FONDAZIONE
BRUNO KESSLER

MULTI-FACTOR AUTHENTICATION CONFIGURATION

USER GUIDE

Indice

1. Introduction **2**

1.1. Defend yourself from identity theft 3

2. Configuration procedure **4**

2.1. Configuration via PC 4

2.2. Additional configuration of the authenticator application 10

2.3. MS Authenticator configuration via smartphone 11

3. User experience from the next sign in **15**

4. What to do in case of device replacement **15**

5. What to do in case of device's loss **17**

1. Introduction

This document provides the users with the procedure for securing their FBK account using multi-factor authentication[1] - hereinafter referred to as MFA. This allows, according to what was reported by Alex Weinert[2] (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 the incoming data, impersonate the user[3]. We therefore 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 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 from (e.g. using different Wifi networks or connecting with your smartphone);
- For administrative actions on Microsoft Azure cloud with an FBK account;
- To independently reset your FBK password or when Microsoft detects abnormal account behaviour[4];
- When Microsoft detects medium or high risk when authenticating[4].

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). For further information or if you have any problem, please contact help-it@fbk.eu.

Below is explained how to configure MFA with Microsoft Authenticator[5] as a mobile application (from a PC illustrated in Section 2.1, from a smartphone in Section 2.3).

We suggest to configure two authentication methods on two different devices, so that you can access FBK services even in case of theft/loss or replacement of the device.

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

[1] For more details on multi-factor authentication, please refer to the following LINK.
[2] For more information on the types of attacks against password-based authentication, see LINK.
[3] For more information on the types of attacks against multi-factor authentication and possible defenses, see LINK.
[4] For behaviors that Microsoft considers at risk during authentication (*Sign-in risk*) or use of the account (*User risk*), refer to LINK.
[5] To configure a different authentication mobile app (e.g. Google Authenticator), select "I want to use a different authentication app" (Point 2.1 V of the Guide).

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] observes the access credentials, anticipating it in the login.

Detection: login failure; receiving notification by email, SMS or mobile application of a new device's or location's access.
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"[6] 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] obtains the access credentials and the 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 (e.g. use an antivirus solution);
(POST) promptly log out of unrecognized sessions and devices - LINK Google, LINK Microsoft.

4. [Remotely] enters into communications between user and server and steals cookies[7].

Detection: even if the lock icon shown by the browser[8] and the details (by clicking on them) show that the connection is secure/reliable[9], 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.
As explained by Microsoft (LINK), there are attack modes whereby the user is not able to distinguish the malicious login experience from that intended: except for the URL, all logos, their location and text (both Google/Microsoft, and any interface customizations introduced by FBK); in addition, if the attack is made through a malicious email[10], an attacker could be able to pre-fill the username field to further mislead the user. Finally, unlike attack #1, the user can access the

[6] The latest recommendations (SP 800-63B) from the National Institute of Standards and Technologies (NIST) recommend a password that is at least 8 characters long (up to 64) and easy to remember (do not force the use of lowercase, uppercase or special characters); obviously, not trivial (e.g., range 1 to 10, *first name, surname and similar*).

[7] 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.

[8] For more details, please refer to LINK Safari, LINK Chrome, LINK Firefox, LINK Edge.

[9] Typically, a rogue attacker uses a server with a valid certificate that also allows connections considered safe by the browser being used.

[10] To learn more about phishing, visit LINK.

requested service, and the portals of Google and Microsoft cannot detect the attacker's login (never happened since it steals the active session of the user).
Possible Mitigations: (PRE) use a hardware key (ex. YubiKey) and check the emails sent by Google/Microsoft as reported in LINK - e.s. "signed by" field with value "accounts.google.com" or "accountprotection.microsoft.com".
(POST) Check the rules set in your email (LINK).

2. Configuration procedure

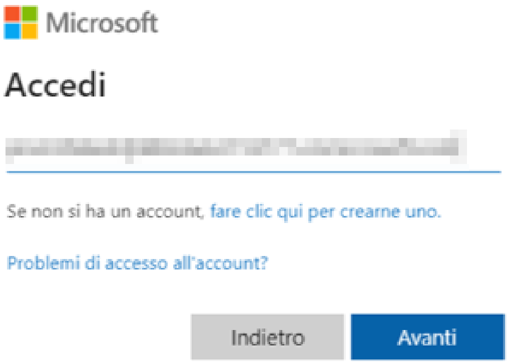
This procedure guides the user in configuring the Microsoft Authenticator app as an additional authentication factor, in order to protect the FBK account.

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 you haven't already done it, **log in with your user credentials**.

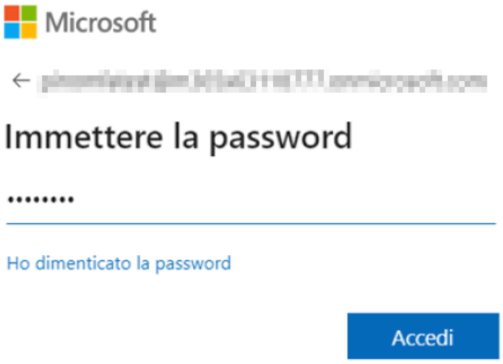


Accedi

[redacted]

Se non si ha un account, fare clic qui per crearne uno.

Problemi di accesso all'account?



← [redacted]

Immettere la password

••••••••

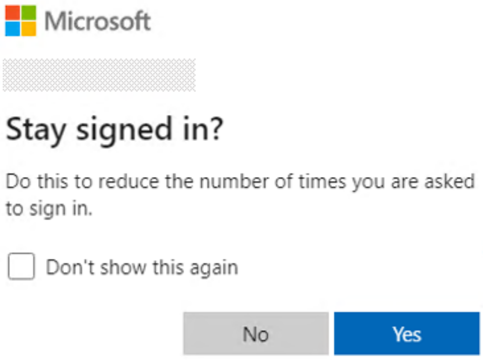
Ho dimenticato la password

Username entry screen

Password entry screen

(email address)

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.



