Service d'authentification LDAP et SSO avec CAS

Clé de l'extension : **ig_ldap_sso_auth**

Le contenu de ce document se réfère à TYPO3

- un GNU/GPL CMS/Framework qui est disponible au www.typo3.com.

Table of Contents

Que fait cette extension ?

L'extension ig_ldap_sso_auth est un service d'authentification TYPO3. Elle permet l'authentification des usagers backend (BE) et/ou frontend (FE) par un serveur LDAP (Lightweight Directory Access Protocol). De plus, en FE, il est possible d'utiliser un service SSO (Single Sign-On) implémenté par un serveur CAS (Central Authentication Service).

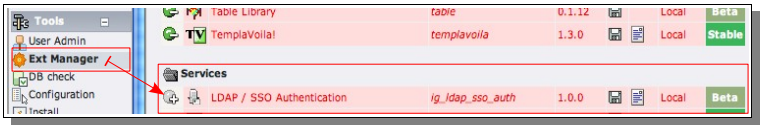
À ce jour elle, permet de :

- Configurer la connexion aux serveurs et la synchronisation des données en BE par un administrateur;
- Authentifier un usager BE et/ou FE par un serveur LDAP;
- Authentifier un usager FE par un serveur CAS;
- Synchroniser les données utilisateurs à partir d'un serveur LDAP;

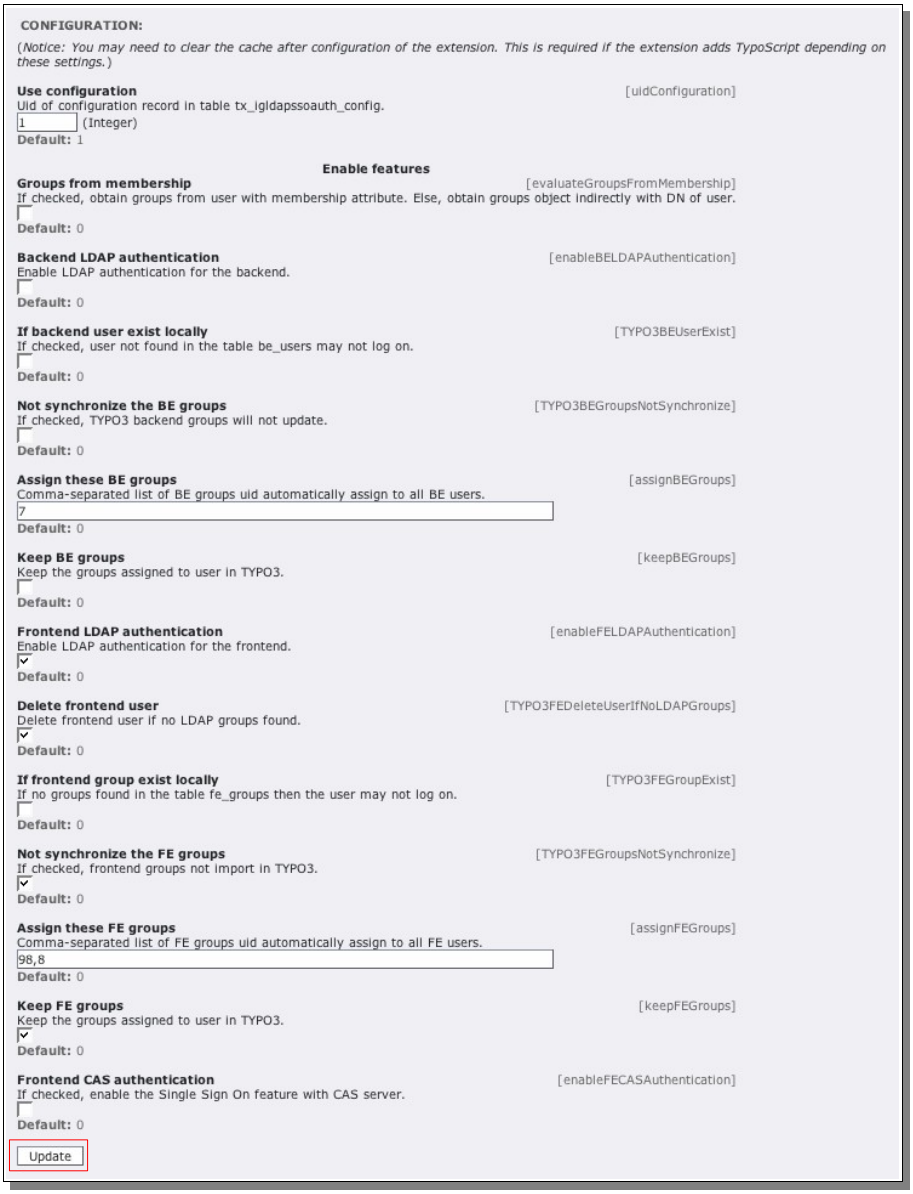
L'extension a été testé, pour le moment, avec les serveurs LDAP openLDAP et eDirectory seulement.

