FONDAZIONE
BRUNO KESSLER

MULTI-FACTOR AUTHENTICATION CONFIGURATION - USER GUIDE

FONDAZIONE
BRUNO KESSLER

Indice

FONDAZIONE
BRUNO KESSLER

1. Introduction

This document provides the user procedure for securing their FBK account using multi-factor authentication - hereinafter referred to as MFA. This allows, according to what was reported by Alex Weinert (Director of Identity Security at Microsoft), to prevent 99.9% of attacks on the user's digital identity. However, it is not a panacea: an attacker can in fact intercept the access request and, by stealing all incoming data, impersonate the user. We suggest paying particular attention to the detection mechanisms presented in Section 1.1.

You will need to use the second factor in the following cases:

- To access from outside the FBK any Microsoft and Google service with FBK account. It is requested the first time and every 30 days; unless you change the address from which you connect (e.g., using different Wifi networks or connecting your smartphone).
- For administrative actions on the Microsoft Azure cloud with an FBK account.
- To independently reset your FBK password or when Microsoft detects abnormal account behavior[4].
- When Microsoft detects medium or high risk when authenticating [1].

The pilot to which this document refers falls within the first of the points identified to protect the FBK infrastructure (two-year Zero Trust project).

Below is an example of how to configure MFA with the available mechanisms:

● Microsoft Authenticator as a mobile application (from a PC illustrated in Section 2.1, from a smartphone in Section 2.3).

● A landline or mobile phone number (Section 2.2 - Steps A, B, C).

We suggest configuring (at least) the first two mechanisms (see page 13), so that you can use the phone number in case of theft / loss or replacement of the device with the Microsoft Authenticator (see procedures - pages 21 to 24).

The user experience after configuring MFA is shown in Section 3.

[1] For behaviors that Microsoft considers at risk during authentication (Sign-in risk) or use of the account (User risk), refer to LINK.

1.1. Defend yourself from identity theft

As introduced, a multi-factor authentication mechanism is also susceptible to cyber attacks. In particular, an attacker is able to impersonate the user if:

1. [In the vicinity of the user] observe the access credentials, anticipating it in the login.

   Detection: login failure; receiving notification by email, SMS or mobile application, Possible mitigations: (PRE) check that you are not observed during login; (POST) promptly log out of unrecognized sessions and devices - LINK Google, LINK Microsoft.

2. [In the vicinity of the user] knows the user's username and password, and takes possession of the device used as a second factor (e.g., mobile phone or hardware key).

   Detection: as in # 1, although the attacker could delete emails / sms quickly and easily. Check active sessions on a recurring basis - LINK Google, LINK Microsoft.

   Possible mitigations: (PRE) choose an "appropriate" password; do not abandon the device used as a second factor (in the case of a mobile device, protect it with one of the supported mechanisms - e.g., PIN or fingerprint); (POST) log out of unrecognized sessions and devices promptly - LINK Google, LINK Microsoft.

3. [Remotely] Get access to the access credentials and second factor by having tampered with the browser, operating system and / or user device. By extension, although less likely, it compromises admin users in FBK, FBK or Google / Microsoft servers.

   Detection: as in # 2.

   Possible mitigations: (PRE) keep the devices used up-to-date and safe (eg use an antivirus solution); (POST) promptly log out of unrecognized sessions and devices - LINK Google, LINK Microsoft.

4. [Remotely] It inserts itself into communications between user and server and steals cookies[2].

   Detection: even if the lock icon shown by the browser and the details (by clicking on it) show that the connection is secure / reliable, the URL prefix is different from https://accounts.google.com/ or https://login.microsoftonline.com/. For example, it could be https://fbk-login.com, https://accounts.fbk.google.com or https://accounts.fbk-google.com/; or even https://login.mcrsft-online.com.

[2] A cookie is an object typically sent to the user's browser when visiting a web page. It is normally used to maintain a session for each user who authenticates: once logged in, the server sends a unique cookie to the browser and this uses it in each subsequent request; in this way, the user does not need to authenticate for each page visited.

Come spiegato da Microsoft (LINK), esistono modalità di attacco per cui l'utente non è in grado di distinguere l'esperienza di login malevola da quella prevista: tranne l'URL, corrispondono tutti i loghi, la loro posizione e il testo (sia di Google/Microsoft, che eventuali personalizzazioni dell'interfaccia introdotte da FBK); in aggiunta, se l'attacco avviene attraverso un'email malevola[3], un attaccante potrebbe riuscire a pre- compilare il campo username per trarre ulteriormente in inganno l'utente. Infine, diversamente dall'attacco #1, l'utente riesce a tutti gli effetti ad accedere al servizio richiesto e i portali di Google e Microsoft non possono rilevare il login dell'attaccante; in quanto mai avvenuto (poiché ruba la sessione attiva dell'utente).

Possibili Mitigazioni: (PRE) utilizzare una chiavetta hardware (es., YubiKey) e verificare le email inviate da Google/Microsoft come riportato in LINK - e.s., campo "firmato da" con valore "accounts.google.com" o "accountprotection.microsoft.com". (POST) Controllare in maniera ricorrente le regole impostate nella propria email (LINK).

[3] To learn more about the Phishing phenomenon, visit LINK.

