Configuring SAML SSO with OPS-COM

What is Single Sign-On (SSO)

Single Sign-On (SSO) simplifies user access to OPS-COM by allowing them to authenticate using their existing, managed corporate accounts. This eliminates the need for separate OPS-COM usernames and passwords, enhancing convenience and security. This article details the setup and configuration of SAML-based SSO with OPS-COM, explaining the necessary fields, metadata exchange, and user synchronization. For more general information about SSO and OPS-COM refer to this wiki article.

Prerequisites and Considerations

Implementing SSO with OPS-COM, specifically using SAML (Security Assertion Markup Language), requires coordination between your organization's Identity Provider (IdP) and OPS-COM as the Service Provider (SP).

- **Paid Feature**: SSO is a paid feature. You must have the setup fee and recurring fees negotiated before proceeding. Contact your Sales Representative or email support@ops-com.com to initiate this.
- > **Login Sources**: You must first follow the instructions to set up Login Sources within OPS-COM, as SSO will be configured as a specific login source.
- **User Management Strategy**: Consider the following:
  - Will you have different Login Sources (e.g., Students/Staff use SSO, but Public Users do not)?
  - Will login sources vary by user type?
  - How do you want to initially get your users into OPS-COM (e.g., pre-import vs. on-the-fly creation)?
  - Do you want users to be created automatically upon their first SSO login?
  - Do you want to keep user information synchronized with your Identity Provider regularly, or will it be a one-time import?

- What user profile data/fields do you want synchronized between your SSO system and OPS-COM?
- Can you take advantage of the UserPush APIs for proactive user synchronization?

Your OPS-COM Client Success team will be happy to discuss these options to ensure a smooth and successful setup.

Once the prerequisites are addressed, the SAML setup involves configuring fields for both OPS-COM (as the Service Provider) and your external SAML system (as the Identity Provider).

Configuring SAML Setup

1. Hover over System Configuration, Users, and click Login Sources.
2. Click the pencil icon to edit your login source you created already as mentioned above. You should already have configured the login source to the point of the Unique ID field.

> The settings below must be filled out correctly and saved before you will see the Metadata tab to continue.

Service Provider Fields (Configured in OPS-COM)

These fields define how OPS-COM will interact with your Identity Provider.

- **Unique ID**: **Required** - This is a crucial part of the XML communication between OPS-COM and your SAML system. It is *supplied by your SAML system* and is the value OPS-COM uses to match against its internal `UniqueID` field to identify a user.
- **Entity ID for Service Provider**: **Required** - This value defines the unique SAML integration path within the URL in the metadata. If your OPS-COM system has more than one SAML integration, each `Entity ID` needs to be unique. The value you supply will appear in the integration path like this: https://client.ops-com.com/auth/saml2/ENTITY_ID_FIELD/acs. ***Only add the ENTITY_ID_FIELD not the whole URL.***
- **x509 Certificate**: (Optional) This certificate is provided by your Identity Provider (IdP) and can be generated and added to the Service Provider (OPS-COM) for secure communication.
- Private Key: (Optional)

