



UNIVERSITÀ
DI PARMA

Autenticazione MFA per gli utenti Unipr

COME CONFIGURARLA

Versione 1.3

Cos'è l'autenticazione a più fattori (MFA)?

Un sistema di autenticazione **verifica l'identità** degli utenti, prima di concedere loro l'accesso ai servizi.

L'autenticazione MFA è una tecnologia di sicurezza che richiede agli utenti di fornire almeno un ulteriore fattore di autenticazione, oltre alla password, per poter accedere ai servizi come il proprio account di posta elettronica.

Serve per **umentare la sicurezza** dell'account e **proteggere gli utenti** dal **furto di credenziali** o da eventuali **accessi non autorizzati** alle proprie risorse.

Puoi configurarla già da ora, prima della data che ti è stata comunicata, in cui diventerà obbligatoria.

Per maggiori informazioni, accedi al [contenuto dedicato sul sito web istituzionale](#)

Come configurare la MFA

- 1) Clicca su questo link:
<https://mysignins.microsoft.com/security-info>
- 2) Nella schermata che si apre inserisci le tue credenziali di Ateneo
- 3) Clicca su «**aggiungere metodo di accesso**»

UNIVERSITÀ DI PARMA

Inserisci le credenziali istituzionali di Ateneo.

Password

Accedi

[nome.cognome@unipr.it](#)
oppure
[nome.cognome@studenti.unipr.it](#)
oppure
[numero@guest.unipr.it](#)

[Vuoi recuperare la password?](#)
[Vuoi cambiare la password?](#)

UNIVERSITÀ DI PARMA | Accessi personali

Informazione di sicurezza

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

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - Notifica [Cambia](#)

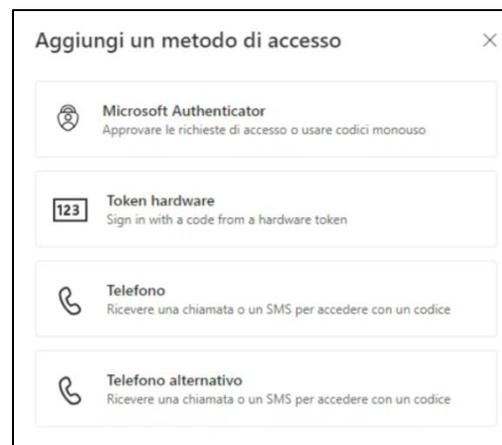
+ Aggiungere metodo di accesso

Ultimo aggiornamento: 3 mesi fa [Cambia](#)

È stato perso il dispositivo? [Disconnetti da tutto](#)

Quali metodi di autenticazione puoi configurare

Ora, dal menu, seleziona il metodo



Ci sono diverse possibilità tra le quali puoi scegliere:



1) Microsoft Authenticator (*scelta raccomandata dall'Ateneo e che garantisce i maggiori livelli di sicurezza*)



2) Telefono cellulare con codice ricevuto via sms



3) Telefono con chiamata (cellulare o numero di linea fissa)





1

MS Authenticator

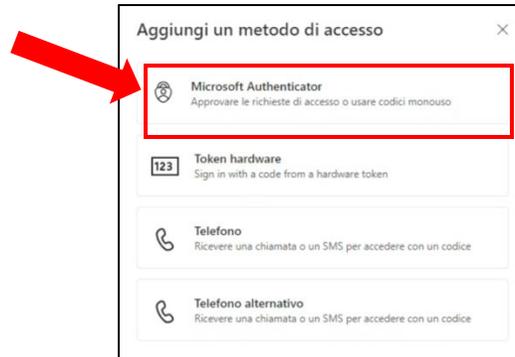


1) Microsoft Authenticator



Dal menu clicca su «**Microsoft Authenticator**». Poi clicca su «**scarica ora**» e su «**avanti**».

