



UNIVERSITÀ
di **VERONA**

MFA – GUIDA OPERATIVA - IPAD



DIREZIONE SISTEMI INFORMATIVI E TECNOLOGIE
AREA SISTEMI DI CALCOLO

Sommario

Ipad.....	3
MFA - Autenticazione a Fattori Multipli presso l'Università degli Studi di Verona.....	3
Generare il codice QR.....	7
1° Metodo: utilizzare la mail privata	7
2° Metodo: utilizzare SPID.....	10
3° Metodo: utilizzare CIE	14
Configurare e ricevere i codici di verifica con Google Authenticator.....	17
Configurare e ricevere i codici di verifica con Microsoft Authenticator	19
Configurare Mail.....	20
Errore di configurazione MFA.....	26

Ipad

MFA - Autenticazione a Fattori Multipli presso l'Università degli Studi di Verona

L'obiettivo della MFA¹ è quello di tenere al sicuro i propri account e ridurre al minimo i rischi per la sicurezza: rendere più difficile per una persona non autorizzata accedere a risorse protette.

L'autenticazione a più fattori (MFA) è un sistema di sicurezza che utilizza più metodi di autenticazione per verificare l'identità dell'utente che desidera accedere.

L'Università degli Studi di Verona per l'accesso ad Office 365 implementa una MFA a 2 fattori:

- 1° fattore di autenticazione: **login/password GIA**
- 2° fattore di autenticazione: **Token² di Accesso Temporaneo**

Il token può essere fornito con due modalità:

- **OTP** (One Time Password) comunicazione del codice di sicurezza all'*email privata* registrata in GIA
- **TOTP** (Time-Based One Time Password) comunicazione del codice di sicurezza utilizzando *Applicazioni Mobile* (Microsoft Authenticator, Google Authenticator, 2FA, ...) o *Applicativi Desktop* in grado di supportare lo standard (es. KeepassXC).

La prima modalità (OTP) funziona senza alcuna configurazione dell'utente che deve controllare la correttezza della propria email privata fornita all'università. Tale controllo è possibile accedendo al proprio profilo in ESSE3 carriere studenti (per gli studenti) o a DBERW (per il personale TA/docenti):

- ✓ [ESSE3](#) – Studenti

UNIVERSITÀ di VERONA
Servizi online

In questa pagina vengono visualizzate le informazioni anagrafiche, residenza e domicilio. Cliccando sulla voce Modifica, delle varie sezioni informative, si possono cambiare i dati. Attenzione! I dati relativi al luogo e alla data di nascita non sono modificabili.

Dati Personali	
Cognome	PALLINO

Recapiti	
Recapito Documenti	Domicilio
Email	pinco.pallino@example.org
Cellulare	+39 045 xxxxxxxx
Dichiaro di aver preso visione dell'informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 (Regolamento europeo in materia di protezione dei dati personali) fornita nella seguente pagina web: https://www.univr.it/it/privacy	<input type="checkbox"/> SI

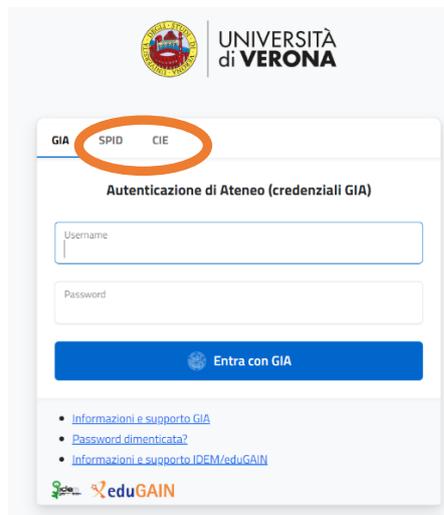
[Modifica Recapiti](#) Utilizza il link per modificare i Recapiti

¹ MFA = Multi Factor Authentication

² TOKEN = Termine informatico, individua un oggetto fisico o logico necessario per l'MFA (E' tipicamente un codice numerico)

✓ [Dberw](#) – Personale

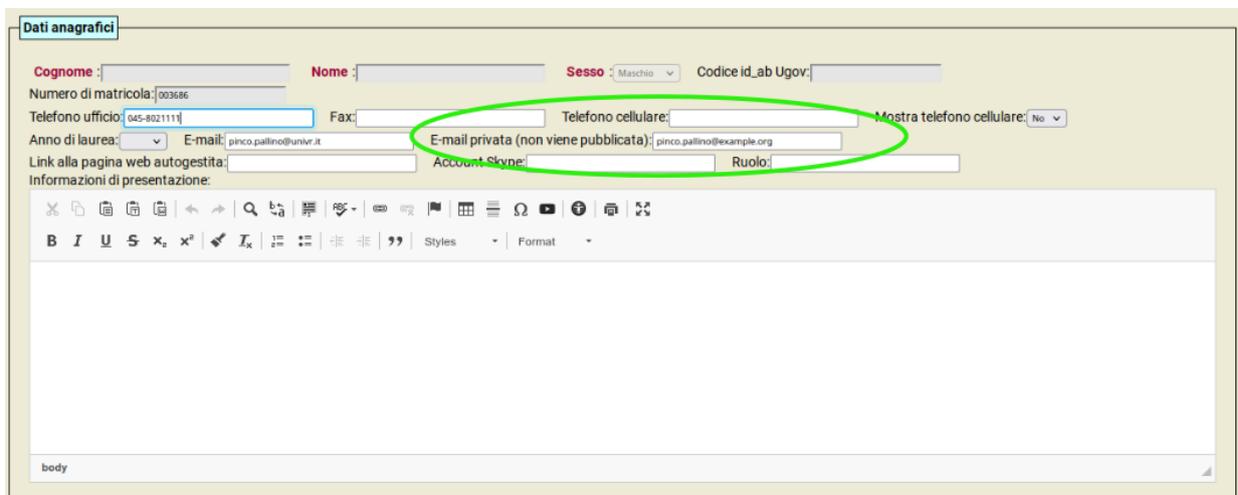
Accedere a Dberw con **SPID** o **CIE**:



Scegliere la prima opzione “Selezionare l’Utenza GIA XXXXX”:



Selezionare “Dati personali”, poi selezionare il proprio nome e cliccare su “Modifica”:



Inserire la mail desiderata nel campo “E-mail privata (non viene pubblicata)”.

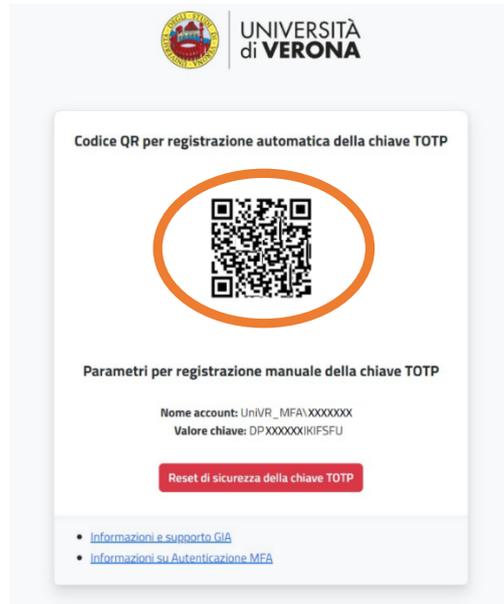
La **seconda modalità (TOTP)** permette la generazione del token anche in assenza di connettività di rete.

