Pillar 3 Data Hub

Multi-Factor Authentication (MFA)

User Guide

Document control information:

Title:	**Pillar 3 Data Hub – Multi-Factor Authentication (MFA) User Guide**
Type:	User Guide
Target audience:	This document is intended for stakeholders from credit institutions who require access to the P3DH solution for submitting Pillar 3 disclosures and/or reviewing the submitted data. The following institutions are in scope of the first implementation of the P3DH: • Large institutions at the highest level of consolidation in the EEA (including stand-alone institutions and including financial holding companies and mixed financial holding companies supervised under Directive 2013/36/EU); • Large subsidiaries, subject to the reduced number of Pillar 3 requirements as established under Article 13; • Other institutions at the highest level of consolidation in the EEA (including stand-alone institutions). The institutions to be onboarded have been identified by the EBA, together with the relevant Competent Authorities (CA), based on Articles 6 and 13 of the CRR and the master data available in the EBA system.
Author(s):	Pillar 3 Technical Support
Version	2.4
Date	3 December 2025

Table of Contents

Introduction

The European Banking Authority (EBA) has developed the Pillar 3 Data Hub (P3DH) solution which configures, reuses, and extends the following existing EBA platforms to support Pillar 3 requirements:

- ERRP (EUCLID Regulatory Reporting Platform)
- EDAP (EBA Data Access Portal)
- EMDM (EUCLID Master Data Management).

The P3DH solution is designed to facilitate the centralization, production, and dissemination of Pillar 3 disclosures.

To ensure secure remote access to its digital resources, the EBA requires all users to authenticate via Multi-Factor Authentication (MFA) (except for resources that are accessible to the general public). For this authentication, the EBA uses Microsoft technology, which provides MFA through the Microsoft Authenticator app: Microsoft Authenticator authentication method - Microsoft Entra ID | Microsoft Learn. This method of authentication enhances account security by requiring a second form of verification in addition to a password.

This guide describes the step-by-step process for the P3DH users to install the Microsoft Authenticator app on their mobile device, set up Multi-Factor Authentication (MFA), and use it to authenticate when accessing the P3DH application. The guide is designed to help users understand the workflow and follow it effectively.

Questions and comments related to this document can be addressed to EBA Pillar 3 Technical Support (p3dh@eba.europa.eu) (please see Section 5).

Glossary

The glossary below provides definitions for key terms, acronyms, and technical language used throughout this document. Its purpose is to ensure clarity and consistency by helping readers—regardless of their familiarity with the subject—understand specific terminology related to the Pillar 3 Data Hub (P3DH) user authentication to support effective communication, reduce ambiguity, and enhances the overall usability of the document.

Term / Concept / Acronym	Definition
EBA	European Banking Authority

Term / Concept / Acronym	Definition
EBA Digital Resources	The information and communication technology (ICT) systems, services, infrastructure, and tools used by the EBA to support its operations, regulatory activities, and secure data exchange. These resources include the Euclid Regulatory Reporting Platform (ERRP), the EBA Data Access Portal (EDAP), and the Pillar 3 Data Hub (P3DH). They are governed by the EBA's ICT and security risk management guidelines, which aim to ensure a consistent, secure, and resilient approach to managing ICT risks across the EU financial sector (please refer to Guidelines on ICT and security risk management | European Banking Authority).
EDAP	EBA Data Access Portal that can be accessed via the following URL: • EDAP
EMDM	Abbreviation for EUCLID Master Data Management, EBA's platform that supports the collection and maintenance of EUCLID reporting entity master data, which is required to support the generation of the reporting obligation calendars of the entity.
ERRP	EUCLID Regulatory Reporting Platform that can be accessed via the following URL: • Production environment: https://errp.eba.europa.eu/portal/login • Test environment: https://errp.test.eba.europa.eu/portal/login
Existing User	An external stakeholder who has previously configured Multi-Factor Authentication (MFA) for accessing EBA Digital Resources. This includes users who have already completed the MFA setup process and can securely access EBA systems such as theP3DH, the ERRP, or the EDAP without needing to repeat the initial configuration.
Multi-Factor Authentication (MFA)	Security process that requires users to provide two or more independent forms of verification to access a system, application, or account. The goal is to enhance protection by combining multiple types of credentials, making unauthorized access significantly more difficult. For the P3DH two-factor authentication is used that includes: • User's institution credentials (i.e., username and password) • Microsoft Authenticator app
New User	An external stakeholder who has not previously configured Multi-Factor Authentication (MFA) for accessing EBA Digital Resources. This includes users who are accessing EBA systems such as the Pillar 3 Data Hub (P3DH), the EUCLID Regulatory Reporting Platform (ERRP), or the EBA Data Access Portal (EDAP) for the first time and therefore need to complete the initial MFA setup to ensure secure access.
P3DH	Abbreviation for Pillar 3 Data Hub, an application provided by EBA to support for managing Pillar 3 regulatory data.