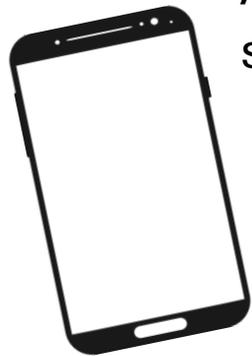
1



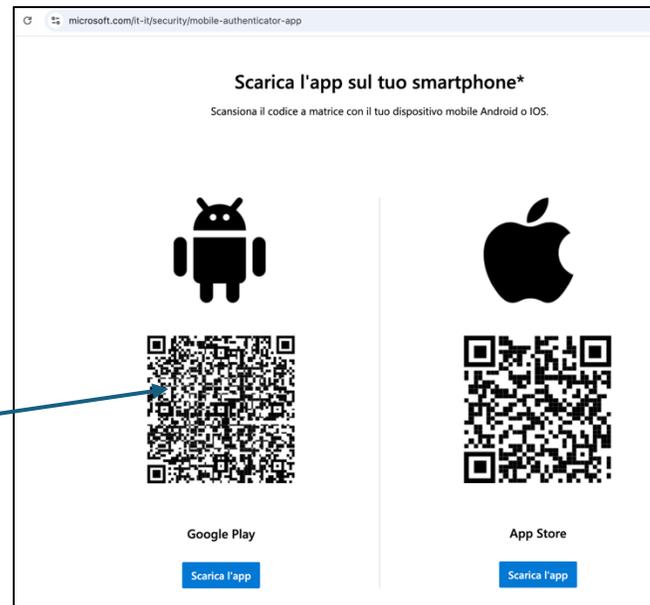
2



A questo punto, **prendi il tuo smartphone** e scansiona il codice QR che vedi sullo schermo del pc (può essere necessario scorrere la pagina verso il basso).



Per smartphone
Android



4

Per Iphone





Da cellulare, sulla app visualizzerai in successione queste schermate e dovrai cliccare sui tasti indicati dalle frecce:

