

Conditional Access- authentication strength

The 425 Show edition

Inbar Cizer Kobrinsky
Senior Product Manager
Microsoft Entra ID



Topics

Introduction

Sign-in experience deep dive

Troubleshooting

Common policies



Entra ID Authentication methods

Bad:

Password

123456

qwerty

password

iloveyou

Password1

Good:

Password and...



SMS



Voice

Better:

Password and...



Microsoft
Authenticator



Software
Tokens OTP



Hardware Tokens OTP

Best:

Passwordless and Phishing-resistant



Windows Hello *



Certificate-based
authentication*



FIDO2 security key *



Microsoft
Authenticator

* Phishing-resistant MFA

Auth Strength 101

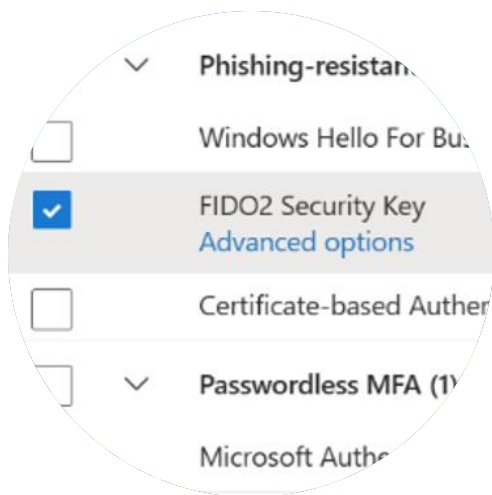




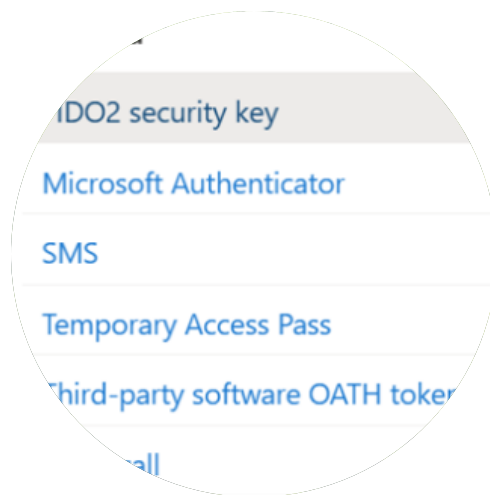
Sign-in experience deep dive



What do we check during sign-in?



Authentication
Strength
requirements



Authentication
methods policy
(New and legacy)



Registered methods



Previously used
methods

Sign-in results



Allow Access



Authentication
prompt

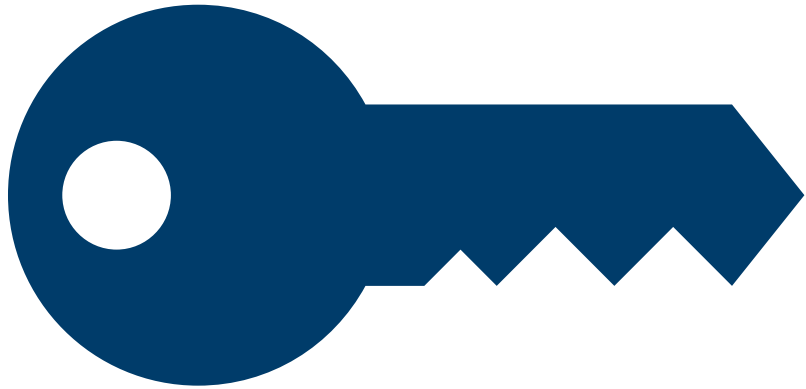


Registration



Block access

Authentication prompt



- Conditional Access policy elevation post primary authentication
- Methods availability
 - 1st and 2nd factor
 - External users
- Federated users

Registration

- My Security Info wizard mode
- Need to meet registration requirements (MFA, auth strength)
- Passwordless and phishing-resistant methods registration
- Other registration policies (SSPR, Identity Protection)

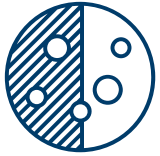


Block access



- User is not allowed to use any of the required methods.
- User has used the “wrong” 1st factor.
- User has not registered a passwordless method.
- User has used FIDO2 key that doesn't meet the required AA GUID.

