SSO implementation for zebrix

What is Single Sign-On

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. (source: wikipedia)

Benefits

Benefits of using single sign-on include:

- Mitigate risk for access to 3rd-party sites (user passwords not stored or managed externally)
- Reduce password fatigue from different user name and password combinations
- Reduce time spent re-entering passwords for the same identity
- Reduce IT costs due to lower number of IT help desk calls about passwords

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

(source: wikipedia)

SSO implementation with zebrix

Compatibility

zebrix has been tested with following authentication/SSO protocols/technologies:

- CAS
- OAuth
- SAMLv2
- ADFS
- Office 365 / Azure AD STS (Please read this tutorial to know how to configure Azure AD for SSO with zebrix)

How to enable SSO with zebrix

1. You need to contact zebrix support

2. You have to integrate zebrix metadata in your authentication server

```
<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>
```

3. You have to send us your metadata file that we have to integrate in zebrix

4. Claims

Required claims are :

- UPN (mandatory)
  - Name (Concatenation of first and last name) (recommended)

- e-mail address (recommended)

How will user login to zebrix thanks to sso?

Users have to connect to https://cmsv2.zebrix.net/cn/yourCompanyName. zebrix server will communicate with your company's authentification server that will check if they are authenticated users. At this step, there are three possibilities:

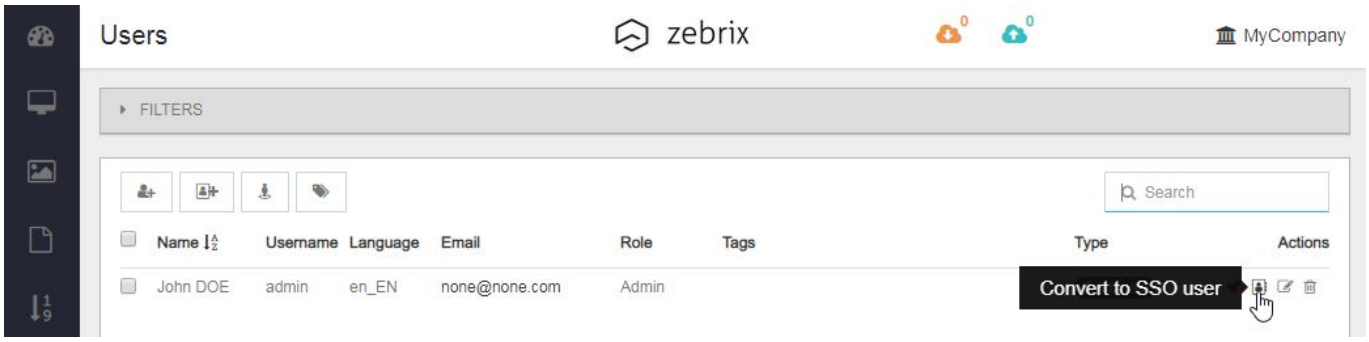
- If a user is already logged on your domain and authorized to use zebrix he will directly be logged into zebrix.
- If a user is not authenticated on your domain yet , he will be redirected on the login page of your company and as soon as he get authenticated he will be automatically redirected to zebrix.
- In both previous cases, if the user is still unknown by zebrix, he will get an “User Awaiting for activation” message. In this case, an admin user must uncheck the “lock” checkbox in the user properties.

Please note that users can also be pre-activated by using the “Add SSO user” button. Existing zebrix regular user can also be converted into SSO user.