Term / Concept / Acronym	Definition
Pillar 3 Data Hub (P3DH)	Digital application provided by the EBA for managing Pillar 3 regulatory data. P3DHconfigures, reuses and extends the ERRP and EDAP platforms to support the Pillar 3 requirements. It is designed to: • support the centralization, production, and dissemination of the Pillar 3 disclosures; • facilitate centralized access by all stakeholders to prudential data from all EEA institutions; • promote transparency and market discipline in the EU banking sector further contributing to the soundness of the European financial system.

1. Overview of the MFA configuration and usage process

As shown in Figure 1, the process of connecting to the P3DH application differs for New and Existing Users (Please see definitions of the New and Existing Users in the Glossary section).

An Existing User can connect directly to the P3DH application by clicking the "Accept invitation" link in the invitation email or by navigating to the ERRP URL (see Glossary). During the connection process, the user receives a push notification on their mobile device via the Microsoft Authenticator app (or another chosen authentication app). To complete the sign-in, the user must approve the attempt by entering in the app the number displayed on the login screen. On Figure 1 this process is marked as #3. Please refer to Section 2.3 for a step-by-step description of the connection process.

A New User will need to set up MFA before connecting to the P3DH application. On Figure 1 this process is marked as #2. Please refer to Section 2.2 for a step-by-step description of the MFA setup process.

Microsoft Authenticator (recommended) or another authentication app should be installed on the user's mobile device to set up MFA. On Figure 1 this process is marked as #1. Please refer to Section 2.1 for the details about Microsoft Authenticator installation.

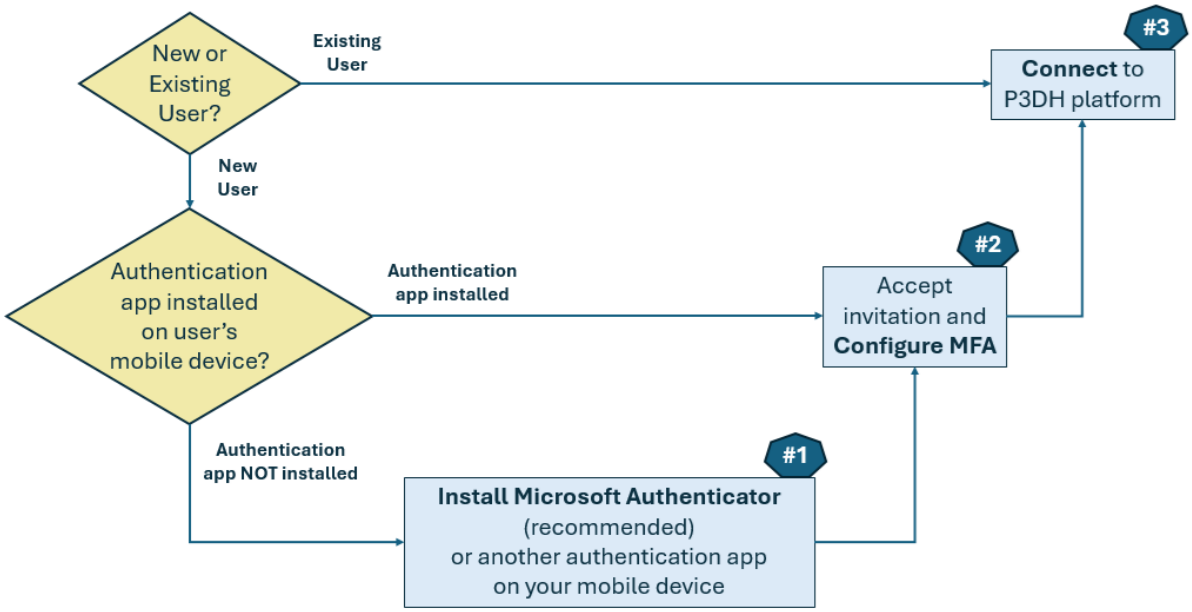

Figure 1: Overview of the MFA configuration and usage process

2. Step-by-step process description

This section outlines the steps that users should follow to configure MFA and connect to the P3DH application. To facilitate readability, this section is divided into sub-sections detailing the steps at each phase of the process.

2.1. Installation of the authentication app

Before accessing the Pillar 3 Data Hub (P3DH) platform the users should install on their mobile device the Microsoft Authenticator app (recommended) or another authentication app.

It is recommended that the app is installed before clicking the "Accept invitation" link in the invitation to connect P3DH.

