Configure Single Sign-On (SSO) for administrators

Overview

**Important:** Only a Druva Cloud Administrator can set up Single Sign-On.

By enabling Single Sign-On (SSO), administrators can access all Druva services without the need for a separate login. You should implement SSO for your inSync setup for the following reasons:

- **Reduced human errors:** SSO eliminates the need for remembering multiple passwords, thus reducing to a great extent, the possibility of human errors while accessing inSync resources.

- **Reduced administration efforts:** With single sign-on, inSync users and administrators logging in from their corporate network are rarely prompted for a username or password. With fewer passwords to manage, system administrators receive fewer requests to reset forgotten passwords.

- **Central management of user database:** Many organizations maintain a database of users. By enabling Single Sign-On for inSync, changes to this database also reflect on the inSync setup. This means that if you delete credentials from this database, users to whom these credentials were previously assigned cannot log in to inSync using the same credentials.

- **Reduced login time:** Typically, a user needs 5 to 20 seconds to log in to an online application. SSO eliminates the efforts required for a manual login thus increasing productivity.

- **Increased security:** The password policies enforced across your organization are applicable when you use SSO for inSync. The one-time authentication tokens used to validate SSO attempts translate to added security for users having access to sensitive data.

Refer [Configure Single Sign-On for inSync](https://docs.druva.com/Endpoints/050_Configure_inSync_Settings/Configure_inSync_for_Single_Sign-On_(SSO)/010_Config…) to configure and manage SSO for inSync.