

MANUALE PER ACCEDERE ALLA COMMUNITY DI OFFICINA – BACK-END



Confidenziale: questo documento e le informazioni in esso contenute sono riservate ad uso esclusivo di Officina [Agenzia del Demanio]. Accenture ha raccolto queste informazioni e preparato questo documento in buona fede e in conformità con le leggi applicabili. Ciascuna parte si impegna a prendere misure per proteggere la segretezza ed evitare la diffusione delle informazioni riservate ivi contenute.

Indice

Introduzione

Processo front-end

Processo back-end

Introduzione

Il presente manuale ha l'obiettivo di descrivere il processo che consente di invitare utenti esterni al dominio Agenzia del Demanio, come Guest User in una specifica Community Viva Engage.

Per permettere l'accesso anche agli utenti provvisti di account personale (no Business), è stata disegnata una soluzione che utilizza un secondo tenant Entra ID (sempre di Agenzia del Demanio) in cui vengono create le utenze degli utenti che richiedono l'accesso alla Community. Queste utenze vengono poi invitate come Guest User nel primo tenant Entra ID (Agenzia del Demanio) e successivamente inserite nella Community di Viva Engage.

Per semplicità, sarà descritto prima il processo front-end, ovvero l'interfaccia utente, per poi concludere con il processo back-end, che riguarda, invece, l'infrastruttura lato server.

Processo front-end

Questo manuale descrive il flusso che parte dal momento in cui l'utente compila il form sul sito di Officina, per richiedere l'accesso alla Community, fino al momento in cui entra effettivamente nella Community di Viva Engage come utente Guest.

Di seguito sono rappresentati gli step che effettua l'utente:

1. L'utente atterra sul sito di Officina, clicca sulla CTA **"Community"** presente nel menù, **compila il form** inserendo i dati personali (nome, cognome, email, codice fiscale), accetta le **dichiarazioni policy privacy** e clicca su **"Avanti"** (Immagine 1):

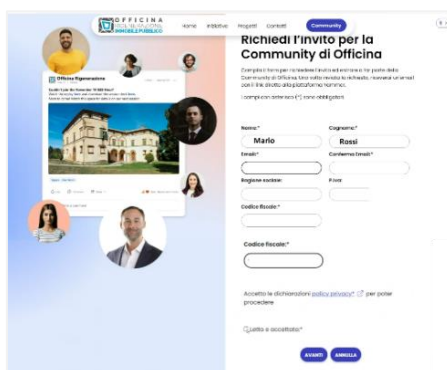


Immagine 1: Compilazione form sul sito di Officina

2. L'utente legge il **riepilogo dei dati**, poi completa l'autenticazione con il **metodo captcha** e clicca su **"Invia"** (Immagine 2):

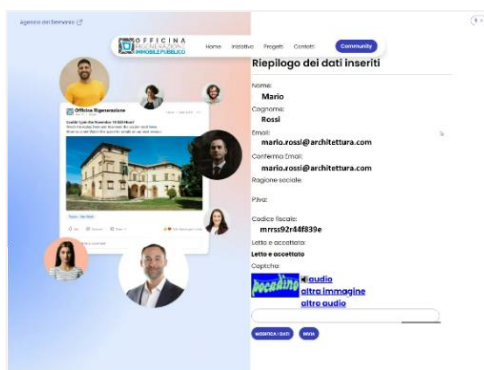


Immagine 2: Metodo captcha

3. Appare una **schermata di conferma** (Immagine 3):

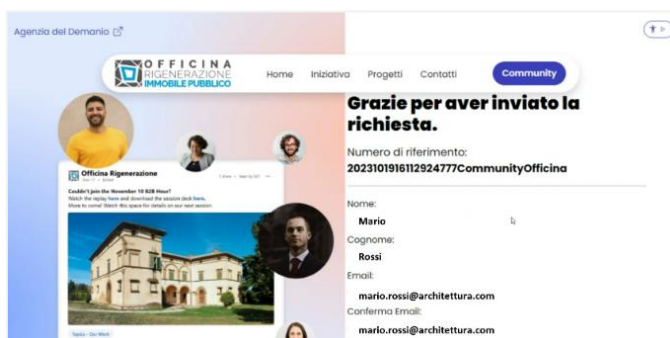


Immagine 3: Schermata di conferma

4. L'utente riceve un'email di conferma e clicca sulla CTA "QUI" (Immagine 4):



Immagine 4: Prima email che arriva all'utente

5. In caso di esito positivo, l'utente visualizza una schermata che lo avverte dell'esito positivo dell'operazione (Immagine 5):



