

Break Glass Account: Nuove Best Practice

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



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)

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name * @ M365ProIT.onmicrosoft.com m365pro.it

Mail nickname *
 Derive from user principal name

Display name *

Password * Auto-generate password

Account enabled

Review + create < Previous Next: Properties >

>Password?

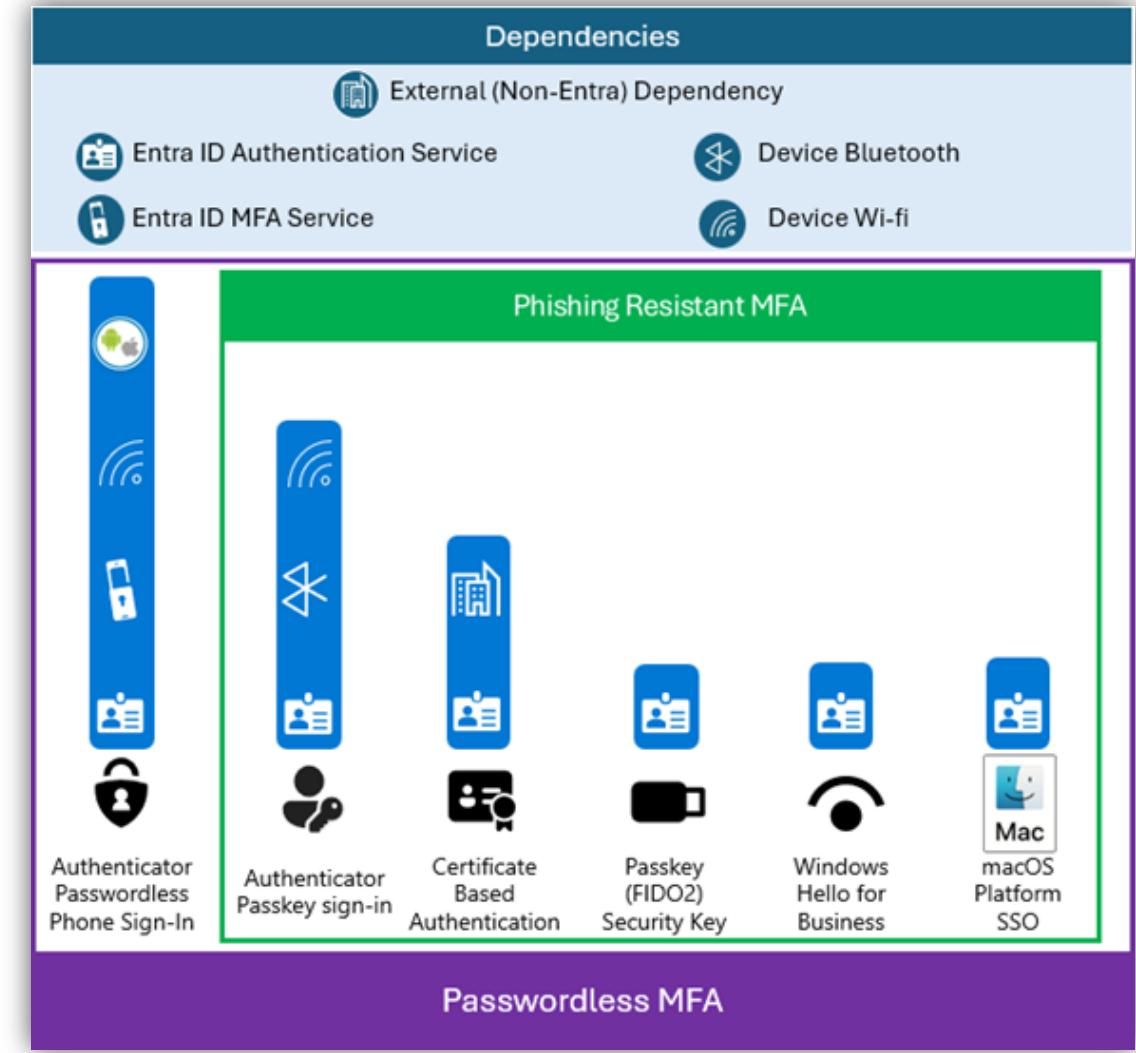
- Robusta e complessa
- Minimo 32 caratteri, suddivisa in almeno 2 parti
- Archiviata in modo sicuro
- Scadenza disabilitata



💡 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.

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

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](#)

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

 Microsoft

Sign in

srv-bg-02@m365x30202728.onmicrosoft.com

[Can't access your account?](#)

[Back](#) [Next](#)



Sign-in options

Configurare una custom authentication strength?

