OT MAIL: Abilitazione Autenticazione a Due Fattori (2FA)

Guida pratica per gli utenti

Sommario

1. Autenticazione a Due Fattori (2FA)

La 2FA, o "Two-Factor Authentication" (autenticazione a due fattori), è un metodo di sicurezza che aggiunge un ulteriore livello di protezione all'accesso ad un account online. La 2FA richiede all'utente di fornire due fattori distinti per verificare la sua identità, anziché uno solo come nel caso della tradizionale autenticazione solo con password. Se un malintenzionato riuscisse a scoprire la password di un account, non avrebbe accesso al secondo fattore di autenticazione necessario per completare il processo di accesso. Un esempio di autenticazione a due fattori è l'accesso al conto corrente: vengono sfruttati un ID, una password e una one-time password o OTP, cioè un codice usabile una volta sola generatosi attraverso un token.

La 2FA è efficace per la sicurezza dei tuoi account OT MAIL, protegge le tue mail, le tue informazioni e dati, ma allo stesso tempo evita l'uso da parte di terzi della tua mail, ad esempio per mandare mail di spam o usare la tua identità.

2. Authenticator

Per la gestione della 2FA è necessario avere a disposizione un'applicazione di autenticazione ("Authenticator"), che si consiglia fortemente di installare su un dispositivo mobile smartphone o tablet (Android/IOS).

Per OT MAIL consigliamo, per i diversi sistemi operativi:

Applicazione	iOS	Android	Windows	macOS
Google Authenticator	✓	✓		
Microsoft Authenticator	✓	✓	✓	
Twilio Authy	✓	✓	✓	✓

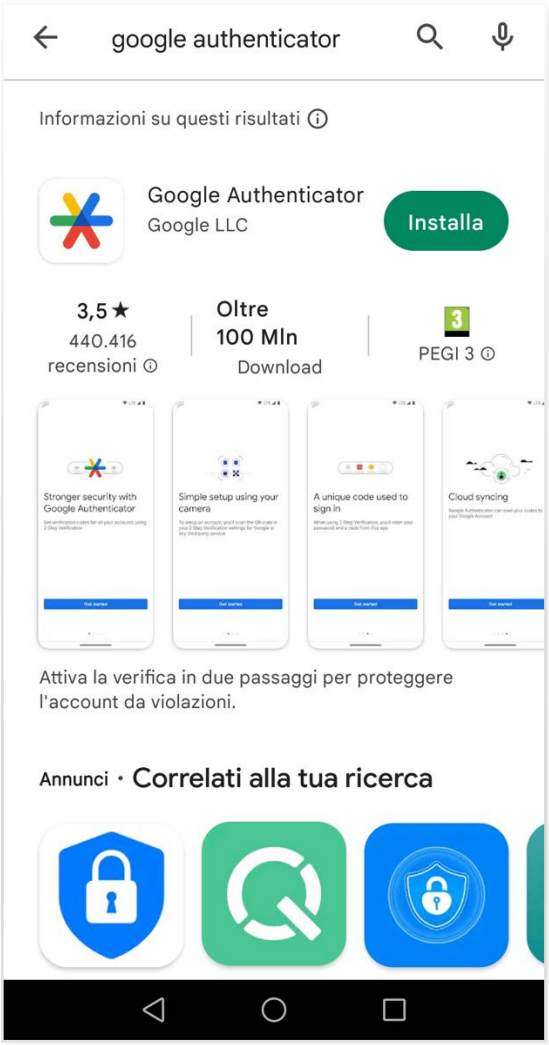
Nel successivo capitolo è descritta la procedura esemplificativa di installazione di Google Autenticator su iOS e Android.

2.1 Installazione Google Authenticator

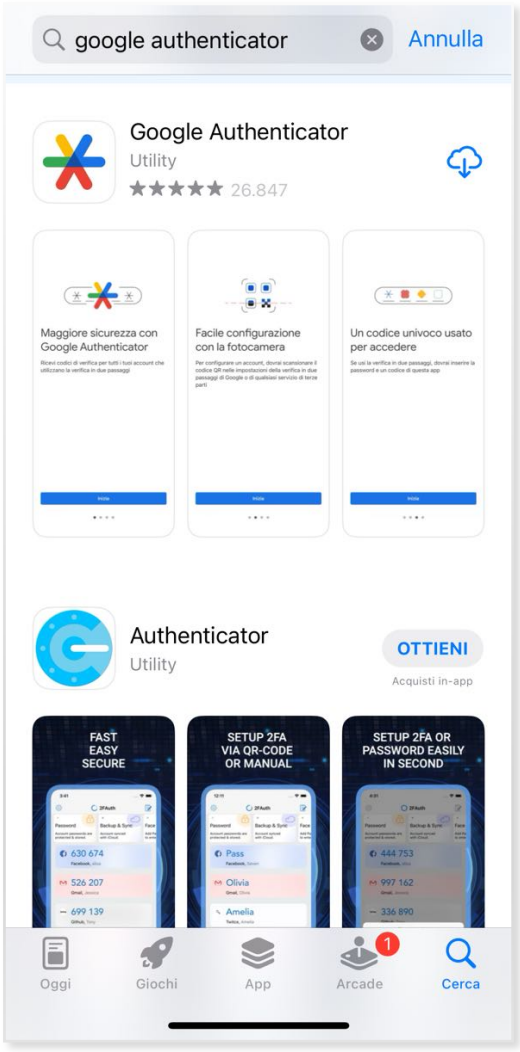
È consigliato installare l'applicazione di autenticazione su uno smartphone, per garantire un ulteriore livello di sicurezza. Una delle applicazioni più utilizzate per la 2FA su OT MAIL è "Google Authenticator", gratuita e disponibile per Android e iOS.
Per l'installazione, accedere con il proprio dispositivo mobile nello store del proprio ecosistema: Google Play Store o App Store.

Cercare "Google Authenticator" e installarlo.