Immagine 5: Schermata sito - Richiesta di accesso andata a buon fine

6. L'utente riceve una seconda email in cui gli viene comunicato che la sua richiesta è stata registrata (Immagine 6):

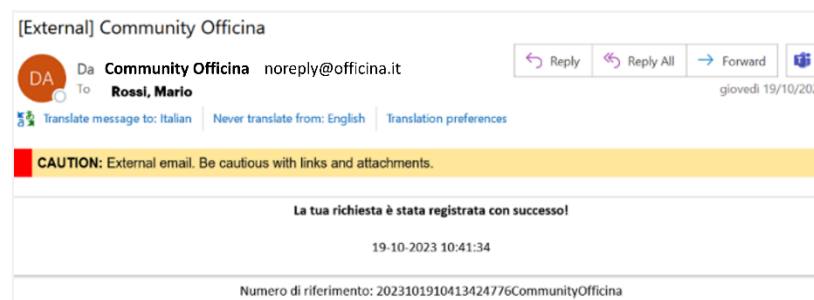


Immagine 6: Seconda email che arriva all'utente

N.B: Contemporaneamente, **al team di Officina arriva un'email di riepilogo** dei dati dell'utente che si è registrato sul form (Immagine 7):



Immagine 7: Email che arriva al team di Officina

7. L'utente riceve una **terza email** (dove trova le sue credenziali per effettuare il primo accesso e un manuale che può consultare per essere guidato nei passaggi) e clicca su **"Accetta invito"** (Immagine 8):



Immagine 8: Terza email che arriva all'utente

8. Al click su **"Accetta invito"**, l'utente viene re-indirizzato su una schermata per fare i controlli necessari per completare la richiesta di accesso. Nello specifico, **inserisce la password temporanea** presente nel contenuto dell'email (vedi immagine 8), poi clicca su **"Accedi"** (Immagine 9):



Immagine 9: Password temporanea

9. L'utente accetta le autorizzazioni cliccando su **"Accetto"** (Immagine 10):



Immagine 10: Autorizzazioni

10. L'utente clicca su "Avanti" (Immagine 11):

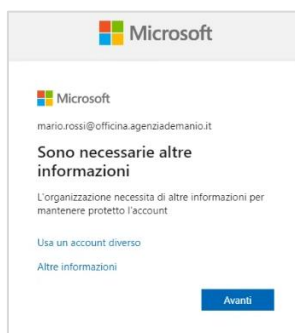


Immagine 11: Verifica dell'account

11. L'utente **configura l'autenticazione multifattoriale** per proteggere l'account. In particolare, può scegliere tra tre opzioni (Immagine 12):

- **Opzione 1** → prevede l'utilizzo dell'app Microsoft "Microsoft Authenticator";
- **Opzione 2** → prevede l'utilizzo di un'app di autenticazione diversa rispetto a quella di Microsoft (es: Google);
- **Opzione 3** → prevede l'inserimento del numero di telefono.

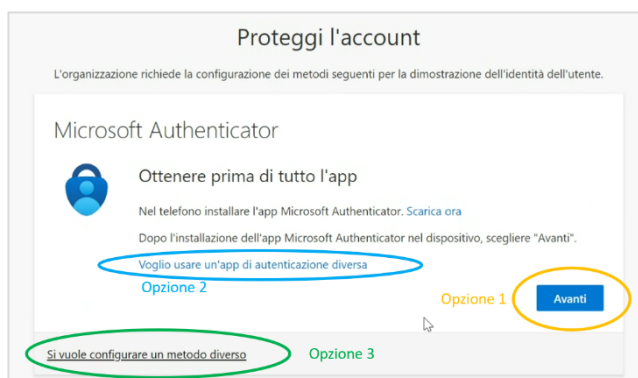


Immagine 12: Configurazione multifattoriale

N.B: Il metodo di autenticazione suggerito è quello che prevede l'utilizzo di "Microsoft Authenticator". Tuttavia, se l'utente è in possesso di un'app diversa, può scegliere di utilizzarla cliccando su "[Voglio usare un'app di autenticazione diversa](#)" e selezionando quella in uso. Di seguito, sono descritti i passaggi da seguire per l'opzione 1 e l'opzione 3.

