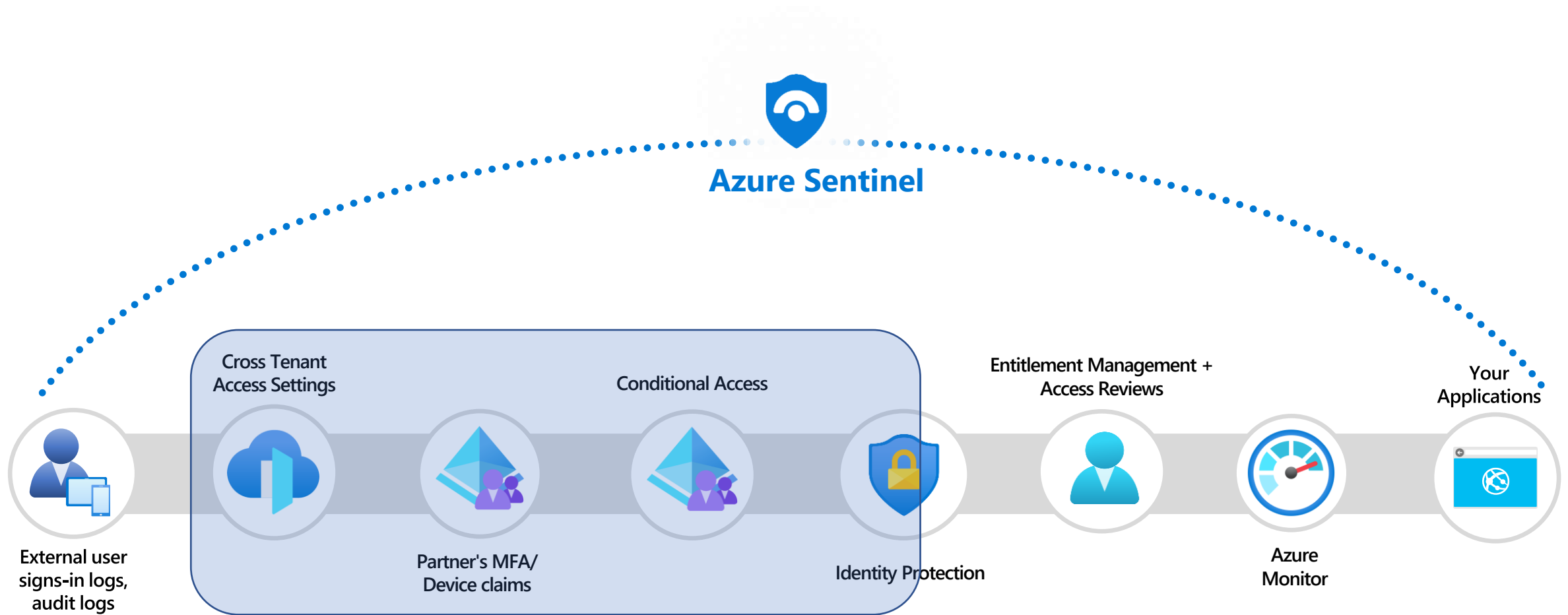


Optimizing external access controls for B2B collaboration

Claus Jespersen, Principal Security Consultant
Security Service Line, EMEA



Collaborate with Zero Trust





Focus for this session



Agenda

- Conditional Access Guidance update
- Conditional Access policy improvements for guest users
 - Base policy
 - Identity Protection
 - Data Protection
 - App Protection
 - Attack Surface Reduction
 - Compliance (no change)

Conditional Access for Zero Trust Guidance update

**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

- Introduction..... 3
- Changelog..... 5
- CA related components..... 5
- General Field Guidance..... 7
- Governance/Roll-out..... 7
- Personas..... 8

Suggested Policies..... 20

- Global Policies (CA001-CA099)..... 20
- Global Base Protection policies..... 20
- Global Attack Surface Reduction policies..... 21
- Admins Policies (CA100-CA199)..... 21
- Admins Base Protection policies..... 22

LinkedIn

Conditional Access for Zero Trust

Article • 10/10/2022 • 2 minutes to read • 4 contributors

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

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.