2. Configuration procedure

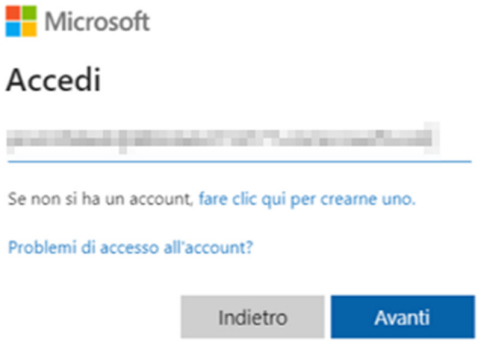
This procedure guides the user in configuring the Microsoft Authenticator app as an additional authentication factor, in order to protect the FBK account.

2.1. Configuration via PC

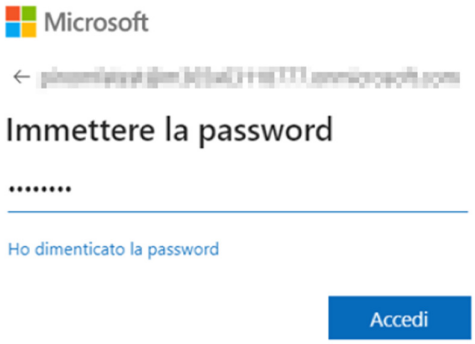
Below are the steps to follow to start the procedure from a PC.

I. **Connect via browser** to the following address: https://aka.ms/mfasetup.

II. If it hasn't already been done, **log in with your user credentials**.

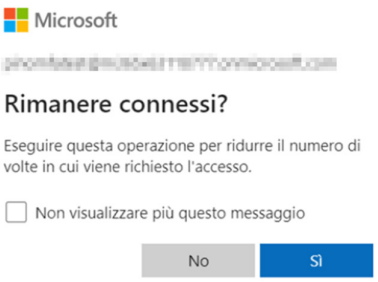


Username entry screen (email address)



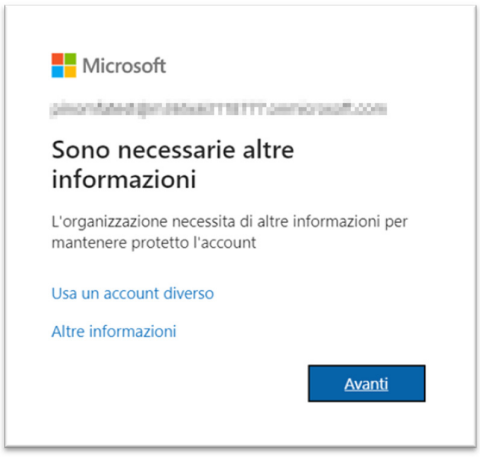
Schermata inserimento password

III. If the following screen appears, click on NO if you are connecting from an external wireless / wired network (non-personal or from FBK) or from a non-personal device.



Session persistence screen

IV. A page will appear asking for additional information to be registered.**Cliccare su *Avanti*:**

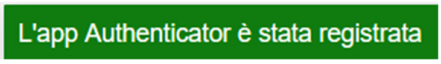


Screen informing you of the need to set up MFA.

V. If not already done, download the Microsoft Authenticator application on your smartphone as suggested by the page and click next. Alternatively, it is possible:

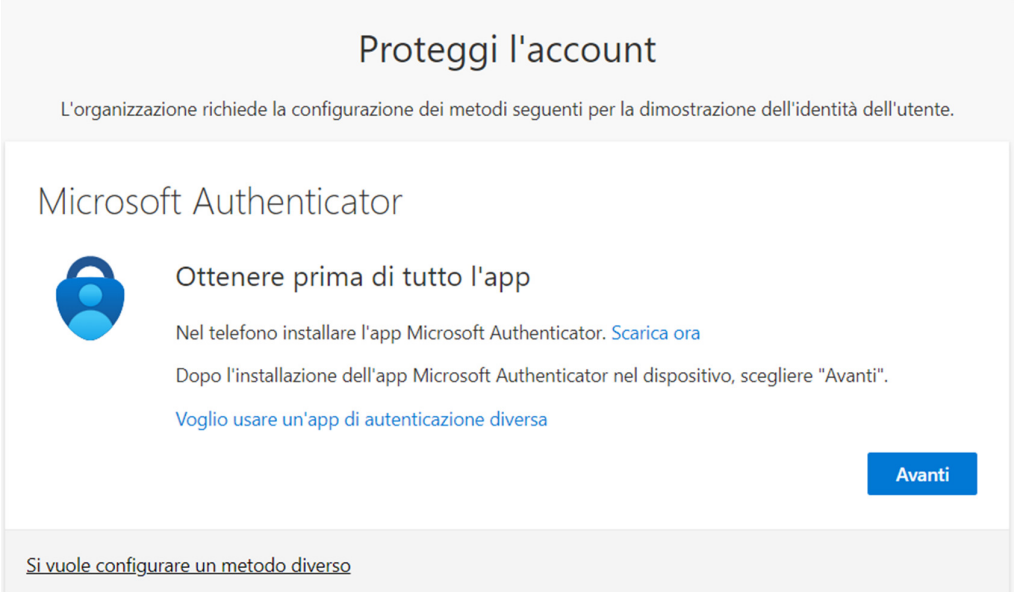
   A. If not already done, download the Microsoft Authenticator application on your smartphone as suggested by the page and click next. Alternatively, it is possible I want to use a different authentication app.

