

Release 5.73

Download the PDF of this article.

In this Article

[Login Method Enforcement on Instance Level](#)

[Highlights](#)

Related Articles

[Login Method Enforcement on Instance Level](#)

FormAssembly offers a feature where admins can configure SSO, SAML, LDAP, or FormAssembly login to be enforced instance-wide. This gives the admin control over their secure login options across all users in one place, reduces complexity and overhead for the admin, as well as makes it easier to control access and application security when users leave the organization.

This feature is available for Essentials and above Plans.

Highlights

- The permission to manage SAML has been moved from the Application Settings page to the Security Page in the Admin Dashboard. This means that all admins you expect to manage SSO will need the permission enabled on their user profile to manage security settings.
- The drop-down permission labeled “Authentication Type” has been renamed to “Instance Login Method” to be clearer and distinguish from the form authentication type settings, which could lead to confusion.
- We’ve introduced a new feature that gives you control over whether admins are required to use SSO exclusively or can override this setting to access the system using other credentials. This flexibility allows you to choose the best option for your organization.

Important note: If you configure the setting to enforce SSO for admins and experience an issue with your Identity Provider, all users, including admins, will be locked out of FormAssembly until the issue is resolved.

However, if you allow admins to override the SSO enforcement, they can still log in using FormAssembly credentials. This ensures admins can access FormAssembly, disable the enforcement setting, and manage critical processes while the Identity Provider issue is being addressed.