[redacted]

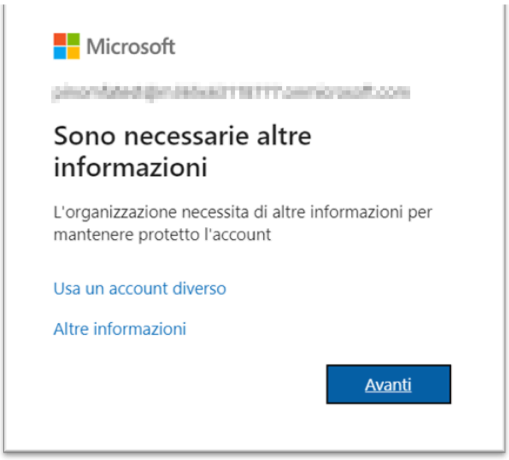
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

Session persistence screen

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



Microsoft

[redacted]

Sono necessarie altre informazioni

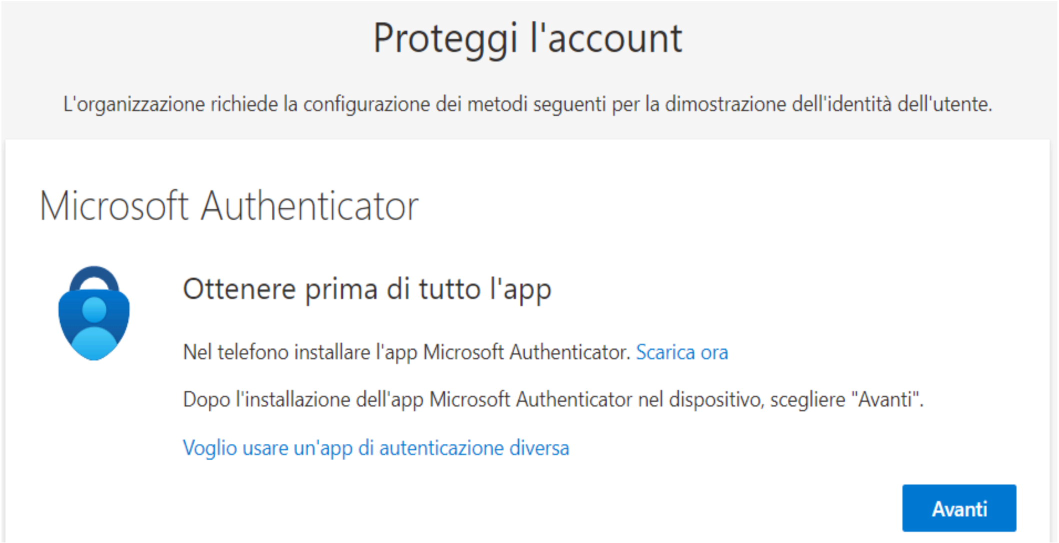
L'organizzazione necessita di altre informazioni per mantenere protetto l'account

Usa un account diverso

Altre informazioni

Screen informing you of the need to set up MFA

V. If you haven't already done it, download the Microsoft Authenticator application on your smartphone as suggested by the page and **click *Next***.



Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator

Ottenere prima di tutto l'app

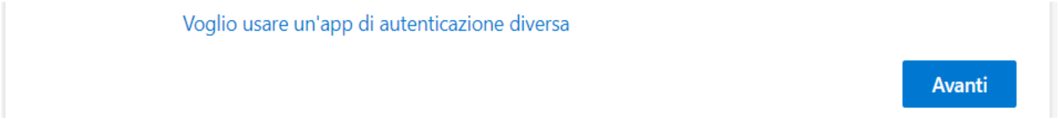
Nel telefono installare l'app Microsoft Authenticator. Scarica ora

Dopo l'installazione dell'app Microsoft Authenticator nel dispositivo, scegliere "Avanti".

Voglio usare un'app di autenticazione diversa

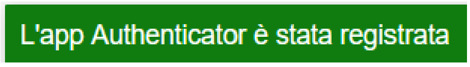
First MFA configuration screen by selecting MS Authenticator (from browser)

Alternatively, you can use an authentication application other than Microsoft Authenticator: in this case click on ***I want to use a different authentication app***.



Voglio usare un'app di autenticazione diversa

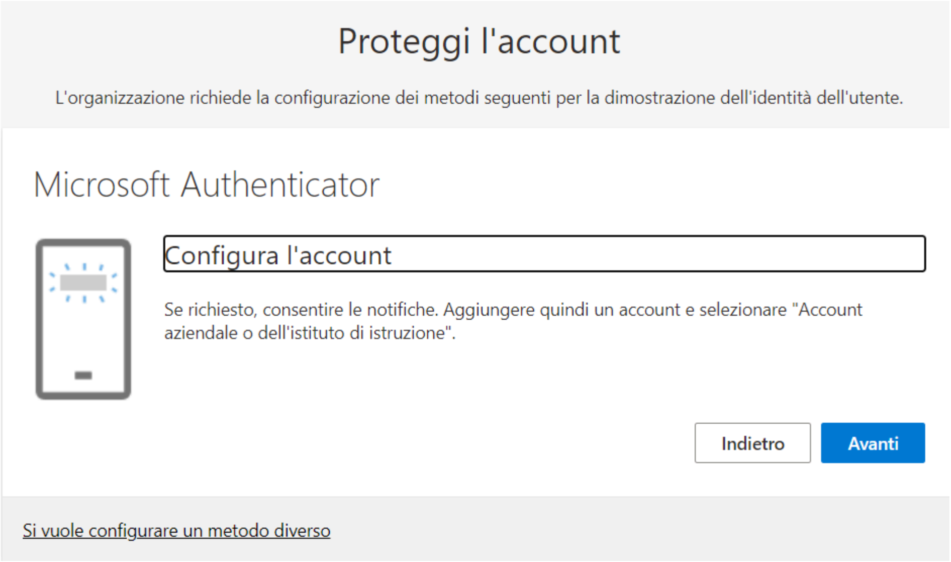
For Google Authenticator, start the application on your mobile device, click on the "+" icon and then "Scan a QR code". Scan the QR code shown on the screen, then click on “next” in the browser and enter the 6-digit code generated by Google Authenticator. By clicking on "next" again, the following notification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



