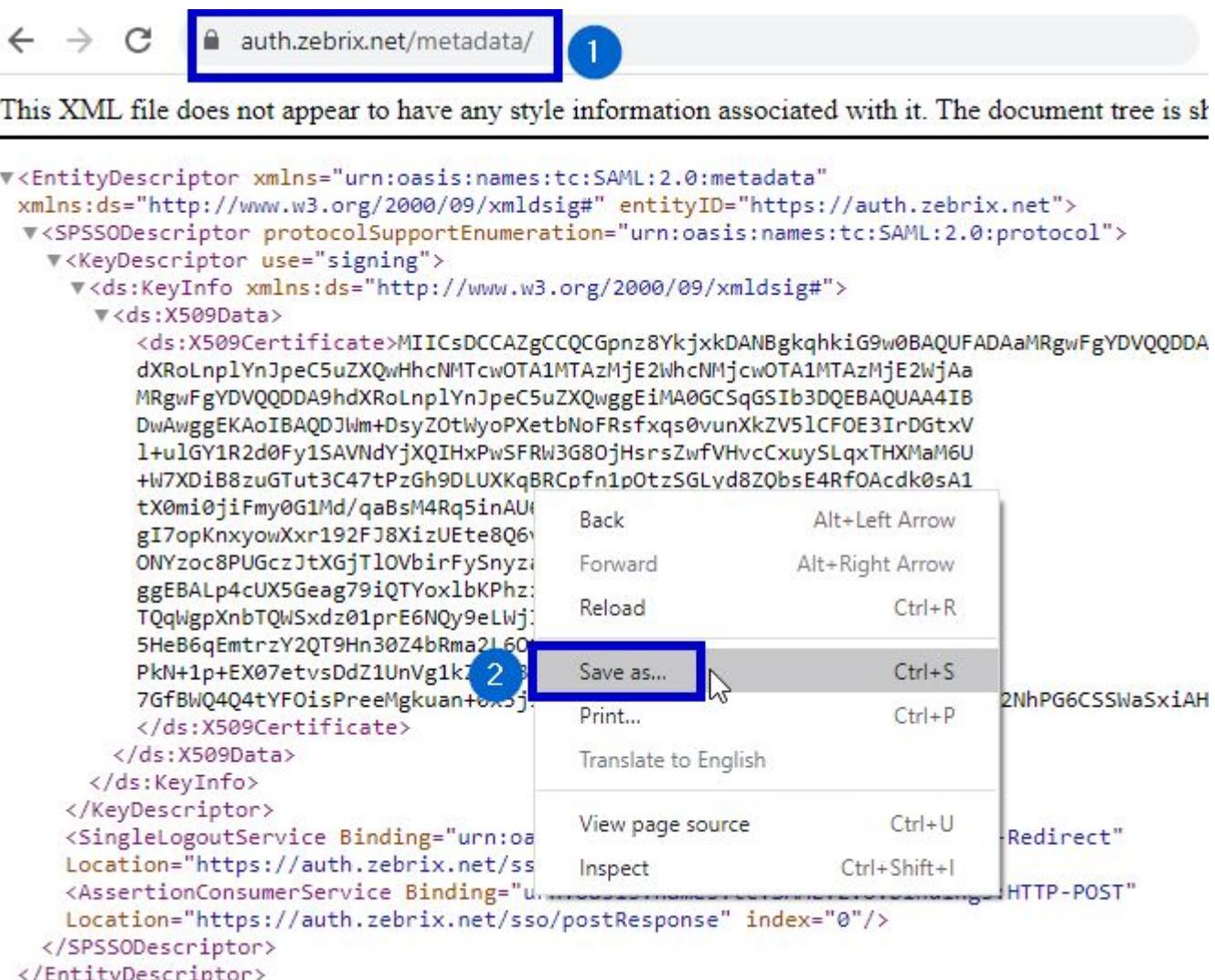


SSO implementation in zebrix with Azure AD (Office 365)

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 selected in the sidebar (1). The main area displays a list of applications with columns for Name and Homepage URL. A callout box highlights the '+ New application' button in the top right corner (2).

Create a new app using these options and call it zebrix

The screenshot shows the 'Create your own application' dialog box. It includes fields for 'What's the name of your app?' (2) and a list of options for what to do with the application (3). The 'Integrate any other application you don't find in the gallery (Non-gallery)' option is selected.

zebrix overview

Azure Active Directory admin center

zebrix | Overview Enterprise Application

Properties

- Name: zebrix
- Application ID: 00000000-0000-0000-0000-000000000000
- Object ID: e01e01e0-01e0-01e0-01e0-01e001e001e0

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

Azure Active Directory admin center

zebrix | Users and groups Enterprise Application

Manage

+ Add user/group

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no if you do not want users to see this application in the Access Panel.

