

# LDAP - Openfire Integration

## LDAP / Openfire Integration for sipXconfig

### Configuring the LDAP Server in sipXconfig

First, navigate to the LDAP / AD screen found under the System tab.

For configuring the LDAP server you have to:

- check 'LDAP configured' option;
- enter the hostname / IP address of your LDAP server;
- enter the port number on which LDAP server is listening (default value is 389 or 636 if you are using TLS/SSL connection);
- enter the user and password.

The screenshot displays the 'LDAP Configuration' screen in sipXconfig. The interface includes a navigation menu at the top with tabs for 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The 'System' tab is active, and the 'LDAP / AD' option is selected in the sub-menu. The main configuration area contains the following fields and options:

- LDAP configured:** A checkbox that is checked.
- Host:** A text input field containing 'ldap.server.com'. Below it, a note states: 'When unconfigured, the LDAP authentication will not be verified. IP address or the name of the host on which LDAP server is running.'
- Use TLS:** A checkbox that is unchecked. Below it, a note states: 'Enable SSL/TLS connections to your LDAP server, default port is 636. 389 or, for a SSL/TLS connection is 636.'
- Port:** A text input field containing '389'. Below it, a note states: 'Port number on which LDAP server is listening for requests. The default port is 389 or, for a SSL/TLS connection is 636.'
- User:** A text input field containing 'cn=Directory Manager'. Below it, a note states: 'Distinguished Name of the user to bind to LDAP directory. Leave empty for anonymous access.'
- Password:** A password input field with masked characters (\*\*\*\*\*).
- Confirm Password:** A password input field with masked characters (\*\*\*\*\*). Below it, a note states: 'Password for simple authentication.'

At the bottom left of the form is a 'Continue' button. On the right side, there is a 'Quick Links' section with a link to 'Certificates'. Below this, there is a note: 'LDAP server needs to be running and be accessible in order to proceed. If LDAP server requires authentication for read-only access, enter User name and Password for basic authentication. **Import Ldap server certificate for enabling SSL/TLS connections**'. Below this note is another section titled 'Active Directory' with the text: 'It is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.'

Next, you have to select the relevant object classes you want to extract from the LDAP database. Select just two classes: "User" and "Person".

If you are using Active Directory you should also select 'securityPrincipal' class.

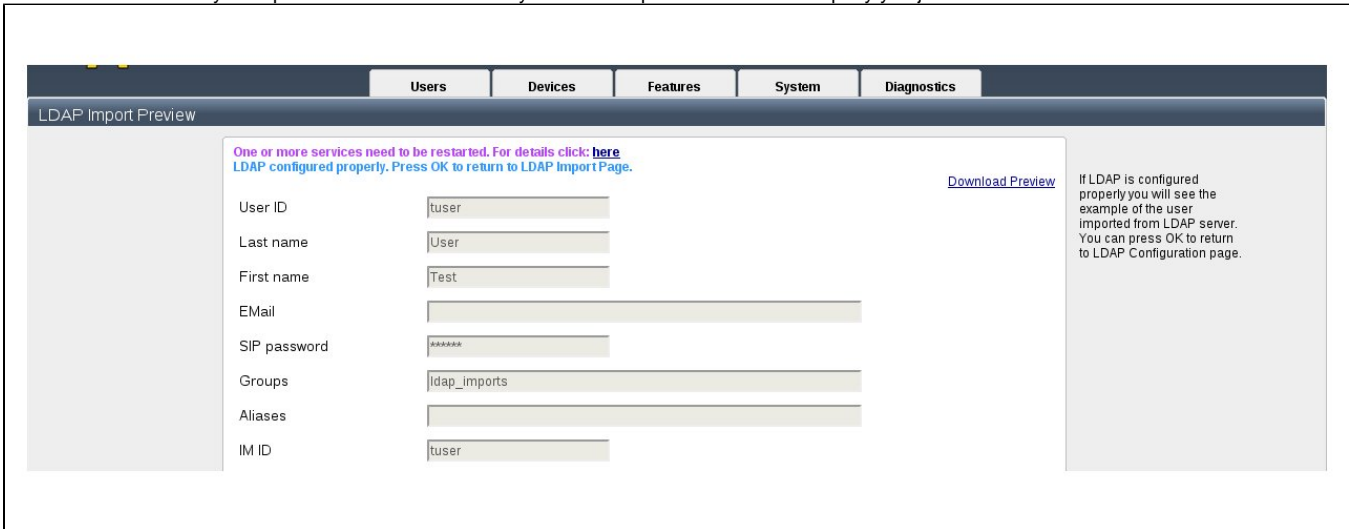
The screenshot shows the 'LDAP Configuration' window with a navigation bar at the top containing 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The 'Users' tab is selected. On the left, there is a sidebar with 'Configuration', 'Import', and 'Settings'. The main area displays a list of object classes, each with a checkbox. A message at the top states: 'One or more services need to be restarted. For details click: [here](#)'. The list includes: aCSPolicy, aCSRResourceLimits, aCSSubnet, account, addressBookContainer, addressTemplate, applicationEntity, applicationProcess, applicationSettings, applicationSiteSettings, applicationVersion, attributeSchema, bootableDevice, builtinDomain, cRLDistributionPoint, categoryRegistration, certificationAuthority, classRegistration, classSchema, classStore, comConnectionPoint, computer, and configuration. On the right, there is a 'Quick Links' section with a link to 'Certificates' and a paragraph explaining that the page displays a list of object classes supported by the configured LDAP server. Below that is an 'Active Directory' section explaining that it is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.

