Break Glass Account: Nuove Best Practice

Come governare e gestire al meglio gli account di Emergenza in Entra ID, Azure e Microsoft 365

Marco Passanisi - Security Architect @ Protiviti

About Me

- Security Architect
- From 56k to Cloud Security
- Microsoft Certified
- Community Contributor

Marco Passanisi

Security Architect @ Protiviti

Domande per te

1. Hai definito almeno due account di emergenza nel tuo ambiente?

2. Come vengono gestiti e monitorati?

📌 Se non hai una risposta chiara, il tuo piano di emergenza potrebbe non essere efficace!

Agenda

- **Introduzione:**
  - Perché ne parliamo?
  - Quando sono necessari?
- **To-Do**
- **Conclusioni**

Perché ne parliamo?

- Presenti nelle normative, standard di sicurezza e linee guida
- Esperienza sul campo
- Introduzione MFA obbligatoria

📌 A partire dal 15/10/2024, Microsoft richiede a tutti gli utenti di utilizzare l'autenticazione a più fattori (MFA) quando accedono ad Azure Portal, Entra Admin e Intune Admin.

Quando sono necessari?

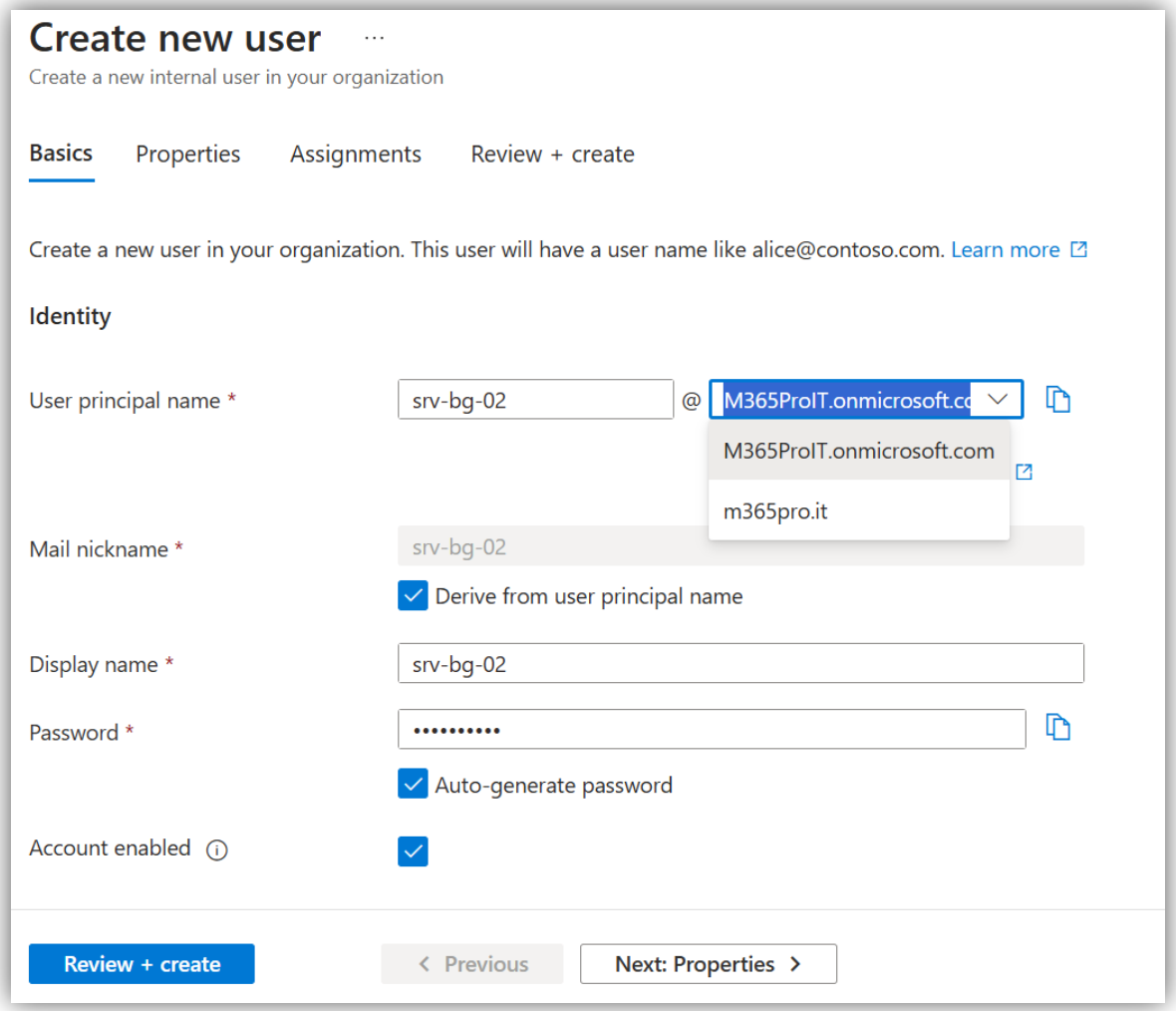
- Problemi con la Federazione
- Problemi tecnici al fornitore di connettività mobile
- L’ultimo account Global Administrator non è disponibile
- Circostanze impreviste, come un'emergenza dovuta a calamità naturali

To-Do

- Crea almeno due account di emergenza
- Configura una strong authentication
- Assegna il ruolo di Global Administrator
- Escludi gli account da tutte le Conditional Access
- Escludi gli account da Phone-based MFA
- Monitora gli accessi e i log di audit
- Valida regolarmente il funzionamento

Crea almeno due account di emergenza

- Cloud-Only
- Non associati a una persona specifica
- Utilizzano il dominio di fallback ***.onmicrosoft.com***
- Adottano nomi strategici
- Senza licenza assegnata (Unlicensed)



Password?

