cognassist

Multi-Factor Authentication

Using MFA with the Cognassist Application

Version 1.0
06/2023

Introduction

Multi-factor authentication (MFA; two-factor authentication, or 2FA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

- Knowledge - Something only the **user knows** like a password or a memorized PIN.
- Possession - Something only the **user has** like a smartphone or a secure USB key.
- Inherence - Something only the **user is** like a fingerprint or facial recognition.

MFA helps to protect user data from being accessed by an unauthorised third party that may have been able to discover a password.

A third-party authenticator (TPA) app enables multi-factor authentication by showing a randomly generated and frequently changing code. Cognassist MFA uses Time-based One-Time Passwords (TOTP) for its randomly generated codes used to access the Cognassist Application. Time-based One-Time Passwords are a common form of MFA where unique numeric passwords are generated with a standardized algorithm that uses the current time as an input.

This document will provide guidance on enabling MFA for your Cognassist User account.

What you will need to complete the MFA enablement.

- The **Vanity Domain** URL for your organization. This will look something like *companyname*.app.cognassist.com.

  Note: The company name used in your vanity domain may be your full company name or a shortened/abbreviated version. This will have been provided to your organization during go live or when your company enabled MFA. Check with your tutor/coach if you do not know the vanity domain being used.
- A working **third-party Authenticator Application** (TPA). This can be any Authenticator Application that you choose as long as it supports Time-based One-Time Password (TOTP) code generation.

  Note: You will find that most Authenticator Applications work on a mobile device and as such this guide assumes you have a mobile device with a working Authenticator Application installed.
- Your **Username and Password** for the Cognassist Application.
- A **device with Internet connectivity**.

Third-Party Authenticator Application (TPA)

You can use any third-party Authenticator Application (TPA) you choose as long as it supports Time-based One-Time Password (TOTP) code generation. The initial setup of the third-party Authenticator Application and the addition of the Cognassist MFA code to the Authenticator App is outside the scope of this user guide.

IMPORTANT: You must have a working third-party Authenticator Application before you begin the process of MFA enablement for your Cognassist account.

If you already have your Authenticator Application setup and working, please move on to the next section "Enabling MFA On Your Cognassist Account"

There are many different third-party Authenticator Applications. Below is a list showing some of the more common Authenticator Applications you may choose to use and some links to help you get started. All the Authenticator Applications included in the list are free to use, some may require you to create a free account in order to access all features.

It is recommended that you always check with your IT Department before installing any applications on your device and we would also recommend you check to see if your organization has a preferred authentication application.

Note: The choice of which Authenticator Application to use is at the sole discretion of the individual. Cognassist do not provide support for the use or operation of Authenticator Applications.

- **Microsoft Authenticator**
    - Microsoft Authenticator is available for Android & iOS.
    - Works offline
    - Supports backup and/or Sync
    - Microsoft Mobile Phone Authenticator App | Microsoft Security
    - Download and install the Microsoft Authenticator app
    - Add non-Microsoft accounts to the Microsoft Authenticator app
    - Manually add an account to the Microsoft Authenticator app
    - Back up and recover account credentials in the Authenticator app

- **Google Authenticator**
  - Google Authenticator is available for Android & iOS.
  - Works offline
  - Supports Sync
  - Get verification codes with Google Authenticator - Android
  - Get verification codes with Google Authenticator - iPhone & iPad

