

Login Sources (SSO)

Login Sources define the various methods by which users can sign into the system. This feature provides administrators with flexible control over user authentication, allowing for standard OPSCOM logins or integration with external identity providers like SAML or LDAP, enhancing convenience and security for diverse user populations.

Setup & Configuration

Login sources are managed under the **System Configuration** menu, within the **Users** section.

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

Default Login Source

- **OPSCOM** is the default login source. This means that, by default, users will log in directly to OPSCOM using a username and password created within the system itself on the standard login screen.
- If you **disable** the **OPSCOM** default login source, then only other configured login sources, such as SAML or LDAP, will be active for user logins.

Adding Login Sources

OPSCOM supports multiple login sources, allowing some users to utilize SSO while others log in directly.

1. On the **Login Sources** page, click the **Add Login Source** button.
2. Fill out the required information:
 - **Red fields** are **required** to be filled before you can click **Save**.
 - **Yellow fields** are technically required for the login source to function correctly, but they will still allow empty or invalid values to be saved initially. **Yellow fields** can also indicate that a change has been made to the field.

The **Login Source - Code** field is crucial as it's what the user profile will match against when associating users with this new login source. However, **only one login source code can be activated at a time** for a particular type (e.g., you can have multiple SAML configurations, but only one primary 'SAML' code active for user matching at a time if the system differentiates by 'type' of code rather than unique code string across all). The source name (code) itself is typically determined by your Identity Provider, with the exception of 'OPSCOM' for direct logins.

3. **Name** can be anything that is identifiable to you.
 4. **Login Source** is what you will see on the user profile to indicate if this user will login with a special source. Often is is called SSO or SAML
 5. **Domain Name for OPSCOM to use** should be set to the OPSCOM domain without any references to admin etc. For example, if the domain name you login looks like CLIENTID.admin.OPSCOM.com/admin, this should be changed to **CLIENTID.OPSCOM.com only**.
 6. Do not fill out the rest of the fields until you are ready to **[follow the instruction for setting up your SSO information](#)**.
 7. Click **Save Changes** to add the new login source.
-

Using this Feature

Once login sources are added, you can manage their status and properties.

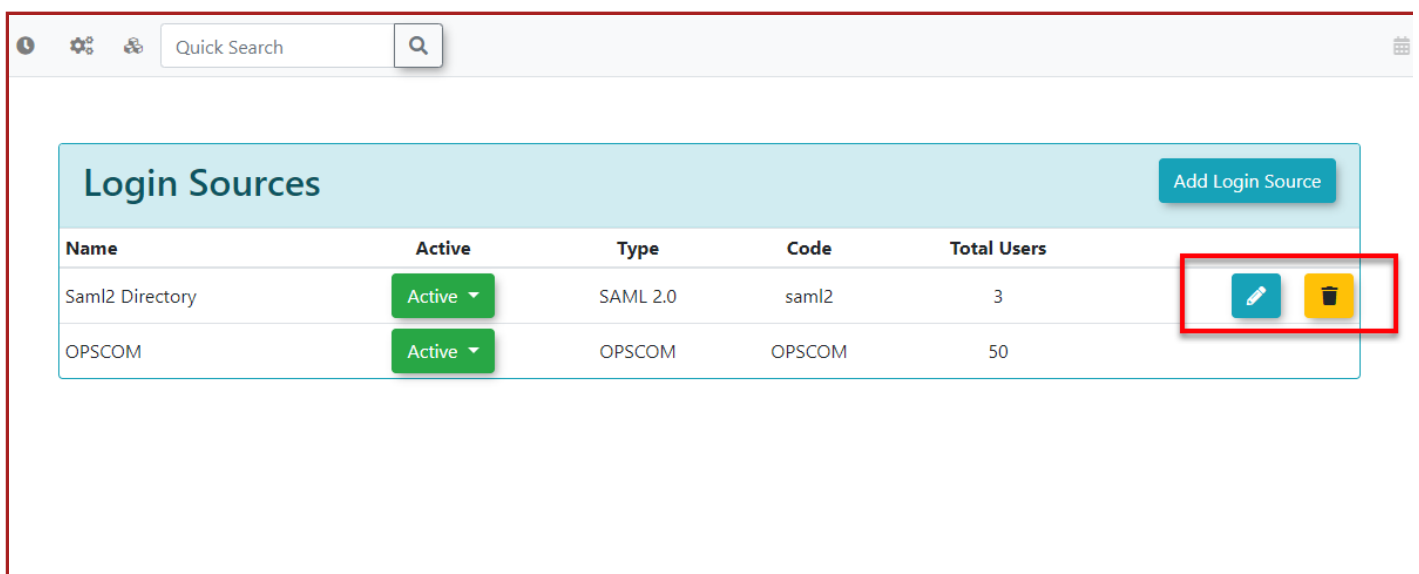
Managing Login Sources

From the **Login Sources** page, you can manage your configured login sources using the buttons next to each entry:

- Click **Edit** to modify an existing login source's details. This will bring up the same form used for adding, allowing you to update its configuration.
- Click **Delete** to permanently remove a login source from the list. A confirmation pop-up will usually appear before deletion.

Active/Inactive/Hidden Login Sources

You can make Login Sources **Active, Inactive or Hidden**. If a source is made **Inactive**, users who were previously connected will no longer be able to login and must be changed to a different login source.



The screenshot displays the 'Login Sources' management page. At the top, there is a 'Quick Search' bar and an 'Add Login Source' button. Below this is a table with the following data:

Name	Active	Type	Code	Total Users
Saml2 Directory	Active ▾	SAML 2.0	saml2	3
OPSCOM	Active ▾	OPSCOM	OPSCOM	50

Next to the 'Saml2 Directory' row, there are two icons: a blue pencil icon (Edit) and a yellow trash can icon (Delete). These icons are highlighted with a red box.

Best Practices & Considerations

- **Strategic Planning for Multiple Sources:** Carefully plan your login source strategy. Determine which user groups will use which login method (e.g., students via SAML, staff via LDAP, public users via OPSCOM direct login).
- **User Provisioning:** Consider how users will be created and linked to their login sources. Will they be auto-created on first login, or pre-imported? This linkage uses the **Login Source - Code** field.
- **Disabling Default OPSCOM:** If you intend for *all* users to access via an external SSO, ensure you disable the **OPSCOM** default login source. Test thoroughly before making this change in a live environment.
- **Testing New Sources:** Always thoroughly test any new login source after configuration to ensure users can successfully authenticate and access the system.
- **Communication with Users:** Clearly communicate to your users how they are expected to log in, especially if you introduce new SSO options or change existing methods. Provide clear instructions and links.
- **Inactive vs. Deleting:** Use the **Inactive** function for temporary deactivation or if you foresee needing to reactivate a login source in the future. Use **Delete** only when a login source is permanently no longer needed and has no associated active users.