- Robusta e complessa
- Minimo 32 caratteri, suddivisa in almeno 2 parti
- Archiviata in modo sicuro
- Scadenza disabilitata

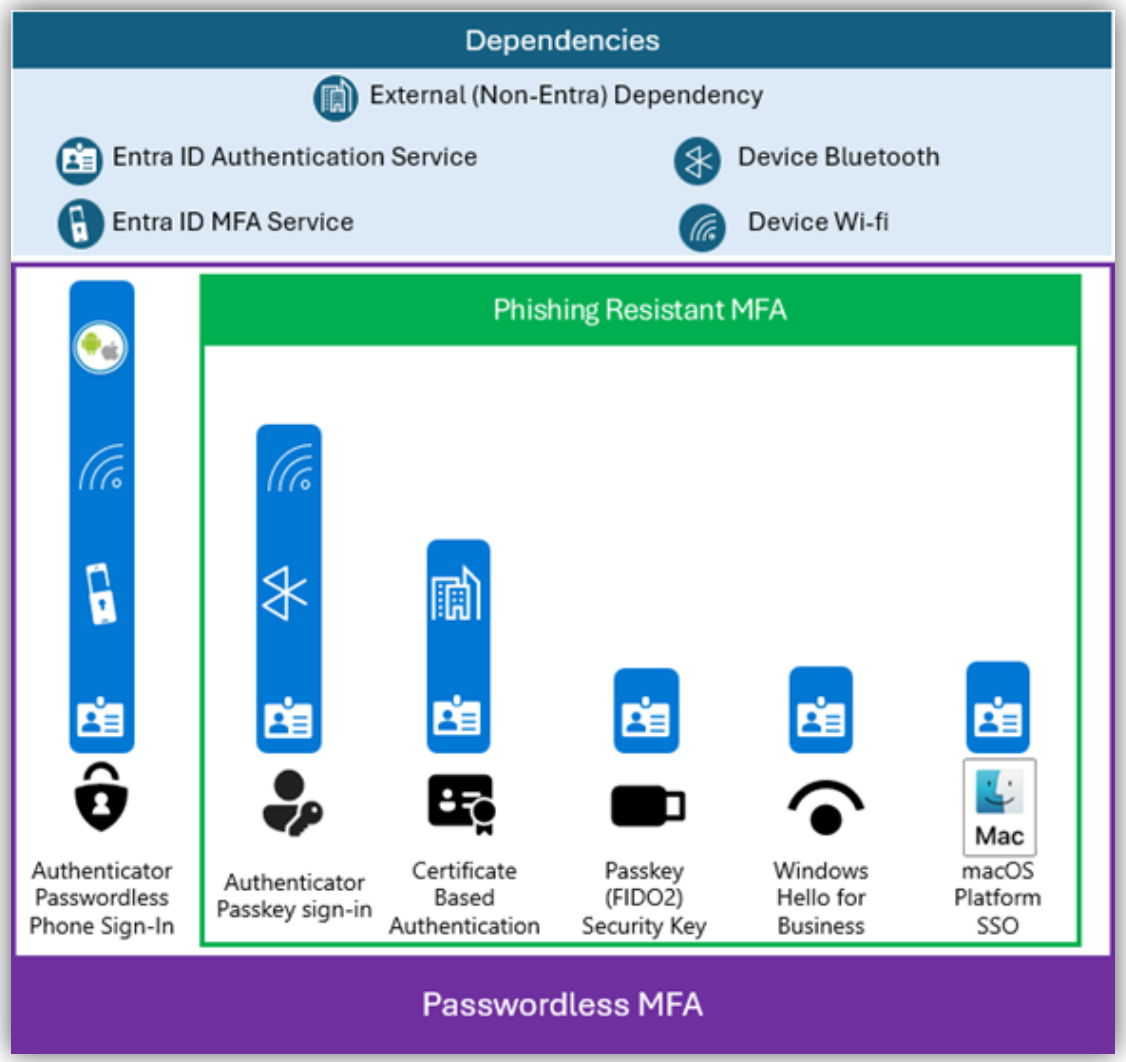
📌 Considera la possibilità di disabilitare SSRP per questi account

Configura una strong authentication

- Metodi consigliati da MS:
  - **Passkeys FIDO 2** (The Gold Standard)
  - **Certificated Based** (Richiede PKI)

- Utilizza metodi di autenticazione distinti per gli account di emergenza rispetto a quelli degli amministratori standard

- Evita requisiti esterni che potrebbero ostacolare l'accesso in situazioni critiche



📌 Microsoft consiglia di registrare due diversi metodi di autenticazione avanzata.

Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Learn & support

M365 Security

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	M365 Security	Users	37
Tenant ID	c3a779c0-2073-416e-a863-3088100dc012	Groups	39
Primary domain	M365x30202728.onmicrosoft.com	Applications	5
License	Microsoft Entra ID P2	Devices	0