Passaggi opzione 1 – Microsoft Authenticator

- L'utente che sceglie di utilizzare l'app di Microsoft clicca su "Avanti" (immagine 13):

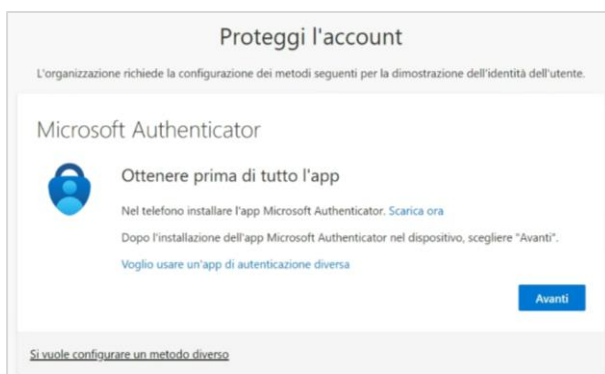


Immagine 13: Configurazione multifattoriale – Microsoft Authenticator

- L'utente clicca su **"Avanti"** (Immagine 14):



Immagine 14: Configurazione multifattoriale – Microsoft Authenticator

- Dopo aver scaricato l'app "Microsoft Authenticator" sul cellulare, l'utente la apre e clicca in alto a destra sul segno **"+"** per aggiungere un altro account (Immagine 15):

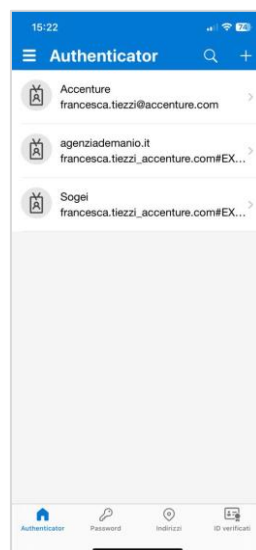


Immagine 15: Configurazione multifattoriale – Microsoft Authenticator

- L'utente clicca su **"Account aziendale o dell'istituto di istruzione"** (Immagine 16):

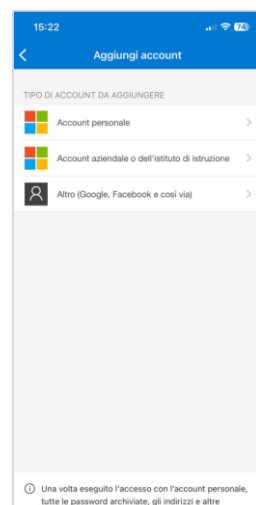


Immagine 16: Configurazione multifattoriale – Microsoft Authenticator

- L'utente clicca su **"Scansione codice QR"** (Immagine 17):

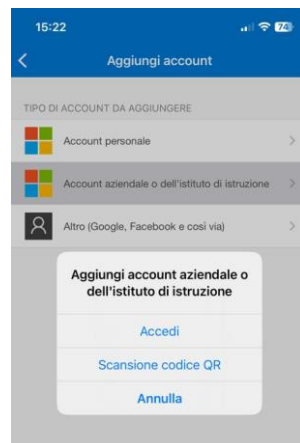


Immagine 17: Configurazione multifattoriale – Microsoft Authenticator

- L'utente **scansiona il codice QR** con il suo cellulare (Immagine 18):



Immagine 18: Configurazione multifattoriale – Microsoft Authenticator

- Sull'app, l'utente vedrà l'account con il quale si è registrato (Immagine 19):

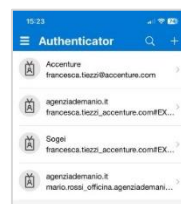


Immagine 19: Configurazione multifattoriale – Microsoft Authenticator

- L'utente **scansiona il codice QR** con il suo telefono, poi fa click su **"Avanti"** (Immagine 20):

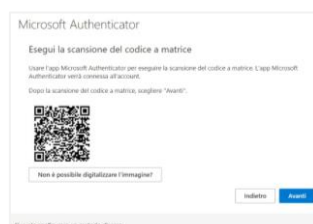


Immagine 20: Configurazione multifattoriale – Microsoft Authenticator

- Sull'app, **inserisce il numero** che gli appare sullo schermo (Immagine 21):

