

Clearspace LDAP and Active Directory Guide

This document explains how to configure Clearspace to integrate with an [LDAP](#) or [Active Directory](#) repository. You'll find the following in this document:

[Overview](#) (page 1)

[Configuring for LDAP During Setup](#) (page 1)

[Getting Debug Messages](#) (page 6)

[Setting a Custom Initial Context Factory](#) (page 7)

[Setting Connection Pool Defaults](#) (page 7)

Overview

You can use LDAP (Lightweight Directory Access Protocol), including Active Directory, for authenticating Clearspace users. A standard for user authentication and for storing user profile data, LDAP is a powerful tool for large organizations (or organizations integrating many applications) to simplify user account management.

By default, Clearspace doesn't use LDAP. Instead, it stores all user data in a database and performs authentication with that data. When you select LDAP instead as the authentication system, you're asking that Clearspace authenticate against your LDAP server. During setup, you specify which users and groups from LDAP you want Clearspace to use (although you needn't use groups defined in LDAP). Clearspace will query your LDAP server to ensure that users and groups (if you want) are nominally represented in the Clearspace database (so that users can be associated with content), but will authenticate against your LDAP server.

This topic will guide you through configuring Clearspace to use your LDAP server for authentication. These instructions assume that you're a competent LDAP administrator and that you're familiar with the Clearspace admin console. Any LDAP-compliant server should work, including Active Directory.

Note: If you're using Active Directory, make sure it allows LDAP querying. You might also be interested in [LDAP Querying Basics](#) at the Microsoft web site, or [LDAP Attributes](#) at the Computer Performance web site.

Configuring for LDAP During Setup

The Clearspace setup tool will guide you through configuring Clearspace for use with LDAP. The setup tool is designed to prompt you for the minimum information Clearspace needs to connect to your LDAP server and retrieve the needed information. At each step along the way, the setup tool will prompt you to test the information you enter before moving forward; this reduces the chances that you'll inadvertently complete the process with settings that won't work in everyday use. **Note:** If you need to update configuration for LDAP after using the setup tool, you can do so by changing values for LDAP-related system properties. In the admin console, you'll find these at System > Management > System Properties; scroll to locate the properties you want to change.

Deciding How to Use Data from LDAP

The default Clearspace settings for LDAP will query for *all* users and groups available at the connection you specify; all of these users and groups will become Clearspace users and groups. If this isn't what you want, you

can use an LDAP filter expression to limit the data retrieved from your server. You can also opt to use user data from your LDAP server, but not use its groups, instead defining groups using Clearspace. **Note:** Clearspace's use of LDAP user and group data is read-only; you can't make changes to LDAP data using Clearspace.

As you use the setup tool to configure Clearspace to use LDAP, you can make specific settings to meet your needs. The tool's three-step wizard includes separate steps for specifying which users to include and specifying which groups (if any) to include.

Here are a few common scenarios. You'll find more details below on how to get these results.

- Add to Clearspace all users and groups available from the LDAP server. This is the typical result when you accept Clearspace's default values for LDAP.
- Add only certain users, such as by limiting to those in a specific group or those who have a specific attribute. You do this in the setup tool by filtering users with a user filter LDAP expression.
- Add only certain groups from the LDAP server. As with users, you can use an LDAP filter to retrieve particular group data from your LDAP server.
- Don't add any group data from LDAP; instead, specify that you will define groups using the Clearspace UI. The groups you define will be stored in the Clearspace database, not the LDAP server. You can do this in the setup tool by opting not to use LDAP groups, then defining groups using the Clearspace admin console.