Per questa modalità bisogna:

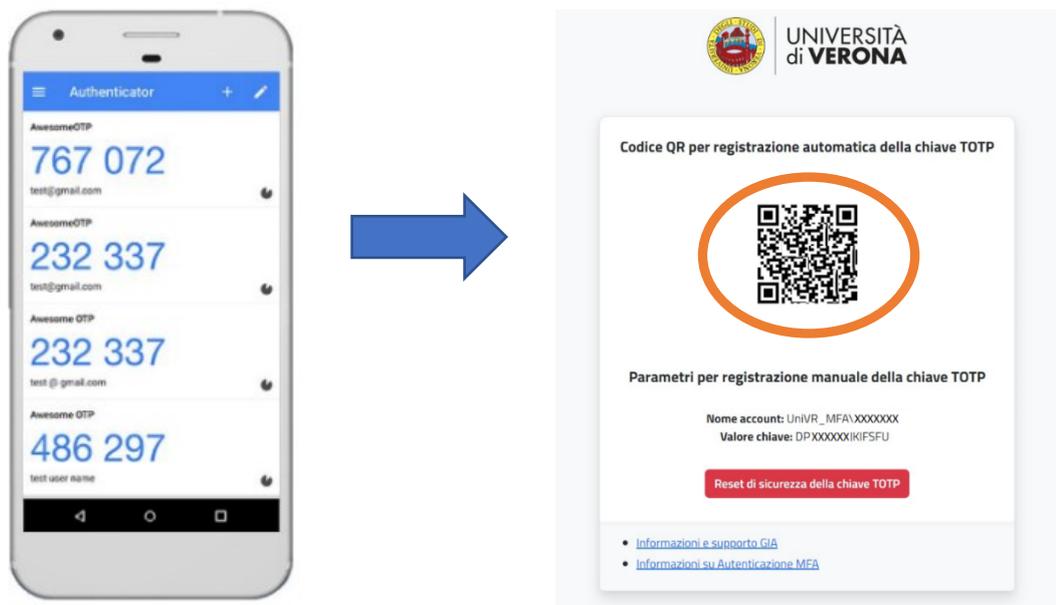
1. generare un **codice QR** per la registrazione automatica della chiave TOTP

E' possibile farlo tramite:

- email privata
- Oppure
- SPID/CIE



2. **configurare** associando a questo codice l'Applicazione Mobile o Applicativi Desktop scelta:



Vedere il relativo paragrafo in questa guida per configurarla.

Nota:

In alternativa all'MFA per l'accesso ad Office 365 rimane sempre attiva l'autenticazione tramite SPID o CIE:

The image displays two screenshots of the University of Verona's login interface. The left screenshot shows the 'Autenticazione di Ateneo (credenziali GIA)' form. At the top, there are three tabs: 'GIA', 'SPID', and 'CIE'. The 'SPID' and 'CIE' tabs are circled in orange. Below the tabs, there are input fields for 'Username' and 'Password', and a blue button labeled 'Entra con GIA'. At the bottom, there are links for 'Informazioni e supporto GIA', 'Password dimenticata?', and 'Informazioni e supporto IDEM/eduGAIN'. The right screenshot shows the 'Selezione Account' screen. It features a blue informational box with text: 'Si prega di selezionare l'Utenza con cui accedere alle applicazioni. Selezionando l'Utenza GIA verranno garantiti tutti i privilegi e i permessi ad essa associati. Continuando con l'Utenza SPID permessi e privilegi saranno discretionalizzati secondo dell'applicazione a cui si accede.' Below this box are two buttons: 'Seleziona l'Utenza GIA XXXXXXXX' and 'Continua con l'utenza SPID/CIE'. The first button is circled in orange.

Generare il codice QR

Requisito

Verificare che l'orario del dispositivo su cui si installa l'App Mobile per l'autenticazione MFA sia corretto per garantire il funzionamento dei codici di sicurezza TOTP.

Procedimento

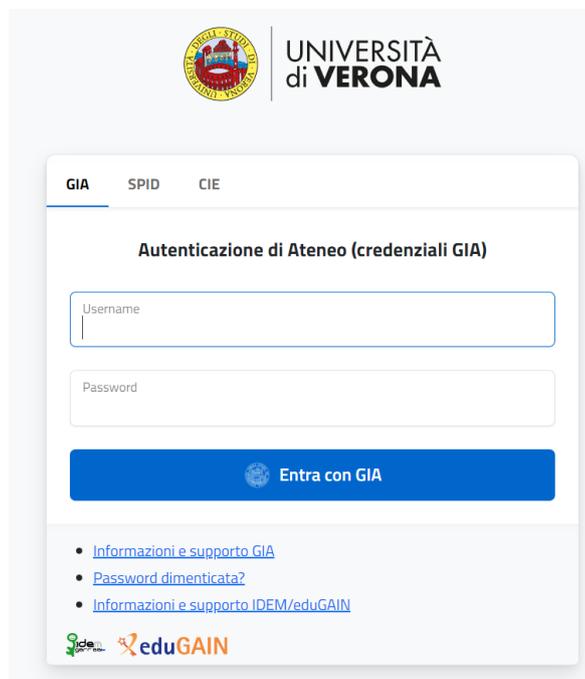
Generare il codice QR per poter registrare l'App Mobile o App Desktop per l'autenticazione MFA e ricevere i codici di verifica TOTP.

1° Metodo: utilizzare la mail privata

Requisito

Questa procedura richiede che ci sia un indirizzo email privata in ESSE3 carriere studenti (per gli studenti) o in DBERW (per il personale TA/docenti) valida ed accessibile dall'utente al momento della registrazione.

1. Accedere alla pagina web:
<https://aap.univr.it/UNIVRMfaQr/qr>
2. Autenticarsi con Login/password GIA:

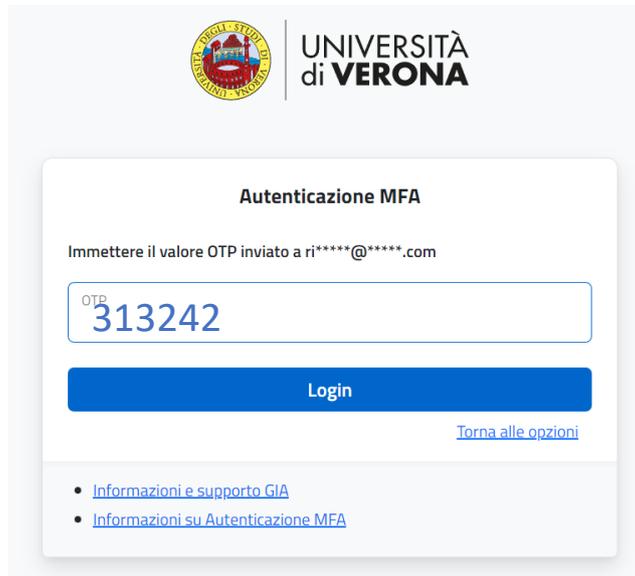


The screenshot shows the login interface for the University of Verona. At the top left is the university's logo, and to its right is the text "UNIVERSITÀ di VERONA". Below this is a navigation bar with three tabs: "GIA" (selected), "SPID", and "CIE". The main heading is "Autenticazione di Ateneo (credenziali GIA)". There are two input fields: "Username" and "Password". Below the fields is a blue button labeled "Entra con GIA". At the bottom, there are three links: "Informazioni e supporto GIA", "Password dimenticata?", and "Informazioni e supporto IDEM/eduGAIN". The footer includes the "eduGAIN" logo.

3. Inserire il codice OTP inviato all'email privata con messaggio dal contenuto simile al seguente:

Subject: One Time Pin

Please use 313242 as a One Time Pin to access the requested resource.