A few more things to keep in mind



Multiple Conditional Access policies

- CA policies are evaluated during sign-in
- Multiple Auth Strength policies
 - Any resource
 - Security info



External Users

- Auth Strength + Cross-tenant Access Settings

Troubleshooting



Sign-in logs – Authentication Details

Activity Details: Sign-ins

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

...

Authentication Policies Applied

Conditional Access

Authentication Strength(s)

Session Lifetime Policies Applied

Remember multifactor authentication

Date	Authentication met...	Authentication meth...	Succeeded	Result detail	Requirement
9/1/2023, 1:49:48 PM	Previously satisfied		true	First factor re...	Phishing-resistant MFA, ...
9/1/2023, 1:49:48 PM	FIDO2 security key	Andres' key - f8a011f3-...	true		Phishing-resistant MFA, ...
9/1/2023, 1:49:48 PM	Other		true	MFA require...	Phishing-resistant MFA, ...

Phishing-resistant MFA, Multifactor authentication

Sign-in logs – Conditional Access

Home > Inbarck Labs | Users > Users > Andres User

Andres User | Sign-in logs

User

Search

«

Download

Export Data Settings

Troubleshoot

Refresh

Columns

Got feedback?

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : Last 24 hours

Show dates as : Local

User contains d658b96e-e477-4f6b-851d-5f190a6b5720

User sign-ins (interactive)

User sign-ins (non-interactive)

Date	Request ID	User	Application	Status
9/1/2023, 1:51:25 PM	062fcc55-dbd9-4da7-b...	Andres User	OfficeHome	Interrupted
9/1/2023, 1:50:08 PM	f3d1c11f-845f-4bd8-81f...	Andres User	Microsoft Account Cont...	Success
9/1/2023, 1:50:08 PM	7d7586d5-a456-4dbf-9...	Andres User	Office365 Shell WCSS-C...	Success
9/1/2023, 1:50:07 PM	9ce47809-fd5d-40a1-8d...	Andres User	Office365 Shell WCSS-C...	Success
9/1/2023, 1:50:07 PM	0c3238e5-c9a0-4149-b...	Andres User	Office365 Shell WCSS-C...	Success
9/1/2023, 1:50:05 PM	65c91694-97d8-4554-9...	Andres User	OfficeHome	Success
9/1/2023, 1:50:05 PM	4f582039-e7f4-48d1-a3...	Andres User	OfficeHome	Success
9/1/2023, 1:49:49 PM	1f0e238d-b0e0-4ea3-8c...	Andres User	Graph Explorer	Success
9/1/2023, 1:49:48 PM	4f638fe5-d2ce-4707-90...	Andres User	Graph Explorer	Success
9/1/2023, 1:49:11 PM	e15fd83a-cba6-4466-a5...	Andres User	OfficeHome	Success
9/1/2023, 1:49:09 PM	95ed7833-212c-4961-9...	Andres User	OfficeHome	Interrupted
9/1/2023, 1:48:57 PM	c447e09a-63af-43e2-a3...	Andres User	OfficeHome	Interrupted
9/1/2023, 1:48:07 PM	e7add511-7cae-417c-b...	Andres User	My Apps	Success
9/1/2023, 1:48:07 PM	527c5a25-613e-4428-a...	Andres User	Office365 Shell WCSS-S...	Success
9/1/2023, 1:48:07 PM	1e9ce46b-66fa-4f9c-9bf...	Andres User	Microsoft Account Cont...	Success
9/1/2023, 1:48:07 PM	d5cd9950-3659-4ba8-a...	Andres User	Office365 Shell WCSS-C...	Success
9/1/2023, 1:48:07 PM	f17b2b39-2d00-4048-af...	Andres User	Office365 Shell WCSS-C...	Success