Azure Architecture Center <https://aka.ms/ca-zt>

microsoft / **ConditionalAccessforZeroTrustResources** Public

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)

main 1 branch 0 tags

[Go to file](#) [Add file](#)

clajes two corrections for workloadidentities based on input from Etan Basse... bc69468 on 25 May

ConditionalAccessSamplePolicies	two corrections for workloadidentities based on input from Etan Basse...	5 n
Presentations	Add files via upload	6 n
Workbooks	Add files via upload	5 n
.gitignore	Initial commit	9 n
CODE_OF_CONDUCT.md	CODE_OF_CONDUCT.md committed	9 n
LICENSE	LICENSE committed	9 n
README.md	Update README.md	5 n
SECURITY.md	SECURITY.md committed	9 n
SUPPORT.md	SUPPORT.md committed	9 n

This repository holds some Conditional Access resources that complement the Azure Architecture design note "Conditional Access Guidance for Zero Trust". See more here for a description on CA configured for Zero Trust

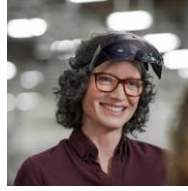
<https://docs.microsoft.com/en-us/azure/architecture/guide/security/conditional-access-zero-trust?msclkid=d1768a34ceda11ec9b6c8f244f8d05bd> and

GitHub

Suggested Personas for Conditional Access



Internals



Guests



Externals



GuestAdmins



Admins



ServiceAccounts



Developers



WorkloadIdentities

CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
Base Protection	The base protection is the base line grant controls that the users must meet. Example - Require MFA
Identity Protection	CA policies that relate to identity. Examples <ul style="list-style-type: none"> • Block legacy authentication • Require extra MFA for high sign-in risk • Session policy with Sign-in frequency
Data Protection	Indicates delta policies that protect data as an extra layer. Examples - CA session policy with App Enforced Restrictions - CA session policy with App Access App Control (MDCA/MCAS)
App Protection	Protection related to a given app. Example - Office 365
Attack Surface Reduction	This type of policy is to mitigate against various attacks. Example - Block unknown platform
Compliance	A compliance policy. Example - TOU: "Terms Of Use"

CA Number

Persona
Guests

Policy Type

App

Platform

Grant

Description

Guest Persona Limitation

- “All or nothing”

Conditional Access policy

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

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

[Specific users included](#)

✖ "Select users and groups" must be configured

Cloud apps or actions ⓘ

[No cloud apps, actions, or authentication contexts selected](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[0 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](#)

What does this policy apply to?

Users and groups

Include

Exclude

☐ None

☐ All users

☒ Select users and groups

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☐ Users and groups

CA Number

Persona
Guests

Policy Type

App

Platform

Grant

Description

Improvement

Assigning
Conditional
Access policies
to external user
types (preview)

[Home](#) > [Contoso | Security](#) > [Security | Conditional Access](#) > [Conditional Access | Policies](#) >

New ...

Conditional Access policy

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

[Specific users included](#)

✗ "Select users and groups" must be configured

Cloud apps or actions ⓘ

[No cloud apps, actions, or authentication contexts selected](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

What does this policy apply to?

Users and groups

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☒ Guest or external users ⓘ

[Specify external Azure AD organizations \(preview\)](#)

☐ All

☒ Select

[Select](#)

0 selected

☐ B2B collaboration guest users (preview)

☐ B2B collaboration member users (preview)

☐ B2B direct connect users (preview)

☐ Local guest users (preview)

☐ Service provider users (preview)

☐ Other external users (preview)