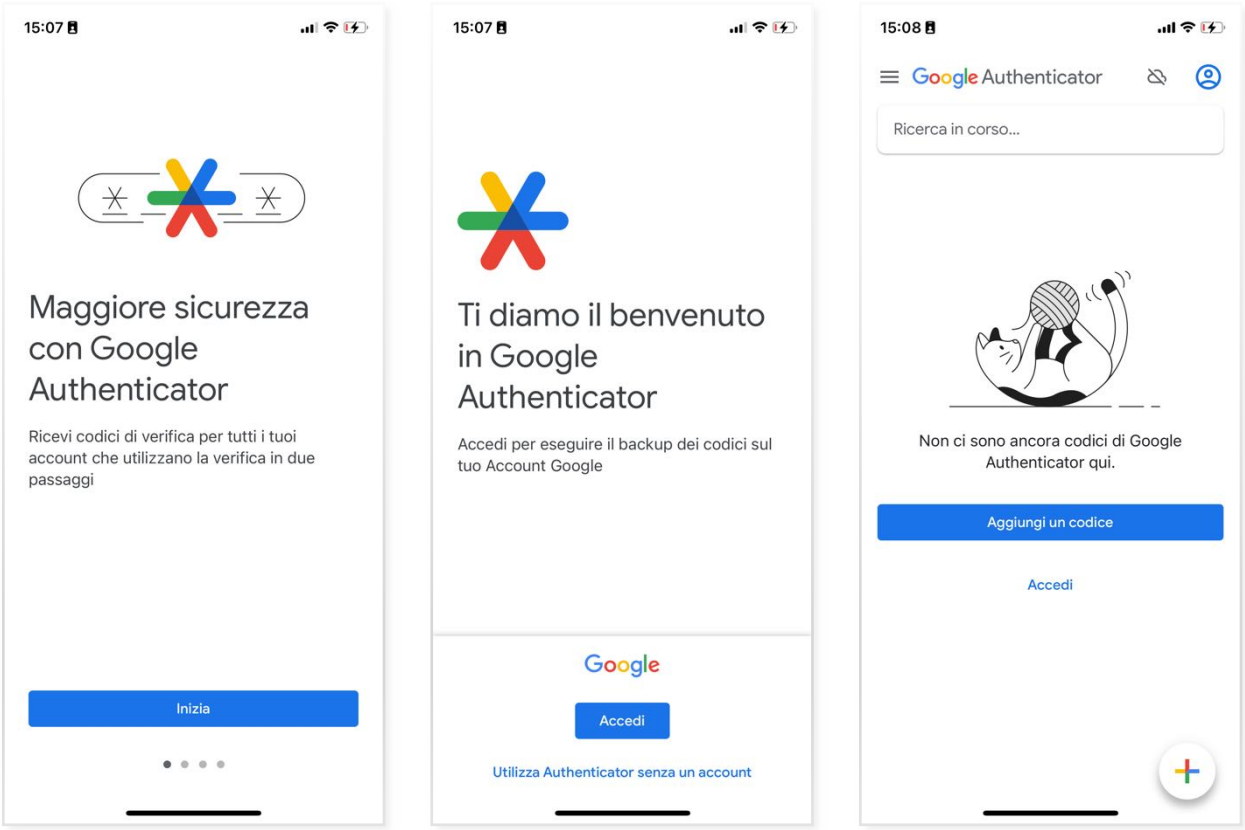
Android:



iOS:



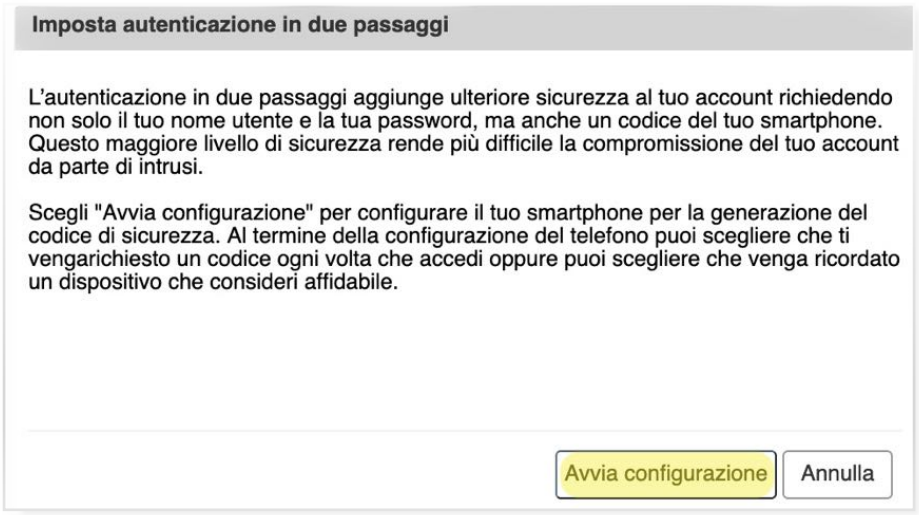
Completata l'installazione, aprire l'applicazione e seguire le indicazioni accedendo all'eventuale account Google personale, oppure continuare con l'opzione "Utilizza Authenticator senza un account".



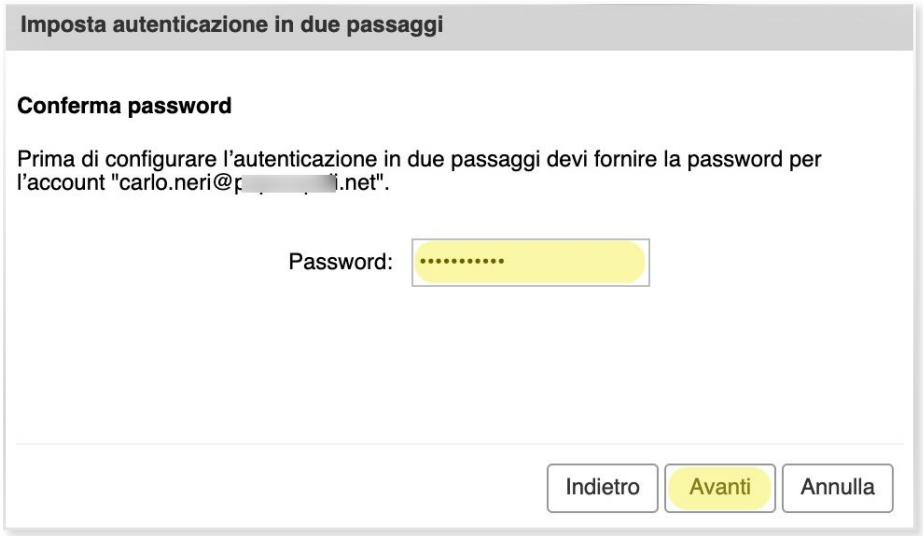
A questo punto siamo pronti per attivare la 2FA su OT MAIL utilizzando “Google Authenticator” per proteggere la nostra mail.

3. Abilitazione 2FA in OT MAIL

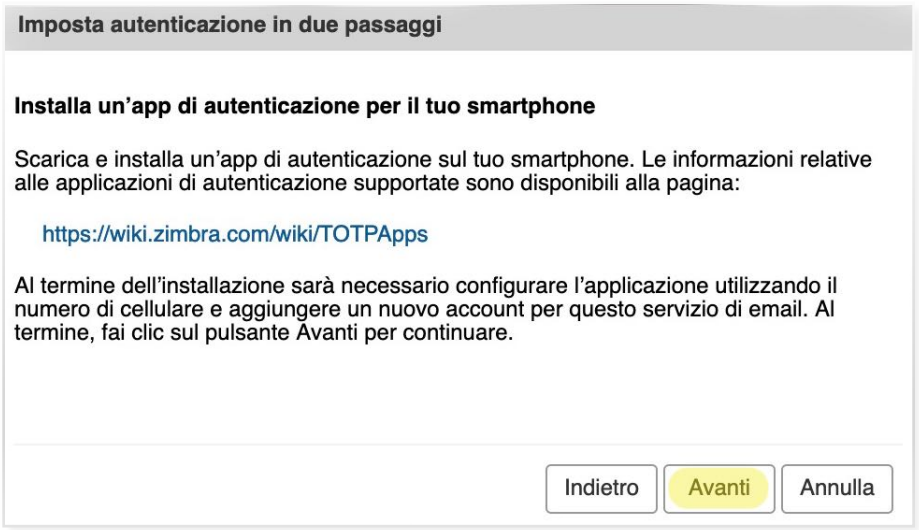
Se l'uso di 2FA è abilitato come necessario dal gestore della posta, **al primo login via web** (https://ot-mail.it) comparirà il seguente avviso:



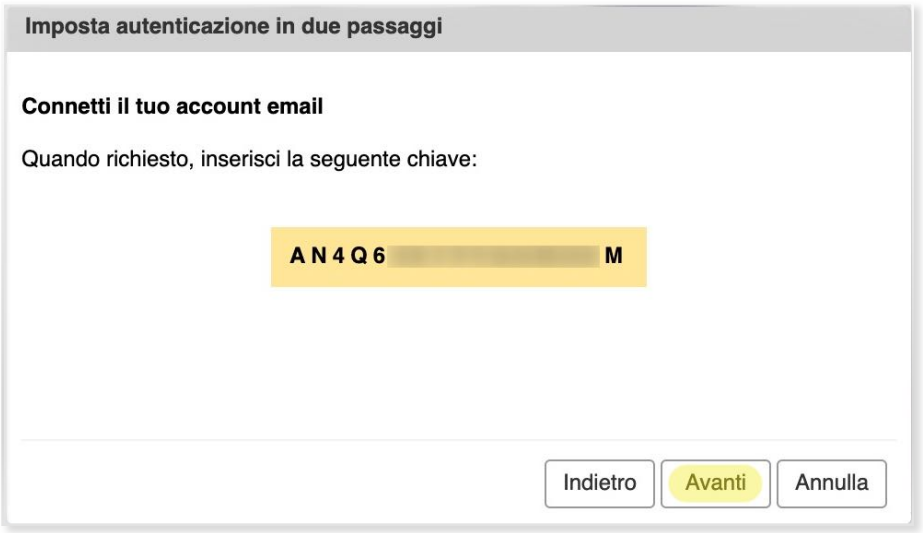
Cliccare "Avvia configurazione" per proseguire.



Inserire la password della propria casella di posta e cliccare su "Avanti".



Aprire l'applicazione Autenticator che si è scelto di usare, o installarla (se non già presente) sul proprio smartphone.
Procedere con "Avanti"

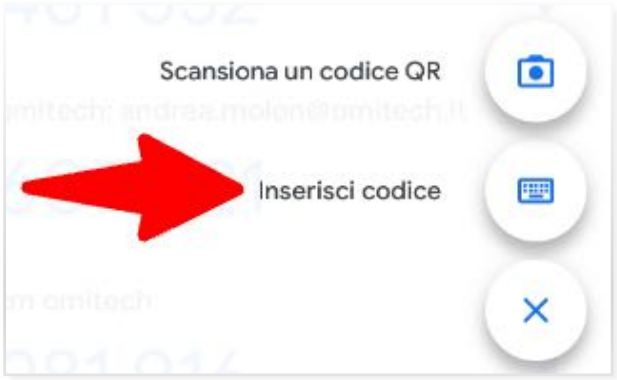


In questa schermata è mostrato il codice di 16 caratteri da inserire come codice di attivazione nell'Autenticator.

Di seguito i passaggi di esempio con Google Authenticator, la stessa procedura è applicabile agli altri Authenticator.

Con Google Authenticator, ad esempio. Aperta l'applicazione selezionare "Aggiungi un Codice" se non è già usato anche per altre applicazioni. Oppure il"+"

Successivamente "inserisce codice"



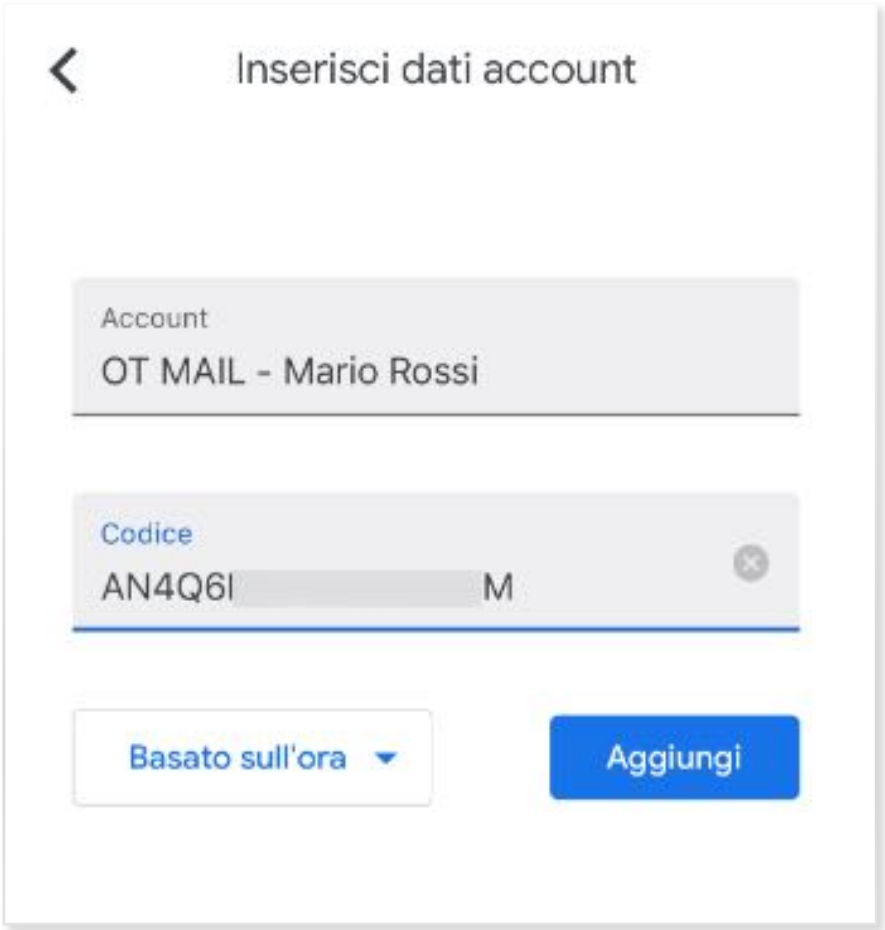
Nella schermata di inserimento codice sono presenti due campi:

- **Account:** nome per riconoscere l'applicazione per cui si sta inserendo il codice.

Ad esempio: OT MAIL o Nome Utente oppure l'indirizzo mail

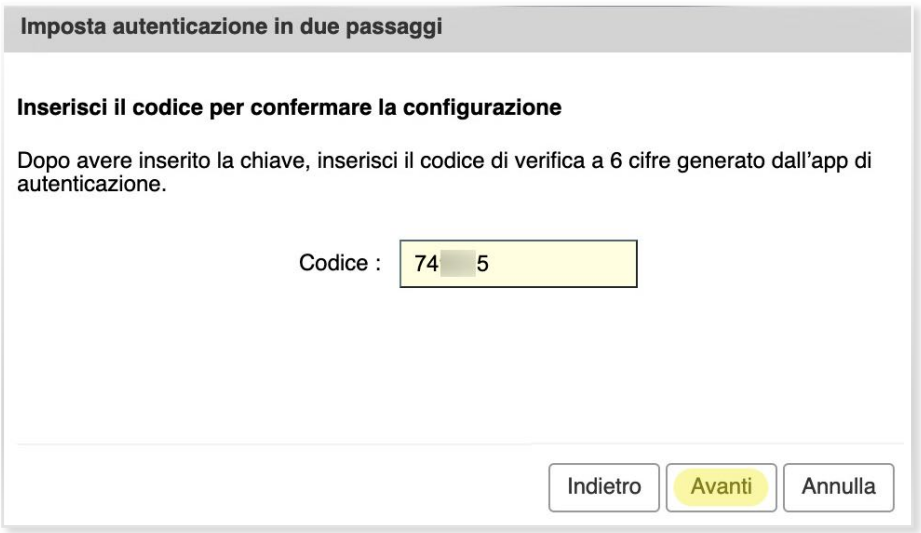
- **Codice**: il codice alfanumerico di 16 cifre generato in OT MAIL

Se dovesse essere richiesta la modalità, selezionare "basato sull'ora".