1



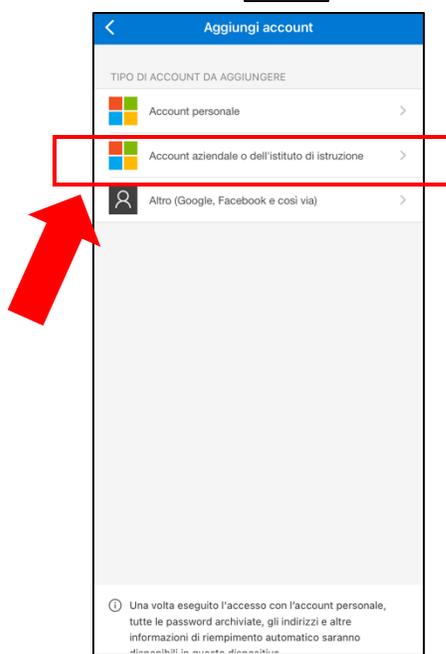
2



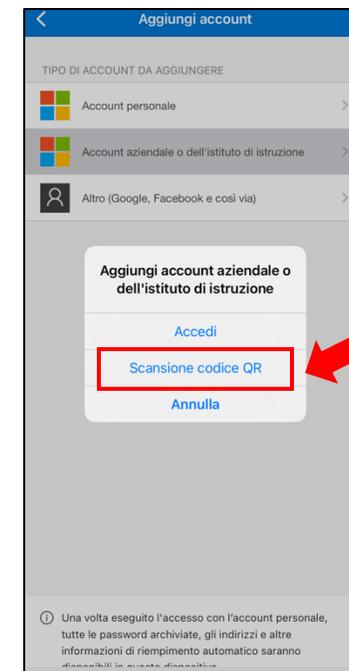
3



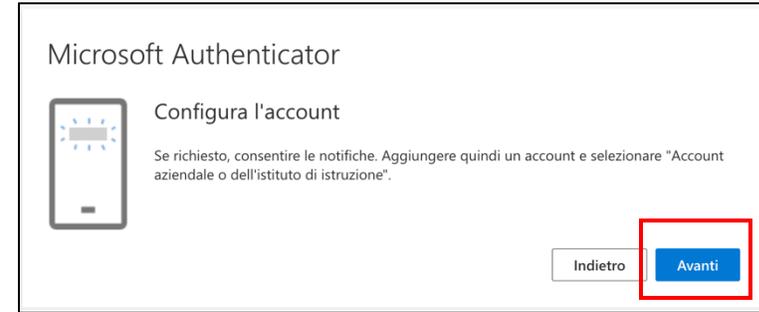
4



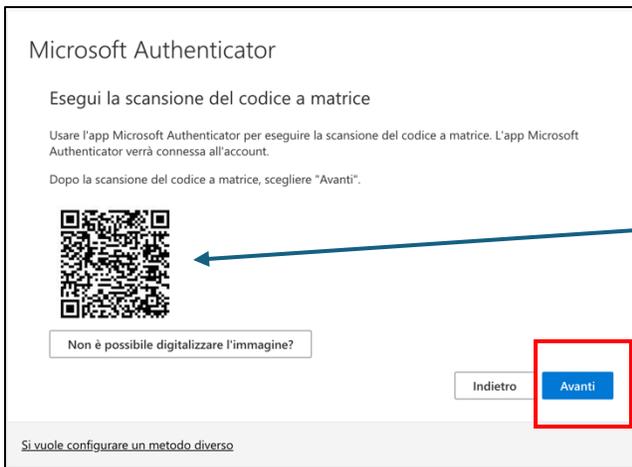
5



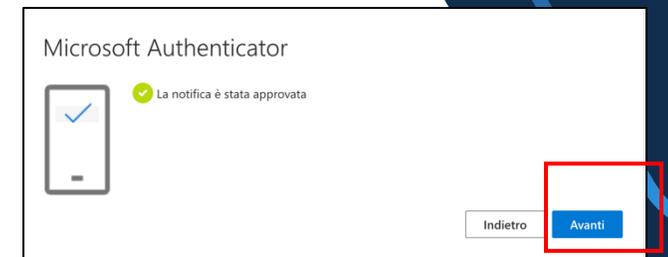
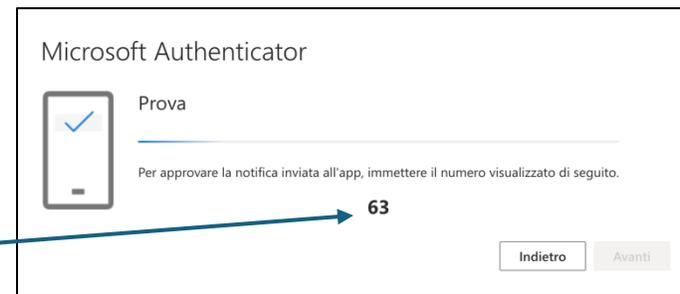
- **Da pc**, in questa schermata, clicca su «avanti».



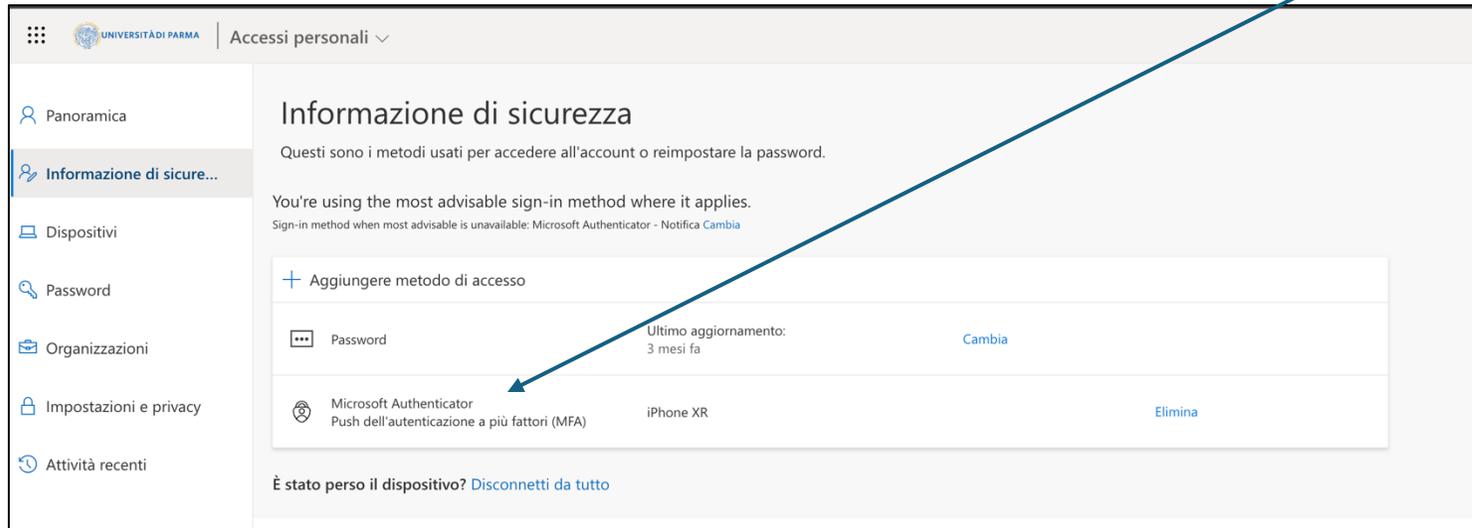
- Con il cellulare, scansiona il codice QR che comparirà sul monitor del pc e clicca su «**avanti**»



- La app su cellulare genera ora **un codice** monouso.
Inseriscilo in questa schermata del pc e clicca su «**avanti**».



- Da pc visualizzerai quindi una schermata come questa e da questo momento avrai concluso la configurazione.
- Vedrai infatti che il secondo fattore di autenticazione (Microsoft Authenticator) è comparso nella riga sotto la password.