Base Protection Policy Limitations



MFA is the only viable grant control for guest users



Multiple MFA prompts



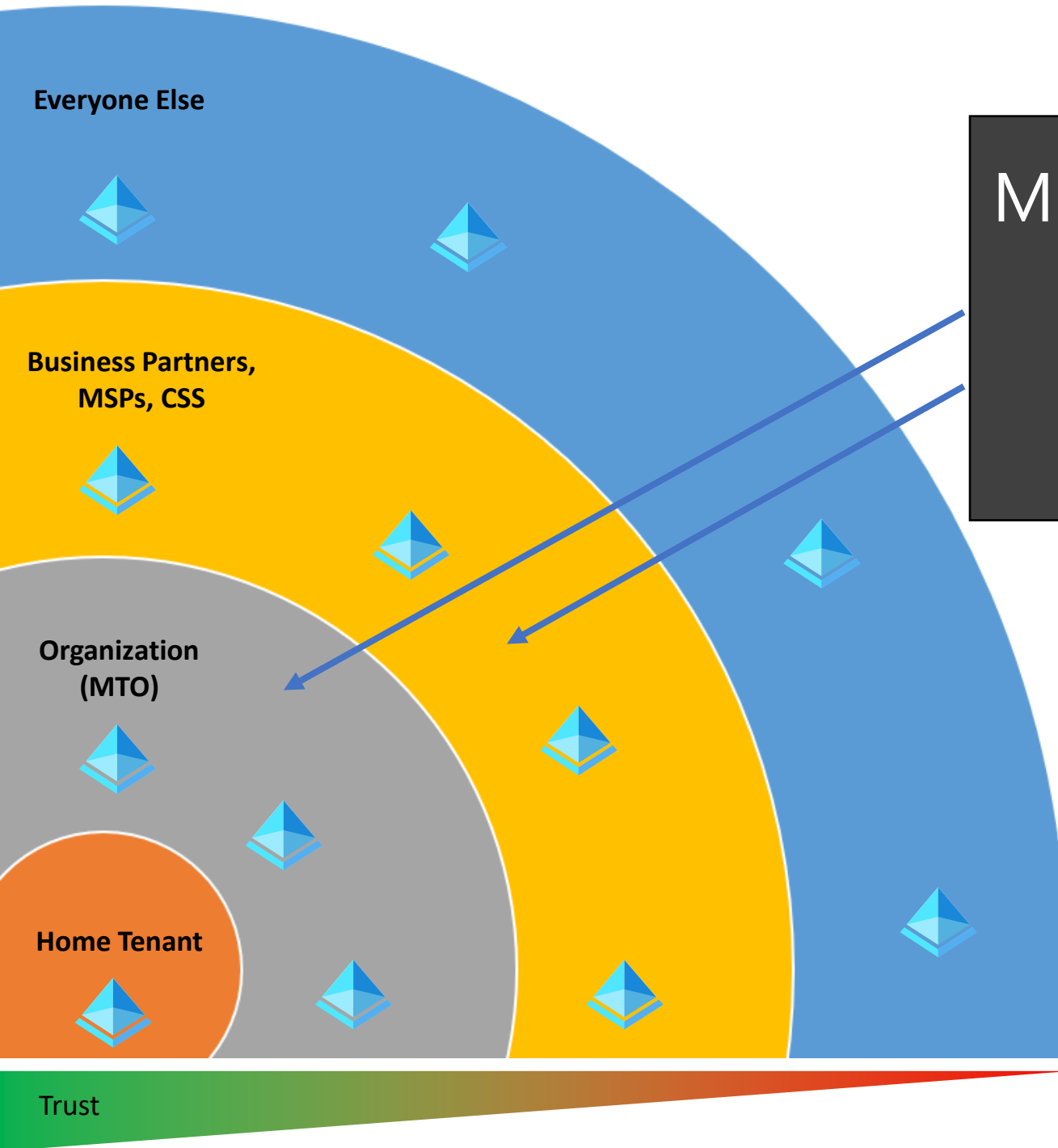
Authentication method can't be enforced



Limited support for blocking access to all apps but Office 365



Limited support for excluding apps from base policy that are not targetable by CA



