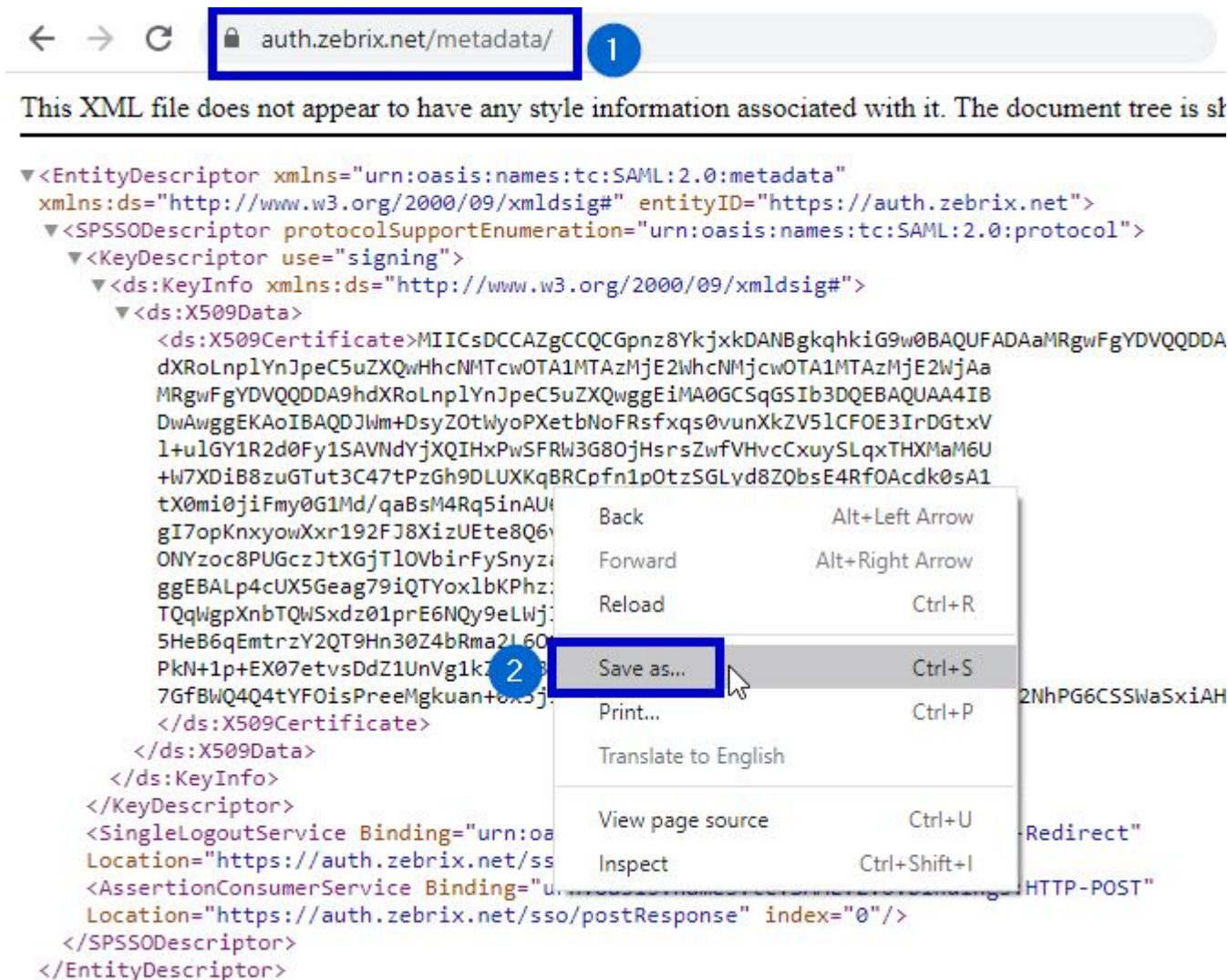


SSO implementation in zebrix with Azure AD

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



Create a new app using these options and call it zebrix



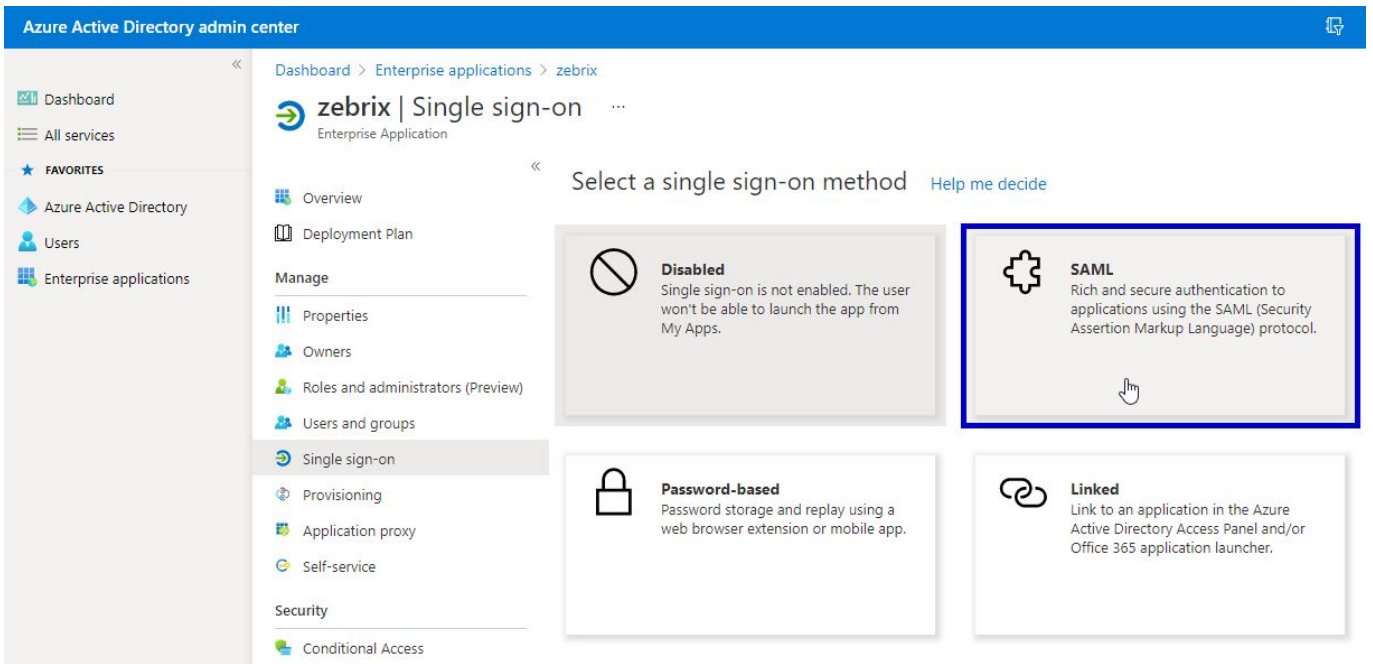
zebrix overview



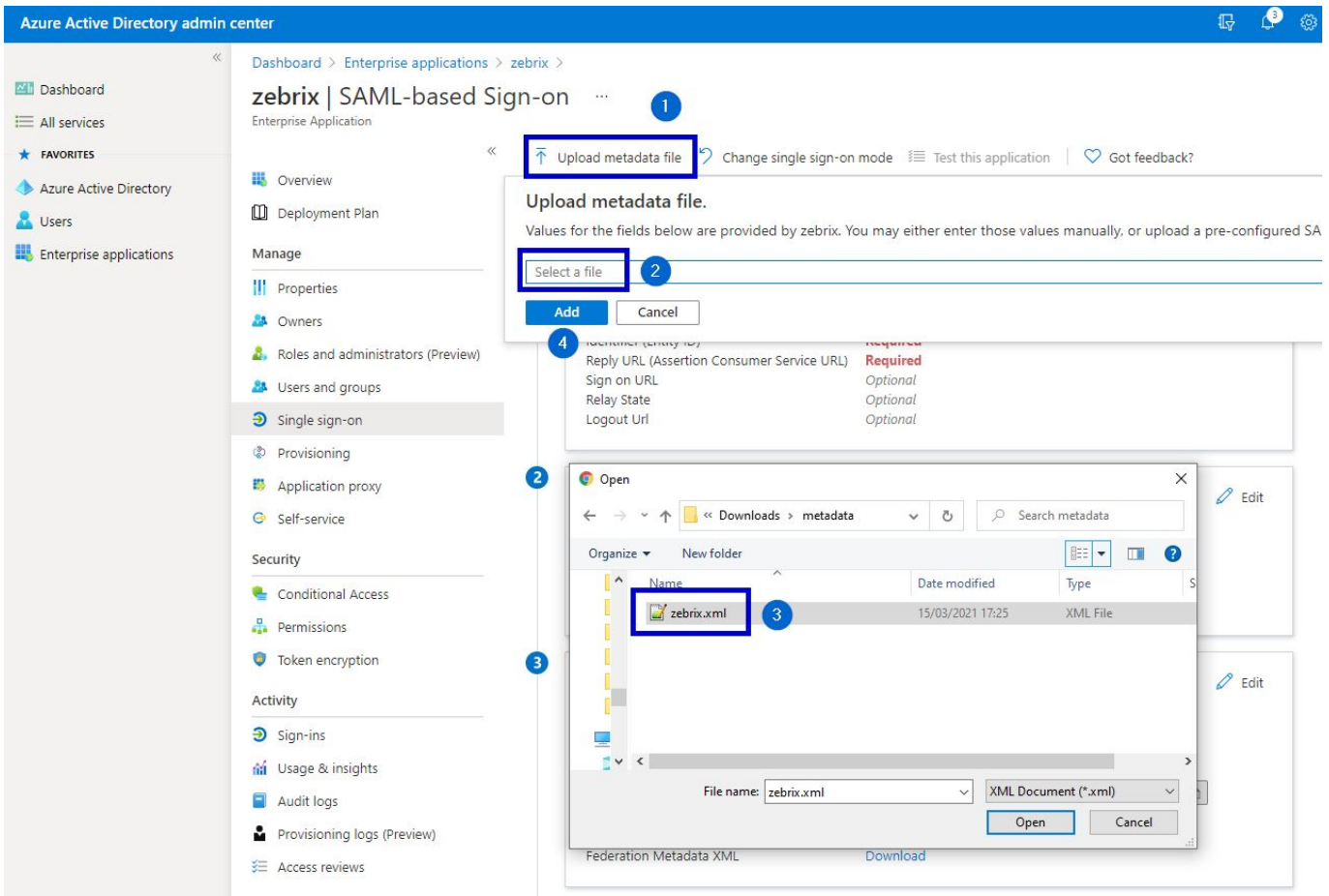
Choose which groups/users will be allowed to login



Set up single sign-on : choose SAML



Upload previously downloaded file to portal



Save the basic SAML configuration

The screenshot shows the Azure Active Directory admin center interface. The left-hand navigation pane includes sections for Dashboard, All services, FAVORITES, Azure Active Directory, Users, Enterprise applications, Provisioning, Application proxy, Self-service, Security, and Activity. The main content area is titled "zebrix | SAML-based Sign-on" and shows a progress indicator with three steps: 1. Basic SAML Configuration, 2. User Attributes & Claims, and 3. SAML Signing Certificate. The "Basic SAML Configuration" step is active, displaying a "Basic SAML Configuration" form. The form includes fields for Identifier (Entity ID), Reply URL (Assertion Consumer Service URL), Sign on URL, Relay State, and Logout URL. The values entered are: Identifier (Entity ID) as https://auth.zebrix.net, Reply URL (Assertion Consumer Service URL) as https://auth.zebrix.net/sso/postResponse, and Logout URL as https://auth.zebrix.net/sso/logout. A "Save" button is highlighted with a red box at the top of the form.

