SSO standard

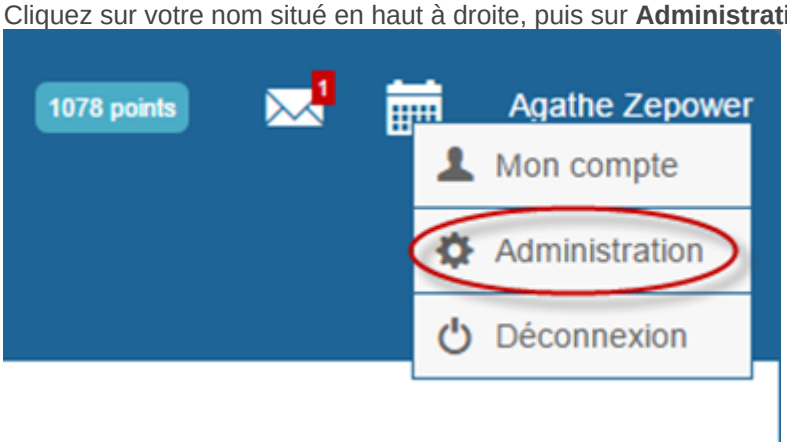
Procédure d'identification par SSO (Single Sign-On)

L'**authentification unique** (ou identification unique ; en anglais *Single Sign-On* : **SSO**) est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.

En étant sur une plateforme externe au **xLMS**, un utilisateur pourra ainsi accéder au **xLMS** sans devoir se réauthentifier (à condition qu'il soit déjà authentifié sur l'autre plateforme et que l'application externe lui fournisse les éléments nécessaires lui permettant de lancer le **xLMS**).

La connexion SSO standard permettra au **xLMS** de récupérer les informations de l'utilisateur qui veut se connecter sous forme d'une donnée cryptée,

Cliquez sur votre nom situé en haut à droite, puis sur **Administration**.



- Sélectionnez l'onglet **Outils**.
- Depuis le menu arborescent, sélectionnez **Réglages du domaine**, puis **Réglage de la connexion** .

  Si vous choisissez l'option :
  - **Connexion SSO standard** :

    - Cochez la case **SSO activé** afin d'activer la connexion SSO standard et de permettre la prise en compte de la clé privée SSO.
    - Saisissez une valeur dans le champ **Clé privée SSO** permettant au **xLMS** de décrypter et lire les données.

    Une image contenant texte, capture d’écran, Police, ligneLe contenu généré par l’IA peut être

- Pour valider votre saisie, cliquez sur **Mettre à jour** en bas de page.

L'application externe peut passer indifféremment les paramètres avec la méthode Post ou la méthode Get en utilisant l'identifiant xLMS (Login) ou l'identifiant externe (extid).

- Avec le login : https://url.net/default.aspx?login=agzep&tstamp=123456&signature=xxxx
- Avec l'identifiant externe : https://url.net/default.aspx?extid=agzep&tstamp=123456&signature=xxxx

Trois paramètres sont attendus par la page d'identification :

1. Le critère d'identification de l'utilisateur (le login ou l'identifiant externe).
2. La valeur timestamp UTC correspondant au temps UNIX. Il s'agit du nombre de secondes écoulées depuis le 1er janvier 1970 00:00:00 UTC jusqu'à l'événement à dater.
3. La signature xxxx est le résultat du cryptage au format MD5 de la formule suivante : md5(login_value + domain_private_key + timestamp UTC)

	*Le hash MD5 doit :* *- Prendre en entrée une chaîne encodée en UTF16.* *- Etre en majuscule.*

La signature est valable 20 minutes.

Techniquement, Cela se résumé en trois étapes principales:

1- Récupérer le **login de l'utilisateur** souhaitant se connecter, la **date et heure actuelle** et **la clé** (une chaine de caractères, connue par les deux parties)

2- Calculer la signature selon l'algorithme **MD5**

3-Envoyer la requête vers WBT avec les trois paramètres:

-**Login, Date & heure et la signature**

4- Utilisateur Authentifié

Exemple d'un client SSO en JAVA:

Etape 1

```
String login = user.getLogin().toString();
String timestamp = "" + (new Date()).getTime() / 1000;
String wbtSiteKey = "SSOWBT3.4"; /* replace this empty value by the secret key */
```

Etape 2

```
String signature = null;
try {
    signature = DigestUtils.md5Hex((extid + wbtSiteKey + timestamp).getBytes("UTF-16LE")).toUpperCase();
} catch (UnsupportedEncodingException e) {
    throw new myException(null, e.getMessage());
}
```

Etape 3

```
urlLogin = "http://monWBT.com/Default.aspx? login =" + login + "&tstamp=" + timestamp + "&signature=" + signature;
```

Quelques détails :

-**Le système de cryptage** :

Le principe consiste à envoyer une requête contenant trois paramètres (login, date & heure et signature),

seule la valeur de la signature qui est hachée avec l'algorithme MD5 ,

la valeur du paramètre "*signature*" va contenir le Hashage MD5 du *login*, *date&heure* et la clé privée.

-La clé privée , c'est une donnée sur laquelle les administrateurs des deux applications se sont mis d'accord et qu'ils ont renseignés manuellement dans la configuration de leur application.

si par exemple on se met d'accord sur la valeur "SSOWBT3.4",c'est cette valeur la qui sera utilisée dans le calcul du hashage du triplet (login="xxxx", date&heure="xxxx", **clé privée="SSOWBT3.4"**)

Revision #2
Created 2 February 2026 14:39:05 by Thomas Etienne
Updated 14 October 2026 13:50:06 by Thomas Etienne