Autenticazione MFA

Immettere il valore OTP inviato a ri*****@*****.com

OTP
313242

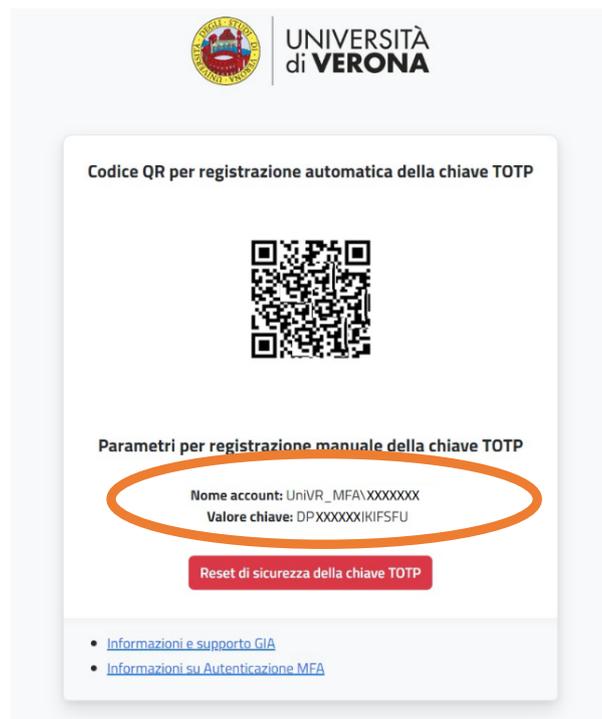
Login

[Torna alle opzioni](#)

- [Informazioni e supporto GIA](#)
- [Informazioni su Autenticazione MFA](#)

Premere “Login”

4. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l'App Mobile o l'App Desktop di autenticazione MFA:



Codice QR per registrazione automatica della chiave TOTP



Parametri per registrazione manuale della chiave TOTP

Nome account: UniVR_MFA\XXXXXXX
Valore chiave: DPXXXXXIKIFSFU

Reset di sicurezza della chiave TOTP

- [Informazioni e supporto GIA](#)
- [Informazioni su Autenticazione MFA](#)

Note

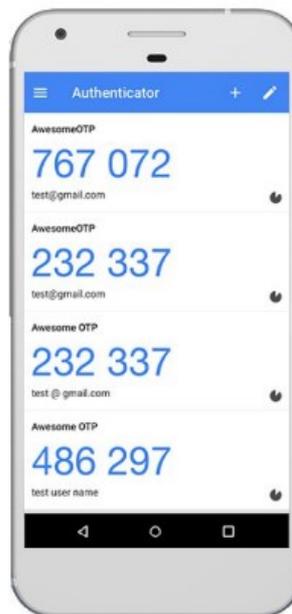
E' possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante "Reset di sicurezza della chiave TOTP". Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall'inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L'App Mobile o App Desktop di autenticazione scelta per l'MFA dovrebbe permettere di inserire manualmente il "Nome account: UNIVR\XXXXX" e la chiave segreta "Valore chiave: XXXXXXXXXXXX". Fare riferimento alle guide specifiche dell'App Mobile o App Desktop di autenticazione scelta per l'MFA per le istruzioni per l'inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, ...) o Applicativi Desktop in grado di supportare lo standard (es. KeePassXC) che permettono la generazione di codici di sicurezza per l'MFA.

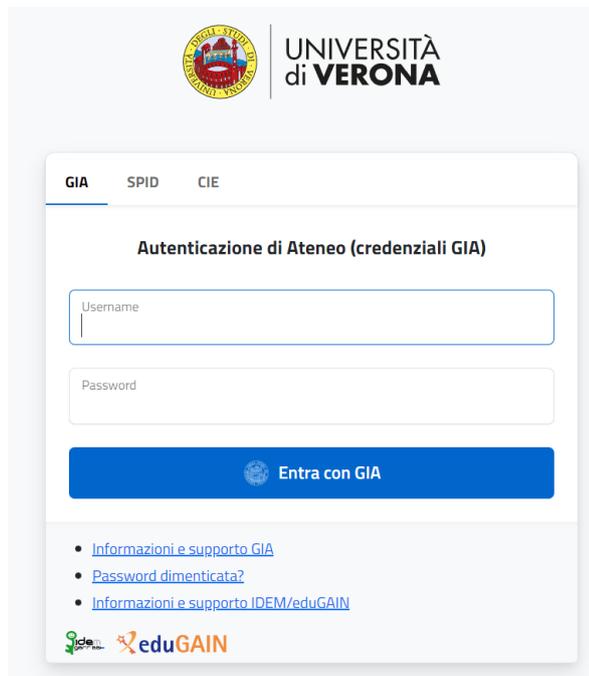
Vi illustriamo come procedere con le App Mobile:

- Google Authenticator
- Microsoft Authenticator



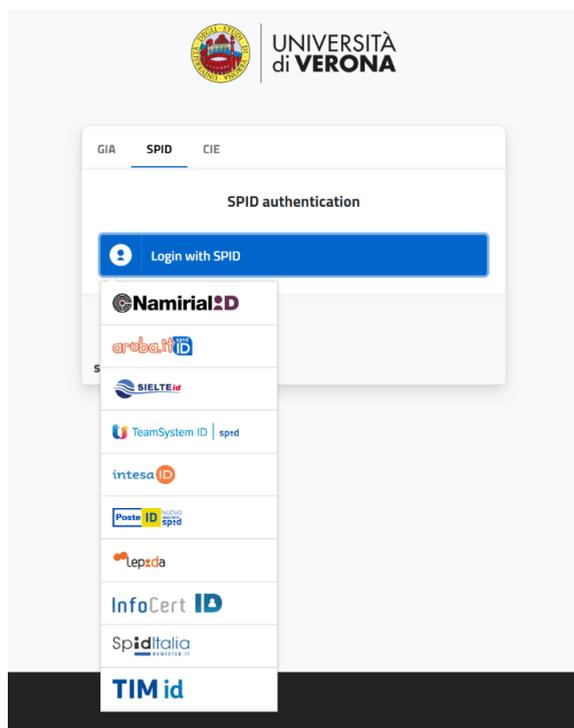
2° Metodo: utilizzare SPID

1. Accedere alla pagina web:
<https://aap.univr.it/UNIVRMfaQr/qr>
2. Autenticarsi con SPID:



The screenshot shows the login page for the University of Verona. At the top, there is the university's logo and the text "UNIVERSITÀ di VERONA". Below this, there are three tabs: "GIA", "SPID", and "CIE". The "GIA" tab is selected, and the page title is "Autenticazione di Ateneo (credenziali GIA)". There are two input fields: "Username" and "Password". Below the fields is a blue button labeled "Entra con GIA". At the bottom, there are three links: "Informazioni e supporto GIA", "Password dimenticata?", and "Informazioni e supporto IDEM/eduGAIN". There are also logos for "eduGAIN" and "eduGAIN" at the bottom left.

3. Scegliere l'Identity Provider del tuo SPID:



The screenshot shows the login page for the University of Verona, with the "SPID" tab selected. The page title is "SPID authentication". There is a blue button labeled "Login with SPID". Below the button is a list of Identity Providers (IDPs) with their logos: "Namirial2D", "ereba.it ID", "SIELTE ID", "TeamSystem ID | spid", "intesa ID", "Poste ID", "Lepzda", "InfoCert ID", "Spiditalia", and "TIM id".

4. Scansionare il codice QR e procedere con l'autorizzazione su APP Poste ID:

sp:d

Poste ID NUOVO ALLIATO sp:d

Richiesta di accesso SPID 2 da
Università di Verona

NOME UTENTE
inserisci e-mail

PASSWORD
inserisci password

Hai dimenticato il nome utente o la password?

