

Why We Replace Security Defaults with Conditional Access

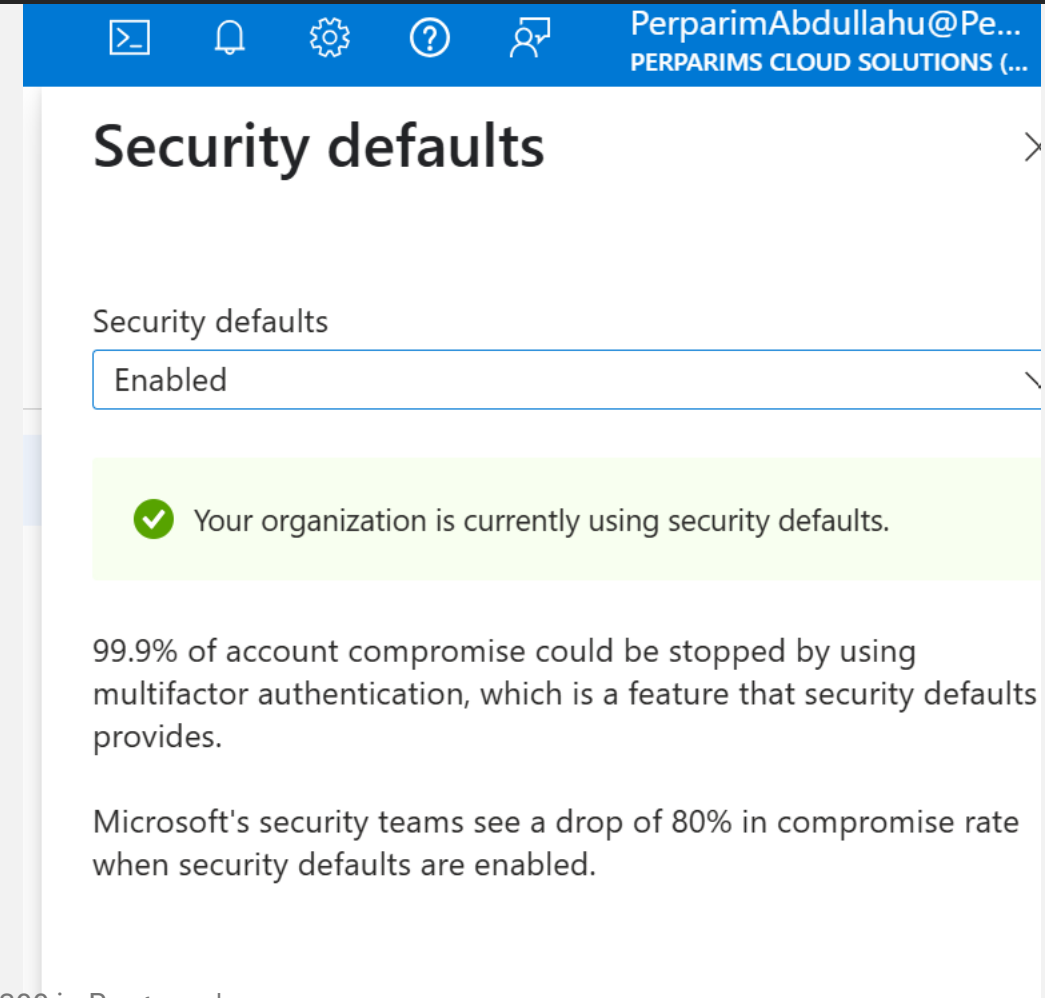


🔒 Microsoft Entra ID – SC-300 Lab Series
💻 Perparim Abdullahu | #PerparimLabs



What Are Security Defaults?

- Basic, free protection enabled by default
- Forces MFA for all users/admins
- Blocks legacy authentication
- Not customizable — all or nothing



The screenshot shows the 'Security defaults' settings page in the Azure portal. The top navigation bar is blue and contains icons for a terminal, notifications, settings, help, and a user profile. The user profile section shows 'PerparimAbdullahu@Pe...' and 'PERPARIMS CLOUD SOLUTIONS (...)'. The main heading is 'Security defaults' with a right-pointing arrow. Below the heading, there is a section titled 'Security defaults' with a dropdown menu set to 'Enabled'. A green checkmark icon is followed by the text 'Your organization is currently using security defaults.' Below this, there is a paragraph stating '99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.' and another paragraph stating 'Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.'

Limitations of Security Defaults

- Cannot target specific users, apps, or locations
- Doesn't support text, call, or app-password-based MFA
- Conflicts with Conditional Access policies

You can't build a real Zero Trust architecture with Security Defaults alone.

Microsoft Azure

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

Home > Perparims Cloud Solutions | Security > Security | Conditional Access >

Conditional Access | Overview

Microsoft Entra ID

+ Create new policy + Create new policy from templates Refresh | Got feedback?