To install Microsoft Authenticator, please follow the following steps:

- On your mobile device (i.e., phone or tablet) open either the Google Play Store (for Android devices) or the Apple App Store (for iOS devices).
- In the search bar, type "Microsoft Authenticator" and press the search icon.
- Find the official Microsoft Authenticator app and click on Install (for Android) or Get (for Apple). You may need to use your password, Face ID, Touch ID, or other authentication method to confirm the download.
- Once the installation is complete, click Open to launch the Microsoft Authenticator app.

2.2. MFA setup

A New User accessing EBA Digital Resources for the first time will need to set up Multi-Factor Authentication (MFA) before connecting to P3DH for submitting Pillar 3 data.

To set up MFA, please follow the following steps:

- In your inbox, open the email received from Invites@Microsoft.com with title: "Microsoft invitation on behalf of European Banking Authority" (see Figure 2).

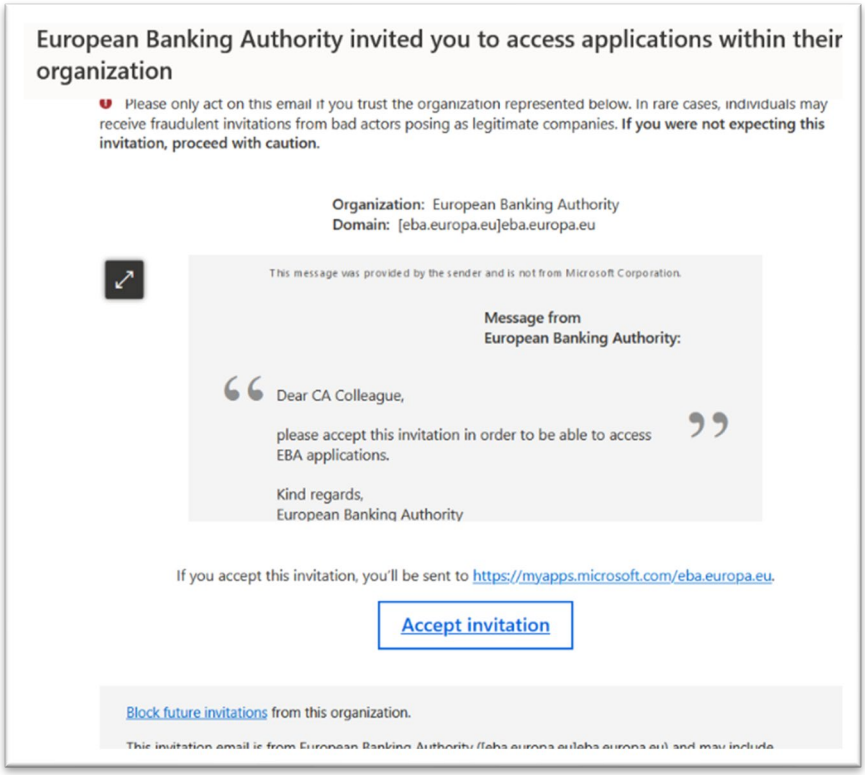

Figure 2: Email received from Invites@microsoft.com with title: "Microsoft invitation on behalf of European Banking Authority".

- Click the "Accept invitation" link in the email, and you will be prompted by your default browser to login to P3DH in the ERRP platform.
- Enter the email address you provided to EBA (should be the same as the one receiving the invitation email) and click "Next" (see Figure 3).

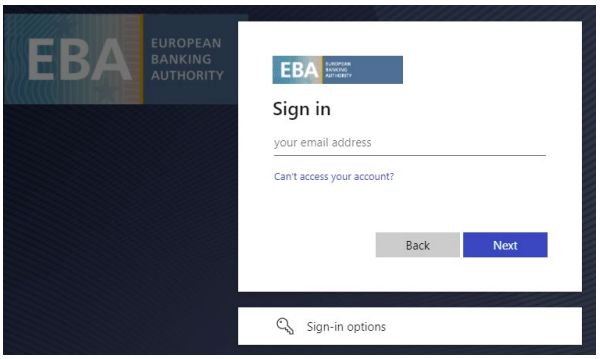

Figure 3: Enter the email address you provided to EBA (should be the same as the one receiving the invitation email) and click "Next"

- Enter your password. This is the same password you use to sign in to your institution's IT resources. (i.e., If your institution uses Microsoft 365, this is the same password you use to sign in to your Microsoft 365 account. Otherwise, use the password associated with your institution's IT systems. No password is provided by the EBA). Click "Sign in" (see Figure 4).

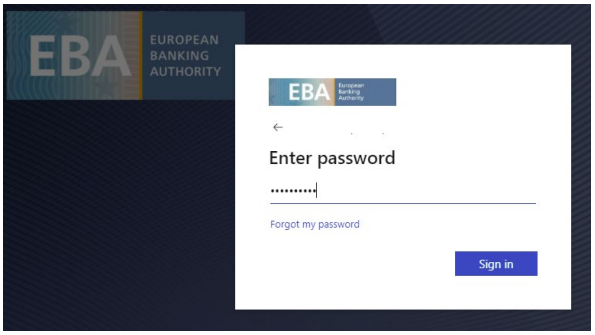

Figure 4: Enter your network password (same as your office login for this user account) and click "Sign in"

- You will see the MFA notification. Click "Next". (see Figure 5).