Installation

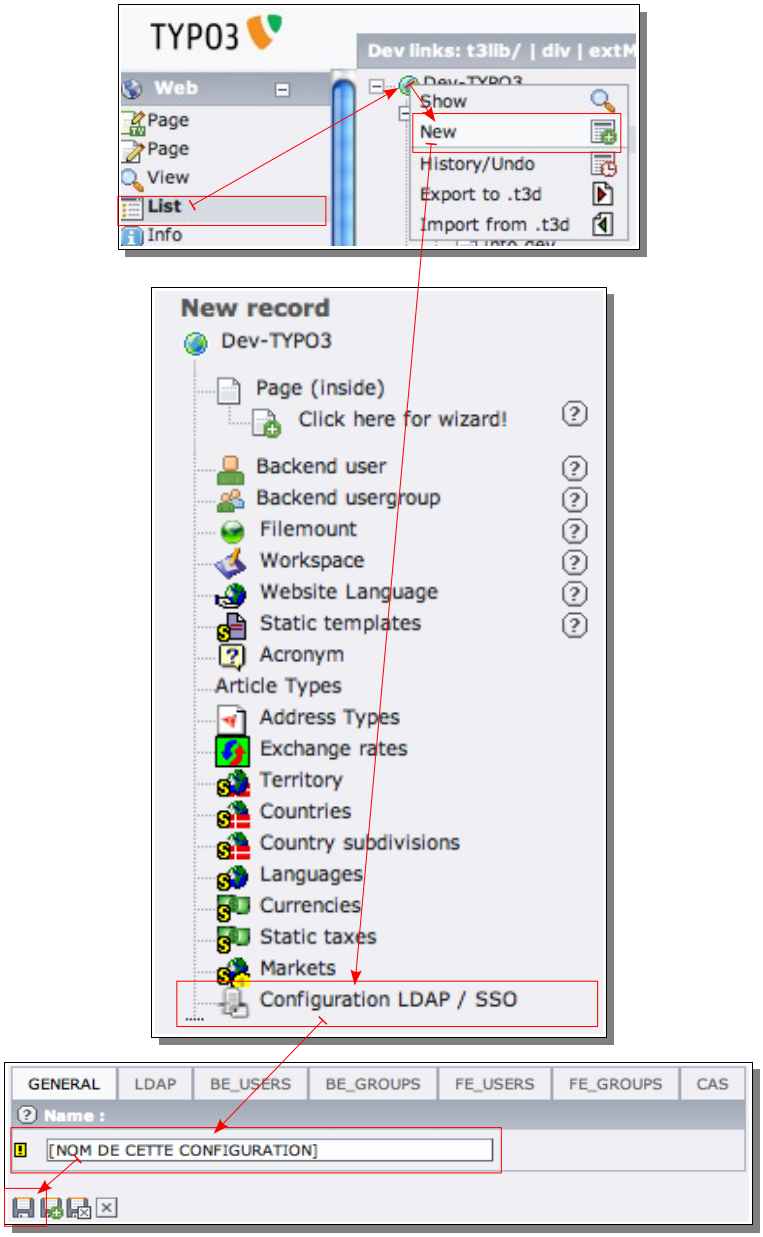
1. Au préalable, installer ou mettre à jour avec la dernière version, l'extension iglib;
2. Installer ig_ldap_sso_auth via le module EM.



