



Multi-Factor Authentication User Guide

1) Overview

Multi-factor authentication (MFA) also known as 2-step verification (2SV) or two-factor authentication (2FA) is a security measure that requires users to provide more than one verification factor to gain access to a service/application. MFA is a core component of a strong identity and access management policy. Rather than just requesting that a user provide a username and password, additional factors are required which decrease the risk of unauthorised users gaining access to sensitive personal data.

Traditional usernames and passwords are vulnerable to brute force attacks and such information is susceptible to be obtained by malicious third parties. Should an attacker gain access to a service using valid credentials, this would grant the attacker the same permissions as the legitimate user and there would be no way to identify the difference between the malicious access and legitimate access. For any system which uses passwords for authentication, there will always be a chance that users and administrators will select machine-guessable passwords or be victims of phishing attacks and thus be susceptible to infiltration by malicious third parties.

Multi-Factor Authentication serves as an effective defence against these third-party attacks and ensures personal data is protected using the strongest available means.

The EmploymentCheck MFA solution requires users to provide the additional authentication factor each time they log on to access the service.

2) Process

There are two MFA methods in use on EmploymentCheck; using a certified third-party iOS/Android authentication app to register a device and generate a One-Time Passcode (OTP) for each logon attempt **or** via an OTP code sent via email to the users registered email address for each logon attempt. In both instances, the OTP code is required each time the authenticated user attempts to access the system.

Using your credentials and the OTP together means two-factors are required to allow access to the system, this helps to protect your organisation information.

2.1. Authentication App Method

This section of this guide will help you set up your MFA details using a downloadable smartphone authentication app. This setup process will only need to be completed once when the online DBS system account is accessed for the first time.

After the initial setup has been completed, the One-Time Password (OTP) generated from the app would need to be entered each time the user logs into the EmploymentCheck system.



The setup process will vary slightly depending on whether you are a new or existing user.

Step 1a – New Users accessing EmploymentCheck for the first time

New users would have received account creation emails from EmploymentCheck which contain a unique Username and Password.

These notifications will have been sent to the email address registered against the user account. Please check your spam / junk folders as well as the inbox if these emails have not been received. These credentials will be needed for Step 3.

Step 1b – Existing users accessing EmploymentCheck for the first time after the MFA functionality has been enabled

Existing users will need to register to use MFA the first time they log in after the MFA functionality has been enabled for their user role.

These users will need to access the system using their existing Username and Password and then will need to follow the steps outlined below.

Step 2 – Downloading the authentication app

To create a security token code each time you login to the online DBS system, you will need to download an authentication app to your mobile device.

The app we recommend is 'Google Authenticator' though you can also use 'Microsoft Authenticator' or 'Authy', all of which are free to download. This guide will show you how to set up and use the 'Google Authenticator' app specifically, but the process is similar across any of the recognised authentication apps.

On an Apple device open the App Store, search for 'Google Authenticator' and click 'GET' to download.

On an Android device open Google Play, search for 'Google Authenticator' and click 'INSTALL' to download.

Step 3 - Logging in to the Online DBS System

1. Go to the online DBS system website – the link should be included in the account creation email. The click on the 'Login' tab.

3. Then click on the 'Login' button.

Step 4 - Linking the Google Authenticator app and the Online DBS System

When you have logged into the online DBS system, you will be presented with the below screen where you will need to register to use two factor authentication:


1. You will need to click on the 'Generate code using mobile app' option which will take you to the 'MFA Registration' page.

!

Register Two Factor Authentication

Device registration for adminplus

Scan the QR code with your authenticator app



Or enter the following code in the authenticator app:

JK PL OF WJ NT WJ AQ WJ

The app will start to generate 6 digit authentication codes against your username.

Enter the current authentication code from the app in the field below and click the Validate button.

Note that the code changes every 30 seconds.

Passcode

Register Device

If you are unable to use the authenticator app, then click on the Receive code by email link below

Receive code by email

Logout

2. Then open the 'Google Authenticator' app on your device.

If this is your first time accessing the app, you'll need to click on the 'Get started' button.

