ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

AREA
SISTEMI E SERVIZI
INFORMATICI

Attivazione dell’autenticazione a più fattori (MFA)

Ultimo aggiornamento 13/07/2026

Sommario

1. Introduzione 2
2. Attivazione di MFA 3
3. Installazione e configurazione di Microsoft Authenticator 7
4. Aggiunta di ulteriori metodi di accesso 10

1. Introduzione

L'autenticazione a più fattori (MFA, acronimo di Multi Factor Authentication) è necessaria per aumentare il livello di sicurezza delle credenziali istituzionali e consiste nell'introduzione di un secondo elemento di autenticazione in aggiunta alla password personale. Il suo utilizzo rientra tra gli obblighi previsti dalla **direttiva (UE) 2022/2555 (NIS 2)**.

Il secondo fattore può essere, ad esempio:

- una notifica inviata alla app Microsoft Authenticator installata nello smartphone
- un codice ricevuto via SMS al numero di telefono indicato durante la procedura di attivazione
- la risposta ad una chiamata automatica al numero di telefono indicato durante la procedura di attivazione

Il secondo fattore non viene richiesto ad ogni accesso ma solo periodicamente, oppure quando si accede ai servizi da una postazione o da un luogo diversi da quelli abituali.

Viene richiesto, ad esempio:

- al primo accesso a ogni applicazione Microsoft dopo l'attivazione
- al primo accesso a ogni applicazione Microsoft su una nuova postazione
- al primo accesso ad una applicazione Microsoft nella versione web (es. casella di posta, OneDrive…). Se dopo l'autenticazione, alla richiesta di "rimanere connessi", si risponde "No", il secondo fattore viene chiesto anche all'accesso successivo.

Una volta completata la procedura di attivazione illustrata nella presente guida (par. 2. "Attivazione di MFA") sarà possibile utilizzare l'autenticazione a più fattori inserendo il codice ricevuto via SMS al numero di telefono indicato durante la procedura di attivazione.

Poiché la app Microsoft Authenticator è il metodo che garantisce il livello di protezione più elevato, dopo l'attivazione di MFA si raccomanda di procedere alla configurazione di questa modalità di autenticazione a due fattori (par. 3 "Installazione e configurazione di Microsoft Authenticator").

La presenza di almeno due modalità di generazione del codice diverse è inoltre raccomandata per evitare possibili difficoltà di accesso qualora un metodo non sia disponibile.

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

2. Attivazione di MFA

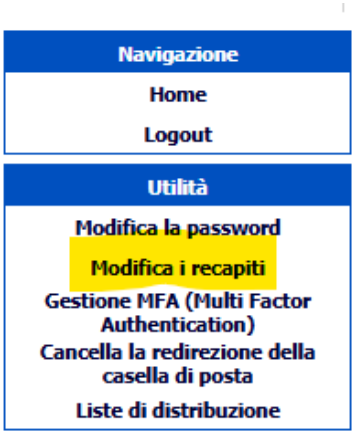
Collegarsi alla pagina www.dsa.unibo.it, fare click su **LOGIN**.

Autenticarsi con la propria identità digitale SPID o CIE: l'utilizzo di SPID o CIE è necessario per avere una garanzia forte dell'identità di chi esegue l'operazione.

Per i titolari sia di un account @unibo.it sia di un account @studio.unibo.it, fare click sul pulsante **LOGIN** in corrispondenza dell'account @unibo.it:

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

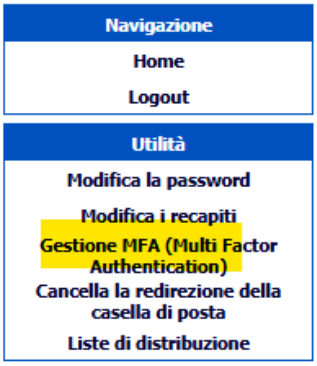
Fare click sulla voce **Modifica i recapiti**.