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

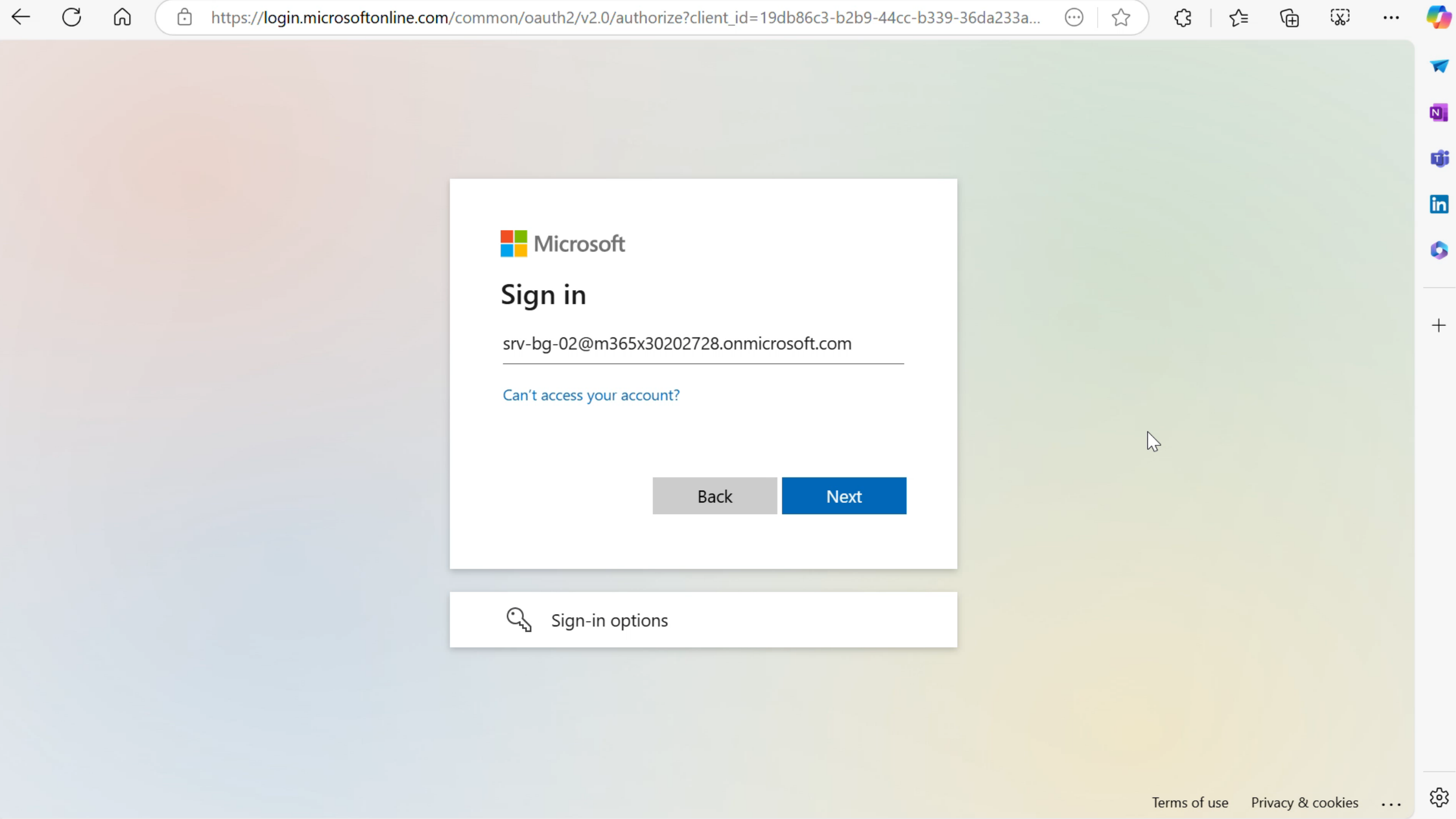
Learn more

Global Administrators

10

Microsoft recommends fewer than 5 Global Administrators.

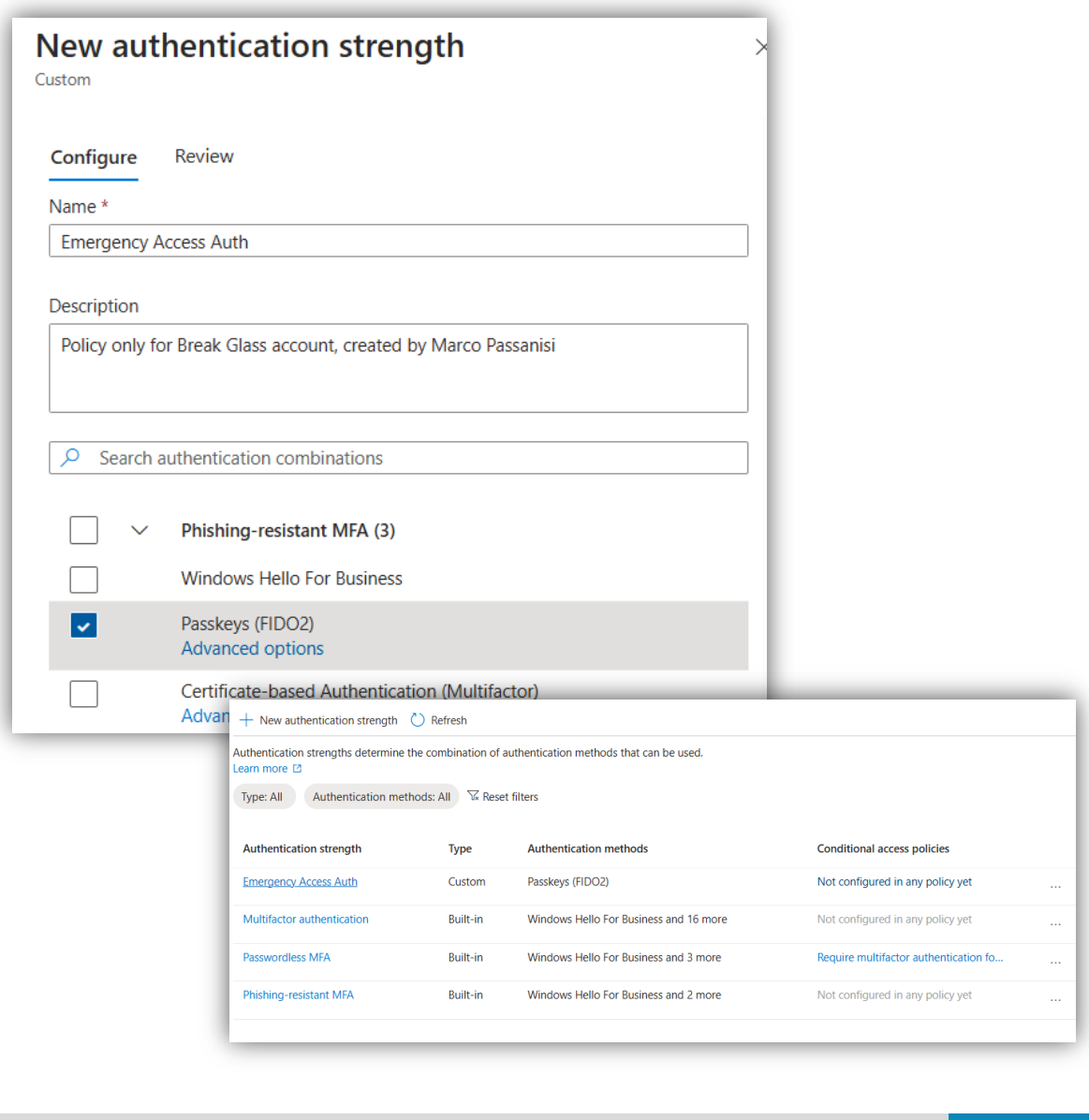
View privileged role assignments


https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=19db86c3-b2b9-44cc-b339-36da233a...
Microsoft
Sign in
srv-bg-02@m365x30202728.onmicrosoft.com
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies

Configurare una custom authentication strength?

