

LDAP / SSO Authentication

Extension Key: ig_ldap_sso_auth

Language: en

Keywords: Idap, sso, authentication

Copyright 2000-2010, Michael Miousse, <mmiousse@infoglobe.ca>

This document is published under the Open Content License available from http://www.opencontent.org/opl.shtml

The content of this document is related to TYPO3

- a GNU/GPL CMS/Framework available from www.typo3.org



Table of Contents

1	LDAP / SSO Authentication
3	Introduction
3	What does it do?

Screenshots3
Users manual7
Administration8

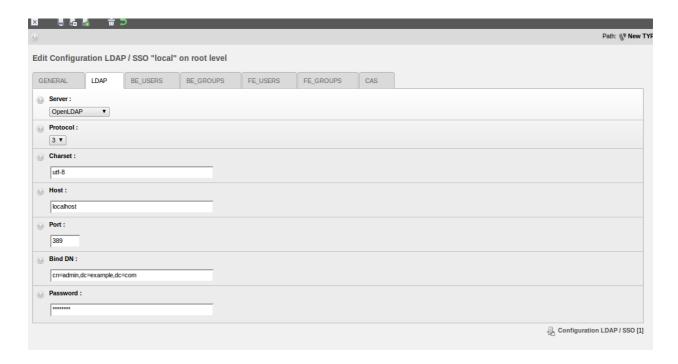


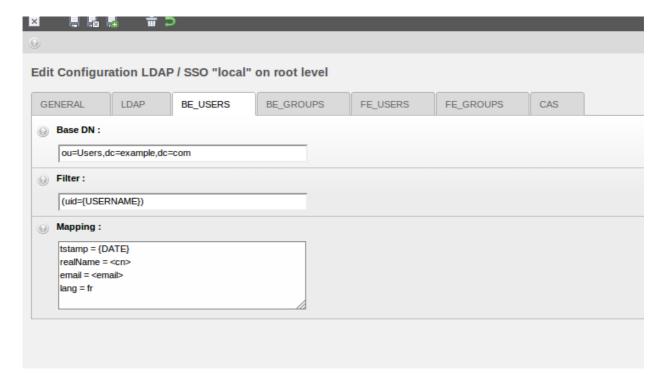
Introduction

What does it do?

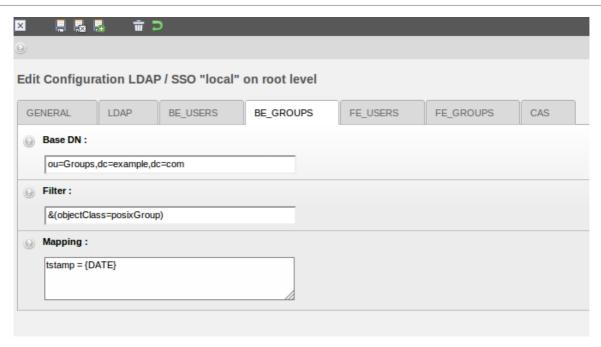
 This extension enables import/update/deletion of users and groups(frontend, backend or both) from a LDAP-directory. In this way, TYPO3 can be used as an intranet CMS. Multiple Idap sever configuration are allowed. Works with openIdap, edirectory and Active directory. You can also use a CAS server to implement SSO.

