

# 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!



- **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 \*  @

Mail nickname \*

☒ Derive from user principal name

Display name \*

Password \*

☒ Auto-generate password

Account enabled ⓘ ☒

[Review + create](#) [< Previous](#) [Next: Properties >](#)



# Password?

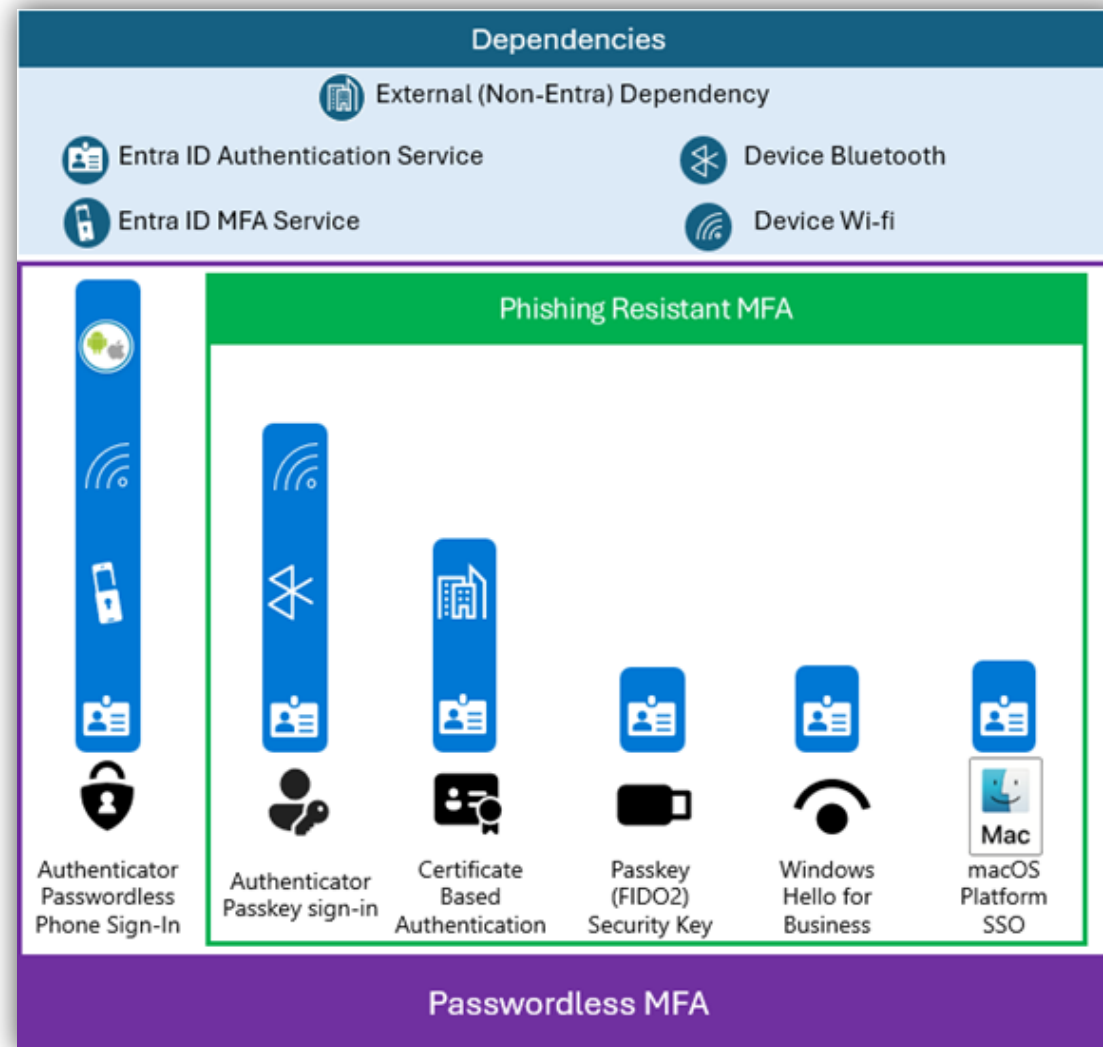
- Robusta e complessa
- Minimo 32 caratteri, suddivisa in almeno 2 parti
- Archiviata in modo sicuro
- Scadenza disabilitata