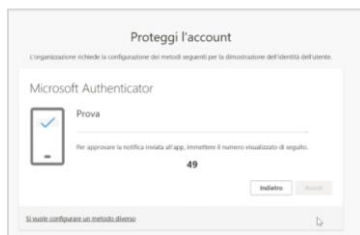


Immagine 21: Configurazione multifattoriale – Microsoft Authenticator

- L'utente clicca su **"Avanti"** (Immagine 22):

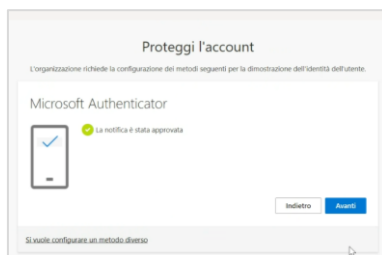


Immagine 22: Configurazione multifattoriale – Microsoft Authenticator

- L'utente clicca su **"Fine"** (Immagine 23):

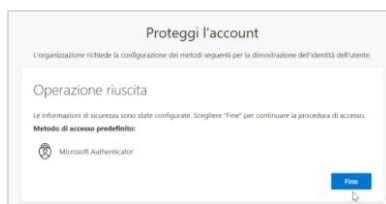


Immagine 23: Configurazione multifattoriale – Microsoft Authenticator

Passaggi opzione 3 – Telefono:

- L'utente che intende configurare l'MFA utilizzando il proprio numero di cellulare, clicca su **"Si vuole configurare un metodo diverso"** che trova in basso a sinistra (Immagine 24):



Immagine 24: Configurazione multifattoriale – Telefono

- Seleziona l'opzione **"Telefono"** dal menù a tendina (Immagine 25):



Immagine 25: Configurazione multifattoriale – Telefono

- Clicca su **"Conferma"** (Immagine 26):

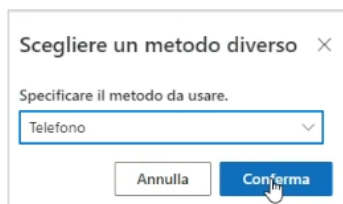


Immagine 26: Configurazione multifattoriale - Telefono

- L'utente **inserisce il numero di telefono** per la verifica dell'identità, poi clicca su **"Avanti"** (Immagine 27):

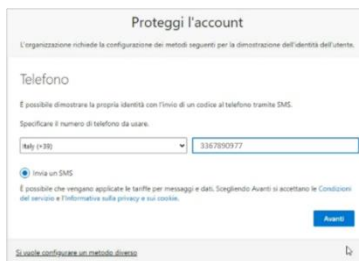


Immagine 27: Configurazione multifattoriale - Telefono

- L'utente **inserisce il codice a 6 cifre** che arriva via SMS, poi clicca su **"Avanti"** (Immagine 28):



Immagine 28: Configurazione multifattoriale - Telefono

- Una volta ricevuta la conferma dell'avvenuta verifica tramite SMS, l'utente clicca su **"Avanti"** (Immagine 29):



Immagine 29: Configurazione multifattoriale - Telefono

- L'utente clicca su **"Fine"** per terminare il processo di configurazione multifattoriale (Immagine 30):



Immagine 30: Configurazione multifattoriale - Telefono

N.B: L'utente ha appena completato tutti gli step dell'autenticazione multifattoriale. Mancano pochi passaggi e potrà accedere alla Community di Officina.

12. L'utente **sceglie una nuova password** e la inserisce nel box, poi clicca su **"Accedi"** (Immagine 31):

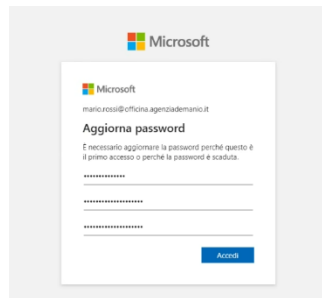


Immagine 31: Aggiornamento password

N.B: La nuova password deve essere formata da 14 caratteri, di cui almeno una maiuscola e un carattere speciale (es: punto esclamativo).

