Access Control Overview

Last Modified on 03/18/2021 12:35 pm EDT

In order to help prevent unauthorized access to user accounts and information, SAP Open Connectors has implemented a number of information security procedures and best practices.

- SAP Open Connectors and best practices require that all access to any information systems containing sensitive and/or customer information, including our platform, use multi-factor authentication.
- Any user account that isn't used for 90 days will be disabled.
- After five failed attempts to sign in to a user account, the account will be disabled. A locked account will automatically reactivate after at least 30 minutes.
- Manager approval is required before access or privileges to SAP Open Connectors information processing systems can be granted.
- You are strictly prohibited from using shared or group accounts, or sharing credentials.
- Except for password resets, all changes to user accounts—including termination, creation, or privilege modification, must be approved by a superorg or org admin.
- For security, user passwords must include at least 10 characters, including at least 3 of the following 4 types of characters:
  - a lower-case letter
  - an upper-case letter
  - a number
  - a special character (such as !@#$%^&*) (no more than 2 identical characters in a row are allowed; eg 111)
  - Note: these password complexity requirements are enforced for existing users on March 15, 2021 for production environment accounts and March 18, 2021 for staging environment accounts. See Enhanced Password Security Requirements for additional details.

Best Practices for Users

We also recommend that your organization implement the following best practices:

- Because users are responsible for all actions performed using under the context of their identity, ensure that all users have their own respective, unique credential. Regardless of its form—a username, badge, or token—this credential must never be shared with any other person, regardless of whether or not they are also part of the same organization.
- Limit administrator privileges to the fewest staff possible to perform sensitive duties. For each person who has administrator rights to any part of the SAP Open Connectors platform, you must have documented justification for their inclusion.
- If a user is terminated, their access to the SAP Open Connectors platform should be immediately revoked.