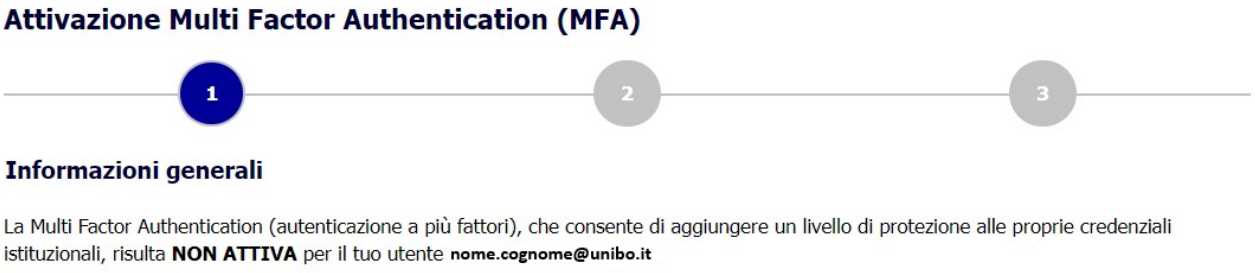
Verificare la correttezza del numero di cellulare privato: se necessario, aggiornarlo e validarlo e quindi fare click su **Conferma**.

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

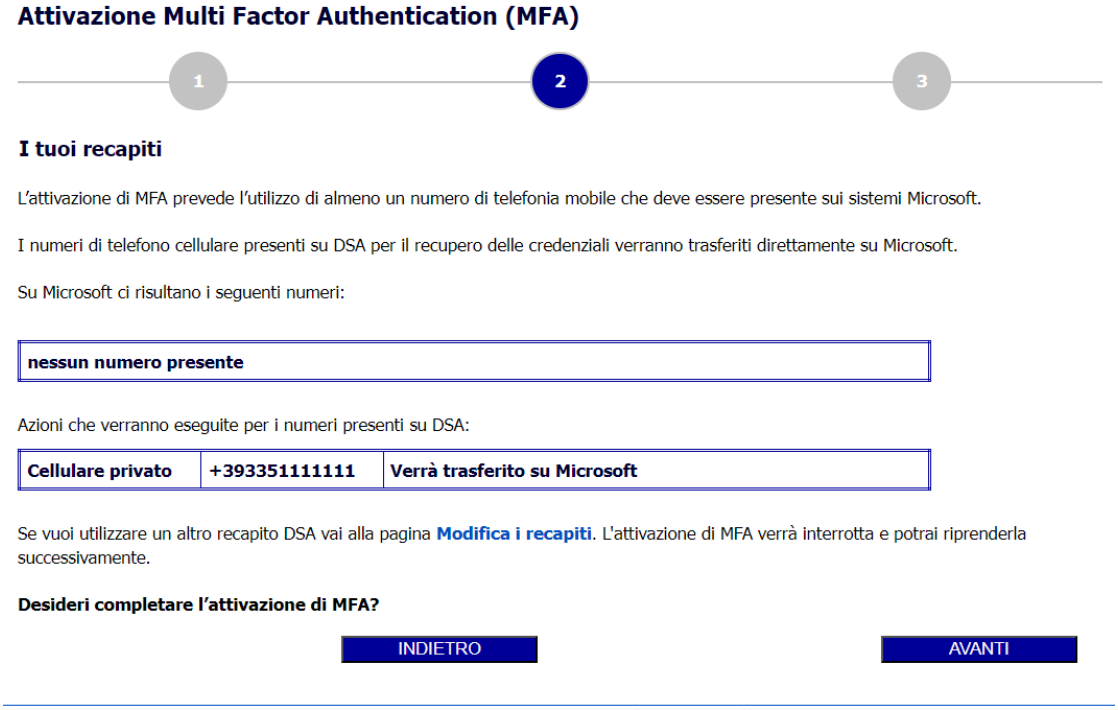
Fare click sulla voce **Gestione MFA (Multi Factor Authentication)**.



Viene presentata una pagina informativa: una volta letta fare click su **AVANTI.**



Al passo successivo è necessario verificare i recapiti telefonici che vengono presentati.

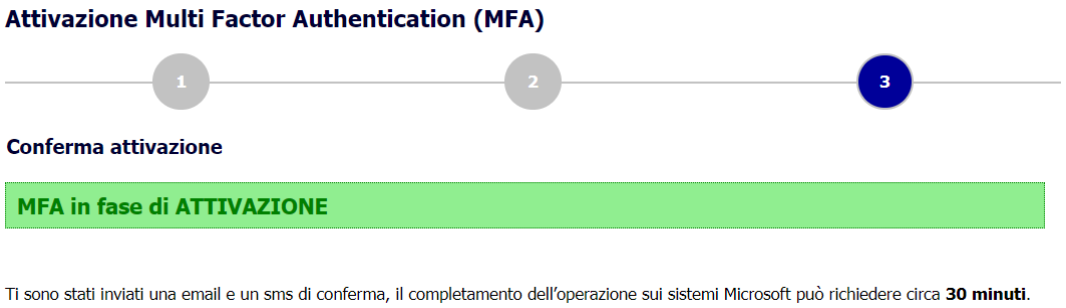


AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

Se necessario, è ancora possibile modificare il recapito DSA facendo click sul link **Modifica i recapiti** presente nella pagina oppure sulla voce **Modifica i recapiti** presente nel menu di sinistra: in questo caso, l'attivazione MFA verrà interrotta.