# 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





- 🔑 Identity ^
- 📘 Overview
- 👤 Users ^
- All users ☆
- Deleted users
- User settings
- 👥 Groups v
- 📱 Devices v
- 🗃️ Applications v
- 🔒 Protection ^
- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- 🧑🏫 Learn & support ^

# M365 Security ...

+ Add v ⚙️ Manage tenants 📄 What's new | 🛠️ Preview features | 🗨️ Got feedback? v

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

OverviewMonitoringPropertiesRecommendationsSetup 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](#)





## 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

 Opzionale, da associare alla conditional access dedicata


### 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)  
[Advanced options](#)

[+ New authentication strength](#) [Refresh](#)

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                                  |
|--|----------|--|--|
| <a href="#">Emergency Access Auth</a>      | Custom   | Passkeys (FIDO2)                       | Not configured in any policy yet ...                         |
| <a href="#">Multifactor authentication</a> | Built-in | Windows Hello For Business and 16 more | Not configured in any policy yet ...                         |
| <a href="#">Passwordless MFA</a>           | Built-in | Windows Hello For Business and 3 more  | <a href="#">Require multifactor authentication fo...</a> ... |
| <a href="#">Phishing-resistant MFA</a>     | Built-in | Windows Hello For Business and 2 more  | Not configured in any policy yet ...                         |



[Home](#)

## What's new


 Diagnose & solve problems

★ Favorites


 Identity

① 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

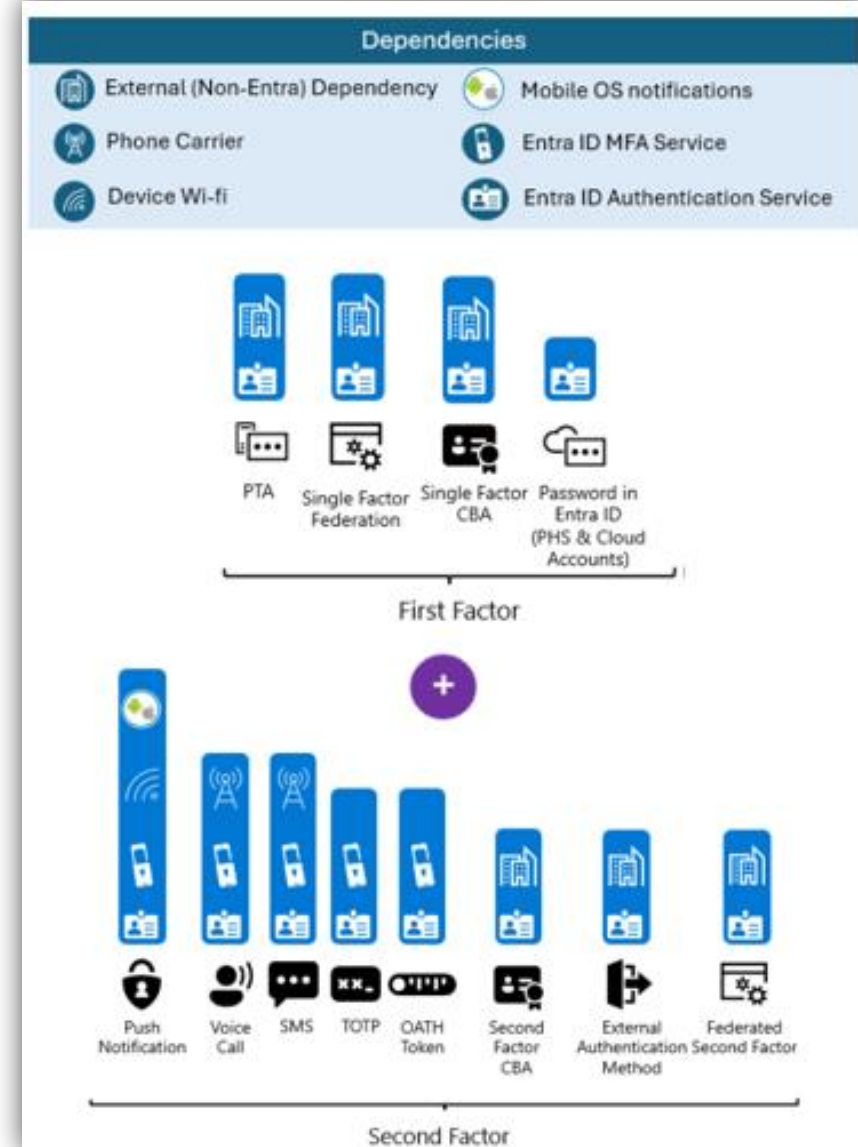
**10** Microsoft recommends fewer than 5 Global Administrators.