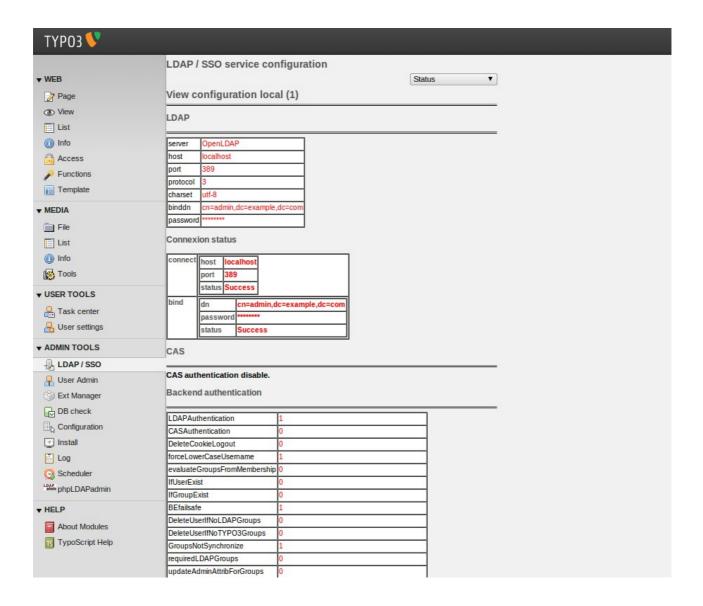
Screenshots



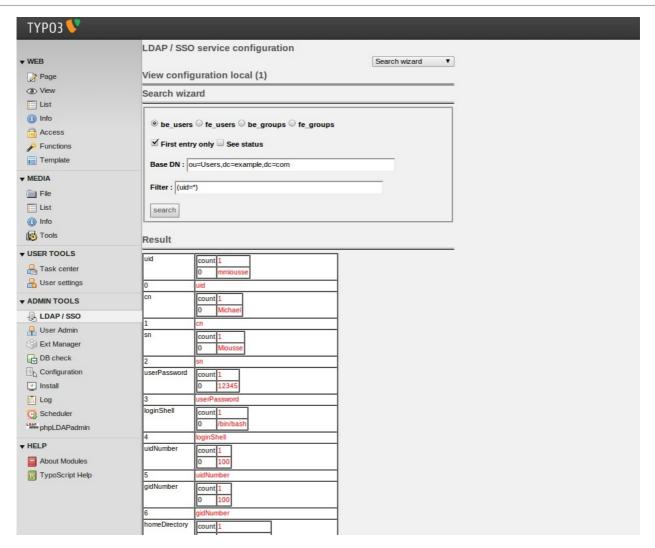




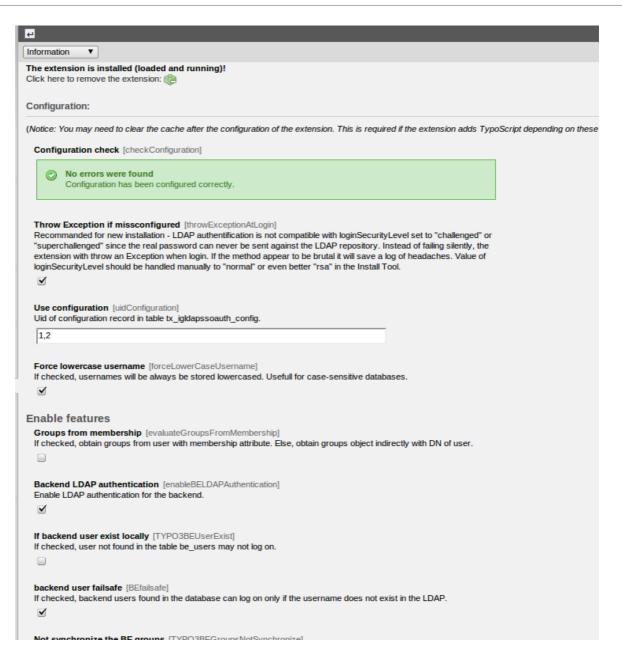












TYP03 🐓 6



Users manual

When a user tries to log on the extension passes the credentials to the LDAP server(s) and verifies them. When a LDAP server can authenticate the user he is logged on. New users (in the directory but not in the TYPO3 database) are imported after authentication. Records of existing users are updated.

For new users imported from the directory random passwords will be inserted!



Administration

-First step for configuring your LDAP authentication is to create one or more server configurations.

All server configurations have to be stored on the root level of your TYPO3 website. Create a Configuration LDAP / SSO records. These records have 7 tabs for specific configurations types.

- 1. The first tab is General.
 - The only thing you have to fill is the configuration name. This is only to name the records you have just created.
- 2. The second tab is the Global configurations about a single LDAP (not that you can create multiple configuration records with the same LDAP)
 - Server: Choose your LDAP type (openIdap or edirectory).

Note that if you are using Active directory, your LDAP type is edirectory

- Protocol: Choose the LDAP protocol version (2 or 3). Recent LDAP use version 3
- Charset: is Charset of your LDAP. Usually utf-8
- Host: is the host of your LDAP
- Port: is the port your LDAP use. Default LDAP port is 389
- Bind DN: is the full DN of the LDAP user you will use to connect to the LDAP

note that your LDAP user need access to the directory where users and groups are stored and full read access to users and groups.