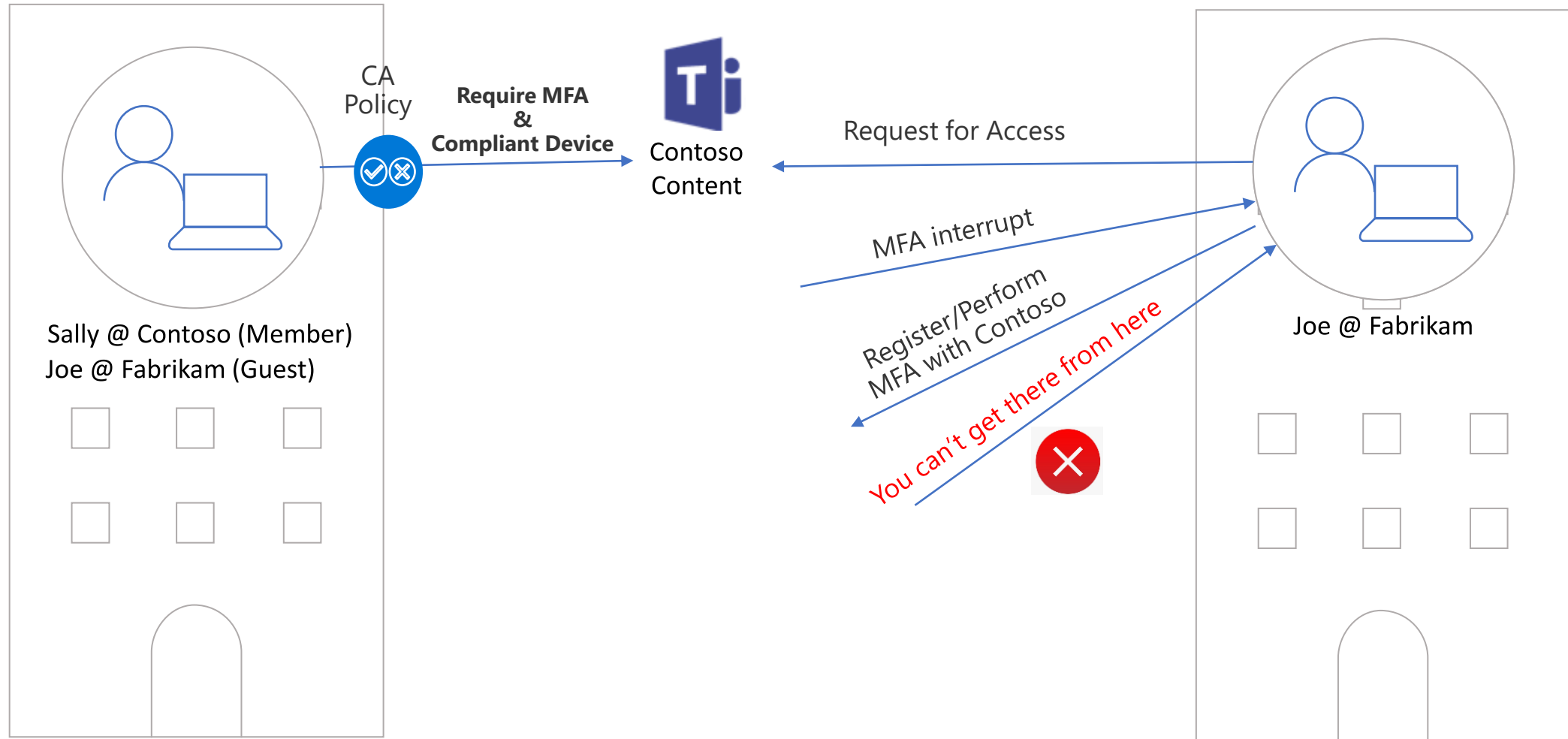
Multi Tenant Orgs/XTAP

- *Inbound coarse grained access controls*
- *Outbound coarse grained access controls*
- *Next version of tenant restrictions*