Starting the Setup Tool

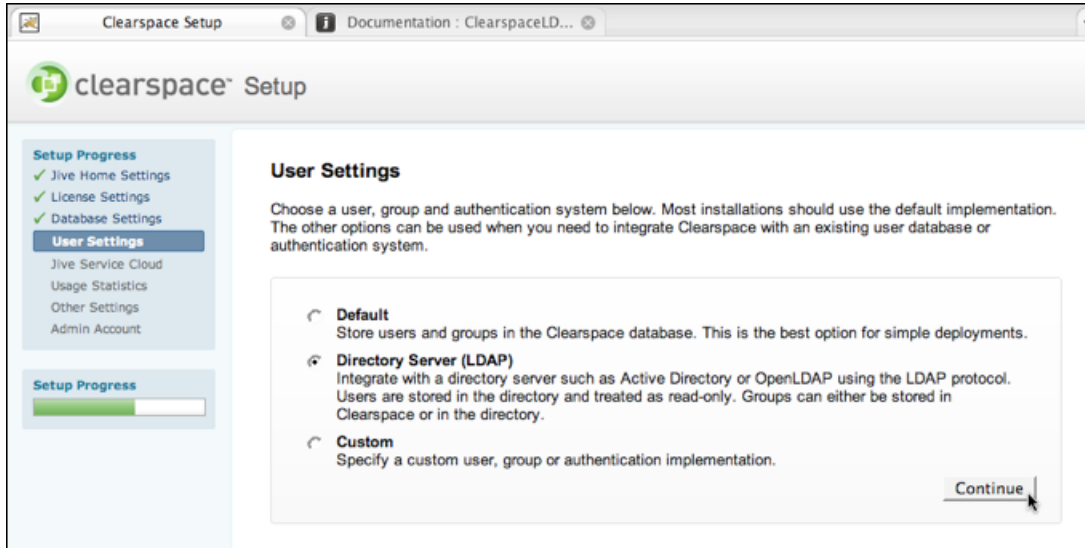
If you've just installed Clearspace, the setup tool will run the first time you access Clearspace. If you've already completed the setup process and need to use the tool again to configure LDAP, do the following:

1. Stop your application server.
2. If you're using Active Directory, make sure it allows LDAP querying.
3. Edit `<jiveHome>/jive_startup.xml` and change `<setup>>true</setup>` to `<setup>>false</setup>`.
4. Start your application server and navigate your browser to Clearspace to display the setup tool.

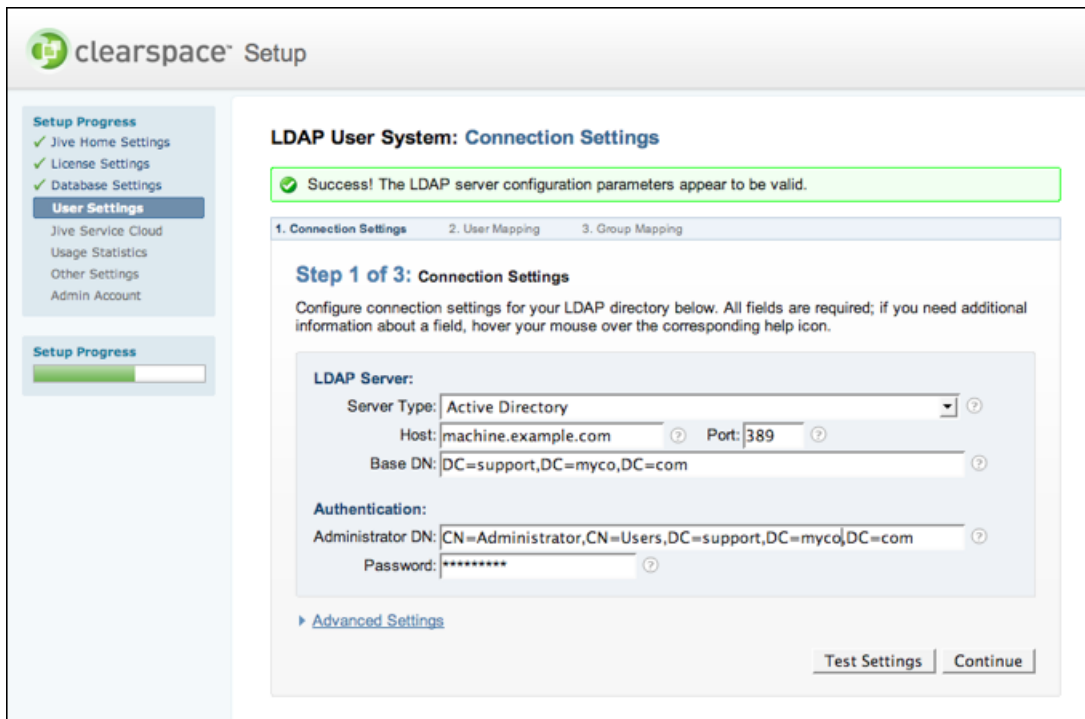
Configuring Clearspace for LDAP

Through three screens in the setup tool, you give information for connecting to the server, for querying for users, and how groups should be handled. At the outset, you choose a server type, such as Active Directory or OpenLDAP.

