Paramétrages SSO

- SSO standard
- Paramétrer le SAML V2

SSO standard

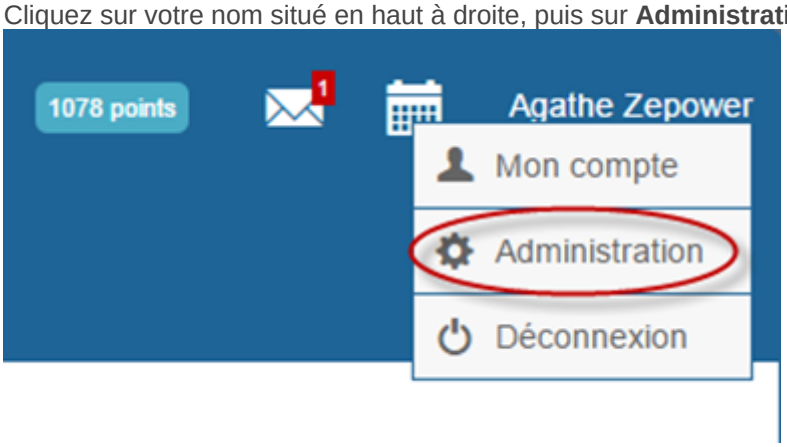
Procédure d'identification par SSO (Single Sign-On)

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"**)

Paramétrer le SAML V2

Vue d’ensemble de SAML V2

SAML 2.0 (Security Assertion Markup Language) est un standard d’échange d’informations d’authentification. Dans un scénario SSO, Le xLMS joue généralement le rôle de fournisseur de services (SP) et délègue l’authentification à un fournisseur d’identité (IdP).

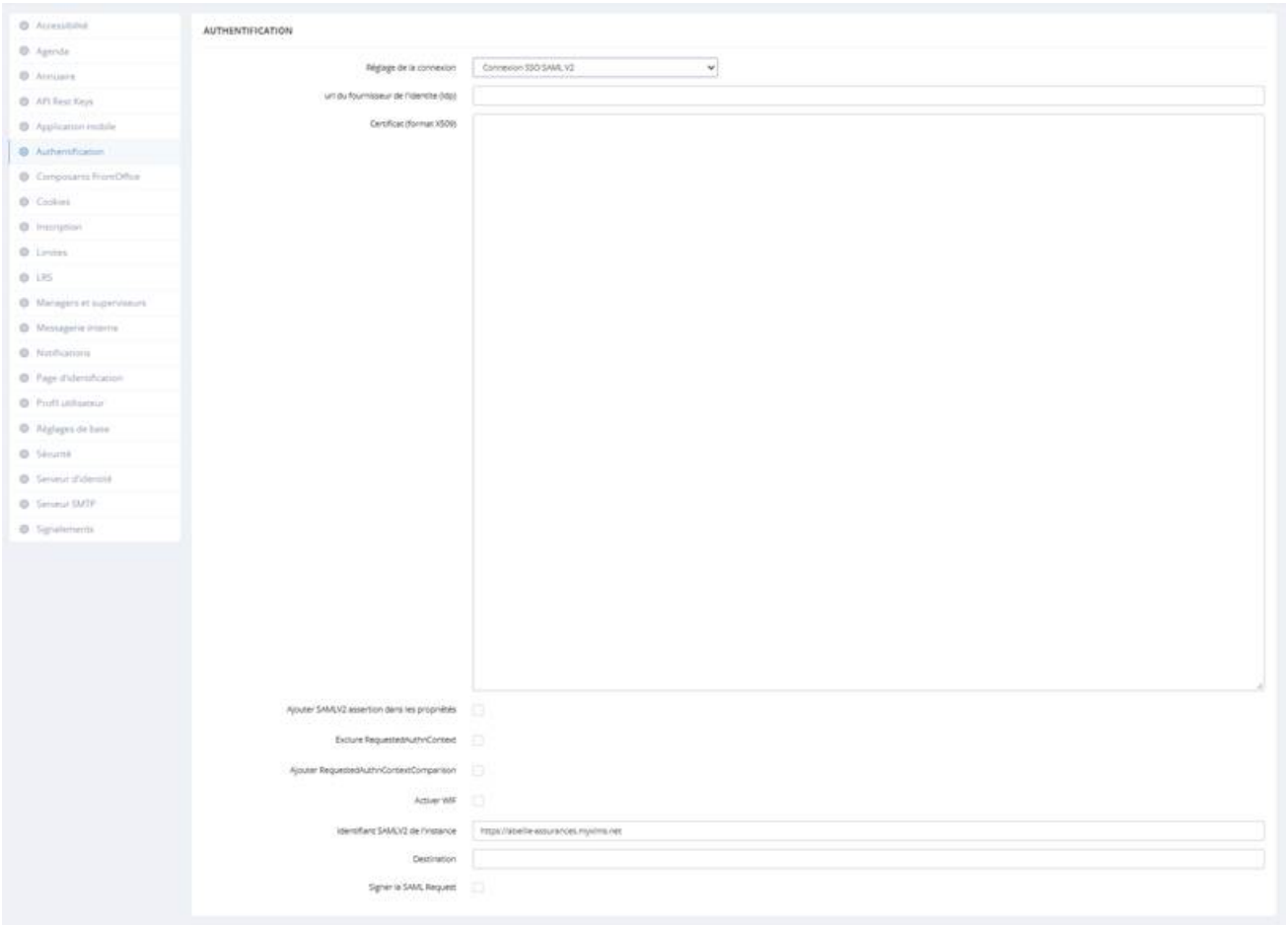
1. L’utilisateur demande l’accès à Le xLMS.
2. Le xLMS émet une requête d’authentification SAML (AuthnRequest) vers l’IdP.
3. L’IdP authentifie l’utilisateur selon les politiques de l’organisation.
4. L’IdP retourne une réponse contenant une assertion SAML signée.
5. Le xLMS valide la réponse, associe l’identité à un compte et ouvre la session.