L'app Authenticator è stata registrata

Example of registration notification

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



Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

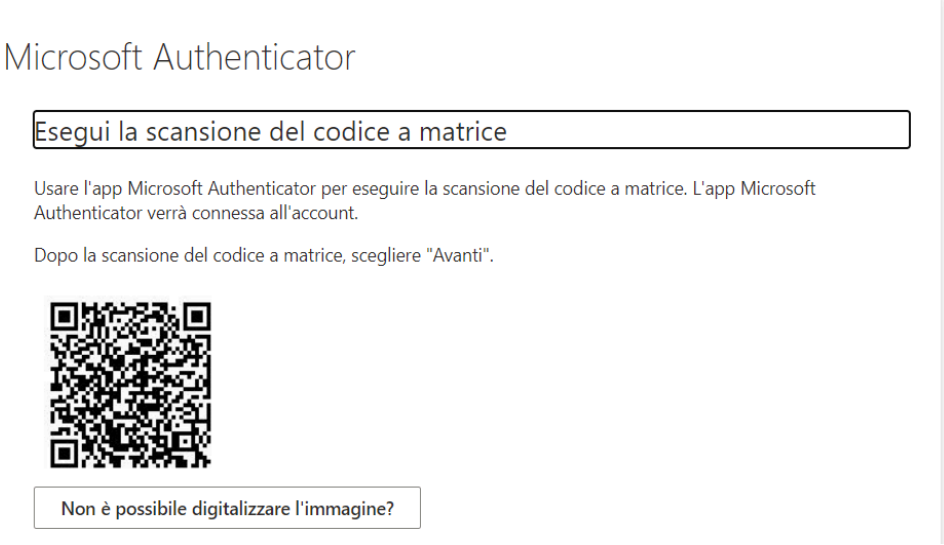
Microsoft Authenticator

Configura l'account

Se richiesto, consentire le notifiche. Aggiungere quindi un account e selezionare "Account aziendale o dell'istituto di istruzione".

Second MFA configuration screen on browser (MS Authenticator)

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



Microsoft Authenticator

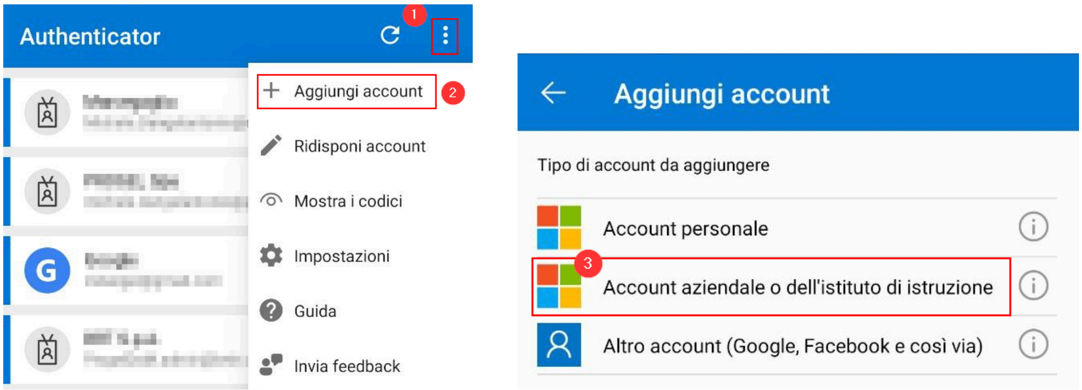
Esegui la scansione del codice a matrice

Usare l'app Microsoft Authenticator per eseguire la scansione del codice a matrice. L'app Microsoft Authenticator verrà connessa all'account.

Dopo la scansione del codice a matrice, scegliere "Avanti".

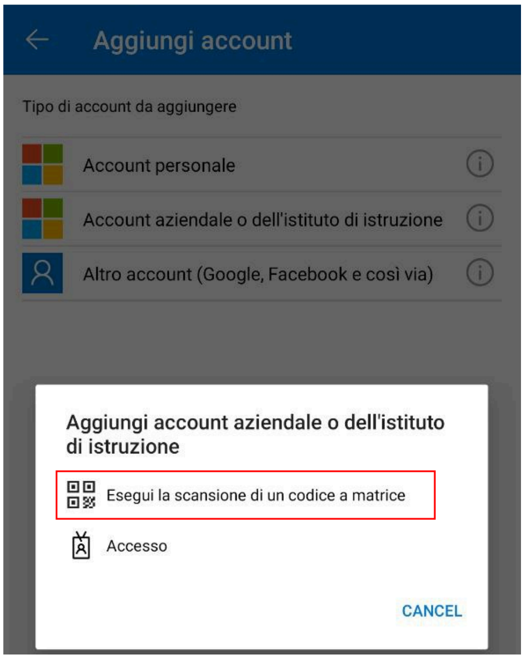
Third browser MFA configuration screen (MS Authenticator)

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 type "***Work or school account***"



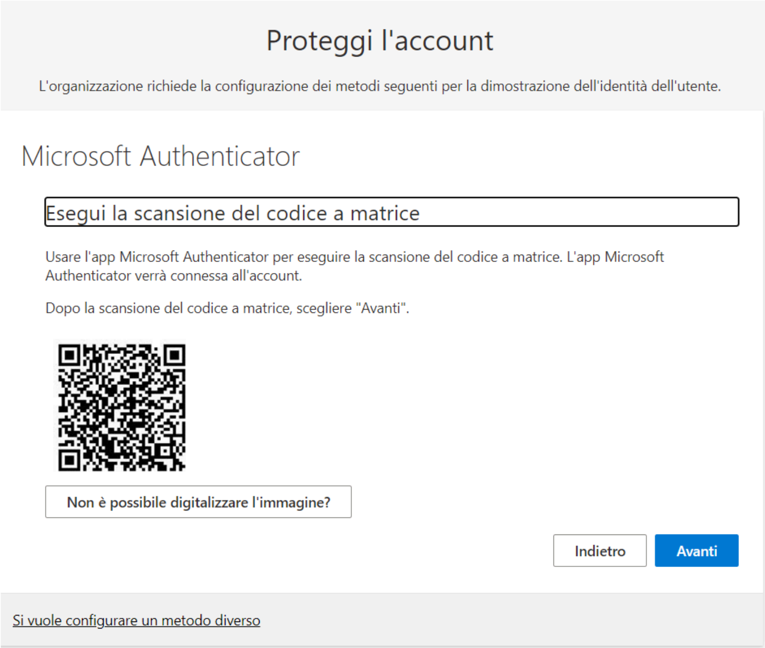
MS Authenticator setup screens on the mobile device

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


Aggiungi account
Tipo di account da aggiungere
Account personale
Account aziendale o dell'istituto di istruzione
Altro account (Google, Facebook e così via)
Aggiungi account aziendale o dell'istituto di istruzione
Esegui la scansione di un codice a matrice
Accesso
CANCEL

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**.



Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator

Esegui la scansione del codice a matrice

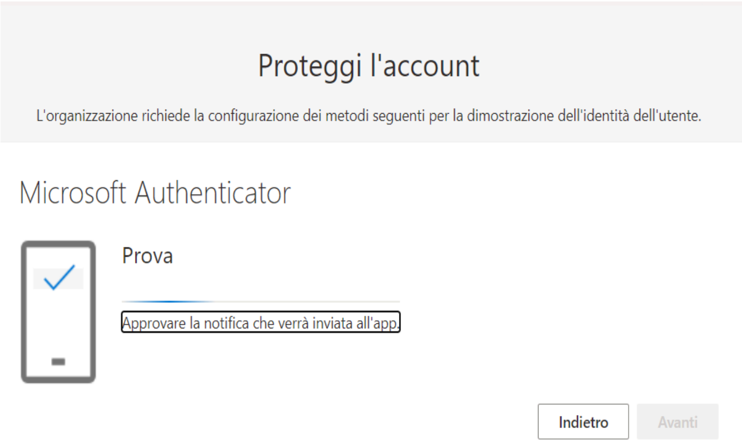
Usare l'app Microsoft Authenticator per eseguire la scansione del codice a matrice. L'app Microsoft Authenticator verrà connessa all'account.

Dopo la scansione del codice a matrice, scegliere "Avanti".

Non è possibile digitalizzare l'immagine?
Indietro
Avanti
Si vuole configurare un metodo diverso

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 through a notification on the mobile application (OTP numeric code); then approve the notification and check from the PC that the operation has been successful.



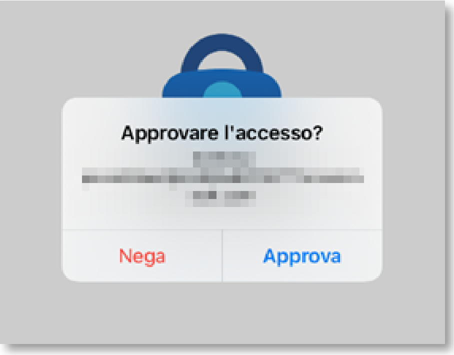
Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

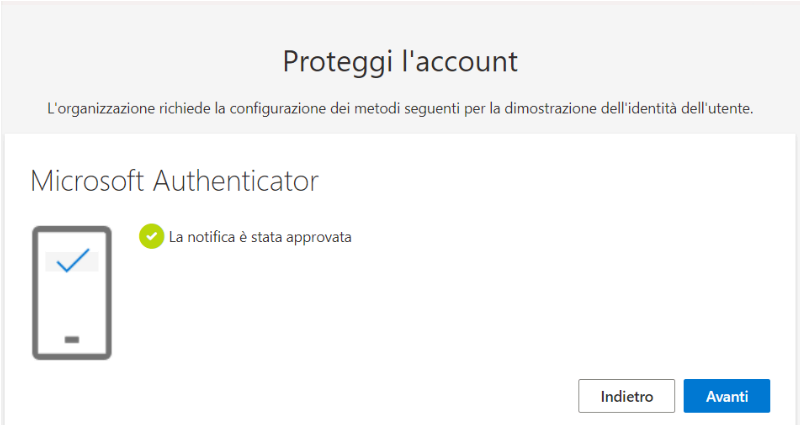
Microsoft Authenticator

Prova

Approvare la notifica che verrà inviata all'app.



Approvare l'accesso?

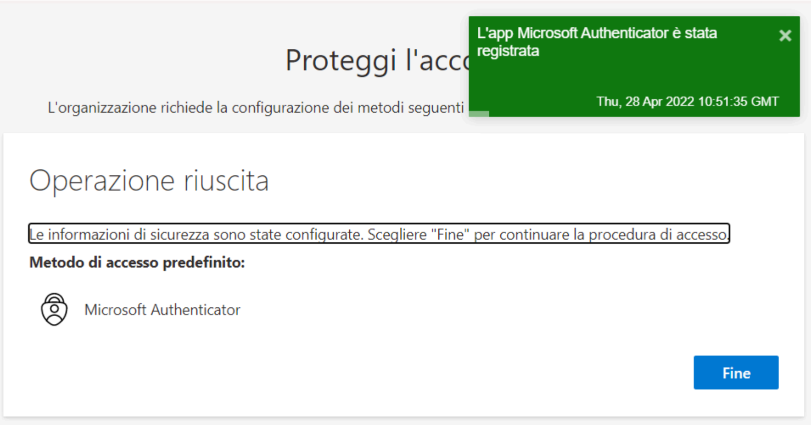


Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator

✓ La notifica è stata approvata



Proteggi l'acc

L'organizzazione richiede la configurazione dei metodi seguenti

L'app Microsoft Authenticator è stata registrata

Thu, 28 Apr 2022 10:51:35 GMT

Operazione riuscita

Le informazioni di sicurezza sono state configurate. Scegliere "Fine" per continuare la procedura di accesso.