Skip SSO login test

The screenshot shows a dialog box titled "Test single sign-on with zebrix". The text inside the dialog asks, "To ensure that single sign-on works for your application, to test now?". There are two buttons: "Yes" and "No, I'll test later". A mouse cursor is pointing at the "No, I'll test later" button. Below the dialog, a portion of a table is visible, showing a column header "Identifier (Entity ID)" and a value "https://auth.zebrix.net/sso/postResponse".

Edit User attributes and claims

Azure Active Directory admin center

Dashboard > Enterprise applications > zebrix CMS >

zebrix CMS | SAML-based Sign-on

Enterprise Application

Overview | Deployment Plan | Manage

Properties | Owners | Roles and administrators (Preview) | Users and groups | **Single sign-on** | Provisioning | Application proxy | Self-service

Security | Conditional Access | Permissions | Token acquisition

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

Add a new claim

Azure Active Directory admin center

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

User Attributes & Claims

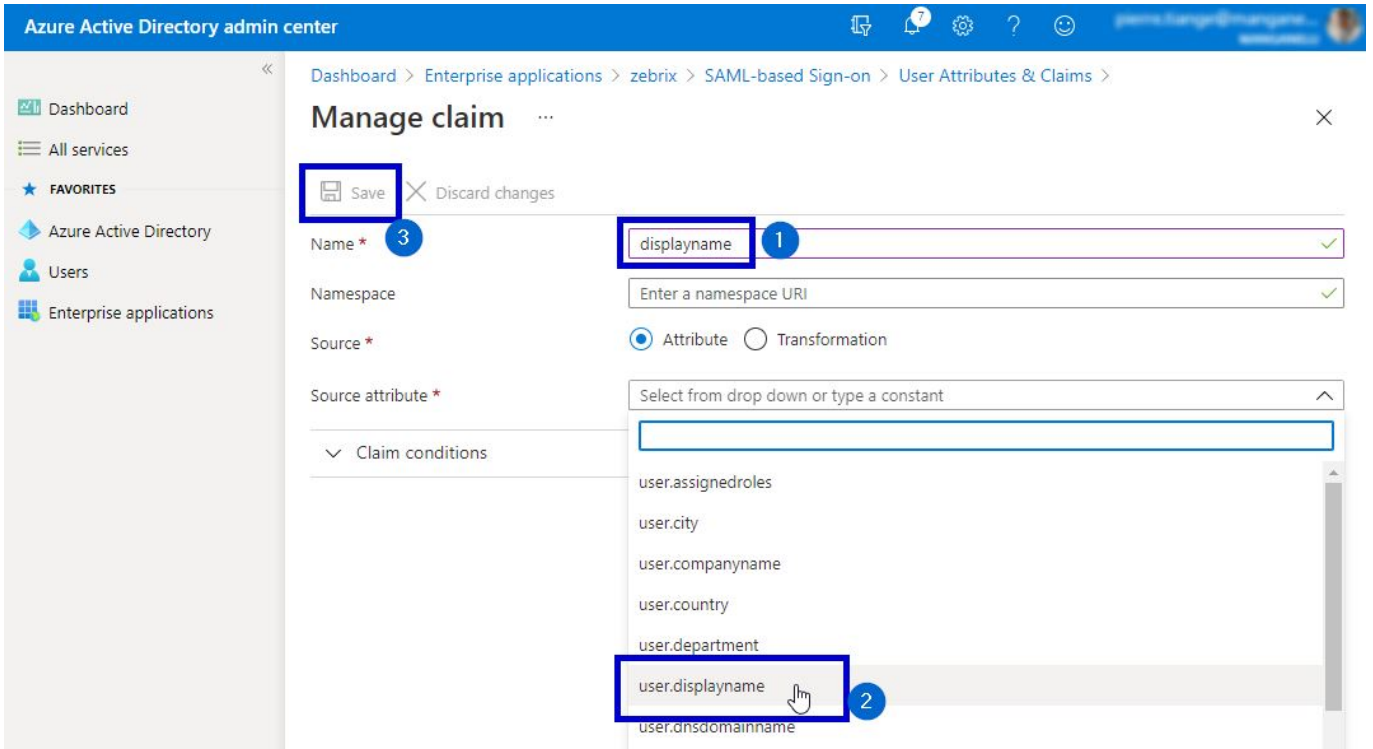
+ Add new claim | + Add a group claim | Columns

