



Password Management

Configure Password Settings

As an administrator, you can determine how stringent the password policy for your organization's users should be.

1. Navigate to **Organization Admin** → **Password Settings**.
2. In the User Password Requirements section of this page, configure the following settings:
 - a. **Minimum character limit** – Enter the minimum number of characters a password must include. This value must be at least 8.
 - b. **Maximum character limit** – Enter the maximum number of characters a password can include. Leave this field blank to set no maximum.
 - c. **One or more uppercase letters** – Toggle this switch to **on** (green) to require that each user's password include at least one uppercase letter (A–Z).
 - d. **One or more lowercase letters** – Toggle this switch to **on** (green) to require that each user's password include at least one lowercase letter (a–z).
 - e. **One or more numbers** – Toggle this switch to **on** (green) to require that each user's password include at least one numeral (0–9).
 - f. **One or more symbols** – Toggle this switch to **on** (green) to require that each user's password include at least one non-alphanumeric character.

Note

There is no restriction on which characters a user can include in their password.

- g. **Re-use limit** – Enter the number of a user's most recent passwords that cannot be reused when setting a new password. For example, if this is set to 1, a user cannot reuse their previous password but could reuse the password prior to that. This value must be at least 1 but no more than 30.
 - h. **Reset period (days)** – Enter the number of days a user's password can be used before it expires and the user must change their password. This value must be at least 30 but no more than 180.
 - i. **Reset link expiration (minutes)** – Enter the number of minutes for which the link a user receives when attempting to reset their password remains valid. This value must be at least 15 but no more than 60.
 - j. **Disable native CRM login** – (This is only available in organizations using a single sign-on (SSO) login configuration.) Toggle this switch to **on** (green) to prevent users in your organization from logging in directly via totalexpert.net; in this case users can only access the system through their SSO provider.
 - k. **Enable Lockout** – Toggle this switch to **on** (green) to lock a user out of the system after a number of attempts specified by the Lockout Count field below. If a user exceeds the allowed number of incorrect attempts, they are prompted to reset their password.
 - i. **Lockout Count** – (This only appears when the Enable Lockout option is switched on.) enter the number of incorrect attempts allowed before a user is prompted to reset their password. For example, if this is set to , the user is allowed 1 incorrect attempt and would be locked out by a 2nd incorrect attempt. This value must be at least 1 but no more than 5.
3. Click the **Save** button in the upper-right corner of the User Password Requirements section.



(Admin) Reset Password for a User

As an administrator, you can reset the password for any user in your organization.

1. Navigate to **Organization Admin → Users**.
2. For the user whose password you want to reset, select **Actions → Edit**.
3. On the Account Settings tab, scroll down to locate the Reset Password section in the right column.
4. Click the **Send Email** button.
5. An email is automatically sent to the user's address with a temporary password.
6. The user should then navigate to <http://totalexpert.net> and log in using this password, then follow the instructions under Account Settings below to create a new permanent password.

Tip

Ensure that the user is ready to log in and change their password before triggering this email. The link expires and can no longer be used after the amount of time set in the Reset link expiration (minutes) field mentioned above.

(User) Reset Password

Note

If your organization is using single sign-on (SSO), check with your system administrator about how to change a password.

Forgot Password? Link

Any user can generate their own temporary password via the Total Expert login page.

1. Navigate to <http://totalexpert.net>.
2. Click the **Forgot Password?** link.
3. Enter the email address associated with your account and click the **Send Reset Email** button.
4. An email is automatically sent to the address you provided with a temporary password.
5. Return to <http://totalexpert.net> and log in using this password.
6. Follow the instructions under Account Settings below to create a new permanent password.

Tip

Ensure that you are ready to log in and change your password before triggering this email. The link expires and can no longer be used after an amount of time set by your administrator.

Account Settings

Any user can change their own password in the system at any time via their Account Settings page. When a user has a password generated and sent to them by email, they should immediately log in and change their password.

1. Navigate to **settings menu → Account Settings**.
2. Scroll down to locate the Update Password section in the right column.
 - On the right side of this section, there is a list indicating the required password parameters.
3. Enter your existing password in the **Current Password** field.



4. Enter whatever you want your new password to be in the **New Password** field. As you meet each requirement listed on the right, its icon turns to a green check mark. If any requirements are not met, you will not be able to save your changes.
5. Type the new password again in the **Confirm Password** field. If this entry does not match the New Password field, a notification appears below in red and you will not be able to save your changes.

Tip

Password characters are obscured as dots by default. Click the eye icon at the right end of each field to reveal the characters in plain text. Click the icon again to obscure the characters again.

6. Click the **Save Changes** button at the top of the page.