Conditional Access Policy details

↑ Previous

↓ Next

Result: Failure

Assignments

User

Andres User

Matched

Application

OfficeHome

Matched

Conditions

Sign-in risk

None

Not configured

Device platform

Windows10

Not configured

Location

Kirkland, US
50.35.68.15

Not configured

Client app

Browser

Not configured

Device

Unknown

Not configured

User risk

Not configured

Access controls

Grant Controls

Not satisfied

Require Authentication strength - Multifactor authentication: The user could satisfy this authentication strength by completing one or more MFA challenges.

What-if

Microsoft Azure

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

admin1@inbarcklab.on...
INBARCK LABS (INBARCKLAB.ON...)

Home > Inbarck Labs > Security | Conditional Access > Conditional Access | Policies >

What If

Policies

Info | Got feedback?

Select device state...

Sign-in risk ⓘ
Select sign-in risk...

User risk ⓘ
Select user risk...

Service principal risk ⓘ
Select service principal risk...

Filter for devices ⓘ

Property	Value
	<Pick a property and operator fir...>

What If

Reset

Evaluation result

⚠ Classic policies are not evaluated by this tool.

Policies that will apply

Policies that will not apply

Search

Policy Name ↑↓	Grant controls ↑↓
Block all legacy authentication	Block access
Block all legacy authentication	Block access
Block all legacy sign-ins that don't support MFA	Block access
MSGraph - Phishing resistant	Authentication strength - Phishing-resistant MFA

Phishing-resistant MFA

● User can satisfy authentication strength requirements

Usable authentication combinat...	Reason
FIDO2	Allowed

Unusable authentication combi...	Reason
Windows Hello for business	Not registered by the user
x509 Certificate MultiFactor	Not allowed by admin policy

Conditional Access Monitoring

Home > Inbarck Labs | Security > Security | Conditional Access >

Conditional Access | Overview ...

Azure Active Directory

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication context

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

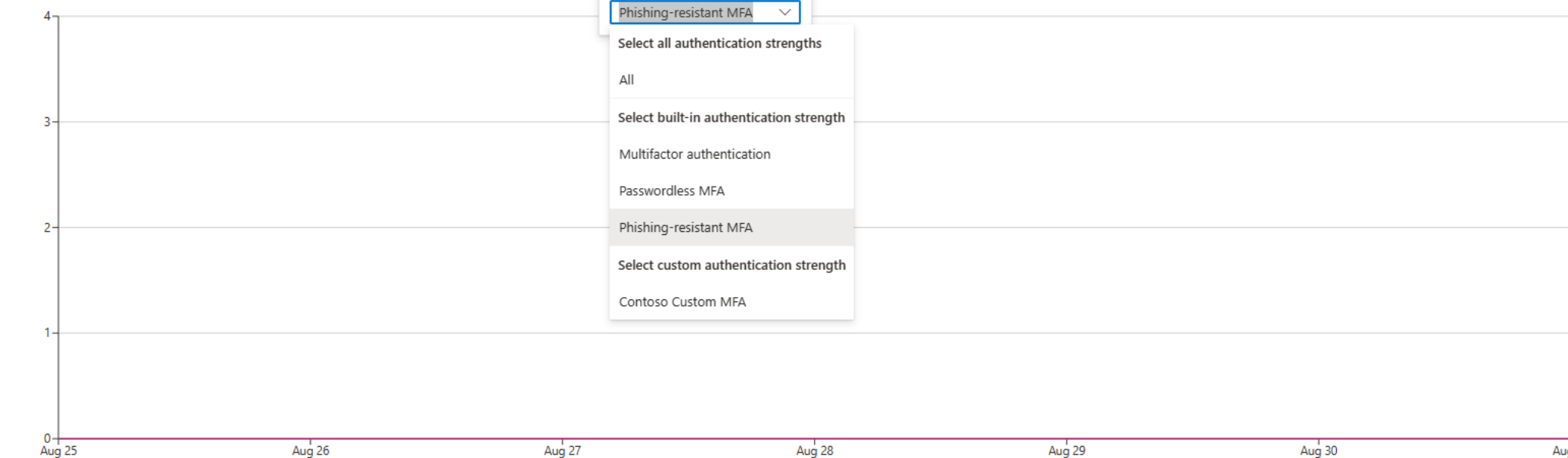
+ Create new policy + Create new policy from templates Refresh Got feedback?