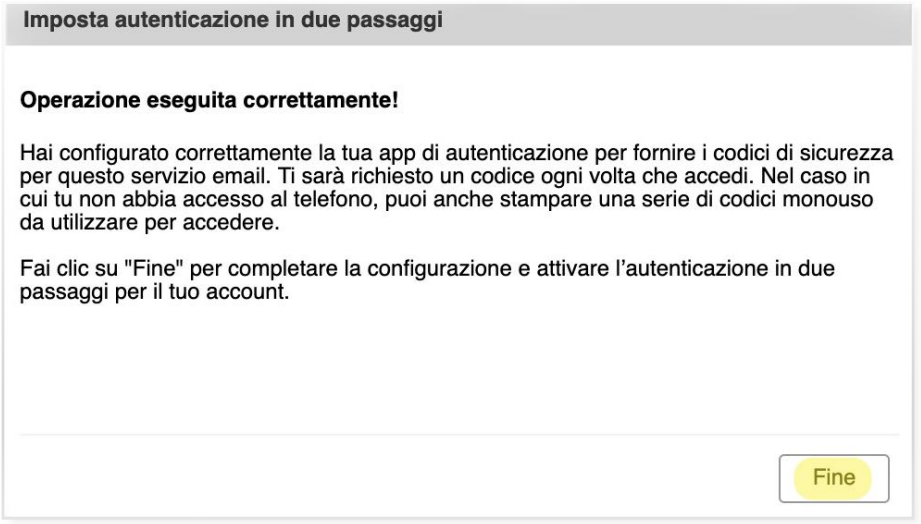
Aggiungendo l'account abbiamo terminato.

Google Authenticator è pronto e ci mostra il primo codice da usare per completare l'abilitazione. Il codice generato dura 30 secondi, alla scadenza non è più valido e ne viene mostrato uno nuovo.



Su OT MAIL inserire il codice di 6 cifre OTP generato in Authenticator.

Procedendo con avanti il codice è validato e avremo la conferma dell'attivazione della 2FA.



A questo punto la 2FA è abilitata e all'utente verrà richiesto un nuovo codice ad ogni nuovo accesso da browser, smartphone o altra app a cui tenta di accedere con il proprio account.

Ricordiamo che i codici hanno una durata di 30 secondi.

Nota: Si consiglia di generare e salvare in modo sicuro una serire di codici monouso, come descritto nel relativo paragrafo "Codici monouso".

4. Accedere a OT MAIL con 2FA

Abilitata la 2FA il nostro account OT MAIL è protetto da un'ulteriore protezione. Per accedere alla posta sarà richiesto un codice OTP oltre alle consuete credenziali utente e password.

4.1 Web Mail

Per accedere a OT MAIL via web procedere come di consueto (https://ot-mail.it) inserendo le proprie credenziali, all'invio sarà visualizzata una nuova schermata per l'inserimento dell'OTP generato dall'app di Authenticator.
Il codice è richiesto ad ogni login, se si accede da una postazione sicura, ad esempio non condivisa o temporanea, è possibile selezionare "Considera questo computer affidabile". In questa modalità il browser in uso è considerato affidabile e non è richiesto ad ogni login l'OTP, ma solo l'inserimento delle credenziali.

Di tanto in tanto la 2FA potrebbe non riconoscere il browser e richiedere nuovamente l'OTP.

Il comportamento è normale, ad esempio, a seguito di aggiornamenti o pulizia della cache locale.

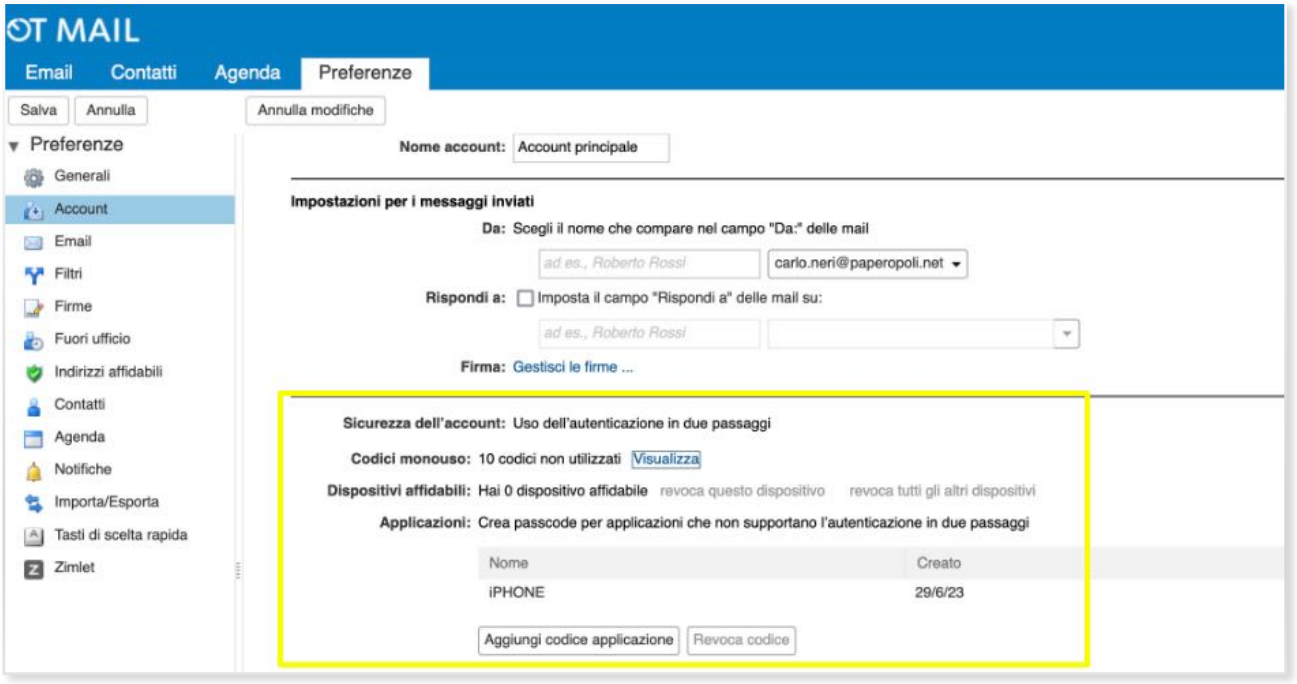
Nei prossimi paragrafi è descritta passo-passo la gestione della 2FA e della sicurezza in OT MAIL, oltre a come configurare un client di posta o lo smartphone per la nuova modalità.

Non appena attivata la 2FA, eventuali smartphone o client (es. Outlook) devono essere configurati al nuovo standard, per evitare che i tentativi di accesso errati generino il blocco dell'account.

4.2 Dispositivi attendibili e Passcode

Fatto l'accesso web a OT MAIL nelle Preferenze avremo la possibilità di gestire la 2FA.