3. Lorsque la page de configuration apparaît, cliquer simplement sur « Update »;



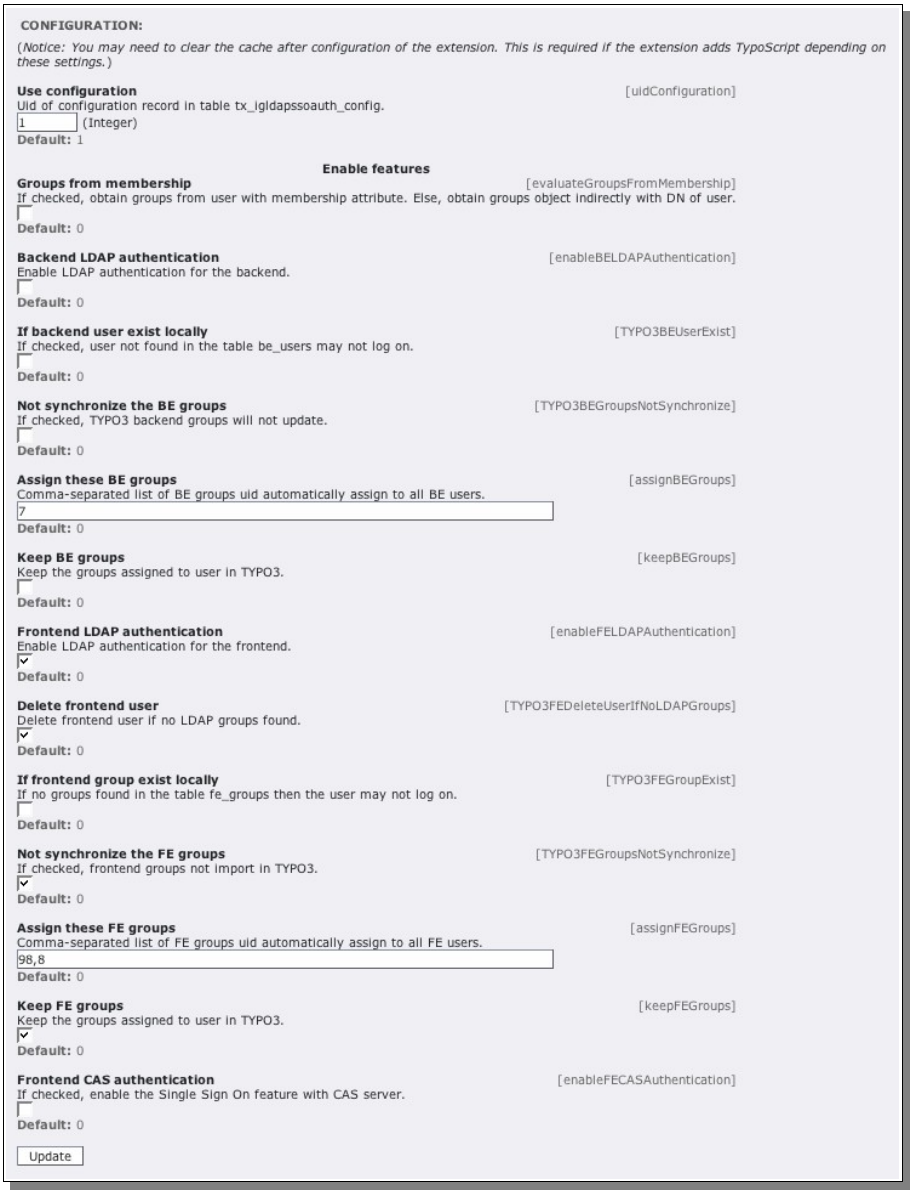
4. En mode « List », créer un formulaire de configuration « Configuration LDAP / SSO » en cliquant sur l'icon de la planète tout en haut de l'arborescence du site Internet. Nommez celui-ci et enregistrer.