13. Al click su **"Accedi"**, l'utente **verifica la sua identità**. In questo caso, a seconda del metodo di autenticazione multifattoriale scelto al passaggio 11, vedrà comparire una schermata. Nello specifico:

- **Se ha scelto Microsoft Authenticator:**

- Apre l'app e **inserisce il numero** che gli appare sullo schermo (Immagine 32):



Immagine 32: Verifica identità – Microsoft Authenticator

- **Se ha scelto il numero di cellulare:**

- Clicca su **"Invia un SMS al numero"** (Immagine 33):

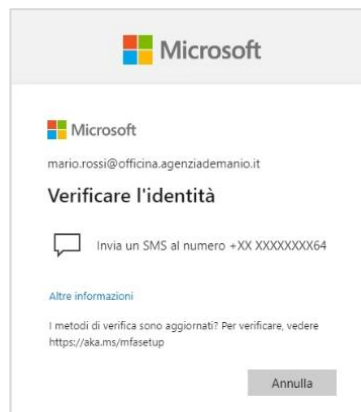


Immagine 33: Verifica identità - Telefono

- **Inserisce** nel box **il codice arrivato tramite SMS**, poi clicca su **"Verifica"** (Immagine 34):

The image shows a Microsoft login verification screen. At the top is the Microsoft logo. Below it, the email address 'mario.rossi@officina.agenziaedemario.it' is displayed. The heading 'Immettere il codice' (Enter the code) is followed by a checkbox and text: 'È stato inviato un SMS al telefono con numero +XX XXXXXXXX64. Immettere il codice per accedere.' (An SMS was sent to the phone with number +XX XXXXXXXX64. Enter the code to access). A text input field contains the code '460584'. Below the field is a link 'Altre informazioni' (More information). At the bottom are two buttons: 'Annulla' (Cancel) and 'Verifica' (Verify), with a mouse cursor clicking on 'Verifica'.

Immagine 34: Inserimento secondo codice di verifica

14. L'utente viene reindirizzato su Viva Engage dove visualizza un **post di benvenuto**, quindi clicca sulla CTA **"Clicca qui"** per entrare nella Community di Officina come utente Guest (Immagine 35):



Immagine 35: Community di Officina

N.B: Dopo essersi registrato, l'utente potrà accedere alla Community di Officina anche cliccando sul link **"Vai ad Officina"** presente nell'email (vedi immagine 8):

- Al click su **"Vai ad Officina"**, l'utente inserisce l'indirizzo email con il quale si è registrato, poi clicca su **"Avanti"** (Immagine 36):

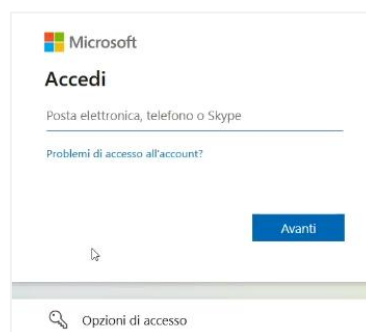
The image shows a Microsoft login screen with the heading 'Accedi' (Sign in). Below the heading is a text input field with the placeholder 'Posta elettronica, telefono o Skype' (Email, phone or Skype). Under the field is a link 'Problemi di accesso all'account?' (Account access problems?). At the bottom right is a blue button labeled 'Avanti' (Next). At the bottom left, there is a magnifying glass icon and the text 'Opzioni di accesso' (Access options).

Immagine 36: Accesso alla Community

- **Inserisce la password** (Immagine 37):

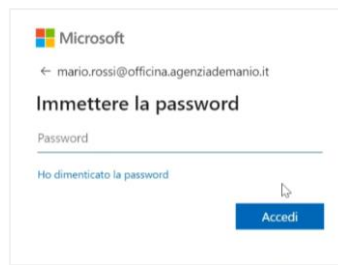


Immagine 37: Inserimento password

- **Approva** la richiesta d'accesso con Microsoft Authenticator (Immagine 38):



Immagine 38: Approvazione richiesta di accesso

- Clicca su "Sì" (Immagine 39):

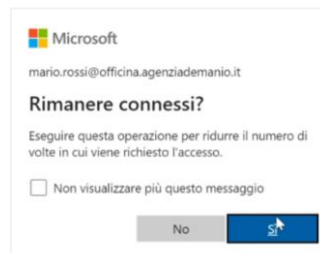


Immagine 39: Accesso alla Community

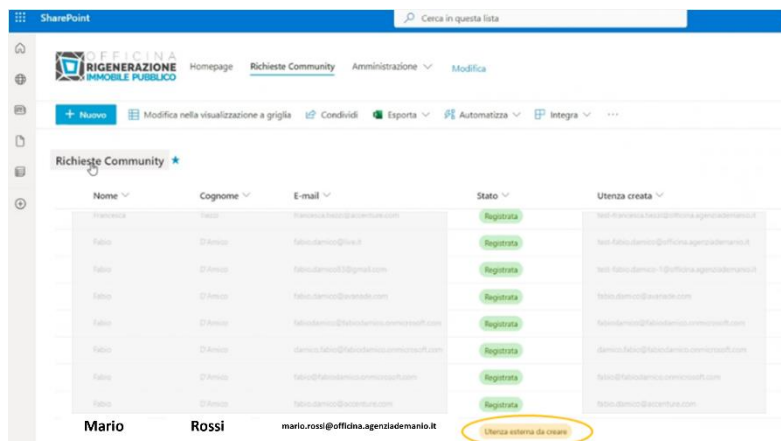
- **Accede** alla Community.