Required claim

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

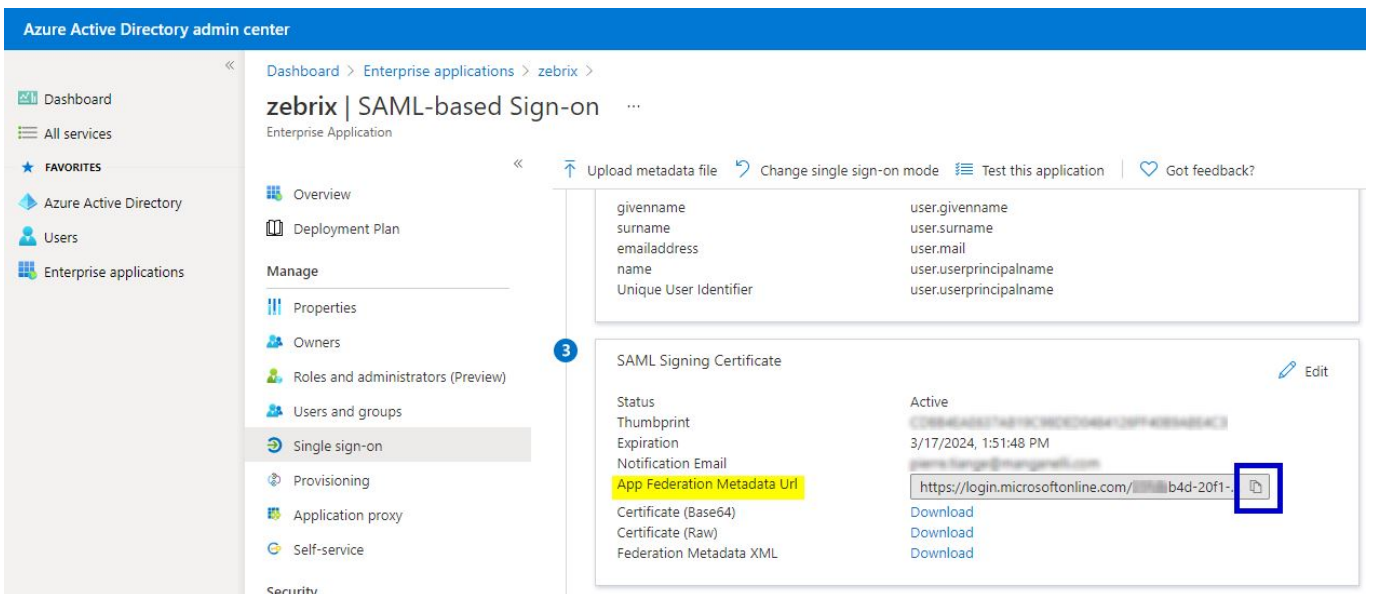
Additional claims

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 ***



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 Metadate URL" and send it to support@zebrix.net



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

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

Permanent link: https://documentation.zebrix.net/doku.php?id=en:sso_implementation_azuread&rev=1616056471

Last update: **2021/03/18 09:34**