5. Vider toutes les caches et actualiser la page afin de mettre à jour le backend. L'extension est maintenant installée mais non fonctionnelle.

Options de configuration

Dans l'« Extension Manager », cliquez sur le service « LDAP / SSO authentication »



CONFIGURATION:

(Notice: You may need to clear the cache after configuration of the extension. This is required if the extension adds TypoScript depending on these settings.)

Use configuration [uidConfiguration]
Uid of configuration record in table tx_igldapssoauth_config.
1 (Integer)
Default: 1

Enable features

Groups from membership [evaluateGroupsFromMembership]
If checked, obtain groups from user with membership attribute. Else, obtain groups object indirectly with DN of user.
Default: 0

Backend LDAP authentication [enableBELDAPAuthentication]
Enable LDAP authentication for the backend.
Default: 0

If backend user exist locally [TYPO3BEUserExist]
If checked, user not found in the table be_users may not log on.
Default: 0

Not synchronize the BE groups [TYPO3BEGroupsNotSynchronize]
If checked, TYPO3 backend groups will not update.
Default: 0

Assign these BE groups [assignBEGroups]
Comma-separated list of BE groups uid automatically assign to all BE users.
7
Default: 0

Keep BE groups [keepBEGroups]
Keep the groups assigned to user in TYPO3.
Default: 0

Frontend LDAP authentication [enableFELDAPAuthentication]
Enable LDAP authentication for the frontend.
Default: 0

Delete frontend user [TYPO3FEDeleteUserIfNoLDAPGroups]
Delete frontend user if no LDAP groups found.
Default: 0

If frontend group exist locally [TYPO3FEGroupExist]
If no groups found in the table fe_groups then the user may not log on.
Default: 0

Not synchronize the FE groups [TYPO3FEGroupsNotSynchronize]
If checked, frontend groups not import in TYPO3.
Default: 0

Assign these FE groups [assignFEGroups]
Comma-separated list of FE groups uid automatically assign to all FE users.
98,8
Default: 0

Keep FE groups [keepFEGroups]
Keep the groups assigned to user in TYPO3.
Default: 0

Frontend CAS authentication [enableFECASAuthentication]
If checked, enable the Single Sign On feature with CAS server.
Default: 0