Vantaggi:

Si riduce la possibilità che altri amministratori possano modificare la policy e compromettere il funzionamento



📌 Opzionale, da associare alla conditional access dedicata

Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Roles & admins
Billing
Settings
Protection
Learn & support

M365 Security

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	M365 Security	Users	37
Tenant ID	c3a779c0-2073-416e-a863-3088100dc012	Groups	39
Primary domain	M365x30202728.onmicrosoft.com	Applications	5
License	Microsoft Entra ID P2	Devices	0

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

Learn more

Global Administrators

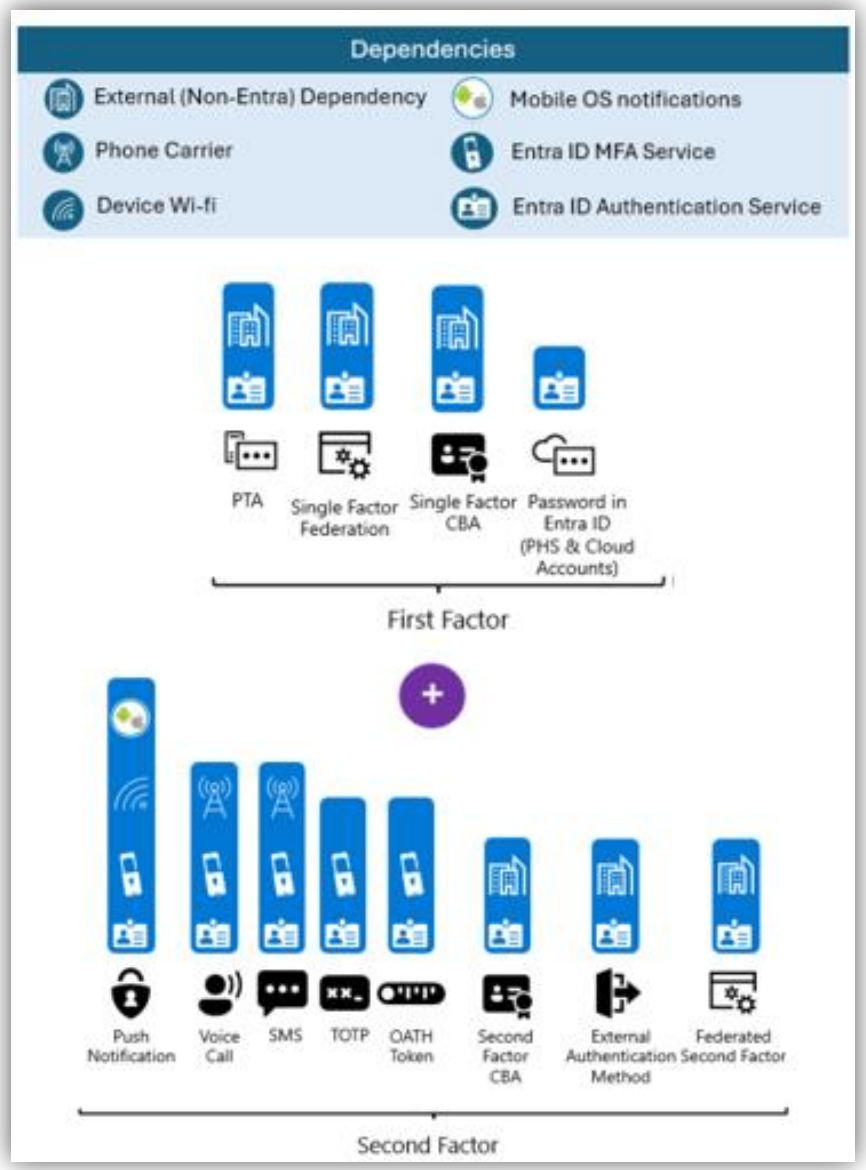
10

Microsoft recommends fewer than 5 Global Administrators.

View privileged role assignments

MFA come opzione alternativa?

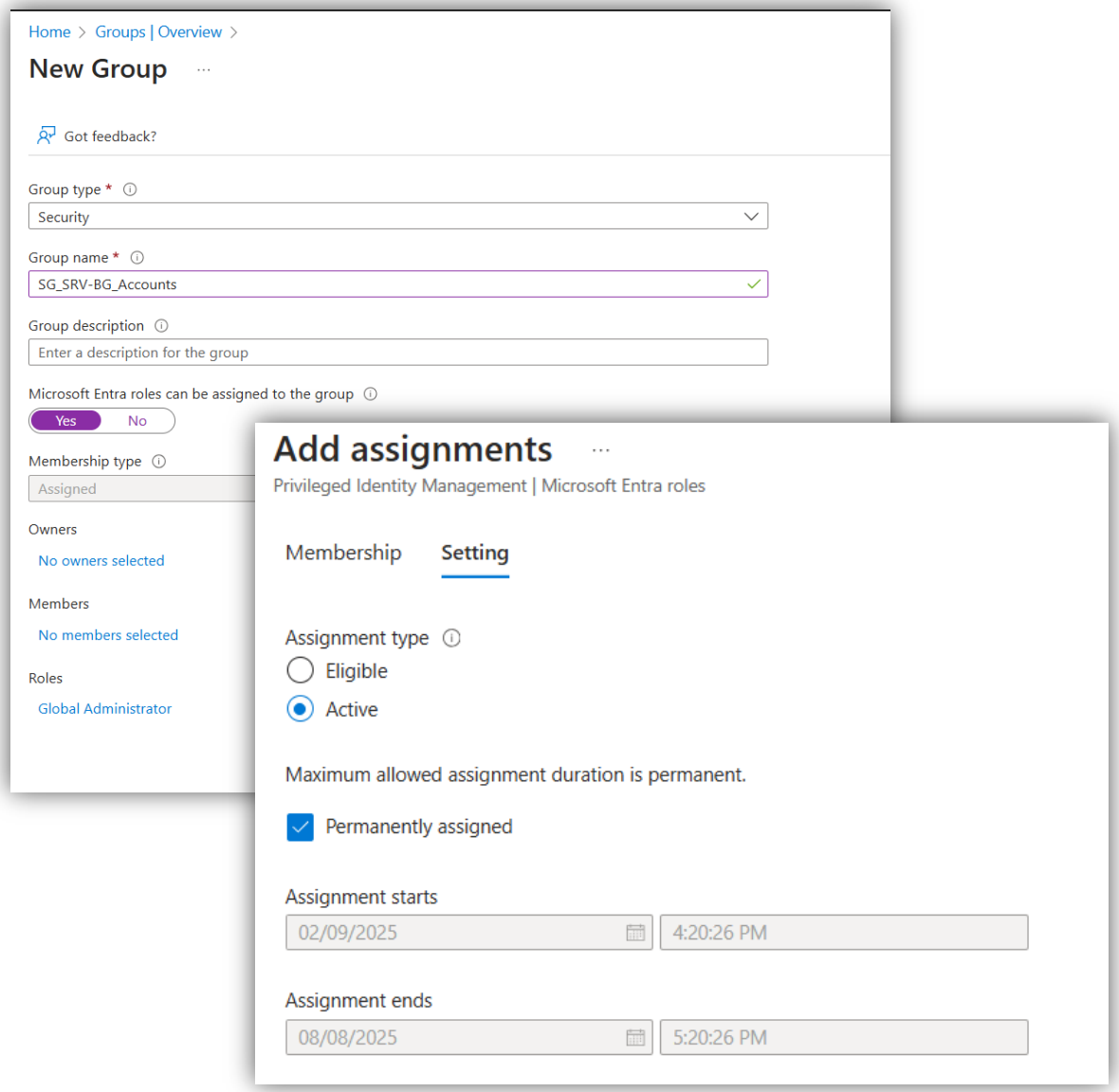
- Attenzione alla resilienza
- Bilancia le dipendenze tra i metodi di autenticazione
- L'OTP può andare bene? Si, meglio se è hardware e conservati in modo sicuro.