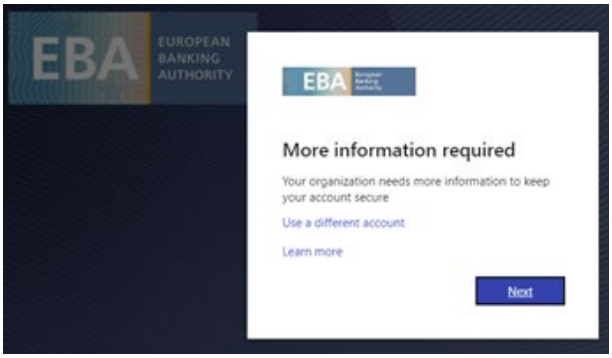

Figure 5: MFA setup notification. Click "Next"

- You will be prompted to set up MFA (see Figure 6).

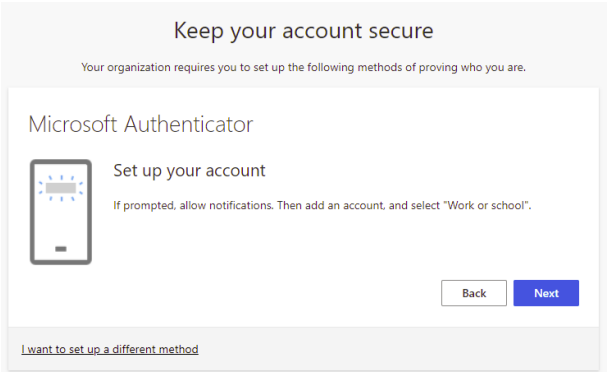

Figure 6: You will be prompted to set up MFA

- Open the Microsoft Authenticator App on your mobile device and scan the QR code displayed on your computer screen to link your account:
    - Open the Microsoft Authenticator App (please refer to Section 2.1 for installation);
    - click "+"to add a new account;
    - Select the "Work or school account" option;
    - Select "Scan QR code";
    - Scan the QR code that appears on the computer screen (see Figure 7);

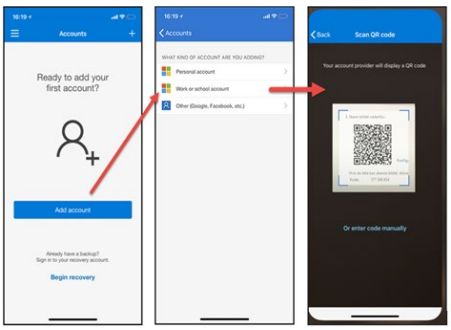

Figure 7: Scan the QR code

    - Approve sign-in notification by clicking "Approve" (see Figure 8) and go back to your computer.

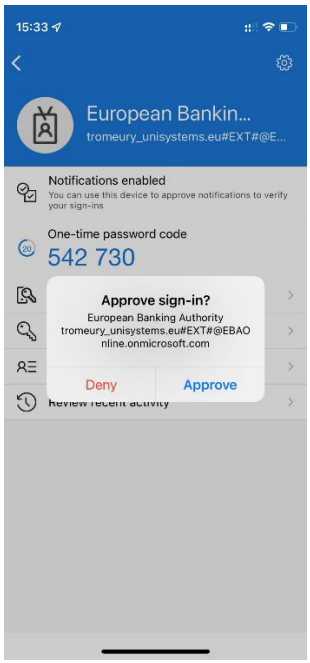

Figure 8: Approve sign-in notification sent to your mobile device through the Microsoft Authenticator App

- On the computer screen:
  - Click “Next” to proceed with connection (see Figure 9);
  - Receive the success confirmation (see Figure 10);
  - Click “Done”, the MFA is set up!

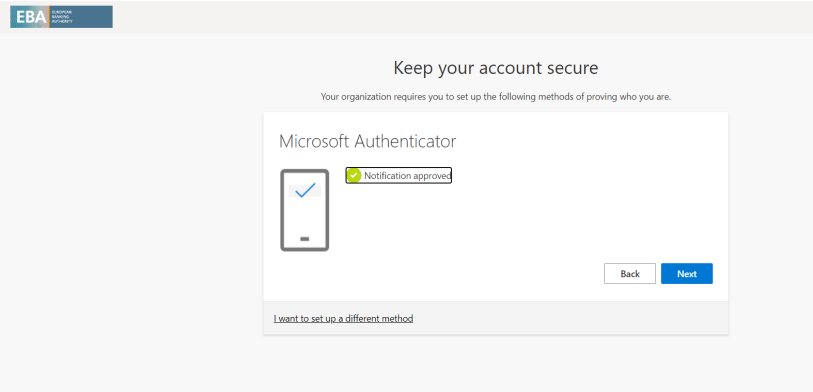

Figure 9: Click "Next" to proceed with connection.