[View privileged role assignments](#)



# MFA come opzione alternativa?

- Attenzione alla resilienza
- Bilancia le dipendenze tra i metodi di autenticazione
- L'OTP può andare bene? Sì, 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 shows a screenshot of the Microsoft Entra Privileged Identity Management (PIM) console. The main window is titled 'New Group' and shows the following fields:

- Group type:** Security (selected)
- Group name:** SG\_SRV-BG\_Accounts (with a green checkmark)
- Group description:** Enter a description for the group
- Microsoft Entra roles can be assigned to the group:** Yes (selected)
- Membership type:** Assigned
- Owners:** No owners selected
- Members:** No members selected
- Roles:** Global Administrator

An overlay window titled 'Add assignments' is shown in the foreground, displaying the 'Setting' tab for the 'Global Administrator' role. The settings are as follows:

- Assignment type:** Active (selected)
- Maximum allowed assignment duration:** permanent
- Permanently assigned:** checked
- Assignment starts:** 02/09/2025 4:20:26 PM
- Assignment ends:** 08/08/2025 5:20:26 PM



- 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 image displays two overlapping screenshots from the Azure portal. The background screenshot is the 'Add administrative unit' page, showing the 'Properties' tab with fields for 'Name' (RMAU - Conditional Access Protection) and 'Description' (Created by Marco Passanisi). The foreground screenshot is the 'Properties' page for a group named 'SG\_SRV\_BG\_Accounts'. It shows a warning message: 'Some groups can't be managed in the Azure portal. Learn where to manage these groups'. Below this, it states: 'This group is a member of restricted management administrative unit. Management rights are limited to administrators scoped on that administrative unit.' The 'General settings' section includes fields for 'Group name', 'Group description', 'Group type' (Security), 'Membership type' (Assigned), and 'Object Id'. At the bottom, there is a toggle for 'Microsoft Entra roles can be assigned to the group'.



- 🏠 Home
- 📰 What's new
- 🔧 Diagnose & solve problems
- ★ Favorites
- 🔑 Identity

⌵
- 📄 Overview
- 👤 Users

⌵
- 👥 Groups

⌵
- 📱 Devices

⌵
- 📊 Applications

⌵
- 👤 Roles & admins

⌵

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](#)



# 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

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

Name <sup>\*</sup>

Assignments

Users ⓘ  
Specific users included and specific users excluded

Target resources ⓘ  
All resources (formerly 'All cloud apps')

Network NEW ⓘ  
Not configured

Conditions ⓘ  
0 conditions selected

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

Include **Exclude**

Select the users and groups to exempt from the policy

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select excluded users and groups

1 group

**SG** SG\_SRV-BG\_Accounts ...



# 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 image shows two overlapping screenshots of the Microsoft Entra ID Conditional Access configuration interface. The background screenshot is the 'SMS settings' page, and the foreground screenshot is the 'Voice call settings' page. Both pages have a breadcrumb trail: '... > Edit default sign-in experience > Conditional Access | Overview > Authentication methods | Policies >'. The 'SMS settings' page has a red box around the 'Enable' toggle switch, which is currently turned off. Below it, the 'Include' tab is selected, and the 'Target' is set to 'All users'. A table below shows the configuration for 'All users' with columns for Name, Type, Use for sign-in, and Registration. The 'Voice call settings' page also has a red box around its 'Enable' toggle switch, which is also turned off. It follows a similar layout with the 'Include' tab selected and 'All users' as the target. Both pages include a warning message at the bottom: 'Be careful not to lock yourself out! This change will disable one or more authentication methods that you may currently use. Are you sure you want to make this change?' with an 'I Acknowledge' button. The 'SMS settings' page also has a 'Save' and 'Discard' button at the bottom.