2-3



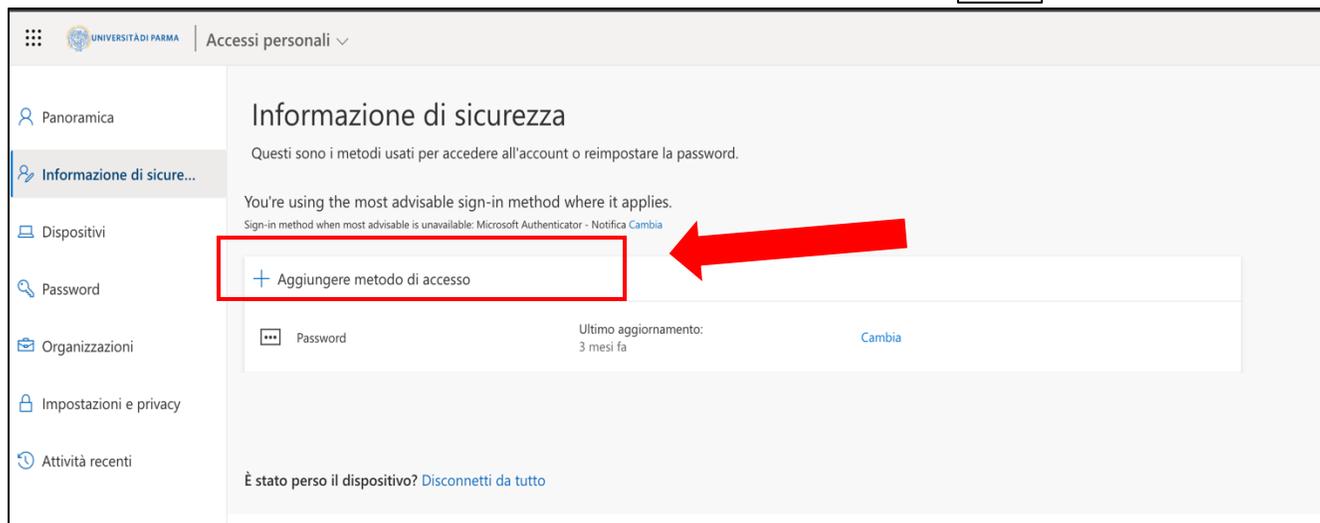
Autenticazione tramite telefono



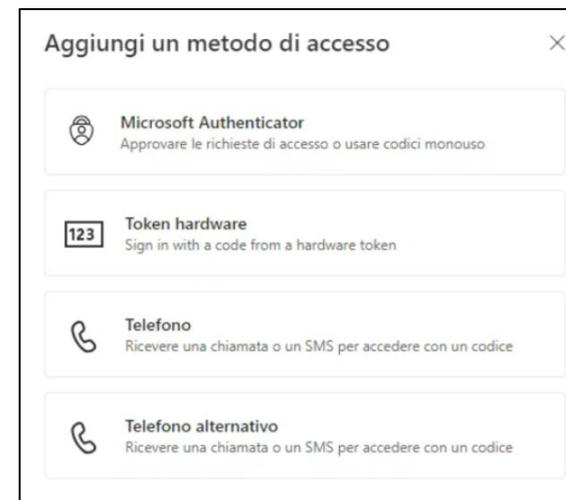
Autenticazione tramite telefono cellulare con SMS

Se non hai a disposizione uno smartphone su cui installare la app Microsoft Authenticator, dal comando «**aggiungere metodo di accesso**» (1), puoi impostare un metodo di autenticazione alternativo, tramite telefono (2) e scegliere di ricevere un SMS.

1



2





Autenticazione tramite telefono cellulare con SMS

- Nella schermata successiva, inserisci il tuo **numero di telefono cellulare** e scegli di ricevere un **codice tramite SMS**.

Telefono

Puoi dimostrare chi sei rispondendo a una chiamata sul telefono o ricevendo un codice sul telefono.

Specificare il numero di telefono da usare.

Italia (+39) 3401234567

Ricevere un codice
 Chiama

È possibile che vengano applicate le tariffe per messaggi e dati. Scegliendo Avanti si accettano le [Condizioni del servizio](#) e l'[Informativa sulla privacy e sui cookie](#).

Annulla Avanti

- Conferma cliccando su «**avanti**».

Telefono cellulare con SMS



- Inserisci il codice ricevuto via SMS nello spazio apposito e clicca su «**avanti**» per validare l'operazione.

Telefono ×

Un codice di 6 cifre è stato appena inviato a +39
Immettere il codice più avanti.

Immettere il codice

[Invia di nuovo il codice](#)

Telefono ×

✓ Verifica completata. Il telefono è stato registrato.

- Da pc visualizzerai quindi una schermata come questa e avrai concluso la configurazione. Vedrai infatti il secondo fattore di autenticazione (tramite cellulare) indicato nella riga sopra la password.