ANNULLA **ENTRA CON SPID**

Accedi più rapidamente.
Inquadra il QR Code con l'App PosteID.
Il codice è valido per 118 secondi

Non hai ancora SPID? Registrati

sp:d AgID Agenzia per l'Italia Digitale

sp:d

Poste ID NUOVO ALLIATO sp:d

Richiesta di accesso SPID 2 da
Università di Verona

I seguenti dati stanno per essere inviati al fornitore dei servizi

- Codice identificativo
- Nome
- Cognome
- Codice fiscale

NON ACCONSENTO **ACONSENTO**

Per consultare l'informativa sul trattamento dei dati personali ai sensi del Regolamento 2016/679/UE clicca qui

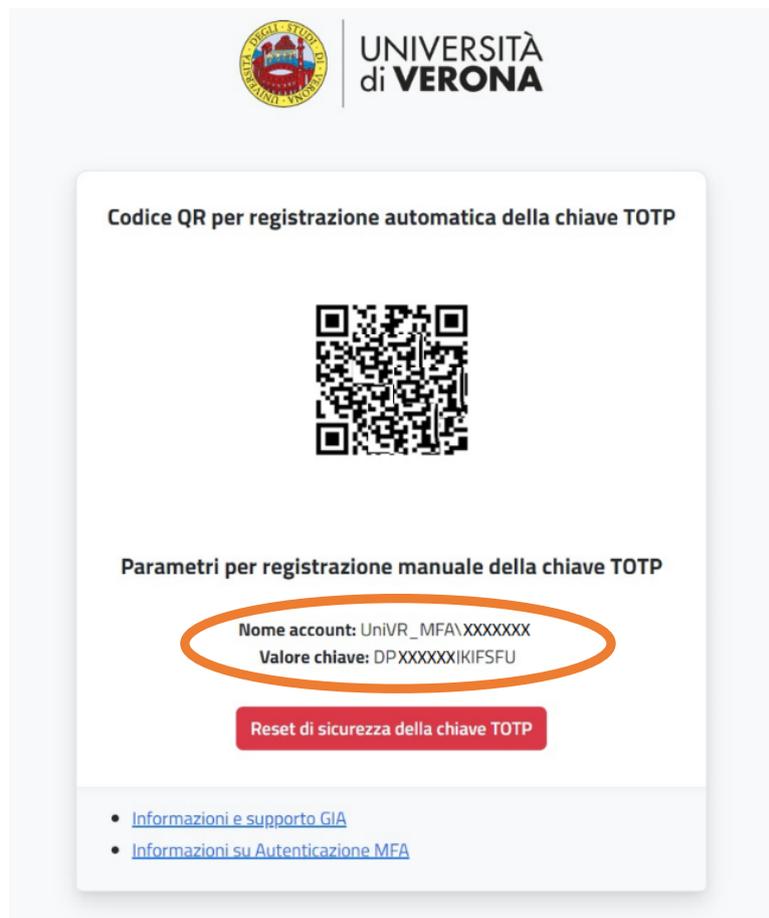
sp:d AgID Agenzia per l'Italia Digitale

Premere "Acconsoento"

5. Scegliere la prima opzione "Selezionare l'Utenza GIA XXXXX"



6. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l'App Mobile o l'App Desktop di autenticazione MFA:



Note

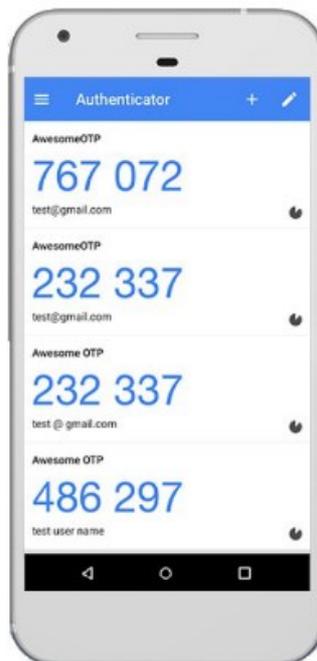
E' possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante "Reset di sicurezza della chiave TOTP". Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall'inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L'App Mobile o App Desktop di autenticazione scelta per l'MFA dovrebbe permettere di inserire manualmente il "Nome account: UNIVR\XXXXX" e la chiave segreta "Valore chiave: XXXXXXXXXXXX". Fare riferimento alle guide specifiche dell'App Mobile o App Desktop di autenticazione scelta per l'MFA per le istruzioni per l'inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, ...) o Applicativi Desktop in grado di supportare lo standard (es. KeePassXC) che permettono la generazione di codici di sicurezza per l'MFA.

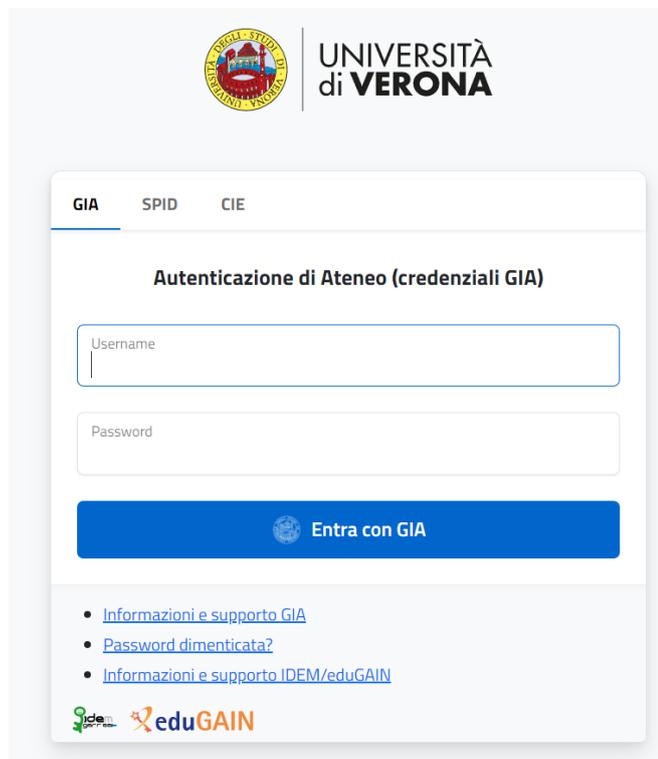
Vi illustriamo come procedere con le App Mobile:

- Google Authenticator
- Microsoft Authenticator



3° Metodo: utilizzare CIE

1. Accedere alla pagina web:
<https://aap.univr.it/UNIVRMfaQr/gr>
2. Autenticarsi con CIE:



The screenshot shows the login interface for the University of Verona. At the top left is the university's logo, and to its right is the text "UNIVERSITÀ di VERONA". Below this is a navigation bar with three tabs: "GIA", "SPID", and "CIE", with "GIA" being the active tab. The main heading is "Autenticazione di Ateneo (credenziali GIA)". There are two input fields: "Username" and "Password". Below these is a blue button labeled "Entra con GIA". At the bottom, there are three links: "Informazioni e supporto GIA", "Password dimenticata?", and "Informazioni e supporto IDEM/eduGAIN". Logos for "idem" and "eduGAIN" are also present.



Seleziona la modalità di autenticazione



Per autenticarti tramite uno smartphone con Android 6.0 o superiore, o iOS 13 o superiore, dotati di tecnologia NFC, munisciti della nuova Carta d'identità elettronica e assicurati di avere l'applicazione **Cie ID** installata e configurata correttamente.

Prosegui con smartphone



Per autenticarti con un lettore di smartcard contactless utilizzando un computer con Windows, Mac o Linux, dotati della nuova Carta d'identità elettronica. Assicurati inoltre di avere il **software Cie** installato e configurato correttamente e di appoggiare la carta sul lettore prima di cliccare sul pulsante prosegui.