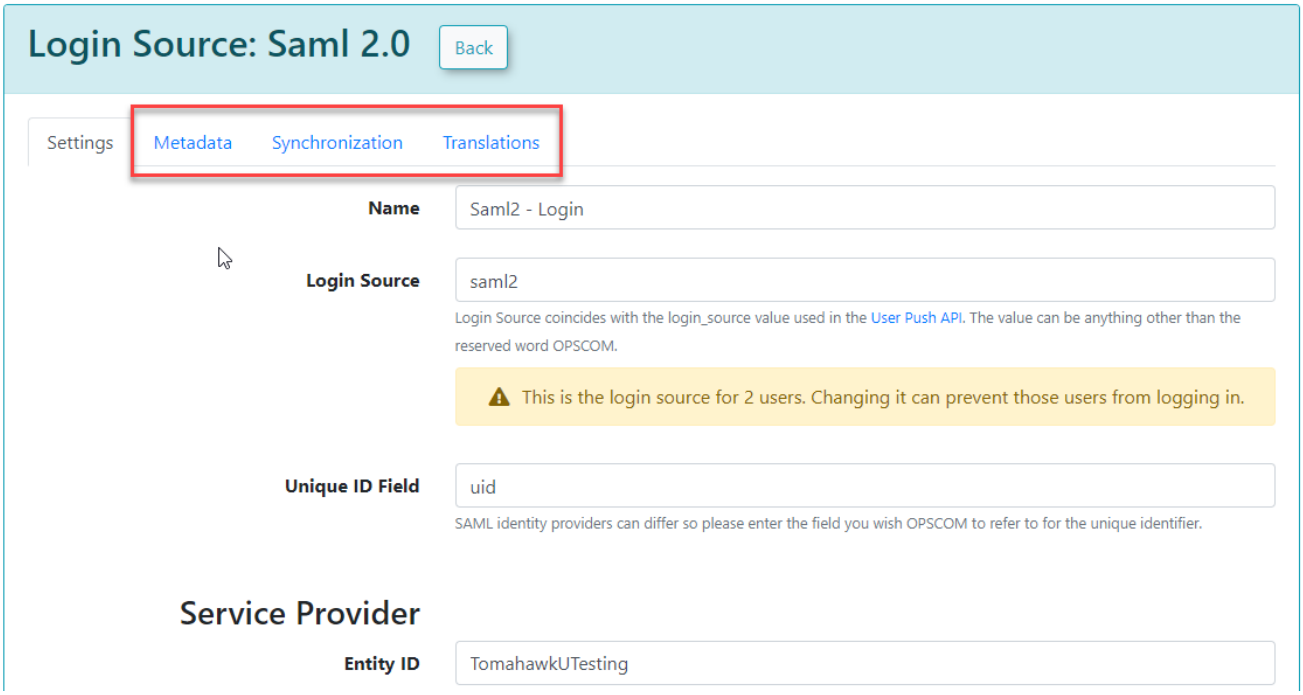
Identity Provider Fields (Configured in OPS-COM, Values from Your SAML System):

These fields capture information from your external SAML system (Identity Provider). You will find these values within your SAML system's metadata (e.g., often displayed under `Federation → Show Metadata` on your SAML installation page).

- You will input values such as the Identity Provider's `Entity ID`, `Single Sign-On URL (SSO URL)`, and `x509 Certificate` (which is often different from the one provided for the Service Provider).