Inbound access w/o Cross Tenant Access setting

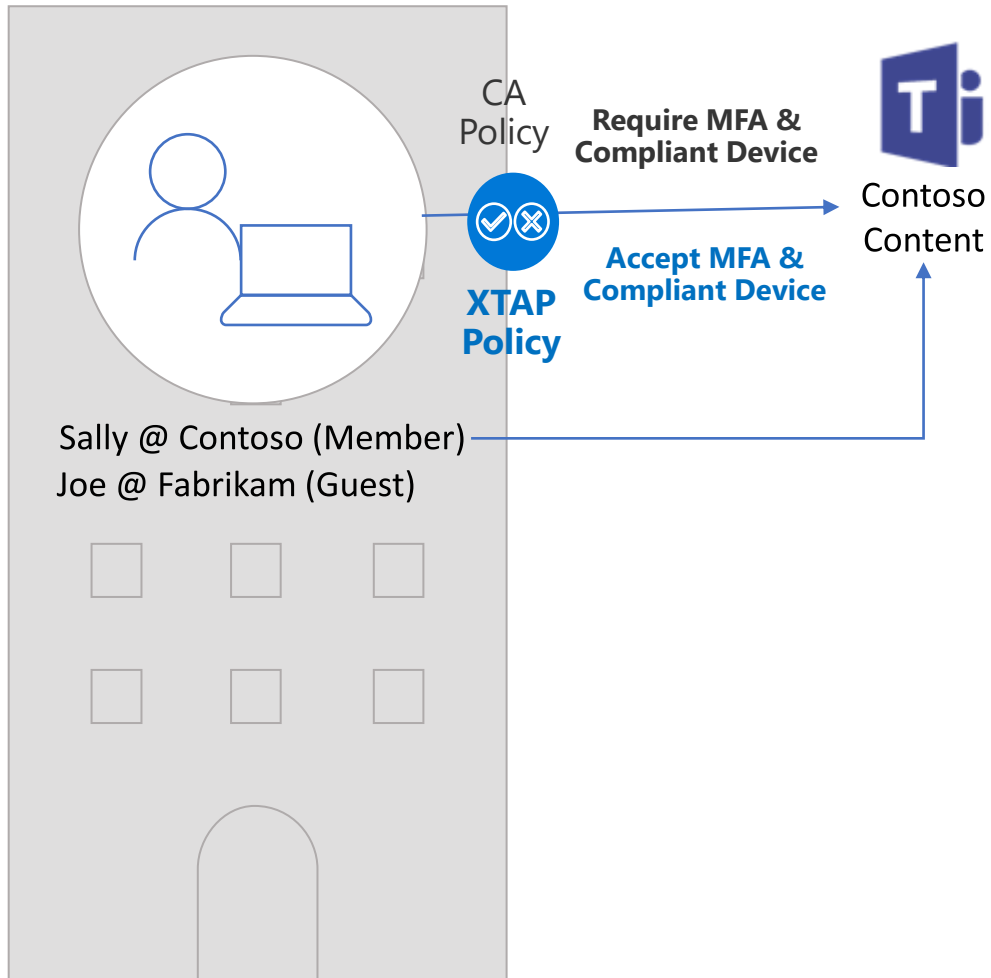
Contoso (Resource Tenant)

Fabrikam (Home Tenant)