Example: cn=admin,dc=example,dc=com

- Password: Password of the user used to connect to the LDAP
- 3. The third tab and the fifth tabs can be fill exactly the same way. The only difference between them is that BE_USERS store the configurations for the backend LDAP user authentication and FE_USERS store the configurations for the frontend LDAP user authenticate. You will only fill the section you need, BE_USERS if you need backend authentication and FE_USERS if you need frontend authentication.
 - **Base DN:** is the full DN path of the directory containing all the users that you want to use with you TYPO3 authentification.

Example: ou=Users,dc=example,dc=com

• Filter: is used to precise which LDAP attribute contain the username of your users.

Example: (uid={USERNAME})

uid is the most common attribute used to keep the username in LDAPs but if you are in an Active directory, the field where the username is stored is usually the sAMAccountName.

Note that the string "{USERNAME}" will be substituted by the username entered in the login form

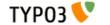
You will also be able to add restrictions that allow you to exclude user from specific properties. The syntax used in this field is the LDAP search syntax.

Example: (&(uid={USERNAME})(objectClass=user)

- **Mapping:** is used to fetch other attributes form the LDAP that we would like users to have. It is quite simple, each line is a new command. Each command have 2 parts separated by a =. the first part is the field form the TYPO3 user that we want to fill and the second part is the value we that the field will have. There is 3 possible value type you could use:
 - a string: this will assign the value directly to the field
 - a LDAP attribute value: LDAP attributes will be recognized by the specific caracters <>.

Example: email = <email> this will set the field email of the TYPO3 user to the value of the attributes email of the user fetch from the LDAP

- a custom marker: custom markers are markers create by the extension to assgin specific type of values. There are only 4 markers available for the moment:
 - {DATE}: the current timestamp





- {RAND}: a random number
- {USERNAME}: the username from the login form (the username will automatically fill the needed field. This markers is only used if you want to put the username in an other field than the one by default)
- {hookparametes}: will only be usefull if an extension il hooked on ig_ldap_sso_auth

```
Example: tstamp = {DATE}
realName = <cn>
email = <email>
lang = fr
```

- 4. The fourth and sixth tabs can be fill exactly the same way. The only difference between them is that BE_GROUPS store the configurations for the backend LDAP usergroup association and FE_GROUPS store the configurations for the frontend LDAP usergroup association. You will only fill the sections you need, BE_ GROUPS if you need backend authentication and FE_GROUPS if you need frontend authentication. You can skip this entire section if you just want to validate the authentication and do not want to use groups from LDAP.
 - **Base DN:** is the full DN path of the directory containing all the groups that are related to your LDAP users and you want to use in your TYPO3.

Example: ou=Groups,dc=example,dc=com

• **Filter:** You will only by used to add restrictions that allow you to exclude obects from specific properties. The syntax used in this field is the LDAP search syntax.

Example: &(objectClass=posixGroup)

- **Mapping:** is used to fetch other attributes form the LDAP that we would like groups to have. It is quite simple, each line is a new command. Each command have 2 parts separated by a =. the first part is the field form the TYPO3 group that we want to fill and the second part is the value we that the field will have. There is 3 possible value type you could use:
 - a string: this will assign the value directly to the field
 - a LDAP attribute value: LDAP attributes will be recognized by the specific caracters <>.
 Example: email = <email> this will set the field email of the TYPO3 group to the value of the type of the value of the type of type of type of the type of type of the type of type
 - Example: email = <email> this will set the field email of the TYPO3 group to the value of the attributes email of the user fetch from the LDAP
 - a custom marker: custom markers are markers create by the extension to assgin specific type of values. There are only 4 markers available for the moment:
 - {DATE}: the current timestamp
 - {RAND}: a random number
 - {USERNAME}: the username from the login form (the username will automatically fill the needed field. This markers is only used if you want to put the username in an other field than the one by default)
 - {hookparametes} : will only be usefull if an extension il hooked on ig_ldap_sso_auth

Example: $tstamp = \{DATE\}$

- 5. The last tab is for CAS configurations. You only have to fill it if you want to use a CAS server to implement some single sing on (SSO)
 - Host: is the host of your CAS server
 - **URI:** path to postpend to the host used if the CAS sever is not at the root of your host Example: /userSSo/cas in the string localhost/userSSo/cas
 - Service URL: this is a specific url for your CAS
 - Port: port on which you CAS is configure
 - Back URL: Url to return to in case of a CAS login