Microsoft

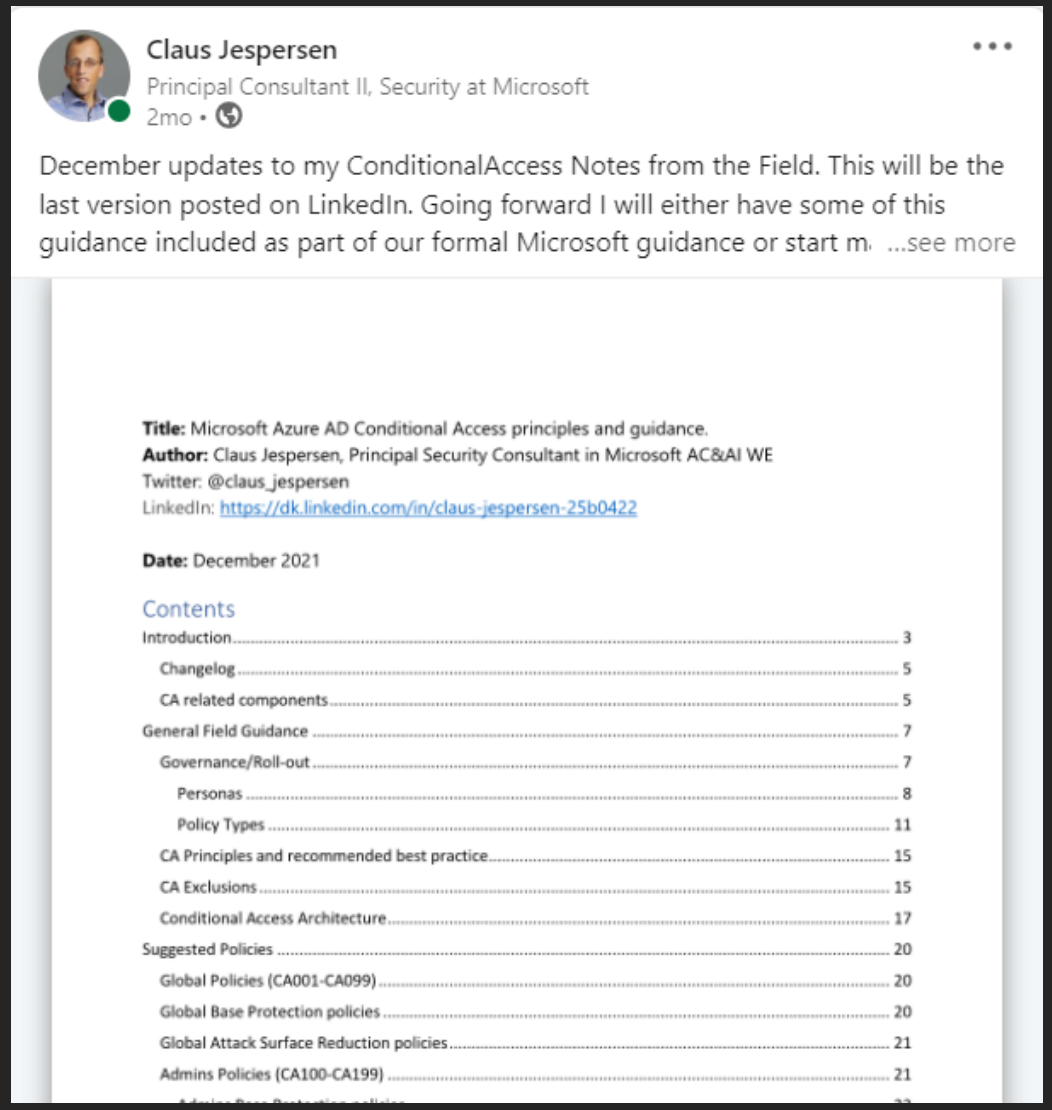
Troubleshooting Conditional Access configured for Zero Trust

Claus Jespersen
Principal Security Consultant
Microsoft Industry Solutions - AC&AI
EMEA, Denmark
@claus_Jespersen
Claus Jespersen | LinkedIn

Agenda

- Conditional Access for Zero Trust - guidance update
- Built-in troubleshooting tools
- Custom troubleshooting workbooks
- Example scenarios
  - Scenario problem statement
  - Scenario troubleshooting
  - Scenario solution(s)

CA Guidance for Zero Trust



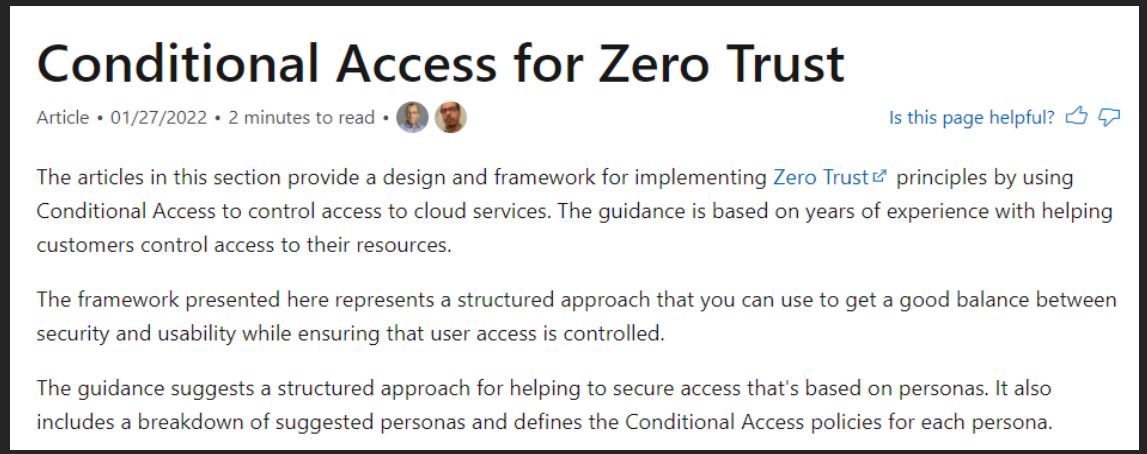
Claus Jespersen
Principal Consultant II, Security at Microsoft
2mo •

December updates to my ConditionalAccess Notes from the Field. This will be the last version posted on LinkedIn. Going forward I will either have some of this guidance included as part of our formal Microsoft guidance or start m ...see more

Title: Microsoft Azure AD Conditional Access principles and guidance.
Author: Claus Jespersen, Principal Security Consultant in Microsoft AC&AI WE
Twitter: @claus_jespersen
LinkedIn: https://dk.linkedin.com/in/claus-jespersen-25b0422

Date: December 2021

Contents



Conditional Access for Zero Trust

Article • 01/27/2022 • 2 minutes to read • Is this page helpful?

The articles in this section provide a design and framework for implementing Zero Trust principles by using Conditional Access to control access to cloud services. The guidance is based on years of experience with helping customers control access to their resources.

The framework presented here represents a structured approach that you can use to get a good balance between security and usability while ensuring that user access is controlled.

The guidance suggests a structured approach for helping to secure access that's based on personas. It also includes a breakdown of suggested personas and defines the Conditional Access policies for each persona.

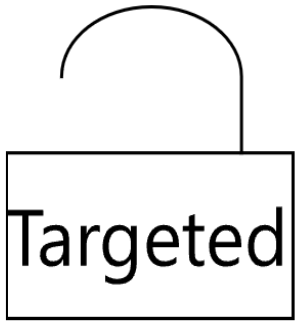
Notes from the field: LinkedIn post:
https://www.linkedin.com/posts/claus-jespersen-25b0422_conditional-access-guidance-december-2021-activity-6872879151271993344-u7Vd

Azure Architecture center design guidance:
Conditional Access for Zero Trust - Azure Architecture Center | Microsoft Docs

Spreadsheet with suggested policies
https://arch-center.azureedge.net/Conditional-Access-policies-for-personas.xlsx

Nordic Virtual Summit – Conditional Access Configured for Zero Trust
https://github.com/NordicVirtualSummit/3rdEdition/blob/main/NordicVirtualSummitConditionalAccessConfiguredforZeroTrustClausJespersen.pdf

Defining CA architecture type



CA for targeted apps

Select what this policy applies to

Cloud apps | User actions

Include | Exclude

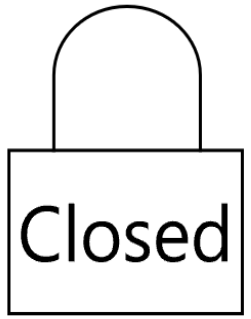
- None
- All cloud apps
- Select apps

Select

Office 365 Yammer and 2 more

- Microsoft Teams ...
- Office 365 Exchange O... ...

Zero Trust



CA for "All Cloud Apps"

Cloud apps or actions

Select what this policy applies to

Cloud apps | User actions

Include | Exclude

- None
- All cloud apps
- Select apps

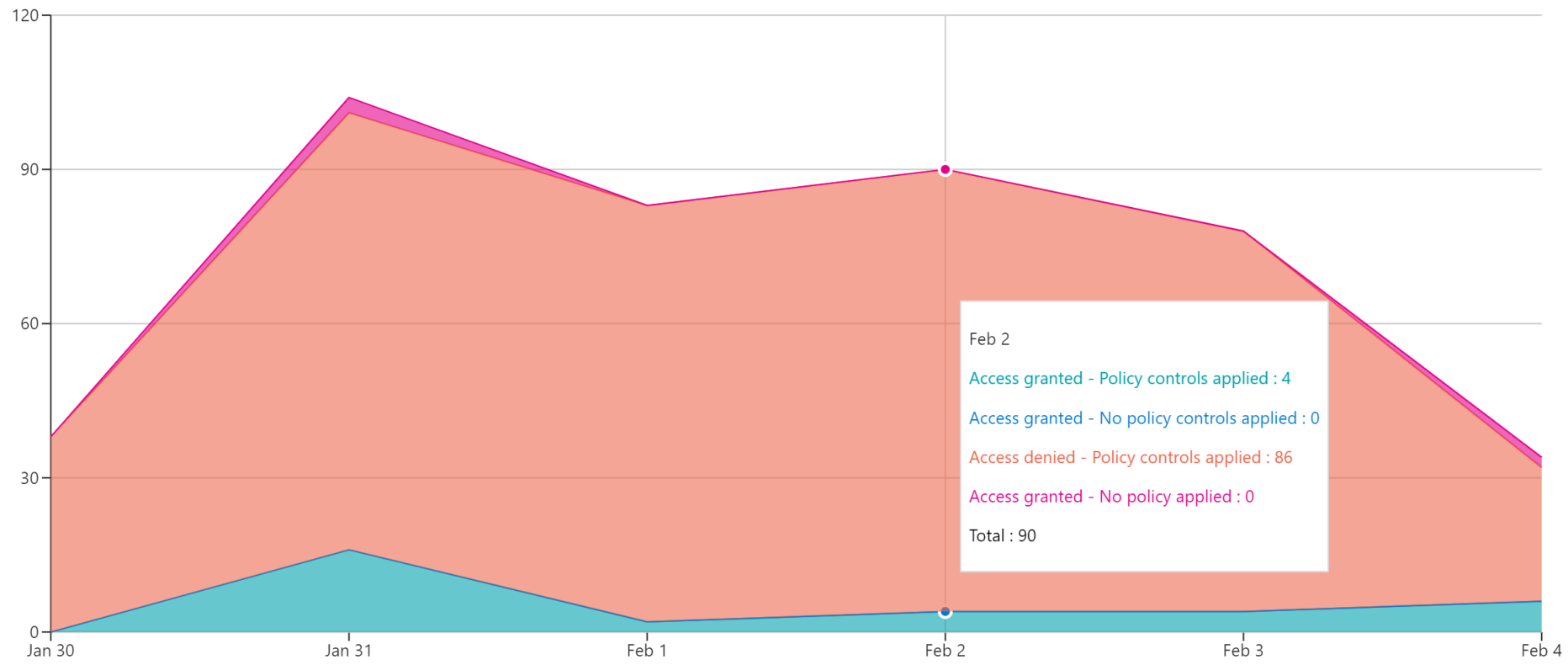
CA built-in troubleshooting tools

Conditional Access Overview

Getting started | Overview | Coverage | **Monitoring** | Tutorials

Sign-ins by Conditional Access result

Add filter | Date range: Last 7 days | Policy evaluated: All enabled policies | Reset filters