Assegna il ruolo di Global Administrator

- Usa **Role-Assignable Group** o un’**assegnazione diretta**

- Se utilizzi Microsoft **Entra Privileged Identity Management** (PIM), assegna il ruolo in modo permanente anziché come eligible (Richiede Microsoft Entra ID P2)



https://entra.microsoft.com/#home

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

admin@M365x3020272...
M365 SECURITY (M365X3020272...

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
    - Overview
    - All groups
    - Deleted groups
    - Group settings
  - Devices
  - Applications
- Learn & support

M365 Security

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	M365 Security	Users	37
Tenant ID	c3a779c0-2073-416e-a863-3088100dc012	Groups	38
Primary domain	M365x30202728.onmicrosoft.com	Applications	5
License	Microsoft Entra ID P2	Devices	0

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

Learn more

Global Administrators

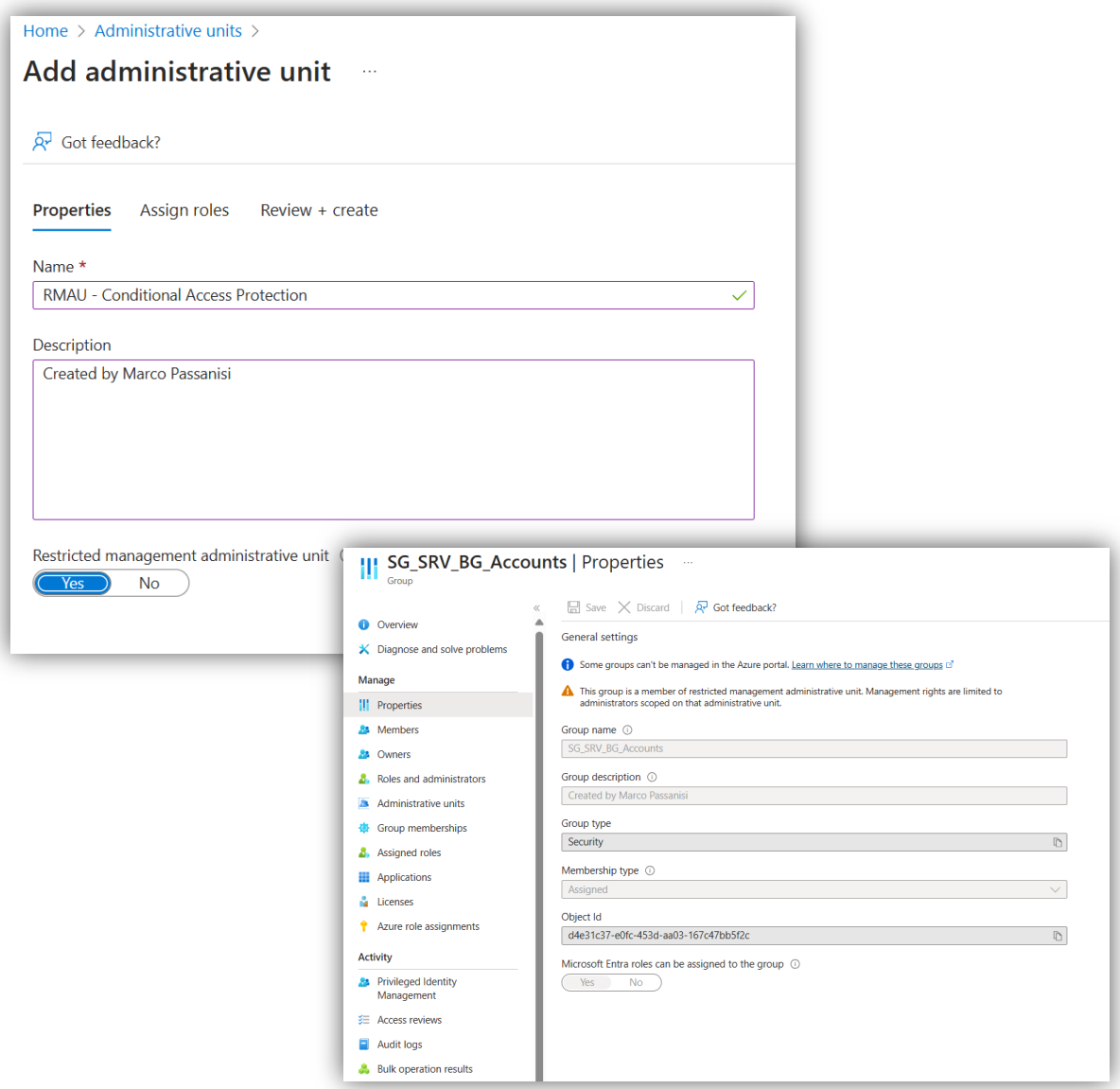
9

Microsoft recommends fewer than 5 Global Administrators.

View privileged role assignments

Gestire il ruolo e le esclusioni con i gruppi?

- role-assignable groups
- Restricted management administrative units (RMAU)



📌 RMAU ancora in preview.

https://entra.microsoft.com/#home

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

admin@M365x3020272...
M365 SECURITY (M365X3020272...