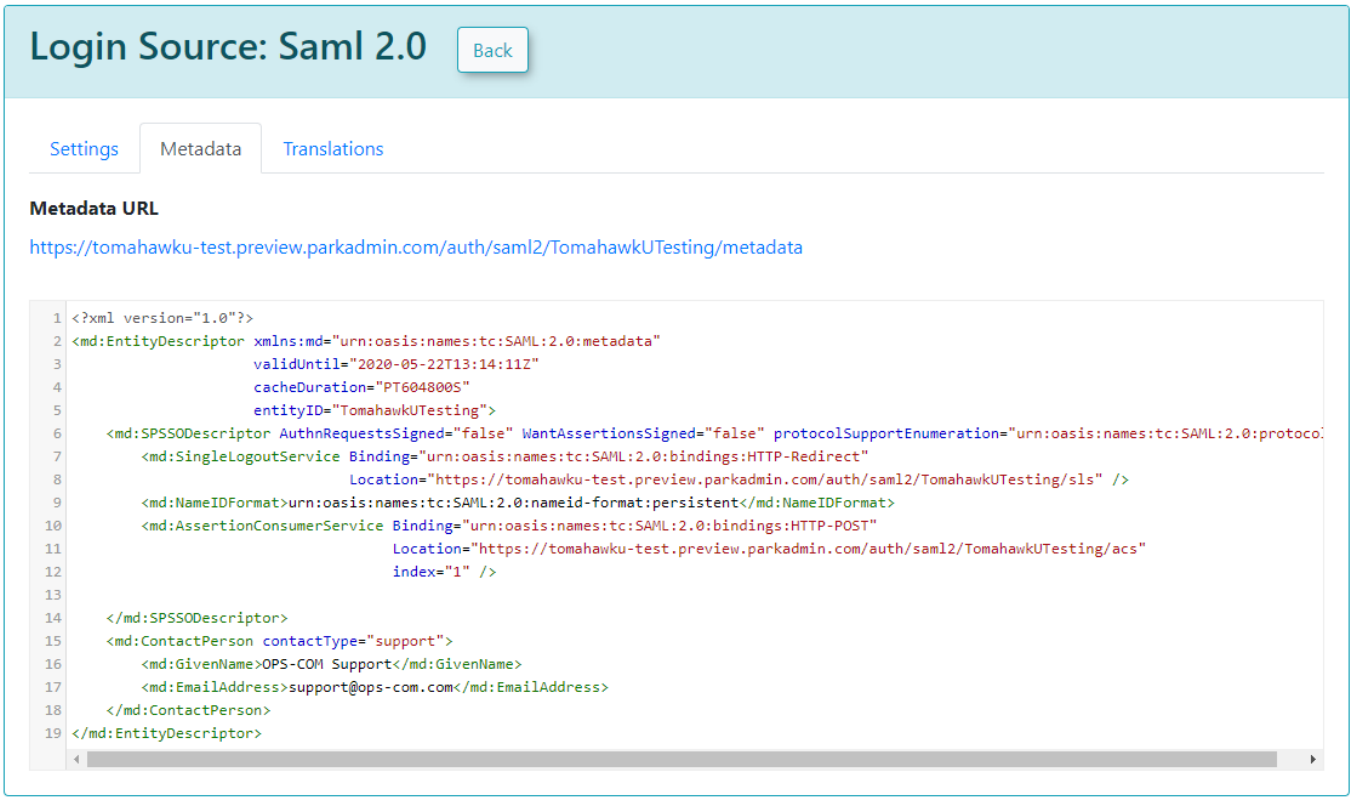
Once these settings have been completed and saved in OPS-COM, you will gain access to additional tabs: ***MetaData****,* ***Synchronization****, and* ***Translations****.*

Using this Feature



Metadata Tab

The **Metadata** tab in OPS-COM provides the XML code that you will need to provide to your Service Provider (OPS-COM, in the context of SAML communication from your IdP's perspective). This XML contains all the necessary information for your Identity Provider to communicate correctly with OPS-COM.



Sample XML File

Sample XML File Explanation: When your external system (e.g., a SimpleSAMLPhp service set up as the identity provider) sends a response back to OPS-COM, it includes an `saml:AttributeStatement` tag containing several attributes. These attributes are required for OPS-COM to match to a user within its system. The most important field in this attribute section is the value used as the permanently unique identifier for a user. For example, if the XML response shows `[uid] => Array ( [0] => 6ddf4027-3397-4e45-8628-0189f60fe91e )`, then `uid` should be entered as the **Unique ID Field** in your **Identity Provider Fields** configuration within OPS-COM. If the unique ID is something else, such as `SAMaccountName`, then that should be used instead.