Total sign-ins	Access granted Controls applied	Access denied Controls applied	Access granted No Policy applied
427	32	390	5

What If ...

Policies

Info

Test the impact of Conditional Access on a user when signing in under certain conditions. Learn more

User or Workload identity

No user selected

Cloud apps, actions, or authentication context

Any cloud app

IP address

Enter IP address (ex: 40.77.182.32)

Country

Select country...

Device platform

Select device platform...

Client apps

Select a client app...

Device state (Preview)

Select device state...

Sign-in risk

Select sign-in risk...

User risk

Select user risk...

Report-only Mode

CA200-Internals-BaseProtection-AllApps-AnyPlatform-CompliantorAADHJ

Conditional Access policy

Delete

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

Name *

CA200-Internals-BaseProtection-AllApps-...

Assignments

Users or workload identities

Specific users included and specific users excluded

Cloud apps or actions

Enable policy

Report-only | On | Off

Conditional Access | Diagnose and solve problems

Azure Active Directory

- Overview (Preview)
- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- Virtual assistant (Preview)

Search for common problems, tools and more...

Troubleshooters

Select Troubleshoot for the problem you are attempting to resolve. Or try

Sign-in Diagnostic

Use the diagnostic to analyze what happened during a sign-in and what actions you can take to resolve problems.

Troubleshoot

Common problems

Problems configuring location-based policies

Restart chat

VA

Hello!

I can help you with a variety of Azure Active Directory topics that include:

- Conditional Access
- Multi Factor Authentication
- Hybrid Identity including AAD Connect
- Enterprise Applications
- Passwords

You can ask me questions such as:

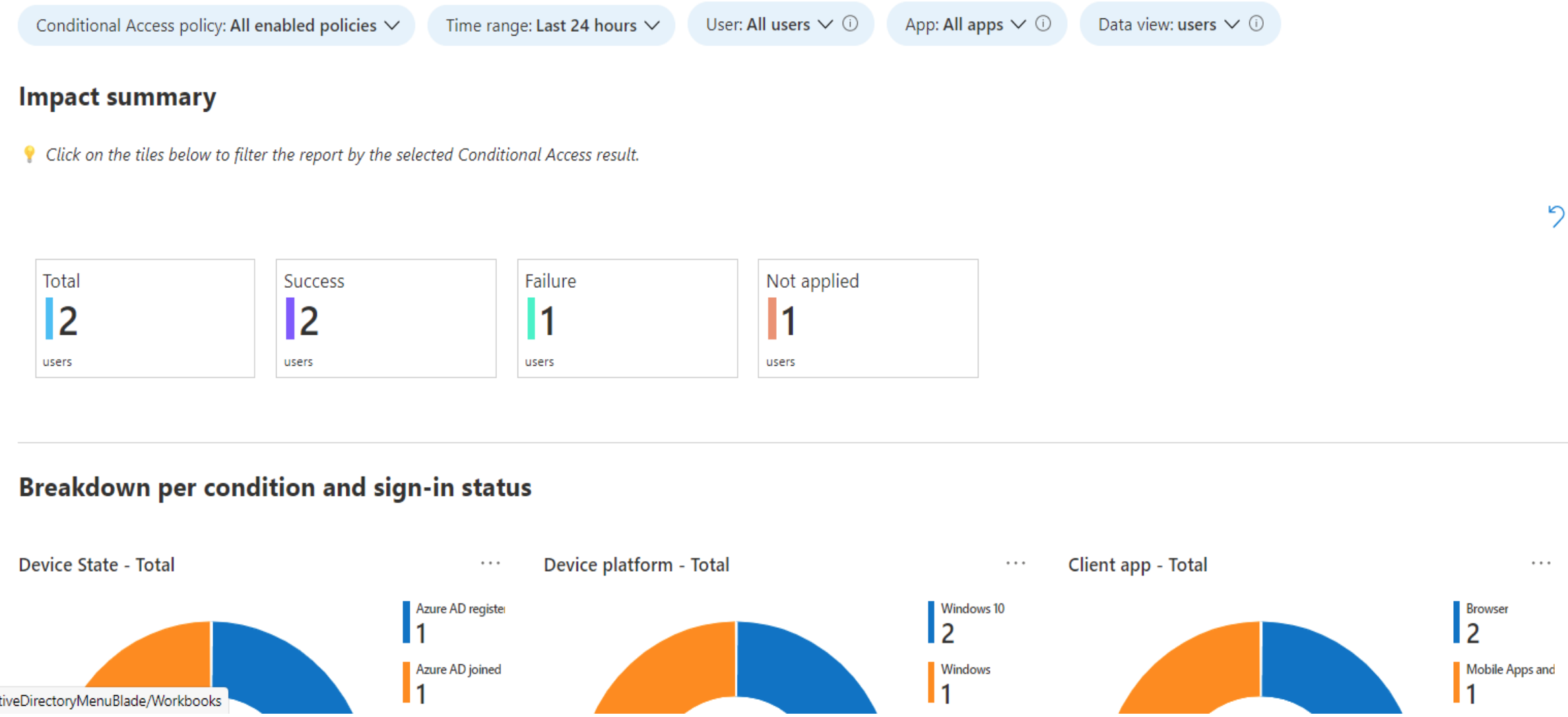
- How do I troubleshoot Conditional Access?
- How do I add MFA to my Radius Server?
- AAD Connect object sync is not working?
- Self Service Password Reset is failing?

So, what can I help you with?

Just now

Troubleshooting workbooks

Built-in workbook for Conditional Access



Challenges using built-in workbook

- CA Insights shows lots of data (user type, CA status: notApplied)
- CA Insights workspace may be hosted in Sentinel, - delegation issues

- Requiring compliance for all devices calls for compliance status details
- Intune compliance status does not show trending data

Conditional Access insights and reporting - enhanced

Workspace: /subscriptions/a0e93de2-0040-... | Guide: Off

User Type Option: Member | Platform: Windows

Guest
Member

User sign-ins | Service principal sign-ins

SigninLogs: fa0f1c37-8e6f-4ccf-81c1-6c8ccb... | AADServicePrincipalSign...: <unset>

In order to view service prinicpal sign-ins, ensure that Diagnostic Settings are configured to send ServicePrincipalSignInLogs to your log analytics workspace. Learn more.

Conditional Access policy: CA200 - Base Policy MDCA poli... | Time range: Last 7 days | User: <unset> | App: <unset> | Data view: users

Impact summary

Click on the tiles below to filter the report by the selected Conditional Access result.

Total	Success	Failure	User action required	Not applied
2 users	1 users	0 users	0 users	2 users

ConditionalAccessforZeroTrustResources/Workbooks at main · microsoft/ConditionalAccessforZeroTrustResources (github.com)

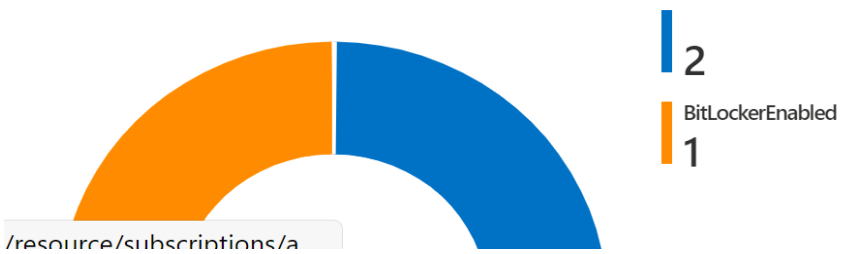
CAInsightsWorkbookimprovedfeb2022.workbook

TimeRange: **Last 60 days** | username: **<unset>** | DeviceName: **<unset>**

IntuneCompliancefeb2022withdevicename.workbook

TimeGenerated	ComplianceState	DeviceName	UPN	LastContact
2/12/2022, 1:20:10 AM	Not compliant	Claus's MacBook Air	testuser@	2021-07-10 07:20:57.2770920
2/12/2022, 1:20:10 AM	Not compliant	DESKTOP-DGPST2E	testuser@	2022-01-04 20:14:11.0000000
2/11/2022, 1:09:28 AM				
2/11/2022, 1:08:28 AM	Compliant	DESKTOP-VFCR8CD	testuser@	2022-02-10 19:43:16.7148783
2/11/2022, 1:08:28 AM	Not compliant	DESKTOP-DGPST2E	testuser@	2022-01-04 20:14:11.0000000
2/11/2022, 1:08:28 AM	Not compliant	DESKTOP-DGPST2E	testuser@	2022-01-31 17:47:46.0000000
2/11/2022, 1:08:28 AM	Not compliant	Claus's MacBook Air	testuser@	2021-07-10 07:20:57.2770920
2/11/2022, 1:08:28 AM	Not compliant	PAWCSM-R90LY8U6	pawuser@	2022-02-01 11:48:41.0000000
2/10/2022, 1:04:34 AM				
2/10/2022, 1:03:34 AM	Not compliant	PAWCSM-R90LY8U6	pawuser@	2022-02-01 11:48:41.0000000
2/10/2022, 1:03:34 AM	Not compliant	Claus's MacBook Air	testuser@	2021-07-10 07:20:57.2770920

