Bien sûr, voici la traduction du texte en français, en conservant les balises :

# Implémentation du SSO pour zebrix

# Qu'est-ce que l'authentification unique (SSO)

L'authentification unique (en anglais Single Sign-On ou SSO) est une méthode de contrôle d'accès permettant à un utilisateur d'accéder à plusieurs applications ou systèmes informatiques (liés mais indépendants). Avec cette fonctionnalité, un utilisateur se connecte avec un seul identifiant et mot de passe pour accéder à un ou plusieurs systèmes connectés sans utiliser de noms d'utilisateur ou de mots de passe différents, ou dans certaines configurations, se connecte de manière transparente à chaque système. (source : Wikipédia)

# Avantages

Les avantages de l'utilisation de l'authentification unique incluent :

Atténuer les risques d'accès aux sites tiers (les mots de passe des utilisateurs ne sont pas stockés ou gérés en externe)

Réduire la fatigue liée aux mots de passe due aux différentes combinaisons de noms d'utilisateur et de mots de passe

Réduire le temps passé à saisir à nouveau les mots de passe pour la même identité

Réduire les coûts informatiques grâce à un nombre moins élevé d'appels au support technique concernant les mots de passe

Le SSO s'appuie sur des serveurs d'authentification centralisés que toutes les autres applications et tous les autres systèmes utilisent à des fins d'authentification et combine cela avec des techniques pour s'assurer que les utilisateurs n'ont pas à saisir activement leurs identifiants plus d'une fois.

(source : Wikipédia)

# Implémentation du SSO avec zebrix

## Compatibilité

zebrix a été testé avec les protocoles/technologies d'authentification/SSO suivants :

CAS

OAuth

SAMLv2

ADFS

Microsoft 365 / Azure AD STS (Veuillez lire ce tutoriel pour savoir comment configurer Azure AD pour le SSO avec zebrix)

# Comment activer le SSO avec zebrix

Pour activer l'authentification SSO sur votre compte zebrix, veuillez suivre ces étapes :

## 1. Ajoutez l'application zebrix dans votre portail d'authentification

Veuillez créer l'application “zebrix” dans votre portail d'authentification. Si vous utilisez Microsoft 365, vous pouvez suivre ce guide technique.

Voici les métadonnées de zebrix que vous devrez utiliser :

```
<EntityDescriptor entityID="https://auth.zebrix.net"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIICsDCCAZgCCQCGpnz8YkjxkDANBgkqhkiG9w0BAQUFADAaMRgwFgYD
VQQDDA9h
dXRoLnplYnJpeC5uZXQwHhcNMTcwOTA1MTAzMjE2WhcNMjcwOTA1MTAzMjE2WjAa
MRgwFgYDVQQDDA9hdXRoLnplYnJpeC5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDJWm+DsyZOtWyoPXetbNoFRsfxqs0vunXkZV5lCFOE3IrDGtxV
l+ulGY1R2d0Fy1SAVNdYjXQIHxPwSFRW3G8OjHsrsZwfVHvcCxuySLqxTHXMaM6U
+W7XDiB8zuGTut3C47tPzGh9DLUXKqBRCpfn1pOtzSGLyd8ZQbsE4RfOAcdk0sA1
tX0mi0jiFmy0G1Md/qaBsM4Rq5inAU6A/IBXgE18MWXJYNAIr0vc1O7IGzqfu2KB
gI7opKnxyowXxr192FJ8XizUEte8Q6v+nWS0VaMw/mLoXZGSIiNGtrwkp1TddGpI
ONYzoc8PUGczJtXGjTlOVbirFySnyzaajFklAgMBAAEwDQYJKoZIhvcNAQEFBQAD
ggEBALp4cUX5Geag79iQTYoxlbKPhzzSogRJ7ufLwWOEniC0jmjvxS5nkr2vcXRO
TQqWgpXnbTQWSxdz01prE6NQy9eLWjIgXpCCa+18RCPJvCykFsnKzKGTsQI+/9HF
5HeB6qEmtrzY2QT9Hn30Z4bRma2L6OCYvwHOZz05XOaRyOHFSIBGGfRNOU4iBMRp
PkN+1p+EX07etvsDdZ1UnVg1kZQD6Br3hn3oAUvIctFrctThMd9hSh5GSx1UOhHv
7GfBWQ4Q4tYFOisPreeMgkuan+0x5j1pJwD3Ws2UDwl89lgACS96XmHtsHiwwJBb
I2NhPG6CSSWaSxiAHjyRZIHWPls=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
```

```
Redirect" Location="https://auth.zebrix.net/sso/logout"/>
<AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://auth.zebrix.net/sso/postResponse" index="0"/>
</SPSSODescriptor>
</EntityDescriptor>
```

Les revendications (claims) requises sont :

UPN (obligatoire)

Nom (Concaténation du prénom et du nom de famille) (recommandé)

Adresse e-mail (recommandé)

### 2. Contactez notre équipe de support pour demander l'activation du SSO à support@zebrix.net

Veuillez mentionner le nom de votre compte zebrix (nom du client)

Veuillez joindre votre XML de métadonnées ou donner l'URL publique pour y accéder

### 3. Notre équipe technique confirme l'activation du SSO

Lorsque la configuration aura été implémentée de notre côté, vous recevrez une confirmation de notre équipe technique, et vous pourrez vous connecter à zebrix en utilisant le SSO.