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
  - Applications
  - Roles & admins
  - Billing
  - Settings
  - Protection
- Learn & support

Roles & admins

M365 Security

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	M365 Security	Users	37
Tenant ID	c3a779c0-2073-416e-a863-3088100dc012	Groups	39
Primary domain	M365x30202728.onmicrosoft.com	Applications	5
License	Microsoft Entra ID P2	Devices	0

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

Learn more

Global Administrators

10

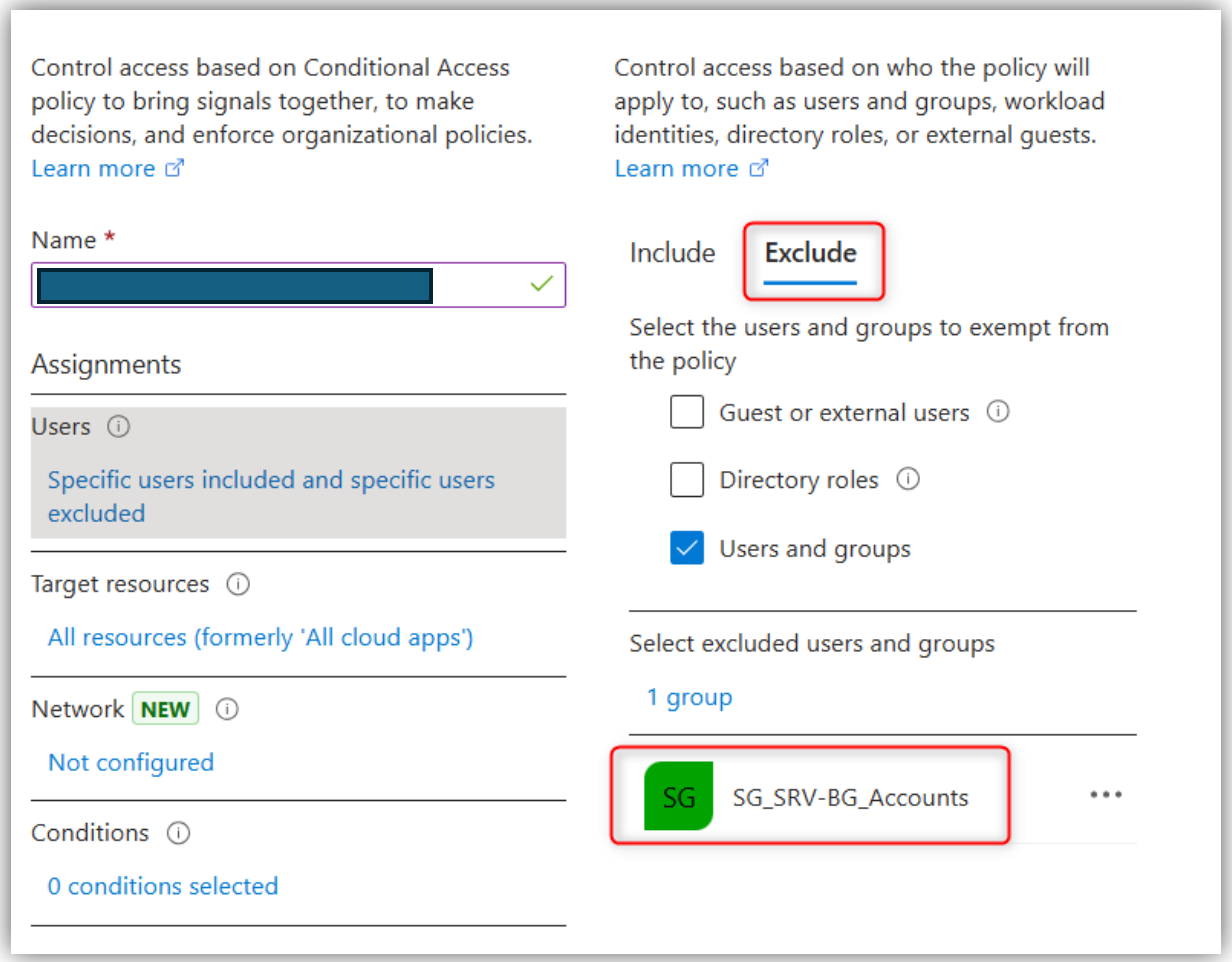
Microsoft recommends fewer than 5 Global Administrators.