Reason for NON Compliant last 30 days



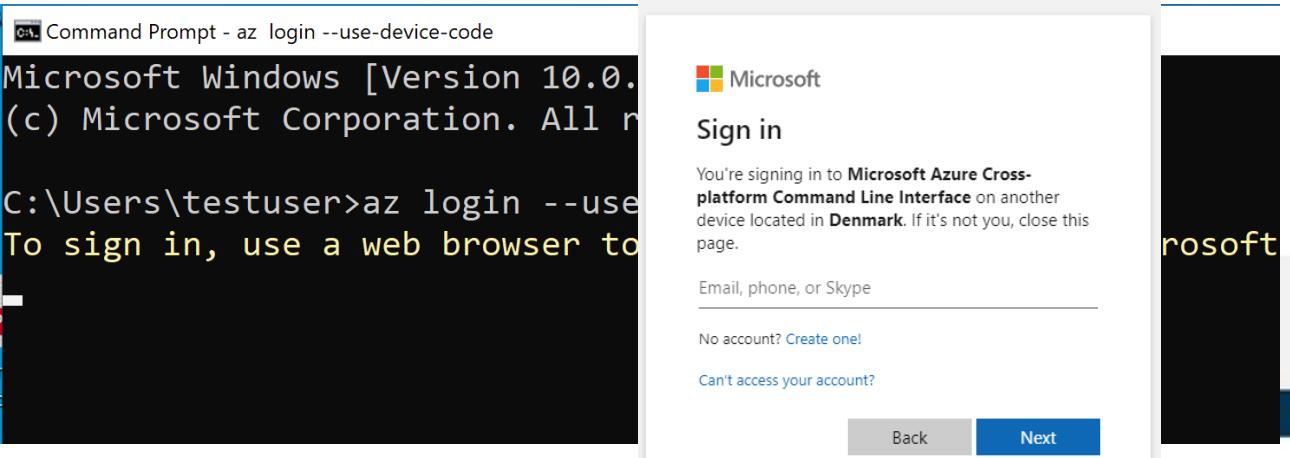
Reason for incompliance

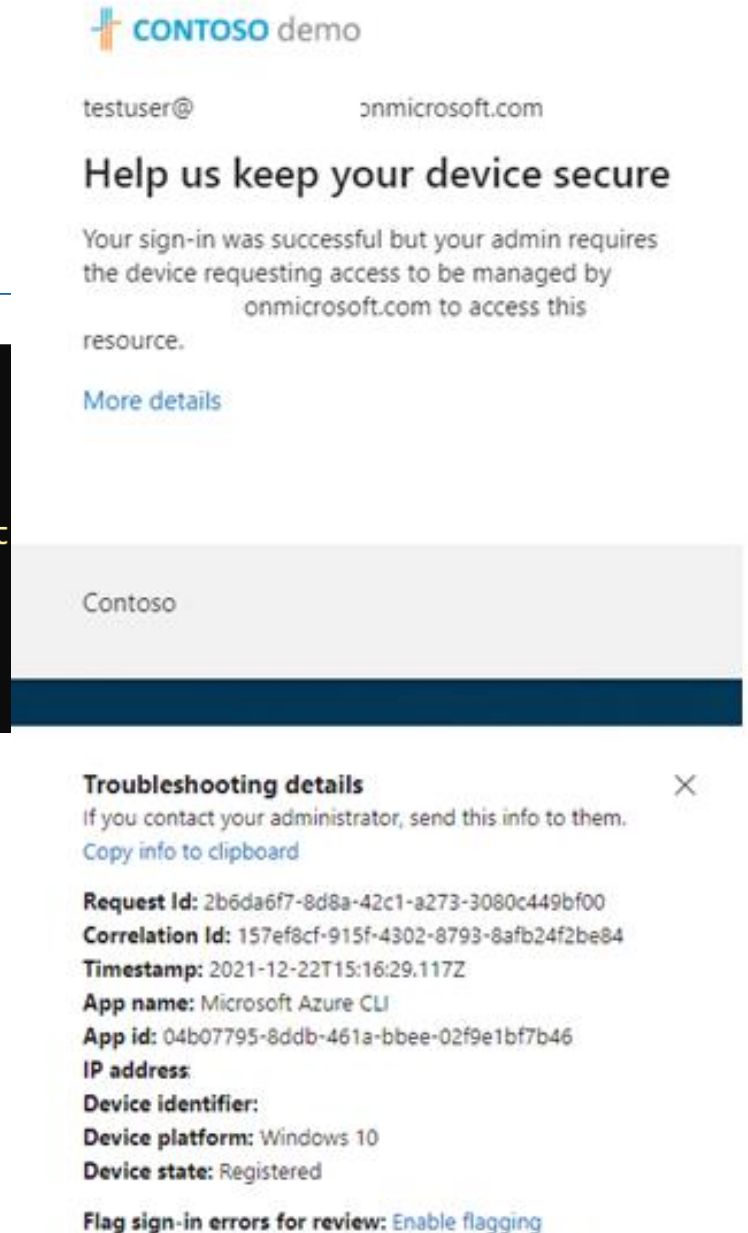
UserName	Reason	DeviceHostName	DeviceOS
testuser		DESKTOP-DGPST2E	Windows 10.0.19043.1415
admin		PAWCSM-R90LY8U6	Windows 10.0.19043.1415
testuser	BitLockerEnabled	DESKTOP-VFCR8CD	Windows 10.0.22000.493

[ConditionalAccessforZeroTrustResources/Workbooks at main · microsoft/ConditionalAccessforZeroTrustResources (github.com)]

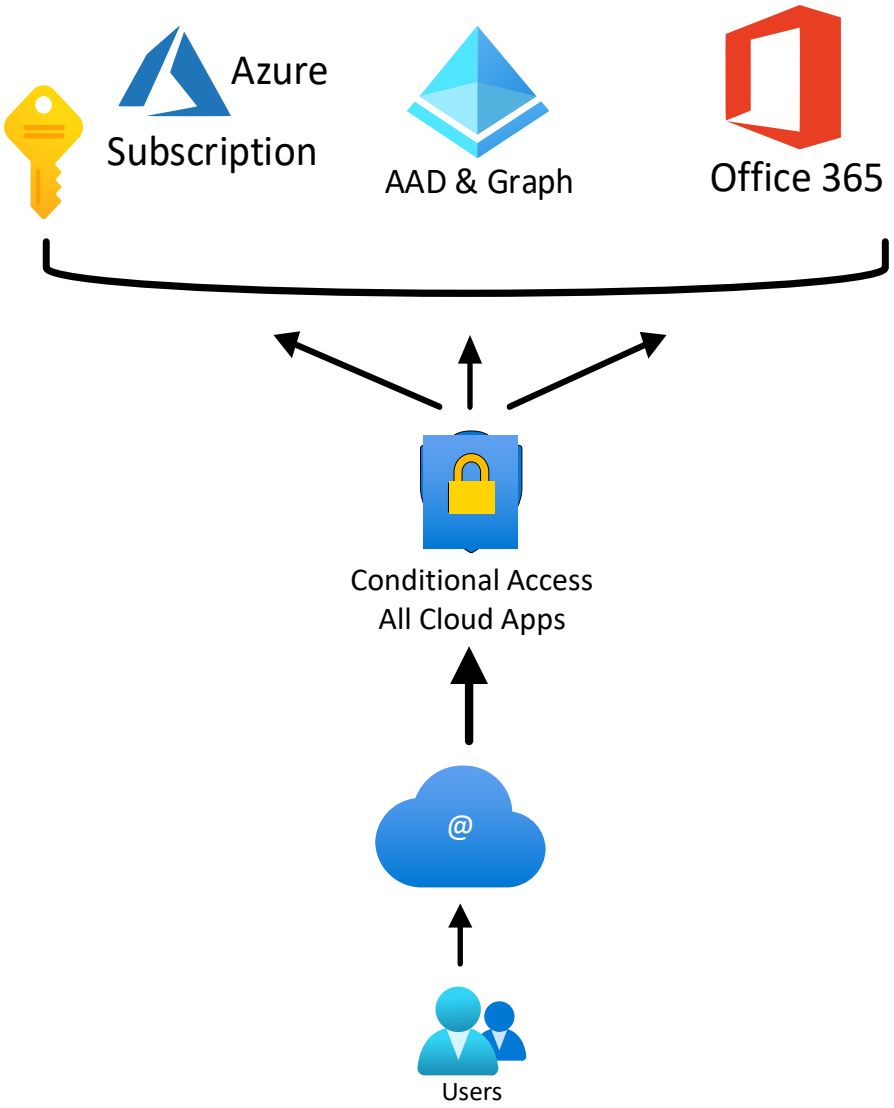
Example scenarios
Device code flow

Device Code Flow – Problem statement





Device Code Flow – Problem Statement..



Device Code Flow – Troubleshooting

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only | ...

Date	12/22/2021, 4:16:25 PM
Request ID	2b6da6f7-8d8a-42c1-a273-3080c449bf00
Correlation ID	157ef8cf-915f-4302-8793-8afb24f2be84
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	530033
Failure reason	Remote device flow blocked due to device based conditional access.
Additional Details	This request is authorizing a remote device, and there is a conditional access policy that requires device authentication. The request is blocked because we cannot assert the properties of the remote device. View the Conditional Access information for this request in the sign-in logs for more details about the policy applied here.
Troubleshoot Event	Follow these steps: 1. Launch the Sign-in Diagnostic. 2. Review the diagnosis and act on suggested fixes.
User	testuser
Username	testuser@
User ID	13564ab9-c28e-4c70-a665-7855937744a2
Sign-in identifier	testuser@
User type	Member
Cross tenant access type	None
Application	Microsoft Azure CLI

Date : **Last 24 hours**

Date	Req
12/22/2021, 4:28:07 ...	c38
12/22/2021, 4:27:22 ...	786
12/22/2021, 4:26:57 ...	8ed
12/22/2021, 4:25:24 ...	8ea
12/22/2021, 4:16:25 ...	2b6
12/22/2021, 4:04:33 ...	971

otocol : **None Selected** | Add filters

ation Protocol

ation

de

Resource	Condit
Windows Azure Acti...	Failure
Windows Azure Acti...	Failure
Windows Azure Acti...	Failure
Windows Azure Acti...	Succes
Windows Azure Serv...	Succes
Windows Azure Acti...	Not Ap

Device Code Flow – Solution option 1 – Exclude apps

CA200-Internals-BaseProtection-AllApps-AnyPlatform-CompliantorAADHJ

Conditional Access policy

Delete

policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA200-Internals-BaseProtection-AllApps-...

