



# Conditional Access Policy Documentation

Tenant ID

Tenant Name

Generated by

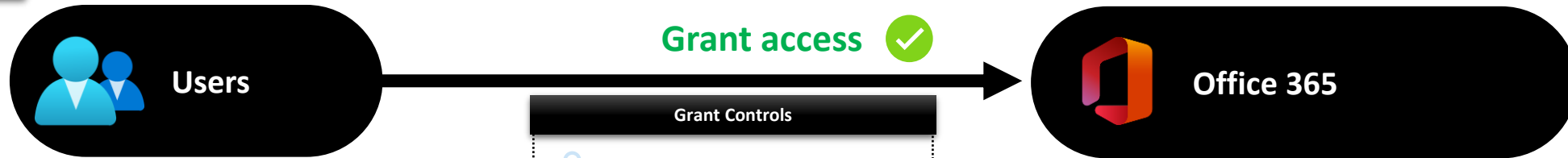
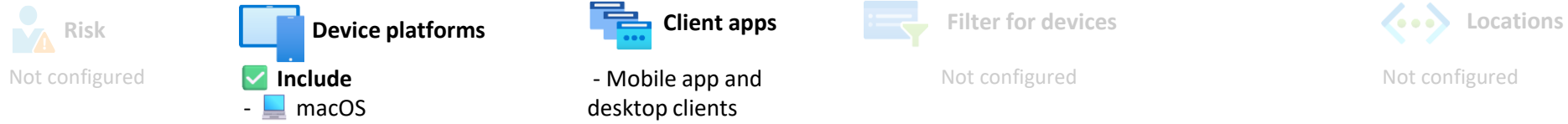
**Kenneth van Surksum**

Generated on

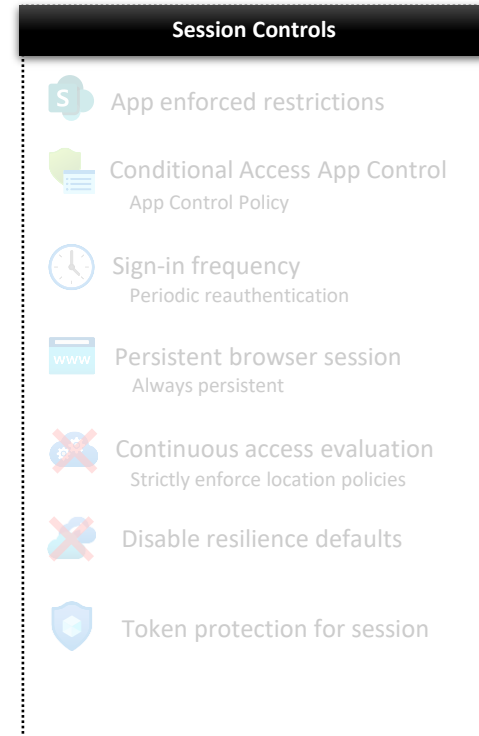
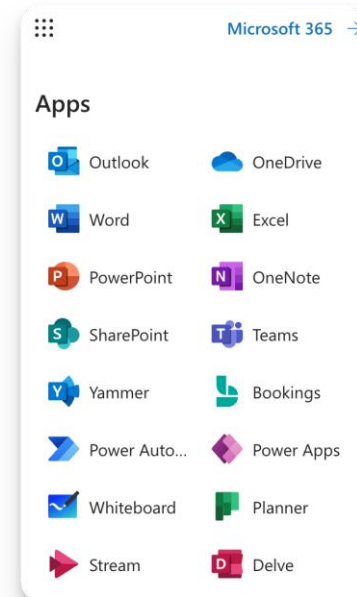
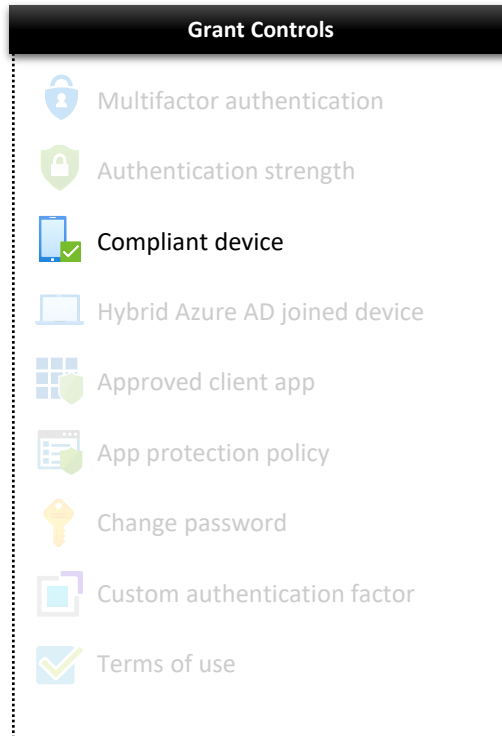
**18 Oct 2025**