Prosegui con computer

Cie ID

3. Inserire il numero di serie della CIE:

Inserisci il numero di serie della tua Carta d'Identità Elettronica

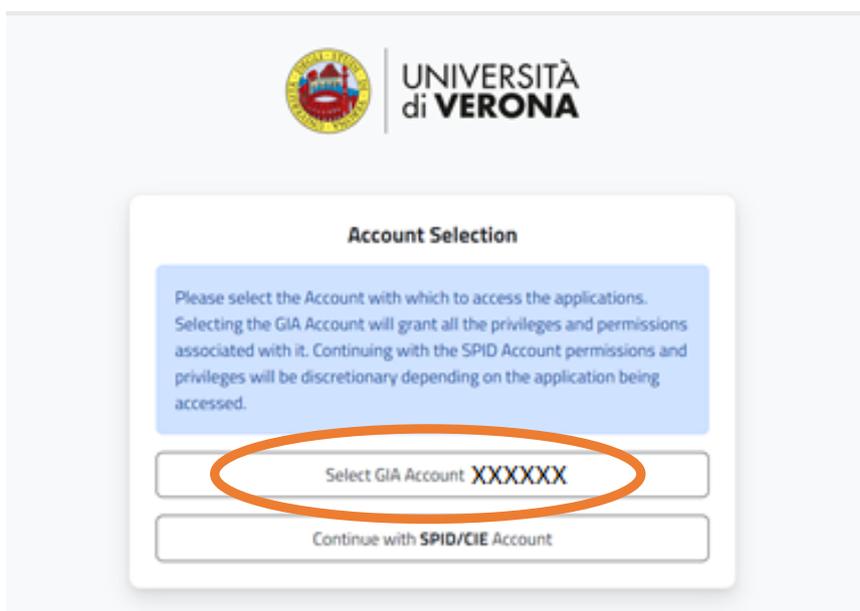


CA XXXXXX

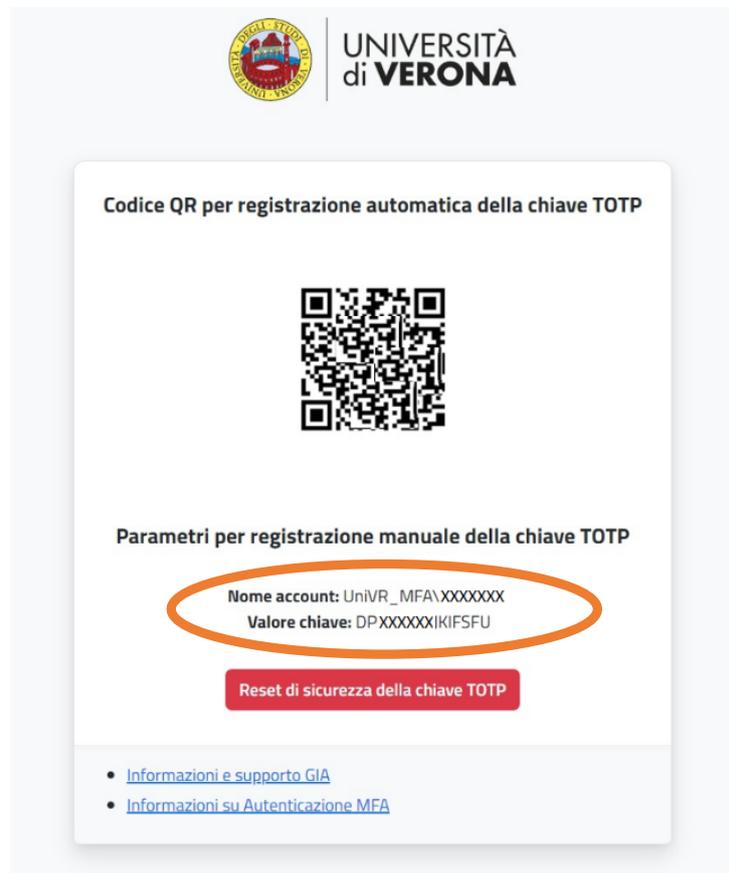
Procedi

Torna al servizio

4. Scansionare il QR code con l'app CIE ed inserire il codice OTP ricevuto
5. Scegliere la prima opzione "Select GIA Account XXXXX"



6. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l'App Mobile o l'App Desktop di autenticazione MFA:



Note

E' possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante "Reset di sicurezza della chiave TOTP". Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall'inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L'App Mobile o App Desktop di autenticazione scelta per l'MFA dovrebbe permettere di inserire manualmente il "Nome account: UNIVR\XXXXX" e la chiave segreta "Valore chiave: XXXXXXXXXXXX". Fare riferimento alle guide specifiche dell'App Mobile o App Desktop di autenticazione scelta per l'MFA per le istruzioni per l'inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, ...) o Applicativi Desktop in grado di supportare lo standard (es. KeepassXC) che permettono la generazione di codici di sicurezza per l'MFA.

Vi illustriamo come procedere con le App Mobile:

- Google Authenticator
- Microsoft Authenticator

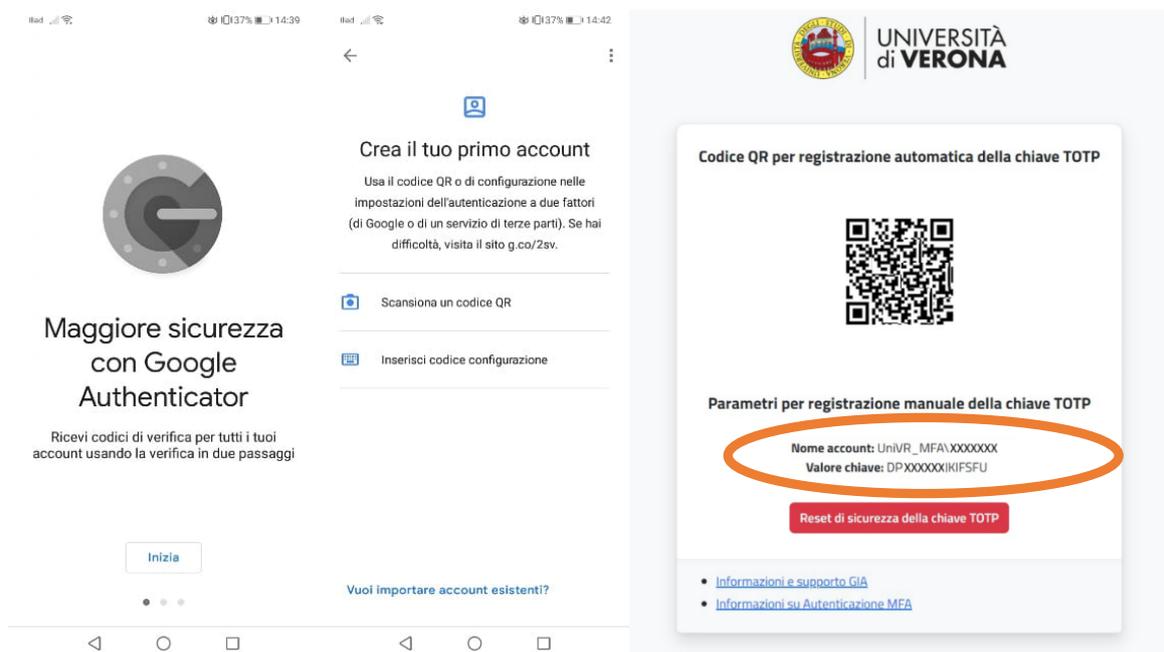
Configurare e ricevere i codici di verifica con Google Authenticator

Requisiti dell'app

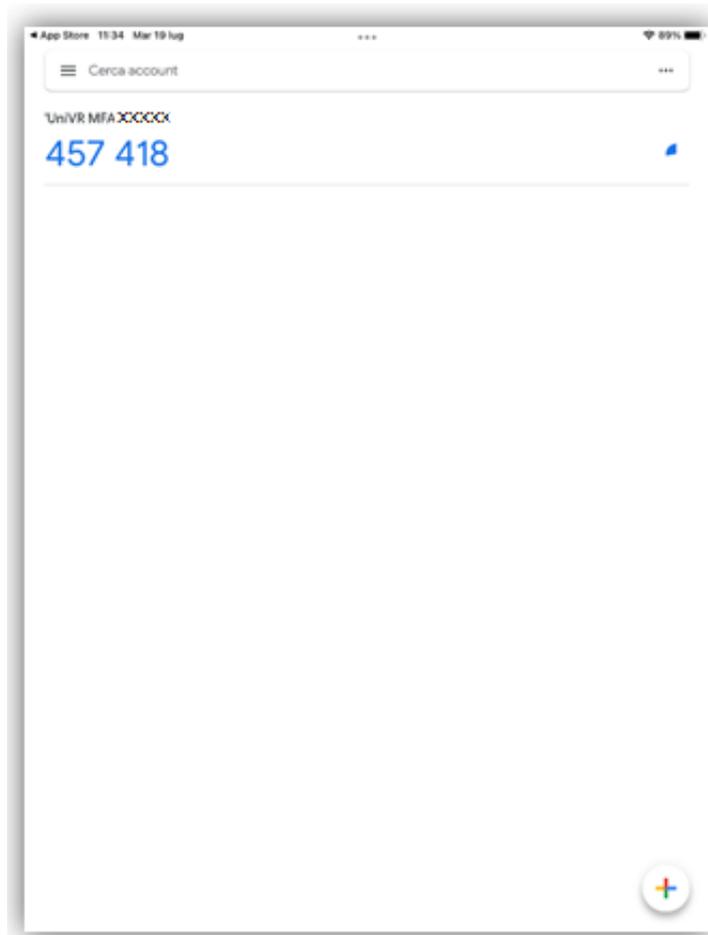
Per poter utilizzare Google Authenticator su iPhone, iPod Touch o iPad, devi disporre di iOS 13.0 o versioni successive