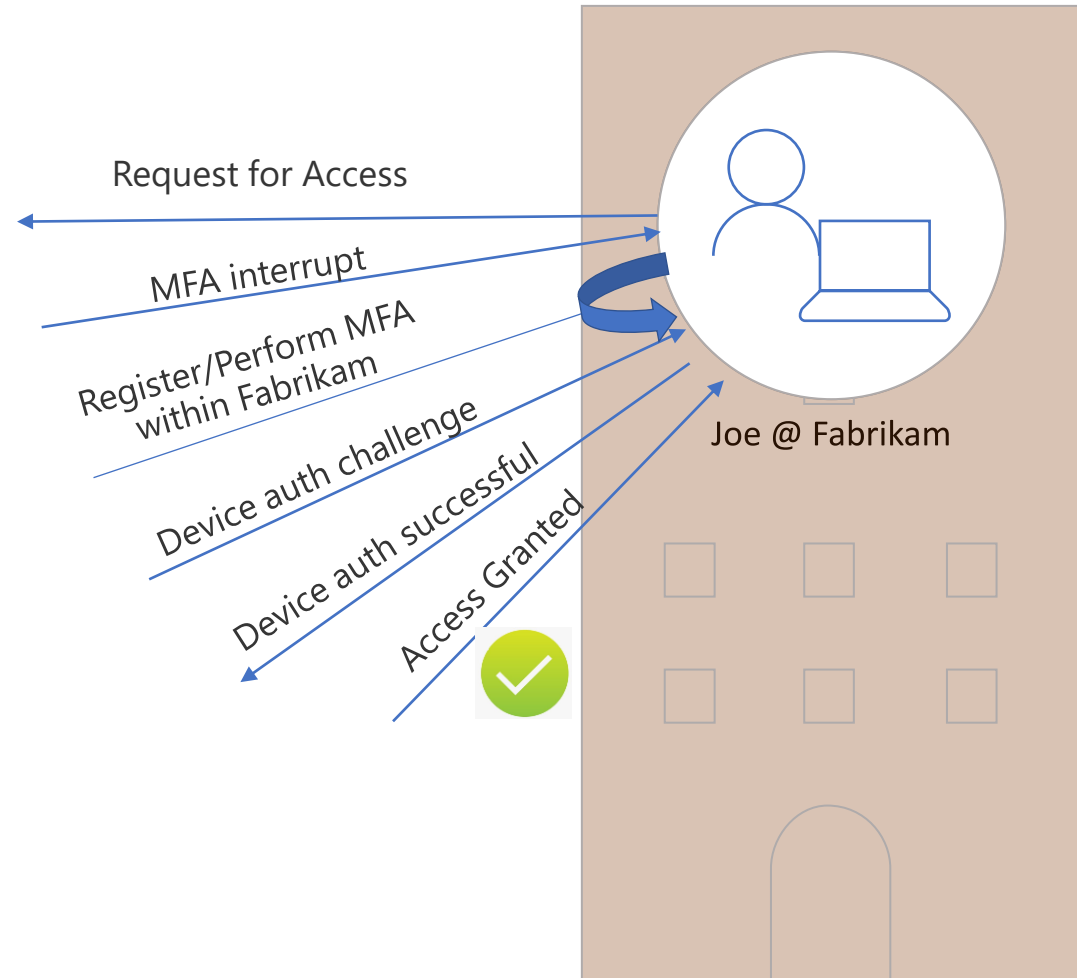


Inbound access w/ Cross Tenant Access setting

Contoso (Resource Tenant)



Fabrikam (Home Tenant)



Base Protection Improvements


[Home](#) > [External Identities](#) | [Cross-tenant access settings](#) >

Inbound access settings - Default settings

[B2B collaboration](#) [B2B direct connect](#) [Trust settings](#)

Configure whether your Conditional Access policies will accept claims from other

You'll first need to configure Conditional Access for guest users on all cloud apps

[Learn more](#) 

- ☐ Trust multifactor authentication from Azure AD tenants
- ☐ Trust compliant devices
- ☐ Trust hybrid Azure AD joined devices

New authentication strength ×

Custom

Configure Review

Name *

The authentication strength name cannot be empty

Description

 Search authentication combinations

▼ Phishing-resistant multifactor authentication (3)

☐ Windows Hello For Business

☐ FIDO2 Security Key
[Advanced options](#)

☐ Certificate Based Authentication (Multi-Factor)

▼ Passwordless multifactor authentication (1)

☐ Microsoft Authenticator (Phone Sign-in)

▼ Multifactor authentication (13)

☐ Temporary Access Pass (One-time use)

☐ Temporary Access Pass (Multi-use)

☐ Password + Microsoft Authenticator (Push Notification)

☐ Password + Software OATH token

☐ Password + Hardware OATH token

Authentication Strengths for Guests

Authentication method	Home tenant	Resource tenant
SMS as second factor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Voice call	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Authenticator push notification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Authenticator phone sign-in	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (Now supports multiple accounts)
OATH software token	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OATH hardware token	<input checked="" type="checkbox"/>	
FIDO2 security key	<input checked="" type="checkbox"/>	
Windows Hello for Business	<input checked="" type="checkbox"/>	
X509 Certificates	<input checked="" type="checkbox"/>	
Temporary Access Pass (TAP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ?? (verify)

Security Attributes for CA

Attribute based Cloud App Targeting
Filter for applications

- **Step 1 – Define Attribute**
- **Step 2 – Assign Attribute**
- **Step 3 – Configure CA to exclude apps with given security attribute**

Dynamic and Explicit cloud apps

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 *

Dynamic and Explicit cloud apps

Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

Dynamic query configured with 3 apps included and 2 apps excluded

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Dynamic targeting

Dynamic query configured

Base Protection Policy updates

CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
Base Protection	<p>The base protection is the base line grant controls that the users must meet. You can now use a mix of these grant controls per guest type and/or per tenant</p> <ul style="list-style-type: none">- Require MFA- Require MFA and/or known/compliant device from home tenant (requires XTAP) (When using inbound XTAP policies, suggest assigning to all apps to avoid issues)- Require different authentication strengths (and auth method policy per groups of users)- Use Conditional Access Application filters based on security attributes assigned to apps- Use MDCA, if you want to block access to all apps but Office 365 with MFA registration

Identity Protection Policies - Limitations



Current guidance only addresses sign-in risk (as opposed to user and/or device risk)



MFA methods can't be enforced for guests (tenant wide MFA settings)



Fresh MFA for risky sign-ins may not be enforced



MFA can be performed from Jailbroken devices



CA risk policies for guests may be intrusive for guests not knowing about risks in own tenant due to lack of AADP2 license

Identity Protection Policy Improvements

MFA registration using GPS as named location

Select what this policy applies to

User actions

Select the action this policy will apply to

☒ Register security information

☐ Register or join devices

Update location (Countries)

Delete

i Only IPv4 addresses are mapped to countries/regions. IPv6 addresses are included in unknown countries/regions.