# CAD001-O365: Grant macOS access for All users when Modern Auth Clients and Compliant-v1.1

Last modified: 2023-06-17



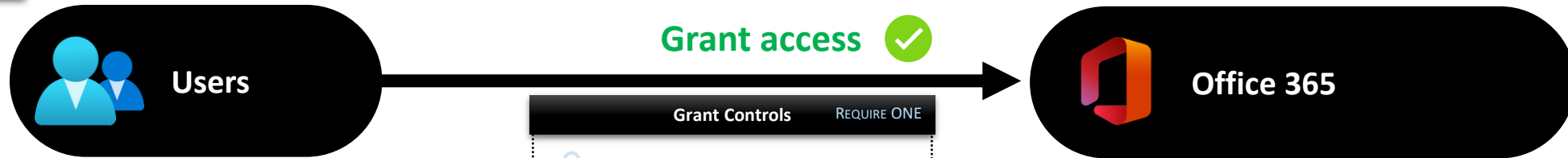
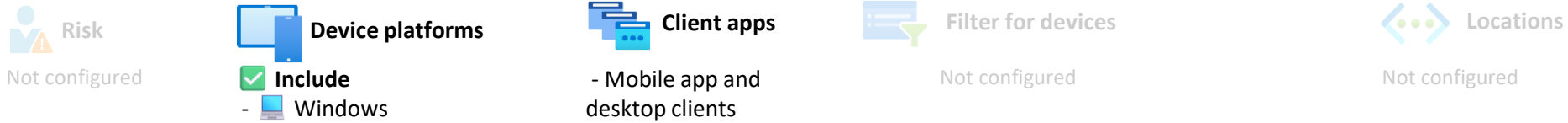
- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Guest or external users**  
**All external Azure AD organizations**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAD001\_Exclude (1)



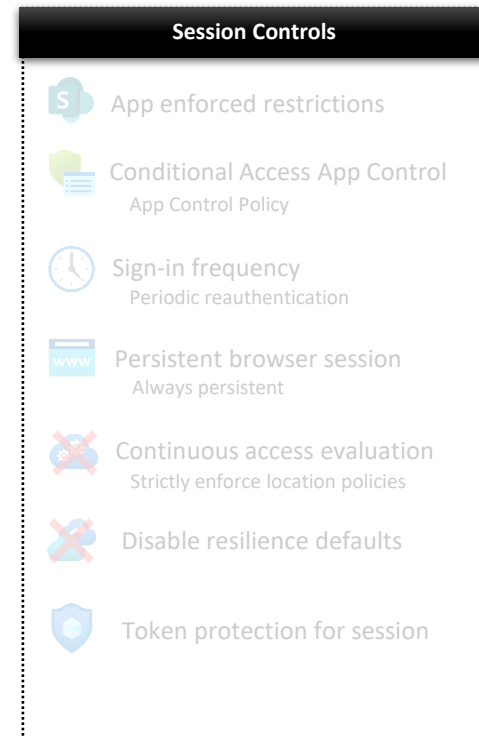
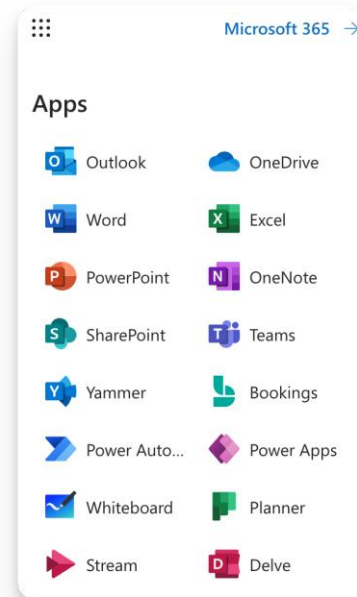
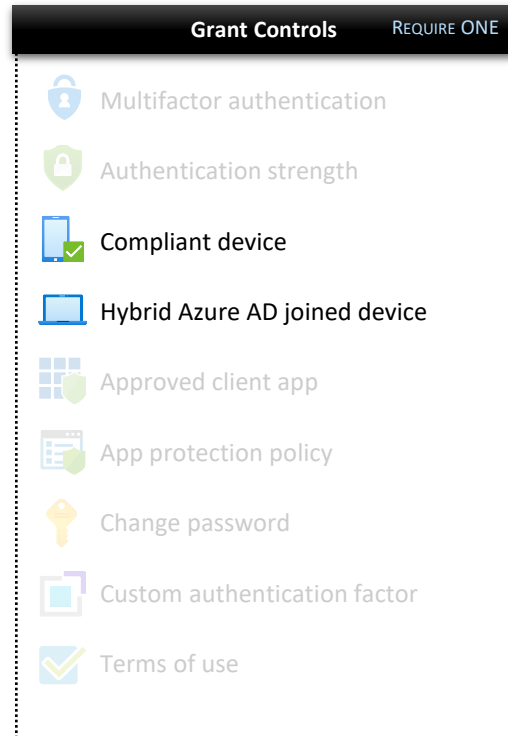