Getting started Overview Coverage **Monitoring (Preview)** Tutorials

Sign-ins by Conditional Access result

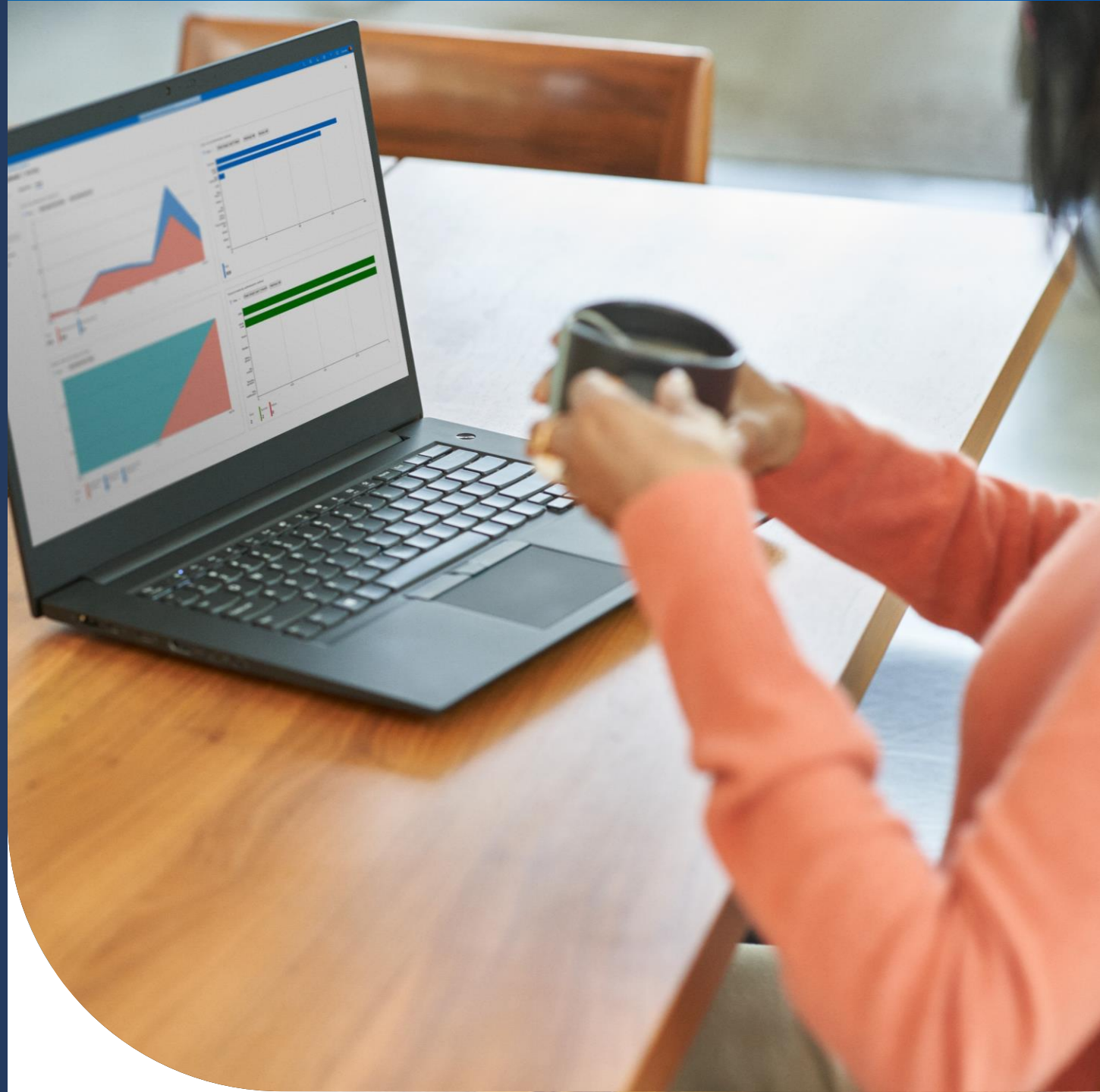
Date range: Last 7 days Show dates as: Local Policy evaluated: All enabled policies Authentication strength: Phishing-resistant MFA Auth requirement: All Client app: All Device state: All Device platform: All Sign-in risk: All User type: All

