**Autenticazione a Fattori Multipli (MFA - Multi factor Authentication)**

In questa guida troverai informazioni su:

* Cos'è l'autenticazione a Fattori Multipli (MFA - Multi factor Authentication)
* Come funziona l’MFA in Univr
* Quali applicativi richiedono l’MFA
* Come risolvere errori di configurazione
* Chi contattare in caso di problemi
* Dove trovo le guide e le informazioni su MFA

Per le seguenti procedure consultare invece la pagina del servizio [Autenticazione a Fattori Multipli (MFA - Multi factor Authentication)](https://www.univr.it/it/i-nostri-servizi/autenticazione-a-fattori-multipli-mfa-multi-factor-authentication/).

* Come inserire la mail privata in DBERW per attivare MFA (personale TA e Docente)
* Come generare il codice QR per registrare l'App Mobile per l'autenticazione MFA via TOTP
* Come resettare l'App Mobile per l'autenticazione MFA via TOTP
* Come utilizzare i codici OTP (su mail) o TOTP (su app) per accedere agli applicativi che richiedono MFA
* Come utilizzare MFA su Android
* Come utilizzare MFA su Iphone
* Come utilizzare MFA su Windows
* Come utilizzare MFA su Mac
* Come utilizzare MFA su Ipad
* Come utilizzare MFA su Linux

**Cos'è l'autenticazione a Fattori Multipli (MFA - Multi factor Authentication)**

L'Autenticazione a Fattori Multipli (MFA - Multi factor Authentication) è una tecnologia di sicurezza che prevede l'utilizzo di credenziali di categorie diverse e indipendenti nella verifica dell'identità di una persona nell'accesso a risorse protette. L'Autenticazione a Fattori Multipli impone l'utilizzo di due o più credenziali di categorie di sicurezza indipendenti: ad esempio qualcosa che una persona conosce (esempio login/password) con qualcosa che un utente possiede (esempio token di sicurezza) oppure con qualche sua caratteristica personale distintiva (esempio caratteristica biometrica).

L'obiettivo della MFA è quello di creare difese a più livelli che rendano più difficile per una persona non autorizzata accedere a risorse protette, siano esse fisiche o informatiche. Infatti, qualora un fattore di autenticazione viene compromesso, nel contesto di autenticazione MFA la persona non autorizzata che tenta di accedere alla risorsa protetta ha comunque una o più barriere aggiuntive da superare per raggiungere lo scopo.

La MFA è una componente essenziale della Gestione delle Identità e degli Accessi, in particolare per la definizione delle politiche di controllo all'accesso che regolano la definizione dei livelli di sicurezza specifici per le varie risorse gestite.

**Come funziona l’MFA in Univr**

L'autenticazione a più fattori (MFA - Multi Factor Authentication) utilizza più metodi di autenticazione per verificare l'identità dell'utente che desidera accedere.

**SPID**



**GIA + TOKEN**

Il token (termine informatico che indica un oggetto fisico o logico necessario per l’MFA) generalmente è un codice numerico e può essere fornito con due modalità:

* **OTP** (One Time Password) - il codice/token viene inviato via mail pertanto è **necessario inserire una mail privata in dberw** (TA e docenti) o in Esse3 (studenti); funziona senza alcuna configurazione dell’utente che ha l'unico compito di controllare la correttezza della propria email privata fornita all’università.
* **TOTP** (Time-Based One Time Password) - il codice/token viene inviato su app pertanto, oltre alla mail privata su dberw, è necessario anche installare una app su pc o smartphone, come ad esempio:
* ***App****licazioni Mobile* (Microsoft Authenticator, Google Authenticator, 2FA, …)
* **A*pp****licativi Desktop* in grado di supportare lo standard (es. KeepassXC).

**Quali applicativi richiedono l’MFA**

* DBERW
* OFFICE 365
* POSTA ELETTRONICA

**Come risolvere errori di configurazione**

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) **e non è stata registrata nessuna applicazione per l’autenticazione MFA via TOTP.**



**Per risolvere ci sono due opzioni:**

* 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
* vedere il paragrafo “Registrare l’Applicazione per l’autenticazione MFA via TOTP” nei manuali Android, Iphone o Ipad

**Chi contattare in caso di problemi**

In caso di problemi con MFA contattare i tecnici dei [**Gruppi di supporto tecnico informatico per area di riferimento**](https://www.univr.it/it/i-nostri-servizi/supporto-informatico-/gruppi-di-supporto-tecnico-informatico-per-area-di-riferimento).

**Dove trovo le guide e le informazioni su MFA**

Tutte le informazioni aggiornati e le guide specifiche distinte per applicativo e dispositivo sono disponibili nella sezione documenti di questa pagina.