Name *

Countries Allowed based on GPS

Determine location by GPS coordinates

i When the location condition of a Conditional Access policy is configured, users will be prompted by the Authenticator app to share their GPS location. [Learn more](#)

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

User risk **i**

Not configured

Sign-in risk **i**

Not configured

Device platforms **i**

Not configured

Locations **i**

1 included

Client apps **i**

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

Configure **i**

Yes

No

Include

Exclude

☐ Any location

☐ All trusted locations

☒ Selected locations

Select

Countries Allowed based on GPS

Countries Allowed based on GPS



Identity Protection Policy Improvements

MFA/SSPR (combined registration methods) now through authentication policies

Home > Contoso | Security > Security | Authentication methods >

Authentication methods | Policies

Contoso - Azure AD Security

Search

Got feedback?

Manage

Policies

Password protection

Registration campaign

Authentication strengths (Preview)

Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

Use this policy to configure the authentication methods for users to authenticate and for password reset (some methods may not be supported).

If your tenant doesn't yet use [combined security information](#), you can use this policy to manage the migration from legacy policies to the new unified policy.

Manage migration

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.
[Learn more](#)

Method

Target

FIDO2 security key

All users

Microsoft Authenticator

All users

SMS (preview)

All users

Temporary Access Pass

All users

Third-party software OATH tokens (preview)

All users

Voice call (preview)

All users

Email OTP (preview)

All users

Manage migration

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.
[Learn more](#)

☐ Pre-migration:

Use policy for authentication only, respect legacy policies.

☐ Migration In Progress:

Use policy for authentication and SSPR, respect legacy policies.

☒ Migration Complete:

Use policy for authentication and SSPR, ignore legacy policies.

Save

Cancel

Authentication methods policy converge

Identity Protection Policy updates

CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
Identity Protection	<p>CA delta policies that relate to identity.</p> <ul style="list-style-type: none">▪ Block legacy authentication▪ Enforce sign-in frequency▪ Require fresh MFA for user and/or sign-in risk (requires sign-in frequency policy)▪ Require authentication strengths for user or sign-in risk (like password-less phone sign-in)▪ MFA registration can enforce GPS through authenticator app, check for jail-broken device

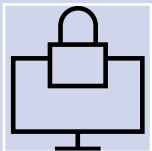
Data Protection Policy Limitations



No (easy) granular data protection policies for apps not targetable in CA



Read-only guest access to resources only supported by EXO, SPO and Teams (without using MDCA)



Lack of native CA support for sensitivity types and labels for guest access

Data Protection Policy updates

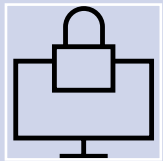
CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
Data Protection	<p>Indicates delta policies that protect data as an extra layer. Examples</p> <ul style="list-style-type: none">▪ CA session policy with App Enforced Restrictions (as before)▪ CA session policy with App Control (MDCA/MCAS) (as before)▪ Look for new feature “MAM policies for Edge” with relevant CA controls announced at Ignite 2022

App Protection Policy Limitations



Limited support targeting access to specific app(s)
(if not targetable by CA policy)



Authentication method can't be enforced for specific app

App Protection Policy updates

CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
App Protection	Protection related to a given app <ul style="list-style-type: none">- Require authentication strength for specific app targetable by CA or security attributes- Block access to specific app based on security attribute assigned to Enterprise Apps

Attack Surface Reduction Policy Limitations



Blocking non-supported platforms may unintentionally block guest users from various unmanaged clients

Attack Protection Policy updates

CA Number	Persona Guests	Policy Type	App	Platform	Grant	Description
-----------	-------------------	-------------	-----	----------	-------	-------------

Policy Type	Description
Attach Surface Reduction	<p>This type of policy is to mitigate against various attacks. Example</p> <ul style="list-style-type: none">Block unknown platforms, but only if XTAP is used to require known or compliant device from home tenant