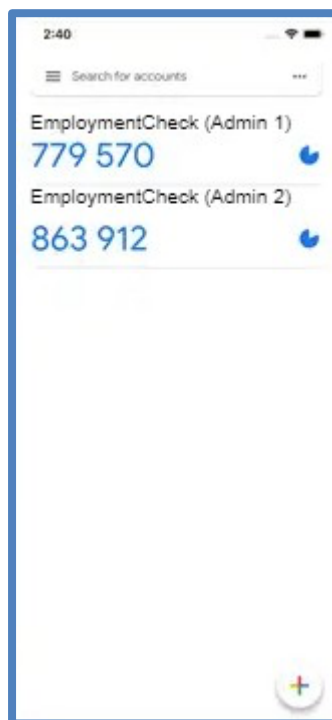
Stronger security with Google Authenticator

Get verification codes for all your accounts
using 2-Step Verification

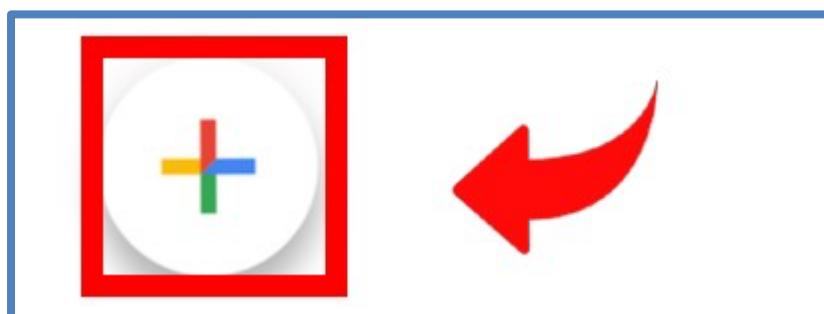
[Get started](#)



If you have used the 'Google Authenticator' app before, when you open the app, you'll see your existing accounts already linked to the authentication app.



3. Tap on the "+" button in the bottom right-hand corner.

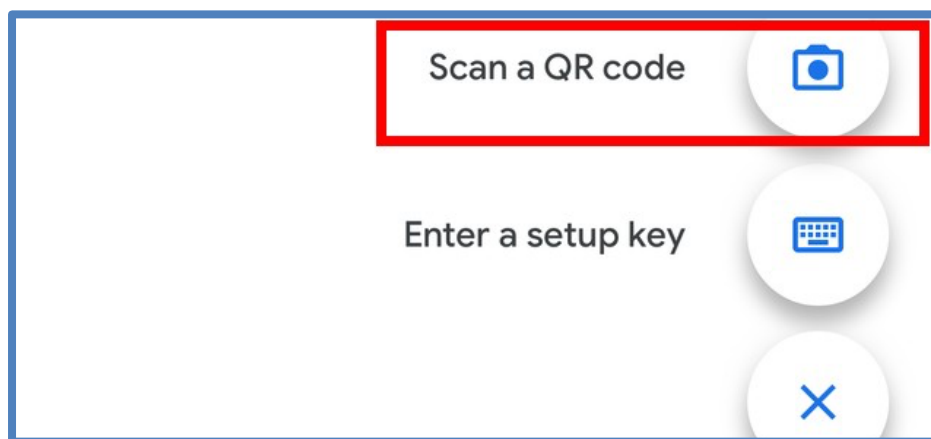


There are then two options to establish the link between the authentication app and the user account; either scan the QR code from the EmploymentCheck webpage or enter the setup key from the EmploymentCheck webpage.

One of either Steps 4a or 4b will need to be undertaken, both methods will achieve the same result.

Step 4a – Scan the QR code to link the account with the authentication app

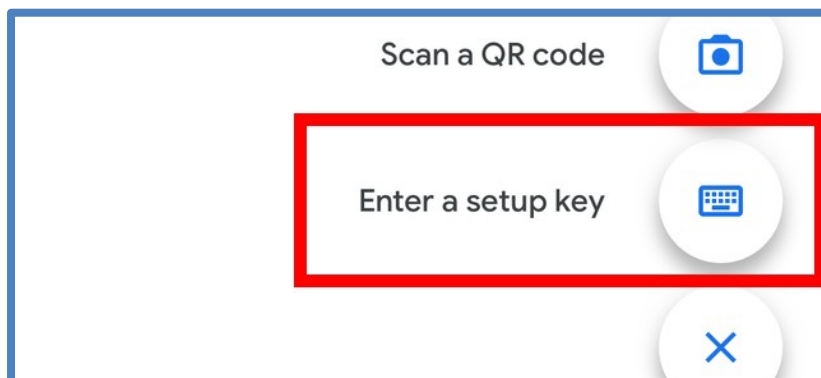
1. To link the account with the authentication app using the QR code, press on the 'Scan a QR code' option on the app.