Reset filters



Total sign-ins

Common policies



Authentication strength role in your access strategy

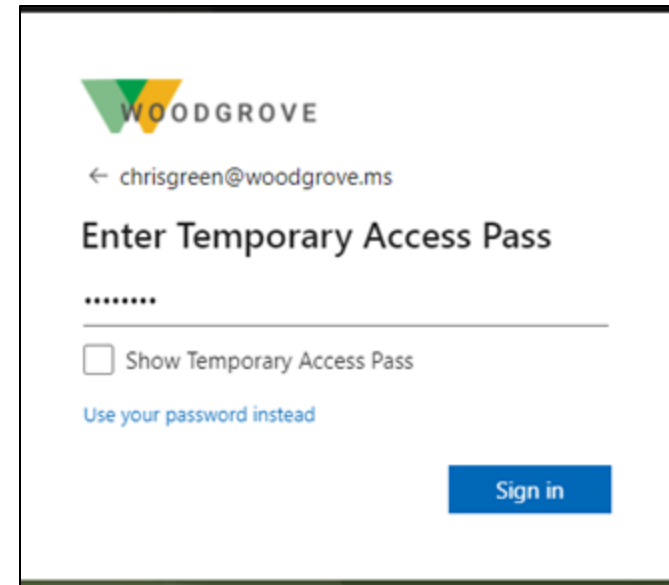
Conditions / Controls	Low	Medium	High
App filter	Sensitivity = Low	Sensitivity = Medium	Sensitivity = High
Authentication strength	MFA	Non-telecom MFA	Phishing-resistant
Device	N/A	Require device to be marked as compliant	Require device to be marked as compliant
Location	Skip MFA for trusted locations	N/A	N/A

Cross apps policies

- * Block high risk sign-ins and users
- * Restrict Temporary Access Pass for bootstrap and recovery
- * Phishing-resistant methods for admins (PIM) and vendors

Temporary Access pass for bootstrap and recovery

- Custom auth strength for bootstrap and recovery
 - Includes Temporary Access Pass and Phishing-resistant MFA
- Conditional Access policies:
 - Target all cloud apps with phishing-resistant MFA (built-in)
 - Target "Register security information" with the custom authentication strength policy.



The screenshot shows a login interface for 'WOODGROVE'. At the top is the company logo. Below it, the email address 'chrisgreen@woodgrove.ms' is displayed with a back arrow. The main heading is 'Enter Temporary Access Pass'. There is a password input field with seven dots. Below the field is a checkbox labeled 'Show Temporary Access Pass'. A link 'Use your password instead' is positioned below the checkbox. A blue 'Sign in' button is located in the bottom right corner.

WOODGROVE

← chrisgreen@woodgrove.ms

Enter Temporary Access Pass

.....

☐ Show Temporary Access Pass

[Use your password instead](#)

Sign in

Resources

<https://aka.ms/authstrengthdocs>

Authentication strength docs

<https://aka.ms/authstrengthAPIdocs>

Authentication Strength APIs

<https://aka.ms/PhishResistantExplained>

How phishing-resistant works?