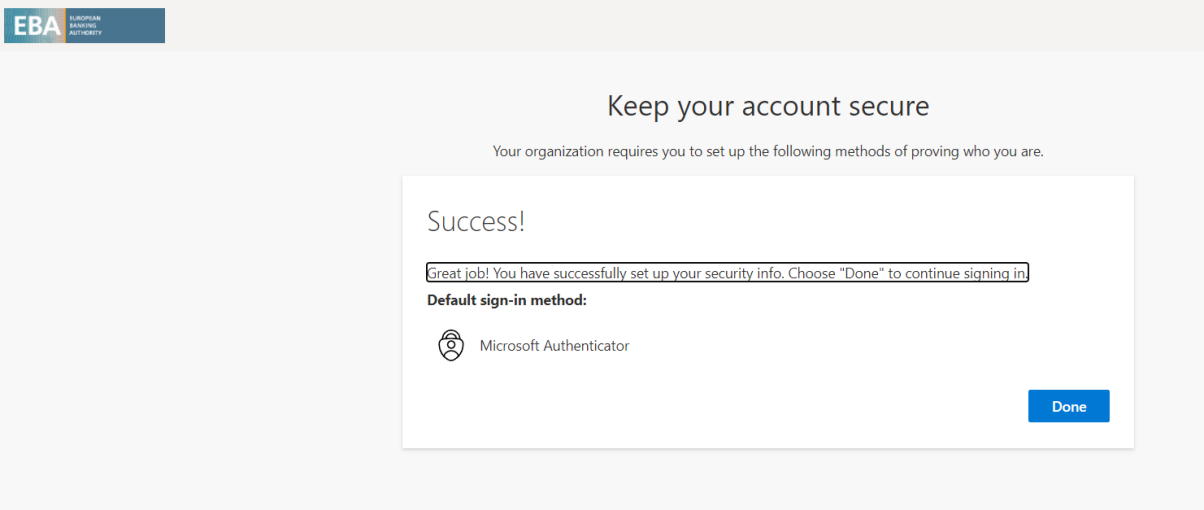

Figure 10: Success screen. You can click "Done"; the MFA is set up!

2.3. Connection to P3DH application in ERRP

When MFA is configured, user can access the P3DH application in ERRP.
To access P3DH, please follow the following steps:

- Navigate to the URLs specified in the Glossary section (see Figures 11 and 12).

Figure 11: ERRP Test environment - Login page

Figure 12: ERRP Production environment - Login page

- Enter your password. This is the same password you use to sign in to your institution's IT resources (i.e., If your institution uses Microsoft 365, this is the same password you use to sign in to your Microsoft 365 account. Otherwise, this is the password associated with your institution's IT systems. Your password is not managed or stored by the EBA). (see Figure 13).

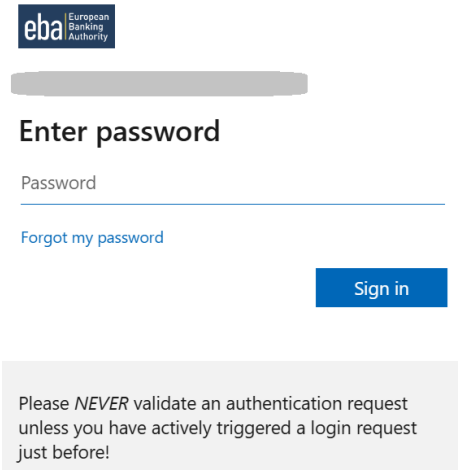

Figure 13: User authentication when entering ERRP - Password

- Enter the generated code into the Microsoft Authenticator app installed on your mobile device (see Figure 14).

Figure 14: User authentication when entering ERRP – Microsoft Authenticator app

- Upon successful authentication via MFA, enter ERRP, where you can see the dedicated "Pillar3" tab (see Figure 15).