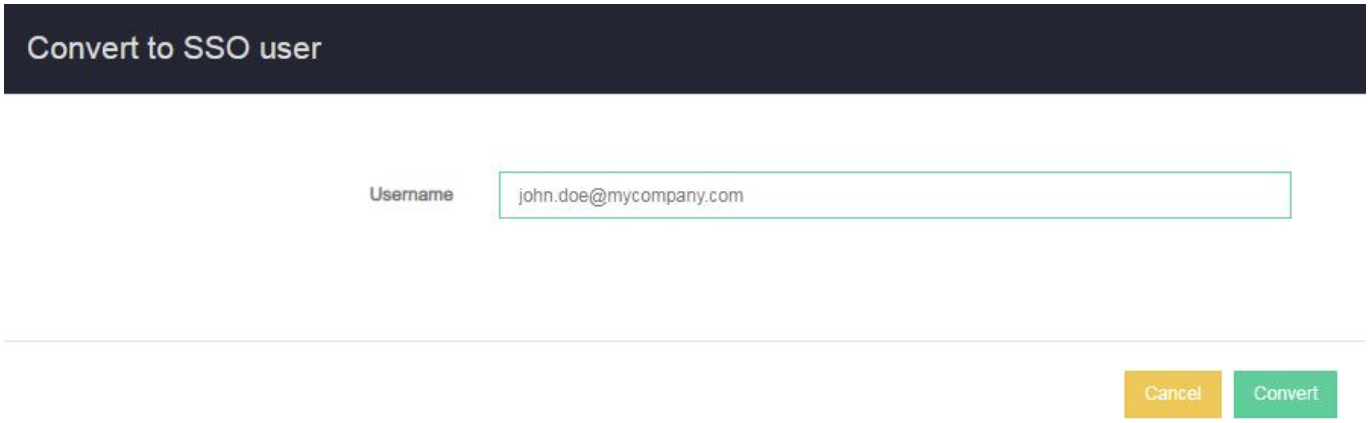
How to enable SSO on an existing zebrix user

Only user known as SSO user will be able to log in via SSO. Here is how you can enable SSO on existing zebrix user.