1. In the setup tool, on the **User Settings** step, choose **Directory Server (LDAP)** as the authentication and user mode, then click **Continue**.



2. On the **Connection Settings** page, enter the connection values required by your LDAP server. Your server type choice will determine the default values displayed later in the setup tool. In order to go to the next step, you need to set values for the **Server Type, Host, Port, and Base DN**, then click **Test Settings** and get a Success message. (Note that while the setup tool doesn't require or test them, your LDAP server might require an administrator DN and password; if so, be sure to enter them.)
3. Click **Advanced Settings** to make other connection-related settings. Be sure to see [Getting Debug Messages](#) (page 6) and [Setting Connection Pool Defaults](#) (page 7) as you make choices about those settings.
4. Click **Test Settings** to confirm the connection settings for host, port, and base DN.



5. When you get a successful test, click **Continue**.
6. On the **User Mapping** page, enter the names of fields your LDAP server uses for user data.

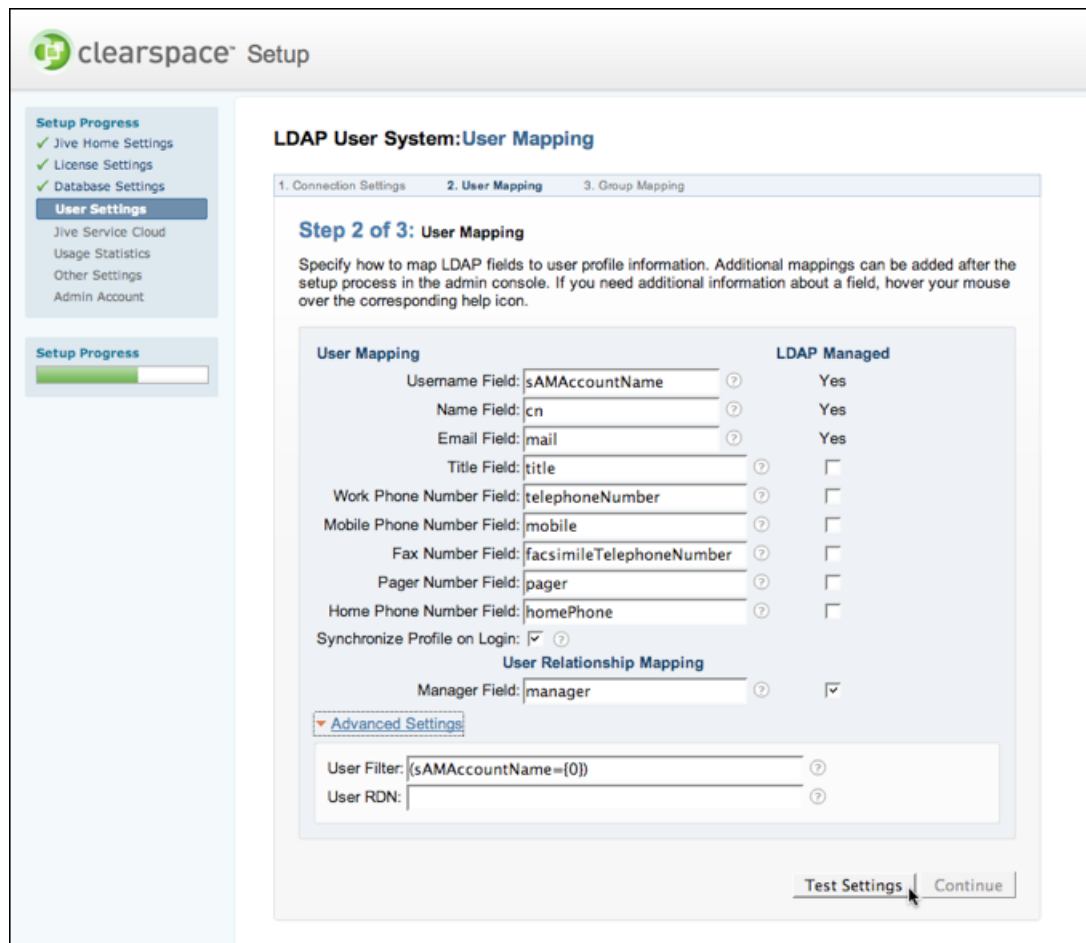
The setup tool provides default values based on the server type you chose in the **Connection Settings** step. In particular, you'll see the following defaults for Active Directory and OpenLDAP:

