Token encryption in Microsoft Azure SSO with Ezeelogin

617 Nesvin KN June 20, 2023 Security Features 689

How to enable token encryption in Microsoft Azure for SAML authentication?

Refer article to integrate Microsoft Azure SSO authentication in Ezeelogin.

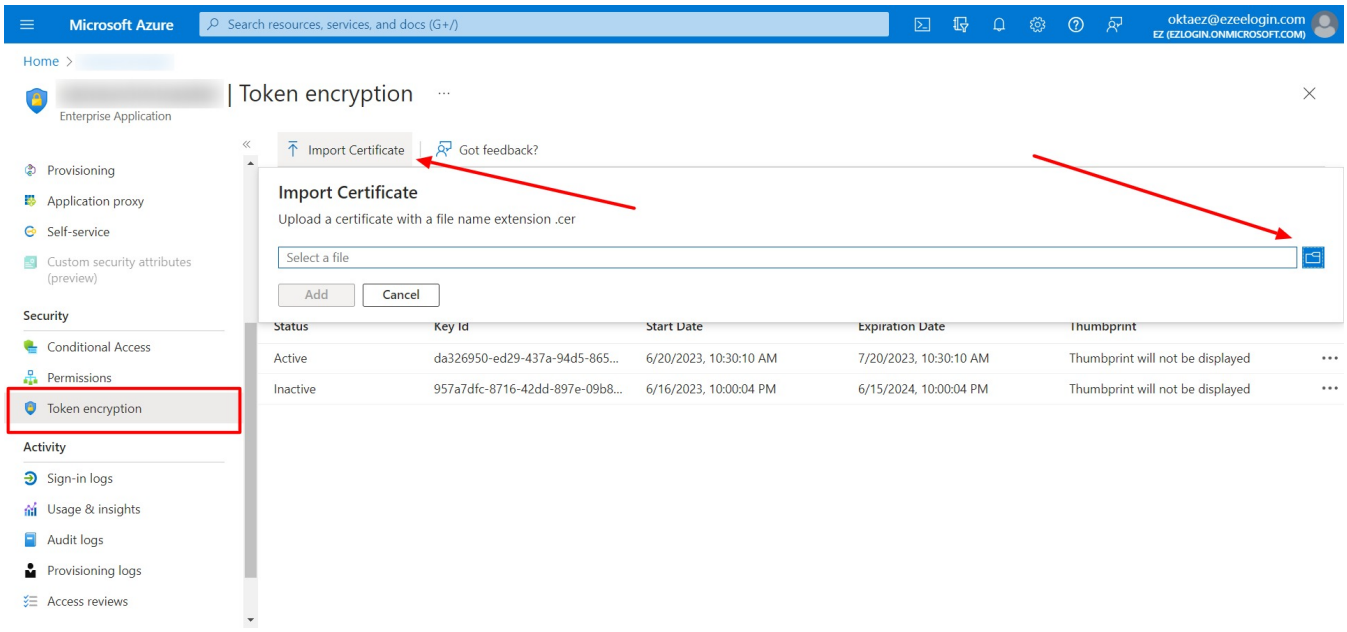
1. Create a new private key

2. Generate a certificate signing request (CSR) associated with your private key.

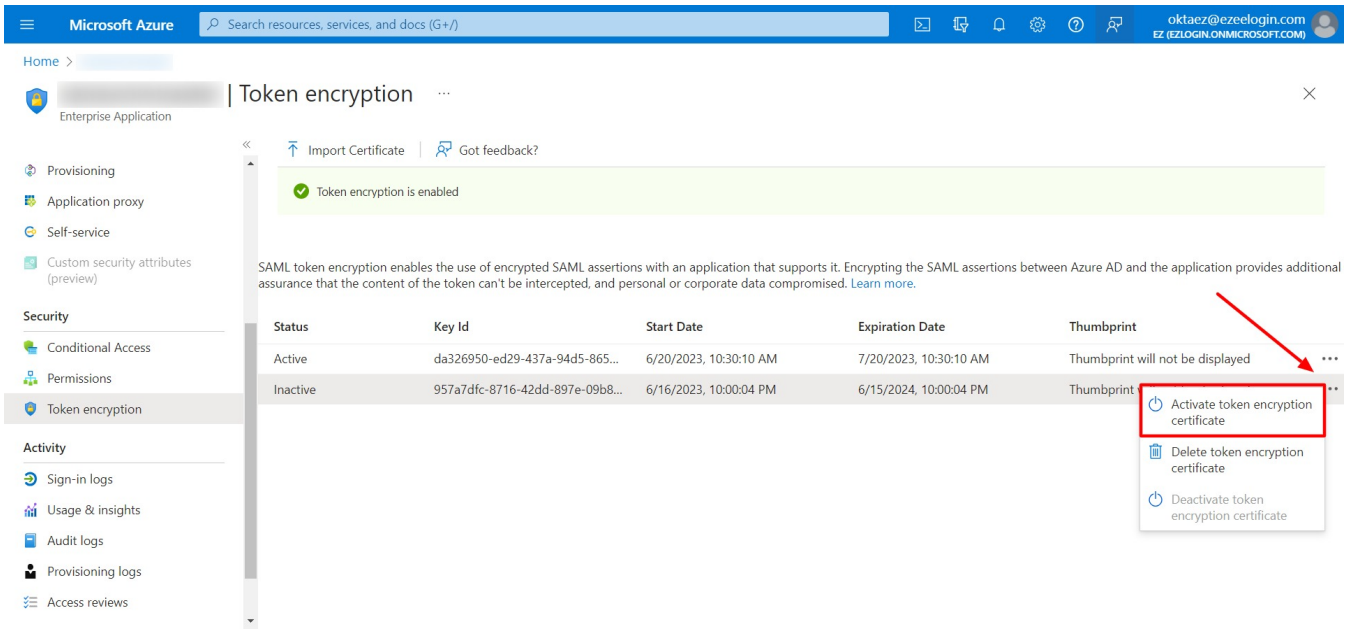
3. Convert a .csr (Certificate Signing Request) file to a .cer (Certificate) file.