      For Google Authenticator, start the application on your mobile device, click on the "+" icon and then "Scan a QR code". Scan the QR code shown on the screen (see point X of the guide for example), then click on “next” in the browser and enter the 6-digit code generated by Google Authenticator. By clicking on "next" again, the following notification confirms registration;

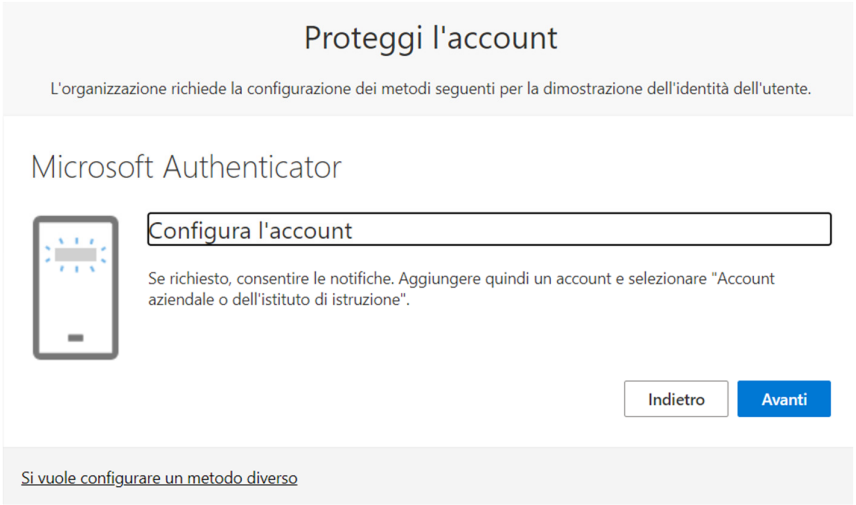
      Example of registration notification

   B. Configure a different authentication method, such as a mobile number, by clicking on the link you want to configure a different method (skip to point XIII).



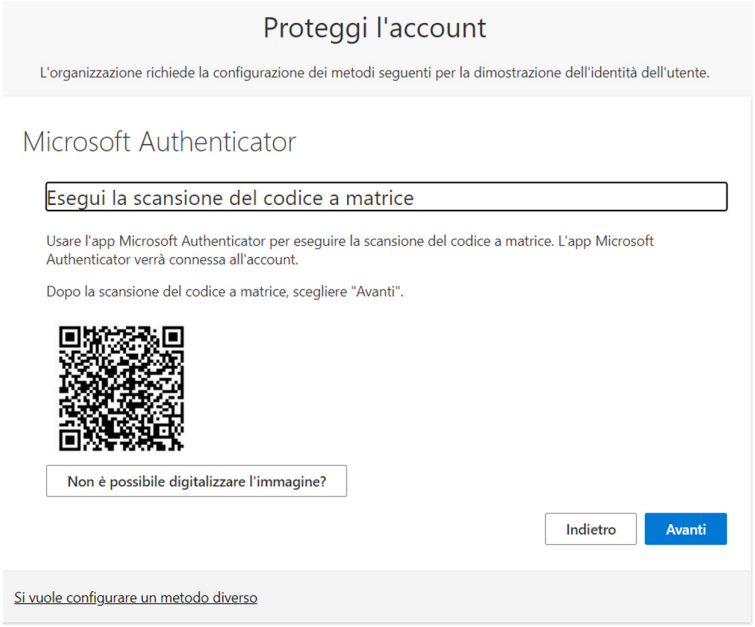
First MFA configuration screen by selecting MS Authenticator (from browser)

VI. **Click <u>Next</u>** on the next screen to start configuring Microsoft Authenticator on your mobile device.



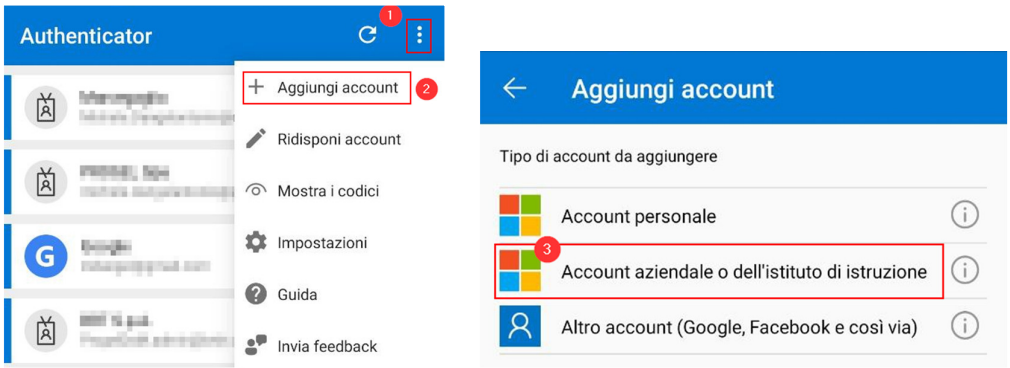
Second MFA configuration screen on browser (MS Authenticator)

VII. Now a screen appears with a QR Code to be framed in the Microsoft Authenticator.



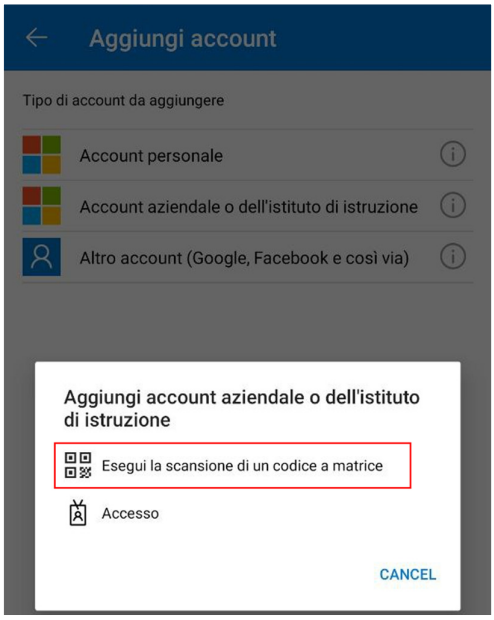
Third browser MFA configuration screen (MS Authenticator)