Metodo di accesso predefinito:

Microsoft Authenticator

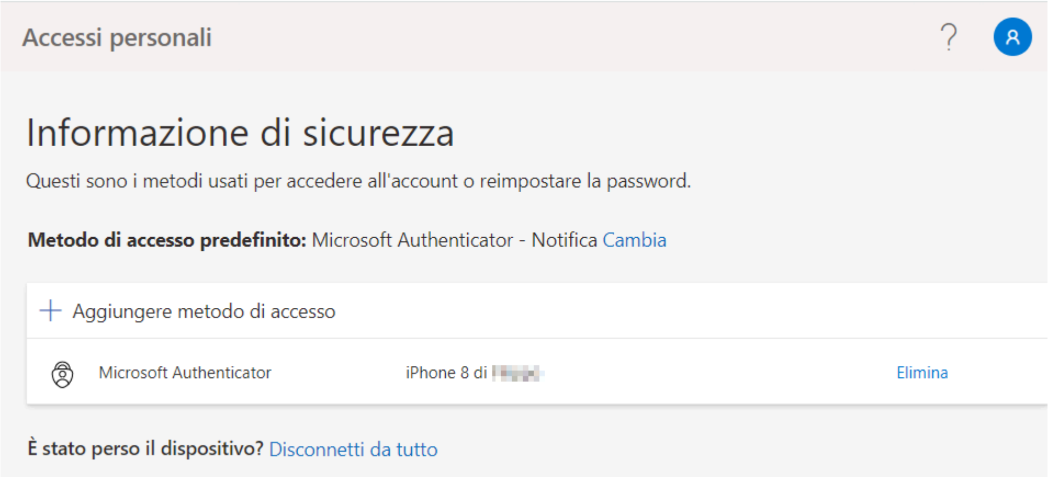
Screens for sending notification from the browser (top left), receiving notification on mobile (top right) and end of configuration confirmations (bottom).

The notification confirms that the setup procedure with MS Authenticator has been **completed**.

2.2. Additional configuration of the authenticator application

Once the procedure is completed (mobile application) the screen shows that you can add additional verification methods among those supported.
Alternatively visit https://mysignins.microsoft.com/security-info entering with the FBK account.

Continue for the authenticator application as indicated in Section 2.1;



Accessi personali

Informazione di sicurezza

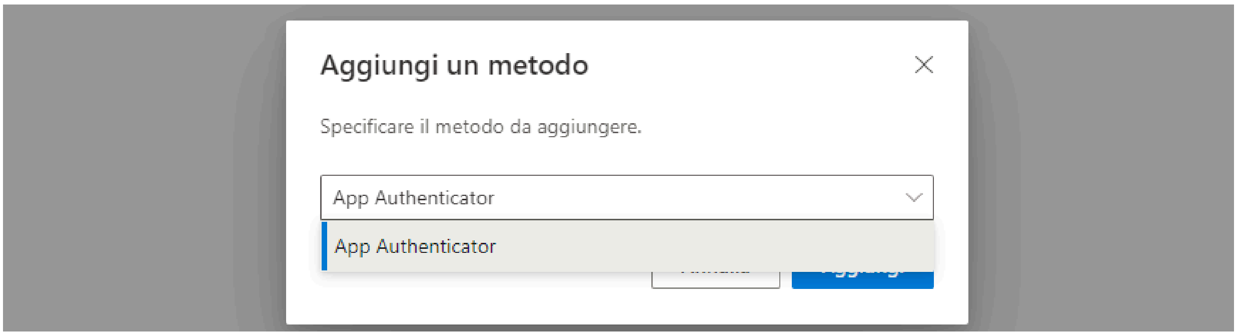
Questi sono i metodi usati per accedere all'account o reimpostare la password.

Metodo di accesso predefinito: Microsoft Authenticator - Notifica Cambia

+ Aggiungere metodo di accesso

Microsoft Authenticator	iPhone 8 di [redacted]	Elimina

È stato perso il dispositivo? Disconnetti da tutto

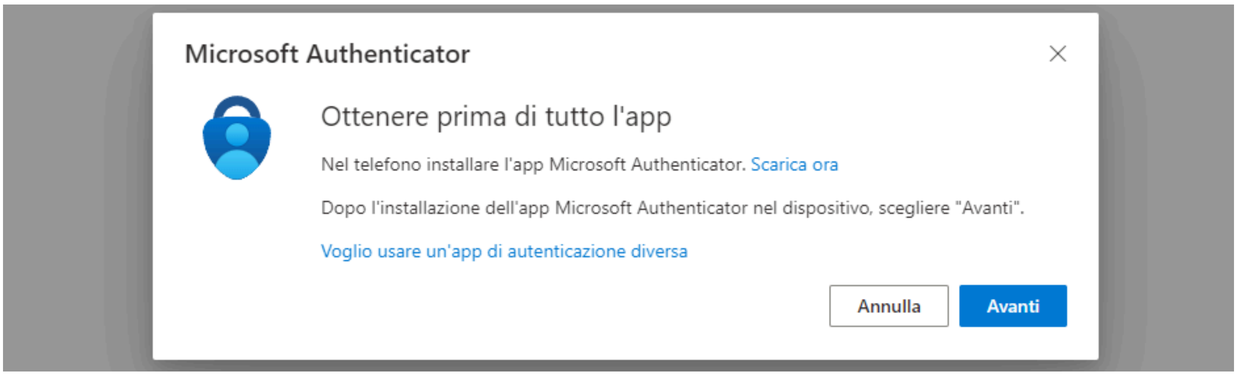


Aggiungi un metodo

Specificare il metodo da aggiungere.

App Authenticator

App Authenticator



Microsoft Authenticator

Ottenere prima di tutto l'app

Nel telefono installare l'app Microsoft Authenticator. Scarica ora

Dopo l'installazione dell'app Microsoft Authenticator nel dispositivo, scegliere "Avanti".