View privileged role assignments

Escludi gli account da tutte le CA

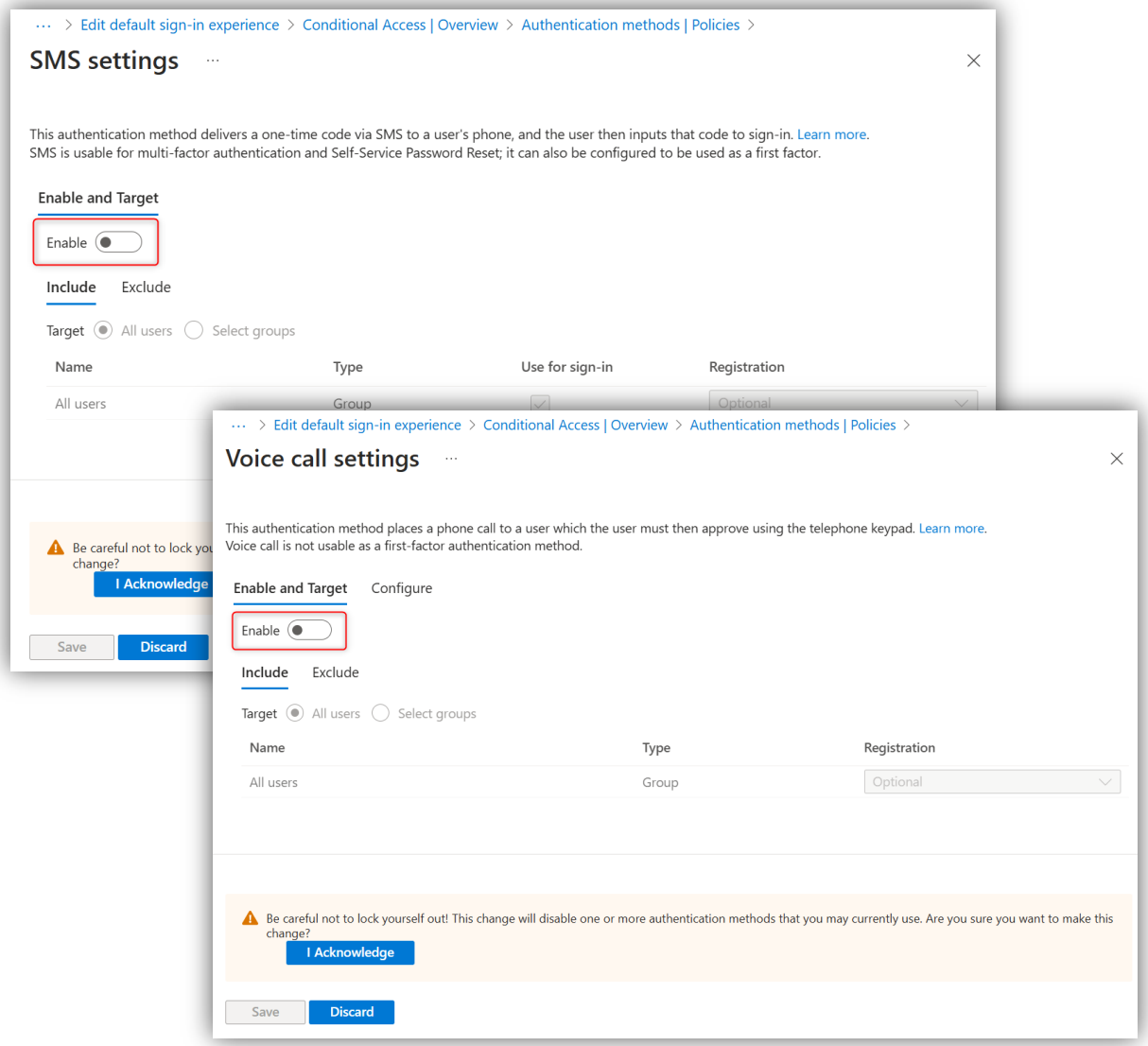
- Rivedi le policy di Accesso Condizionale e assicurati che almeno un account sia completamente escluso da tutte le policy *(Non da "quasi tutte", ma da tutte!)*

- Utilizza strumenti per le verifiche come:
  - **Maester**
  - Logic App **AutoExcludeCAP** su su GitHub



Escludi gli account da Phone-based MFA

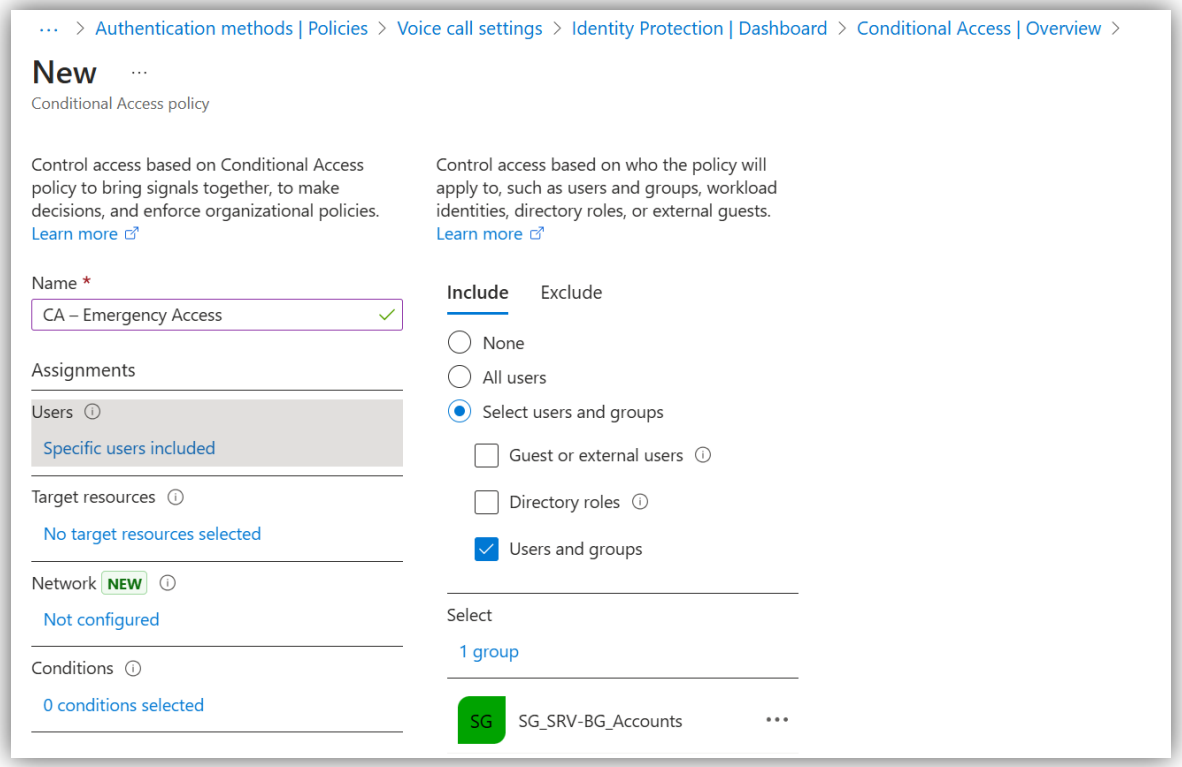
Almeno uno di questi non deve usare l’MFA basata su telefono o metodi comuni agli altri account amministrativi



Creare una Conditional Access dedicata?

- Limitare l'accesso a policy di Conditional Access per agli account di emergenza

- **Caratteristiche:**
  - ***Name:*** *"Grant – Emergency Access"*
  - ***Users include:*** *"Emergency Access" group*
  - ***Users exclude:*** *–*
  - ***Target resources:*** *All cloud apps*
  - ***Grant: Require authentication strength:*** *"Emergency Access Auth"*
  - ***Session:*** *Sign-in frequency: every time*
  - ***Session:*** *Persistent browser session: Never persistent*



📌 Opzionale, solo se è richiesto un accesso limitato.

https://entra.microsoft.com/#home

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

admin@M365x3020272...
M365 SECURITY (M365X3020272...

- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
  - Applications
  - Roles & admins
  - Billing
  - Settings
  - Protection
  - Identity Governance
  - External Identities
- Learn & support

M365 Security

Add | Manage tenants | What's new | Preview features | Got feedback?

