

LDAP and Active Directory Guide

jive

Contents

LDAP and Active Directory Guide	2
Overview	2
Configuring for LDAP During Setup	2
Deciding How to Use Data from LDAP.....	2
Starting the Setup Tool.....	3
Configuring the Application for LDAP.....	3
Getting Debug Messages	7
Setting a Custom Initial Context Factory	7
Setting Connection Pool Defaults	7
Example LDAP Filters	7
Selecting a Subset of LDAP Users.....	7

LDAP and Active Directory Guide

When you have your own LDAP or Active Directory repository, you can configure your community to integrate with it.

Overview

You can use LDAP (Lightweight Directory Access Protocol), including Active Directory, for authenticating 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, the application 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 the application authenticate against your LDAP server. During setup, you specify which users and groups from LDAP you want the application to use (although you needn't use groups defined in LDAP). Jive SBS will query your LDAP server to ensure that users and groups (if you want) are nominally represented in the application database (so that users can be associated with content), but will authenticate against your LDAP server.

This topic will guide you through configuring the application to use your LDAP server for authentication. These instructions assume that you're a competent LDAP administrator and that you're familiar with the 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 Jive SBS setup tool will guide you through configuring the application for use with LDAP. The setup tool is designed to prompt you for the minimum information the application 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 Jive SBS settings for LDAP will query for *all* users and groups available at the connection you specify; all of these users and groups will become application 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 the application.

Note: The application's use of LDAP user and group data is read-only; you can't make changes to LDAP data using the application.

As you use the setup tool to configure the application 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 all users and groups available from the LDAP server. This is the typical result when you accept 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 UI. The groups you define will be stored in the application 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 admin console.

Starting the Setup Tool

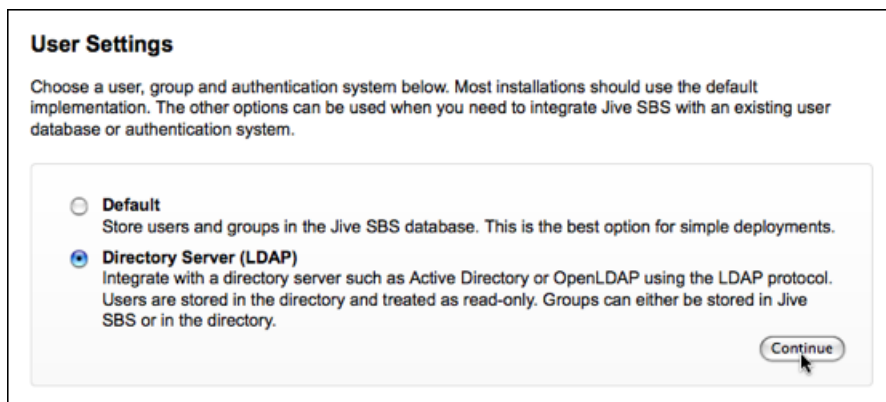
If you've just installed, the setup tool will run the first time you access the application. If you've already completed the setup process and need to use the tool again to configure LDAP, do the following:

1. Stop the jive-application service from the command prompt: `/etc/init.d/jive-application stop`
2. Edit `/usr/local/jive/applications/sbs/home/jive_startup.xml` so that the `<setup>` element has the value "false" (meaning "setup has not been run").
3. Start the jive-application service from the command prompt: `/etc/init.d/jive-application start`
4. Point your browser at Jive SBS using the URL above and rerun the setup tool.

Configuring the Application 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 7) 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.

LDAP User System: Connection Settings

1. Connection Settings 2. User Mapping 3. Group Mapping

Step 1 of 3: Connection Settings

Configure connection settings for your LDAP directory below. All fields are required; if you need additional information about a field, hover your mouse over the corresponding help icon.

LDAP Server:

Server Type: ?

Host: ? Port: ?

Base DN: ?

Authentication:

Administrator DN: ?

Password: ?

[Advanced Settings](#)

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.

LDAP User System: User Mapping

1. Connection Settings 2. User Mapping 3. Group Mapping

Step 2 of 3: User Mapping

Specify how to map LDAP fields to user profile information. Additional mappings can be added after the setup process in the admin console. If you need additional information about a field, hover your mouse over the corresponding help icon.