The next screen allows you to map the sipXconfig fields and the LDAP attribute.

'User ID attribute' is the unique user identification. Default value for it is 'ipPhone' but you should use 'uid' for other ldap servers but Active Directory. 'IM ID' is the instant message id. Default value for it is 'sAMAccountName' but you should use 'uid' for other ldap servers but Active Directory.

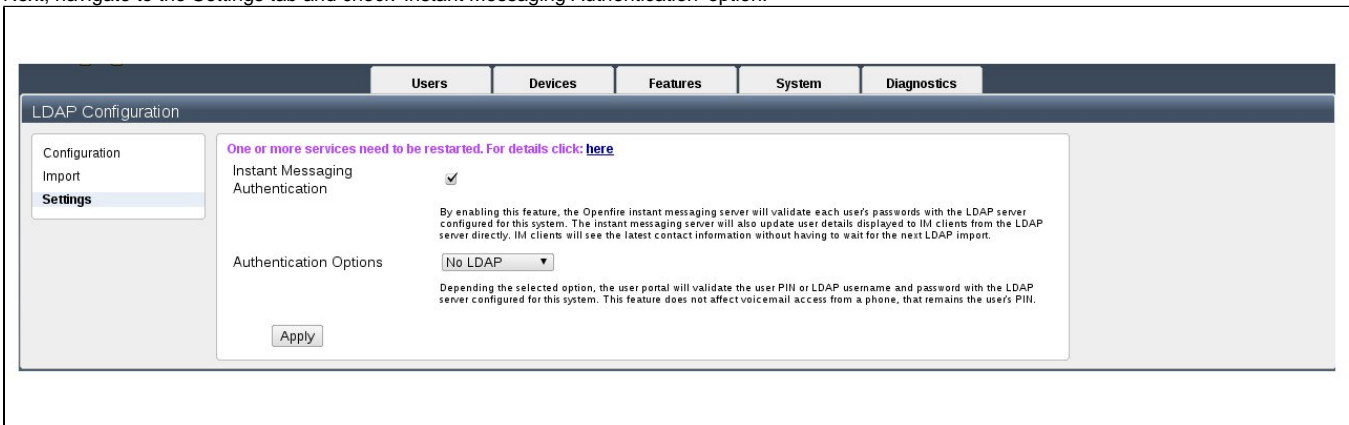
The screenshot shows the 'LDAP Configuration' window with the 'Users' tab selected. The sidebar on the left has 'Configuration', 'Import', and 'Settings'. The main area contains a form for mapping LDAP attributes to user fields. A message at the top states: 'One or more services need to be restarted. For details click: [here](#)'. The form includes: 'Search base' (text input: dc=example,dc=com), 'User object class' (dropdown: person), 'Filter' (text input), 'User ID attribute' (dropdown: sAMAccountName), 'First name attribute' (dropdown: givenName), 'Last name attribute' (dropdown: sn), 'Alias attribute' (dropdown: telephoneNumber), 'EMail attribute' (dropdown), 'User group attribute' (dropdown: ou), 'PIN attribute' (dropdown), 'Default PIN' (text input: \*\*\*\*), 'Confirm Default PIN' (text input: \*\*\*\*), 'SIP password attribute' (dropdown), and 'IM ID' (dropdown: sAMAccountName). Each dropdown is accompanied by explanatory text. On the right, there is a 'Quick Links' section with a link to 'Certificates' and a paragraph explaining that the page allows for associating LDAP attributes with users properties. Below that is an 'Active Directory' section explaining that it is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.