VIII. Then open the application on your mobile device and click on the button to add an account. In Microsoft Authenticator, click on "**+ add account**" and add a new account of type "**Work or school account**"



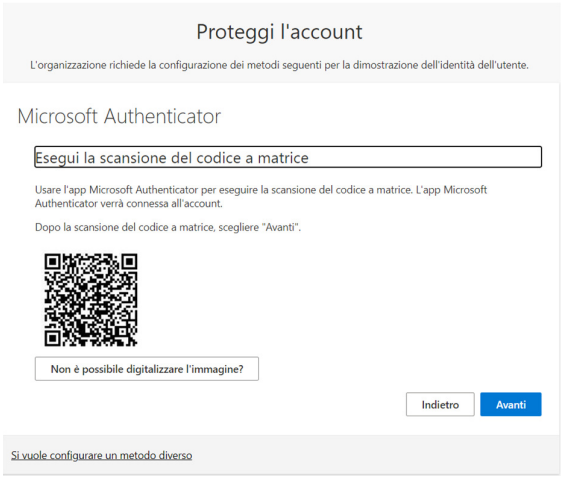
MS Authenticator setup screens on the mobile device

IX. In Microsoft Authenticator, tap on **"Scan a QR code".**



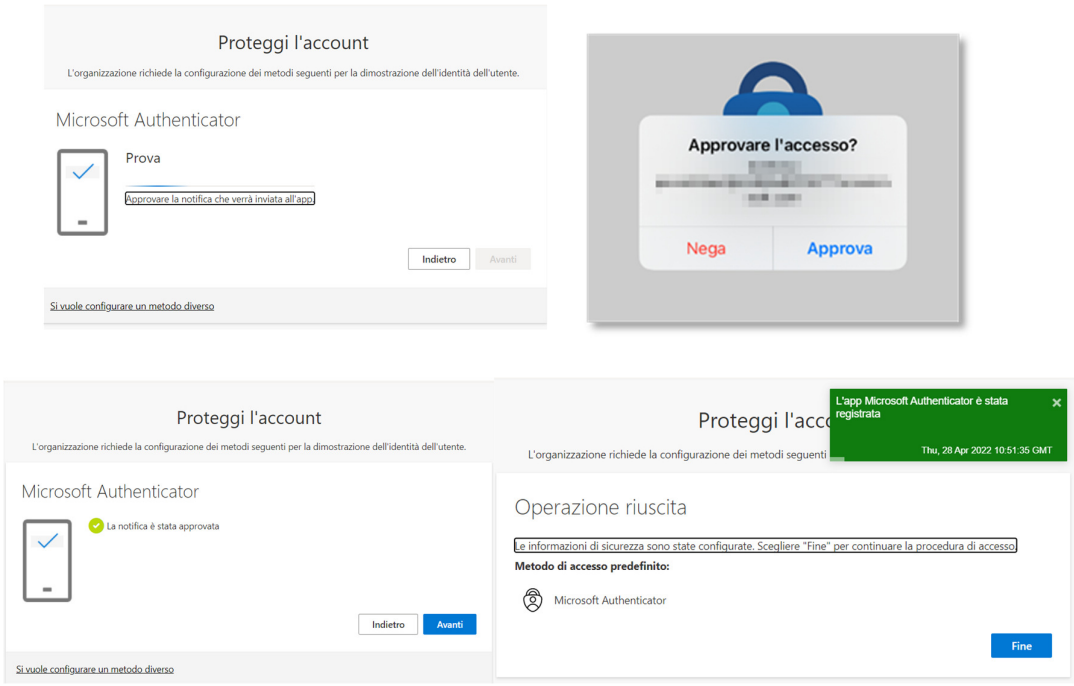
MS Authenticator setup screen on the mobile device

X. Use Microsoft Authenticator (or other authentication app) **to frame the QR code on the PC screen with the camera**.



Fourth screen of MFA configuration on browser (MS Authenticator)

XI. In the case of Microsoft Authenticator, you need to **click Next** to get to the screen waiting for approval of a notification on the mobile application; then approve the notification and check from the PC that everything went well.

