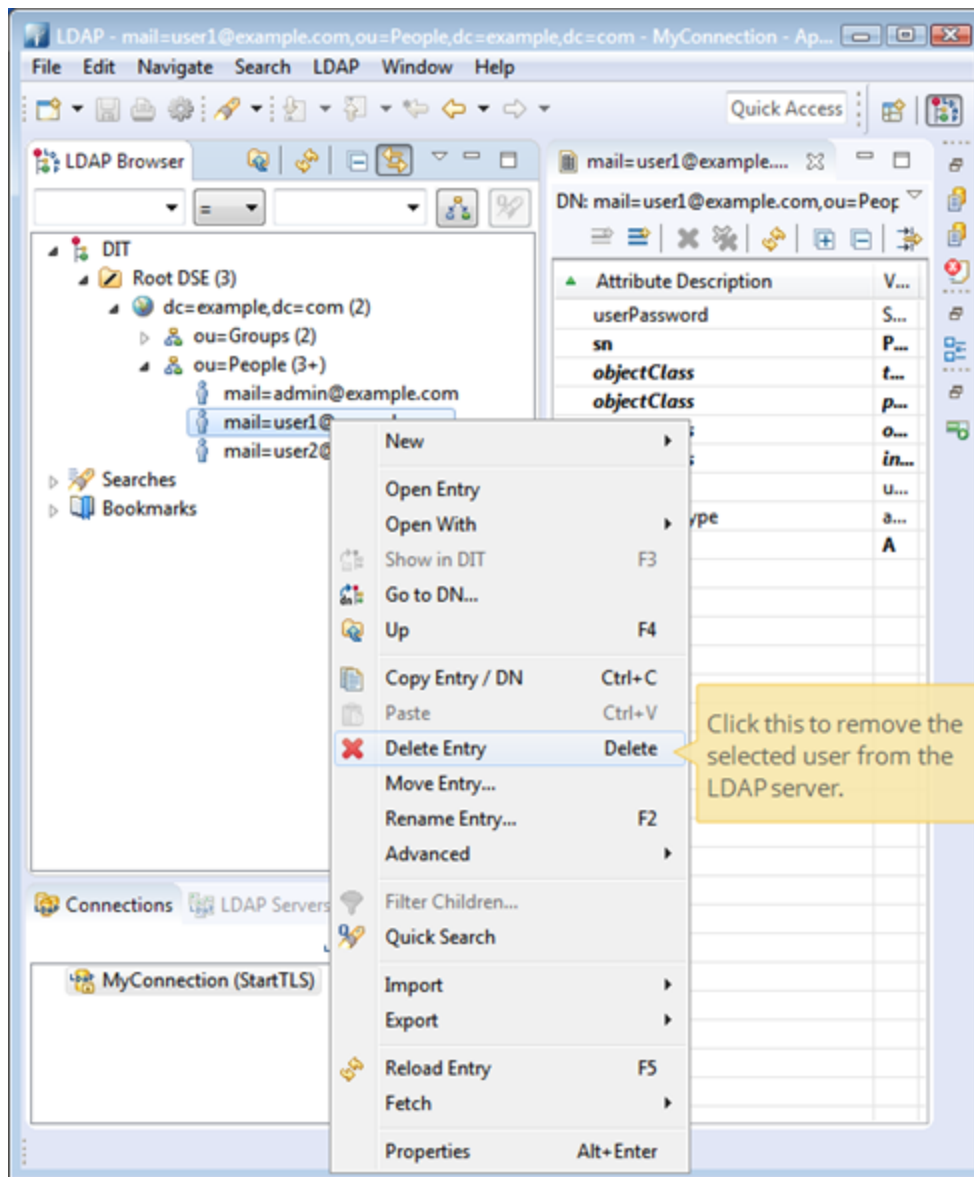
The following screenshot shows how to change a Xcalar user account to a Xcalar administrator account.



