Login Sources (SSO)

> The Login Sources SSO feature allows administrators to define the various methods by which users authenticate and sign into the system. Its primary purpose is to provide flexible control over user access, allowing for standard direct logins or integration with external identity providers like SAML or LDAP to enhance convenience and security. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing system access and user authentication.

Setup and Configuration

This feature is a core administrative tool used to manage how different user populations access the portal.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the configuration menus and manage SSO integrations.

User Side: Users will interact with the configured login sources when accessing the portal. If a Single Sign-On (SSO) source is enforced, they will automatically be redirected to their institution's secure login page before accessing the system.

Using this Feature

Administrators can use the following instructions to manage the default login source, add new external identity providers, and modify existing authentication methods.

Managing the Default Login Source

OPSCOM is the default login source for the system. This means that, by default, users will log in directly to the portal using a standard username and password created within the system itself.

If you disable the OPSCOM default login source, then only your other configured login sources, such as SAML or LDAP, will be active. Users will be forced to authenticate through those external providers.

Adding Login Sources

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

1. Hover over **System Configuration** and click **Users** then **Login Sources**.
2. Click the **Add Login Source** button.
3. Enter a descriptive label into the **Name** field.
4. Enter the display identifier into the **Login Source** field. This is what you will see on the user profile to indicate if the user logs in with a special source (e.g., SSO or SAML).
5. Enter the root domain into the **Domain Name for OPSCOM to use** field. This must be the domain without any references to the admin portal (for example, use *CLIENTID.ops-com.com* instead of *CLIENTID.admin.ops-com.com/admin*).

6. Define the **Login Source - Code** field. This is a crucial identifier that the user profile will match against when associating users with this new login source.
7. Complete the remaining SSO fields when you are ready to apply the specific setup instructions provided by your Identity Provider.
8. Click the **Save Changes** button to add the new login source.

> When filling out the configuration form, fields highlighted in red are strictly required before you can save. Fields highlighted in yellow are technically required for the login source to function correctly, but the system will temporarily allow empty or invalid values to be saved initially. Yellow fields can also indicate that an unsaved change has been made to that specific field.

Available Actions and Buttons

From the main management page, you can manage your configured login sources using the following actions:

- **Edit:** Click this button to modify an existing login source's details. This will bring up the configuration form, allowing you to update its connection properties.
- **Delete:** Click this button to permanently remove a login source from the system.
- **Status Drop-down:** Select a status of Active, Inactive, or Hidden for any login source. If a source is made inactive, users who were previously connected to it will no longer be able to log in and must be manually migrated to a different login source.

Best Practices and Considerations

- **Strategically plan for multiple sources: Carefully plan your login source strategy before implementation.** Determine exactly which user groups will use which login method (e.g., students via SAML, staff via LDAP, and public users via direct login).
- **Manage user provisioning: Consider how users will be created and linked to their login sources.** Decide whether profiles will be auto-created upon their first successful SSO login or if they must be pre-imported. This linkage strictly relies on the exact string match of the **Login Source - Code** field.
- **Test before disabling direct logins: If you intend for all users to access the system via an external SSO, thoroughly test the integration before disabling the default OPSCOM login source in a live environment.**
- **Deactivate instead of deleting: Use the inactive status for temporary deactivation or if you foresee needing to reactivate a login source in the future.** Only use the **Delete** action when a login source is permanently retired and has absolutely no associated active users.
- **Communicate changes to users: Clearly communicate to your users how they are expected to log in.** If you introduce new SSO options or change existing methods, provide clear instructions and direct links on your portal homepage to prevent login confusion.

Revision #20
Created 21 May 2024 11:19:05
Updated 13 July 2026 14:02:26