

Token encryption in Microsoft Azure SSO with Ezeelogin

617 Nesvin KN June 20, 2023 [Security Features](#) 1346

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**.

Microsoft Azure | Search resources, services, and docs (G+)

Enterprise Application | Token encryption

Import Certificate

Upload a certificate with a file name extension .cer

Select a file

Add Cancel

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

Security

- Conditional Access
- Permissions
- Token encryption**

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

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

Microsoft Azure | Search resources, services, and docs (G+)

Enterprise Application | Token encryption

Token encryption is enabled

SAML token encryption enables the use of encrypted SAML assertions with an application that supports it. Encrypting the SAML assertions between Azure AD and the application provides additional assurance that the content of the token can't be intercepted, and personal or corporate data compromised. [Learn more.](#)

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

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Activate token encryption certificate

Delete token encryption certificate

Deactivate 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**.

The screenshot displays the Ezeelogin administration console. 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 highlight 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', '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'.

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>