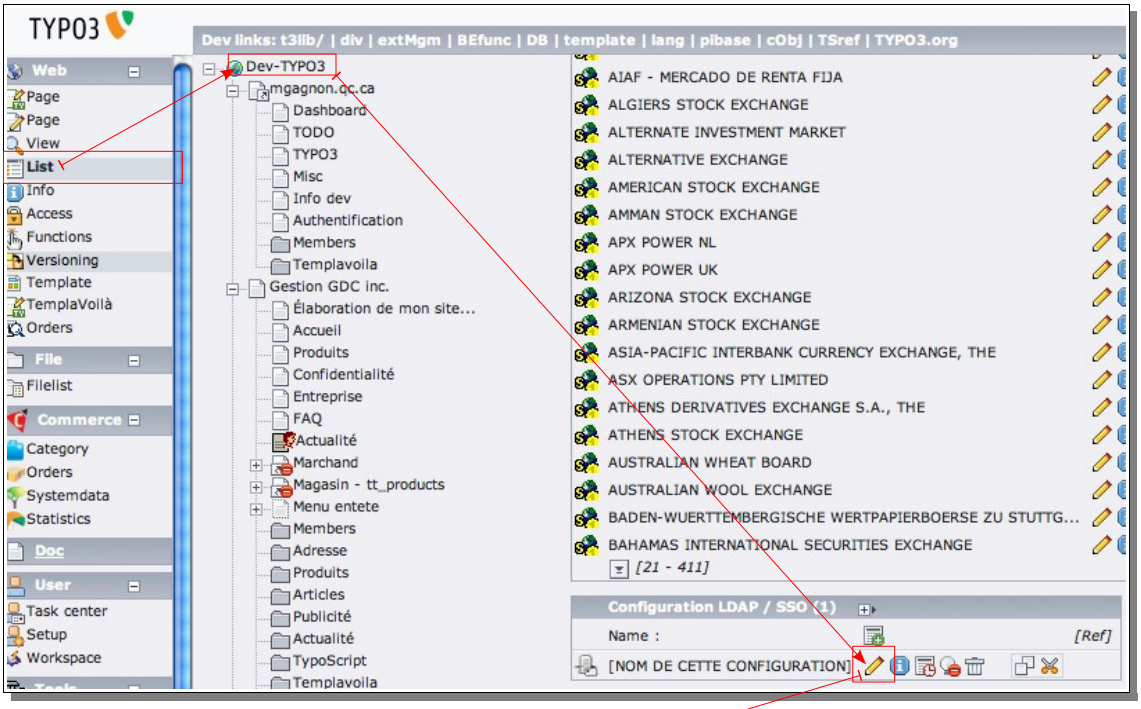
Update

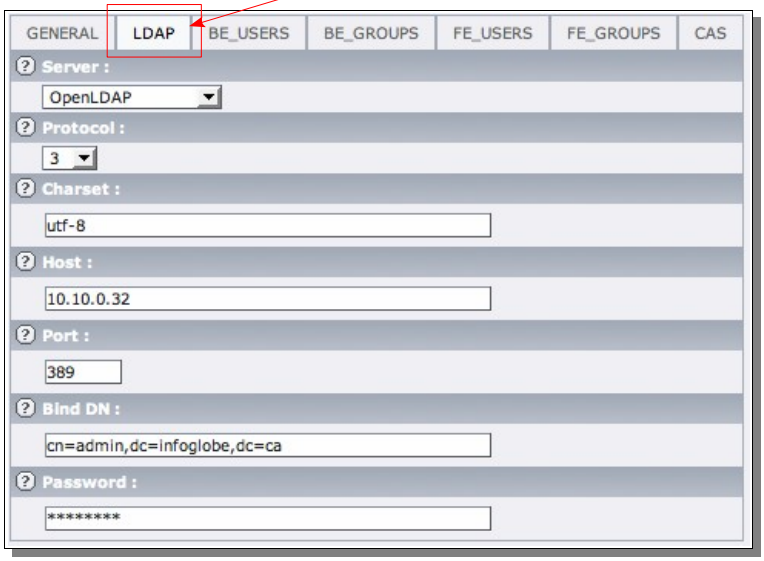
Variables	Type	Description	Defaut
Configuration générale			
uidConfiguration	integer	Identifiant unique (uid) de l'enregistrement de la table MySQL (tx_igldapssoauth_config) de la configuration à utiliser.	1
evaluateGroupsFromMembership	boolean	Recherche des groupes à partir de l'attribut « membership ».	0
Authentification backend			
enableBELDAPAuthentication	boolean	Activer l'authentification LDAP en backend.	0
TYPO3BEUserExist	boolean	Lors de l'authentification LDAP BE, l'usager est valide seulement s'il existe dans TYPO3. Il faut donc le céé pour qu'il puisse s'authentifier.	0
TYPO3BEGroupsNotSynchronize	boolean	Ne pas synchroniser les groupes BE lors de l'authentification.	0
assignBEGroups	string	Liste des uid de groupes BE, séparée par des virgules, à assigner automatiquement lors de l'authentification.	0
keepBEGroups	boolean	Ne pas remplacer les groupes TYPO3 assignés à l'usager lors de l'authentification BE.	0
updateAdminAttribForGroups	string	Tous les utilisateurs BE ayant un des groupes mentionnés par ce champs seront automatiquement promut administrateur.	0
requiredLDAPBEGroups	string	Seul les utilisateurs BE appartenant à un des groupe mentionnés par ce champs seront autorisés à se connecter.	0
Authentification frontend			
enableFELDAPAuthentication	boolean	Activer l'authentification LDAP en frontend.	0
TYPO3FEDeleteUserIfNoLDAPGroups	boolean	Si l'usager n'appartient à aucun groupe sur le serveur LDAP celui-ci sera supprimer.	0
TYPO3FEDeleteUserIfNoTYPO3Groups	boolean	Lors de l'authentification LDAP FE, l'usager est valide seulement s'il appartient à un groupe existant dans TYPO3. Si l'usager n'appartient à aucun groupe TYPO3, il n'est jamais importer.	0
TYPO3FEGroupsNotSynchronize	boolean	Ne pas synchroniser les groupes FE lors de l'authentification.	0
TYPO3FEGroupExist	boolean	Lors de l'authentification LDAP FE, l'usager est valide seulement s'il appartient à un groupe existant dans TYPO3. Il faut donc créer les groupes localement, en affectant au champ « DN » la valeur de l'attribut DN de l'entré d'un groupe LDAP dans le formulaire de gestion des groupes TYPO3 afin que l'usager puisse s'authentifier. Il est également possible d'importer des groupes LDAP via le module « LDAP / SSO => Import LDAP groups » .	0
requiredLDAPBEGroups	string	Seul les utilisateurs FE appartenant à un des groupe mentionnés par ce champs seront autorisés à se connecter.	0
assignFEGroups	string	Liste des uid de groupes TYPO3 FE, séparée par des virgules, à assigner automatiquement lors de l'authentification.	0
enableFECASAuthentication	boolean	Activer l'authentification CAS en frontend. Pour que l'authentification CAS fonctionne, il faut activer « enableFELDAPAuthentication » également.	0
keepFEGroups	boolean	Ne pas remplacer les groupes TYPO3 assignés à l'usager lors de l'authentification FE.	