Assignments

Users or workload identities

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps included and 3 apps excluded

Conditions

1 condition selected

Access controls

Grant

apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include **Exclude**

Select the cloud apps to exempt from the policy

Select excluded cloud apps

Microsoft Intune Enrollment and 2 more

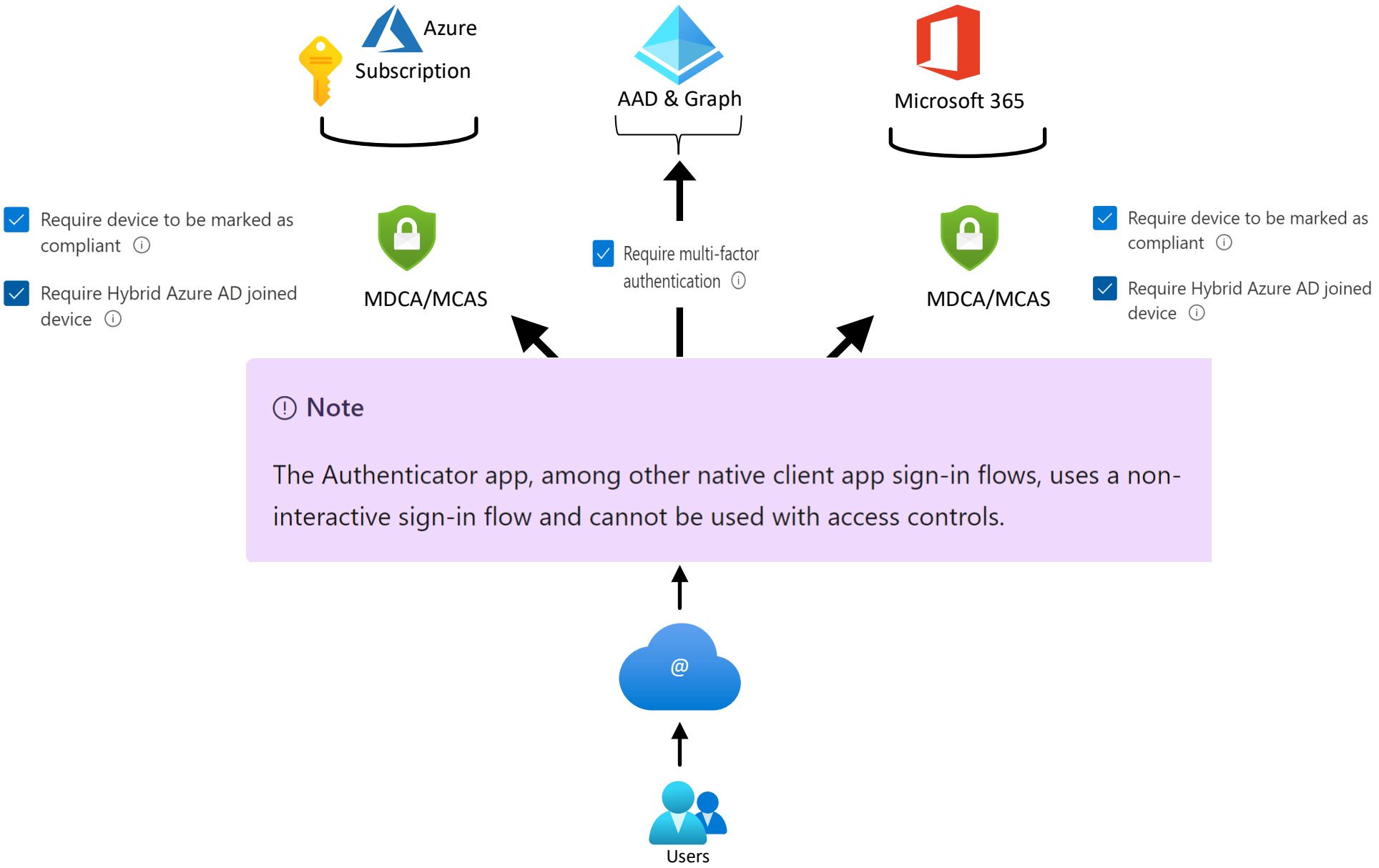
MA Microsoft Azure Management
797f4846-ba00-4fd7-ba43-dac1f8f63013

CM CMG-ServerApp
bd8fdeba-e743-437f-8cf9-411db47fa6...

MI Microsoft Intune Enrollment
d4ebce55-015a-49b5-a083-c84d1797a...

...and create separate CA policy to require MFA for Microsoft Azure Management

Device Code Flow – Solution option 2 – Use MDCA/MCAS



CA200-Internals-BaseProtection-AllApps-AnyPlatform-CompliantorAADHJ

Conditional Access policy

Delete

Users or workload identities

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps included and 2 apps excluded

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

Use Conditional Access App Control

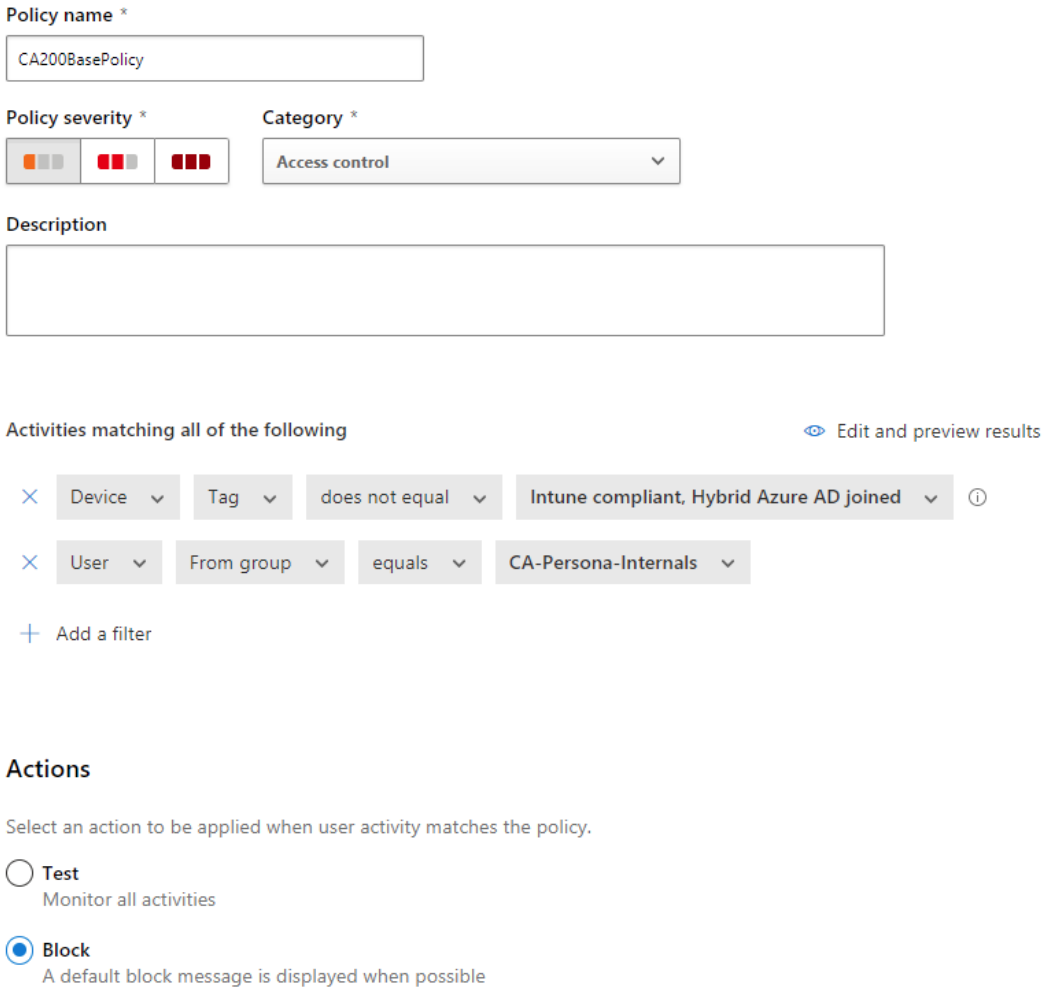
Grant

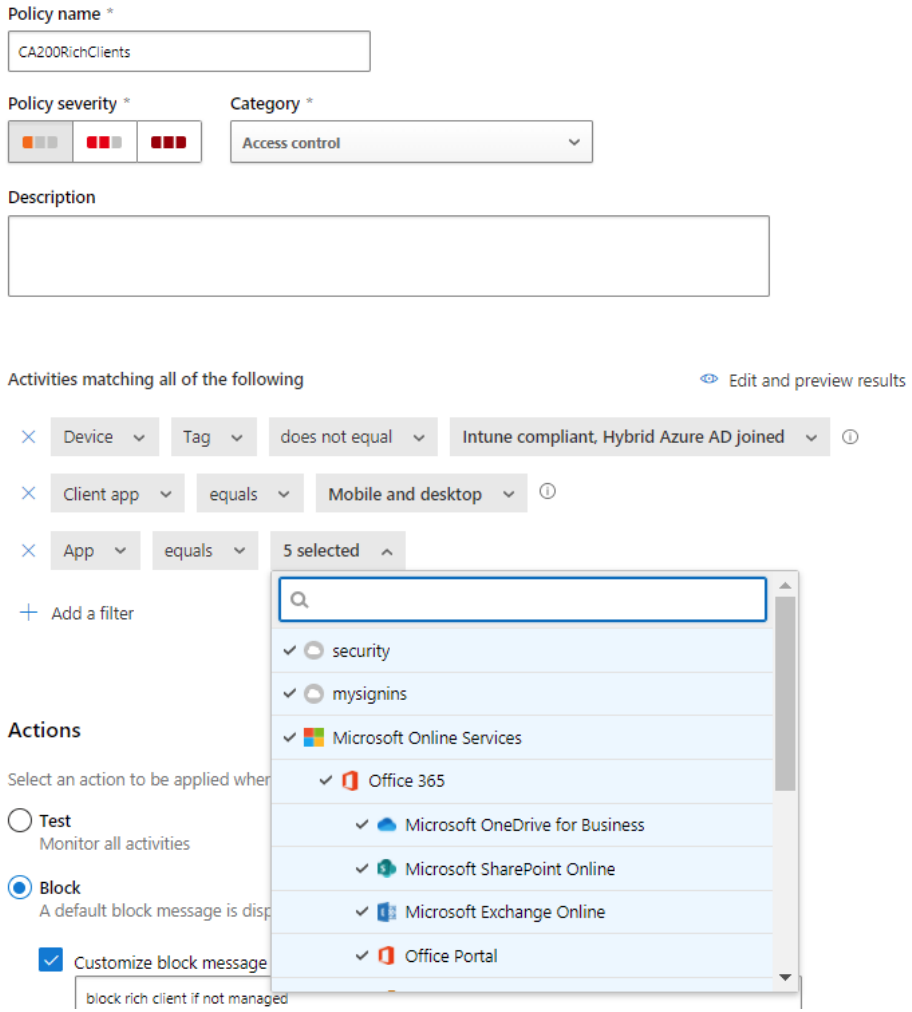
Control access enforcement to block or grant access. Learn more

- ○ 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
- ☐ TermsOfUseforCA

MDCA/MCAS Policy





CA200-Internals-BaseProtection-AllApps-AnyPlatform-MFAforUnmanaged

Conditional Access policy

Delete

Name *

CA200-Internals-BaseProtection-AllApps-...