... DEV-2K8 - DEBUG: Saml2 Incoming User Array ([uid] => Array ([0] => 6ddf4027-3397-4e45-8628-0189f60fe91e) [full name] => Array ([0] => Sarah Knowles) [email] => Array ([0] => sknowles@tomahawk.ca)) []

```
<? xml version = "1.0" ?>
    < samlp:Response xmlns:samlp = "urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml =
"urn:oasis:names:tc:SAML:2.0:assertion" ID = "_aa1963115aa6490e728c7376f4c8849813bbb..." >
        ...
        < saml:Assertion xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance" xmlns:xs =
"http://www.w3.org/2001/XMLSchema" ID = "_9efd79bf6425983ee9176f3d33a99d1a9176180..." >
            ...
            < saml:Subject >
                < saml:NameID SPNameQualifier = "MinionOpsComStaff" Format = "urn:oasis:names:tc:SAML:2.0:nameid-
format:transient" >_7a426e0be71f14c1f349db00d7d543b6f7dcb52baa</ saml:NameID >
                < saml:SubjectConfirmation Method = "urn:oasis:names:tc:SAML:2.0:cm:bearer" >
                    < saml:SubjectConfirmationData NotOnOrAfter = "2021-08-24T16:00:41Z" Recipient = "https://minion-
3.dev.parkadmin.com/auth/saml2/MinionOpsComStaff/acs" InResponseTo = "ONELOGIN_bb8a09203c888cf59af4c621a71cfa8f7559c016"
/>
                </ saml:SubjectConfirmation >
            </ saml:Subject >
            < saml:Conditions NotBefore = "2021-08-24T15:55:11Z" NotOnOrAfter = "2021-08-24T16:00:41Z" >
                < saml:AudienceRestriction >
                    < saml:Audience >MinionOpsComStaff</ saml:Audience >
                </ saml:AudienceRestriction >
            </ saml:Conditions >
            < saml:AuthnStatement AuthnInstant = "2021-08-24T15:34:46Z" SessionNotOnOrAfter = "2021-08-24T23:34:46Z"
SessionIndex = "_a7a68666092117d24aab8adecf1b0830622855b85..." >
                < saml:AuthnContext >
                    < saml:AuthnContextClassRef >urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</
saml:AuthnContextClassRef >
                </ saml:AuthnContext >
            </ saml:AuthnStatement >


            < saml:AttributeStatement >
                < saml:Attribute Name = "uid" NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:basic" >
                    < saml:AttributeValue xsi:type = "xs:string" >6ddf4027-3397-4e45-8628-0189f60fe91e</ saml:AttributeValue >
                </ saml:Attribute >
                < saml:Attribute Name = "full name" NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:basic" >
                    < saml:AttributeValue xsi:type = "xs:string" >Sarah Knowles</ saml:AttributeValue >
                </ saml:Attribute >
                < saml:Attribute Name = "email" NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:basic" >
                    < saml:AttributeValue xsi:type = "xs:string" >sknowles@tomahawk.ca</ saml:AttributeValue >
                </ saml:Attribute >
            </ saml:AttributeStatement >


        </ saml:Assertion >
    </ samlp:Response >
```

Synchronization Tab

The **Synchronization** tab allows you to configure how user information is managed between your SSO system and OPS-COM.

- **Auto Create/Update User**: To begin, ensure you enable the **Auto Create/Update User** checkbox. This feature allows OPS-COM to automatically create new user profiles when they first log in via SAML, if they don't already exist in OPS-COM. It also enables the system to update existing user information.

- **User Attribute Mapping**: On this tab, you will map the user attributes from your SSO system (your Identity Provider) to the corresponding fields in OPS-COM. For example, your SSO system might send "full name" and "email" attributes, which you would map to OPS-COM's `firstName`, `lastName`, and `email` fields.
- Any field that is mapped and has a value from your SSO side should get updated to the value from SAML.

After you have provided the information in each field, click **Save Changes**.

Your users will then begin to be created or updated automatically upon their SSO login attempts. If any of the supplied fields are incorrect or don't match, the corresponding information will be blank in OPS-COM when the user logs in, or it will remain unchanged if the user already existed.

Login Source: Saml 2.0

Back

Settings | Metadata | Synchronization | Translations

✔ Auto Create/Update User

Field Mapping

Map the attributes from the Identity Provider to this service provider. In the example below, address_city and first_name are attributes supplied by the Identity Provider. OPS-COM will know to map that to the internal field name.

```
<saml:AttributeStatement>
    <saml:Attribute Name="first_name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">John</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="last_name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">Smith</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="address_city" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">Borden</saml:AttributeValue>
    </saml:Attribute>
    ...
```