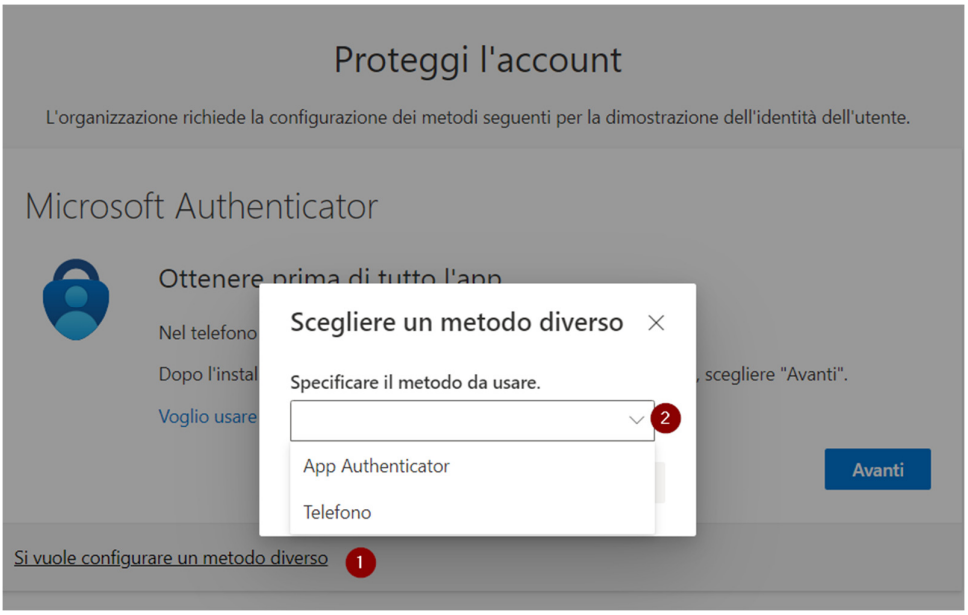


Screens for sending notification from the browser (top left), receiving notification on mobile (top right) and end of configuration confirmations (bottom).

The notification confirms that the setup procedure with MS Authenticator is completed.

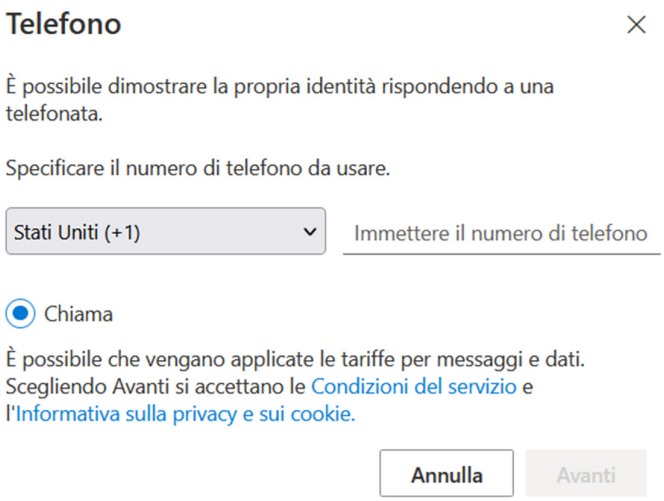
2.2. Configuring a method other than app authenticator

A. To set up a different authentication method, select I want to set up a **different method** and then Phone, Alternate Phone, or Work Phone.



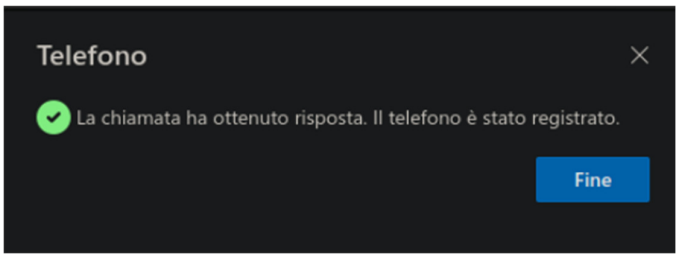
Menu (from browser) with supported MFA mechanisms

B. Enter your mobile number and press next.



Phone number entry screen to receive a call during login

C. You will receive a call asking you to press the # key to confirm the registration.



Registration confirmation screen

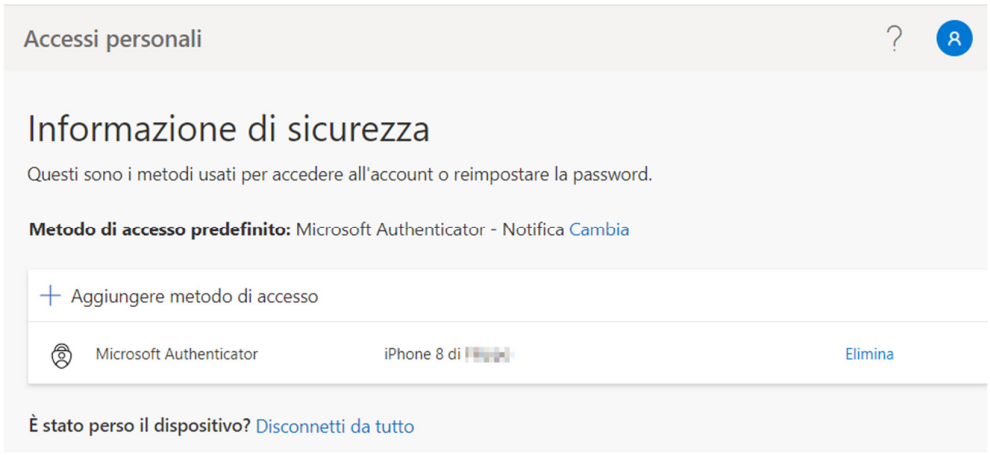
The call verification setup procedure is **completed**.

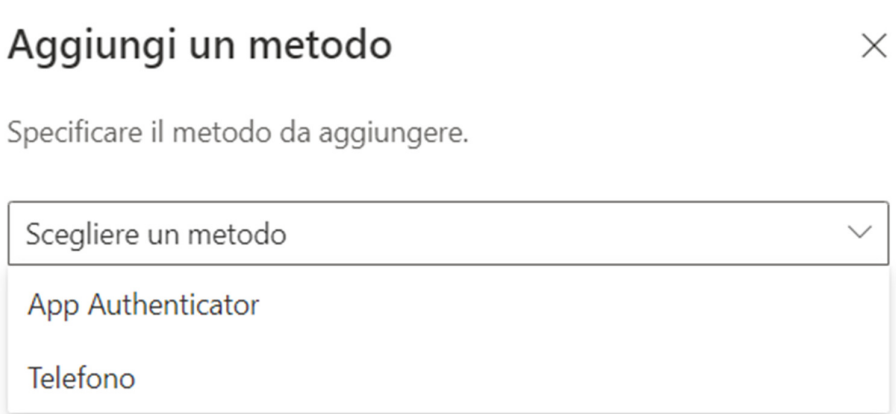
2.3. Additional configuration of the authenticator application or phone number

Once the procedure is completed (mobile application or telephone) you will arrive in a screen where you can add additional verification methods among those supported. Alternatively visit https://mysignins.microsoft.com/security-info by entering with the FBK account.