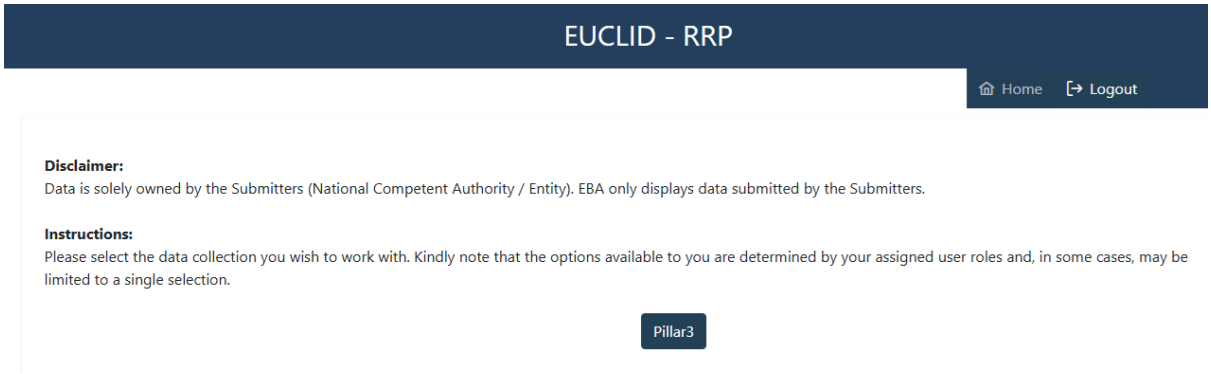

Figure 15: ERRP screen with the Pillar3 tab to enter the P3DH application

- After clicking the "Pillar 3" tab you enter the P3DH application where you can view or/and submit the Pillar 3 disclosures (see Figure 16).

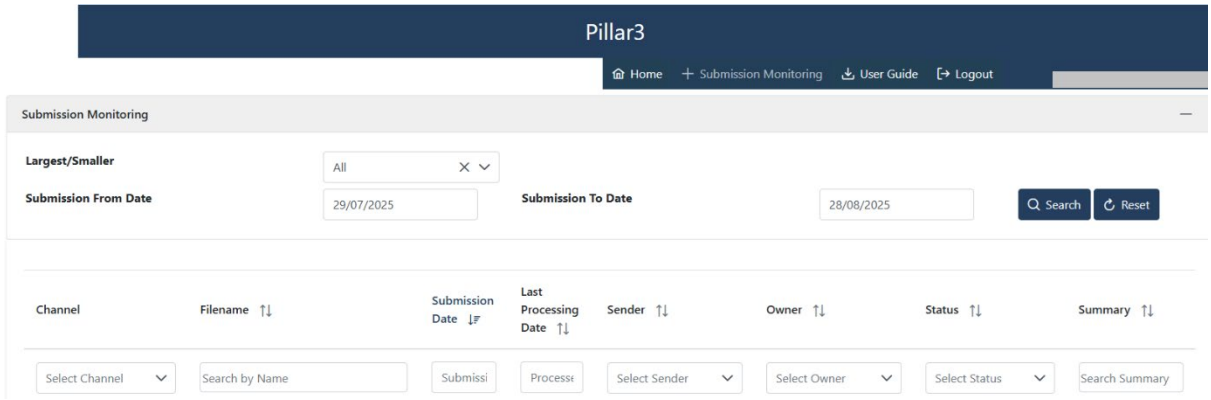

Figure 16: P3DH application

3. Additional (optional) MFA methods

If you wish to use an alternative MFA (Multi-Factor Authentication) method—other than Microsoft Authenticator—you can select it when you reach the MFA prompt during sign-in. On the authentication screen, click "Choose a different method" to pick from available options such as another authentication app, text message or phone call (see Figure 17).

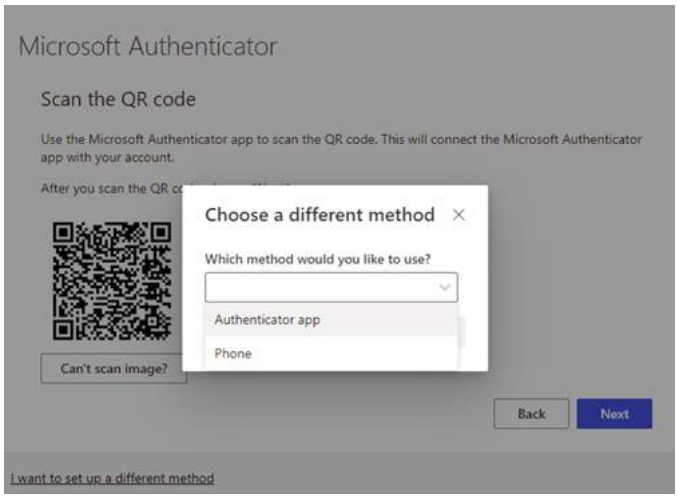

Figure 17: Select an alternative MFA method

- Another authentication app: User can use an authentication app other that Microsoft Authenticator (please see Section 3.1)
- Text message verification: A verification code will be sent via SMS to user's mobile device. To complete the sign-in process, the user needs to enter the code into the sign-in interface (please see Section 3.2)
- Phone call verification: User will receive an automated voice call at the registered phone number. To complete the sign-in process, the user should follow the instructions and press # on the keypad when prompted (please see Section 3.3)

3.1. Other Authenticator Apps

To select an alternative MFA method please follow the following steps:

- Click on "Choose a different method" on the Microsoft Authenticator screen (see Figure 17)
- Select "Authenticator app"
- Follow the instructions of the selected Authenticator app manual to add an account.