Authentification LDAP

Connexion au serveur

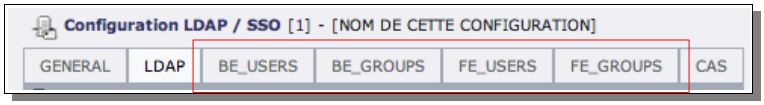
Ouvrez le formulaire de configuration créé à l'étape de l'installation et selectionnez l'onglet « LDAP ».

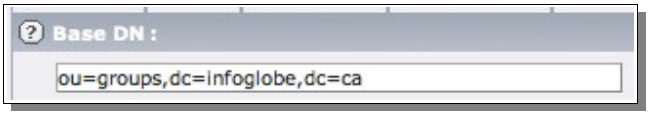




Champ	Description	Défaut
Server	Type du serveur LDAP utilisé pour l'authentification.	OpenLDAP
Protocol	Version du protocole utilisé pour la communication avec le serveur LDAP.	3
Charset	Jeux de caractères du serveur LDAP.	utf-8
Host	Adresse du serveur LDAP.	
Port	Port utilisé.	389
Bind DN	Nom d'usager à utiliser pour la connexion. Une connexion anonyme est possible si ce champ et celui du « Password » est vide.	
Password	Mot de passe utilisé pour la connexion. Une connexion anonyme est possible si ce champ et celui du « Bind DN » est vide.	

Synchronisation des données utilisateur



Champ	Description
Base DN	Utilisé lors de la recherche sur le serveur LDAP afin de contenir celle-ci dans une portion de l'arborecense du serveur. Exemple : 
Filter	Filtre utilisé lors de la recherche sur le serveur LDAP afin d'éliminer les entrées non désirées et identifier les attributs à comparer avec le nom d'usager du formulaire d'authentification et le DN de l'utilisateur pour la recherche de ses groupes. Filtre simple pour l'authentification d'un usager :  Filtre de groupe si l'option « evaluateGroupsFromMembership » n'est pas activé : 

Mapping

Association des champs TYPO3 avec leurs valeurs lors la synchronisation des données.