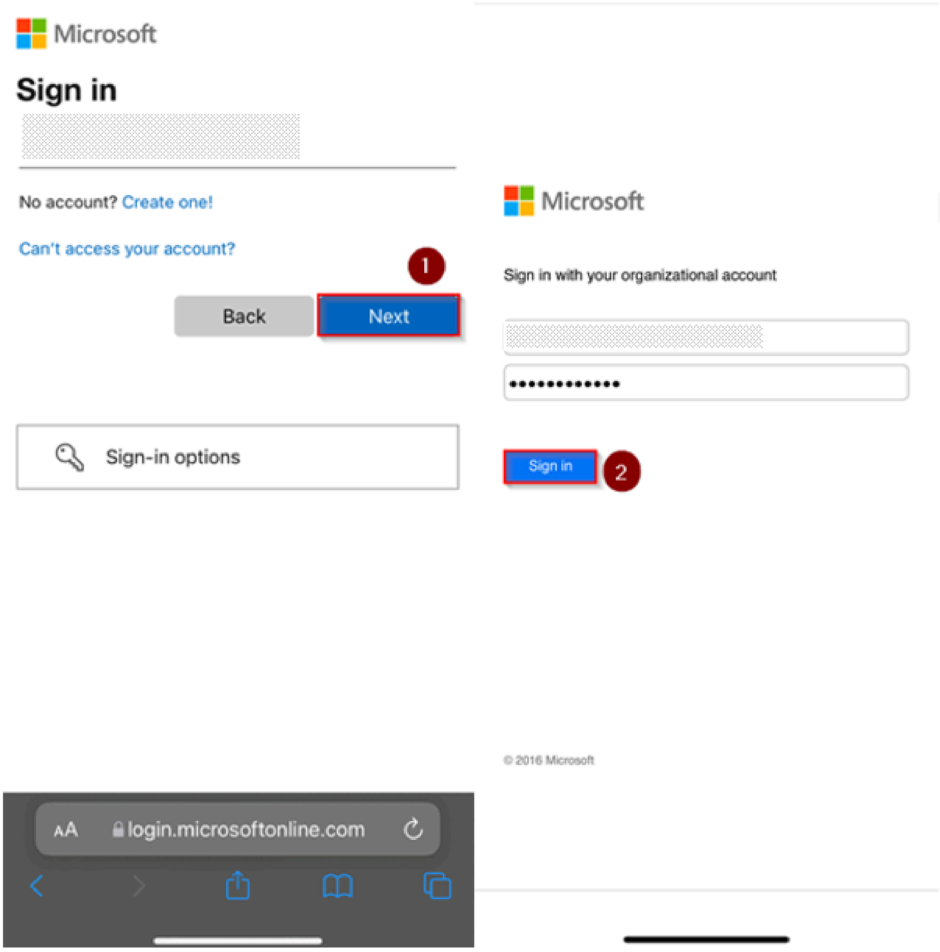
Voglio usare un'app di autenticazione diversa

2.3. MS Authenticator configuration via smartphone

Below you find 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 you haven't already done it, **log in with your user credentials** (FBK account or external account used to access FBK resources).



Sign in

[redacted]

No account? Create one!

Can't access your account?

login.microsoftonline.com

Sign in with your organizational account

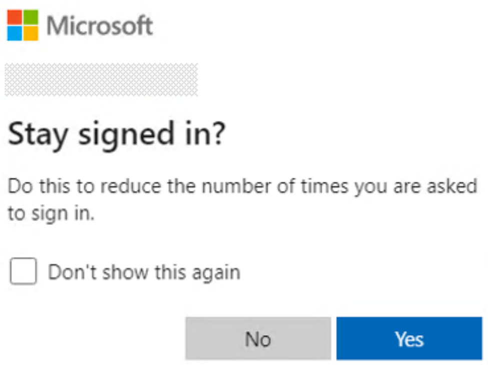
[redacted]

•••••••••••••

© 2016 Microsoft

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.



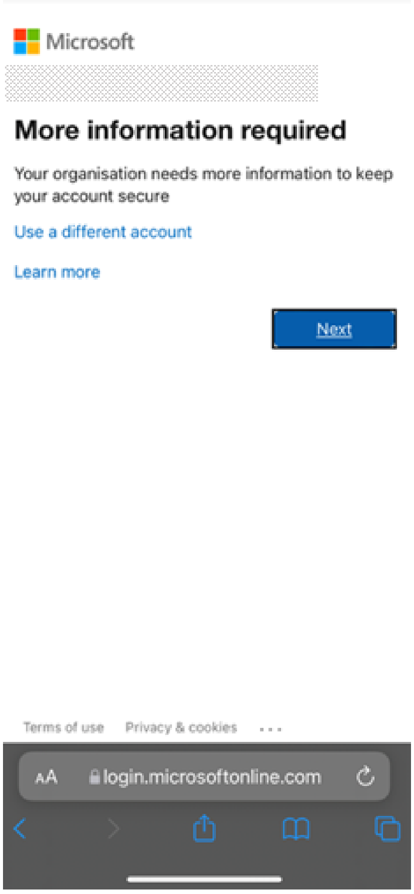
Microsoft

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

Session persistence screen

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



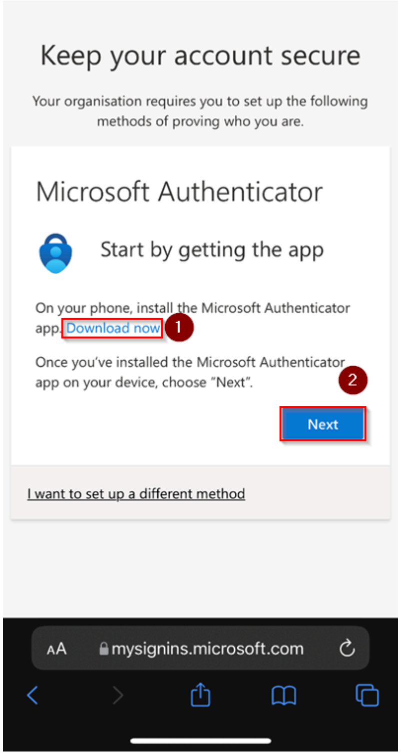
Microsoft

More information required

Your organisation needs more information to keep your account secure

First MS Authenticator configuration screen from mobile device

V. If you haven't already done it, download the Microsoft Authenticator application and **click *Next***:



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

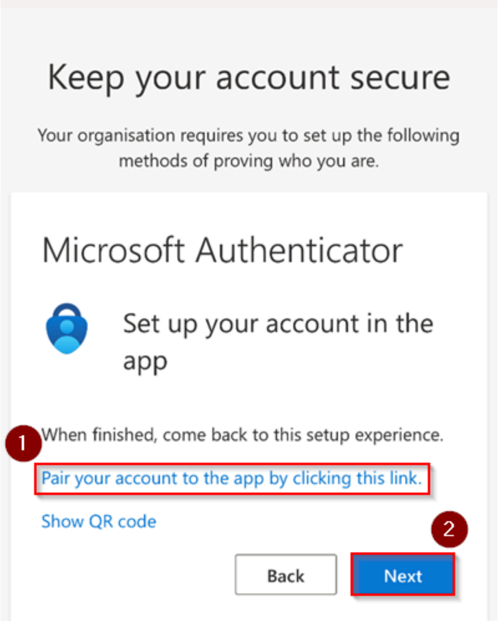
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