4. Download the certificate to your PC.

5. Click on the **Token encryption** on your **Enterprise application**. Click on **import certificate** and import the certificate file from your PC with the **.cer extension**.

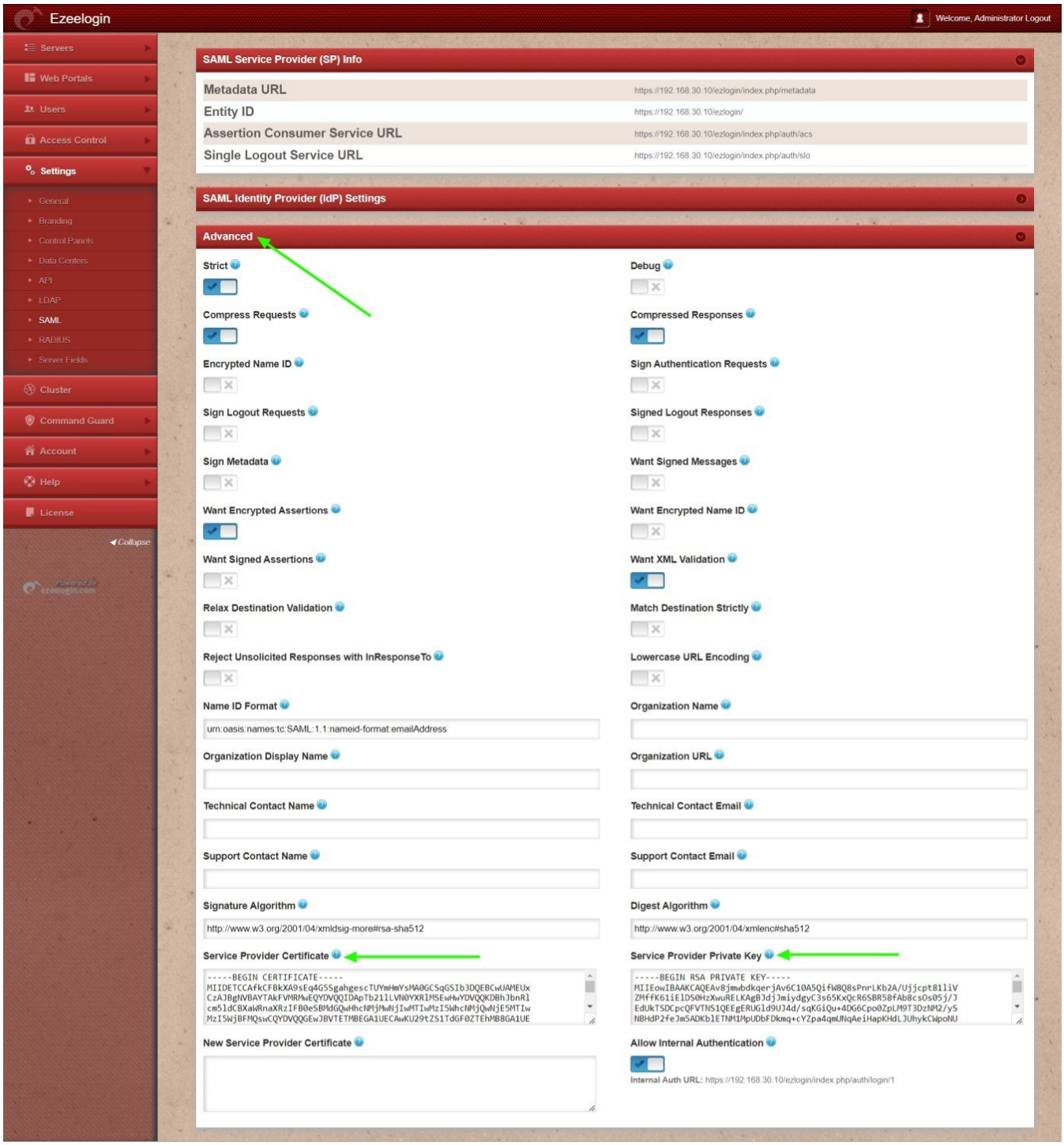


6. Activate the certificate by clicking on three dots and **Activate token encryption certificate.**



7. Add the certificate and private key in **Ezeelogin SAML advanced settings**.

Use the certificate and private key in **Service Provider Certificate** and **Service Provider Private Key.**



Enable **Auto Create** and change **web panel authentication to SAML**. Clear the browser cache and try to log in to Ezeelogin with Azure login credentials.

Common errors while accessing Ezeelogin with Microsoft Azure token encryption configured

No private key available, check settings

This error happens because **Service Provider Certificate** or **Service Provider Private Key** field is empty.

Key is missing data to perform the decryption

This error happens because the **private key saved in Ezeelogin is different from the key used to generate the certificate used in Azure token encryption**.

Related Articles

- Integrate Microsoft Azure SSO and AD with Ezeelogin
- Unable to login with Azure SSO
- Integrate GSuite SSO with Ezeelogin
- Integrate Jumpcloud SSO with Ezeelogin
- Integrate AWS SSO with Ezeelogin
- Integrate Okta SSO with Ezeelogin
- Integrate OneLogin SSO with Ezeelogin
- Disable SAML /SSO Authentication on Ezeelogin

Online URL:
https://www.ezeelogin.com/kb/article/token-encryption-in-microsoft-azure-sso-with-ezeelogin-617.html