

Multi-Factor Authenticator Setup Guide

Embrace the power of Multi-Factor Authentication (MFA) to stay secure and confident in your online interactions. MFA is a security feature that provides an extra layer of protection to your accounts and data by requiring multiple forms of identification. The MFA One-Time passcode will be required at each login and cannot be bypassed.

FOR ADMINISTRATORS:

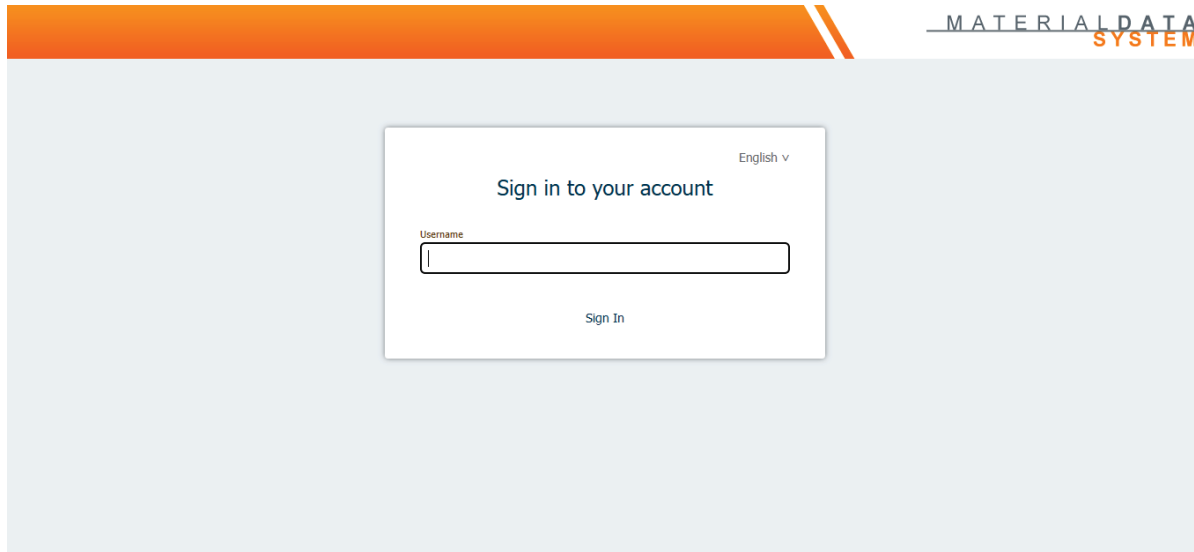
It is the responsibility of the administrator of the company to manage user accounts, which includes account creation, extension, password resets, MFA resets, and account deletion.

You can reset the MFA of any account by following these steps:

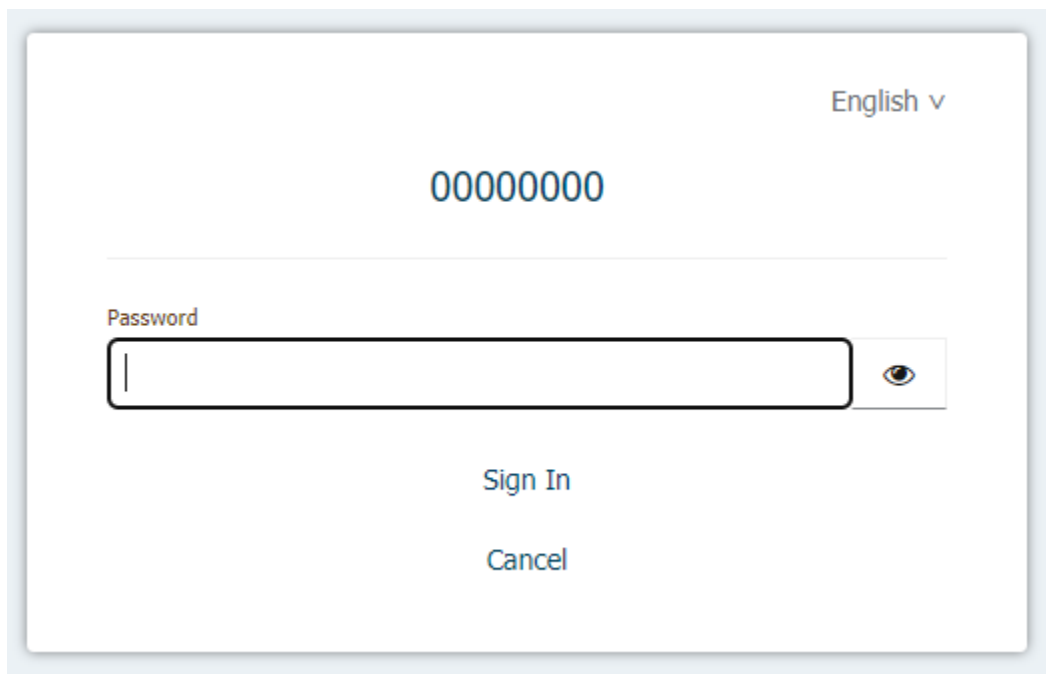
1. Log in to the Portal.
2. Go to: Administration / User.
3. Find the user account, right-click their name, and choose Edit.
4. At the bottom right you will have the option "Reset MFA"