Once you've installed the Microsoft Authenticator app on your device, choose "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*":



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

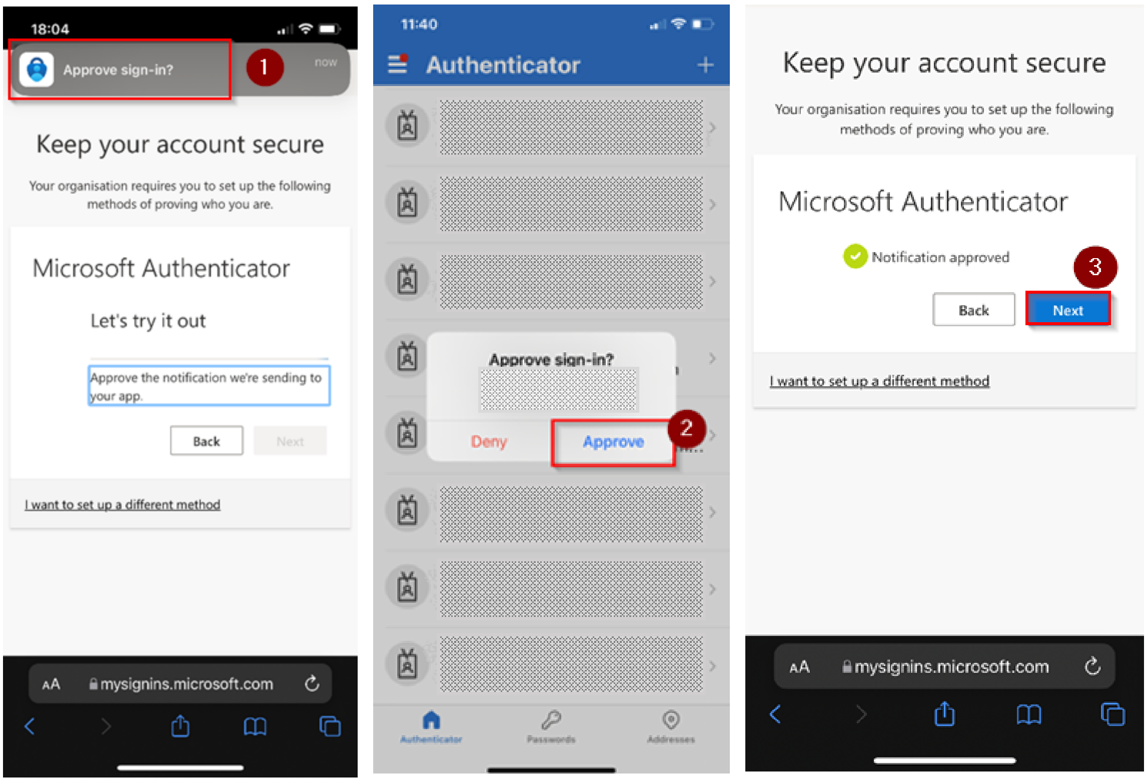
Set up your account in the app

When finished, come back to this setup experience.

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 then **click *Next***:



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Let's try it out

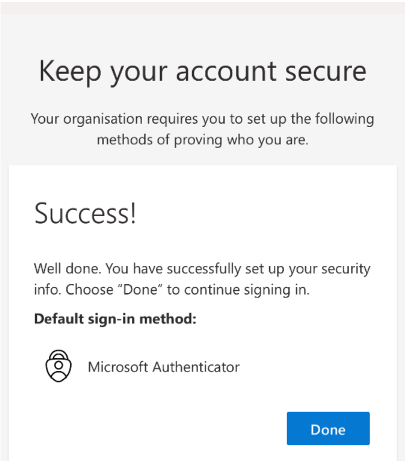
Approve the notification we're sending to your app.

Notification approved

I want to set up a different method

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

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



Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Success!

Well done. You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

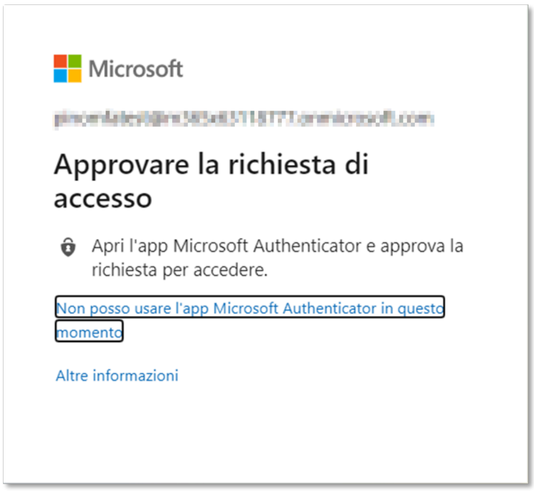
Registration confirmation screen

The setup procedure has been **completed**.

3. User experience from the next sign in

From the next login, after entering the password, the users will be asked to verify their identity with one of the previously configured methods.

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



Microsoft

[redacted]

Approvare la richiesta di accesso

Apri l'app Microsoft Authenticator e approva la richiesta per accedere.

Non posso usare l'app Microsoft Authenticator in questo momento

Altre informazioni

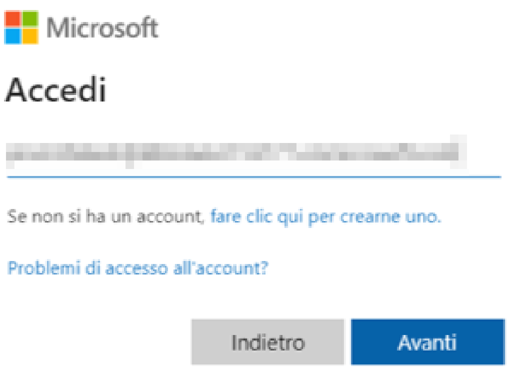
Additional factor request screen for authentication

4. What to do in case of device replacement

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

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

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



Microsoft

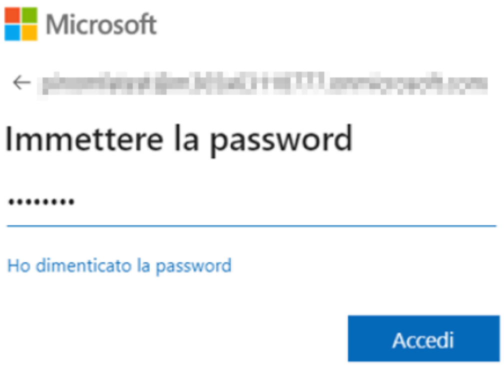
Accedi

[redacted]

Se non si ha un account, fare clic qui per crearne uno.

