

# Two-Factor Authentication

---

Two-Factor Authentication (2FA) requires users to verify their identity using both a password and a code sent to their mobile device in addition to their password. It provides an added layer of security, particularly for users with extensive permissions such as knowledgebase administrators.

## Prerequisites

---

For users who will sign in with two-factor authentication, the Cell Phone field in their user record must contain a validly formatted number. Non-US phone numbers must be preceded by "+" and the country code. For US numbers, the country code (+1) is optional.

The system ignores spaces, hyphens, and parentheses in the phone number. The following formats are all accepted:

- US Numbers:
  - 555-111-2222
  - 5551112222
  - 1 (555) 111 2222
  - +15551112222
  
- International Numbers:
  - +382 5555555555
  - +91 5555-5555
  - +7 012 345 6789

## Enabling Two-Factor Authentication

---

You can enable two-factor authentication from a knowledgebase or the admin console. Admin console access is only available for on-premise customers who maintain their own Agiloft server.

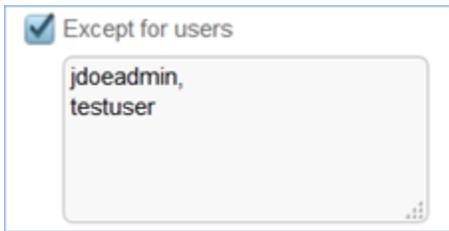
1. To enable 2FA:

- In a specific knowledgebase, log in as an admin and go to **Setup > Access > Two Factor Authentication**.
- In the admin console, log in and go to **General > Settings** and click **Two Factor Authentication**.

 If you don't see Two Factor Authentication, you likely need to upgrade to a later Agiloft release.

2. Select the checkbox Require two factor authentication.

3. You can optionally Exclude groups or Exclude users from two-factor authentication. For instance, you might allow users with low permission levels to log in with only a password, while admin-level users must provide two forms of authentication. When excluding specific users from 2FA, enter the user's Login. Use a comma to separate multiple logins.



The screenshot shows a configuration window with a checked checkbox labeled "Except for users". Below the checkbox is a text input field containing the usernames "jdoeadmin," and "testuser" on separate lines. The input field has a light gray background and rounded corners.

4. Choose whether two-factor authentication is required For every login, or only For the first login from a particular device.
5. Optionally, choose an expiration period after which users must reauthenticate.
6. Choose an authentication method, either standard SMS or the Google Authenticator app. If Google Authenticator is chosen, users must download the app to their smart device and create an account before receiving verification codes.

 Two-factor authentication uses cookies, which are both browser and device-specific. Logging in from a different device, a different browser on the same device, or after clearing cookies from the browser cache will prompt the user for reauthentication.

Google Authenticator is compatible with Android, BlackBerry, and iOS devices.

## Signing in with Two-Factor Authentication

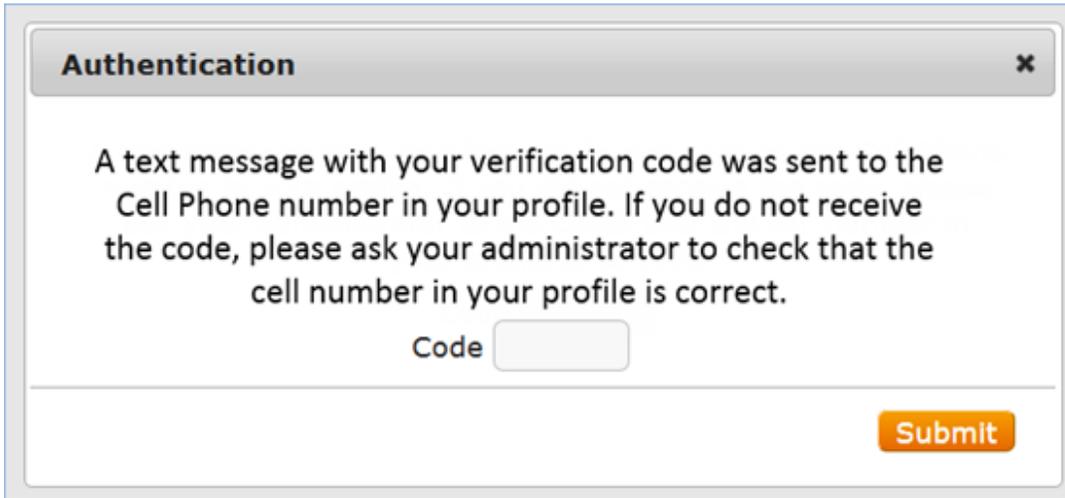
---

When 2FA is set up in your system, you'll use it when you log in.