Continue

- for the authenticator application as indicated in Section 2.1;
- for the telephone number - Section 2.2.



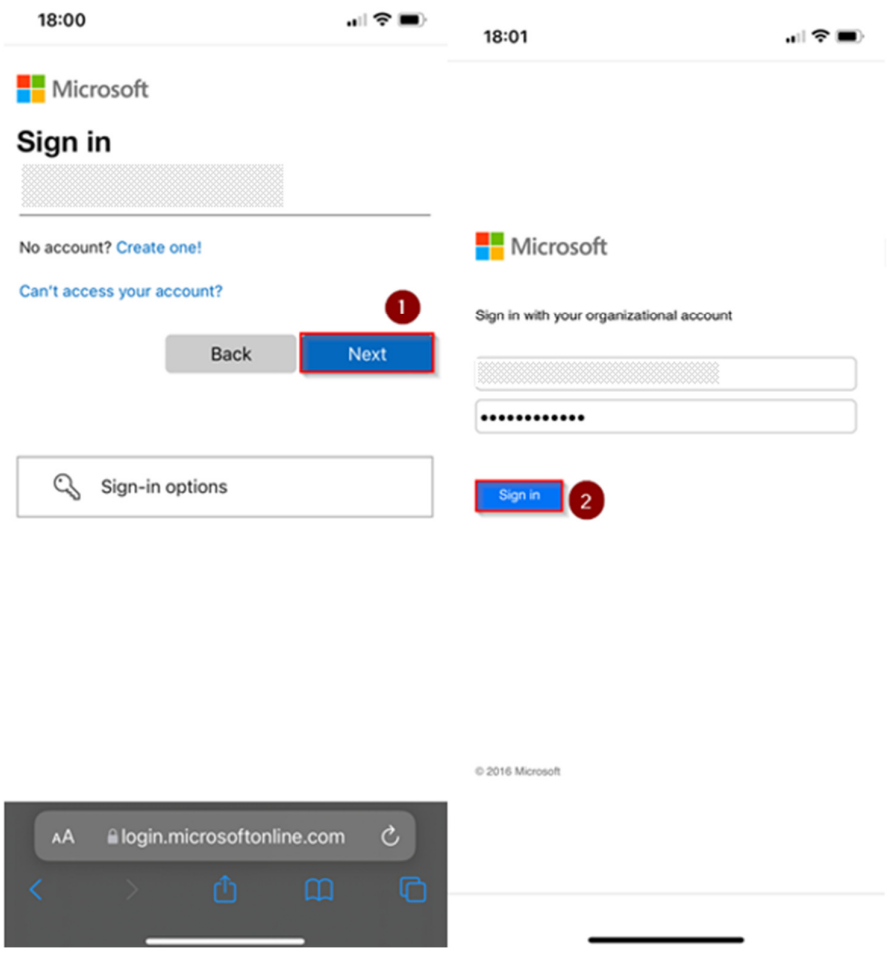


2.4. 2.4. MS Authenticator configuration via smartphone

Below are the steps to follow to register the mobile device as a secondary authentication factor to your FBK account using the mobile phone.

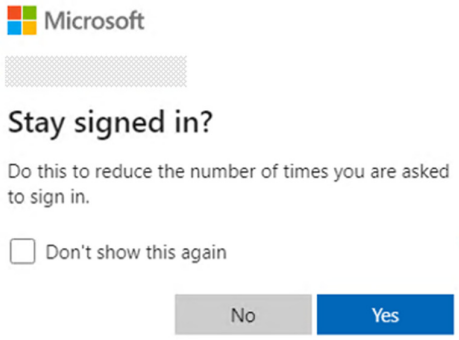
I. **Connect via browser** to the following address: https://aka.ms/mfasetup.

II. If it hasn't already been done, **log in with your user credentials** (FBK account or external account used to access FBK resources).



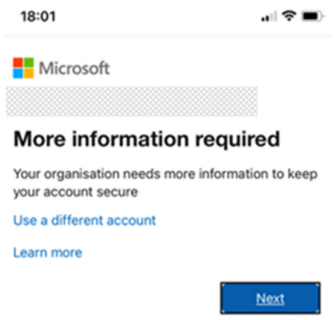
Login screens on the mobile device

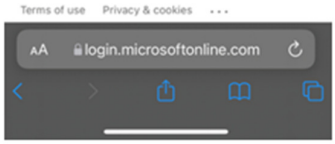
III. If the following screen appears, click on NO if you are connecting from an external wireless / wired network (non-personal or from FBK) or from a non-personal device.



