2-step authentication for Single Touch Payroll

2-step authentication is a method to secure online accounts. Single Touch Payroll uses 2-step authentication to verify your identity before submitting data to the ATO. It requires you to *know* something, a password, and *possess* something, an authentication code created by an app installed on your mobile device, to log in.

The benefit of this approach is that even if someone guesses your password, they also need to be in possession of your mobile device to break into your account.

Related resources

Learn how to set up 2-step authentication for Single Touch Payroll (2.15 mins video)

Set up 2-step authentication with Google Authenticator

You will need your iOS or Android device to complete these steps.

To set up 2-step authentication:

1. Install the Google Authenticator app on your iOS or Android device.
2. Open the app and allow it to access your camera.
3. Tap plus **+** (iOS) or *Begin Setup* (Android).
4. Tap *Scan a barcode*.
5. Scan the QR code displayed on your **Single Touch Payroll** screen. If you can't scan the QR code, type the key in to the Google Authenticator app.
6. Enter the 6-digit verification code displayed in the app and click **Verify**.

You now have 2-step authentication set up on your mobile device to securely access Single Touch Payroll.

Use 2-step authentication with Single Touch Payroll

To use 2-step authentication:

- Open Google Authenticator on the device where it is set up.
- Enter the 6-digit code in the **Google Authenticator Code** field on the Single Touch Payroll screen and click **Verify**.

Note: The 6-digit verification code updates every 30 seconds and is valid for two minutes. If the time expires, return to your device to get an updated code.

Change your authentication device

If you need to verify using a different device, ask your organisation administrator to cancel your existing 2-step authentication so you can set up another device.

Cancel 2-step authentication

An organisation administrator can cancel an existing 2-step authentication for an employee.

To cancel an employee's 2-step authentication:

1. Log in to Attaché Online and select your organisation.
2. Select the **Employees** menu.
3. Find the employee who requested the cancellation by typing the employee's name in the search field.
4. Click the employee's name.
5. From the **Actions** drop-down menu, select **Cancel 2-step authentication**.
6. Review the on-screen information and click **Yes**.

The employee will receive an email confirming the cancellation. The employee can then set up a different device via the **Single Touch Payroll** menu.

2-step authentication frequently asked questions

If you don't have a smartphone install a Google Authenticator extension for use with the Chrome browser, such as Authy Chrome Extension. Once installed, the Google Authenticator icon displays on the Chrome toolbar. Click the icon to scan the QR code. It also displays your 6-digit google verification code.

Another option is to use an open-source authenticator for Windows, such as WinAuth.

If you are having trouble scanning the barcode, manually enter the key on your device.

1. In Google Authenticator, tap **+**.
2. Ensure that *Time-based* is selected as the key type.
3. In *Account*, type your full email address.
4. In *Key* (or *Your key*), type the key displayed on the Single Touch Payroll screen.
5. Tap **Done**/**ADD**.

Google Authenticator displays the 6-digit verification code.

If your Google Authenticator codes are not working, check that the time is synced correctly in the app:

1. Go to the Google Authenticator main menu.
2. Click **Settings**.
3. Click **Time correction for codes**.
4. Click **Sync now**.
5. The app displays a message confirming the time has been synced. The sync only affects Google Authenticator, your device's date and time settings remain unchanged.

You should now be able to use your verification code to sign in to Single Touch Payroll.

You must have an internet connection to use 2-step authentication. If your internet connection is not available you will not be able to log in to your Attaché Online *organisation* to enter the verification code.

If your mobile device is lost or stolen change your password immediately via My Profile in Attaché Online.

We recommend your organisation administrator cancels your 2-step authentication from your account.

You can set up Google Authenticator to generate verification codes from more than one device.

1. Install Google Authenticator on **all** devices you wish to use.
2. Follow directions as usual to set up 2-step authentication for the mobile app, ensuring to either scan the generated QR code for **all** devices at the same time or enter the generated secret key on **all** devices.
3. Check to ensure all devices are working correctly by entering the verification codes from each device and clicking **Verify**.