Manage Security Settings

Last Modified on 09/13/2021 7:16 am EDT

Use the Security Settings page to manage organization information, reset your organization secret, configure passwords, and set up two-factor authentication. Only the organization administrator can access the Security page.

Minimum Password Length and Complexity

While not managed from the Security Settings page, it is required that user passwords include at least 10 characters, including at least 3 of the following 4 types of characters:

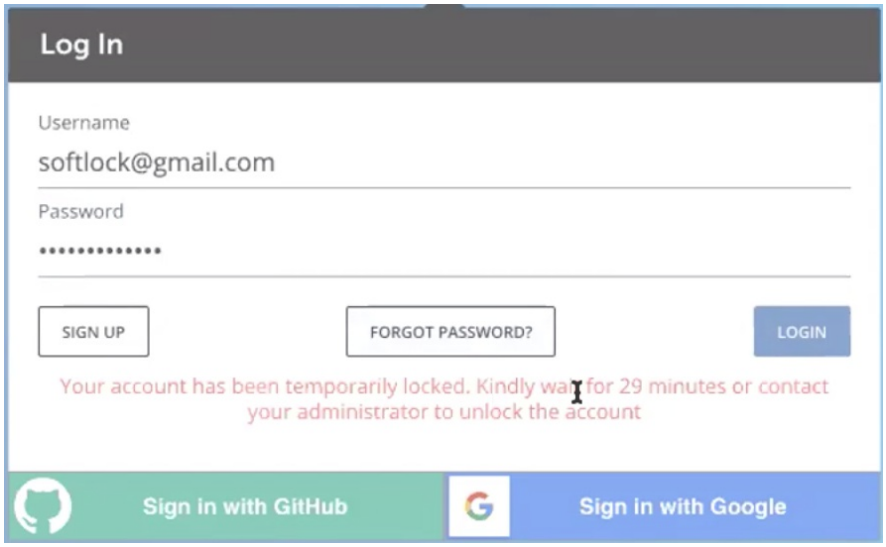
- a lower-case letter
- an upper-case letter
- a number
- a special character (such as !@#$%^&*) (Note: no more than 2 identical characters in a row are allowed; eg 111)

Note: the above 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.

Managing Account Lockouts

Note: the account lockout policies and procedure detailed here do not apply to SSO or SAML-based authentication.

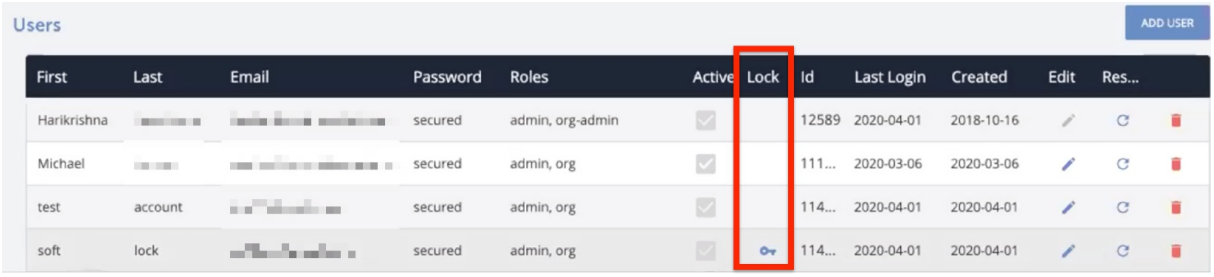
After five failed login attempts, user accounts are temporarily locked out for 30 minutes and credentials cannot be reset using the `Forgot Password?` button on the login screen. If no additional invalid login attempts are made, users can select `Forgot Password?` to reset after thirty minutes.



If three more failed login attempts occur on the locked account, the lockout must be removed their Org Admin.

If you are the Org Admin and need to unlock a user within your organization, follow these steps:

1. Access the Security page, and select the Accounts tab (see Accounts and Users for more information).
2. From the Users section of the Accounts tab, find the locked user as indicated by the Lock column.



3. Click the Edit icon, then click the key icon to unlock the user account.

Note: If an Org Admin user account is locked, the user must contact Customer Support.

Two-Factor Authentication

SAP Open Connectors supports two-factor authentication through SMS and Google Authenticator. Both methods require users to enter authentication codes after the successfully enter their user name and password. They can resend the code repeatedly, but if they enter the code incorrectly three times, SAP Open Connectors locks them out.

To set up two-factor authentication:

1. Access the Security page.

> Note: If you don't see Security, your assigned role does not have access to it.

2. In **Two-Factor Authentication** select a two-factor authentication method.
3. Click **Update**.

SMS

If you set up two-factor authentication with SMS, users receive an authentication code sent to their phone. After you set up two-factor authentication with SMS, the next time that users in your organization log in, they will be prompted to enter their phone number. The number entered must be able to receive texts. Users can resend the code as often as they want, but they'll get locked out for 24 hours if they enter an incorrect code three times.

Google Authenticator

Google Authenticator is an app that generates two-factor authentication codes. Before you set up two-factor authentication with Google Authenticator, make sure that your users have the Google Authenticator app for Android or iOS.

After you set up two-factor authentication with Google Authenticator, the next time that users in your organization log in, they will be prompted to scan a QR code with the Google Authenticator app. After scanning the code, the app displays an authentication code. After the first login, users just retrieve a new code from the app and do not need to scan another QR code.

Resetting Organization Token via UI

SAP Open Connectors requires the organization token — or organization secret — along with each individual user secret for every call to our Platform APIs like `/instances`, `/organizations`, or `/formulas`. You can reset your organization token, creating a new random string, at any time. Remember to update all of your API request headers to use the new organization token.

To reset an organization token via the UI:

1. Access the Security page.
2. In the **Profile** section, click **Reset Organization Token**, and then confirm.

Resetting Organization or User Token via API

To reset an organization token or user token via API, use the `POST /authentication/user-secret-reset` and `POST /authentication/organization-secret-reset` endpoints. Reseting these secrets takes effect immediately and the old ones no longer work.

> **Note**: You must have the 'Modify Security' privilege on their role in order to reset the organization secret.

Example:

```
curl -X POST \
  https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/authentication/user-secret-reset \
  -H 'authorization: User , Organization ' \
  -H 'content-type: application/json'
```

```
curl -X POST \
  https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/authentication/organization-secret-reset \
  -H 'authorization: User , Organization ' \
  -H 'content-type: application/json'
```

FAQ

Q: Is it possible to reset a Google Authenticator identifier so that a user can re-register?

Users cannot themselves reset Google authentication identifiers; contact support for a reset. Once support implements the reset, users can re-register on their next login.