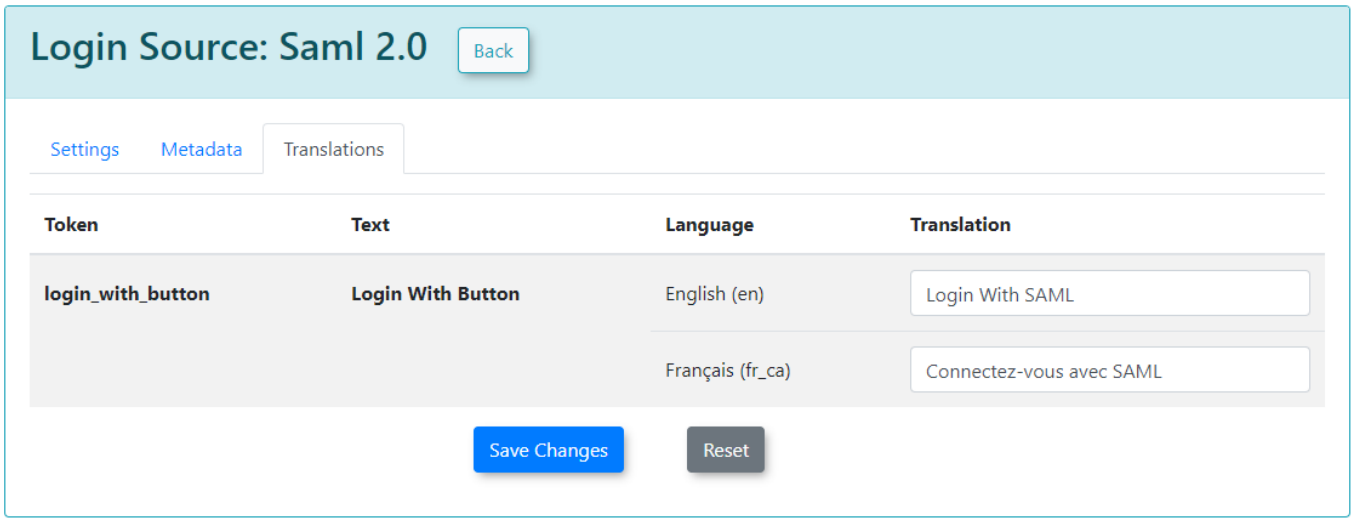
Enabled	enabled
User Type	user_type
First Name	full name
Middle Name	
Last Name	
Username	username
Email Address	email
Address	address_street
City	address_city
Province	address_province
Postal Code	address_postal
Phone Number	phone
profile.student_number	student_number
Employee Number	employee_number
Employer	employer
Building	building
Supervisor Name	supervisor_name
Supervisor Title	supervisor_title

Save Changes Reset

> The exact sample values from our test system may differ from your actual SAML system attributes.

Translations Tab

The **Translations** tab allows you to customize the text displayed on your login button from the user side. You can create as many different translations as are available in your system (e.g., English and French). This ensures that the SSO login experience is localized for your users.



Best Practices & Considerations

- **Coordinate with IT/SAML Administrator**: Successful SSO implementation requires close collaboration with your organization's IT department or the administrator of your SAML Identity Provider. They will provide the necessary metadata and attribute names.
- **Unique User Identifiers**: Ensure the **Unique Identifier** chosen for matching users is truly unique and persistent within your SSO system. Incorrect or changing identifiers will lead to duplicate accounts or login failures.
- **Attribute Mapping Accuracy**: Carefully map all desired user attributes from your Identity Provider to OPS-COM. Inaccurate mapping will result in missing or incorrect user data.
- **Test Thoroughly**: After initial configuration, conduct thorough testing with various user types and scenarios to ensure seamless login, proper user creation/updates, and correct data synchronization.
- **User Experience**: Clearly communicate the new SSO login process to your users. Provide instructions on how to access OPS-COM via SSO and address any potential questions.
- **Error Handling**: Be prepared to troubleshoot potential issues. Common problems include incorrect Entity IDs, expired certificates, or mismatched attribute names. The SSO system logs can be invaluable for diagnosing such issues.

Revision #15
Created 21 May 2024 11:20:41
Updated 17 July 2025 09:08:14 by Shannon Jones