Display Name	Object Type
No application assignments found	

Set up single sign-on : choose SAML

Last update: 2021/04/28 en:sso_implementation_azuread https://documentation.zebrix.net/doku.php?id=en:sso_implementation_azuread&rev=1619594287 09:18

The screenshot shows the Azure Active Directory admin center interface. On the left, there's a navigation sidebar with links like Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main area shows the 'zebrix | Single sign-on' page under 'Enterprise applications'. A sub-menu on the left includes Overview, Deployment Plan, Manage (Properties, Owners, Roles and administrators (Preview), Users and groups), Single sign-on (selected), Provisioning, Application proxy, Self-service, Security, and Conditional Access. The main content area is titled 'Select a single sign-on method' with a 'Help me decide' link. It lists four options: 'Disabled' (disabled), 'SAML' (selected and highlighted with a blue border), 'Password-based', and 'Linked'. The 'SAML' option is described as 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

Upload previously downloaded file to portal

The screenshot shows the 'zebrix | SAML-based Sign-on' page in the Azure Active Directory admin center. The left sidebar has the same structure as the previous screenshot. The main area shows the 'SAML-based Sign-on' configuration with fields for Reply URL, Sign URL, Relay State, and Logout URL. A 'Change single sign-on mode' link is also present. A 'Test this application' button and a 'Got feedback?' link are at the top right. Below the configuration, there's a 'Upload metadata file' section with a 'Select a file' button. A file dialog is open, showing a file named 'zebrix.xml' in the 'Downloads > metadata' folder. The file details show it's an XML Document (*.xml) from 15/03/2021 17:25. Buttons for 'Open' and 'Cancel' are at the bottom of the dialog.

Save the basic SAML configuration

The screenshot shows the Azure Active Directory admin center with the following details:

- Left sidebar:** Shows navigation sections like Dashboard, All services, FAVORITES (Azure Active Directory, Users), and Enterprise applications.
- Top navigation bar:** Includes icons for Home, Notifications (6), Settings, Help, and Logout.
- Current location:** Dashboard > Enterprise applications > zebrix > Overview.
- Page title:** zebrix | SAML-based Sign-on
- Section:** Basic SAML Configuration
- Buttons:** Save (highlighted with a blue box).
- Form fields:**
 - Identifier (Entity ID) ***: https://auth.zebrix.net (Default checked)
 - Reply URL (Assertion Consumer Service URL) ***: https://auth.zebrix.net/sso/postResponse (Default checked)
 - Sign on URL**: Enter a sign on URL
 - Relay State**: Enter a relay state
 - Logout Url**: https://auth.zebrix.net/sso/logout
- Help text:** The default identifier will be the audience of the SAML response for IDP-initiated SSO; The default reply URL will be the destination in the SAML response for IDP-initiated SSO.
- Side navigation:** Shows sections 1 (Basic SAML Configuration), 2 (User Attributes & Claims), and 3 (SAML Signing Certificate).

Skip SSO login test

Test single sign-on with zebrix

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

Yes

No, I'll test later

Identifier (Entity ID)

No, I'll test later

http|

Edit User attributes and claims

Last update: en:sso_implementation_azuread https://documentation.zebrix.net/doku.php?id=en:sso_implementation_azuread&rev=1619594287
2021/04/28 09:18

Azure Active Directory admin center

Dashboard > Enterprise applications > zebrix CMS >

zebrix CMS | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan

Upload metadata file Change single sign-on mode Test this application Got feedback?

Set up Single Sign-On with SAML

Read the configuration guide for help integrating zebrix CMS.

Basic SAML Configuration

Identifier (Entity ID)	https://auth.zebrix.net
Reply URL (Assertion Consumer Service URL)	https://auth.zebrix.net/sso/postResponse
Sign on URL	https://cms.zebrix.net/cn/customername
Relay State	Optional
Logout Url	https://auth.zebrix.net/sso/logout

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
displayname	user.displayname
Unique User Identifier	user.userprincipalname

1 Edit

2 Edit

Edit user attributes & claims

Properties Owners Roles and administrators (Preview) Users and groups Single sign-on Provisioning Application proxy Self-service Security Conditional Access Permissions Token acquisition

Add a new claim

Azure Active Directory admin center

Dashboard > Enterprise applications > zebrix > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***]

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

The screenshot shows the 'Manage claim' page in the Azure Active Directory admin center. The 'Name' field contains 'displayname' (step 1). In the 'Source attribute' dropdown, 'user.displayname' is selected (step 2). The 'Save' button is highlighted (step 3).

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 in the Azure Active Directory admin center. The 'App Federation Metadata Url' link is highlighted (step 3).

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=1619594287

Last update: **2021/04/28 09:18**