Problemi di accesso all'account?

Username entry screen



Microsoft

← [redacted]

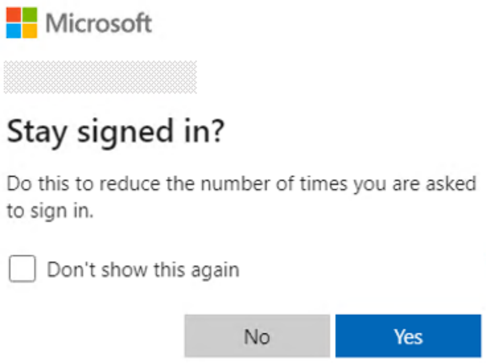
Immettere la password

••••••••

Ho dimenticato la password

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.



Microsoft

[redacted]

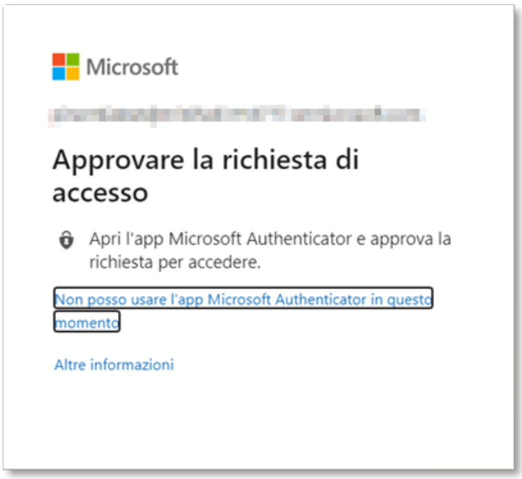
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Session persistence screen

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



Microsoft

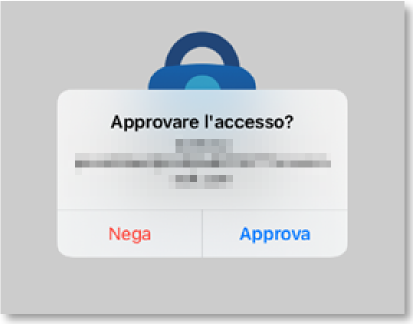
[redacted]

Approvare la richiesta di accesso

Apri l'app Microsoft Authenticator e approva la richiesta per accedere.

Non posso usare l'app Microsoft Authenticator in questo momento

Altre informazioni

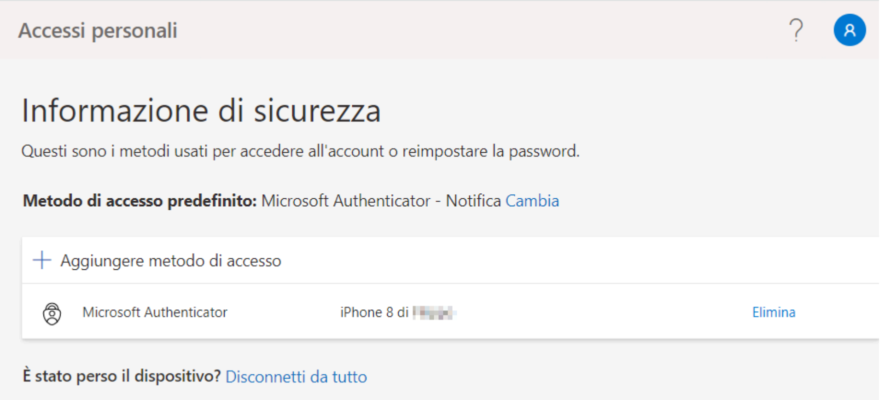


Approvare l'accesso?

[redacted]

Authentication's notification

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



Accessi personali

Informazione di sicurezza

Questi sono i metodi usati per accedere all'account o reimpostare la password.

Metodo di accesso predefinito: Microsoft Authenticator - Notifica Cambia

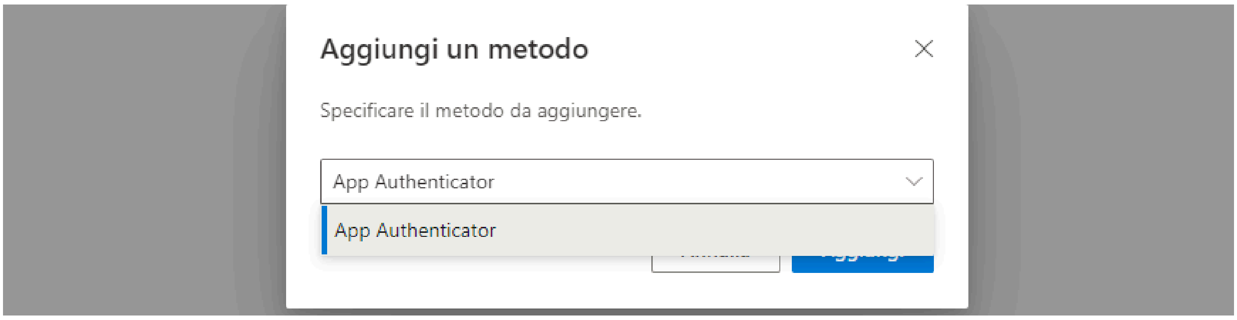
+ Aggiungere metodo di accesso

Microsoft Authenticator iPhone 8 di [redacted] Elimina

È stato perso il dispositivo? Disconnetti da tutto

Screen for adding MFA mechanisms to your account

VI. From the drop-down menu choose another configuration method



Aggiungi un metodo

Specificare il metodo da aggiungere.

App Authenticator

Screen with available mechanisms

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

5. What to do in case of device’s loss

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

Once the Help Desk has reset it, you can proceed with registering a new authenticator application for MFA, following the steps in Section 2.