

# Cisco Secure Access - SAML Certificate Renewal with IDP(Microsoft Entra ID)

## Contents

---

---

## Issue

When using SSO authentication with Microsoft Entra ID SAML as the Identity Provider (IdP) for Cisco Secure Access, SAML verification certificates are approaching expiration.

Organizations need to understand the correct certificate renewal process to avoid authentication interruptions and determine whether a new Single sign on configuration must be created in Secure Access when renewing Entra ID SAML certificates.

## Environment

- Cisco Secure Access with SSO authentication configured
- Microsoft Entra ID SAML as Identity Provider
- SAML verification certificates with upcoming expiration dates
- Existing SSO configuration for SWG (Secure Web Gateway) and ZTNA (Zero Trust Network Access)

## Resolution

### Step 1 – Detect Certificate Renewal

- Identity Provider (IdP) renews or rotates its **SAML signing certificate**.
- This typically happens when the certificate approaches expiration.

### Step 2 – Obtain Updated IdP Metadata

- Export the **new IdP metadata XML** or **new signing certificate** from the IdP.

### **Step 3 – Verify Certificate Change**

Confirm the certificate has actually changed.

Check:

- **Thumbprint**
- **Expiration date**
- **Issuer**

This ensures the SP is updated with the correct certificate

### **Update Service Provider Configuration**

Login to the Cisco Secure Access Dashboard and update the Configuration.

Navigate to Connect - User and Groups.

Click Configuration Management

Under SSO Authentication - Edit the SSO Authentication Profile - either upload the Metadata file using new Certificate or upload the Certificate if manual configuration.

### **Step 5 – Save and Apply Configuration**

- Save the updated configuration

### **Step 6 – Validate SSO Authentication**

Perform an SSO login test.

## **Cause**

Identity Provider (IdP) signing certificate is used by the Service Provider to verify the SAML assertion signature, and when the IdP renews the certificate, the SP must update its trusted certificate to continue validating authentication requests

## Related Content

- Cisco Secure Access – SAML Single Sign-On Overview and Configuration
- Configure SAML SSO for Cisco Secure Access (Microsoft Entra ID example)
- [Cisco Technical Support & Downloads](#)