The next screen allows you to preview user records as they would be imported based on the query you just defined.



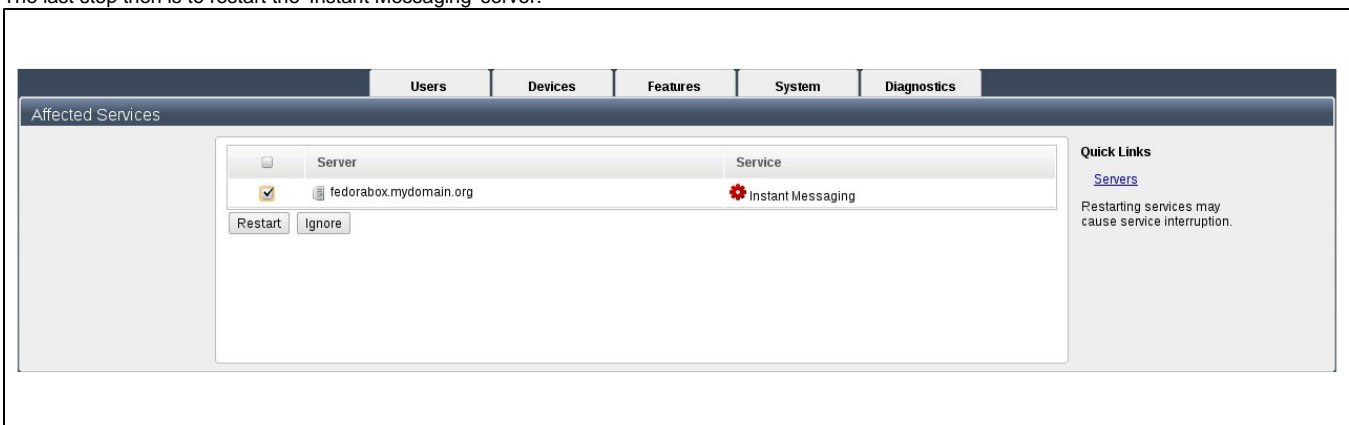
The screenshot shows the 'LDAP Import Preview' interface. At the top, there are navigation tabs: 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. Below the tabs, a message states: 'One or more services need to be restarted. For details click: [here](#) LDAP configured properly. Press OK to return to LDAP Import Page.' A 'Download Preview' link is also present. The main area contains a form with the following fields: 'User ID' (tuser), 'Last name' (User), 'First name' (Test), 'EMail' (empty), 'SIP password' (\*\*\*\*\*), 'Groups' (ldap\_imports), 'Aliases' (empty), and 'IM ID' (tuser). On the right side, a note reads: 'If LDAP is configured properly you will see the example of the user imported from LDAP server. You can press OK to return to LDAP Configuration page.'

Next, navigate to the Settings tab and check 'Instant Messaging Authentication' option.



The screenshot shows the 'LDAP Configuration' interface. At the top, there are navigation tabs: 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. On the left, there is a sidebar with 'Configuration', 'Import', and 'Settings' (selected). The main area contains a message: 'One or more services need to be restarted. For details click: [here](#)'. Below this, the 'Instant Messaging Authentication' option is checked. A note explains: 'By enabling this feature, the Openfire instant messaging server will validate each user's passwords with the LDAP server configured for this system. The instant messaging server will also update user details displayed to IM clients from the LDAP server directly. IM clients will see the latest contact information without having to wait for the next LDAP import.' The 'Authentication Options' dropdown is set to 'No LDAP'. A note below states: 'Depending the selected option, the user portal will validate the user PIN or LDAP username and password with the LDAP server configured for this system. This feature does not affect voicemail access from a phone, that remains the user's PIN.' An 'Apply' button is at the bottom left.

