A Password Policy is a set of rules that encourage the use of strong passwords for ensuring added data security. inSync supports password policies for the users and administrators. You can define a Password Policy such that:

- Strong passwords are mandated. A password is strong if it is at least 12 characters long and contains at least one alphabet [a-z, A-Z], one numeric character [0-9], and one special character.
- A given number of preceding passwords used to login cannot be reused
- The number of login attempts is defined. When this limit is reached, inSync locks the account for an hour.
- Mandate password change at regular intervals.

Enable Password Policy for administrators

Password Policy for administrators can be configured only from the Druva Cloud Platform Console. To enable Password Policy for administrators, see Configure Password Policy for administrators.