Vantaggi:

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

New authentication strength

Custom

Configure Review

Name *

Emergency Access Auth

Description

Policy only for Break Glass account, created by Marco Passanisi

Search authentication combinations

Phishing-resistant MFA (3)

Windows Hello For Business

Passkeys (FIDO2)
Advanced options

Certificate-based Authentication (Multifactor)

Authenticator

Authentication strengths determine the combination of authentication methods that can be used.
Learn more

Type: All Authentication methods: All Reset filters

Authentication strength	Type	Authentication methods	Conditional access policies
Emergency Access Auth	Custom	Passkeys (FIDO2)	Not configured in any policy yet
Multifactor authentication	Built-in	Windows Hello For Business and 16 more	Not configured in any policy yet
Passwordless MFA	Built-in	Windows Hello For Business and 3 more	Require multifactor authentication fo...
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more	Not configured in any policy yet

⭐ Opzionale, da associare alla conditional access dedicata

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

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot 5 ⚙️ ⓘ 🔍 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

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.

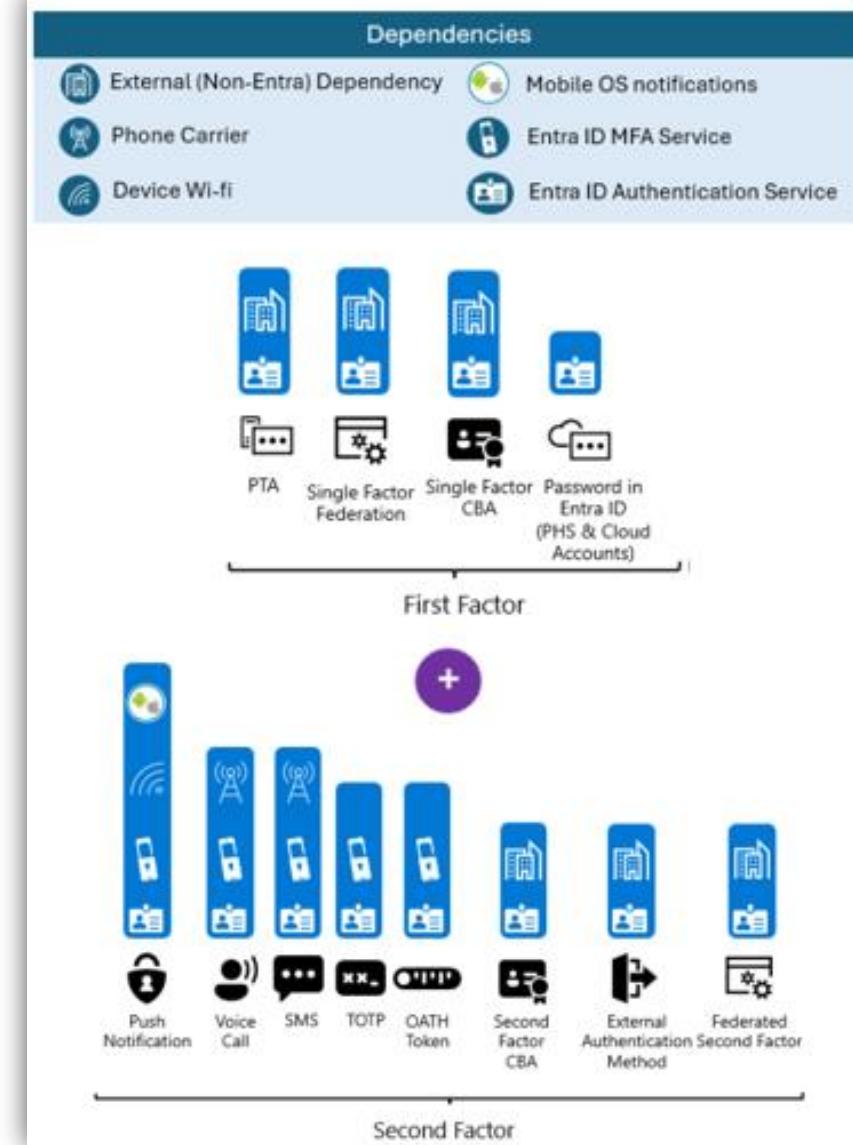
[Learn more](#)

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)

The image consists of two side-by-side screenshots from Microsoft's cloud services interface.