Overview

Policies

Insights and reporting

Getting started Overview Coverage Monitoring (Preview) Tutorials

What is Conditional Access?

Define with visuals:

- Signal-based access control (user, device, location, app, risk)
- Enforce MFA only when needed
- Block or allow access based on real-time logic

Security defaults

Security defaults

Disabled

⚠ With security defaults disabled, your organization is vulnerable to common identity-related attacks.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Reason for disabling *

This feedback will be used to improve Microsoft products and services. [View privacy statement](#)

- ☐ My organization is unable to use apps/devices
- ☐ Too many multifactor authentication sign-up requests
- ☐ Too many sign-in multifactor authentication challenges
- ☒ My organization is planning to use Conditional Access

⚠ Once you disabled security defaults, your organization will not be protected until you create Conditional Access policies to protect your identities. [Learn more](#)

☐ Other

Conditional Access policy

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

Name *

Require MFA for Admins ✓

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Network NEW

Any network or location

Conditions

4 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Report-only On Off

Create

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk

User risk level is the likelihood that the user account is compromised.

1 included

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

1 included

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms

3 included

Locations

Any network or location

Client apps

Not configured

Filter for devices

Not configured

Authentication flows

Not configured

Control user access based on their network or physical location. [Learn more](#)

Configure

Yes No

Include Exclude

- ☒ Any network or location
- ☐ All trusted networks and locations
- ☐ All Compliant Network locations
- ☐ Selected networks and locations

ⓘ To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to [enable GSA Adaptive Access Signaling](#).

ⓘ 'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure Access capability of 'All Compliant network locations'. No action required. [Learn more](#)

Grant

Control access enforcement to block or grant access. [Learn more](#)

- ☐ Block access
- ☒ Grant access

☒ Require multifactor authentication ⓘ

ⓘ Consider testing the new "Require authentication strength". [Learn more](#)

☐ Require authentication strength ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☒ Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant. [Learn more](#)

☒ Require Microsoft Entra hybrid joined device ⓘ

⚠ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. [Learn more](#)

☐ Require approved client app [See list of approved client apps](#)

Select

Grant

☐ Require authentication strength ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☒ Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant. [Learn more](#)

☒ Require Microsoft Entra hybrid joined device ⓘ

⚠ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. [Learn more](#)

☐ Require approved client app [See list of approved client apps](#)

☐ Require app protection policy [See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

- ☒ Require all the selected controls
- ☐ Require one of the selected controls

Select

Common Conditional Access Use Cases

- ✓ Require MFA for admins
- ✓ Block legacy authentication
- ✓ Only allow compliant devices
- ✓ Restrict access by location (e.g. block China)

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 *
Require MFA for Admins ✓

Assignments

Users ⓘ
Specific users included

Target resources ⓘ
No target resources selected

Network NEW ⓘ
Any network or location

Conditions ⓘ
4 conditions selected

Access controls
Grant ⓘ
3 controls selected

Session ⓘ
0 controls 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 user

ES

Emma Smith
emma.smith@PerparimSC30...

...

Enable policy
Report-only On Off

Policies in Report-only mode requiring compliant devices may prompt users on macOS, iOS, Android, and Linux to select a device certificate. [Learn more](#)

☒ Exclude device platforms macOS, iOS, Android, and Linux from this policy.

☐ Proceed with selected configuration. Users on macOS, iOS, Android, and Linux may receive prompts when the device is checked for compliance.

Create

Require MFA for Admins ...

Conditional Access policy

Delete View policy information View policy impact

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

Name *
Require MFA for Admins

Assignments

Users ⓘ
Specific users included

Target resources ⓘ
No target resources selected

Network NEW ⓘ
Any network or location

Conditions ⓘ
4 conditions selected

Access controls
Grant ⓘ
3 controls selected

Session ⓘ
0 controls selected

Enable policy
Report-only On Off

Save



Security Defaults vs Conditional Access

Feature	Security Defaults	Conditional Access
MFA enforced for users/admins	✓	✓ (customizable)
Legacy auth blocked	✓ (basic)	✓ (fully scoped)
Risk-based controls	✗	✓ (with Entra P2)
Target specific users/groups	✗	✓
Report-only testing	✗	✓
Best for	Small orgs	Enterprises / Zero Trust

Conditional Access gives us real-world flexibility, testing, and targeted protection—this is how we move from default security to true governance.

Microsoft Entra ID: Identity Governance with Conditional Access



-  Follow for more labs
-  DM for collab or questions

Lab by Perparim Abdullahu | SC-300 Candidate
Built with real policies replacing Security Defaults
#PerparimLabs | Microsoft Certified Azure Architect

- ✓ Replaced Security Defaults with scoped CA policies
- ✓ Enforced MFA for users and admins
- ✓ Blocked legacy auth with custom conditions
- ✓ All deployed in Report-only mode for safe rollout