Référentiel externe : Microsoft Learn - Protocole SAML d’authentification unique

Écran de configuration Le xLMS

Dans

- Réglages
- Réglages du domaine
- Communs
- Authentification



Paramètres SAML V2 disponibles

Paramètre Le xLMS	Format / valeur attendue	Rôle technique	Points de vigilance
Réglage de la connexion	Liste de sélection : Connexion SSO SAML V2	Active le mode d'authentification SAML V2 dans Le xLMS.	Prévoir un accès administrateur de secours avant toute bascule.
URL du fournisseur de l'identité (IdP)	URL HTTPS fournie par l'IdP	Point de redirection vers le service SSO de l'IdP.	Vérifier le domaine, HTTPS, l'environnement et l'absence d'espace.
Certificat (format X509)	Certificat public X.509, généralement PEM	Permet à Le xLMS de vérifier la signature des messages ou assertions reçus.	Surveiller l'expiration et préparer la rotation du certificat.
Ajouter SAML V2 assertion dans les propriétés	Case à cocher	Option Le xLMS liée à l'exposition ou au stockage de l'assertion dans les propriétés.	Finalité et portée à confirmer avec l'éditeur ; limiter les données personnelles.
Exclure RequestedAuthnContext	Case à cocher	Empêche l'envoi du bloc RequestedAuthnContext dans la requête SAML.	Utile en cas d'incompatibilité IdP ; tester les effets sur les politiques MFA.
Ajouter RequestedAuthnContextComparison	Case à cocher	Ajoute un mode de comparaison au contexte d'authentification demandé.	Valeur exacte et comportement à confirmer dans la documentation éditeur.
Activer WIF	Case à cocher	Active une option d'intégration WIF visible dans Le xLMS.	Compatibilité et prérequis non déductibles de la capture ; ne pas activer sans validation.

Identifiant SAML V2 de l'instance	URI / URL identifiant l'instance	Correspond à l'identifiant d'entité du SP (Entity ID / Issuer).	La valeur doit être strictement identique à celle déclarée dans l'IdP.
Destination	URL	Renseigne la destination SAML attendue ou ciblée.	La signification exacte côté Le xLMS doit être confirmée par test ou documentation éditeur.
Signer la SAML Request	Case à cocher	Demande la signature de la requête AuthnRequest émise par Le xLMS.	Nécessite généralement une clé/certificat SP et une configuration cohérente côté IdP.

Caractéristiques techniques synthétiques

Caractéristique	SAML V2 dans Le xLMS
Famille	SSO fédéré basé sur des assertions XML.
Rôles	Le xLMS : SP ; annuaire/fédération d'entreprise : IdP.
Données de confiance visibles	URL IdP et certificat public X.509.
Identifiant SP visible	Identifiant SAML V2 de l'instance.
Requête d'authentification	AuthnRequest, avec option de signature.
Contexte d'authentification	Options RequestedAuthnContext visibles dans l'interface.
Provisioning des comptes	Non déterminable à partir de la capture.
Attribut de correspondance utilisateur	Non visible ; à documenter (ex. identifiant interne, email, NameID).
Single Logout	Non visible ; prise en charge à confirmer.
Algorithmes cryptographiques	Non visibles ; à confirmer pour la signature et, le cas échéant, le chiffrement.
Compatibilité IdP	À valider en recette pour l'IdP retenu, notamment Microsoft Entra ID, ADFS, Okta ou autre.