3.2. Authentication via text message or phone call

To set up authentication via text message or phone call please follow the following steps:

- Click on "Choose a different method" on the Microsoft Authenticator screen (see Figure 17)
- Select "Phone"
- Select the country from dropdown list and enter mobile phone number (see Figure 18)

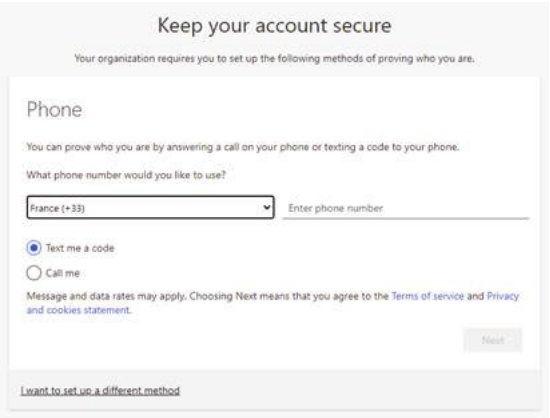

Figure 18: Select country from dropdown list and enter mobile phone number

- Select “Text me a code” if you wish to receive a text message or “Call me” if you wish to receive a phone call. Press “Next” (see Figure 18).

When using the authentication via text message or phone call, please be aware that:

- for “call me” option, the calls to verify access to application must be answered, as human response is required for the automated voice-based instructions;
- for “Text me a code” option, a verification code will be sent via SMS and human response is required to enter code on screen.

4. Common issues users may encounter

Users may occasionally experience issues during MFA setup or login. This chapter outlines the most frequent connectivity related issues, explains their possible causes, and provides practical steps to resolve them or seek further assistance.

4.1. Invitation not received

There can be several reasons why a user might not receive the MFA setup invitation from invites@microsoft.com:

- The invitation may have been sent to an incorrect email address.
- The email may have been filtered as spam or quarantined by the user's email system.
- The domain microsoft.com or the specific address invites@microsoft.com might be blocked or not whitelisted in the organization's email settings.
- The user’s email may not have been properly registered in EBA’s Azure Active Directory.
- If the user has already set up MFA or accepted a previous invitation, a new one might not be triggered.

To resolve this issue, we recommend the following steps:

- Check your spam or junk folder for an email from invites@microsoft.com.
- Confirm that the correct email address was communicated to EBA for setting up the user account for accessing EBA Digital Resources (e.g., the email address indicated for the user in the P3DH Contact Person form).
- Ensure that you are checking the right inbox (especially if you have multiple accounts).
- Ask the IT team of your institution to whitelist or allow emails from invites@microsoft.com in your email system.
- If you have already accepted a previous invitation (for example, to connect to other EBA Digital Resources), you may not receive a new one. In this case, try accessing the ERRP directly. Please refer to the URLs provided in the Glossary section.

If none of the steps above works, please contact the EBA P3DH Technical Support (see Section 5). P3DH Technical Support will reset the redemption status of your account, which will trigger a new invitation to be sent from invites@microsoft.com. Please monitor your inbox (including spam/junk folders) for the updated invitation. If the new invitation is not received, the P3DH Technical Support Team will initiate further investigation. This may involve direct communication with your institution's IT team to help resolve the issue.

4.2. "403 Forbidden" error

This error can occur after user accepts the invitation to connect to P3DH (i.e. when s/he clicks the "Accept invitation" link in the email received from received from Invites@Microsoft.com).

This error indicates that the server understands the request but is refusing to authorize it.

One common cause for this error is corrupted cookies in the browser, which can interfere with access. To help determine whether this is the case, one of the following methods is recommended:

- Use a different browser (e.g., if you normally use Microsoft Edge, try Google Chrome or Firefox).
- Use private browsing mode:
    - InPrivate in Microsoft Edge
    - Incognito in Google Chrome
    - Private Browsing in Mozilla Firefox

If you experience this error and you're able to access the system using one of the above methods, it's likely that the issue is related to corrupted cookies in your usual browser. In that case, to resolve the issue we suggest clearing your browser's cache and cookies to resolve the problem.

If the issue persists, it may be caused by another factor—such as network restrictions or security settings. In this case, please contact the EBA P3DH Technical Support (see Section 5).

4.3. EBA's domain blocked by user's institution

This message can occur after user accepts the invitation to connect to P3DH (i.e. when s/he clicks the "Accept invitation" link in the email received from Invites@Microsoft.com).