Se i dati relativi ai recapiti sono corretti fare click su **AVANTI**.

Viene infine presentata una pagina riepilogativa:



Fare click su **FINE.**

La richiesta di attivazione è terminata e il sistema invia una e-mail e un sms di conferma.

L'aggiornamento delle impostazioni sui sistemi Microsoft può richiedere fino a **30 minuti** e, una volta terminata, se si è collegati ad applicazioni che lo richiedono, verrà chiesta l'autenticazione a più fattori inserendo il codice ricevuto via SMS al numero di telefono indicato durante la procedura di attivazione.

Successivamente è possibile collegarsi alla pagina https://mysignins.microsoft.com/security-info, autenticarsi con le proprie credenziali istituzionali e il codice ricevuto via SMS, e aggiungere ulteriori metodi di accesso.

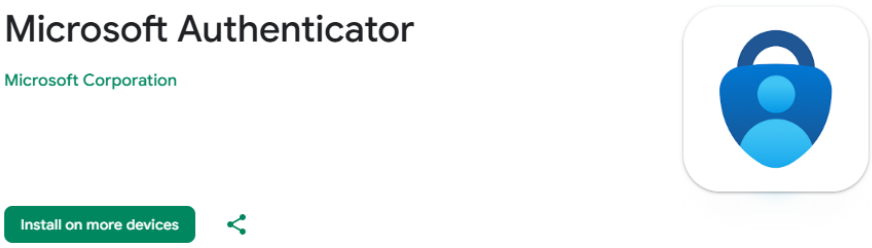
Poiché la app Microsoft Authenticator è il metodo che garantisce il livello di protezione più elevato, dopo l'attivazione di MFA si raccomanda di procedere alla configurazione di questa modalità di autenticazione a due fattori (par. 3 "Installazione e configurazione di Microsoft Authenticator").

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

3. Installazione e configurazione di Microsoft Authenticator

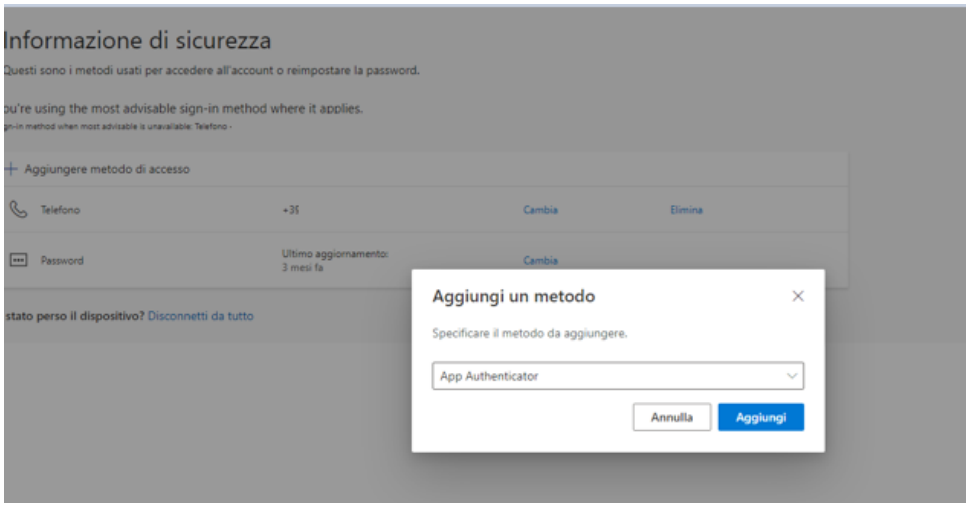
La app Microsoft Authenticator, disponibile per sistemi Android e IOS, è il metodo di generazione del codice di sicurezza con il livello di protezione più elevato: dopo l'attivazione di MFA si raccomanda di procedere con la configurazione di questa modalità di autenticazione a due fattori, seguendo i passaggi indicati.

Scaricare la app Microsoft Authenticator dallo store del proprio smartphone.