Informations à collecter avant configuration

- Environnement concerné : recette, préproduction ou production.
- URL de connexion SSO de l'IdP.
- Certificat public de signature de l'IdP et date d'expiration.
- Entity ID / Issuer de Le xLMS.
- URL ACS (Assertion Consumer Service) attendue par Le xLMS.
- Format du NameID et attribut utilisé pour rapprocher l'utilisateur du compte Le xLMS.
- Liste des attributs obligatoires et optionnels transmis dans l'assertion.
- Politique de création, mise à jour, désactivation et suppression des comptes.
- Exigences de signature de l'AuthnRequest et de l'assertion/réponse.
- Politique MFA, niveau d'authentification et éventuel RequestedAuthnContext.
- Gestion de la déconnexion et comportement de session.
- Compte administrateur local de secours et procédure de retour arrière.

Procédure de configuration recommandée

1. Préparer l'IdP : Créer l'application d'entreprise, définir l'Entity ID, l'URL ACS, les attributs et les utilisateurs ou groupes autorisés.

2. Renseigner Le xLMS : Sélectionner “Connexion SSO SAML V2”, saisir l’URL IdP, importer le certificat X.509 et compléter les paramètres SP.
3. Aligner les options avancées : Configurer RequestedAuthnContext, la signature des requêtes et les options spécifiques uniquement après validation des exigences IdP.
4. Tester en recette : Valider un accès nominal, un utilisateur non autorisé, les attributs manquants, l’expiration de session et le retour d’erreur.
5. Sécuriser la mise en production : Conserver un accès local de secours, documenter la restauration, journaliser les changements et planifier la rotation du certificat.
6. Passer en exploitation : Définir la supervision, les contacts, les preuves de test et le processus de renouvellement du certificat.

Plan de tests minimal

ID	Cas de test	Résultat attendu
T01	Connexion SP-initiated	Redirection IdP, authentification, retour vers Le xLMS et ouverture de session.
T02	Utilisateur autorisé existant	Association correcte au compte et aux droits attendus.
T03	Utilisateur non autorisé	Refus contrôlé, sans création ou élévation de droits inattendue.
T04	Attribut d’identification absent	Échec explicite et journalisation exploitable.
T05	Certificat incorrect ou expiré	Rejet de la réponse SAML.
T06	Réponse modifiée ou signature invalide	Rejet de la réponse et absence d’ouverture de session.
T07	Horodatage hors tolérance	Rejet ou comportement conforme à la politique définie.
T08	MFA / contexte d’authentification	Respect de la politique IdP et compatibilité RequestedAuthnContext.
T09	Déconnexion / expiration	Fin de session conforme au comportement attendu.
T10	Retour arrière	Accès administrateur de secours et restauration validés.

Sécurité et exploitation

- Utiliser exclusivement des endpoints HTTPS et contrôler les domaines déclarés.
- Exiger la validation cryptographique des réponses/assertions et documenter les algorithmes autorisés.
- Limiter les attributs SAML au strict nécessaire et éviter d’exposer des données sensibles.
- Définir une alerte avant expiration du certificat et une procédure de rotation testée.
- Restreindre les droits d’administration de la configuration SSO.
- Conserver les journaux nécessaires au diagnostic sans enregistrer inutilement le contenu complet des assertions.
- Tester toute modification dans un environnement non productif et prévoir un retour arrière.

Points restant à confirmer avec l’éditeur Le xLMS

- URL ACS exacte et disponibilité de métadonnées SP téléchargeables.
- Formats NameID acceptés et attribut de rapprochement par défaut.
- Attributs obligatoires, règles de mapping et gestion des rôles/groupes.
- Création automatique des comptes et cycle de vie des utilisateurs.
- Prise en charge du chiffrement des assertions et algorithmes acceptés.
- Prise en charge du Single Logout.
- Comportement exact des options “Ajouter SAML V2 assertion dans les propriétés”, “Activer WIF” et “Destination”.
- Procédure de rotation simultanée de certificats et possibilité de gérer plusieurs certificats IdP.
- Journaux disponibles et messages d’erreur exploitables.