

Token encryption in Microsoft Azure SSO with Ezeelogin

617 Nesvin KN April 8, 2025 [Security Features](#) 1603

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

Overview: This article helps to enable token encryption in Microsoft Azure for SAML authentication.

Refer article to [integrate Microsoft Azure SSO authentication in Ezeelogin](#).

Step 1: Create a new private key

```
root@gateway:~# openssl genrsa -out key_name.key key_strength
```

EXAMPLE

```
root@gateway:~# openssl genrsa -out private_key.key 2048
```

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

```
root@gateway:~# openssl req -new -key path_to_private_key.key -out  
csr_name.csr
```

EXAMPLE

```
root@gateway:~# openssl req -new -key private_key.key -out CSR.csr
```

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

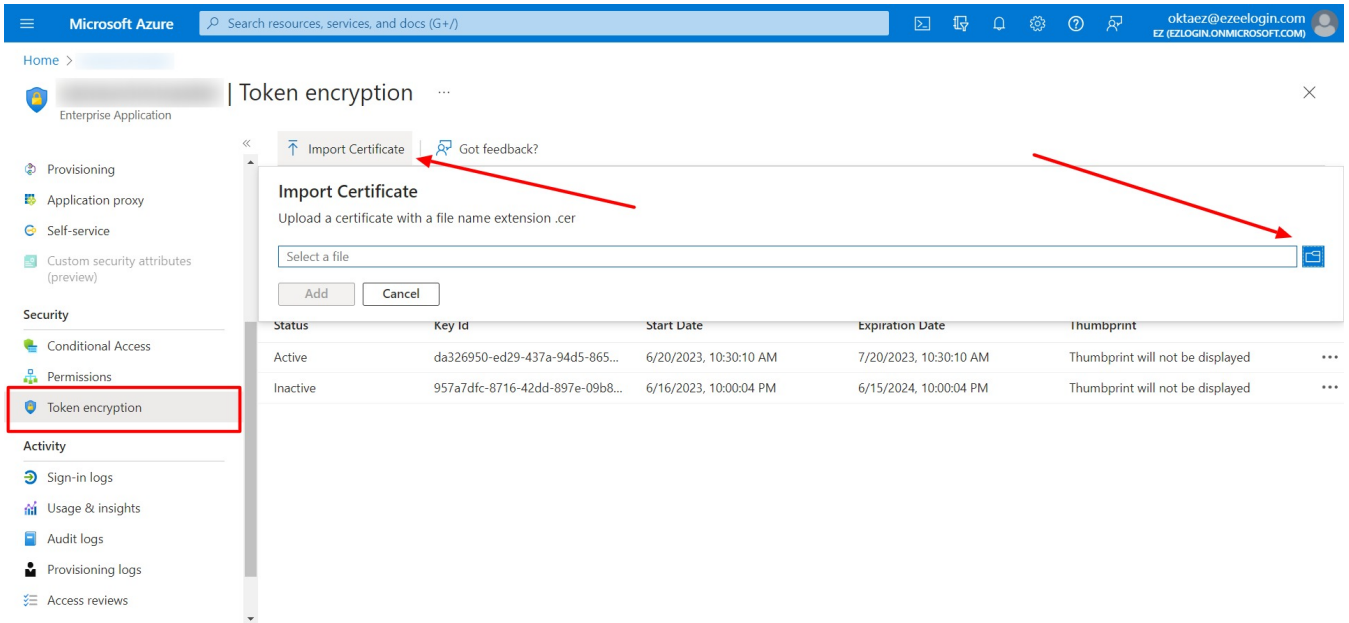
```
root@gateway:~# openssl x509 -req -in yourfile.csr -out yourfile.cer  
-signkey yourfile.key -days 365
```

EXAMPLE

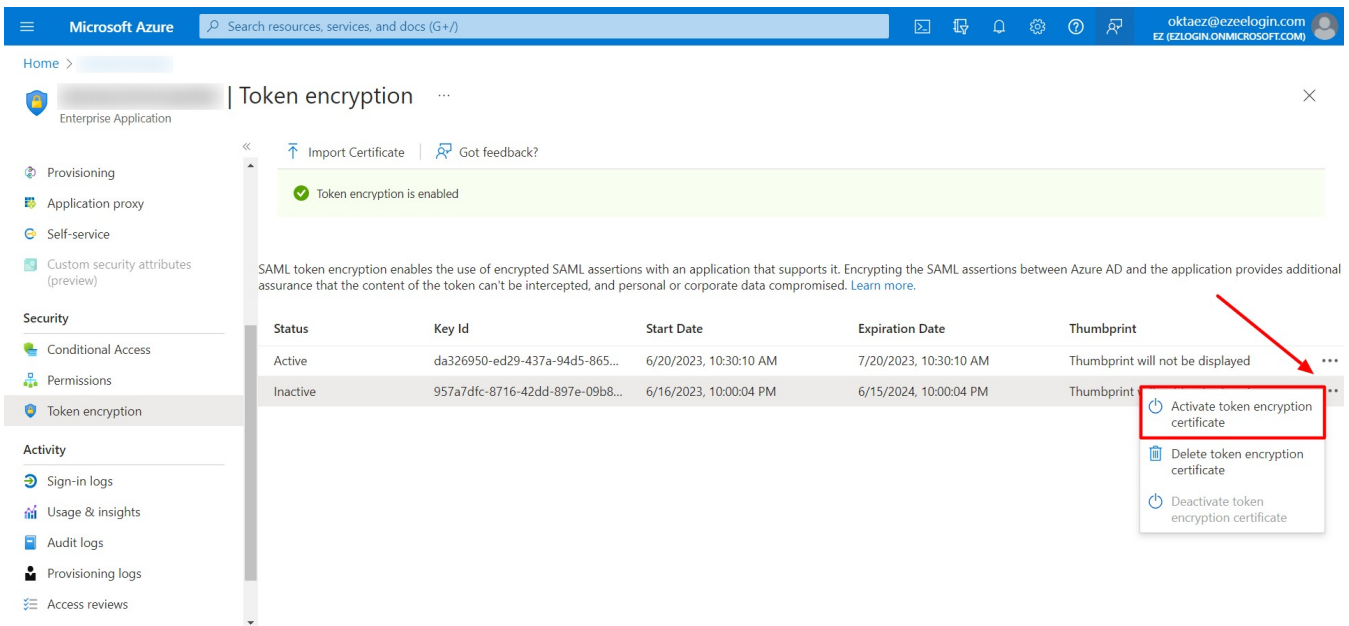
```
root@gateway:~# openssl x509 -req -in CSR.csr -out CSR.cer -signkey  
private_key.key -days 365
```

Step 4: Download the certificate to your PC.

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



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



Step 7: Add the certificate and private key to **Ezeelogin SAML advanced settings**.

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

The screenshot shows the Ezeelogin administration interface. On the left is a navigation menu with categories like Servers, Web Portals, Users, Access Control, and Settings. The main content area is divided into two sections: 'SAML Service Provider (SP) Info' and 'SAML Identity Provider (IdP) Settings'. The 'Advanced' sub-tab is active. Two green arrows point to the 'Service Provider Certificate' and 'Service Provider Private Key' fields, which contain Base64-encoded strings. Other settings include checkboxes for 'Strict', 'Compress Requests', 'Encrypted Name ID', etc., and text input fields for 'Name ID Format', 'Organization Display Name', and 'Signature Algorithm'.

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>