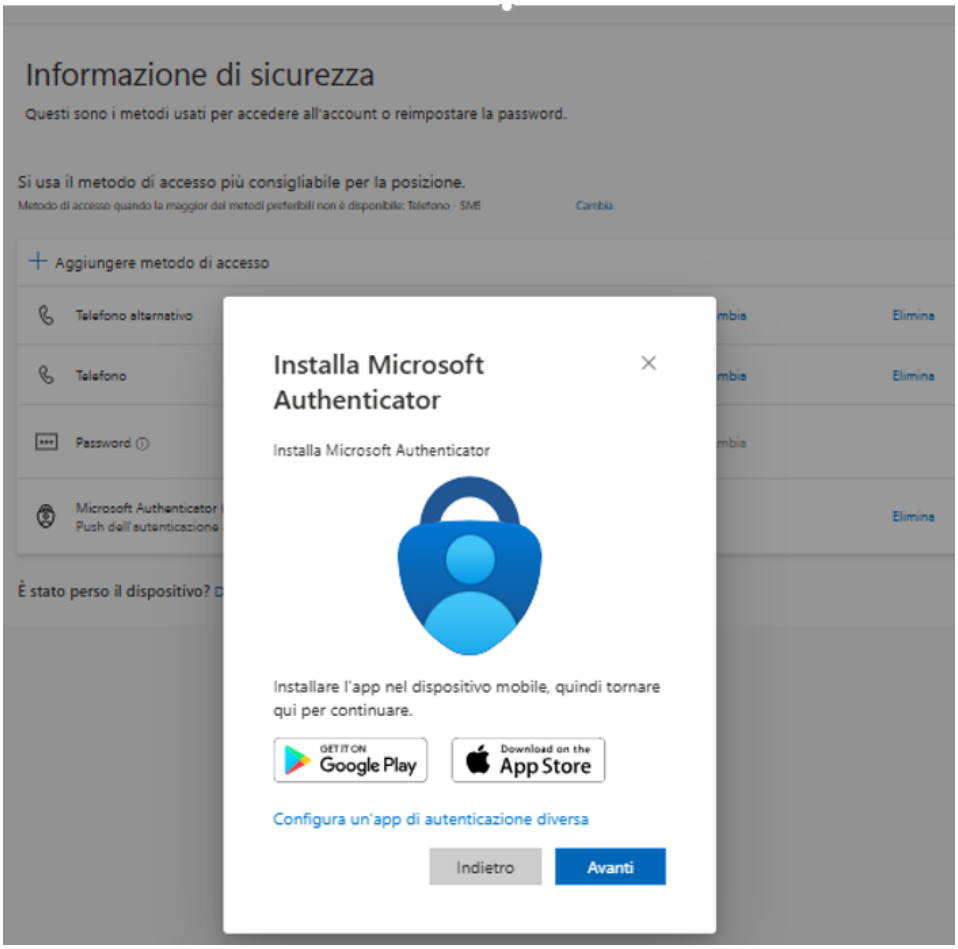
Collegarsi alla pagina https://mysignins.microsoft.com/security-info, autenticarsi con le proprie credenziali istituzionali e, se richiesto, inserire il secondo fattore di autenticazione.

Fare click su **Aggiungi Metodo di Accesso**. Selezionare dal menu a tendina App Authenticator. Fare click su **Aggiungi**:



Premere "Avanti" e aprire la app Microsoft Authenticator precedentemente installata sul proprio dispositivo:

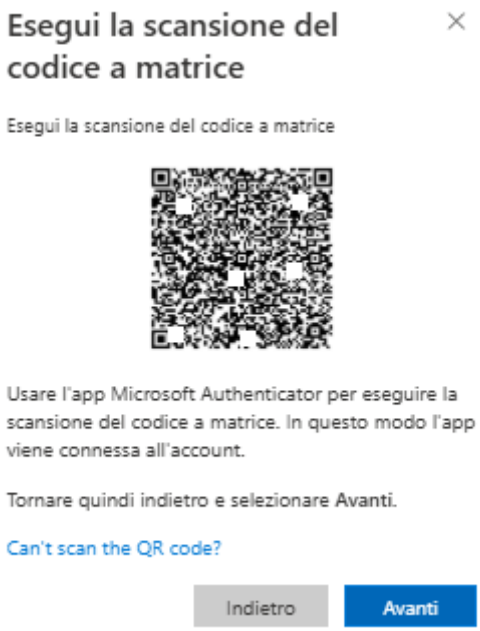
AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it