## Removing users

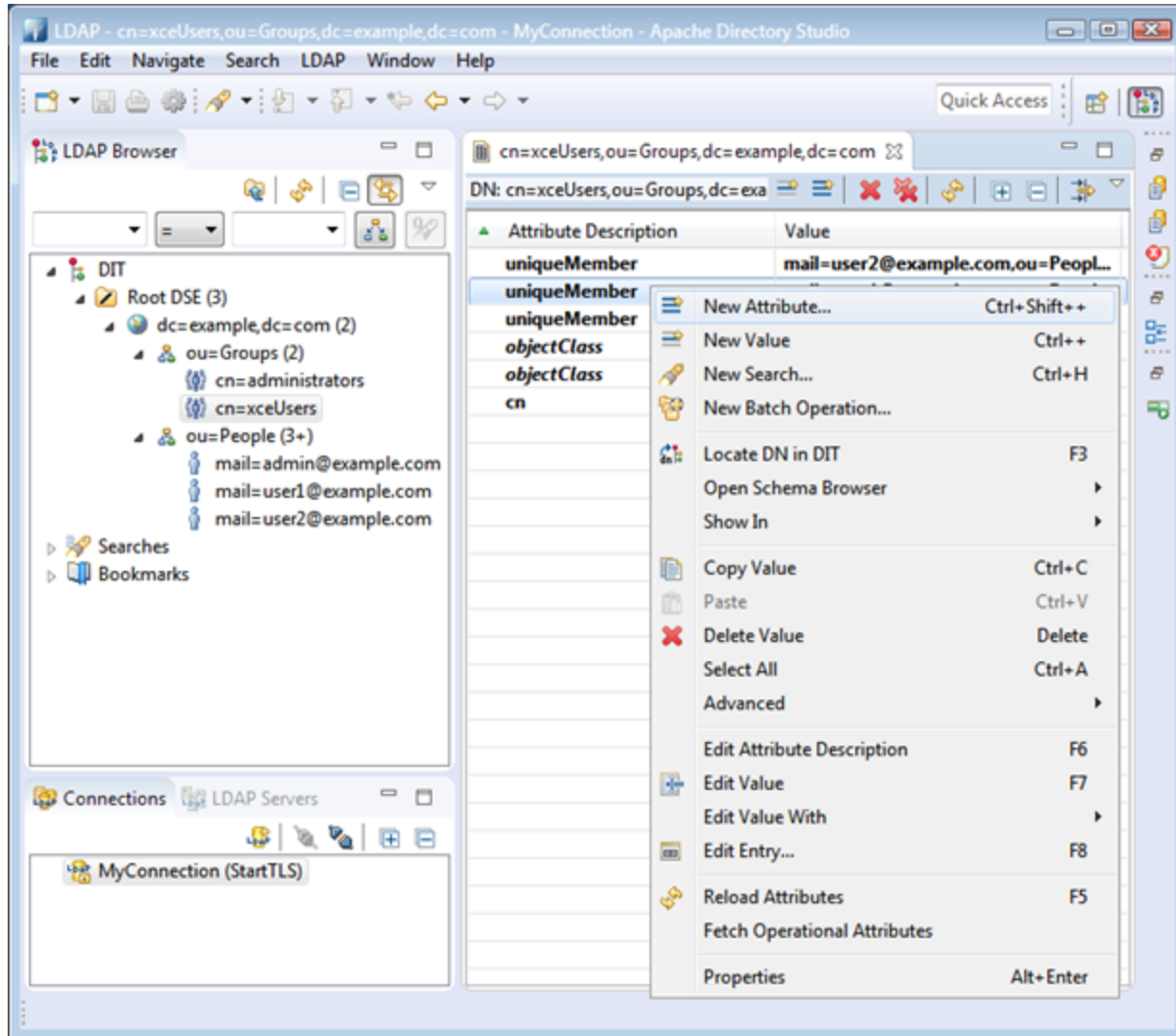
Follow these steps for removing a user:

1. Right click the user under **ou=People** in the DIT, as shown in the following screenshot:



2. Select **Delete Entry** in the drop-down menu.

- Depending on whether the user is in the xceUsers group or administrators group, click **cn=xceUsers** or **cn=administrators**.
- Locate the uniqueMember entry corresponding to the user. Right click the entry to display a drop-down menu, as shown in the following screenshot:



- Select **Delete Value** in the drop-down menu.

## Copyright and trademark information

© 2017 Xcalar, Inc. All rights reserved. Xcalar is a registered trademark of Xcalar, Inc.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

The Xcalar logo, Fundamental Discovery, True Data in Place, Xcalar Compute Engine, Xcalar Data Prep, Xcalar Data Science, Xcalar Design, Xcalar Operational Analysis, Xcalar TeraRow, and Xcalar Virtual Data Warehouse are trademarks of Xcalar, Inc.