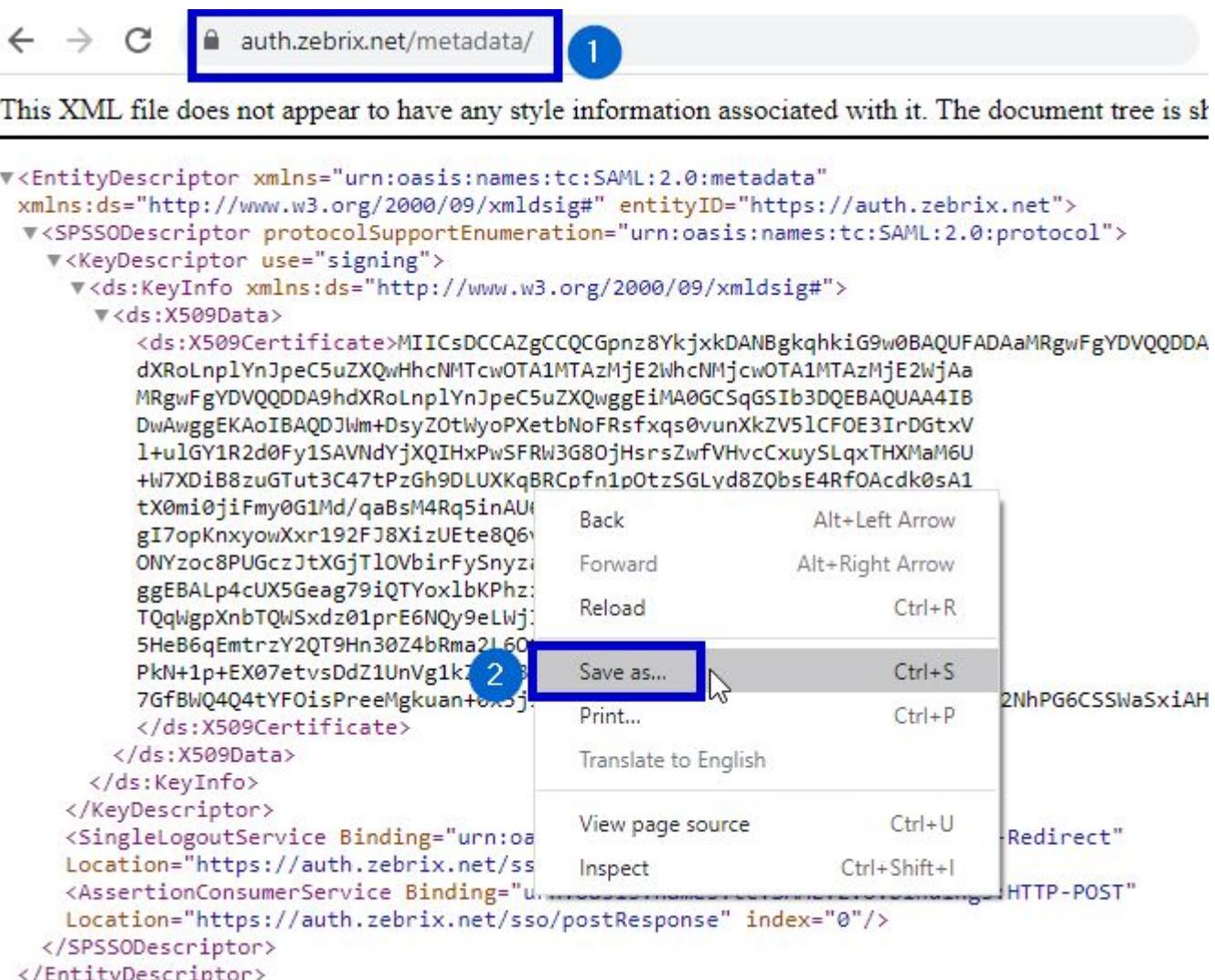


SSO implementation in zebrix with Azure AD (Office 365)

Save zebrix metadata in a file

1. Surf on <https://auth.zebrix.net/metadata>
2. Right click and save the file to a file with .xml extension



In the Azure AD admin center, add a new app

The screenshot shows the Azure Active Directory admin center with the 'Enterprise applications' page. A blue box labeled '1' highlights the 'Enterprise applications' link in the left sidebar. A blue box labeled '2' highlights the '+ New application' button in the top right corner of the main content area.

Create a new app using these options and call it "zebrix" or "zebrix CMS"

The screenshot shows the 'Create your own application' dialog box. A blue box labeled '1' highlights the '+ Create your own application' button. A blue box labeled '2' highlights the 'What's the name of your app?' input field containing 'zebrix'. A blue box labeled '3' highlights the 'Integrate any other application you don't find in the gallery (Non-gallery)' radio button.

zebrix overview

Properties

- Name: zebrix
- Application ID: 00000000-0000-0000-0000-000000000000
- Object ID: 00000000-0000-0000-0000-000000000000

Getting Started

- 1. Assign users and groups** 1
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on** 2
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

Choose which groups/users will be allowed to login

Manage

+ Add user/group

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no

Display Name	Object Type
No application assignments found	

Set the zebrix logo

Save the following logo



and upload it in the configuration

Dashboard > Enterprise applications > Browse Azure AD Gallery > zebrix CMS

zebrix CMS | Properties ...

Enterprise Application

Save Discard Delete Got feedback?