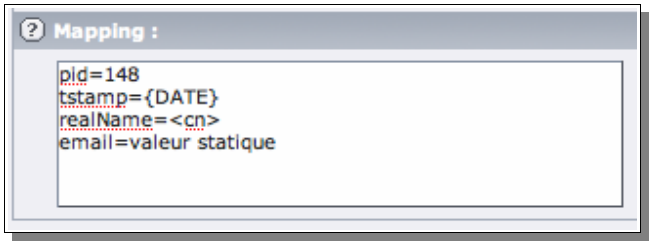
Syntaxe : « **Champ_TYPO3=Valeur** »

Valeur	Type	Description
{DATE}	Constante	Date et l'heure lors de la synchronisation.
{RAND}	Constante	Valeur numérique au hazard.
<« Attribut LDAP »>	Attribut LDAP	Sera remplacé par la valeur de cette attribut lors de la synchronisation des données.
Valeur statique	Statique	Le champ TYPO3 prendra simplement la valeur indiquée.

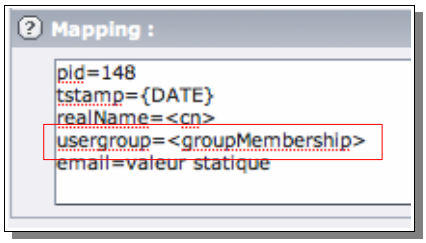
Le champ « pid » doit être spécifié afin de synchroniser le données du bon dossier système. S'il ne l'est pas, 0 sera la valeur par defaut.

Pour les groupes, si le champ « title » n'est pas spécifié, le DN de celui-ci sera utilisé par défaut.

Exemple :

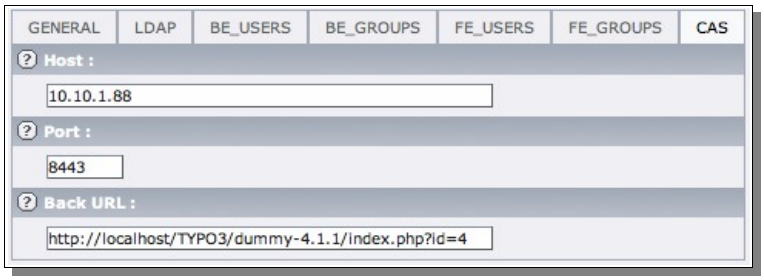


Si l'option « evaluateGroupsFromMembership » est activé, vous devez affecter l'attribut LDAP au champ « usergroup » d'un usager :