The screenshot shows the Microsoft account security settings page. The browser address bar displays 'mysignins.microsoft.com/security-info'. The page title is 'Informazione di sicurezza'. Below the title, there is a section for configuring the default access method. A table lists the current methods:

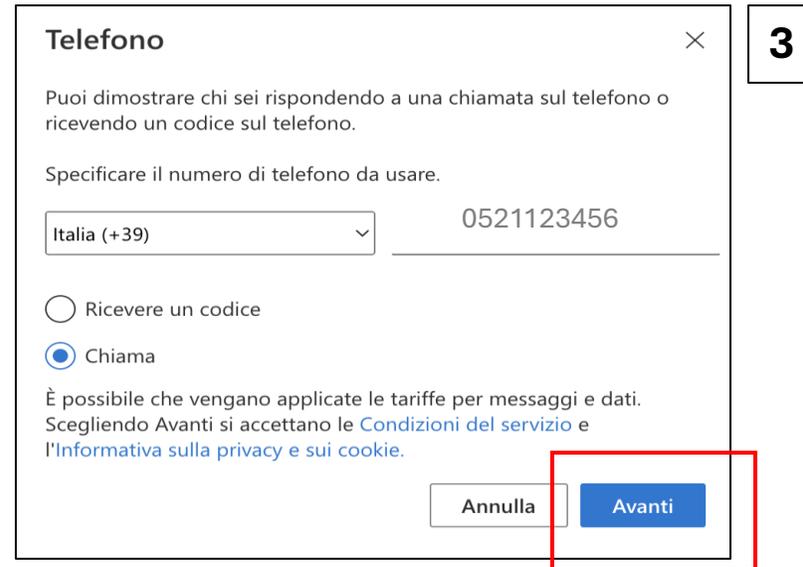
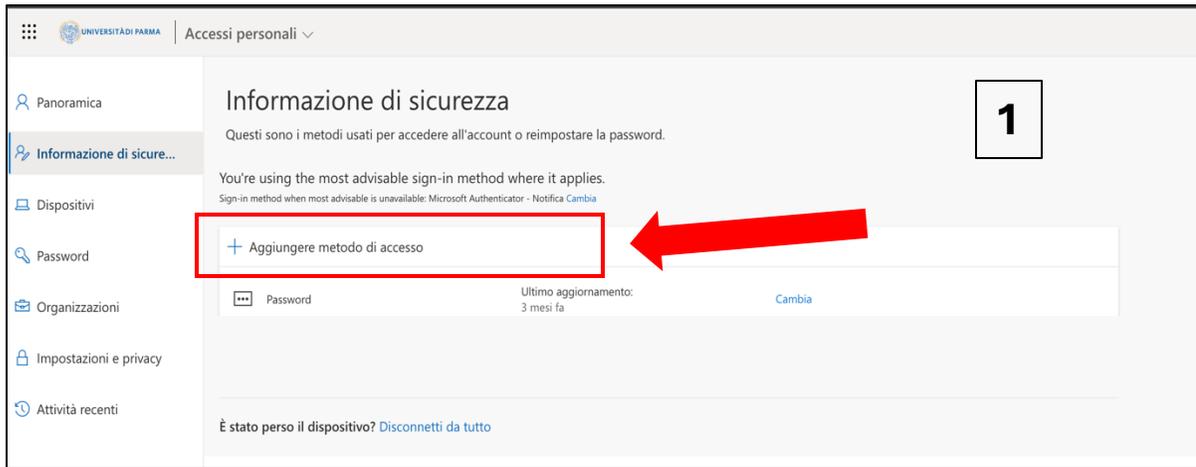
Configura il metodo di accesso predefinito			
+ Aggiungere metodo di accesso			
Telefono	+39	Cambia	Elimina
Password	Ultimo aggiornamento: un mese fa	Cambia	

At the bottom of the page, there is a link: [È stato perso il dispositivo? Disconnetti da tutto](#)

Telefono con chiamata



Nel caso in cui, invece, si voglia ricevere una chiamata, occorre eseguire i seguenti passaggi: «aggiungere metodo di accesso» **(1)**, «telefono» **(2)** inserire il numero telefonico, selezionare «chiama» e infine cliccare su «avanti» **(3)**



N.B.

Se inserisci un numero di rete fissa, tieni presente che tutte le volte in cui ti autenticherai e ti verrà richiesta la doppia autenticazione, dovrai trovarti vicino a quel telefono per riuscire a rispondere alla chiamata e autorizzare l'accesso.