Nella schermata “Configura l’account nell’app” fare click su **Avanti**:

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it

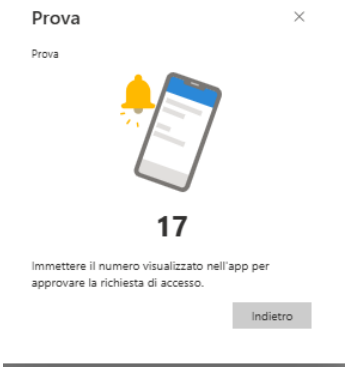
Utilizzando la app Microsoft Authenticator installata sul proprio dispositivo fare click su “Esegui la scansione di un codice a matrice” e inquadrare il QR Code mostrato a schermo (è necessario fornire alla app le autorizzazioni per scattare foto e registrare video):



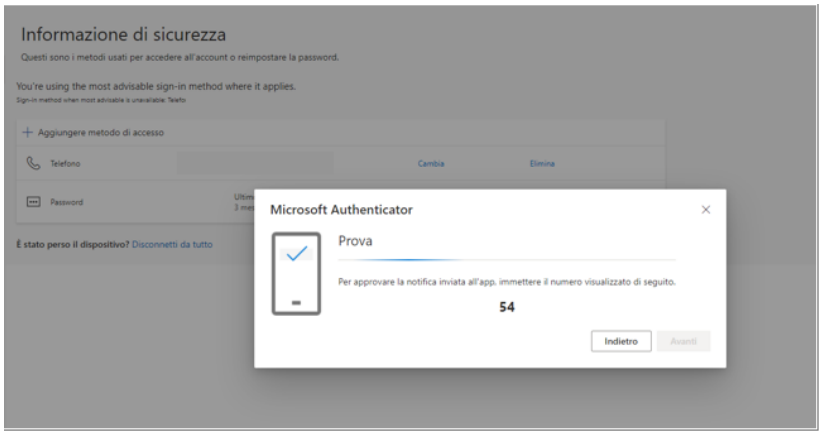
Una volta terminata la scansione del QR Ccode, selezionare sul proprio smarthone la voce “Account aziendale o dell’istituto di istruzione”. Se la scansione del QR Ccode non va a buon fine, è possibile fare click sul link “Can’t scan the QR Code” e quindi inserire a mano i dati indicati a schermo.

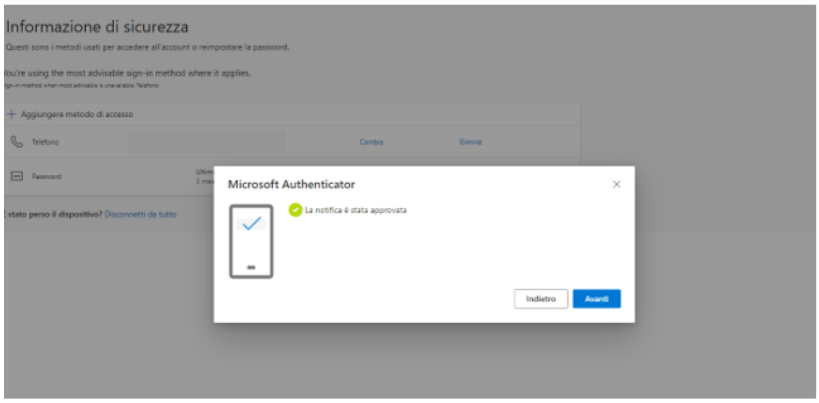
Attendere il completamento della configurazione automatica del proprio account sulla app, quindi fare click su **Avanti**.

Inserire nella app il codice di verifica prodotto a schermo (nell’esempio, il n. 17), attendere la verifica da parte del sistema e fare click su “Avanti”:



AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it





La procedura di configurazione della app Microsoft Authenticator è terminata.

4. Aggiunta di ulteriori metodi di accesso

È sempre possibile aggiungere ulteriori metodi di autenticazione: per farlo collegarsi alla pagina https://mysignins.microsoft.com/security-info, autenticarsi con le proprie credenziali istituzionali e, se richiesto, inserire il secondo fattore di autenticazione.

Fare click su “Aggiungi Metodo di Accesso”. Selezionare dal menu a tendina il metodo di accesso desiderato, e seguire la procedura guidata.

AREA SISTEMI E SERVIZI INFORMATICI – CESIA
Viale Filopanti, 3 | 40126 Bologna | Italia | Tel. +39 051 2080300; assistenza.cesia@unibo.it