Authentification FE avec CAS

Connexion au serveur

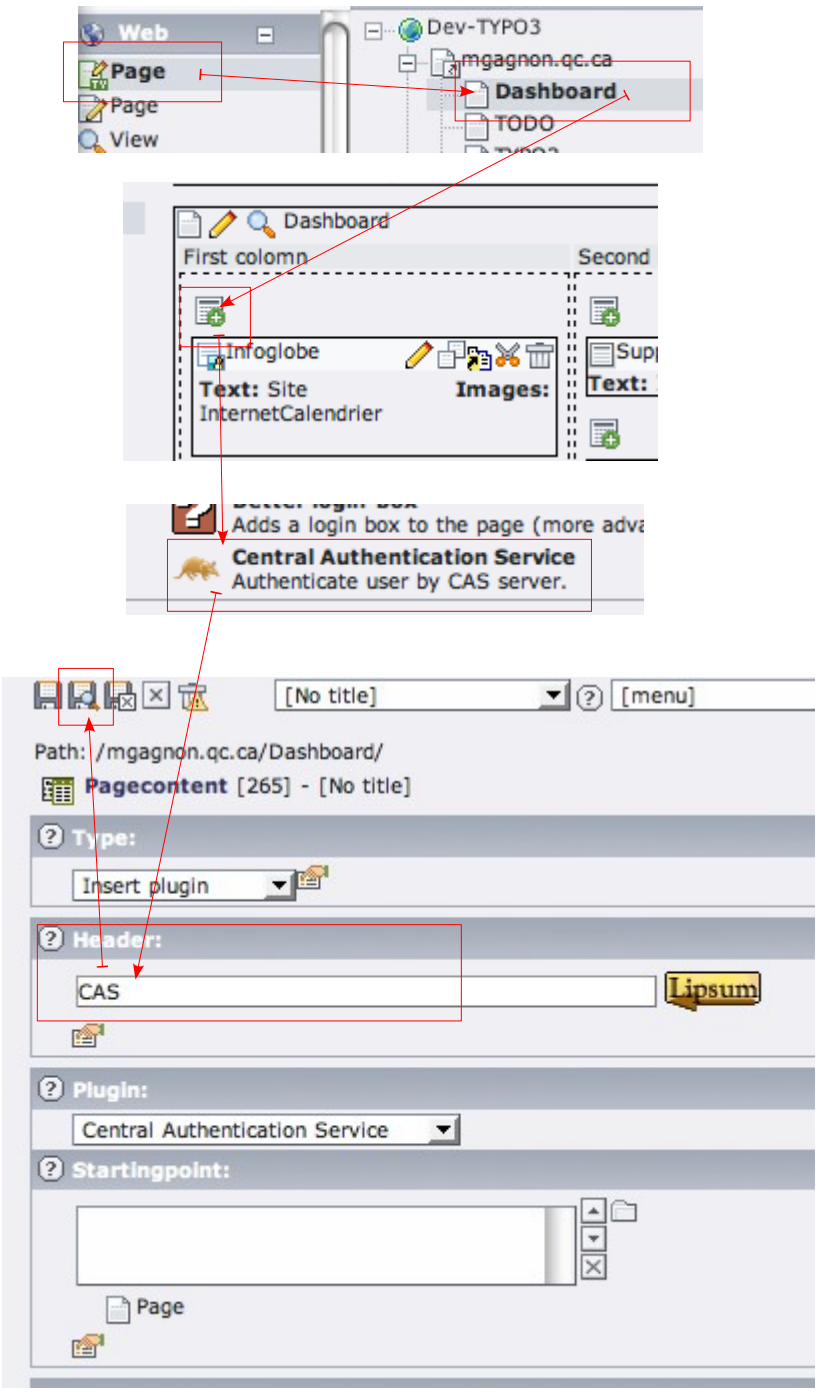


Champ	Description
Host	URL du serveur CAS.
Port	Port utilisé par le serveur.
URI	URI du serveur CAS
Service URL	URL de retour lors de la connexion d'un usager
Back URL	URL de retour lors de la déconnexion de l'usager.

Activation du service

1. Activer les options de configuration « enableFELDAPAuthentication » et « enableFECASAuthentication »;

2. Ajouter le plugin « Central Authentication Service » sur une page de votre site.



3. Un bouton vous permet maintenant d'authentifier les usagers par le serveur CAS. Si l'usager est valide lors de l'authentification, la synchronisation de ses données est faite avec le serveur LDAP basé sur l'identifiant retourné par CAS.

ConfigurationTypoScript

```
plugin.tx_igldapssoauth_pi1 {
        userFunc = tx_igldapssoauth_pi1->main
        #templateFile = fileadmin/...
        _CSS_DEFAULT_STYLE (
            .login {
            border:0px solid #000000;
            }
            .logout {
             border:0px solid #000000;
            }
            .disable {
            border:0px solid #000000;
            }
        )
        _LOCAL_LANG.default {
            login = Connexion
            logout = Déconnexion
            disable = Plugin non activé.
        }
}
```

Le module LDAP / SSO

En backend, dans la section « Tools », sélectionnez « LDAP / SSO ». Dans ce module, à l'aide du menu déroulant en haut à droite, vous avez trois options :

Choix du menu	Description
Status	Statut de votre configuration et visionnement des valeurs de configuration de l'extension.
Search wizard	Tester la configuration de synchronisation des données utilisateur.
Import LDAP groupes	Importer les groupes LDAP selon la configuration afin d'en faire la gestion dans TYPO3.

Utilisation de l'extension phpLDAPAdmin

Cette extension aide à configurer ig_ldap_sso_auth car il permet de visualiser les entrées du serveur LDAP.