

# About me

 @HannesLagler

 <https://cloudblogger.at>



**Hannes Lagler-Gruener**

Multi Cloud Architect

 <https://cloudblogger.at>

 <https://www.linkedin.com/in/hannesl1>

 @HannesLagler



# Welcome to a new session about

 @HannesLagler

 <https://cloudblogger.at>

## Azure AD CA policy

Video type: Nugget

Video category: Level-200



# Session Agenda

 @HannesLagler

 <https://cloudblogger.at>

- What is Conditional Access
- Primary goals
- CA options
  - Assignments
  - Access controls
  - Enable policy
- Troubleshooting
- Live DEMO



# What is Conditional Access


- Can help to archive:
  - Prevent access to data from locations/clients that are undesirable
  - Prevent data download to devices that you are not comfortable with
  - Help you manage and reduce user and sign in risk
  - Reduce user friction, too many MFA prompts teach the user the wrong thing



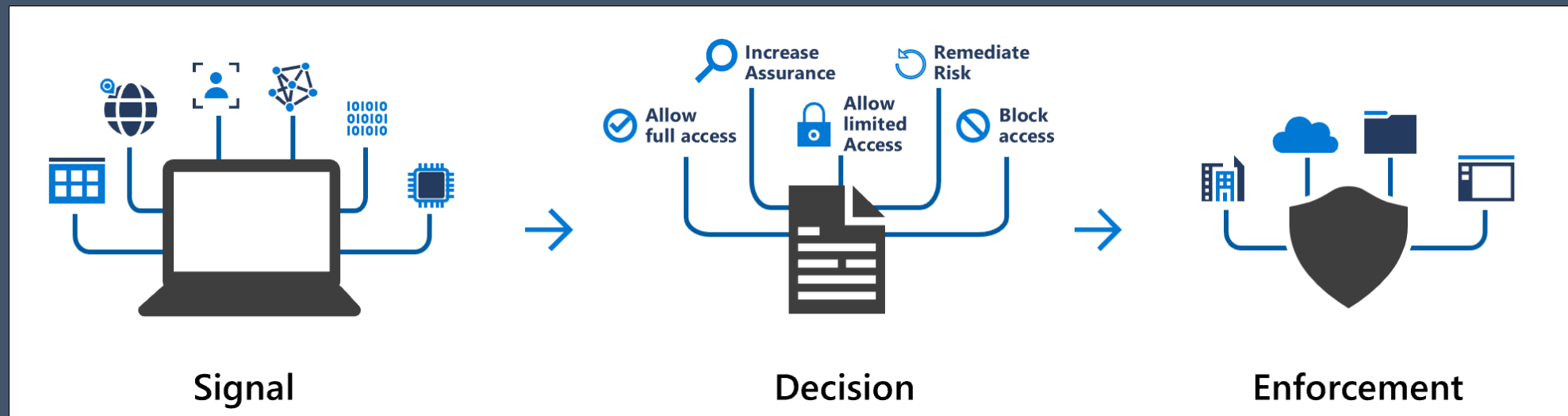
# Primary goals

 @HannesLagler

 <https://cloudblogger.at>

- 
- Empower users to be productive wherever and whenever
  - **Protect** the organization's assets

Conditional Access is at the heart of the new identity driven control plane.



# Assignments

Name \*  
Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ  
0 users and groups selected

Cloud apps or actions ⓘ  
No cloud apps or actions selected

Include Exclude

☒ None  
☐ All users  
☐ Select users and groups

☐ All guest and external users ⓘ  
☐ Directory roles ⓘ  
☐ Users and groups

Name \*  
Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ  
0 users and groups selected

Cloud apps or actions ⓘ  
No cloud apps or actions selected

Select what this policy applies to


Cloud apps User actions

Include Exclude

☒ None  
☐ All cloud apps  
☐ Select apps

- Users and groups
- Cloud apps or actions

# Assignments



Name *	User risk ⓘ
<input type="text" value="Example: 'Device compliance app policy'"/>	Not configured
Assignments	Sign-in risk ⓘ
Users and groups ⓘ	Not configured
0 users and groups selected	Device platforms ⓘ
Cloud apps or actions ⓘ	Not configured
No cloud apps or actions selected	Locations ⓘ
Conditions ⓘ	Not configured
0 conditions selected	Client apps ⓘ
	Not configured
	Device state (Preview) ⓘ
	Not configured

- Conditions
  - Sign-in risk requires Identity protection!



# Access controls

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Grant

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

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

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

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

☐ Require password change ⓘ

☐ DemoTerms of User

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Access controls

Grant ⓘ

0 controls selected


Session ⓘ

0 controls selected

Session

Control user access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

☐ Use app enforced restrictions ⓘ

 This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

- Grant
  - Block access
  - Grant access but require...
- Session
  - Define current session settings

# Enable policy

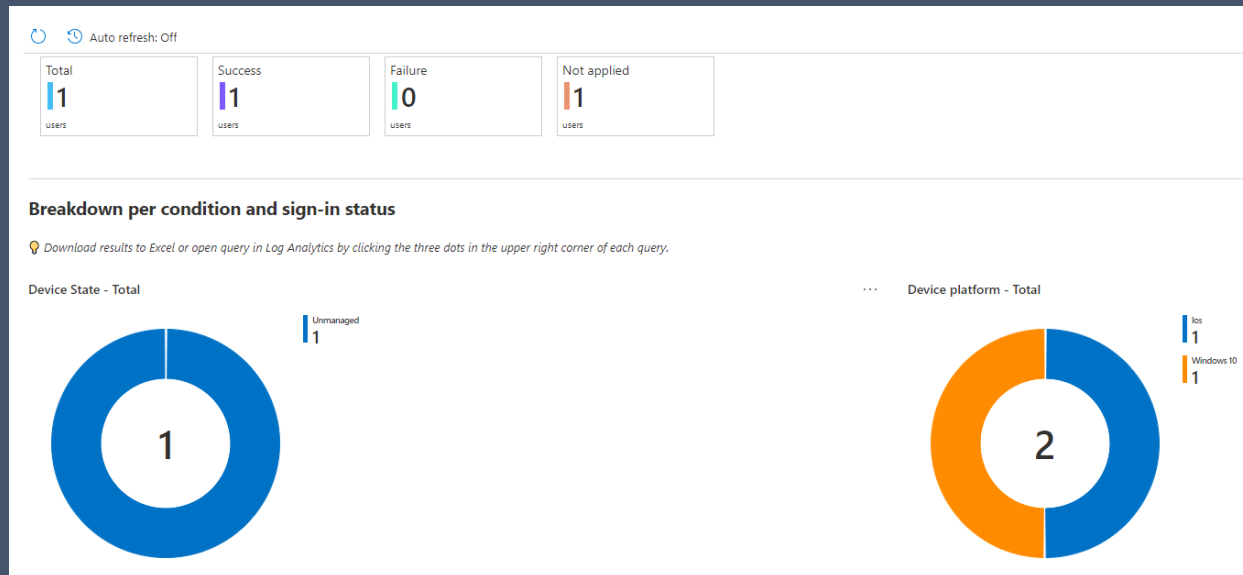
 @HannesLagler

 <https://cloudblogger.at>

Enable policy

☒ Report-only ☐ On ☐ Off

Create



- On
- Off
- Report-only

- 
- Start with “Report-only” policies
    - Check the Insights and reporting
  - Always implement excluding groups
  - Using the “What If” functionality
  - Backup policies!

# Switch to the Live Demo!

APPLAUSE

- Create a simple CA policy
- Troubleshoot the policy
- Backup policy solution