

Token encryption in Microsoft Azure SSO with Ezeelogin

617 Nesvin KN April 8, 2025 [Security Features](#) 1720

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.

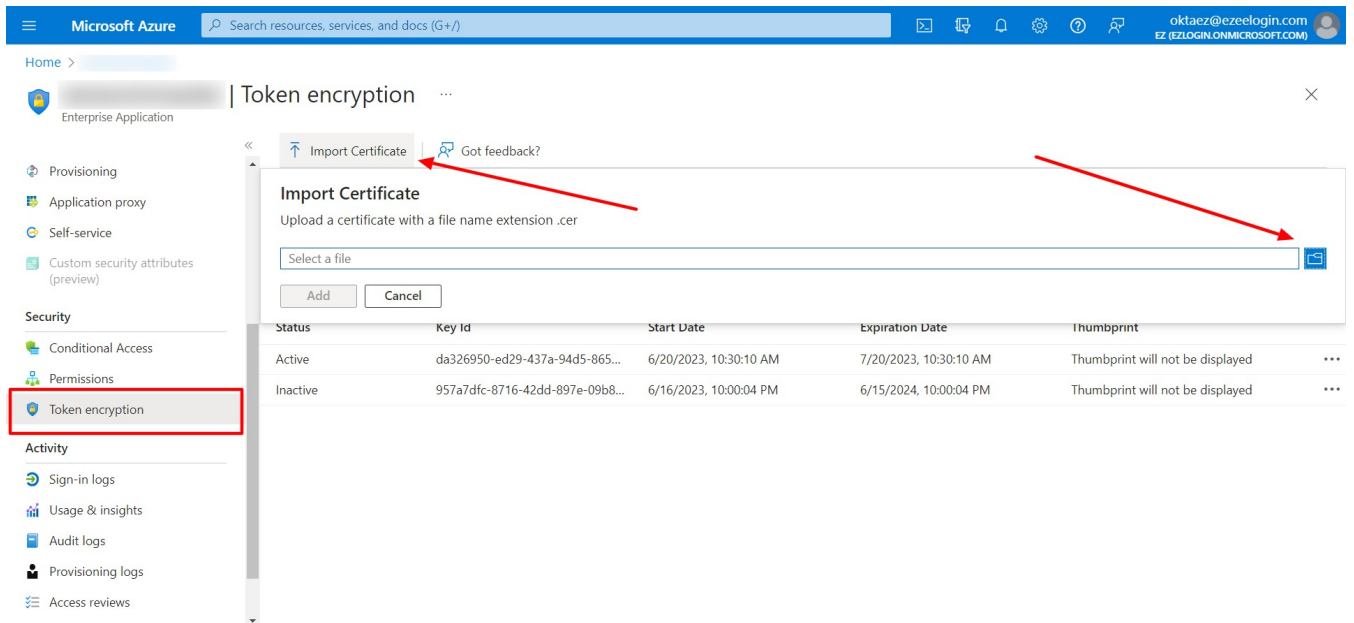
```
root@gateway:~# openssl x509 -req -in yourfile.csr -out yourfile.cer  
-signkey yourfile.key -days 365
```

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.