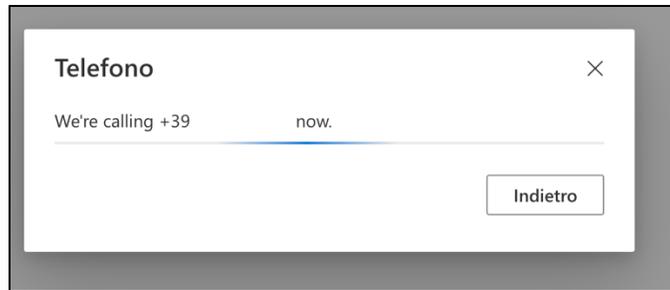
Telefono con chiamata



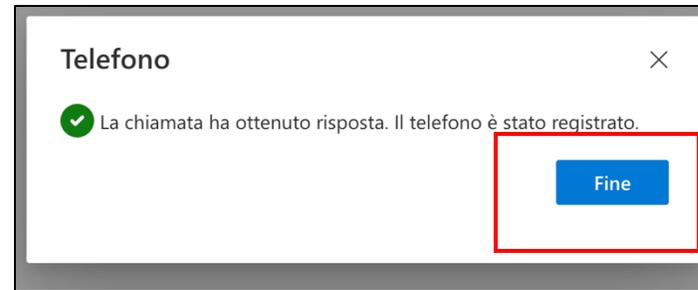
Sul pc visualizzerai due schermate **(1)** e **(2)** che ti avvisano che la chiamata è in corso.

Rispondi alla chiamata e esegui quello che ti viene richiesto. Al termine, sul pc, clicca sul pulsante «fine».

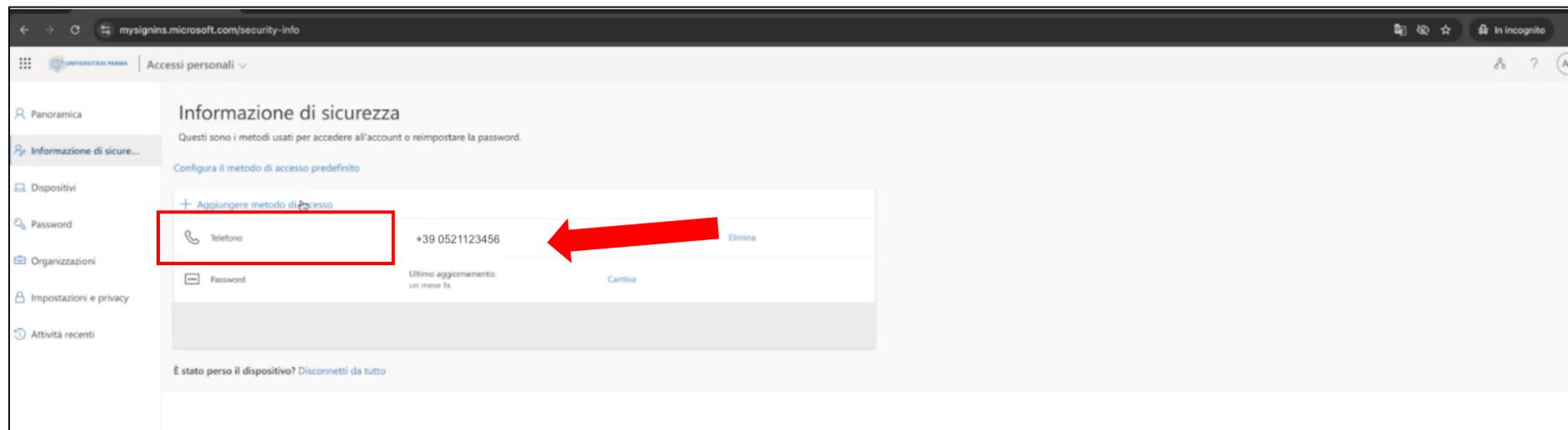
1



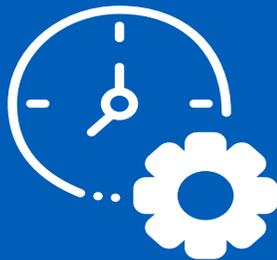
2



- Alla fine, da pc visualizzerai quindi una schermata come quella in basso e avrai concluso la configurazione. Vedrai infatti il secondo fattore di autenticazione (tramite telefono) indicato nella riga sopra la password.



Con che frequenza viene richiesta la MFA?



Quando si accede ad un servizio online, il secondo fattore di autenticazione (MFA) non viene richiesto ad ogni accesso, ma solo durante la prima autenticazione con il dispositivo in uso.

Ad esempio, se utilizzando il tuo computer abituale ti venisse richiesta l'autenticazione a 2 fattori accedendo al servizio online di posta elettronica, detta autenticazione non ti verrà richiesta la volta successiva, a meno che non siano trascorsi molti giorni.

Il periodo di validità della sessione di autenticazione dipende sostanzialmente da 2 fattori: tipo di dispositivo utilizzato e frequenza di utilizzo e di norma dura 30-90 giorni.

Nel caso in cui i sistemi che monitorano la sicurezza informatica di Unipr rivelino una compromissione o delle attività anomale con il vostro account, è possibile che venga richiesta una nuova autenticazione e/o un cambio password.

Si può cambiare il metodo di autenticazione scelto?

Se in un secondo momento, dopo aver impostato il telefono come metodo di autenticazione, vuoi optare invece per la **app**, puoi farlo.