User Mapping	LDAP Managed
Username Field: <input type="text" value="sAMAccountName"/> ?	<input checked="" type="checkbox"/> Yes
Name Field: <input type="text" value="cn"/> ?	<input checked="" type="checkbox"/> Yes
First Name Field: <input type="text" value="givenName"/> ?	<input type="checkbox"/>
Last Name Field: <input type="text" value="sn"/> ?	<input type="checkbox"/>
Email Field: <input type="text" value="mail"/> ?	<input checked="" type="checkbox"/> Yes
Title Field: <input type="text" value="title"/> ?	<input type="checkbox"/>
Department Field: <input type="text" value="department"/> ?	<input type="checkbox"/>
Work Phone Number Field: <input type="text" value="telephoneNumber"/> ?	<input type="checkbox"/>
Mobile Phone Number Field: <input type="text" value="mobile"/> ?	<input type="checkbox"/>
Fax Number Field: <input type="text" value="facsimileTelephoneNumber"/> ?	<input type="checkbox"/>
Pager Number Field: <input type="text" value="pager"/> ?	<input type="checkbox"/>
Home Phone Number Field: <input type="text" value="homePhone"/> ?	<input type="checkbox"/>
Synchronize Profile on Login: <input type="checkbox"/> ?	
User Relationship Mapping	
Manager Field: <input type="text" value="manager"/> ?	<input type="checkbox"/>

[Advanced Settings](#)

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

Option	Active Directory	OpenLDAP
Name Field	cn	cn
First Name Field	givenName	givenName
Last Name Field	sn	sn
Email Field	mail	mail
User Filter	(sAMAccountName={0})	(uid={0})

The application will use these values to query your LDAP server to retrieve information about the people who will be using the application.

Note: If you're upgrading the application from a version that supported only "Name Field," you can still switch the first-and-last configuration. After you upgrade, go to the admin console page at System > Management > System Properties. At the bottom of the page, add the following system properties:

Property	Value
ldap.firstNameField	givenName
ldap.lastNameField	sn
jive.user.lastname.firstname.enabled	true

After you add the properties, navigate in the console to **People > Settings > User Data Synchronization Settings**. To pick up changes immediately, click **Run Synchronization Task Now**. If you already have synchronization enabled, you can also wait for its nightly run.

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. If any of the fields were not represented in the test results, you'll see those fields highlighted in red. For those highlighted values that you know should be mapped anyway, click the **LDAP Managed** check box.

1. Connection Settings 2. User Mapping 3. Group Mapping

Step 2 of 3: User Mapping

Specify how to map LDAP fields to user profile information. Additional mappings can be added after the setup process in the admin console. If you need additional information about a field, hover your mouse over the corresponding help icon.

User Mapping		LDAP Managed ?
Username Field:	sAMAccountName ?	Yes
Name Field:	cn ?	Yes
First Name Field:	givenName ?	<input checked="" type="checkbox"/>
Last Name Field:	sn ?	<input checked="" type="checkbox"/>
Email Field:	mail ?	Yes
Title Field:	title ?	<input checked="" type="checkbox"/>
Department Field:	department ?	<input checked="" type="checkbox"/>
Work Phone Number Field:	telephoneNumber ?	<input checked="" type="checkbox"/>
Mobile Phone Number Field:	mobile ?	<input type="checkbox"/>
Fax Number Field:	facsimileTelephoneNumber ?	<input type="checkbox"/>
Pager Number Field:	pager ?	<input type="checkbox"/>
Home Phone Number Field:	homePhone ?	<input type="checkbox"/>
Synchronize User's Profile on Login:	<input checked="" type="checkbox"/> ?	
User Relationship Mapping		
Manager Field:	manager ?	<input checked="" type="checkbox"/>

[Advanced Settings](#)

Test Settings Continue

- When you get a successful test, click **Continue**.
- On the **Group Mapping** page, choose whether to use groups defined in LDAP or to define your own groups using the application. Select **Use LDAP to manage groups** if you have groups in LDAP that you want Jive SBS to be aware of. With this option selected, the application will retrieve your LDAP server's group information just as it did for your LDAP users. Select **Use Jive SBS to manage groups** if you want the application to ignore groups you have defined in LDAP. This option is useful if you want to use the application to define groups that are used only by it. Your LDAP server won't be aware of groups you define in the application. You can use the 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
Member Field	memberOf	(Depends on installation.)
Group Filter	(objectClass=group)	'

Use the Member Field option as a way to increase performance. When your LDAP installation provides a way to have user objects be aware of the groups each user is a member of, giving the user object's "member of" attribute provides a more efficient (and faster) way for the application to get the list of groups a user is in.

Jive SBS 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 the application.

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 system administrator.

13. Click **Continue** to finish setting up.

Note: In the **Admin Account** step of the setup tool, you'll be prompted to choose a location for the admin account: **LDAP** (using the administrator from the LDAP server you just set up) or **the database** (meaning an account in the application database). If you choose LDAP, be sure to enter in the **Current Username** box the account of a valid LDAP user. The name displayed there by default might not be an account you can actually use.

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 debug information by turning on verbose debugging inside the application. Jive SBS 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.

Example LDAP Filters

Selecting a Subset of LDAP Users

If you know that only some of the users in your LDAP database should be known to the application, one way to get that subset is to create an LDAP group (such as "Jive SBS users"), then filter off that group attribute for users. Here's an example:

```
(&({sAMAccountName={0}})(memberOf=CN=applicationUsers,OU=ExampleGroups,DC=example,DC=com))
```

This way you don't have to create any new OUs or move records around. You can simply modify group membership attributes on the user, something the LDAP administrator can do.