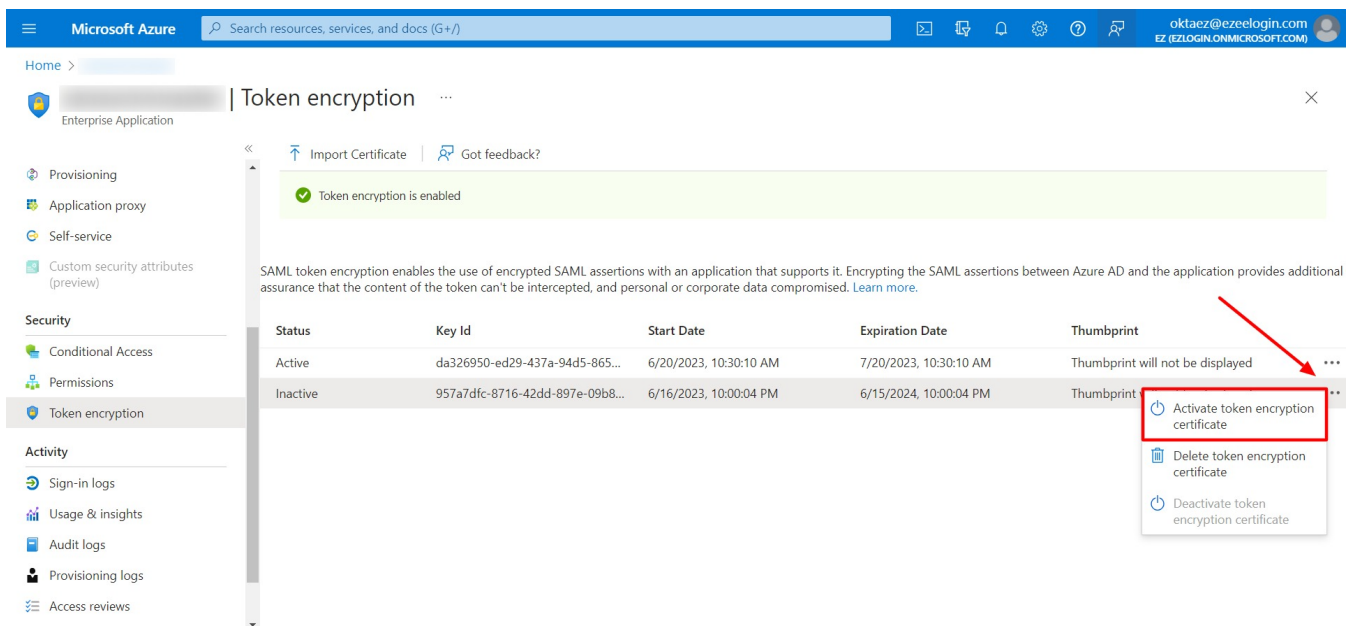
Step 5: Click on **Token encryption** on your **Enterprise application**. Click on **import certificate** and import the certificate file from your PC with the **.cer** extension.



The screenshot shows the 'Token encryption' page in the Azure portal. On the left sidebar, 'Token encryption' is highlighted with a red box. In the main content area, the 'Import Certificate' button is highlighted with a red arrow. Below this, a table displays the status of the encryption certificates.

Status	Key Id	Start Date	Expiration Date	Thumbprint
Active	da326950-ed29-437a-94d5-865...	6/20/2023, 10:30:10 AM	7/20/2023, 10:30:10 AM	Thumbprint will not be displayed
Inactive	957a7dfc-8716-42dd-897e-09b8...	6/16/2023, 10:00:04 PM	6/15/2024, 10:00:04 PM	Thumbprint will not be displayed

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



The screenshot shows the 'Token encryption' page with a green banner stating 'Token encryption is enabled'. Below this, a table lists the status of the encryption certificates. For the 'Inactive' certificate, a dropdown menu is open, and the 'Activate token encryption certificate' option is highlighted with a red arrow.

Status	Key Id	Start Date	Expiration Date	Thumbprint
Active	da326950-ed29-437a-94d5-865...	6/20/2023, 10:30:10 AM	7/20/2023, 10:30:10 AM	Thumbprint will not be displayed
Inactive	957a7dfc-8716-42dd-897e-09b8...	6/16/2023, 10:00:04 PM	6/15/2024, 10:00:04 PM	Thumbprint will not be displayed

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 sidebar with navigation options: Servers, Web Portals, Users, Access Control, Settings (selected), Cluster, Command Guard, Account, Help, and License. The 'Settings' section is expanded, showing various configuration options. The 'SAML Identity Provider (IdP) Settings' section is active, and the 'Advanced' tab is selected. This tab contains numerous checkboxes for SAML configuration, such as 'Strict', 'Compress Requests', 'Encrypted Name ID', 'Sign Logout Requests', 'Sign Metadata', 'Want Encrypted Assertions', 'Want Signed Assertions', 'Relax Destination Validation', 'Reject Unsolicited Responses with InResponseTo', 'Name ID Format', 'Organization Display Name', 'Technical Contact Name', 'Support Contact Name', 'Signature Algorithm', 'Service Provider Certificate', 'New Service Provider Certificate', 'Debug', 'Compressed Responses', 'Sign Authentication Requests', 'Signed Logout Responses', 'Want Signed Messages', 'Want Encrypted Name ID', 'Want XML Validation', 'Match Destination Strictly', 'Lowercase URL Encoding', 'Organization Name', 'Organization URL', 'Technical Contact Email', 'Support Contact Email', 'Digest Algorithm', and 'Allow Internal Authentication'. Two green arrows are drawn on the image: one points to the 'Strict' checkbox, and the other points to the 'Service Provider Private Key' text area, which contains a long string of characters.

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>