Avremo una nuova sezione in *Preferenze* → *Account*

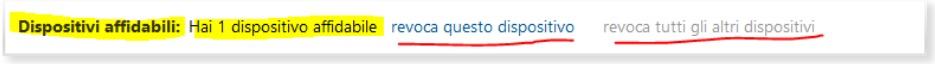


Qui è possibile:

- Gestire i dispositivi affidabili
- Generare i codici monouso
- Gestire le applicazioni

4.2.1 Dispositivi affidabili

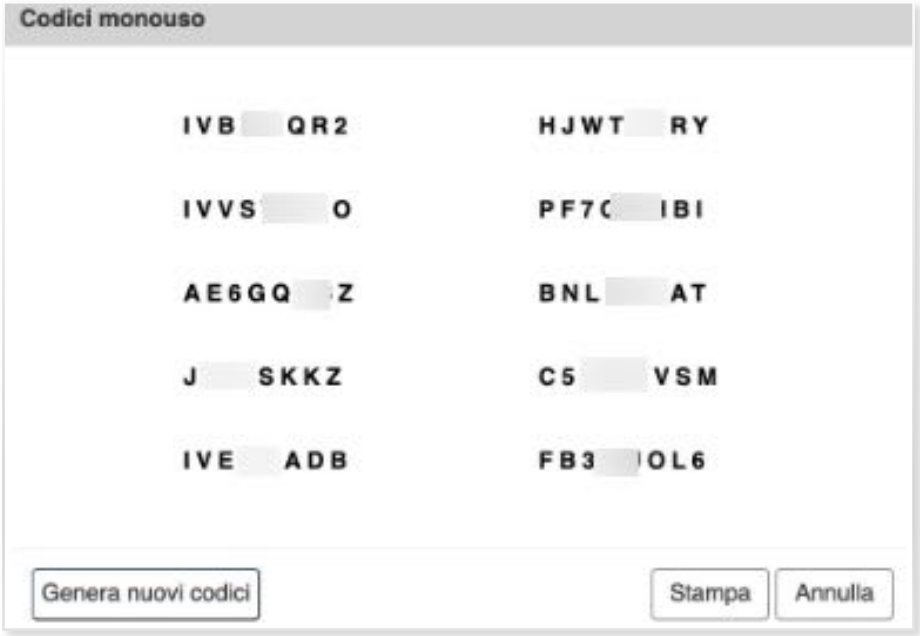
Quando, accedendo a OT MAIL, selezioniamo "Considera questo computer affidabile", non sarà richiesto per questo dispositivo l'autenticazione a 2 fattori: esclusione potrà essere modificata in questa sezione.



Qui è possibile revocare lo stato di "affidabilità" di questo dispositivo o tutti gli altri, la funzione è utile per eliminare precedenti dispositivi autorizzati.

4.2.2 Codici monouso

È consigliato generare i codici monouso, salvarli in posto sicuro o stamparli.



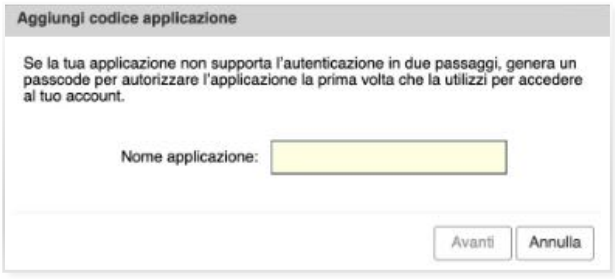
Questi codici, di 8 cifre, non 6 come i normali OTP, possono essere usati una sola volta per accedere.

Nel caso in cui l'app Authenticator non sia disponibile, permettono l'accesso a OT MAIL.

4.2.3 Applicazioni che non supportano l'autenticazione a due fattori

È possibile usare OT MAIL, con la sicurezza dell'autenticazione in due passaggi, anche con applicazioni che non la supportano grazie alla "passcode", che è praticamente una nuova password da usare solo in quell'applicazione.

Per generare un "passcode" cliccare "Aggiungi codice applicazione".

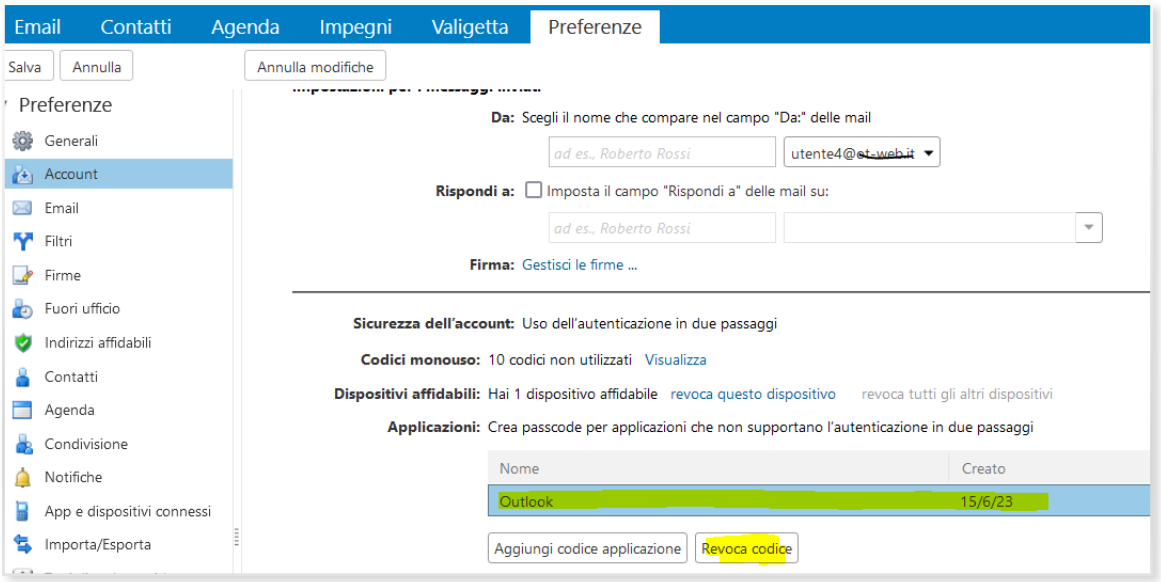


Inserire un nome per l'applicazione, ad esempio "telefono" e confermare.

Il sistema ci presenterà il "passcode" specifico che sarà usato dall'applicazione per autenticarsi.

Il "passcode" è usabile per una sola applicazione e solo una volta.

Le applicazioni autorizzate sono elencate sempre in *Preferenze → Account.*

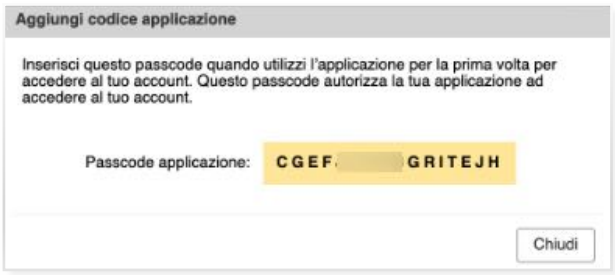


È possibile revocare i "passcode" selezionando l'applicazione e Cliccando su "Revoca Codice".

4.3 Smartphone

Le applicazioni dei telefoni non supportano solitamente l'autenticazione a due fattori.

Per continuare ad utilizzare, o riconfigurare, un account OT MAIL deve essere impostata come password dell'account sullo smartphone un "passcode" generato come sopra descritto.