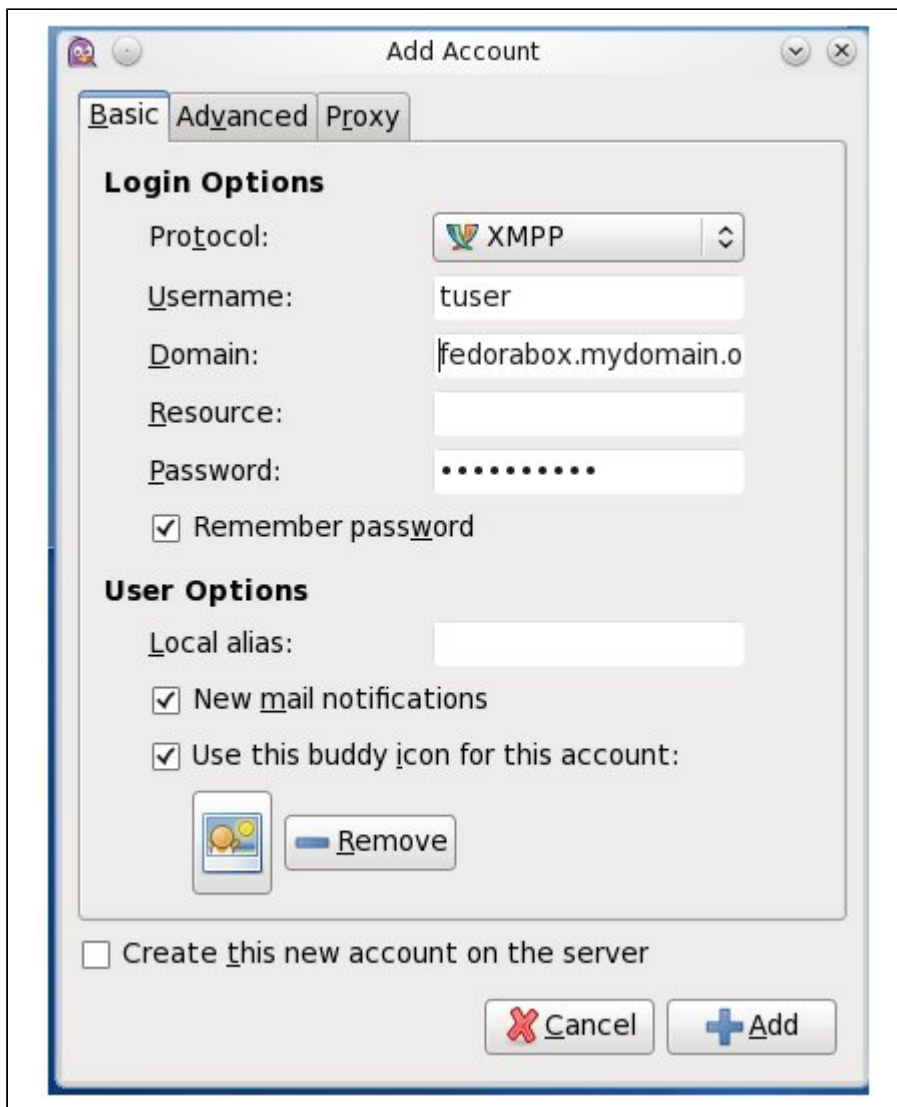
The last step then is to restart the 'Instant Messaging' server.



The screenshot shows the 'Affected Services' interface. At the top, there are navigation tabs: 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The main area displays a table with the following columns: 'Server' and 'Service'. The table contains one row: 'fedorabox.mydomain.org' with 'Instant Messaging' service. Below the table, there are 'Restart' and 'Ignore' buttons. On the right side, there is a 'Quick Links' section with a 'Servers' link and a note: 'Restarting services may cause service interruption.'

You can now register any LDAP user (with User ID configured above and LDAP password) in a IM client (Spark, Pidgin, etc) and start a chat.

For example, in Pidgin you should add the user account (Accounts / Manage accounts / Add)



and accept the the certificate from the sipX server.