Procedimento

Dopo aver generato il codice QR (vedere il relativo paragrafo):



1. Scaricare e installare l'app nello Store Apple.
2. Creare un nuovo account e premere "Inizia"
3. Premere "Scansiona il codice QR"
4. e usare la fotocamera del dispositivo per analizzare il codice
5. Compare un nuovo account "UniVR_MFA\XXXXXX"
6. Premere su "Aggiungi account"



NB

1. Se si è già installato l'app:
2. Nell'app Authenticator selezionare il pulsante “+” (in basso a destra) quindi “Aggiungi account”
3. Premere “Scansiona il codice QR”
4. Compare un nuovo account “UniVR_MFA\XXXXXX”
5. Premere su “Aggiungi account”

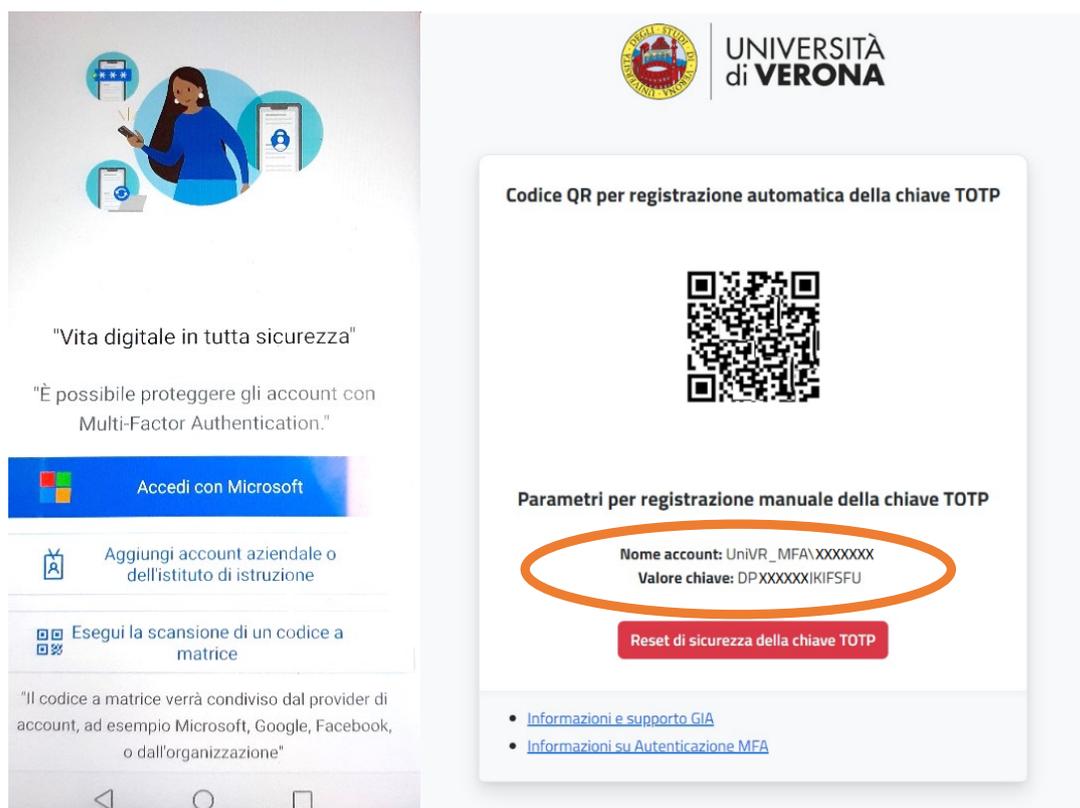
Configurare e ricevere i codici di verifica con Microsoft Authenticator

Requisiti dell'app

Per utilizzare Microsoft Authenticator sul su iPhone, iPod Touch o iPad, devi disporre di iOS 13.0 o versioni successive

Procedimento

Dopo aver generato il codice QR (vedere il relativo paragrafo):



1. Scaricare e installare l'app nello Store Apple.
2. Nell'app aggiungere un account e scegliere "Esegui la scansione di un codice matrice"
3. Premere "or enter code manually"
4. Inserire "Account name" e "Key Value" del codice QR generato nei rispettivi campi e premere "Fine"

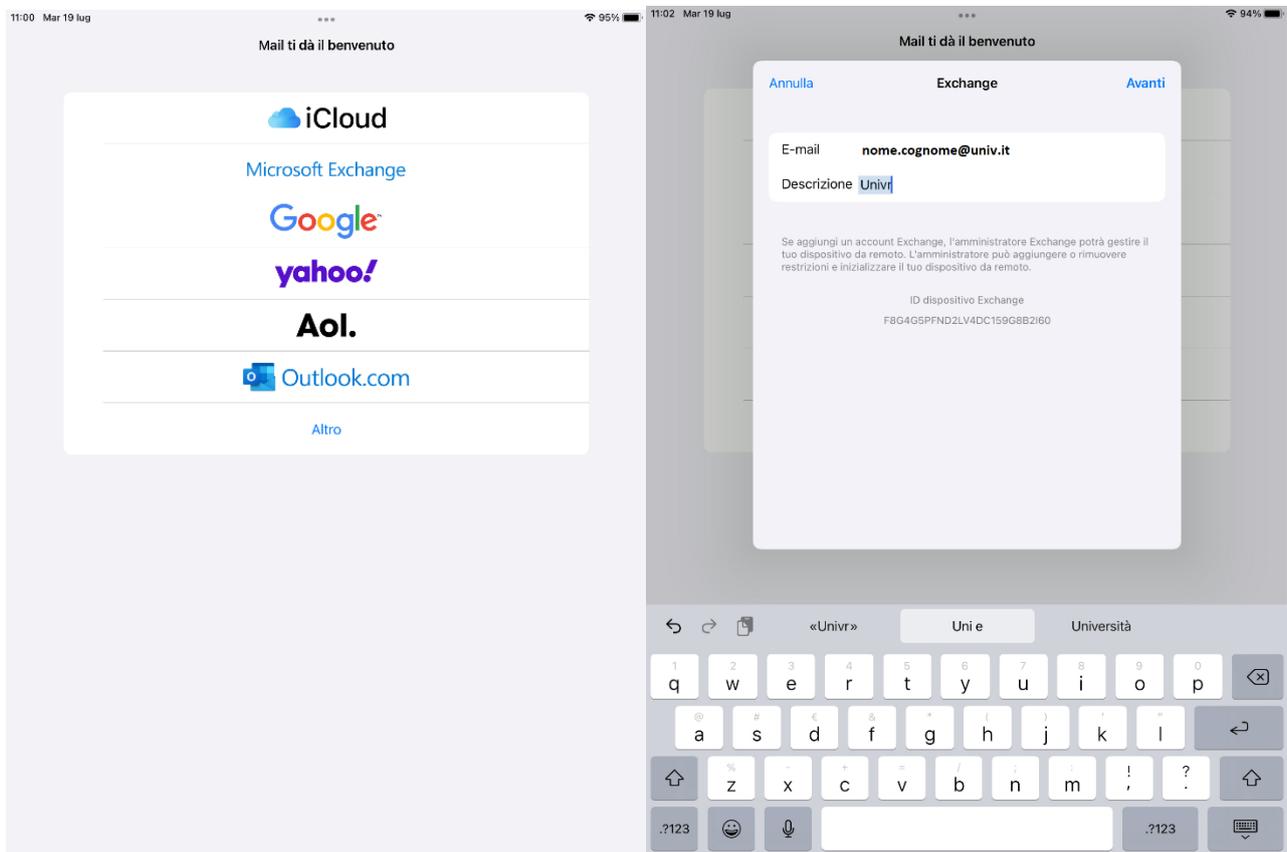
NB

1. Se si è già installato l'app
2. Nell'app Microsoft Authenticator selezionare [tre puntini] quindi + Aggiungi account
3. Scegliere "Altro account (Google, Facebook e così via)"
4. Premere "or enter code manually"
5. Inserire "Account name" e "Key Value" del codice QR generato nei rispettivi campi e premere "Fine"