## Comment l'utilisateur se connectera-t-il à zebrix grâce au SSO ?

Les utilisateurs doivent se connecter à https://cmsv2.zebrix.net/cn/**votreNomDeSociete**. Le serveur zebrix vérifiera si l'utilisateur est déjà authentifié sur le portail d'authentification de votre entreprise. À cette étape, il y a trois possibilités :

Si un utilisateur est déjà authentifié sur votre portail et autorisé à utiliser zebrix, il sera directement connecté à zebrix et pourra l'utiliser.

Si un utilisateur n'est pas authentifié, il sera redirigé vers la page de connexion de votre entreprise et dès qu'il sera authentifié, il sera automatiquement redirigé vers zebrix.

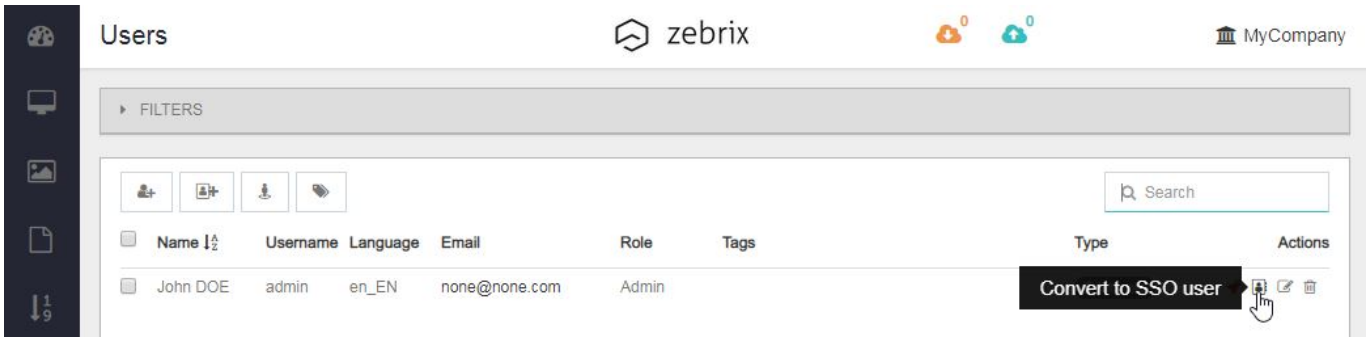
Dans les deux cas précédents, si l'utilisateur est encore inconnu de zebrix, il recevra un message “Utilisateur en attente d'activation”. Dans ce cas, un autre utilisateur zebrix (avec les droits d'administrateur) doit décocher la case “verrouiller” dans les propriétés de l'utilisateur.

Veuillez noter que les utilisateurs peuvent également être pré-activés en utilisant le bouton “Ajouter un utilisateur SSO”. Un utilisateur zebrix standard existant peut également être converti en utilisateur SSO.

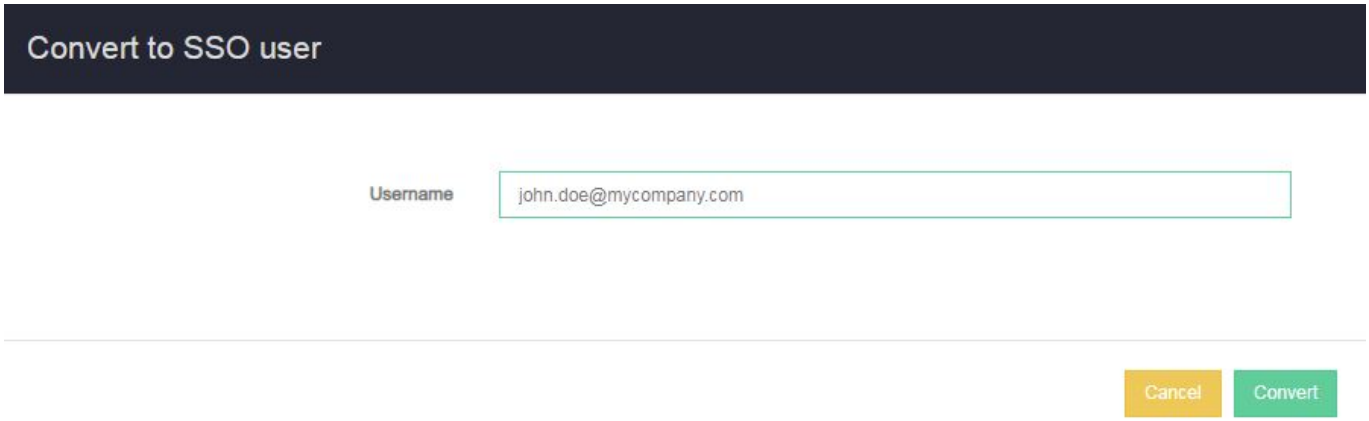
# Comment activer le SSO sur un utilisateur zebrix existant