Top Screenshot: New Group (Microsoft Entra ID)

- Header: Home > Groups | Overview >
- Title: New Group
- Form fields:
 - Group type * (Security)
 - Group name * (SG_SRV-BG_Accounts)
 - Group description (Enter a description for the group)
 - Microsoft Entra roles can be assigned to the group (Yes)
 - Membership type (Assigned)
- Side panel:
 - Owners: No owners selected
 - Members: No members selected
 - Roles: Global Administrator

Bottom Screenshot: Add assignments (Microsoft Entra Privileged Identity Management)

- Header: Add assignments
- Section: Privileged Identity Management | Microsoft Entra roles
- Tab: Setting (selected)
- Form fields:
 - Assignment type (Eligible is off, Active is on)
 - Maximum allowed assignment duration is permanent.
 - Permanently assigned (checkbox checked)
 - Assignment starts (02/09/2025 at 4:20:26 PM)
 - Assignment ends (08/08/2025 at 5:20:26 PM)

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)

The screenshot shows two overlapping Azure portal windows. The top window is titled "Add administrative unit" and has tabs for "Properties", "Assign roles", and "Review + create". The "Properties" tab is selected, showing a "Name" field with "RMAU - Conditional Access Protection" and a green checkmark. Below it is a "Description" field containing "Created by Marco Passanisi". The bottom window is titled "SG_SRV_BG_Accounts | Properties" and shows the properties of a group named "SG_SRV_BG_Accounts". It includes sections for "General settings", "Manage", and "Activity". A modal dialog box from the bottom window is overlaid on the top one, asking "Restricted management administrative unit" with "Yes" and "No" buttons, with "Yes" being highlighted.

⭐ RMAU ancora in preview.

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

Microsoft Entra admin center

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

Copilot 1 🔍 ⚙️ 🌐 🎯 admin@M365x3020272... M365 SECURITY (M365X3020272...)

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](#)

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Roles & admins

Billing

Settings

Protection

Learn & support

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 GitHub

The screenshot shows the 'Conditional Access' blade in the Azure portal. A specific policy is being edited. The 'Exclude' tab is highlighted with a red box. The policy details are as follows:

- Name:** [REDACTED] (with a green checkmark icon)
- Assignments:** Under 'Users', it says 'Specific users included and specific users excluded'.
- Target resources:** Set to 'All resources (formerly 'All cloud apps')'
- Network:** Status is 'Not configured'.
- Conditions:** '0 conditions selected'.
- Select excluded users and groups:** A group named 'SG_SRV-BG_Accounts' is listed, also highlighted with a red box.

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

The screenshot shows two separate configuration pages for Azure Conditional Access policies:

SMS settings

This page describes the SMS authentication method, which sends a one-time code via SMS to a user's phone for sign-in. It includes sections for "Enable and Target" (with an "Enable" toggle switch highlighted with a red box), "Include" and "Exclude" targeting options (set to "All users"), and a table for defining authentication rules based on Name, Type, Use for sign-in, and Registration.

Voice call settings

This page describes the Voice call authentication method, which places a phone call to a user who must approve it using a telephone keypad. It follows a similar structure with "Enable and Target" (disabled), targeting "All users", and a warning message about potentially locking oneself out if changes are made.

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

... > Authentication methods | Policies > Voice call settings > Identity Protection | Dashboard > Conditional Access | Overview >

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
[Learn more](#)

Name *

CA – Emergency Access

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

No target resources selected

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Include Exclude

None

All users

Select users and groups

Guest or external users ⓘ

Directory roles ⓘ

Users and groups

Select

1 group

SG SG_SRV-BG_Accounts

...

 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 !\[\]\(3bdd611265e4586876f5531ec9f2440a_img.jpg\)](#)

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.

The screenshot shows two overlapping dialog boxes from the Azure portal:

- Configure signal logic**: This dialog displays a chart titled "Activity on Break Glass Account Detected" showing a single data point at 11 AM. Below the chart is a search query editor with a red border around it. The query is: `SigninLogs | project UserId | where UserId == "49e2f604-5c21-412c-9580-51c91069c9ba" or UserId == "a253eb9f-e960-4fec-9eae-d91530e08c24"`. A tooltip below the query says "View result of query in Azure Monitor - Logs".
- Add action group**: This dialog is used to define notification actions. It includes fields for Action group name (Notify GA's, Security Admins, and Privileged Role Admins), Short name (Email DL), Subscription (Visual Studio Enterprise), and Resource group (Default-ActivityLogAlerts). The "Actions" section contains a table with one row, also highlighted with a red border. The table columns are ACTION NAME, ACTION TYPE, STATUS, DETAILS, and ACTIONS. The ACTION NAME is "Email Admin Distribution List", ACTION TYPE is "Email/SMS/Push/Voice", and STATUS is "Edit details".

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

