Set Password Requirements

If you are using Apperian authentication rather than SSO (Single Sign On) to authenticate your users, administrators can enforce a stricter password policy in your Apperian organization. For more information, see Specify the Authentication Method.

These settings can be set differently for *administrators* (which includes developers and user administrators) and for regular *users*.

On This Page

Set Password Complexity

By default, a user's password must be at least five characters and contain no spaces. You can modify this default password complexity criteria for your organization to include the following specifications:

- Minimum password length
- Minimum number of upper case characters required
- Minimum number of lower case characters required
- Minimum number of numeric characters required
- Minimum number of special characters (symbols) required

Once these password requirements are set, all users in your organization must create passwords that meet the defined complexity criteria.

To configure password complexity criteria

1. Click **Settings** on the Admin Portal navigation bar.
2. Click **Password Requirements**.
3. Choose either the **Users** or **Administrators** tab.
4. Under **Password Complexity**, set your password complexity requirements.
5. Click **Save** at the bottom of the page.

Back to Top

Set Password Expiration

You can set a password expiration time period that forces users to reset their passwords after a specified number of days. When a user logs in to the App Catalog or Admin Portal after their password has expired they are prompted to set a new password.

A user's new password cannot be the same as the current password, and must also adhere to any password complexity criteria set for the organization. Once a new password is set, the user can log in normally. When the expiration time period has elapsed, the user must again reset their password.

To configure password expiration

1. Click **Settings** on the Admin Portal navigation bar.
2. Click **Password Requirements**.
3. Choose either the **Users** or **Administrators** tab.
4. Under **Password Expiration**, in **Password expiration time (in days)**, enter a value to define the password expiration time period after which users are forced to reset their passwords.
5. Click **Save** at the bottom of the page.

Back to Top

Set Password History

You can set password history requirements that prevent users from continually reusing the same passwords.

Enforce password history sets the number of unique new passwords that must be associated with a user before an old password can be reused. Minimum password age sets the amount of time (in hours) that must pass before users can create a new password.

Administrators can change a user's password at any time, regardless of how these settings are configured.

To configure password history

1. Click **Settings** on the Admin Portal navigation bar.
2. Click **Password Requirements**.

3. Choose either the **Users** or **Administrators** tab.
4. Under **Password History**, do the following:
    a. In **Enforce password history**, enter a value to define the number of unique passwords.
    b. In **Minimum password age (in hours)**, enter a value to define the number of hours that must pass before users can change their password.
5. Click **Save** at the bottom of the page.

Back to Top

Set Account Lockout Threshold

You can set the number of times a user can enter an incorrect password before their account is disabled (locked out). Once a user's account is disabled in this way, the user is prevented from logging in again until an administrator manually enables the user's account. Or, you can enable a temporary lockout, so the user can log in again after a specified amount of time.

Administrators can enable users at any time, but can't unlock their own account.

To configure account lockout

1. Click **Settings** on the Admin Portal navigation bar.
2. Click **Password Requirements**.
3. Choose either the **Users** or **Administrators** tab.
4. Under **Account Lockout**, in **Account lockout threshold**, enter a value to define the number of incorrect password attempts.
5. In **Reset account lockout timer after**, enter a value (in minutes) to specify the length of time until the account lockout timer resets.
6. Choose whether the account lockout will be **Permanent** or **Temporary**.
    a. If you select **Temporary lockout**, set a duration (in minutes).
7. Click **Save** at the bottom of the page.

Back to Top