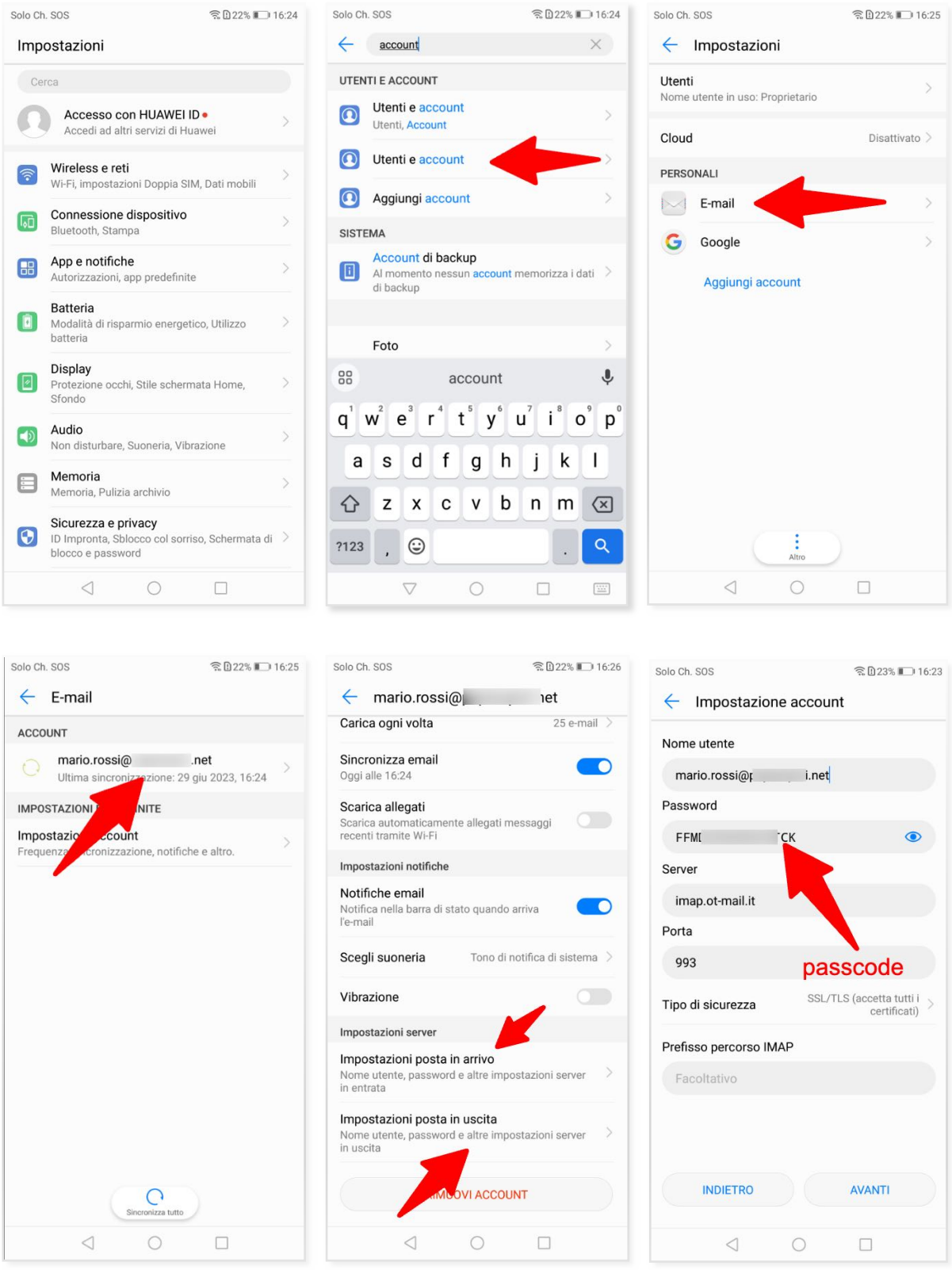


Aggiungere una nuova applicazione in *Preferenze → Account → Applicazioni*; inserire un nome riconoscibile es iPhone, Telefono, Samsung, Cellulare etc e generare il "passcode".

Se non era già configurato un account OT MAIL nello smartphone seguire la guida disponibile in https://msp.omitech.it/assistenza/ per impostare un nuovo account. Inserire il "passcode" generato al posto della password.

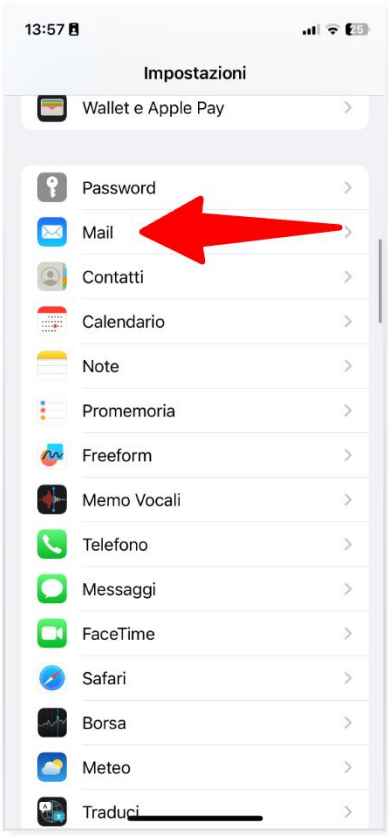
Nel caso ci sia già un account configurato procedere accedendo ad Impostazioni → *Account → Selezionare l'account da modificare → Inserire il "passcode" al posto della password.*

Android

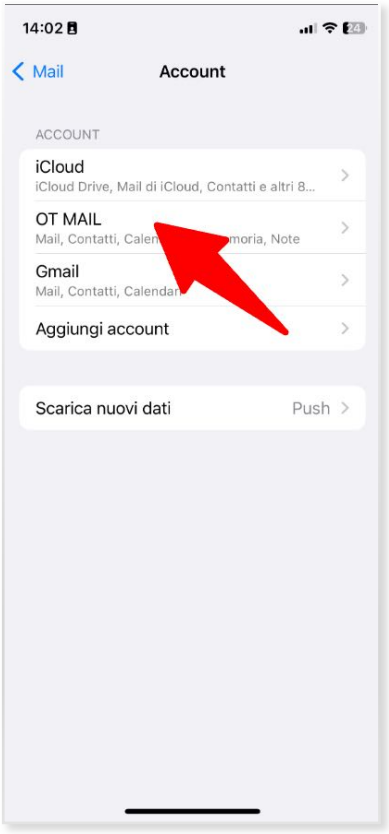


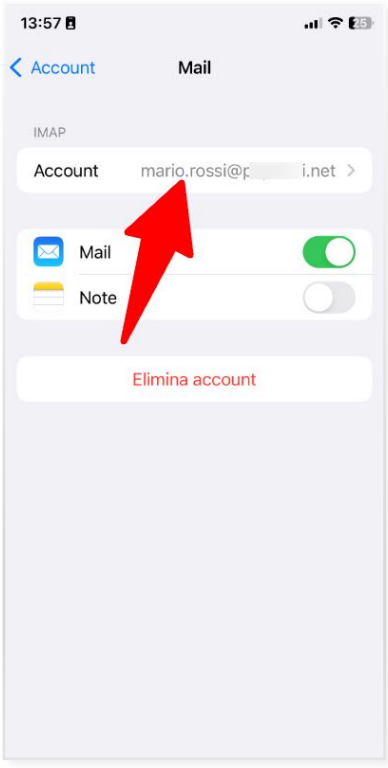
A seconda della versione software e della modalità di configurazione potrebbe essere necessario impostare la nuova password anche per la posta in uscita.

