

Using SSO (Single Sign-On)

Published on 10/25/2016

What is Single Sign-On?

Single Sign-On allows you to validate usernames and passwords against other client applications or a corporate database instead of managing permissions through inMotion. inMotion easily integrates with most popular SSO applications, including Federated Service Solutions that support SAML 1.1 or 2.0.

There are numerous benefits to integrating SSO with your inMotion account, including:

- **Security:** Your company's security policies for user passwords will also apply for inMotion user passwords. Access restrictions within your organization will also cascade to inMotion.
- **Easy Administration:** Users already authenticated in your company network will be able to seamlessly log in to inMotion. inMotion can also automatically create new users when they attempt to log in to the application through SSO.
- **Quick Information Access:** Messages from inMotion with links to reports and reviews will conveniently open automatically, without needing users to log in.

Federated Single Sign-On

The inMotion Federation environment consists of a development/staging and production environment. The development/staging environment is used for initial setup, with identity providers and user acceptance testing. After sufficient testing and when sign-off is received, applications will be set up within the inMotion production environment. Your identity provider solution will need to supply an identity provider metadata XML file. This file will need to be supplied to inMotion to initialize the trust relationship. A name and email address are required for SSO integration.

User Provisioning

inMotion allows for automatic provisioning of new users. When user provisioning is enabled for your account, a user will be inserted when there is no match for the supplied identifier. User provisioning requires an additional field mapping for a user's name. If no role is supplied for the newly provisioned user, the role will default to "Reviewer."

Review Link Exclusion

If review link exclusion is enabled in your inMotion SSO settings, any link supplied by inMotion for review will not require authentication through the identity provider. This feature allows reviewable content to be released to individuals outside your organization's user pool, while still relying on identity authorization for users working within the application. If content for review is only internal to your organization, it is recommended that this feature be disabled.