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	M365 Security	Users	37
Tenant ID	c3a779c0-2073-416e-a863-3088100dc012	Groups	39
Primary domain	M365x30202728.onmicrosoft.com	Applications	5
License	Microsoft Entra ID P2	Devices	0

Alerts

MSOnline PowerShell Retirement

Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.

Learn more

Global Administrators

10

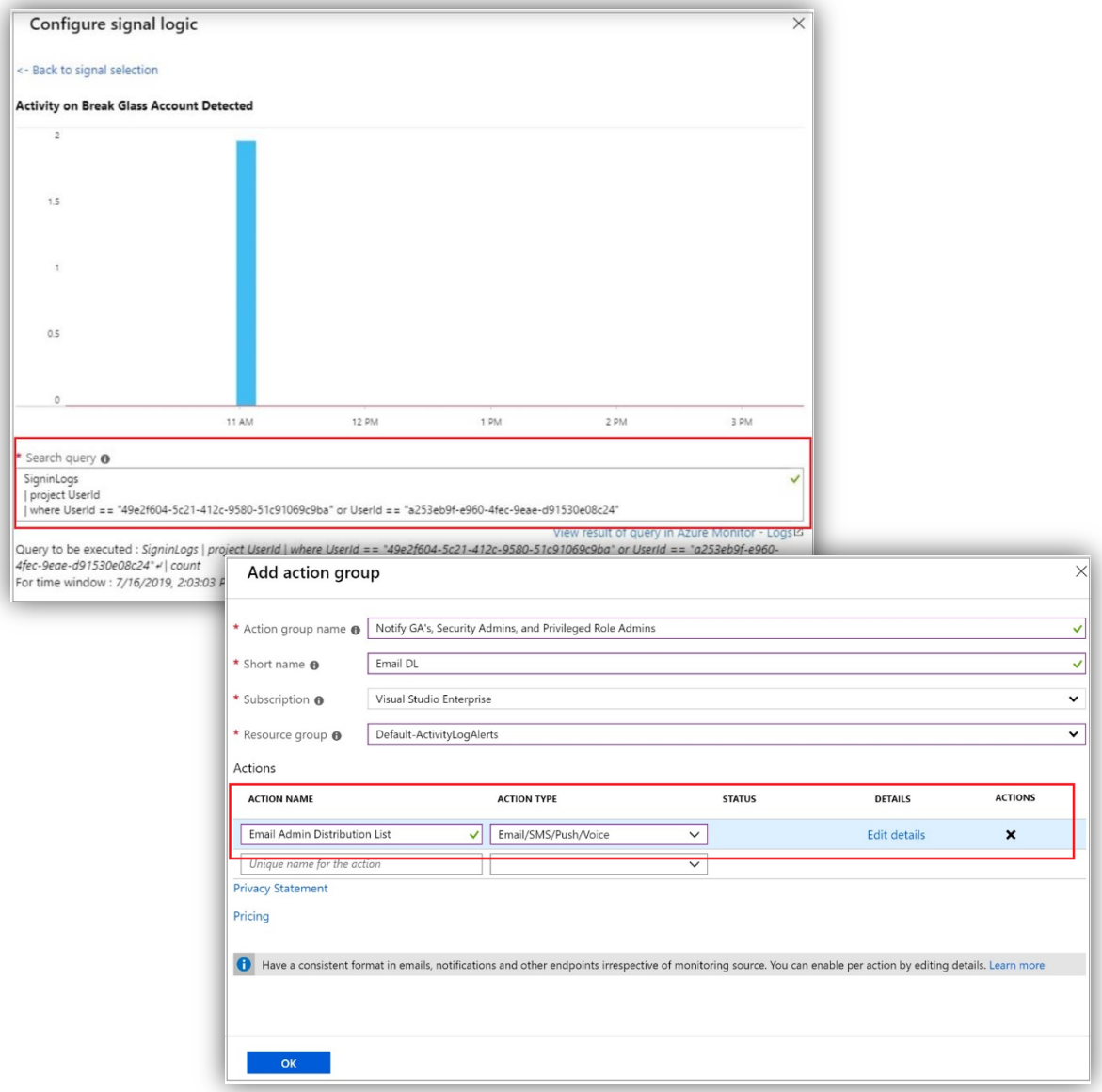
Microsoft recommends fewer than 5 Global Administrators.

View privileged role assignments

Monitora gli accessi e i log di audit

- Monitorare l'attività di accesso e i log di audit e attivare notifiche per altri amministratori.

- Strumenti consigliati:
  - **Azure Log Analytics** → Controlla i log di accesso e configura notifiche via email/SMS.
  - **Microsoft Sentinel** → Usa Analytics Rules con Watchlist per monitoraggio avanzato.



Valida regolarmente il funzionamento

Perché è importante?

- Garantisce che gli account di emergenza siano sempre funzionanti e sicuri
- Riduce il rischio di problemi durante situazioni critiche.

Come validare correttamente?

- **Simula un accesso di emergenza** → Tratta il test come un vero scenario critico.
- **Verifica le credenziali** → Assicurati che funzionino senza problemi.
- **Controlla notifiche e allarmi** → Devono attivarsi come previsto.

Quando eseguire questi controlli?

 Ogni 90 giorni

 Dopo cambiamenti nel personale IT (nuove assunzioni, dimissioni, cambi di ruolo)

 Quando cambiano le sottoscrizioni di Microsoft Entra

 Opzionale, dopo aver utilizzato la password

Conclusioni

- 🔍 **Verifica la tua configurazione attuale** e assicurati di seguire le best practice.
- 🛠️ **Simula un accesso di emergenza** per validare il funzionamento degli account.
- 📊 **Attiva il monitoraggio degli accessi** e imposta notifiche in caso di anomalie.
- 📌 **Integra la procedura di accesso d’emergenza** nel piano di disaster recovery.

📌 Non aspettare un'emergenza per scoprire che il tuo accesso di emergenza non funziona!

Risorse Utili

Manage emergency access accounts in Microsoft Entra ID

Build resilience with credential management

Use Microsoft Entra groups to manage role assignments

FIDO2 security keys eligible for attestation with Microsoft Entra ID

Planning for mandatory multifactor authentication for Azure and other admin portals

Restricted management administrative units in Microsoft Entra ID (Preview)

Grazie!

🙏 Grazie infinite per l’attenzione!

💬 Domande? Commenti?

/MarcoPassanisi

marco.passanisi@protiviti.it