2. Your phone will now switch to its camera, then scan the QR code displayed on the EmploymentCheck MFA Registration page.

Step 4b – Enter the setup key to link the account with the authentication app

1. To use the setup key, press on the 'Enter a setup key' option.



2. Enter the 16-letter code which is displayed on the EmploymentCheck MFA Registration page into the 'Key' field on the app. You can also enter an account name. We recommend you enter your EmploymentCheck Username into the 'Account' field.

3. Then click on the 'Add' button.

Step 5 – You're all set!

After scanning the QR code or entering the setup code, 'Google Authenticator' will now display an OTP linked to your EmploymentCheck account.

The OTP will reset every 30 seconds automatically.

Step 6 – Enter the OTP code on EmploymentCheck

1. Once the device has been registered, you can then enter the OTP in the 'Passcode' field on EmploymentCheck.

2. Once the 'Passcode' field has been completed with the OTP, then click on the 'Register Device' button.

3. You will then be presented with the EmploymentCheck Terms and Conditions for your user role(s). Accepting these terms will grant you access into the system.

Once you have linked your account to the authentication app, you will be required to enter the OTP each time you need to access the EmploymentCheck system.

2.2. Email Authentication OTP Method

For users who are unable to access/download the authentication app, an alternative email authentication route is available.

This section of the guide will outline how the email MFA route can be used to access EmploymentCheck. This process will need to be completed each time the user logs into the system.



We recommend the mobile app authentication route is used wherever possible.

Step 1a – New Users accessing EmploymentCheck for the first time

New users would have received account creation emails from EmploymentCheck which contain a unique Username and Password.

These notifications will have been sent to the e-mail address you provided.

Please check your spam / junk folder as well as your inbox.

Step 1b – Existing users accessing EmploymentCheck for the first time after the MFA functionality has been enabled

Existing users will need to register to use MFA the first time they log in after the MFA functionality has been enabled for their user role.

These users will need to access the system using their existing Username and Password and then will need to follow the steps outlined below.

Step 2 - Logging into the Online DBS System

1. Go to the online DBS system website – the link should be included in the account creation email.
2. Click on the 'Login' tab.
3. Enter your Username and Password exactly as they appear in account creation email into the relevant fields. Then click 'Login'.

Step 3 – Use the email MFA route to access EmploymentCheck

When you have logged into the online DBS system, you will be presented with the below screen where you will need opt to receive the one-time code via email.

1. You will need to click on the 'Receive one time code via email' option.

! Register Two Factor Authentication

To log in to the EmploymentCheck page, you will need a unique access code that is different each time you log in.

This code can be generated using a mobile app, or you can receive a code to your registered email account.

Please select the method you would like to use by clicking the relevant button below

☐ Generate code using mobile app

☒ Receive one time code via email

2. An automated email will be triggered by the system and will be sent to the email address registered against your account.

A confirmation message will be displayed onscreen.

Once the email has been received, you will need to click on the 'Login using email code' button.

One time email code has been sent to mfauserguidetest@cantium.solutions

[Login using email code](#)

3. You will then be presented with the Email OTP verification page as below.

CA

Cantium Admin

An Email has been sent to you from the EmploymentCheck system containing a code. Enter the code below and click the Validate button to login.

Code by
Email

If the email hasn't arrived, please check your SPAM folder and add us to your safe sender list

A new email code can be requested by clicking the **Send email code** link below

4. You will then need to enter the OTP code sent to your registered email address into the 'Code by Email' field.

5. You will then need to click on the 'Validate' button. A new OTP code can be generated using the 'Send new email code' button. Please note that if you request multiple codes, only the most recent code will be valid.

6. You will then be presented with the EmploymentCheck Terms and Conditions for your user role(s). Accepting these terms will grant you access into the system.

If the email method is used, this process will need to be completed each time you need to access the online DBS system.

Disclaimer

This document has been prepared by Cantium Business Solutions and HR Connect in good faith. The document is, however, supplied on the basis that neither Cantium Business Solutions nor HR Connect accepts no liability for statements made in the document or for conclusions drawn or actions taken based on the product description unless the contract for provision of the complete system is with Cantium Business Solutions/HR Connect. The liability accepted by Cantium Business Solutions/HR Connect will be determined by the terms of such a contract.