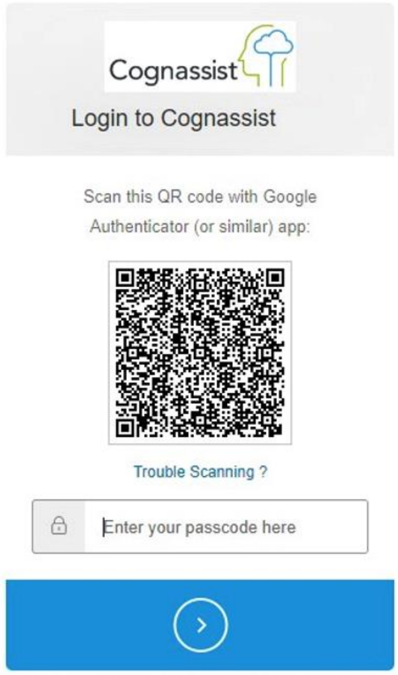
- **Twilio Authy**
  - Twilio Authy is available for Android, iOS, Windows, MacOS & Linux.
  - Works offline
  - Supports backup and/or Sync
  - Supports Encryption
  - Downloading and Installing Authy Apps
  - Add a New Two Factor Authentication Account Token in the Authy App
  - Welcome to Authy
  - Backups and Sync in Authy
- **2FAS**
  - 2FAS is available for Android, iOS & Browser extension.
  - Works offline
  - Supports backup and/or Sync
  - Supports Encryption
  - 2FA Authenticator App (2FAS)
  - 2FA Authenticator (2FAS) on the App Store (apple.com)
  - 2FA Authenticator (2FAS) - Apps on Google Play
  - 2FAS Browser Extension
  - Help Center - 2FAS

Enabling MFA On Your Cognassist Account

With MFA activated and enforced in your organization's environment, the first time you log in to the Cognassist application you will be presented with the MFA setup screen. You will need to register your Cognassist account with the third-party Authenticator Application running on your device.

As Authentication Applications are all slightly different in the way that they work please use the steps that follow as a guide on how to enable MFA on your Cognassist Account and add the required MFA token to your chosen third-party Authenticator Application.

1. Open your preferred web browser application on your device.
2. Launch the Cognassist website using your organization's vanity domain which will look like the following *https://companyname*.app.cognassist.com
3. Enter your username and password then click '**Log in >**'.
4. You will be presented with the MFA setup prompt showing a QR code as per the image below.

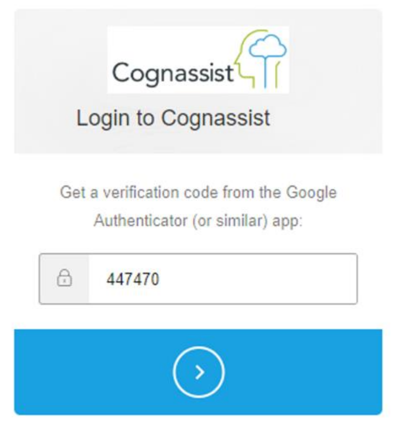


Login to Cognassist

Scan this QR code with Google Authenticator (or similar) app:

5. Open your Authenticator Application.
6. Click the relevant button to register a new account.
   a. If prompted select a generic (other) account type.

7. Adding the Cognassist token:
    a. Most Authenticator Applications support QR codes and this is the simplest method to add the token. Scan the QR code which is displayed on your screen and follow the on-screen prompts within your Authenticator App to register the Cognassist MFA token.
    b. If your Authenticator App does not support QR codes you will need to add the token manually. In your Authenticator App select the option to enter a code manually.
        i. On the MFA setup screen click the link ‘Trouble Scanning ?’ under the QR code.
        ii. The MFA setup prompt will now show a long number, this is your MFA secret token.
        iii. Enter the MFA secret token into your Authenticator Application and follow the on-screen prompts to register the Cognassist MFA token.
8. The Cognassist MFA code will now be available within your Authenticator Application.
9. Once you select the Cognassist MFA connection from within your Authentication Application you will see a 6 digit number, this number is your Time-based One-Time Passwords (TOTP) code. The TOTP code will change every 30 seconds. A countdown timer within your Authentication Application will show the time remaining for the TOTP code to remain active.
10. Return to your device and the Cognassist Application website.
11. Enter the TOTP code from your Authenticator Application into the text field on the MFA setup prompt as per the image below and click ‘**>**’.



Login to Cognassist

Get a verification code from the Google Authenticator (or similar) app:

447470

12. If your identity has been successfully verified you will be redirected to the Cognassist Application webpage.

    Note: If the TOTP code timed-out before you were able to click the button get the next valid TOTP code from the Authenticator App and repeat step 11.

Congratulations you have successfully enabled MFA for your Cognassist user account.