Clicca su questo link

<https://mysignins.microsoft.com/security-info>

e segui i passaggi indicati nelle slide da 5 a 9 (*che corrispondono alla sezione 1 Ms Authenticator di questa guida*).



4

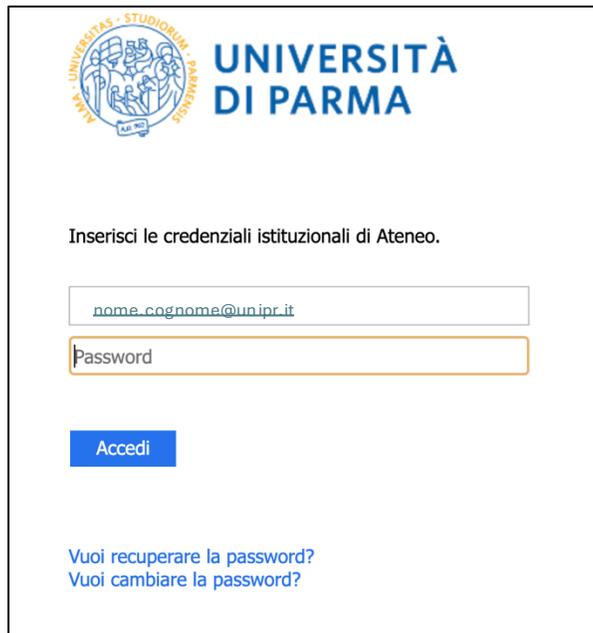
Come avviene l'autenticazione con MFA

Ora che hai configurato l'MFA, nelle schermate seguenti ti viene mostrato come avverrà l'autenticazione a due fattori

MFA con App MS Authenticator

1° FATTORE

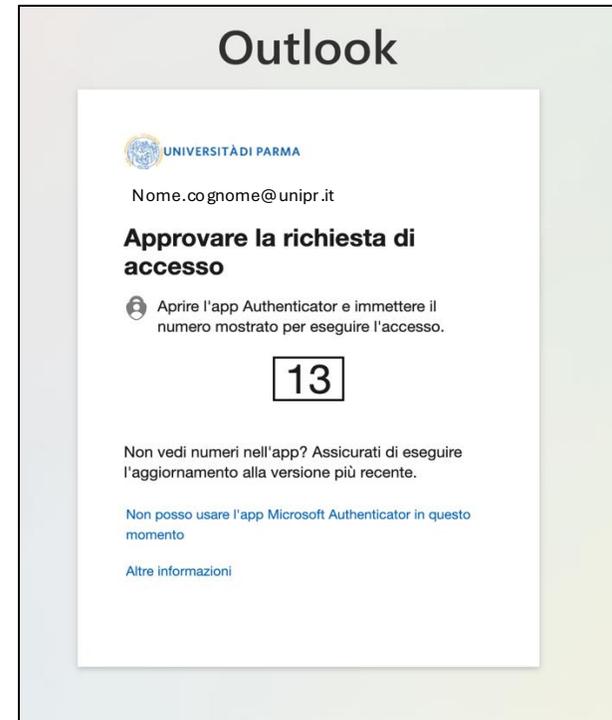
Inserisci le tue credenziali di Ateneo



The screenshot shows the login page for the University of Parma. At the top left is the university's logo, a circular emblem with the text 'UNIVERSITAS · STUDIORUM · PARMAE · 1545'. To its right, the text 'UNIVERSITÀ DI PARMA' is displayed in blue. Below the logo, the instruction 'Inserisci le credenziali istituzionali di Ateneo.' is shown. There are two input fields: the first contains the email address 'nome.cognome@unipr.it' and the second is labeled 'Password'. A blue 'Accedi' button is positioned below the fields. At the bottom, there are two links: 'Vuoi recuperare la password?' and 'Vuoi cambiare la password?'.

2° FATTORE

Inserisci sull'App il numero che compare sul dispositivo che stai utilizzando per accedere



