# Configuring SAML SSO with OperationsCommander (OPSCOM)

> The Configuring SAML SSO with OPSCOM feature simplifies user access by allowing them to securely authenticate using their existing, managed corporate accounts. Its primary purpose is to eliminate the need for separate usernames and passwords, significantly enhancing user convenience and overall system security through automated synchronization. This article is intended for OPSCOM administrators.

## Setup and Configuration

Implementing Security Assertion Markup Language (SAML) requires coordination between your organization's Identity Provider (IdP) and OPSCOM as the Service Provider (SP).

> Single Sign-On (SSO) is a premium paid feature. You must have the setup and recurring fees negotiated with your Sales Representative before proceeding. You must also configure your baseline login sources prior to completing this setup.

**Admin Side:**

### Configuring the Login Source

1. Hover over **System Configuration**, hover over **Users**, and click **Login Sources**.

2. Click the pencil icon to edit your previously created SSO login source.
3. Fill out the Service Provider and Identity Provider fields detailed below.
4. Click the **Save Changes** button to reveal the required configuration tabs.

## Service Provider Fields (OPSCOM)

These fields define exactly how OPSCOM will interact with your Identity Provider.

- **Unique ID:** This required field is a crucial part of the XML communication. It is supplied by your SAML system and is the exact value OPSCOM uses to match against its internal unique identifier.
- **Entity ID for Service Provider:** This required value defines the unique SAML integration path. Supply only the specific entity ID name, not the entire URL.
- **SP x509 Certificate:** This optional certificate is used to sign or decrypt SAML messages. Configure this field only if you are enabling signed logout requests or encrypted assertions.
- **Private Key:** This field is only required if the SP certificate above is actively in use.

## Identity Provider Fields (External SAML)

You must input values from your external SAML system's metadata into OPSCOM. This typically includes the Identity Provider's **Entity ID**, **Single Sign-On URL**, and **IdP x509 Certificate**.

> The **IdP x509 Certificate** field must contain the specific certificate issued by your Identity Provider (e.g., the certificate embedded in Azure's

> Federation Metadata). Do not copy the OPSCOM SP certificate into this field. Entering the wrong certificate will cause validation to silently fail.

### Synchronization Tab Configuration

1. Click the **Synchronization** tab.
2. Enable the **Auto Create/Update User** checkbox to allow the system to automatically create or update user profiles upon their first SAML login.
3. Map the user attributes from your SSO system directly to the corresponding fields in OPSCOM (e.g., mapping your IdP's "email" attribute to the OPSCOM email field).
4. Click the **Save Changes** button.

> Do not rename your Login Source after users have been associated with it. The Login Source value is permanently stored against every user record created via SSO. Changing it will immediately lock out those users on their next attempt.

### Translations Tab Configuration

1. Click the **Translations** tab.
2. Customize the text displayed on the login button for the user portal to ensure the experience is localized for your specific audiences.

**User Side:** End-users do not interact with the SAML setup. Once configured, they simply navigate to the User Portal and click the newly customized login button to seamlessly authenticate with their corporate credentials.

## Using this Feature

Administrators interact with this feature primarily by establishing the initial metadata handshake and monitoring the system for synchronization errors.

## Exchanging Metadata

To establish the connection, you must provide your Identity Provider with the OPSCOM Service Provider metadata.

1. Click the **Metadata** tab to view your system's XML code and integration URL.
2. Copy the live metadata URL (e.g., `https://[your-domain]/auth/saml2/[ENTITY_ID]/metadata`).
3. Provide this live URL directly to your Identity Provider.

> We strongly recommend providing your Identity Provider with the live URL rather than a downloaded, static XML file. When an IdP pulls from a live URL, it automatically fetches fresh metadata, ensuring the integration stays current and bypasses strict expiration timestamps.

## Troubleshooting Synchronization

If users encounter issues logging in, administrators should review the following common causes:

- **User not found:** Verify that the **Unique ID** field in OPSCOM perfectly matches the attribute name being sent by the IdP.
- **Assertion validation failure:** Check the **IdP x509 Certificate** field to ensure it contains the correct external certificate, not the OPSCOM SP certificate.

- **InvalidNameIDPolicy error:** Disable the **Require Name ID Policy** setting within the login source configuration (this is highly common with Microsoft ADFS integrations).
- **Incorrect auto-created data:** Use your IdP's debug tool to confirm the exact claim names in the assertion, and adjust your **Synchronization** tab mapping to match.

---

## Best Practices and Considerations

- **Coordinate with IT administrators: Successful SSO implementation requires close collaboration with your organization's IT department or the administrator of your SAML Identity Provider.** They must provide the necessary metadata and accurate attribute names.
- **Keep your certificates separated: Never enter the SP certificate in the IdP certificate field, or vice versa.** The SP certificate is generated by OPSCOM, while the IdP certificate comes from your external Identity Provider's metadata. Treating them as identical will break the integration.
- **Map Azure AD attributes carefully: Azure AD does not send a combined "full name" attribute by default.** If using Azure, always map the First Name and Last Name to completely separate attributes (e.g., givenname and surname) to prevent the entire display name from being stuffed into a single field.
- **Use true unique identifiers: Ensure the Unique Identifier chosen for matching users is truly unique and persistent within your SSO system.** Incorrect or changing identifiers will rapidly lead to

duplicate accounts or widespread login failures.



Revision #24
Created 21 May 2024 11:20:41
Updated 5 November 2026 13:45:29