Schermata per la persistenza della sessione

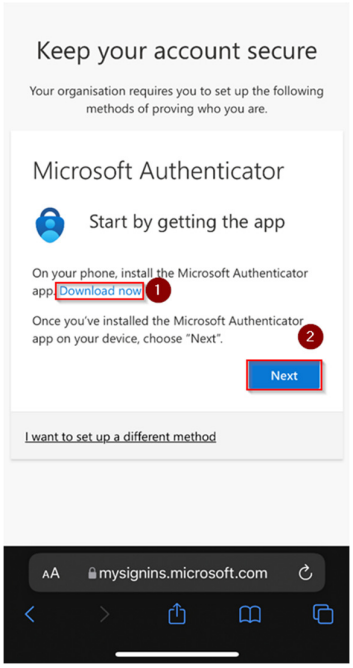
IV. A page will appear asking for additional information to be registered. **Click on next / next:**





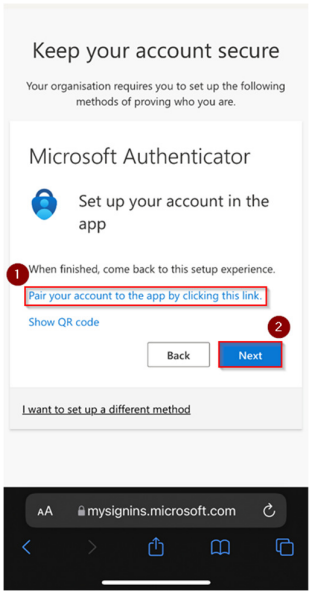
First MS Authenticator configuration screen from mobile device

V. If not already done, download the Microsoft Authenticator application and **click on Next / Next**:



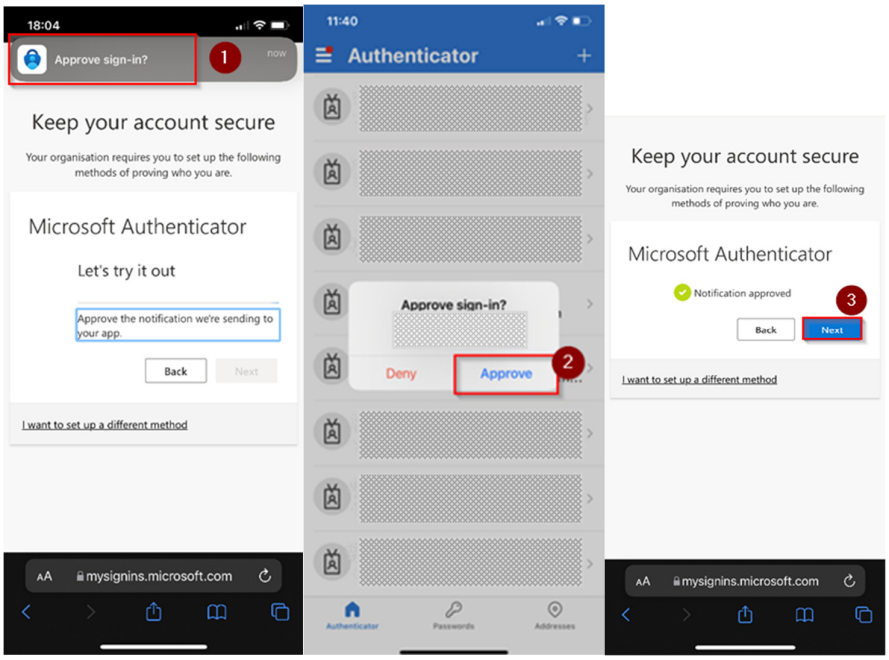
Screen that prompts you to download MS Authenticator

VI. After downloading the app click on "*Pair your account to the app by clicking this link*":



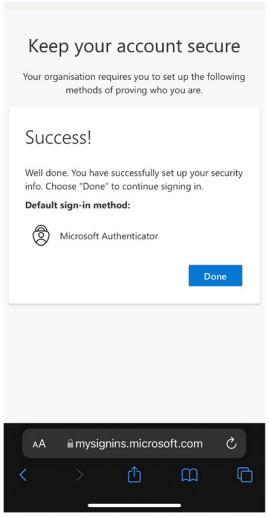
Screen for sending a notification to the MS Authenticator mobile application

VII. From the authenticator app, **approve the authentication request** notification. On the browser screen **click Next**:



Approval and confirmation of the notification for registering MS Authenticator on mobile

VIII. On the next screen **click on Done**:



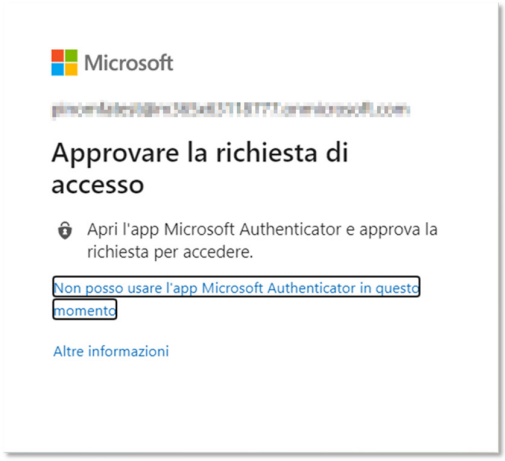
Registration confirmation screen

The setup procedure is completed.

3. User experience from the next sign in

From the next login, after entering the password, the user will be asked to verify their identity with one of the previously configured methods (authenticator application or phone number).

The default method is notification via Microsoft Authenticator, the user will approve the notification on their device and continue with authentication.



Additional factor request screen for authentication

If the user does not want or cannot use the notification on the app, he can click on the link in blue I cannot use the Microsoft Authenticator app at this time to get to the following screen and choose a different verification method (previously configured). If you have no others, please contact help-it@fbk.eu.

