Password Management

Password options in Agiloft satisfy military-grade security requirements and can be made as strict or lenient as you require. Users are often granted access to change their own passwords, but the default settings only allow admin users to change other users' passwords.

Creating secure passwords is very important. For passwords to be resistant to attack and malicious users, they should adhere to several guidelines:

- Be at least 8 characters in length
- Contain a mixture of upper and lowercase characters
- Contain one or more numbers or other non-alphabetic characters
- Not be derived in any obvious way from the username

All power user accounts should be secured with such passwords, especially those in the Admin group. If you wish to give end user accounts simple passwords for their convenience, then these users should be severely restricted in their permissions. For example, you might only allow them access to a single record form to complete. If you allow end users to modify existing records or view sensitive data, they should be given secure, attack-resistant passwords.

For the most secure passwords, we recommend requiring a minimum password length of 12–14 characters with at least one uppercase, one lowercase, one numeric, and one symbolic character.

Password Field Wizard

The Password Field wizard is used for creating new Password fields and editing existing Password fields. To work with Password fields for a table, navigate to the Fields tab of the Table wizard and select **New > Password**, or edit an existing Password field.

The wizard is very similar to other Field wizards, with General, Options, Permissions, and Display tabs. Only the Options tab contains unique settings, which determine the password requirements mentioned above, as well as additional options that improve password security:

- Preventing the login and password from being the same value and a password from containing the login string
- Requiring users to change their password if it is reset
- Invalidating passwords or locking an account after a number of failed login attempts
- Controlling password reuse
- Controlling password expiration time
- Adding password encryption
- Requiring confirmation of new passwords
- Excluding dictionary words from passwords

Password Fields and Subtables

Password fields, like other data types, allow for different settings on different subtables. For instance, the out-of-the-box KB has Employees and External Users subtables on the People table. If only employees log in to the system, it's reasonable to make the Password field required on the Employees subtable but not the External Users subtable.

In other cases, you may want to require longer and stricter passwords for employees and let end users create passwords with fewer characters and requirements. Although this option provides useful flexibility, every unique password configuration requires additional future maintenance.

Changing Passwords

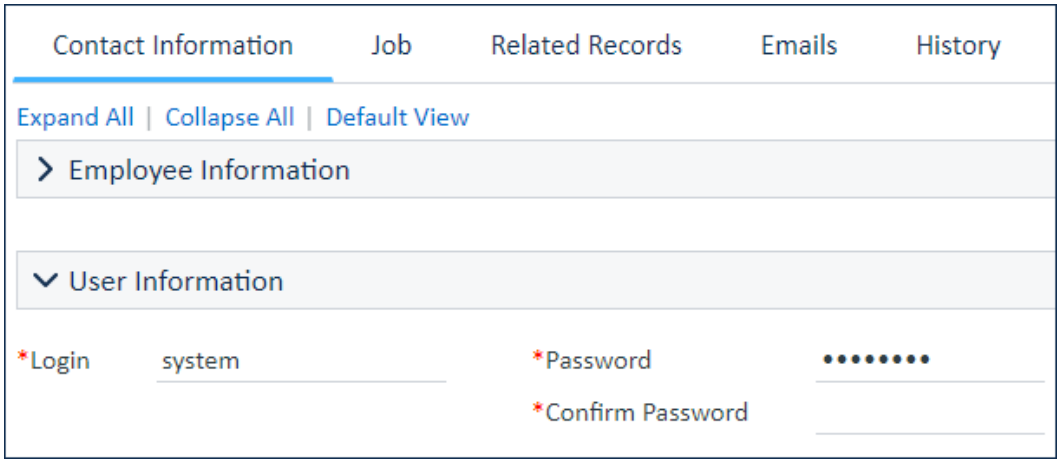
By default, only admin users are able to change other users' passwords. Admin users are also able to change the password of the admin console for on-premise installations.

Non-admin users are able to manage their own passwords once they have logged in to the system. For more information on this process, see Change Passwords.

Changing Other Users' Passwords

In some cases, admins may want or need to change the passwords for other users in the system. Use the following steps to change another user's password:

1. In the nav bar, select the People table.
2. Edit a user's record.
3. On the Contact Information tab, enter the new password in the fields and click Finish.



Password fields in a Person record

Changing Many Users' Passwords

You might occasionally need to provide a temporary password to many users at once. You can automate the process of sharing logins and temporary passwords for users in the People table.

1. First, go to Setup Employees and edit the Password field. Set this field to require the user to edit their password on their next login.
2. Go to Setup People and create a new Text field:
    - Name the field Temporary Password.
    - Set the default value to: random_password(15)
    - In the Permissions tab, allow all groups to see this field in their own Person record, but allow only the admin group to edit the field and to see the field in other users' Person records.
3. In the People table, select all records and click Edit or Mass Edit in the action bar. Select the Temporary Password field and set it to: random_password(15)
4. Return to the People table and this time, select the users who need to receive their login credentials. Click Email > Send Email in the action bar, and compose a message:
    - Expand the To section and select Email Fields, then select the Email field.
    - Compose an email explaining that the recipient will need their login credentials to use hotlinks going forward. In the body, include or add $_login and $temporary_password to include the credentials.
5. Send the email. This sends individual emails to everyone you selected, so they receive their logins and temporary passwords. When they log in for the first time, they will be prompted to change their password.

> If you usually use an automated process to create user accounts, you can automate these steps with rules in the People table to make sure new users receive logins and temporary passwords.

Changing the Admin Console Password

All on-premise installations are given the same default admin console password, so it's critical to change the password during the initial installation:

1. Log in to the admin console.
2. On the left pane, click People.
3. Edit the admin user record and click Change Password.
4. Enter the existing and new password, and then click Save.
5. Save the admin user record.

Sample User Passwords

Each out-of-the-box knowledgebase is automatically populated with a number of sample users. Sample users are given easy-to-remember and therefore insecure passwords by default. These passwords should be changed if you plan to keep these user records. You can also simply delete the sample users, with some exceptions.

Three users are essential for certain functionalities and should never be deleted: anonymous, register, and guest. The system also contains four admin-level users that should be given highly secure passwords:
admin, busadmin, ewsystem, and system.