iOS


13:57
Impostazioni
Wallet e Apple Pay
Password
Mail
Contatti
Calendario
Note
Promemoria
Freeform
Memo Vocali
Telefono
Messaggi
FaceTime
Safari
Borsa
Meteo
Traduci


13:57
Impostazioni
Mail
CONSENTI A MAIL DI ACCEDERE A:
Siri e ricerca
Notifiche
Immediate
Dati cellulare
LINGUA PREFERITA
Italiano
Account
4
ELENCO MESSAGGI DI POSTA
Anteprima
2 righe
Mostra etichette A/Cc
Opzioni scorrimento
MESSAGGI
Conferma eliminazione
Protezione della privacy


14:02
Mail
Account
ACCOUNT
iCloud
iCloud Drive, Mail di iCloud, Contatti e altri 8...
OT MAIL
Gmail
Aggiungi account
Scarica nuovi dati
Push


13:57
Account
Mail
IMAP
Account
Mail
Note
Elimina account

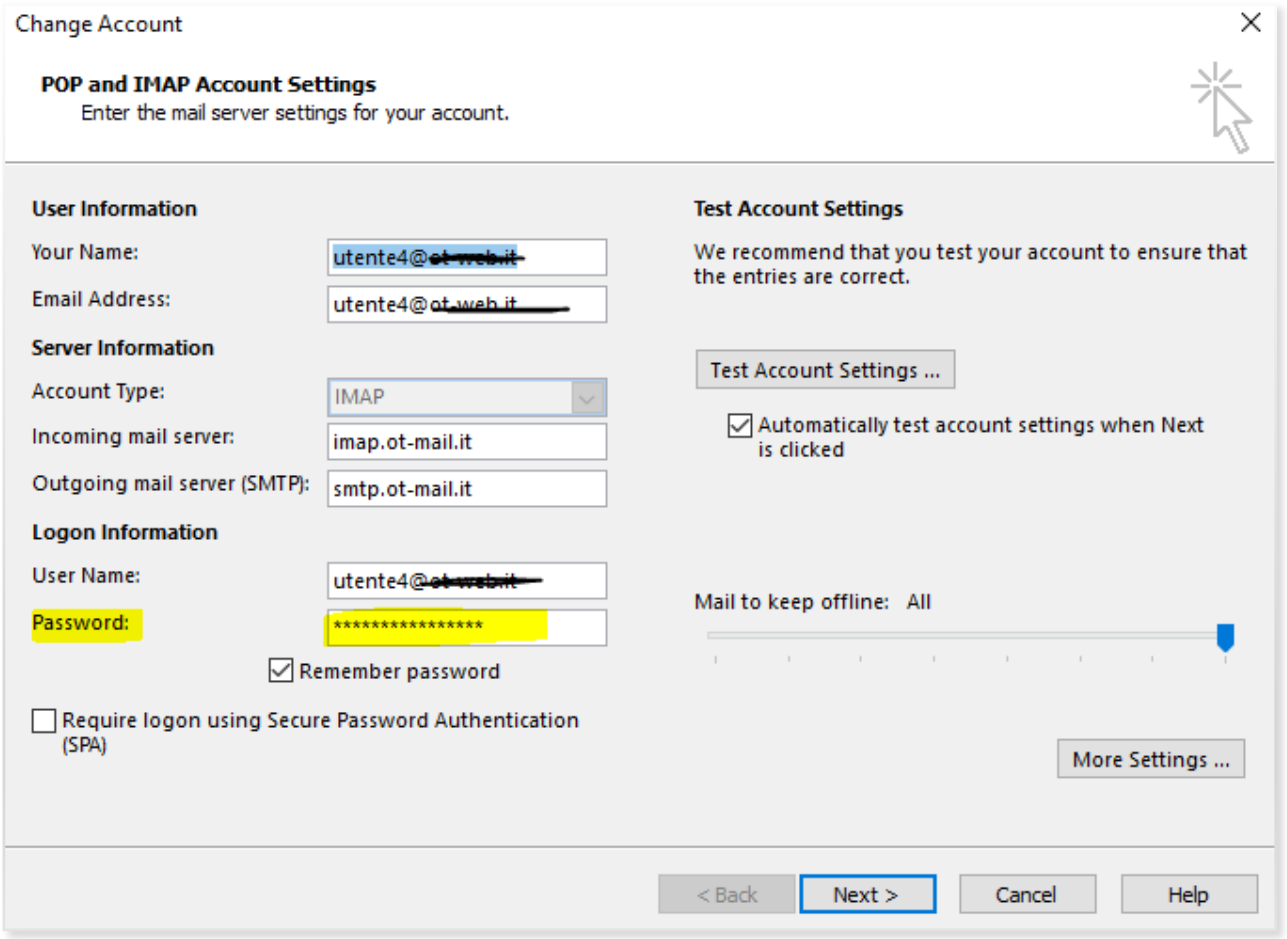

13:57
Annulla
Account
Fine
INFORMAZIONI ACCOUNT IMAP
Nome
Mario Rossi
Email
Descrizione
Mail
SERVER POSTA IN ARRIVO
Nome host
imap.ot-mail.it
Nome utente
Password
SMTP
smtp.ot-mail.it
passcode
Avanzate

4.4 Microsoft Outlook

Se per esempio si vuole creare il passcode per account configurati in Outlook, una volta cliccato su “Aggiungi Codice Applicazione”

Aggiungere una nuova applicazione in *Preferenze* → *Account* → *Applicazioni*; inserire un nome riconoscibile es OUTLOOK e generare il “passcode”.

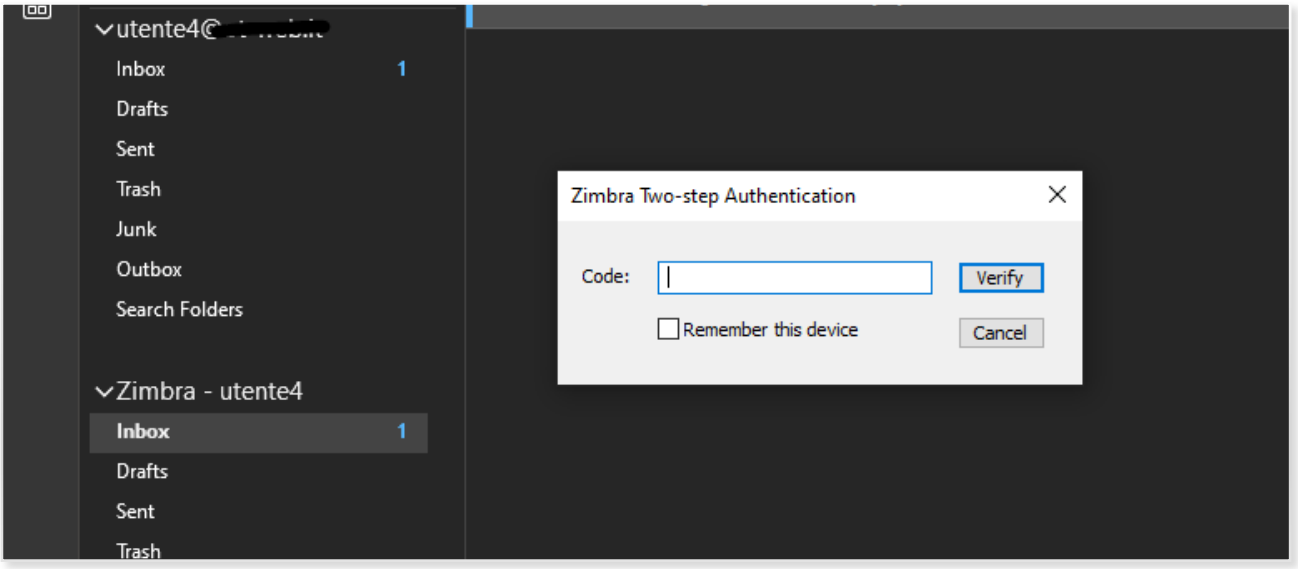
Il Passcode applicazione generato dovrà essere inserito come password durante la configurazione dell’account sul client di posta, aprendo le impostazioni dell’Account Outlook:



In caso di modifica di un account già configurato, il passcode andrà a sostituire la password standard precedentemente inserita. In caso di configurazione ex-novo, andrà inserito direttamente il passcode generato.
È possibile naturalmente creare più passcode per ogni applicazione utilizzata.

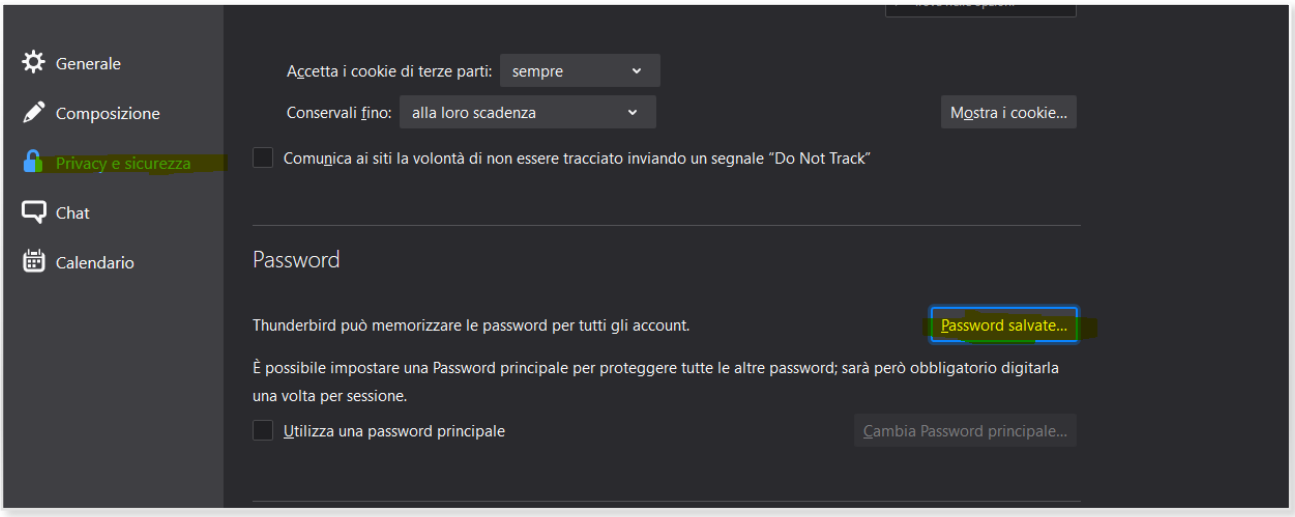
4.5 Connettore Zimbra

Se in uso il connettore Zimbra con Outlook, eseguendo un "Invia&Ricevi", dovrebbe apparire in automatico un box per l'inserimento del passcode generato via Web, come sopra descritto. Inserendo il passcode e procedendo con la verifica è possibile far ricordare il dispositivo, per trattarlo come autorizzato.

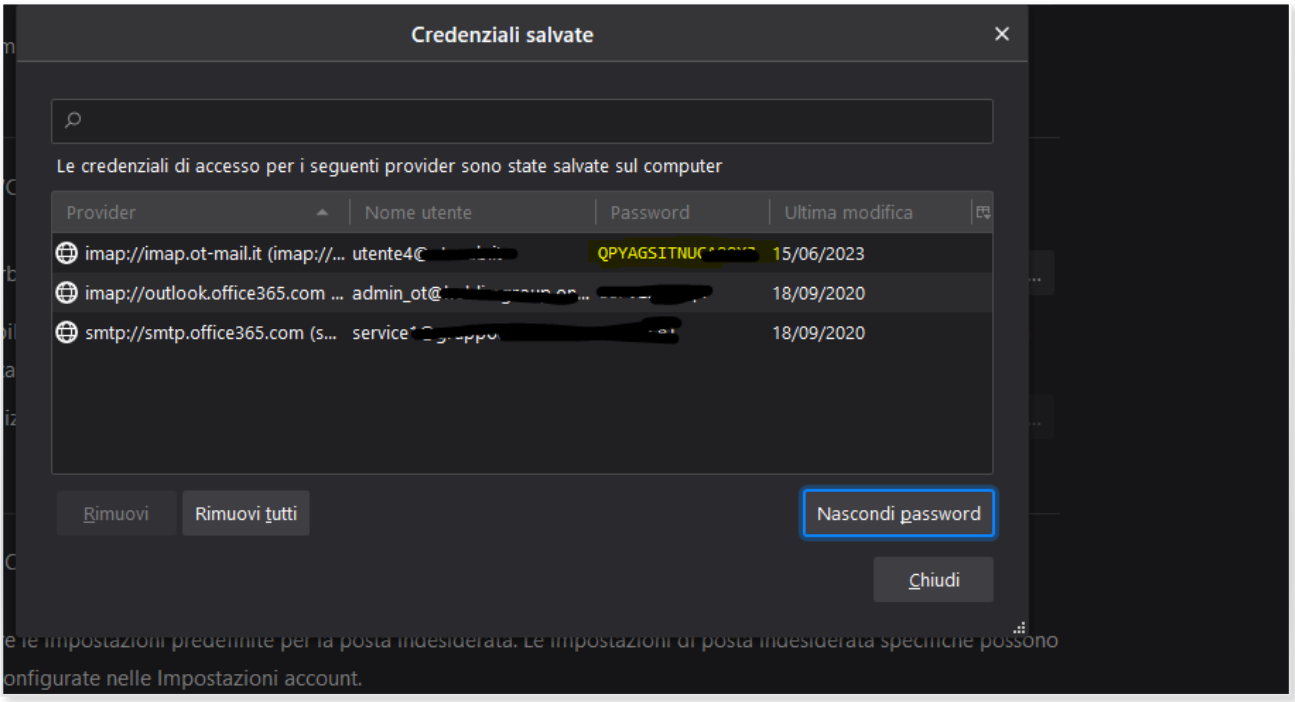


4.6 Altri Client es Mozilla Thunderbird

Procedere con la creazione di un nuovo passcode, come sopra descritto.
Il passcode generato dovrà essere utilizzato su Thunderbird nel campo password dell'account. Se l'account fosse già configurato, in base alla versione installata di Thunderbird utilizzata, andare in Opzioni → Privacy e Sicurezza



Cliccando su "Password Salvate" è possibile modificare la password con il passcode generato.



Se l'account viene configurato ex-novo, inserire il passcode in fase di configurazione.