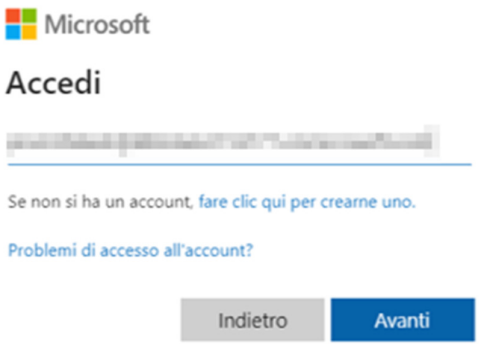
Screen with the MFA mechanisms configured

4. What to do in case of device replacement

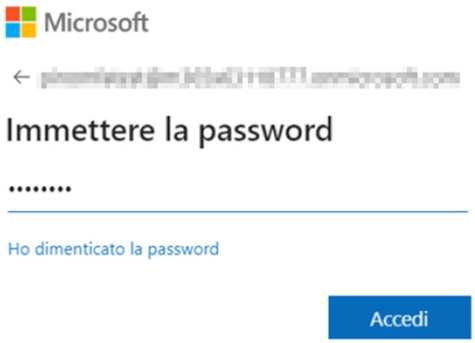
In case of replacement of your mobile device on which the mobile authenticator is installed, you must follow the procedure described here before decommissioning the device. Operations are easier using a PC browser.

I. **Connect via browser** to the following address: https://aka.ms/mfasetup.

II. If it hasn't already been done, **log in with your user credentials** (FBK account or external account used to access FBK resources).

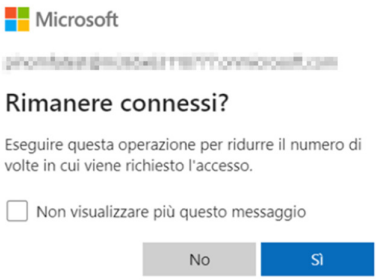


Username entry screen



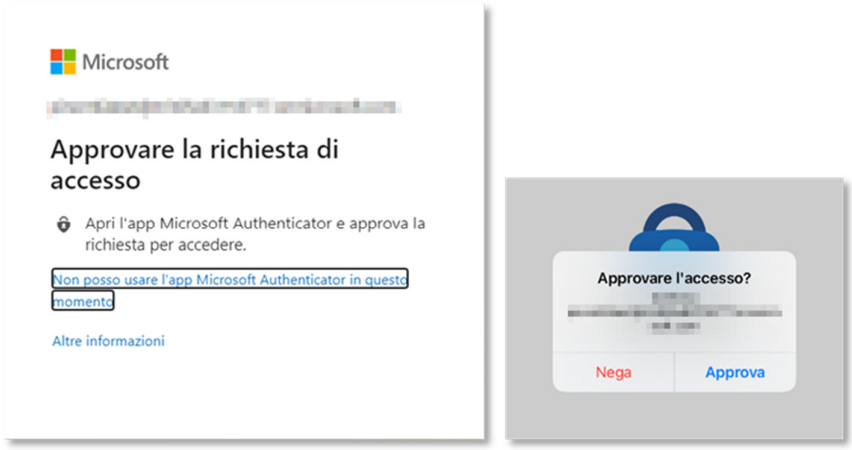
Password entry screen

III. If the following screen appears, click NO if you are connecting from an external wireless / wired network (non-personal or from FBK) or from a non-personal device.



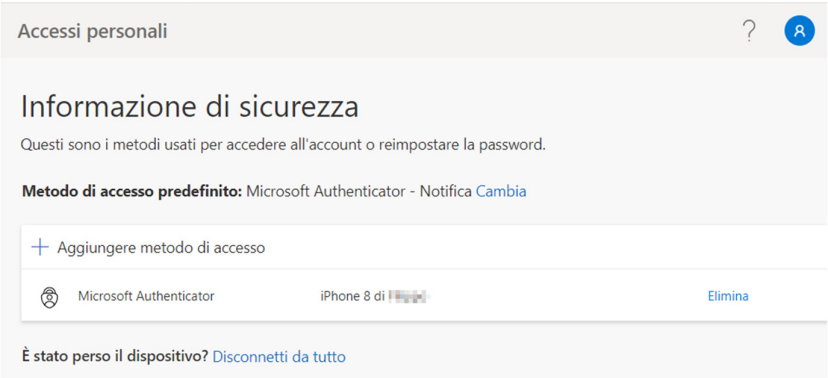
Schermata persistenza sessione

IV. From the Authenticator app, **approve the authentication request notification**:



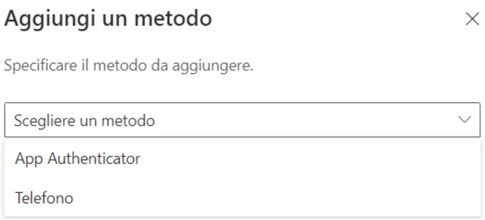
Notification authentication

V. In the page that appears, **click on add login method**:



Screen for adding MFA mechanisms to your account

VI. From the drop-down menu choose another configuration method (we recommend App Authenticator in case of device replacement)



Screen with available mechanisms

Continue with the configuration procedure and once finished, delete the mobile app of the old device using the appropriate **delete button**.

5. What to do if the device is lost

In the event that the device used as the second authentication factor (with the Microsoft Authenticator application) should be lost or otherwise unusable, it is necessary to contact the Help Desk (help-it@fbk.eu). In fact, it is necessary on their part to re-force the request for registration of the second authentication factor.

Once the Help Desk has reset, you can proceed with registering a new authenticator application or phone number; follow the steps in Section 2.