Assignments

Users or workload identities

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

1 condition selected

Access controls

Grant

1 control selected

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure

Yes | No

Devices matching the rule:

- (•) Include filtered devices in policy
- ( ) Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Not equals	True
And	TrustType	Not equals	Hybrid Azure AD joined

+ Add expression

Rule syntax

```
device.isCompliant -ne True -and device.trustType -ne "ServerAD"
```

Grant

Control access enforcement to block or grant access. Learn more

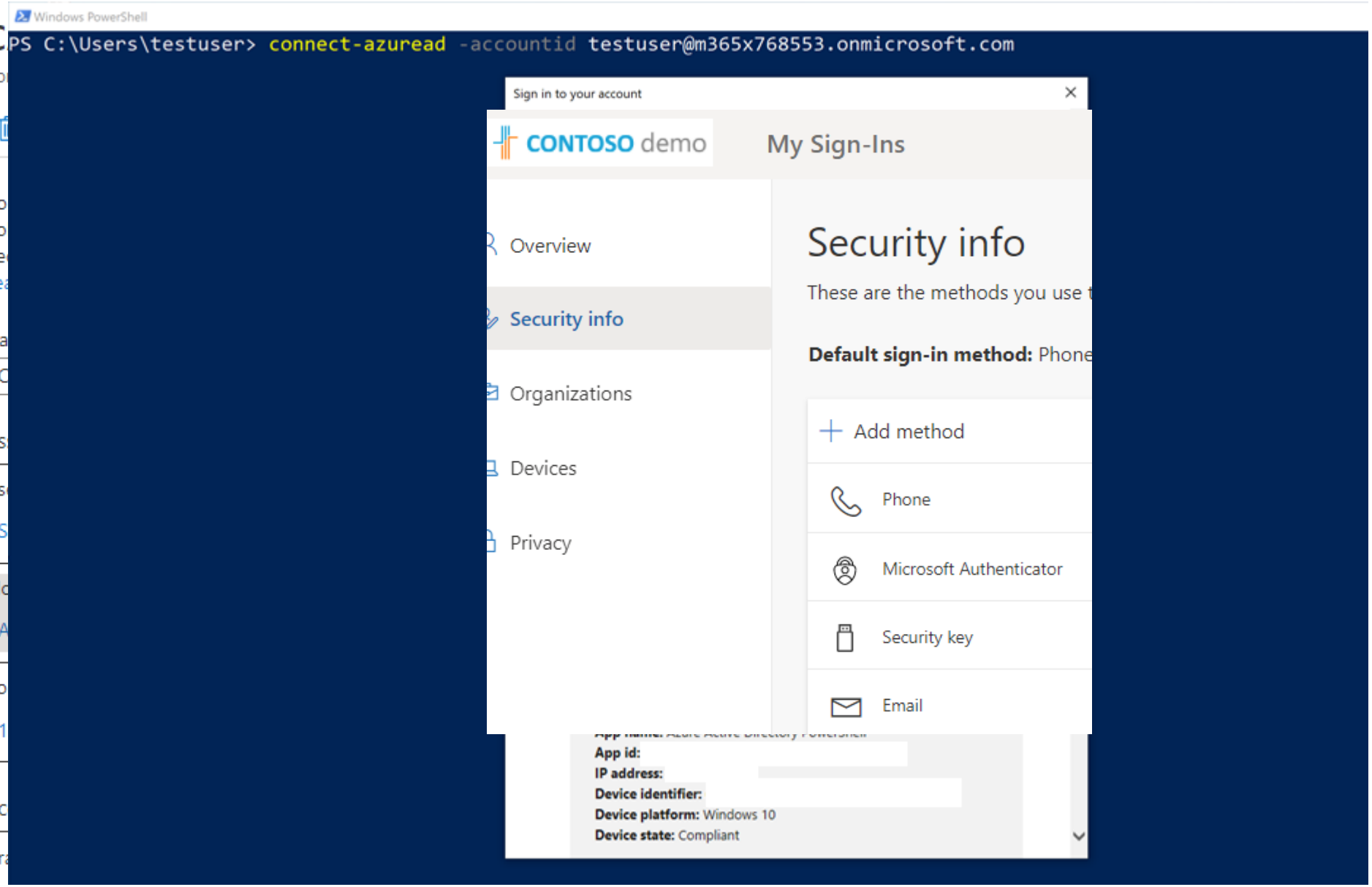
- ( ) Block access
- (•) Grant access

- [x] 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
- [ ] TermsOfUseforCA

Example scenarios
Attack Surface Reduction

“Block access to All Cloud Apps except..”

Attack Surface Reduction – Problem statement



Block access

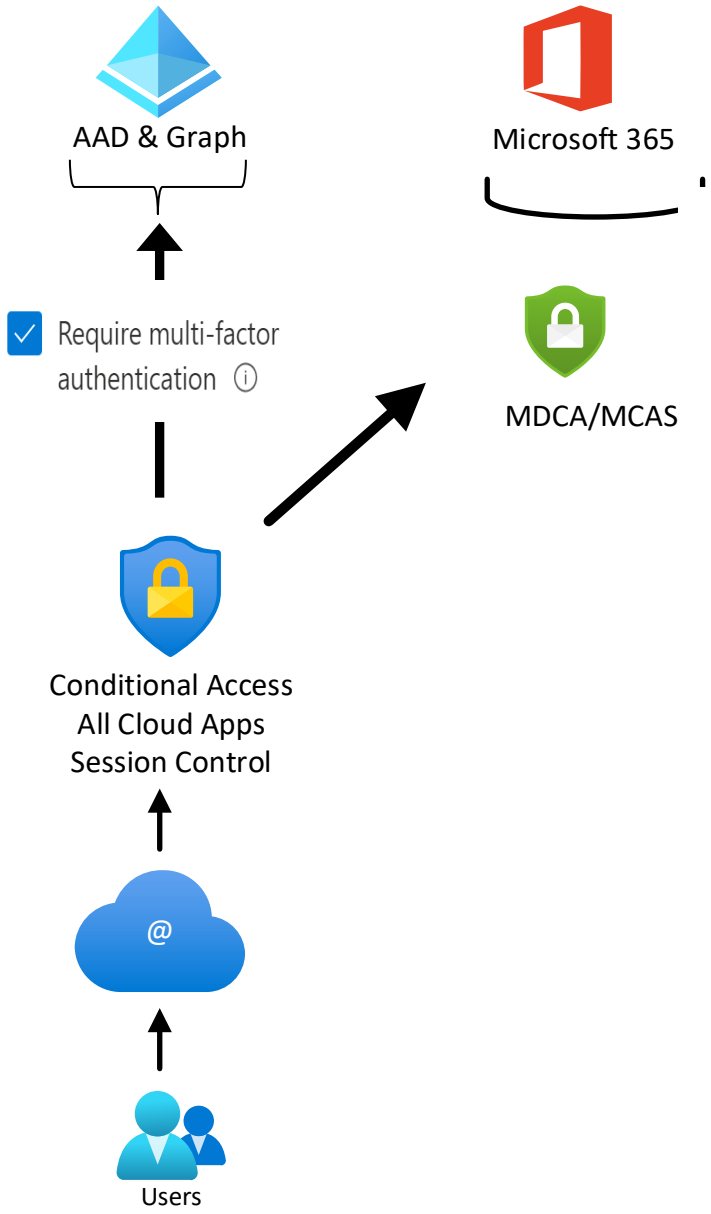
Attack Surface Reduction - Troubleshooting

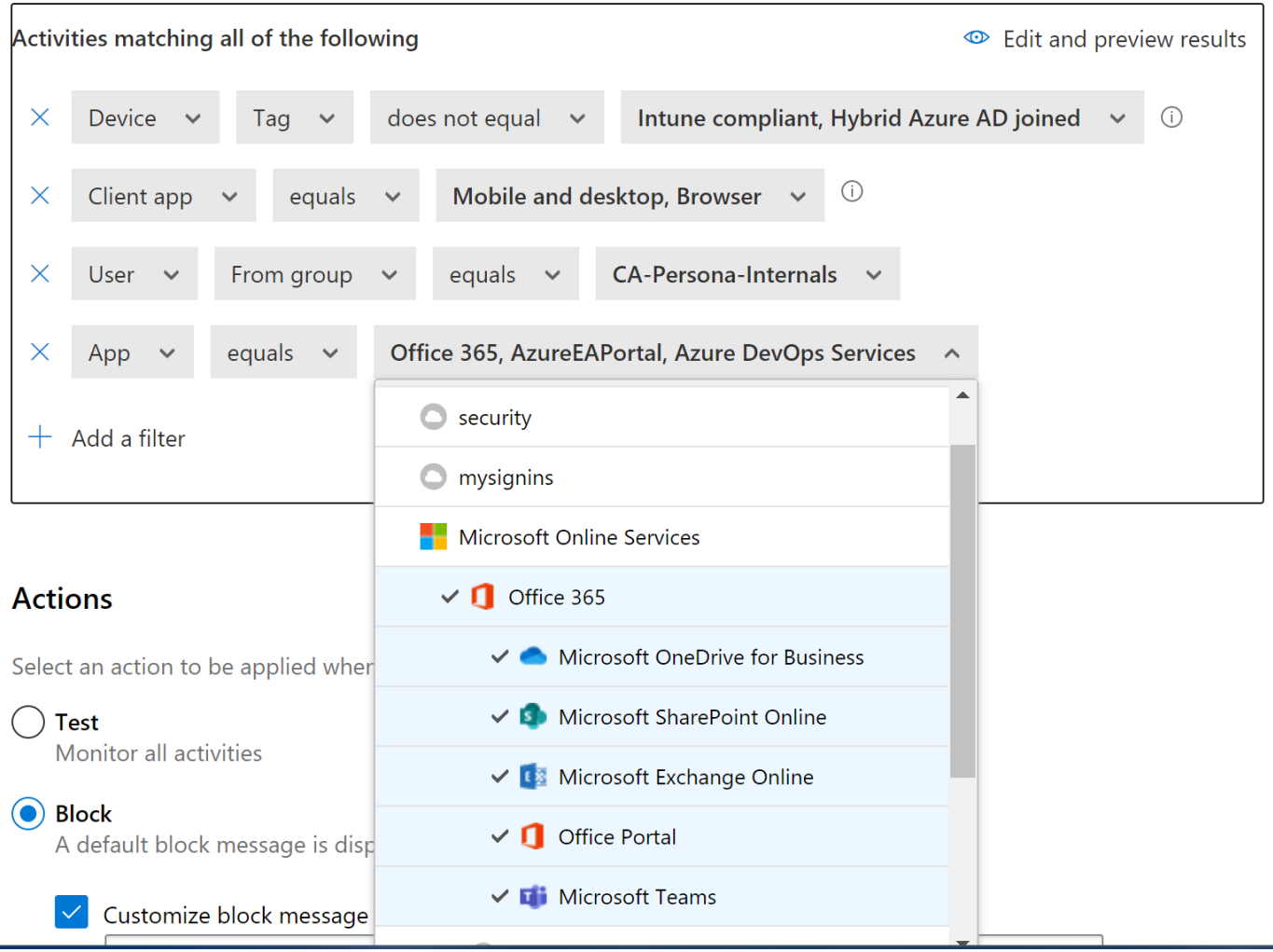
Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only | ...

