LDAP Authentication How-To

Table of contents

1 Configuring and activating LDAP in Lenya.... 2
2 Allowing LDAP users to work with Lenya....2
3 Going further with LDAP....2
4 Encrypted LDAP....3
5 Notes....3
6 An example publication using LDAP Authentication: the University of Zurich Lenya Publication.... 3

Lenya supports LDAP authentication out-of-the-box, and was tested with OpenLDAP and MS Active Directory servers.

Authentication means that password checking is handled through LDAP, so that the user does not need a Lenya-specific password. Note that only the authentication is done through LDAP; the Lenya administrator still has to tell Lenya which LDAP users to allow and to assign Lenya roles to these users. LDAP setup is handled in Lenya configuration files; adding users and assigning them roles is handled within the Lenya Admin GUI.

1 Configuring and activating LDAP in Lenya

1. Go to the directory *lenya/pubs/<your-publication-name>/config/ac*
2. Edit the file *ac.xconf* and uncomment the line regarding "LDAP support"
3. Go to the subdirectory *passwd* and copy the file *lenya/pubs/<your-publication-name>/config/ac/passwd/ldap.properties.sample* to the file *ldap.properties* in this directory.
4. Edit the file *ldap.properties* with your settings (the sample file contains explanations for the entries)
5. Restart your servlet container, so that the changes take effect
6. Login as administrator. In the user's section, you can now add LDAP users: enter the LDAP id, and provide a Lenya id (which may be the same as the LDAP id). Now add group memberships for this id.
7. You should now be able to login with this LDAP user and password.

2 Allowing LDAP users to work with Lenya

Once you have everything configured OK, you can tell Lenya to allow certain LDAP users. It is important to understand that, just because a user exists in LDAP, does not mean she has access to Lenya. The user needs to be explicitly added in Lenya, along with the group memberships. However, the authentication itself (password handling) is then completely handled through LDAP.

1. In the administration GUI, add the "LDAP user" in order to make this user known to Lenya. You can use the same id for Lenya as the existing LDAP id.
2. Click on the user and add group settings - if user belongs to no groups at all, she will not be able to login
3. Logout and login with the newly created id.

3 Going further with LDAP

The LDAP implementation in Lenya is based on the premise that you have an existing LDAP directory containing users and passwords, but you do not want to (or are not allowed to) add anything particular to Lenya within this LDAP directory, such as Lenya roles.

As a consequence, the Lenya specific user information is *not* stored in LDAP, but instead with the same mechanism as non-LDAP users. What Lenya does do for you is delegate authorization (the checking of the user's password in LDAP), meaning that the user does not require an additional "Lenya password".

This implementation of LDAP authentication in Lenya works can be replaced by a tighter integration of LDAP, which would possibly provide these advantages:

- Maintenance of roles, groups in LDAP as well.
- Remove the need to separately enable each LDAP user in Lenya.

There is a patch (nb 34737) (http://issues.apache.org/bugzilla/show_bug.cgi?id=34737) which replaces Lenya's default LDAP handling and fully integrates Lenya with an LDAP where users are stored according to the Posix scheme.

4 Encrypted LDAP

- in the file *ldap.properties*, set *security-protocol* to the value *ssl* and set *key-store* to the name of your keystore file
- add the LDAP server certificate file to the local keystore using this command:

```
keytool -import -keystore .keystore -file <ca_cert_file> -alias <yourdomain.com>
```

5 Notes

- If you modify *ldap.properties*, it may be necessary to restart your servlet container or at least to reload your webapp in order for the changes to take effect.

6 An example publication using LDAP Authentication: the University of Zurich Lenya Publication

The "University of Zurich Publication" is an example of a publication which uses LDAP authentication. You may wish to install and configure it to authenticate against your LDAP server: this way, you can check whether LDAP authentication is working, before proceeding to activate it in another application.

Note: this HOW-TO was tested using the "University of Zurich Publication" state on May 26th, 2004. If another version is incompatible with your Lenya installation, don't despair, you will still be able to use the LDAP relevant stuff.

1. Retrieve the University of Zurich Lenya publications (unitemplate, unizh) described on http://wyona.org/
2. Go to the *unitemplate/config/ac/passwd* directory and edit *ldap.properties* as described above
3. if secure LDAP is required, add the server certificate to the keystore as described above
4. Deploy the publications (see ? (../../../docs/1_2_x/how-to/deploy_publication.html) Deploy Publication How-To)
5. In your browser, refresh your Lenya start page. You should now see, on the left hand side, a link to the "Unitemplate" publication. Login as lenya / levi user and go the Admin area to add a user.
6. Click on "Add University User" (this means LDAP user). In the field "UniAccessID", use the LDAP userid. In the field "CMS User", use the id with which you want to user to log in to Lenya. This may be the same id as for LDAP.
7. Add the desired groups for this user and log out of Lenya.
8. You should now be able to login to Lenya using this new user and his/her LDAP password.