Processo back-end

Di seguito sono descritti gli step che avvengono lato back-end.

Dopo che l'utente clicca sulla CTA **"QUI"** (vedi immagine 4), a back-end viene inviata un'email nella casella di posta elettronica condivisa che scatena **tre flussi**:

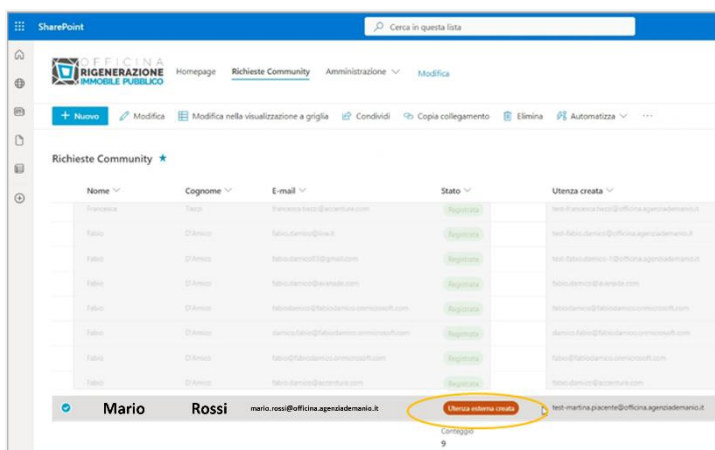
1. Il primo flusso prevede la registrazione sulla lista Sharepoint dell'utente con lo stato **"Utenza esterna da creare"** (Immagine 40):



Nome	Cognome	E-mail	Stato	Utenza creata
Francesca	Rossi	francesca.rossi@agenziaademanio.it	Registrata	test-francesca.rossi@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico@iva.it	Registrata	test-fabio.damico@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico2@gmail.com	Registrata	test-fabio.damico-1@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico@avantea.com	Registrata	fabio.damico@avantea.com
Fabio	D'Amico	fabio.damico@fabiodamico.com	Registrata	fabio.damico@fabiodamico.com
Fabio	D'Amico	damico.fabio@fabiodamico.com	Registrata	damico.fabio@fabiodamico.com
Fabio	D'Amico	fabio@fabiodamico.com	Registrata	fabio@fabiodamico.com
Fabio	D'Amico	fabio.damico@agenziaademanio.it	Registrata	test-fabio.damico@officina.agenziaademanio.it
Mario	Rossi	mario.rossi@officina.agenziaademanio.it	Utenza esterna da creare	

Immagine 40: Lista Sharepoint - Utenza esterna da creare

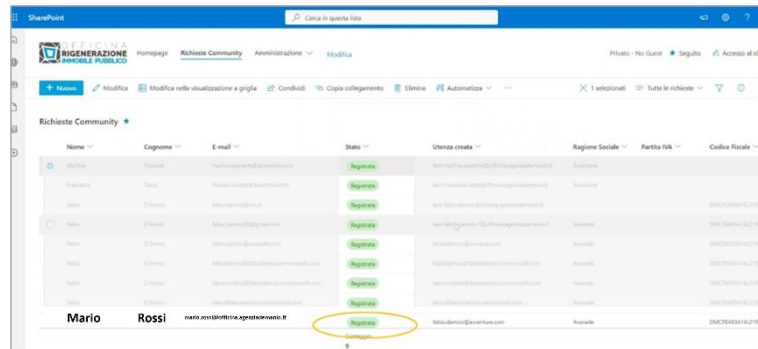
2. Il secondo flusso prevede la creazione dell'utente sull'Active Directory nel secondo tenant (officina.agenziaademanio.it). In particolare, l'automatismo prende tutti gli elementi con lo stato **"Utenza esterna da creare"** e crea tali utenze sul secondo tenant, le quali avranno la dicitura **"Member"**. A questo punto l'utente compare nella lista Sharepoint con la sua email (nome.cognome@officina.agenziaademanio.it) e lo stato passa da **"Utenza esterna da creare"** a **"Utenza esterna creata"** (Immagine 41):