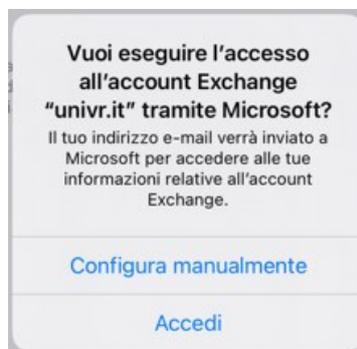
Configurare Mail

Procedimento

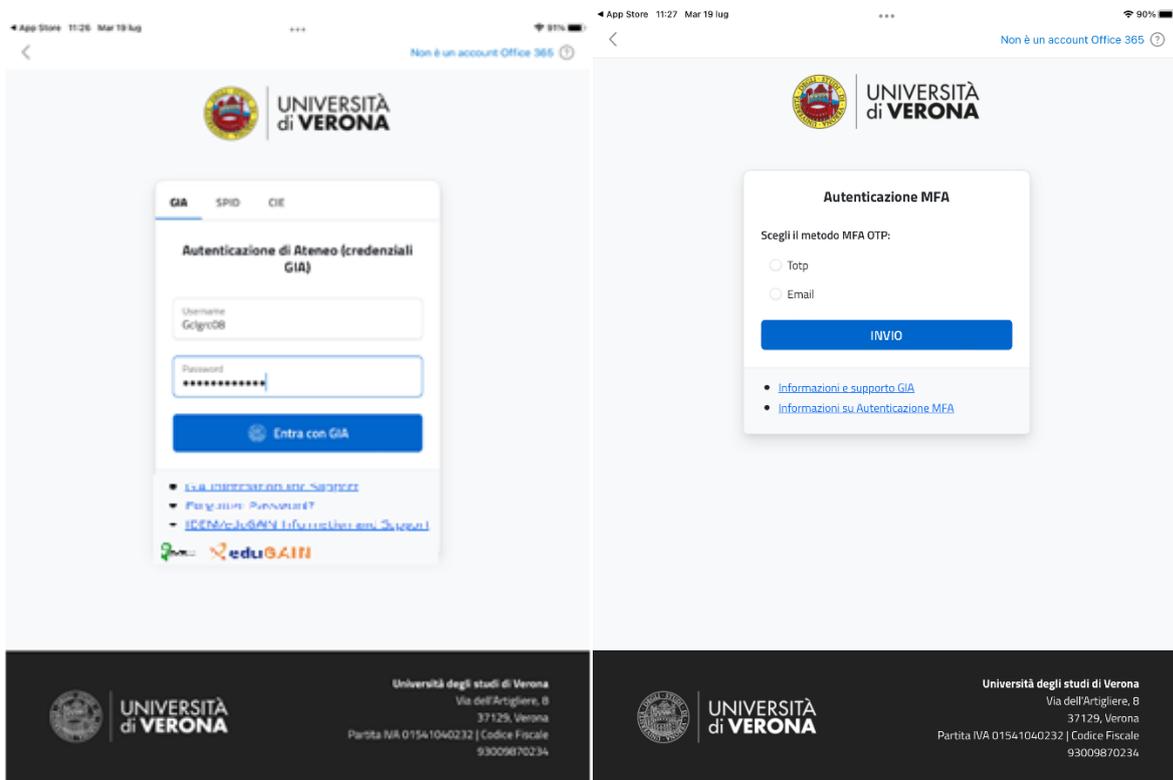
Selezionare “Microsoft Exchange” ed inserire la mail:



Premere il pulsante “Accedi”

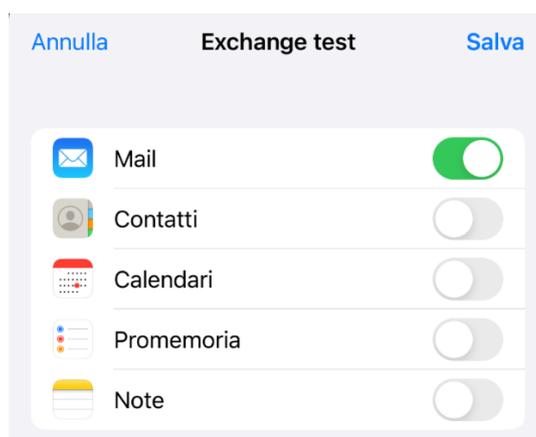


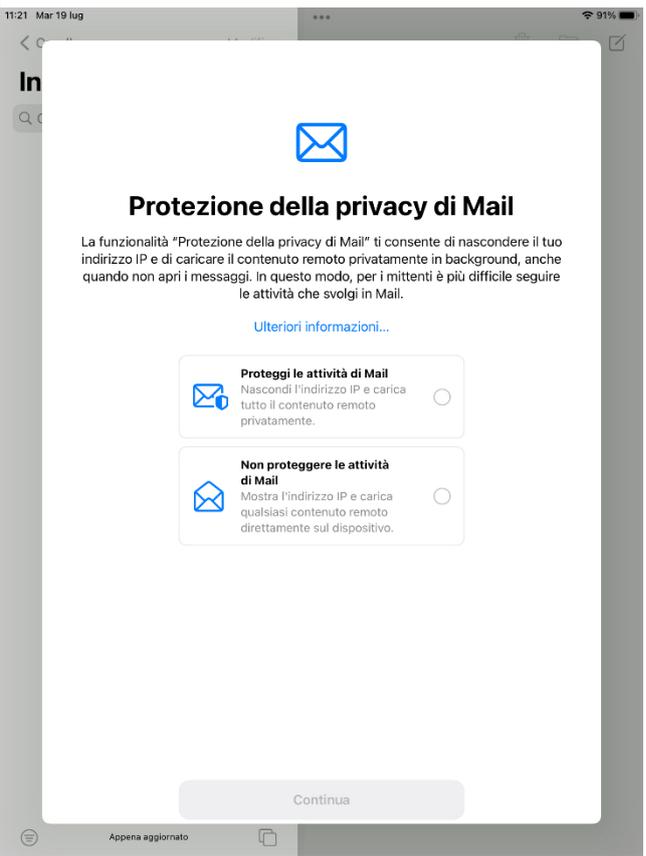
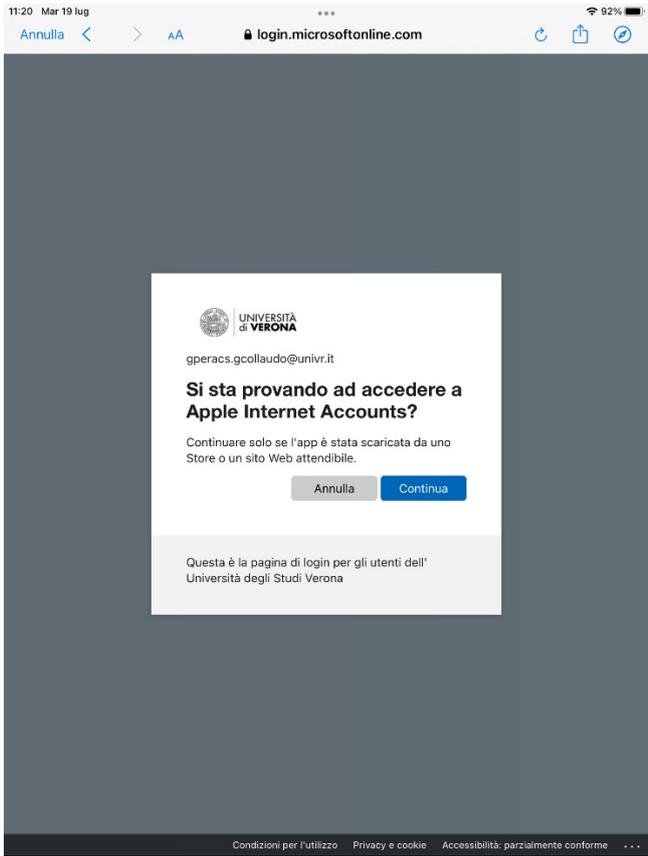
Autenticarsi con Login/password GIA e scegliere il metodo di autenticazione MFA preferito:



Inserire il codice di sicurezza OTP ricevuto e premere "Login"

Scegliere cosa sincronizzare (contatti, etc..)