1 Login

Go to the login page and press on the “Login” button.
Type in your username (IMDS User ID), press “Sign In”



Type in your password, press “Sign in”



2 Set up an authenticator app

You will be prompted to set up your Multi-Factor Authenticator (MFA). Choose your preferred application proceed for installation:

- Microsoft Authenticator (mobile application),
- Google Authenticator (mobile application),
- Free OTP (mobile application),
- Microsoft Authenticator (browser extension)



English v

Mobile Authenticator Setup

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:

- Google Authenticator
- FreeOTP
- Microsoft Authenticator

2. Open the application and scan the barcode:



[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

One-time code *

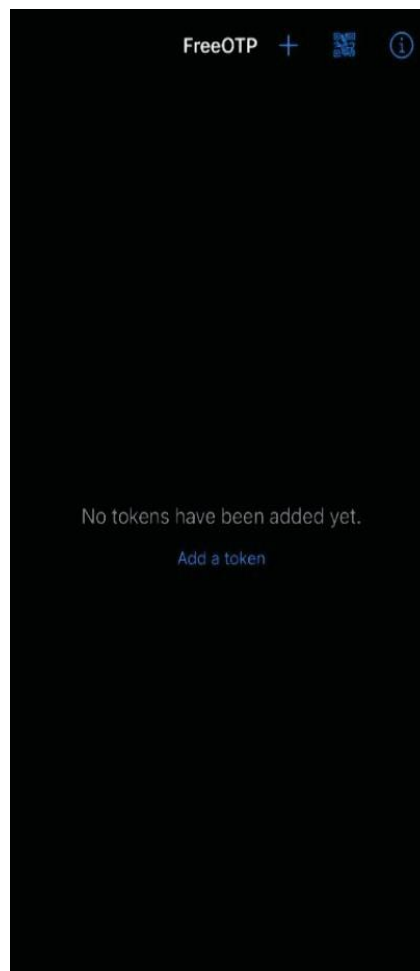
Device Name

☒ Sign out from other devices

Submit

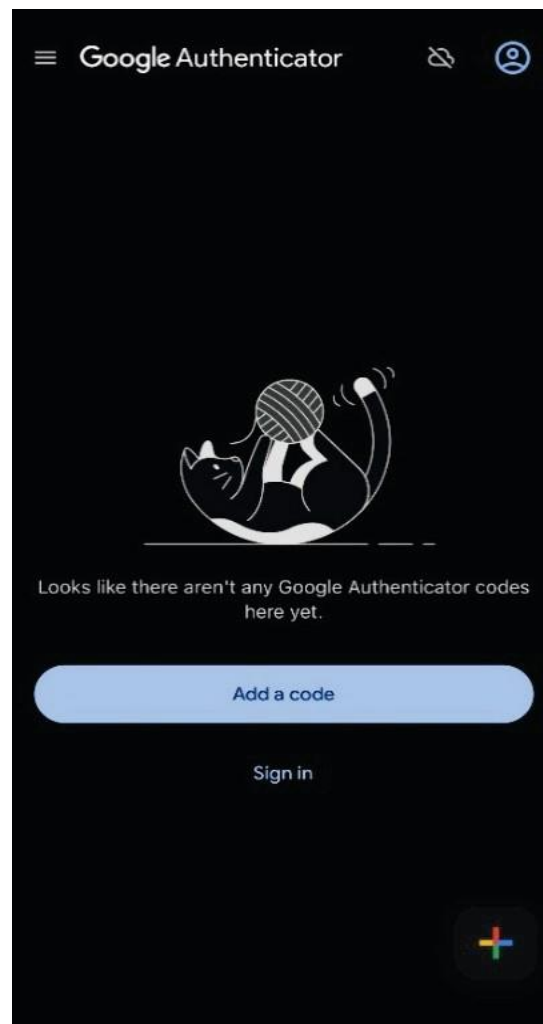
2.1 Setup FreeOTP

1. Download the “FreeOTP Authenticator” app (available for Android and iOS)
2. Open the application
3. Press on “Add token”
4. Scan the QR code *(If you previously added an MFA factor for your account in your MFA application, first remove it before scanning the QR code.)*
5. Choose a device name, it can be anything you want, there are no requirements
6. Enter the One-Time passcode code displaying on FreeOTP app under the IMDS account.
7. The code will change every 30 seconds, if it changes during your set up, you need to input the one currently displaying or it will be considered as invalid. Please note that the code should be entered without spaces, for example, "123456" and not "123 456."
8. press “Submit”



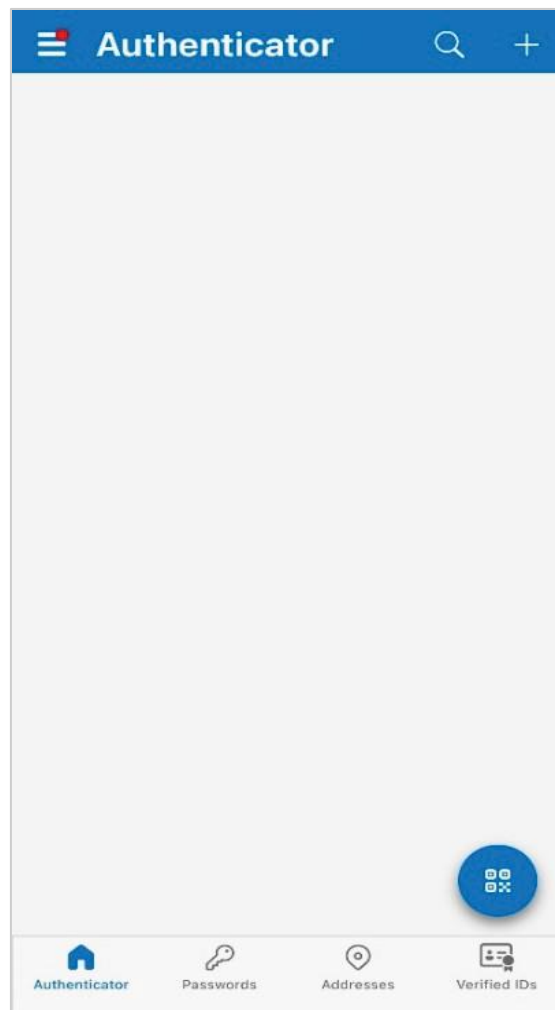
2.2 Setup Google Authenticator

1. Download the "Google Authenticator" app (available for Android and iOS)
2. Open application
3. Press on "Add a code"
4. Choose Scan a QR code