Nome	Cognome	E-mail	Stato	Utenza creata
Francesca	Rossi	francesca.rossi@agenziaademanio.it	Registrata	test-francesca.rossi@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico@iva.it	Registrata	test-fabio.damico@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico2@gmail.com	Registrata	test-fabio.damico-1@officina.agenziaademanio.it
Fabio	D'Amico	fabio.damico@avantea.com	Registrata	fabio.damico@avantea.com
Fabio	D'Amico	fabio.damico@fabiodamico.com	Registrata	fabio.damico@fabiodamico.com
Fabio	D'Amico	damico.fabio@fabiodamico.com	Registrata	damico.fabio@fabiodamico.com
Fabio	D'Amico	fabio@fabiodamico.com	Registrata	fabio@fabiodamico.com
Fabio	D'Amico	fabio.damico@agenziaademanio.it	Registrata	test-fabio.damico@officina.agenziaademanio.it
Mario	Rossi	mario.rossi@officina.agenziaademanio.it	Utenza esterna creata	test-mario.rossi@officina.agenziaademanio.it

Immagine 41: Lista Sharepoint - Utenza esterna creata

3. Il terzo flusso prevede l'invito dell'utenza creata come Guest all'interno della Community di Officina: a questo punto, parte una **fase di controllo** per verificare che quella specifica utenza non sia già stata registrata come Guest sul primo tenant. Qualora l'esito del controllo sia positivo parte una comunicazione verso l'utente che vedrà arrivare nella sua casella di posta, all'indirizzo indicato al momento della registrazione, un'email con l'invito ad accedere alla Community (vedi immagine 8). Una volta che l'utente riceve l'email, l'utenza assume lo stato **"Registrata"** (Immagine 42):



Nome	Cognome	E-mail	Stato	Utenza creata	Regione Sociale	Partita IVA	Codice Fiscale
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000
Mario	Rossi	mario.rossi@officina.agricoltura.gov.it	Registrata	Non esiste una utenza di Office 365 associata a questo ID.	Emilia-Romagna		04070000990000000

Immagine 42: Lista Sharepoint - Utenza esterna "Registrata"

N.B: Fin quando l'utente non accetta l'invito come Guest all'interno della Community, nella sua vista di dettaglio sul primo tenant lo stato dell'account ha la dicitura "Abilitata" ma lo stato invito rimane in "Pending acceptance" (Immagine 43) fino al momento in cui l'utente non effettua il primo accesso come Guest nella Community a cui è stato invitato; soltanto dopo questo passaggio lo stato passerà in "Accepted".

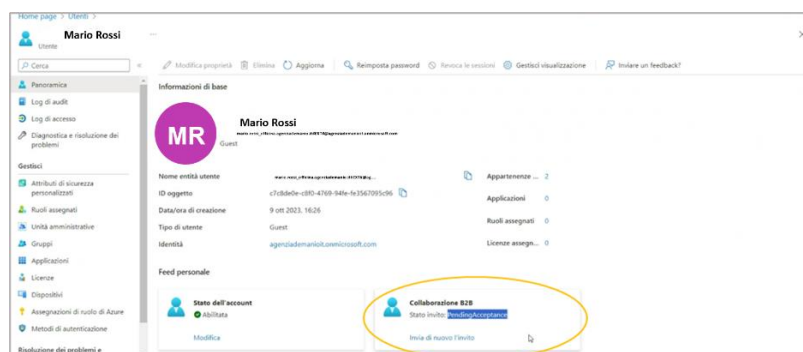


Immagine 43: Stato invito "Pending acceptance"

N.B: Oltre agli status elencati precedentemente, c'è anche lo status **"Duplicata"** che si attiva quando un utente già registrato prova a registrarsi nuovamente; in questo caso, la seconda registrazione non sarà gestita in quanto l'utenza già esiste.

Per ulteriori approfondimenti, è possibile consultare i seguenti link:

- [Metodo di autenticazione di Microsoft Authenticator | Microsoft Learn](#);
- [Creare linee guida per l'utilizzo del sito - SharePoint in Microsoft 365 | Microsoft Learn](#);
- [Introduzione a Microsoft Viva Engage | Microsoft Learn](#).