Option	Active Directory	OpenLDAP
Username Field	sAMAccountName	uid
Name Field	cn	cn
Email Field	mail	mail
User Filter	(sAMAccountName={0})	(uid={0})

Clearspace will use these values to query your LDAP server to retrieve information about the people who will be using Clearspace. The default values will include *all* users found with the connection settings you gave. You can limit this to only certain users by using an LDAP filter expression. For example, to retrieve only those users who work at the Portland office, you could enter something like the following in the **User Filter** box:

```
(&(physicalDeliveryOfficeName=Portland))
```

- After you've entered the values you need, click **Test Settings** to confirm that the values you entered are valid for your LDAP server.



- When you get a successful test, click **Continue**.

9. On the **Group Mapping** page, choose whether to use groups defined in LDAP or to define your own groups using Clearspace.

Select **Use LDAP to manage groups** if you have groups in LDAP that you want Clearspace to be aware of. With this option selected, Clearspace will retrieve your LDAP server's group information just as it did for your LDAP users.

Select **Use Clearspace to manage groups** if you want Clearspace to ignore groups you have defined in LDAP. This option is useful if you want to use Clearspace to define groups that are used only by Clearspace. Your LDAP server won't be aware of groups you define in Clearspace. You can use the Clearspace admin console to define groups; in the admin console, go to People > Management.

If you select **Use LDAP to manage groups**, the setup tool provides default values based on the server type you chose in the **Connection Settings** step. In particular, you'll see the following defaults for Active Directory and OpenLDAP:

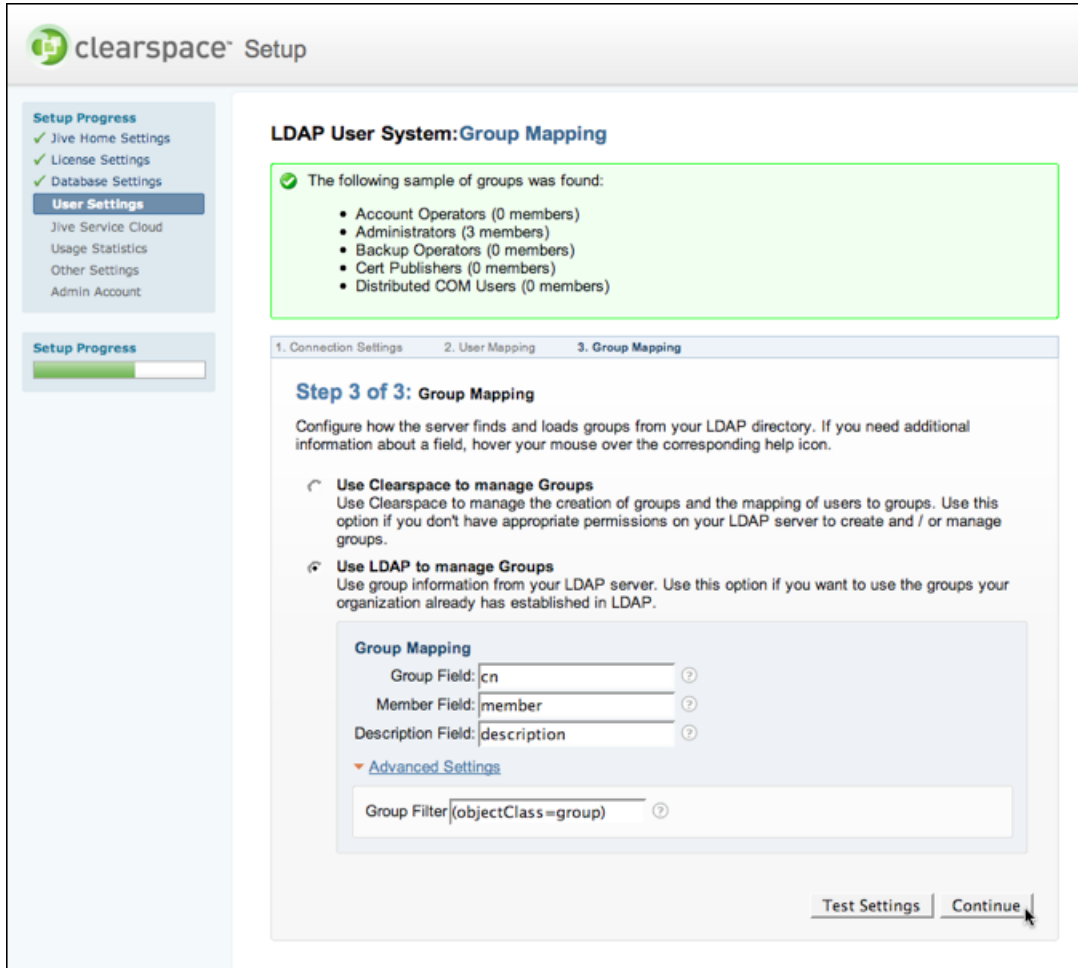
Option	Active Directory	OpenLDAP
Group Field	cn	cn
Member Field	member	member
Description Field	description	description
Group Filter	(objectClass=group)	