5. Scan the QR code *(If you previously added an MFA factor for your account in your MFA application, first remove it before scanning the QR code.)*
6. Enter the One-Time passcode code displaying on Google Authenticator app under the IMDS account
7. The code will change every 30 seconds, if it changes during your set up, you need to input the one currently displaying or it will be considered as invalid. Please note that the code should be entered without spaces, for example, "123456" and not "123 456"
8. Press "Submit"



2.3 Setup Microsoft Authenticator

1. Download the "Microsoft Authenticator" app (available for Android and iOS)
2. Open the application
3. Press on the round QR code icon
4. Scan the QR code
5. Choose a device name, it can be anything you want, there are no requirements
6. Enter the One-Time passcode code displaying on Microsoft Authenticator app under the IMDS account
7. The code will change every 30 seconds, if it changes during your set up, you need to input the one currently displaying or it will be considered as invalid. Please note that the code should be entered without spaces, for example, "123456" and not "123 456"
8. Press "Submit"



2.4 Setup Microsoft Authenticator extension

1. Go to <https://authenticator.cc/>
2. Choose your browser
3. Add the extension
4. Press the scan sign
5. Scan the QR code *(If you previously added an MFA factor for your account in your MFA application, first remove it before scanning the QR code.)*
6. Choose a device name, it can be anything you want, there are no requirements
7. Enter the One-Time passcode code displaying on Microsoft Authenticator extension app under the IMDS account.
8. The code will change every 30 seconds, if it changes during your set up, you need to input the one currently displaying or it will be considered as invalid. Please note that the code should be entered without spaces, for example, "123456" and not "123 456."
9. Press "Submit"