Seul un utilisateur connu comme utilisateur SSO pourra se connecter via le SSO. Voici comment vous pouvez activer le SSO sur un utilisateur zebrix existant.

Cliquez sur le bouton de conversion

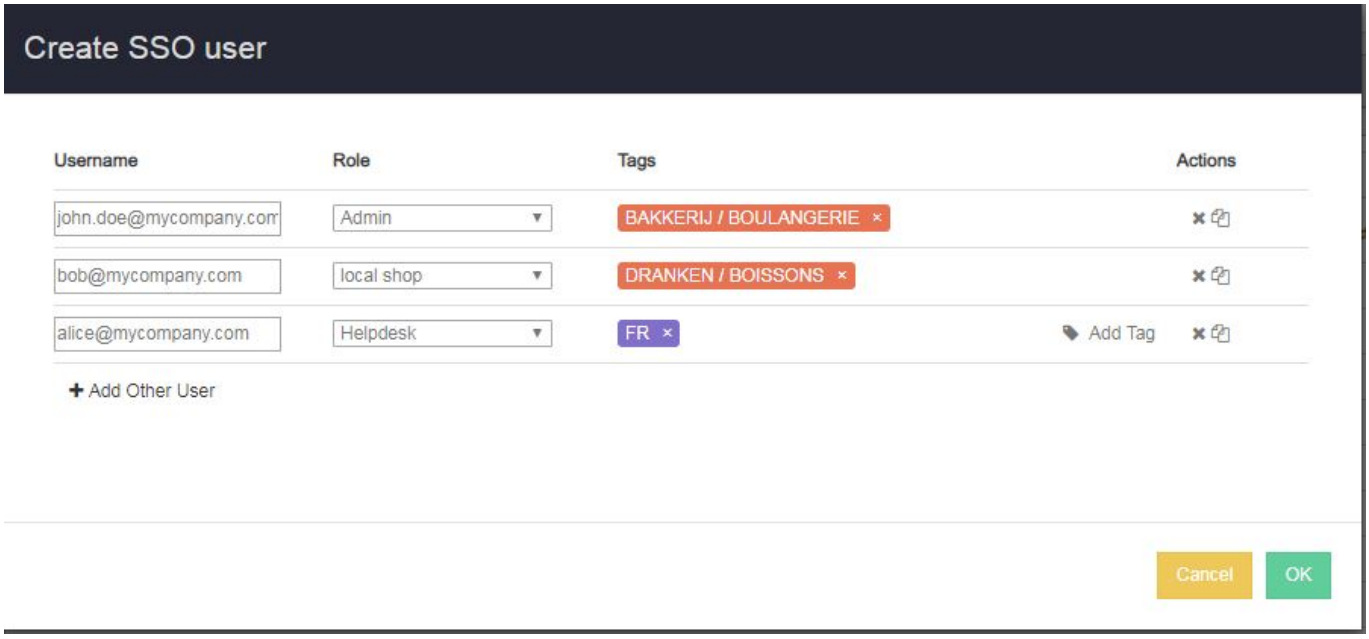



Spécifiez l'UPN de l'utilisateur tel qu'il sera reçu dans les revendications (claims)




# Comment créer de nouveaux utilisateurs SSO

Seul un utilisateur connu comme utilisateur SSO pourra se connecter via le SSO. Voici comment vous pouvez déclarer des utilisateurs SSO dans zebrix.




Grâce à cette fenêtre pop-up, vous pouvez créer/déclarer un ou plusieurs utilisateurs SSO en une seule opération.

## Comment activer le SSO sur les utilisateurs ajoutés automatiquement

Si un utilisateur SSO (inconnu de zebrix) essaie d'accéder à zebrix, il sera automatiquement déclaré dans zebrix comme un utilisateur SSO connu mais sera verrouillé. Il est nécessaire qu'un utilisateur de niveau administrateur active le compte.