PASSWORDS SECURITY SETTINGS

Form.com lets you set up security regulations and manage password settings.

Note: This option is available for white-labeled subscription types and customers who are self-hosted outside of our SaaS infrastructure.

Here are the available settings:

User passwords expire in

Manages the password validity term.

The supported options are:

- Never expires (Default)
- Expires in ... days (The value must be between 0 and 365)

Enforce password history

Determines the number of unique new passwords that must be associated with a user account before an old password can be reused.

The supported options are:

- Is not logged (Default)
- Remember ... passwords (The value must be between 0 and 10)

Password complexity requirement

Sets the password complexity requirements. Each option among listed below can be added or removed individually.

The supported options are:

- No restriction (Default)
- Must mix alpha and numeric (The password must contain at least one numeral and one letter)
- Must contain special characters (The password must contain one of the following non-alphabetic characters: !, ", #, $, %, &, ', (,), *, +, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~)

US: +1 781 849 8118 | UK: +44 (0) 1252 551 600

Minimum password length

Sets the minimum password length.

The supported options are:

- Not limited (Default)
- At least ... characters (The value must be between 0 and 16)

Account expiration requirement

Limits the term the account can stay idle.

The supported options are:

- Never expires (Default)
- Expires if idle for ... days (The value must be between 0 and 365)

Account lockout policy

Disables a user account if an incorrect password is entered a specified number of times over a specified period.

The supported options are:

- Do not lock accounts (by default)
- Lock accounts for ... minutes after ... invalid attempts (The value must be more than 0 minutes and between 1 and 10 attempts)

US: +1 781 849 8118 | UK: +44 (0) 1252 551 600