Enabled for users to sign-in? Yes No

Name * zebrix CMS

Homepage URL

Logo

"zebrix rounded logo.png"

User access URL https://myapps.microsoft.com/signin/zebrix%20CMS/a4610c37-b629-...
Application ID a4610c37-b629-4261-bdcd-6615c83ad15a

Overview Deployment Plan Manage Properties Owners Roles and administrators (Preview) Users and groups Single sign-on Provisioning Application proxy

The screenshot shows the Microsoft Azure portal's "Properties" page for the "zebrix CMS" enterprise application. The "Properties" tab is selected. The "Logo" field contains the previously uploaded black and white logo. The "Name" field is set to "zebrix CMS". The "Enabled for users to sign-in?" switch is set to "Yes". The "User access URL" field contains a placeholder URL, and the "Application ID" field contains a unique GUID.

Set up single sign-on : choose SAML

The screenshot shows the Azure Active Directory admin center with the URL https://aad.portal.azure.com/#blade/Microsoft_AAD_B2B/EnterpriseApplications/EnterpriseApplicationManagementBlade/~/appDetails/appId/{app-id}/singleSignOnMethod. The left sidebar shows 'Enterprise applications' selected. The main area shows the 'zebrix | Single sign-on' configuration. A blue box highlights the 'SAML' method under 'Select a single sign-on method'. Other options shown are 'Disabled' (not enabled) and 'Linked'.

Upload previously downloaded file to portal

The screenshot shows the Azure Active Directory admin center with the URL https://aad.portal.azure.com/#blade/Microsoft_AAD_B2B/EnterpriseApplications/EnterpriseApplicationManagementBlade/~/appDetails/appId/{app-id}/singleSignOnMethod. The left sidebar shows 'Enterprise applications' selected. The main area shows the 'zebrix | SAML-based Sign-on' configuration. A blue box highlights the 'Upload metadata file' button. A file dialog is open, showing a list of files in the 'Downloads' folder. The file 'zebrix.xml' is selected and highlighted with a blue box. Numbered callouts (1-4) point to the 'Upload metadata file' button, the 'Select a file' button in the dialog, the 'zebrix.xml' file in the list, and the 'Add' button in the dialog respectively.

Add a "Sign On URL" and save the basic SAML configuration

Some fields will be prefilled thanks to the imported .XML file, but the "Sign On URL" needs to be filled manually. Please specify the following URL: <https://cms.zebrix.net/cn/customername> (please

replace **customername** with your actual customer name on zebrix)

Basic SAML Configuration

 Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

`https://auth.zebrix.net`



Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

`https://auth.zebrix.net/sso/postResponse`



Sign on URL ⓘ

Please adjust to your zebrix customer name

`https://cms.zebrix.net/cn/customername`



Relay State ⓘ

Enter a relay state

Logout Url ⓘ

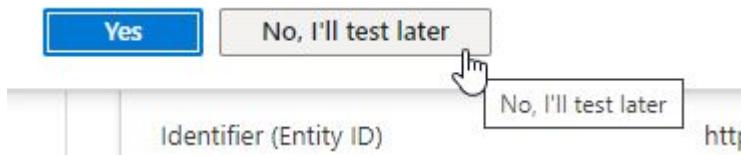
`https://auth.zebrix.net/sso/logout`



Skip SSO login test

Test single sign-on with zebrix

To ensure that single sign-on works for your application, to test now?



Edit User attributes and claims

A screenshot of the Azure Active Directory admin center. The left sidebar shows navigation options like Dashboard, All services, Favorites, Azure Active Directory, Users, and Enterprise applications. Under 'Enterprise applications', 'zebrix CMS' is selected. The main content area shows the 'zebrix CMS | SAML-based Sign-on' configuration. It includes sections for 'Basic SAML Configuration' (with fields for Identifier (Entity ID), Reply URL, Sign on URL, Relay State, and Logout URL) and 'User Attributes & Claims' (with a table mapping attributes like givenname, surname, emailaddress, name, displayname, and Unique User Identifier to their corresponding user properties). A callout box highlights the 'Edit user attributes & claims' link.

Add a new claim

A screenshot of the Azure Active Directory admin center. The left sidebar shows navigation options like Dashboard, All services, Favorites, Azure Active Directory, Users, and Enterprise applications. Under 'Enterprise applications', 'zebrix' is selected. The main content area shows the 'User Attributes & Claims' configuration. It includes sections for 'Required claim' (with a table for Unique User Identifier (Name ID)) and 'Additional claims' (with a table for emailaddress, givenname, name, and surname). A callout box highlights the '+ Add new claim' button.

The screenshot shows the 'Manage claim' page in the Azure Active Directory admin center. The 'Name' field is set to 'displayname'. In the dropdown for 'Source attribute', 'user.displayname' is selected. The 'Save' button is highlighted.

1. Use **displayname** as name
2. In the name space field please copy / paste the following namespace
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims>
3. In the dropdown list, select the value **user.displayname**
4. Press the **Save** button

Copy the "App Federation Metadata URL" and send it to support@zebrix.net

The screenshot shows the 'zebrix | SAML-based Sign-on' page. Under 'Single sign-on', the 'App Federation Metadata Url' link is highlighted.

Our Technical team will implement your settings on zebrix side and activate to SSO on your account

From:

<https://documentation.zebrix.net/> - **zebrix documentation**

Permanent link:

https://documentation.zebrix.net/doku.php?id=en:sso_implementation_azuread&rev=1623864278

Last update: **2021/06/16 19:24**