Date	12/22/2021, 4:26:57 PM
Request ID	8ed0a85d-04ae-4d25-9f67-c3822f9c9f00
Correlation ID	dd531212-1add-453c-a23b-7558a6e5670d
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	53003
Failure reason	Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.
Additional Details	If this is unexpected, see the conditional access policy that applied to this request in the Azure Portal.
Troubleshoot Event	Follow these steps: 1. Launch the Sign-in Diagnostic. 2. Review the diagnosis and act on suggested fixes.
User	testuser
Username	testuser@
User ID	
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Azure Active Directory PowerShell

Attack Surface Reduction – Solution option 1 - Use MDCA/MCAS





Attack Surface Reduction – Solution option 2 - Block app

Conditional Access policy

Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

2 apps included

Conditions

0 conditions selected

Access controls

Grant

Block access

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select

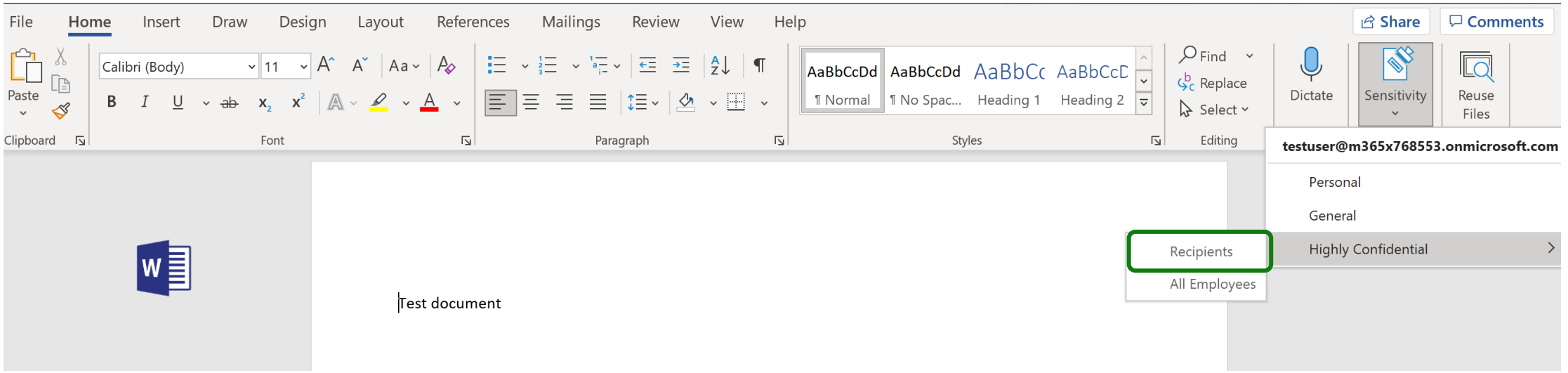
Microsoft Cloud App Security (Internal) and 1 more

MA Microsoft Azure Management
797f4846-ba00-4fd7-ba43-dac1f8f63013

Microsoft Cloud App Security (I
25a6a87d-1e19-4c71-9cb0-16e88ff608...

Example scenario
Unified Labeling

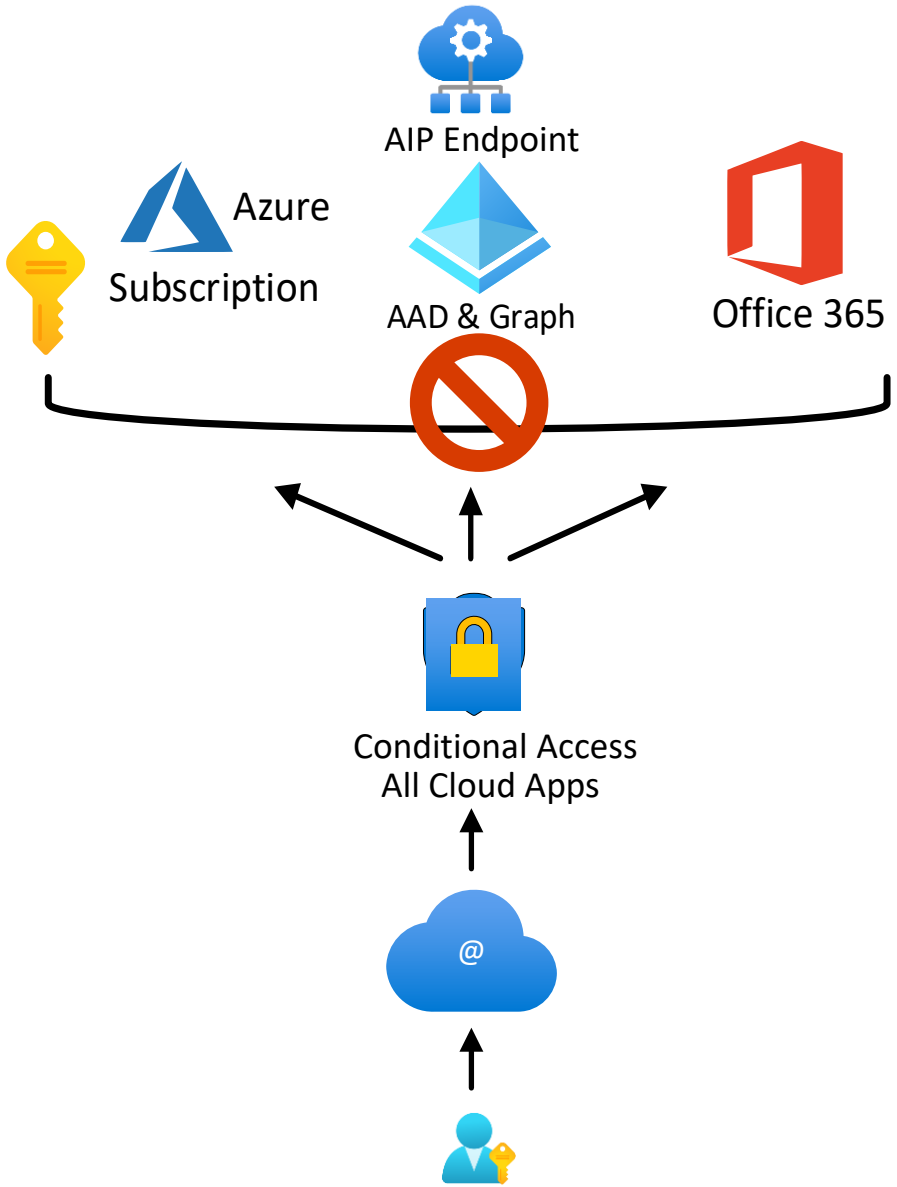
Unified Labeling – Problem statement



Send to external user

External User,
not a B2B/Guest user

Unified Labeling – Problem statement..



Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	12/25/2021, 6:49:26 PM
Request ID	
Correlation ID	96615b29-b063-4776-8b45-8ba96bfd4f2f
Authentication requirement	Multi-factor authentication
Status	Failure
Failure reason	Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.
User	
Username	
User ID	
Sign-in identifier	
User type	Guest
Cross tenant access type	B2B collaboration
Application	Microsoft Office
Application ID	d3590ed6-52b3-4102-aeff-aad2292ab01c
Resource	Microsoft Rights Management Services

CA400-Guests-BaseProtection-AllApps-AnyPlatform-MFA

Conditional Access policy

Delete

Learn more

Name *

CA400-Guests-BaseProtection-AllApps-An...

Assignments

Users or workload identities

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

1 condition selected

Access controls

Grant

1 control selected

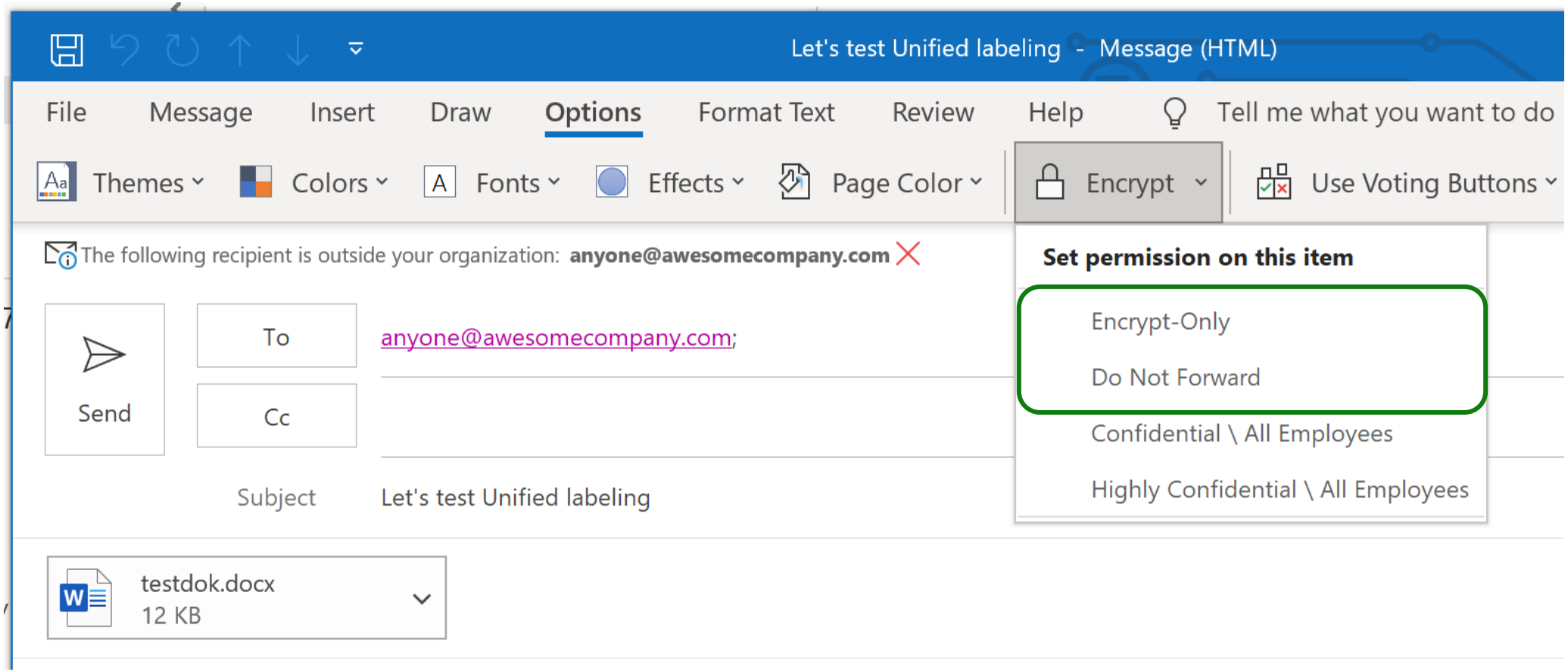
Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

Require multi-factor authentication

Unified Labeling - Solution option 2 – use OME



Unified Labeling - Solution option 3 – exclude AIP

CA001-Global-BaseProtection-AllApps-AnyPlatform-MFA

Conditional Access policy

Delete

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

Name *

CA001-Global-BaseProtection-AllApps-An...