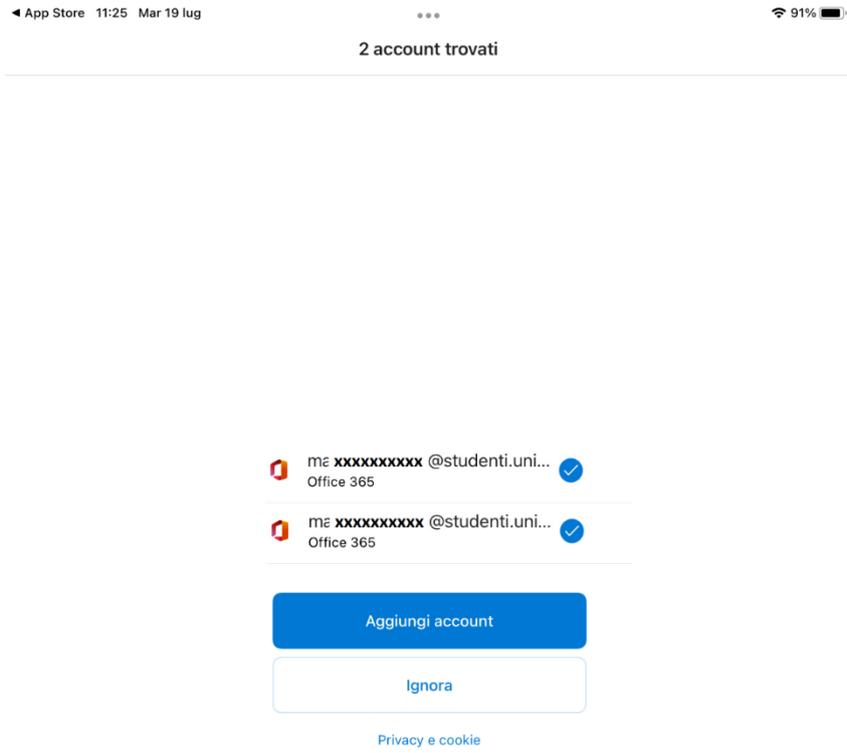




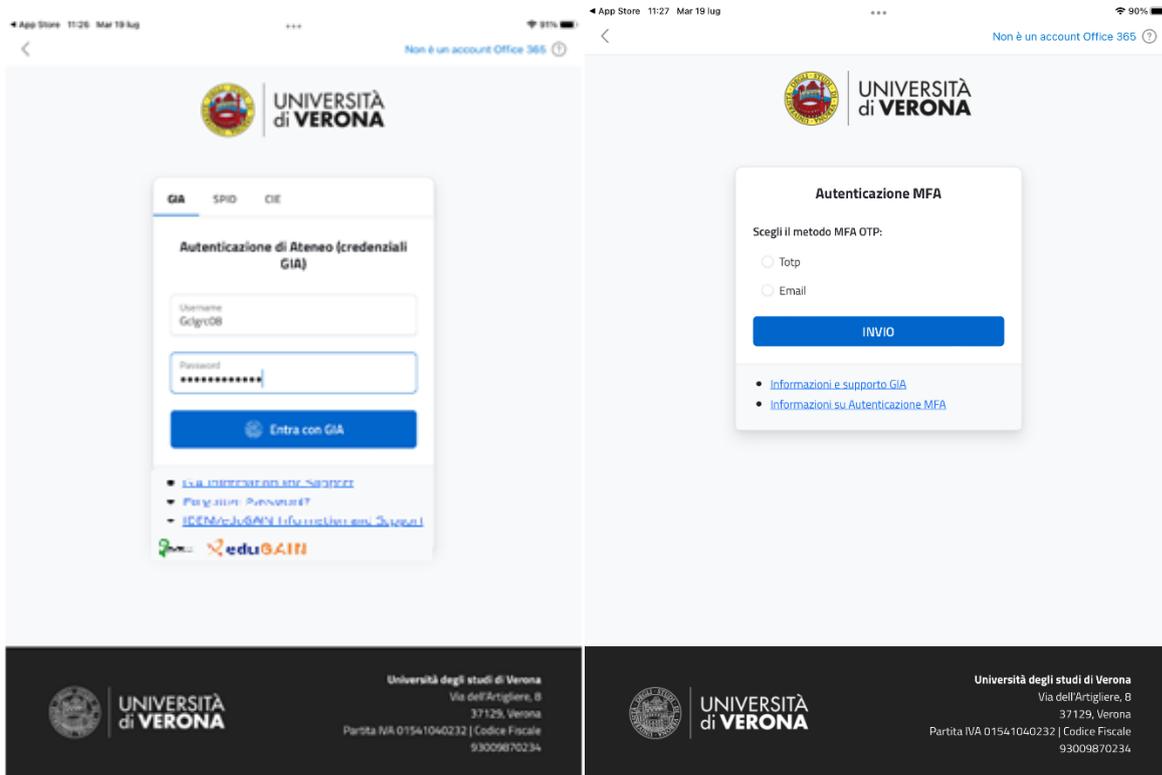
Configurare Outlook

Procedimento

Aprire Outlook e selezionare "Aggiungi account":



Autenticarsi con Login/password GIA e scegliere il metodo di autenticazione MFA preferito:



Inserire il codice di sicurezza OTP ricevuto e premere "Login"

Evidenziata Altro Filtro

La settimana scorsa

- MA** Microsoft Audio Confe... giovedì
Il Servizio di audioconferenza di...
– Il Servizio di audioconferenza di Office 365 è ora disponibile – Il...

maggio

- D** donotreply@univr.it 29/05/22
Reset Password
Password has been reset for user Gperacs Gcollaudo . You will be r...
- D** donotreply@univr.it 27/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...
- D** donotreply@univr.it 26/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...
- D** donotreply@univr.it 25/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...
- D** donotreply@univr.it 24/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...
- D** donotreply@univr.it 23/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...
- D** donotreply@univr.it 21/05/22
GIA Avviso Scadenza Password [...]
Gestione Identità di Ateneo Si avvisa che la password dell'acco...



Nessun messaggio selezionato

Seleziona un messaggio per leggerlo o scrivine uno nuovo.

[Nuovo messaggio](#)

Errore di configurazione MFA

Se compare il seguente *errore*:



Significa che:

Non è stata fornita una *email privata* all'università e quindi non è presente in ESSE3 carriere studenti (per gli studenti) o a DBERW (per il personale TA/docenti)

- ✓ [ESSE3](#) – Studenti
- ✓ [Dberw](#) - Personale

e non è stata registrata nessuna applicazione per l'autenticazione MFA via TOTP

Per risolvere:

- inserire un indirizzo email privata in ESSE3 carriere studenti (per gli studenti) o in DBERW (per il personale TA/docenti) ed autenticarsi con Login/password GIA e scegliere il metodo invio "Email" inserendo il codice OTP ricevuto. Vedi il paragrafo "Accesso da portale web – Metodo Email" nei manuali Windows o MAC

Oppure

- vedere il paragrafo "Generare il codice QR" nei manuali Android, Iphone o Ipad