### Text Message (SMS)

1. Navigate to the login page for your Agiloft knowledgebase.
2. Enter your username and password and click Log In.

3. A verification code is sent to your cell phone number on record. Enter the code in the pop-up window when prompted:



**Authentication** ✕

A text message with your verification code was sent to the Cell Phone number in your profile. If you do not receive the code, please ask your administrator to check that the cell number in your profile is correct.

Code

**Submit**

4. Click Submit. You will be logged in to your Agiloft knowledgebase.

## Google Authenticator

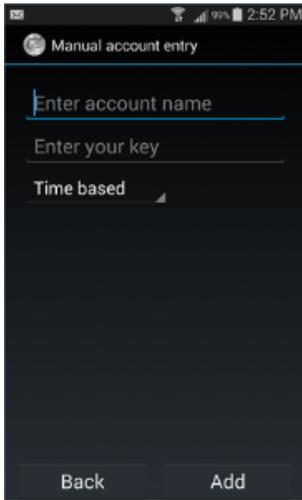
You can use the Google authenticator app instead of SMS. For an example of setting up and using Google Authenticator, see [2-Step Verification with Google Authenticator](#).

### First time setup

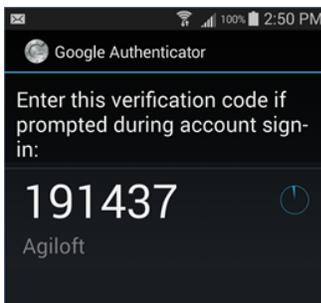
---

1. Navigate to the login page for your Agiloft knowledgebase. Enter your credentials and click Log In.
2. When the pop-up dialog appears, click Send Secret Key to send the 16-digit key to your cell phone.
3. On your mobile phone, go to the Play Store or App Store and search for Google Authenticator to find, download, and install the app.
4. Open the Google Authenticator app.
5. From the menu, select Set up account, then select Enter provided key.

6. Enter an account name for this knowledgebase. Enter the secret key sent to your mobile device via text message in step 2. Click Add.



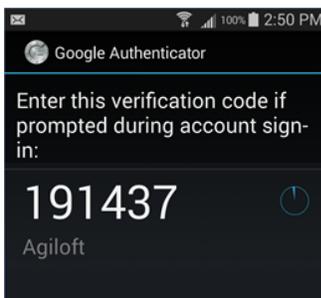
7. The verification codes now appear when you open the account in the app. The code changes every 60 seconds.



## Logging in

---

1. Navigate to the login page for your Agiloft knowledgebase.
2. Enter your username and password and click Log In. A pop-up dialog appears.
3. Open the Google Authenticator app on your smart device to retrieve the current 6-digit verification code.

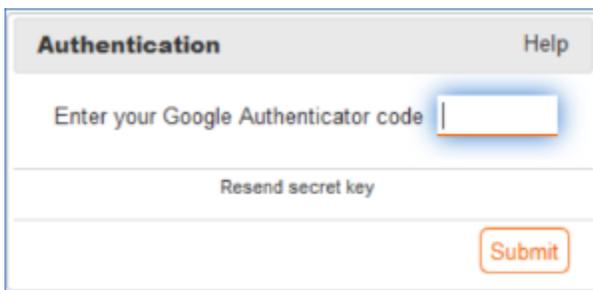


4. Return to the browser. Enter the code in the pop-up dialog and click Submit. You will be logged in to your Agiloft knowledgebase.

## Resend the secret key

---

If you lose your secret key, such as when reinstalling the app or changing your device, use the authentication pop-up dialog option to Resend secret key. The key is sent to your email address or to your cellphone by SMS, depending on the method defined by the administrator. The option to resend the key only appears once you have entered your login and password.



The image shows a dialog box titled "Authentication" with a "Help" link in the top right corner. Below the title bar, there is a text input field with the placeholder text "Enter your Google Authenticator code". Below the input field, there is a link labeled "Resend secret key". At the bottom right of the dialog, there is a "Submit" button.