Clearspace will use these values to query your LDAP server to retrieve information about the groups to use. The default values will include *all* groups found with the connection settings you gave. You can limit this to only certain groups by using an LDAP filter expression.

10. After you've entered the values you need:

Click **Test Settings** if you're choosing to use LDAP groups; this will confirm that the values you entered are valid for your LDAP server. When you get a successful test, click **Continue**.

Click **Continue** if you're choosing to define groups in Clearspace.



11. Complete the **Other Settings** page and click **Continue**.
12. On the **LDAP User Data Storage Mode** page, enter the name of the user (retrieved from your LDAP server) who should be the Clearspace system administrator.
13. Click **Continue** to finish setting up.

Getting Debug Messages

You can get LDAP-specific debug information by selecting **Yes** for **Enable Debug** in the setup tool's **Step 3: Connection Settings** page. **Note:** If you turn on LDAP debugging, connection pooling will not be enabled.

You can also get broader Clearspace debug information by turning on verbose debugging inside the Clearspace application. Clearspace provides a fair number of debug messages. To enable this, turn on the debug log via the Log Viewer in the admin console. (In the console, go to **System > Management > Log Viewer**, click **Enabled**, then click **Update**. You'll need to restart the application server for this to take effect.) Due to the large amount of debug information this can generate (and the performance impact that has), you should run this only while developing or testing.

Once you've enabled debug messages, watch the jive.debug.log file. It should describe the steps it's going through to load users and authenticate them, as well as any errors it might run into. (You can view, download or email the debug log from within the admin console at the Log Viewer page described above.)

Setting a Custom Initial Context Factory

Some LDAP servers or application servers might require that a different LDAP initial context factory be used rather than the default (`com.sun.jndi.ldap.LdapCtxFactory`). You can set a custom initial context factory by adding the following to `jive_startup.xml`:

```
<ldap>
  ... other ldap settings here
  <initialContextFactory>your.FactoryClassName</initialContextFactory>
</ldap>
```

Setting Connection Pool Defaults

You might want to set Java system properties to change default pool settings. For more information, see the following pages:

<http://java.sun.com/products/jndi/tutorial/ldap/connect/pool.html>
<http://java.sun.com/products/jndi/tutorial/ldap/connect/config.html>

Note: If you turn on LDAP debugging, connection pooling will not be enabled.

Notes About LDAP, Active Directory, and the Clearspace Database

Don't Allow Duplicate Email Addresses

Clearspace doesn't currently support more than one user account with the same email address. When synchronizing with LDAP, Clearspace will include only the first account it finds with a given email address and will ignore other accounts with the same email address.

Handling Deleted Users

Because Clearspace doesn't currently support deleting users from its database, you'll need to work around situations in which you delete a Clearspace user from LDAP. When a user first logs in to Clearspace (or when you first synchronize LDAP with Clearspace), the application creates profile information for them in its database. After that, you'll be unable to delete the user from Clearspace. In addition, if you later add a user whose email address is the same as the deleted user's, the new user won't be able to log in.

One workaround is to disable the deleted user and alter their email address in Clearspace. After deleting the user from LDAP, use the Clearspace admin console to edit their account. *Disable the user*, then change their email address to something that's unique in the system and doesn't belong to another user (for example, you might use an `example.com` address).