If you receive this message, this indicates that the connection cannot be established because the domain associated with EBA tenant is currently blocked or not whitelisted by your institution's security policies. This means that your network may be preventing access to the URLs or endpoints required for the MFA setup and system integration.

To resolve this issue please contact your institution's IT team to ensure that the EBA's domain is unblocked to allow access.

You can share with your institution's IT team the following technical details:

- EBA Tenant ID: 3bacb4ff-f1a2-4c92-b96c-e99fec826b68
- EBA primary domain: eba.europa.eu
- Default domain for the EBA tenant: EBAOnline.onmicrosoft.com

If your IT team needs support to resolve this issue, please contact the EBA P3DH Technical Support (see Section 5).

4.4. Push notifications do not arrive on user's mobile device

This issue can occur when a user is redirected to a screen requesting an MFA code but does not receive any push notification on their mobile device, despite having the Microsoft Authenticator app installed.

This can occur when user's mobile device is in a mode that could prevent notifications from arriving. These modes may silence or delay alerts. These are some common modes that may block notifications:

- Do Not Disturb (iOS & Android): Silences calls and notifications.
- Focus Mode (iOS): Includes Sleep, Work, and Personal modes that restrict notifications.
- Battery Saver / Low Power Mode: May limit background activity, including push notifications.
- Airplane Mode: Disables all network connections, preventing notifications.
- App Notification Settings: If notifications are disabled for the authenticator app, you won't receive prompts.

If you experience this issue, please follow the steps below to help resolve it:

- Ensure the mobile device has a stable internet connection (Wi-Fi or mobile data).
- Avoid using Battery Saver if it restricts background activity.
- Turn off Do Not Disturb or Focus Mode.
- Ensure that notifications are enabled in your mobile device:
    - Go to the phone's Settings > Notifications.
    - Make sure notifications are allowed for Microsoft Authenticator.
- Sometimes push notifications don't arrive, but the code is still available in the app. Please open the Microsoft Authenticator app and check for the 6-digit code under the account name.
- Check Time Synchronization:
    - On Android: In the Authenticator app, go to Settings > Time correction for codes > Sync now.
    - On iPhone: Ensure the system time is set to automatic.

If the issue persists, please contact the EBA P3DH Technical Support (see Section 5).

4.5. "Wrong password" message

This issue - where a user inputs the correct password for their own organisation but receives a "Wrong Password" message – can occur when the user tries to access the EBA tenant via B2B to perform MFA setup as described in the section 2.2 (Please see Figure 17).

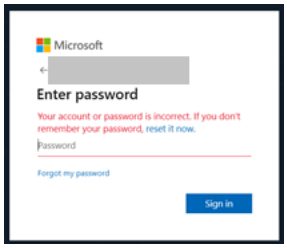

Figure 17: Wrong password message

This issue can be caused by several factors:

- Incorrect Identity Provider Routing: If the user's domain is not federated with Microsoft Entra ID, Microsoft may route the login attempt incorrectly
- Tenant Invitation Issue: The user may not have been properly invited to the EBA tenant, or the invitation may have expired
- Cash Issue: User browser can cache login credentials, including passwords, and a wrong password can be auto-filled when a user tries to connect

If you experience this issue, please follow the steps to exclude the possibility of the Cash Issue:

- Use a different browser (e.g., if you normally use Microsoft Edge, try Google Chrome or Firefox).
- Use private browsing mode to avoid cached credentials interfering with login:
    - InPrivate in Microsoft Edge
    - Incognito in Google Chrome
    - Private Browsing in Mozilla Firefox
- Use the direct link to ERRP instead of accepting the Invitation (Please see the URL to access ERRP in the Glossary section)

If you're able to access the system following the above steps, it's likely that the issue is related to the password cashed by your usual browser. In that case, to resolve the issue we suggest clearing your browser's cache to resolve the problem.

If the issue persists, it may be caused by another factor. In this case, please contact the EBA P3DH Technical Support (see Section 5). We will remove the existing account and create a new account to ensure that your account is correctly configured in the EBA tenant.

4.6. Shared mailbox is indicated as User ID

Using shared mailboxes for individual users is not recommended. Shared email accounts often lack clear ownership and accountability, which can lead to delays in communication, missed notifications, and difficulties in tracking actions. For security and audit purposes, it is essential that each role is associated with a named individual's corporate email address, ensuring traceability and compliance with regulatory requirements.

5. How to contact EBA P3DH Technical Support

If you have questions or need assistance, please contact the EBA P3DH Technical Support by sending an email to p3dh@eba.europa.eu.

To help ensure timely and effective support, please follow these recommendations when communicating with the EBA P3DH Technical Support Team:

- Include the name of your institution and its LEI in the email subject line.
- Provide a brief (2–3 word) description of the issue in the subject line to help categorize and prioritize your request.

- If applicable, include relevant screenshots into your message to facilitate faster investigation and resolution.