... > Edit default sign-in experience > Conditional Access | Overview > Authentication methods | Policies >

## SMS settings

This authentication method delivers a one-time code via SMS to a user's phone, and the user then inputs that code to sign-in. [Learn more.](#) SMS is usable for multi-factor authentication and Self-Service Password Reset; it can also be configured to be used as a first factor.

**Enable and Target**

Enable ☐

**Include** Exclude

Target ☒ All users ☐ Select groups

| Name      | Type  | Use for sign-in                     | Registration |
|-----------|-------|-------------------------------------|--------------|
| All users | Group | <input checked="" type="checkbox"/> | Optional     |

Be careful not to lock yourself out! This change will disable one or more authentication methods that you may currently use. Are you sure you want to make this change?

[I Acknowledge](#)

Save Discard

... > Edit default sign-in experience > Conditional Access | Overview > Authentication methods | Policies >

## Voice call settings

This authentication method places a phone call to a user which the user must then approve using the telephone keypad. [Learn more.](#) Voice call is not usable as a first-factor authentication method.

**Enable and Target**

Enable ☐

**Include** Exclude

Target ☒ All users ☐ Select groups

| Name      | Type  | Registration |
|-----------|-------|--------------|
| All users | Group | Optional     |

Be careful not to lock yourself out! This change will disable one or more authentication methods that you may currently use. Are you sure you want to make this change?

[I Acknowledge](#)

Save Discard



# 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.

... > 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](#)

Name \*

CA – Emergency Access ✓

Assignments

Users ⓘ

[Specific users included](#)

Target resources ⓘ

[No target resources selected](#)

Network **NEW** ⓘ

[Not configured](#)

Conditions ⓘ

[0 conditions selected](#)

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

**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](#)

⚠️

**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 image shows two overlapping screenshots from the Azure Monitor console. The top screenshot is the 'Configure signal logic' window, which displays a bar chart titled 'Activity on Break Glass Account Detected'. The chart shows a single bar at 11 AM with a value of 2. Below the chart, the search query is shown: `SignInLogs | project UserId | where UserId == "49e2f604-5c21-412c-9580-51c91069c9ba" or UserId == "a253eb9f-e960-4fec-9eae-d91530e08c24"`. The bottom screenshot is the 'Add action group' window. It shows the configuration for an action group named 'Notify GA's, Security Admins, and Privileged Role Admins'. The short name is 'Email DL', the subscription is 'Visual Studio Enterprise', and the resource group is 'Default-ActivityLogAlerts'. Under the 'Actions' section, there is a table with one row: 'Email Admin Distribution List' with an action type of 'Email/SMS/Push/Voice'. The table has columns for 'ACTION NAME', 'ACTION TYPE', 'STATUS', 'DETAILS', and 'ACTIONS'. Below the table, there is a 'Unique name for the action' field and a 'Privacy Statement' link. At the bottom, there is an 'OK' button.

**Configure signal logic**

<- Back to signal selection

Activity on Break Glass Account Detected

Search query

```
SignInLogs  
| project UserId  
| where UserId == "49e2f604-5c21-412c-9580-51c91069c9ba" or UserId == "a253eb9f-e960-4fec-9eae-d91530e08c24"
```

Query to be executed : SignInLogs | project UserId | where UserId == "49e2f604-5c21-412c-9580-51c91069c9ba" or UserId == "a253eb9f-e960-4fec-9eae-d91530e08c24" | count  
For time window : 7/16/2019, 2:03:03 PM

**Add action group**

Action group name: Notify GA's, Security Admins, and Privileged Role Admins

Short name: Email DL

Subscription: Visual Studio Enterprise

Resource group: Default-ActivityLogAlerts

Actions

| ACTION NAME                   | ACTION TYPE          | STATUS | DETAILS      | ACTIONS |
|-------------------------------|----------------------|--------|--------------|---------|
| Email Admin Distribution List | Email/SMS/Push/Voice |        | Edit details | X       |

Unique name for the action

Privacy Statement

Pricing

Have a consistent format in emails, notifications and other endpoints irrespective of monitoring source. You can enable per action by editing details. [Learn more](#)

OK



# 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](mailto:marco.passanisi@protiviti.it)