Assignments

Users or workload identities

All users included and specific users excluded

Cloud apps or actions

All cloud apps included and 1 app excluded

Conditions

1 condition selected

Access controls

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include **Exclude**

Select the cloud apps to exempt from the policy

Select excluded cloud apps

Microsoft Azure Information Protection

Microsoft Azure Information Pro...

00000012-0000-0000-c000-000000000...

Grant

grant access. Learn more

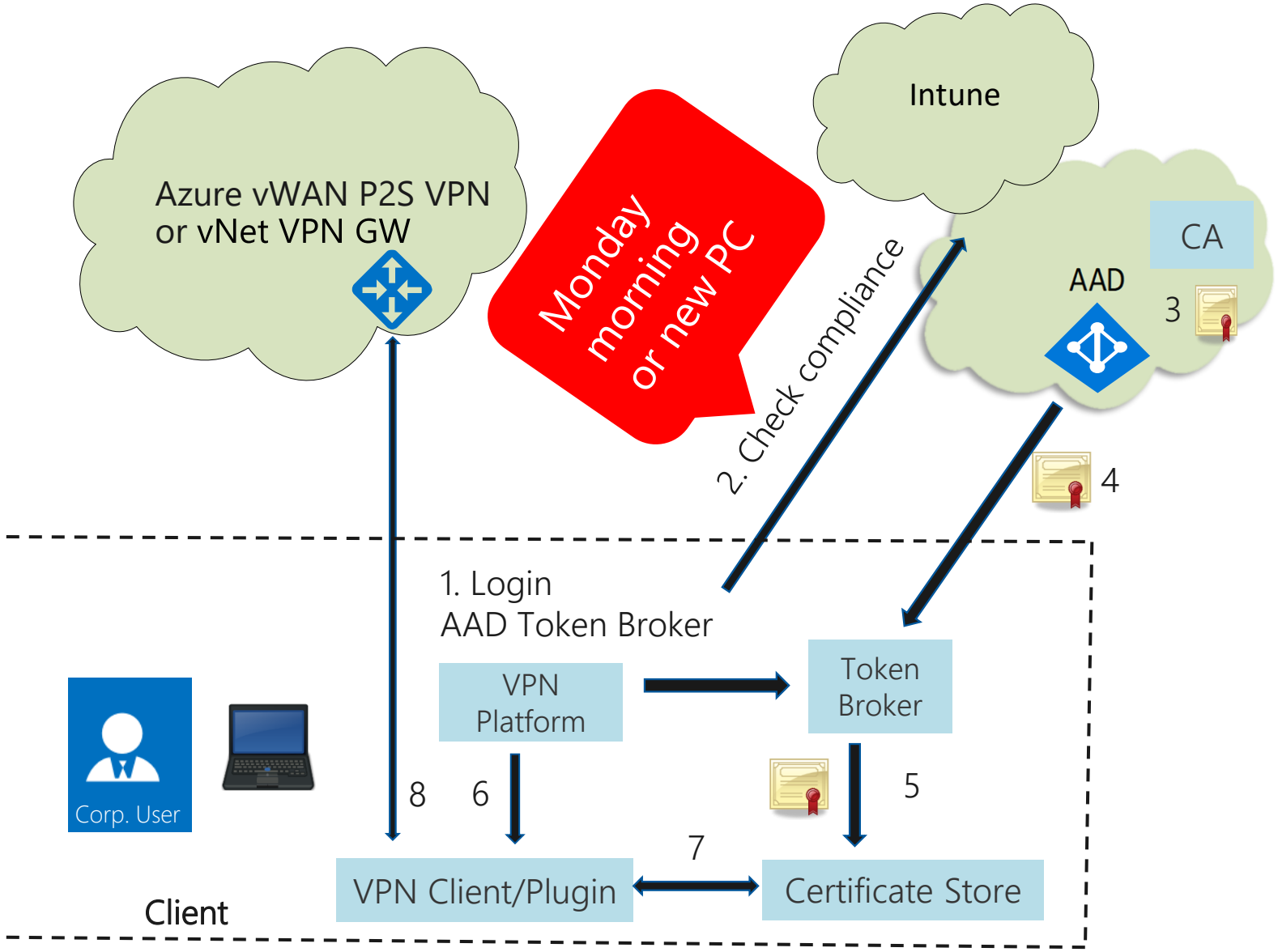
Block access

Grant access

Require multi-factor authentication

Example scenario
CA based VPN

CA based VPN (IPSec) – Problem statement



CA based VPN – Troubleshooting workbook

Compliance Trend Workbook

Compliance Trend Workbook in Contoso

The purpose of this dashboard is to give you full oversight of your Windows client compliance health.

Note: Figures are updated on a 24 hour cycle.

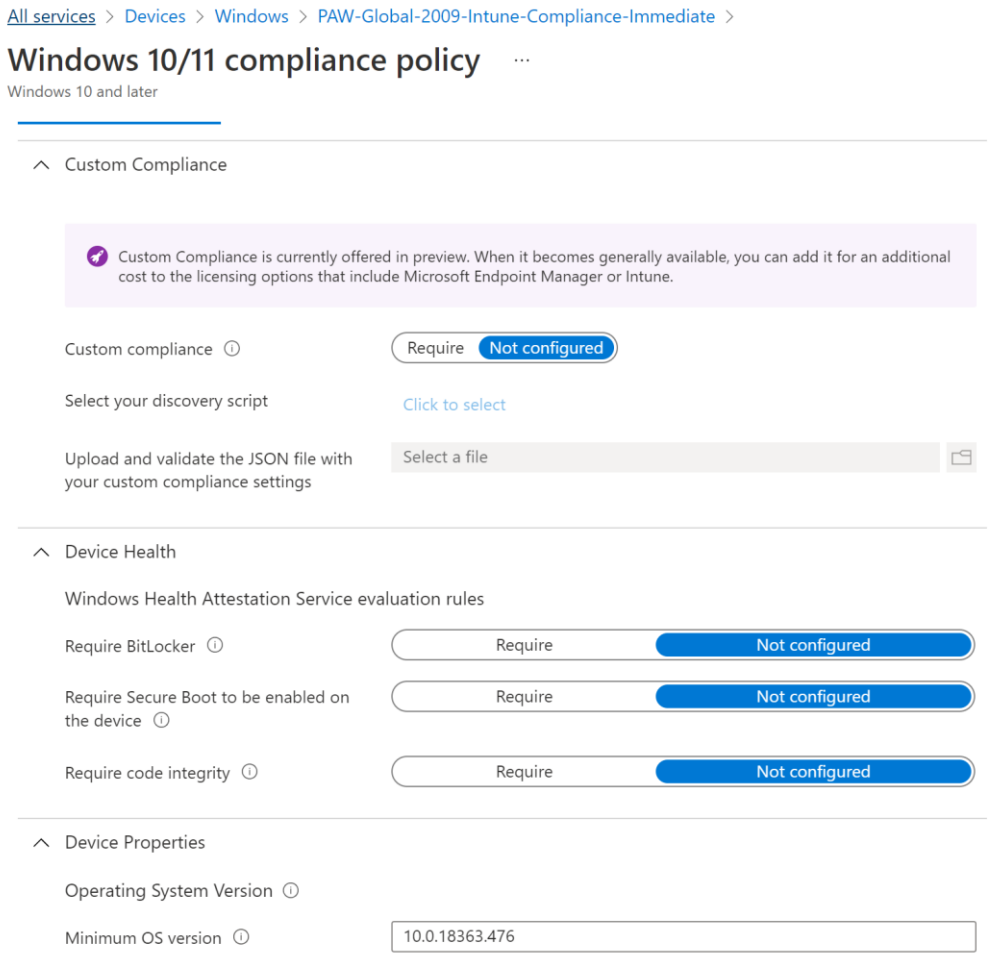
TimeRange: **Last 60 days** username: **<unset>**

TimeGenerated	ComplianceState	DeviceName	UPN	LastContact	DeviceId
2/10/2022, 1:04:34 AM					
2/10/2022, 1:03:34 AM	Not compliant	PAWCSM-R90LY8U6	pawuser@ onmicrosoft.com	2022-02-01 11:48:41.0000000	
2/10/2022, 1:03:34 AM	Not compliant	Claus's MacBook Air	testuser@ onmicrosoft.com	2021-07-10 07:20:57.2770920	
2/10/2022, 1:03:34 AM	Compliant	DESKTOP-VFCR8CD	testuser@ onmicrosoft.com	2022-02-09 14:56:11.0000000	
2/10/2022, 1:03:34 AM	Not compliant	DESKTOP-DGPST2E	testuser@ onmicrosoft.com	2022-01-31 17:47:46.0000000	
2/10/2022, 1:03:34 AM	Not compliant	DESKTOP-DGPST2E	testuser@ onmicrosoft.com	2022-01-04 20:14:11.0000000	
2/9/2022, 1:02:10 AM					
2/9/2022, 1:01:10 AM	Not compliant	DESKTOP-DGPST2E	testuser@ onmicrosoft.com	2022-01-04 20:14:11.0000000	
2/9/2022, 1:01:10 AM	Not compliant	Claus's MacBook Air	testuser@ onmicrosoft.com	2021-07-10 07:20:57.2770920	
2/9/2022, 1:01:10 AM	Not compliant	PAWCSM-R90LY8U6	pawuser@ onmicrosoft.com	2022-02-01 11:48:41.0000000	
2/9/2022, 1:01:10 AM	Not compliant	DESKTOP-DGPST2E	testuser@ onmicrosoft.com	2022-01-31 17:47:46.0000000	