MFA con telefono con SMS

1° FATTORE

Inserisci le tue credenziali di Ateneo



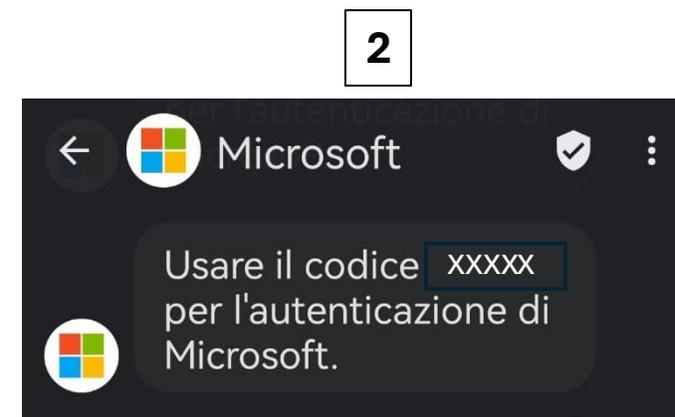
The screenshot shows the login page for the University of Parma. At the top left is the university's logo, a circular emblem with the text 'UNIVERSITAS · STUDIORUM · PARMAE' and '1545'. To the right of the logo is the text 'UNIVERSITÀ DI PARMA'. Below this, the instruction 'Inserisci le credenziali istituzionali di Ateneo.' is displayed. There are two input fields: the first contains the placeholder 'nome_cognome@unipr.it' and the second is labeled 'Password'. A blue 'Accedi' button is positioned below the fields. At the bottom, there are two links: 'Vuoi recuperare la password?' and 'Vuoi cambiare la password?'.

2° FATTORE

Inserisci nella schermata sul pc (1) il codice che riceverai con un SMS sul tuo telefono (2) e clicca su verifica (3)



The screenshot shows the MFA verification page. At the top left is the University of Parma logo. The page displays the email address 'Nome.cognome@unipr.it' and the instruction 'Immettere il codice'. Below this, there is a checkbox with the text 'È stato inviato un SMS al telefono con numero +XX XXXXXXXX45. Immettere il codice per accedere.' followed by a text input field containing 'XXXXX'. A blue 'Verifica' button is located at the bottom right. A blue box highlights the entire page, with a '1' in a white box at the top left and a '3' in a white box at the bottom right, with an arrow pointing to the 'Verifica' button.

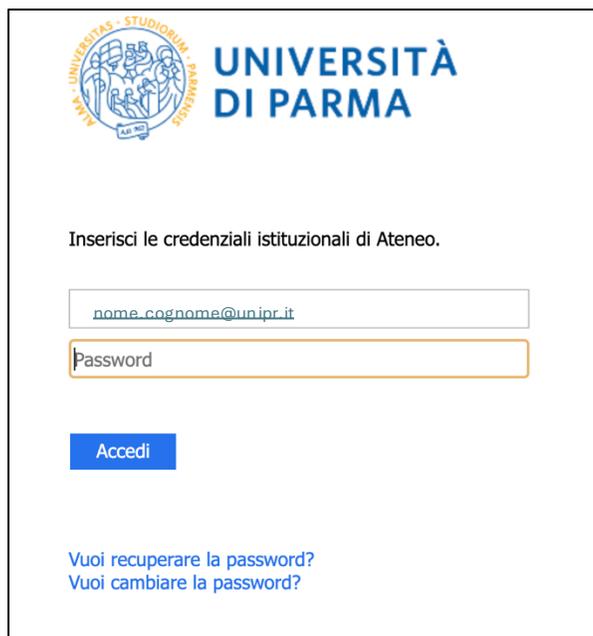


The screenshot shows a Microsoft authentication screen. At the top left is the Microsoft logo. The text 'Microsoft' is displayed in the top right. Below this, the instruction 'Usare il codice XXXXX per l'autenticazione di Microsoft.' is shown, with 'XXXXX' in a text box. A blue box highlights the entire screen, with a '2' in a white box at the top right.

MFA con telefono con chiamata

1° FATTORE

Inserisci le tue credenziali di Ateneo



The screenshot shows the login interface for the University of Parma. At the top left is the university's logo, a circular emblem with the text 'UNIVERSITAS · STUDIORUM · PARMENSIS' and '1808'. To its right is the text 'UNIVERSITÀ DI PARMA'. Below the logo, the instruction 'Inserisci le credenziali istituzionali di Ateneo.' is displayed. There are two input fields: the first contains the placeholder 'nome_cognome@unipr.it' and the second is labeled 'Password'. A blue 'Accedi' button is positioned below the fields. At the bottom left, there are two links: 'Vuoi recuperare la password?' and 'Vuoi cambiare la password?'.

2° FATTORE

Ti apparirà la schermata che ti chiede di approvare la richiesta di accesso (1). Rispondi alla chiamata che riceverai sul telefono e segui le istruzioni (2).

1



The screenshot shows a mobile application interface for MFA approval. At the top left is the University of Parma logo and the text 'UNIVERSITÀ DI PARMA'. Below it, the email address 'Nome.cognome@unipr.it' is displayed. The main heading is 'Approvare la richiesta di accesso'. A small telephone icon is followed by the text: 'Verrà inviata una chiamata al telefono dell'utente. Rispondere alla chiamata per continuare.' Below this, there is a link: 'Se si verificano problemi, accedere in modo diverso' and another link: 'Altre informazioni'.

2



Per supporto tecnico

Se hai bisogno di ulteriori chiarimenti o se riscontri problemi nella procedura, puoi scrivere a:

 helpdesk.informatico@unipr.it