Click on the convert button

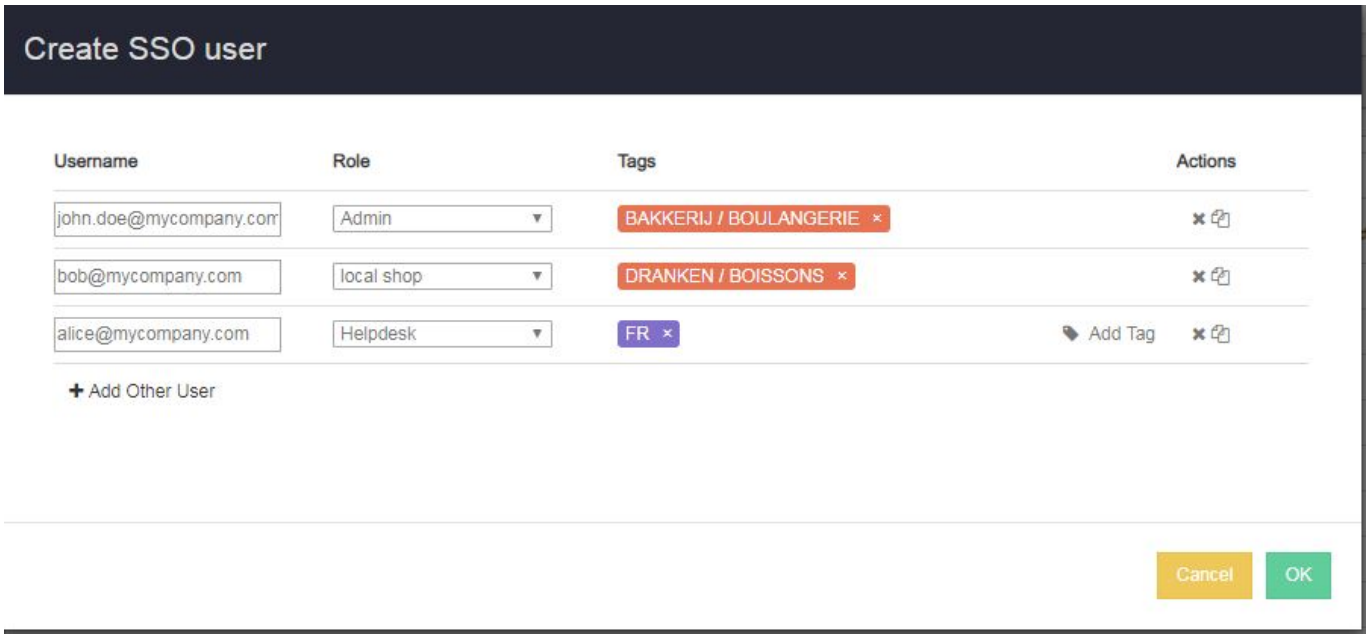


Specify the UPN of the user as it will be received in claims



How to create new SSO users

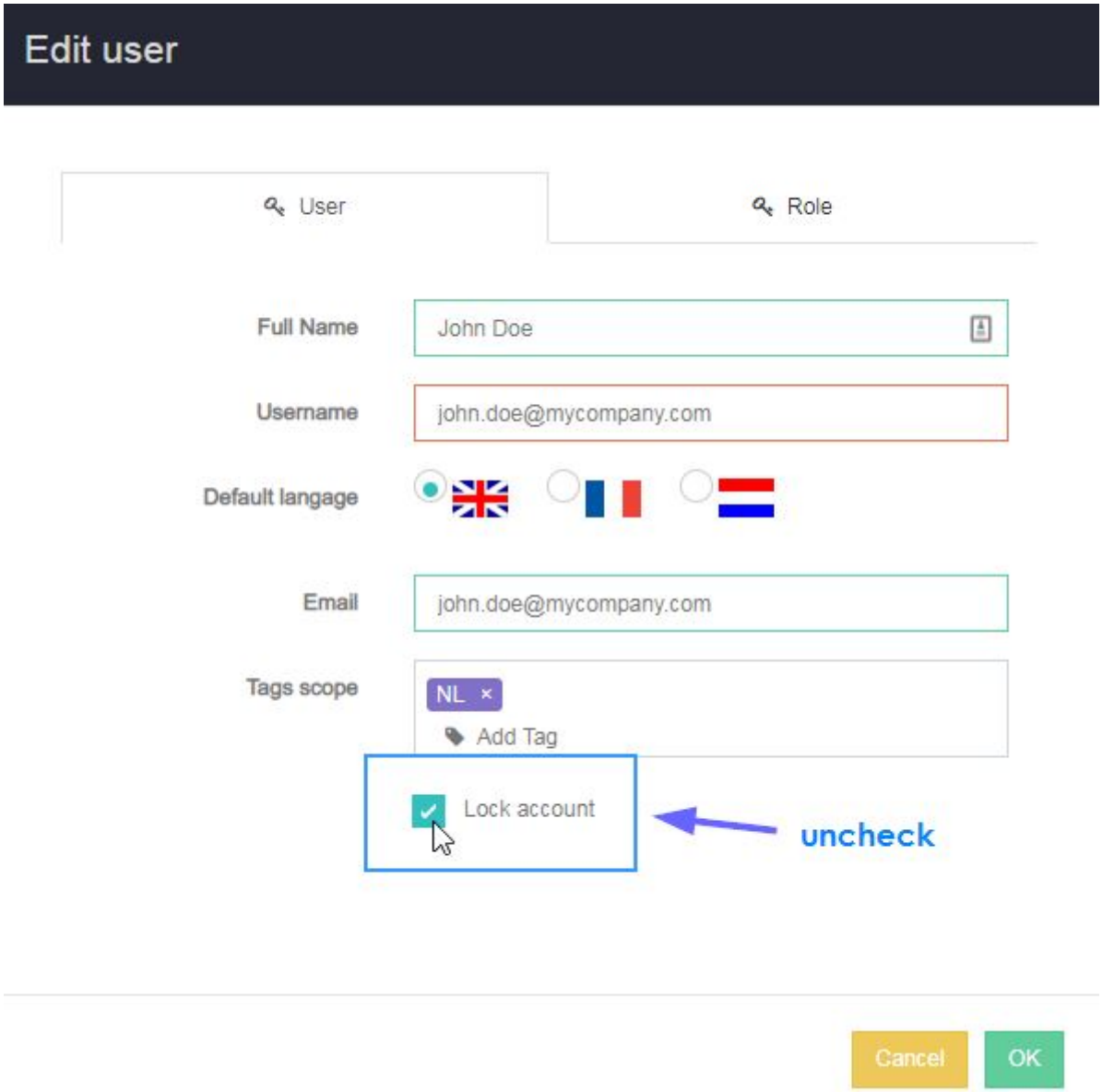
Only user known as SSO user will be able to log in via SSO. Here is how you can declare SSO users in zebrix.



Thanks to this pop-in window, you can create/declare one or many SSO users in one operation

How to enable SSO on auto-added users

If a SSO user (unknown by zebrix) tries to access zebrix, it will automaticaly declared in zebrix as know SSO user but will be locked. It is required that an admin level user enable the account



From:
https://documentation.zebrix.net/ - **zebrix signage documentation**

Permanent link:
https://documentation.zebrix.net/doku.php?id=en:sso_implementation&rev=1629880175

Last update: **2021/08/25 10:29**