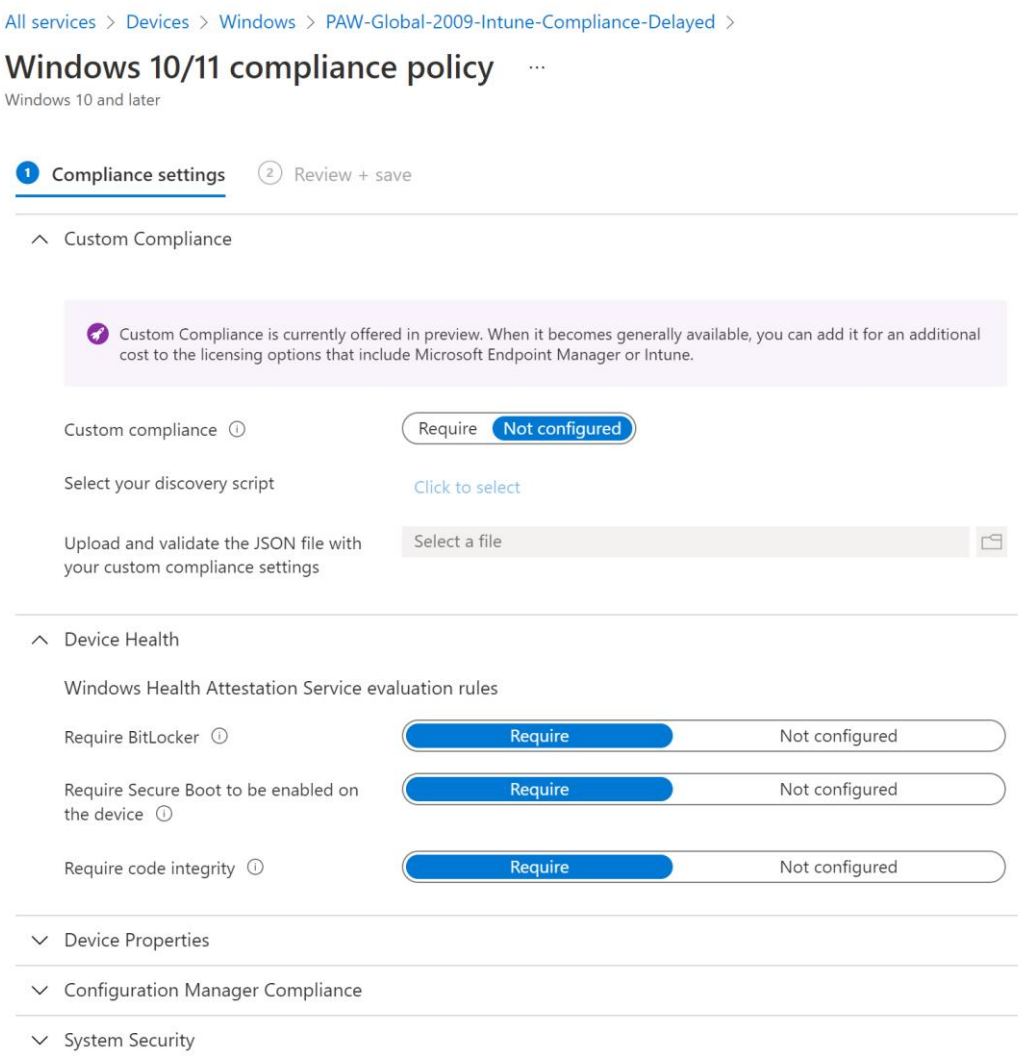
AzureVPNworkbookwiki.pdf

CA based VPN – Solution option 1 – split policy

Immediate



Delayed – grace period

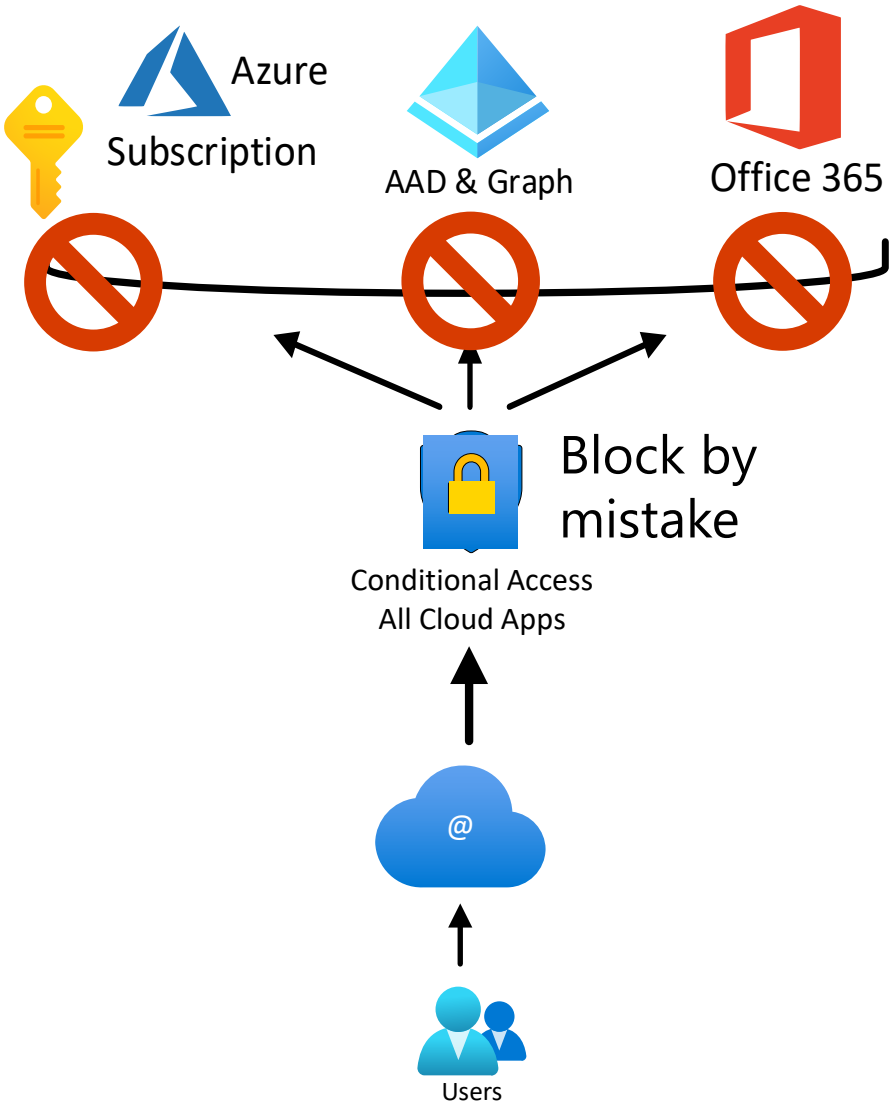


CA based VPN – Solution option 2 – Azure VPN

…use Azure AD VPN which is a VPN client natively integrated with Azure AD

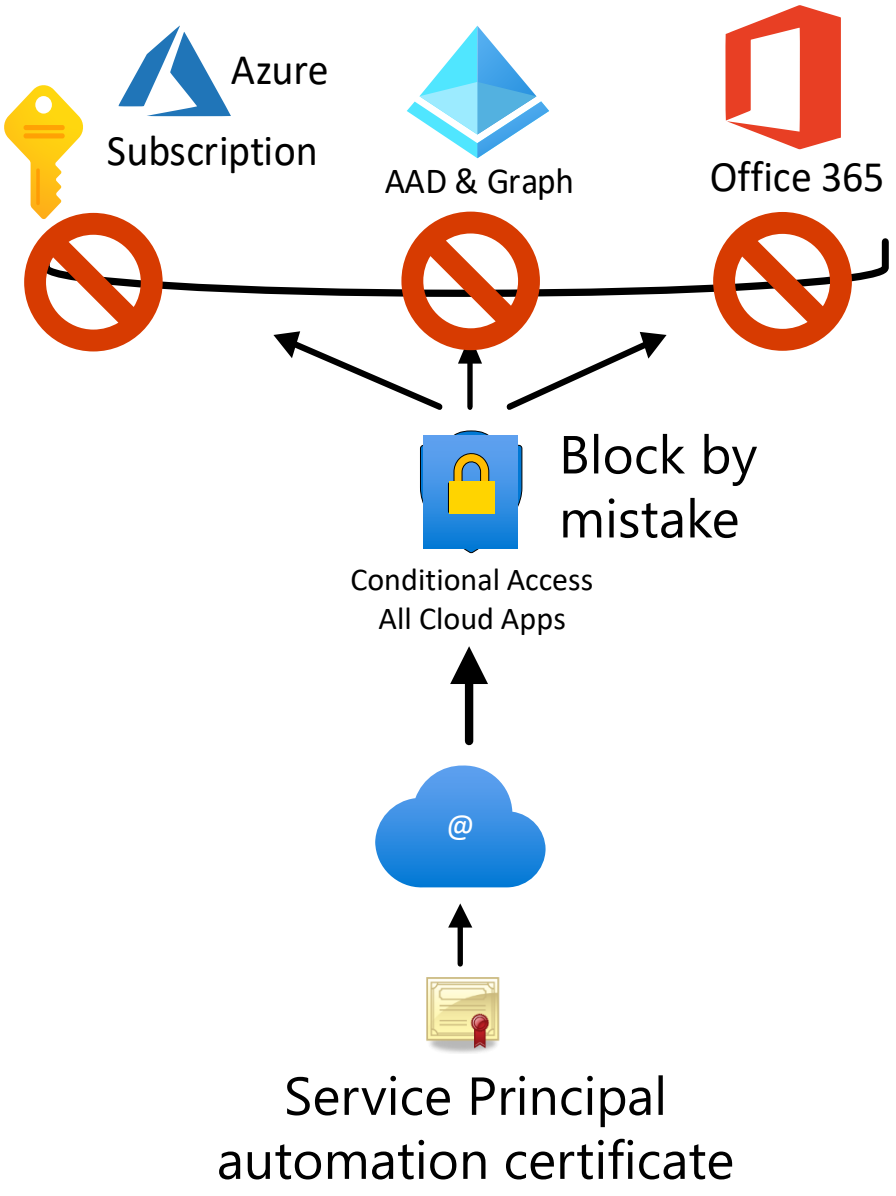
Example scenarios
Break glass Account

"Breakglass account" – Problem statement



Use Breakglass account

"Breakglass account" – Problem solution – use SP



Summary

- Troubleshooting can be time consuming
- Use persona-based approach to contain specific access scenarios
- CA setup for Zero Trust still blocks some scenarios, but is considered worthwhile
- Various workarounds exist to address scenarios blocked by the CA ZT framework
- The need for workarounds will be less over time as we address these in the product

Ask to you, - let us know if you see scenarios not working with CA configured for Zero Trust. Use you local MS Account team, Microsoft GTP/CXE team or PM to clajes@microsoft.com