# CAD002-O365: Grant Windows access for All users when Modern Auth Clients and Compliant- v1.1

Last modified: 2022-12-29



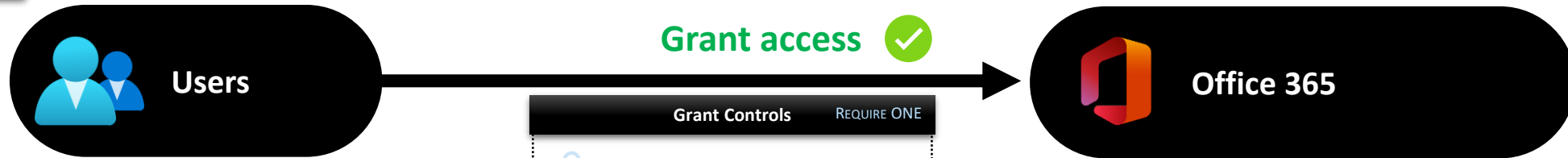
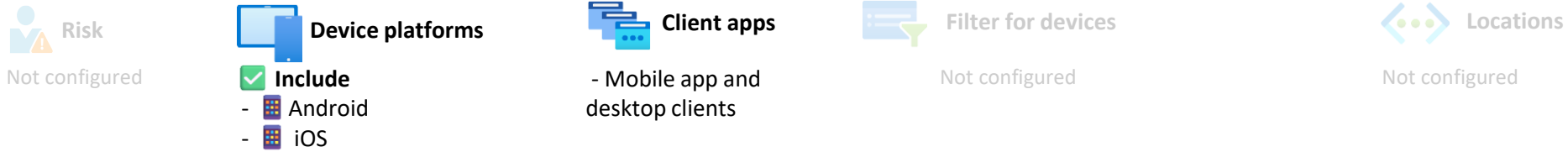
- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Guest or external users**  
**All external Azure AD organizations**  
**Groups**  
- AAD\_UA\_CAD002\_Exclude (3)  
- AAD\_UA\_ConAcc-Breakglass (6)



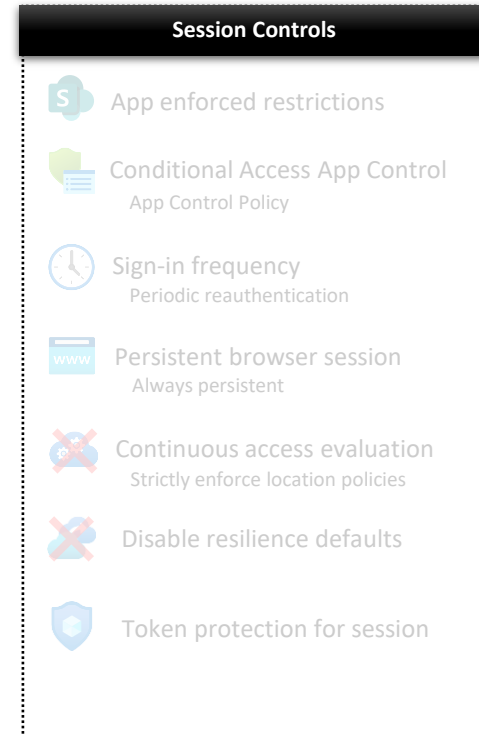
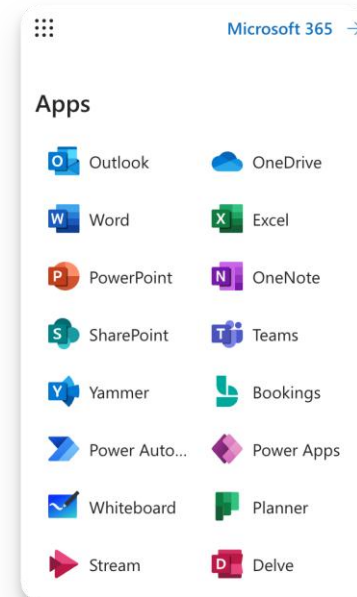
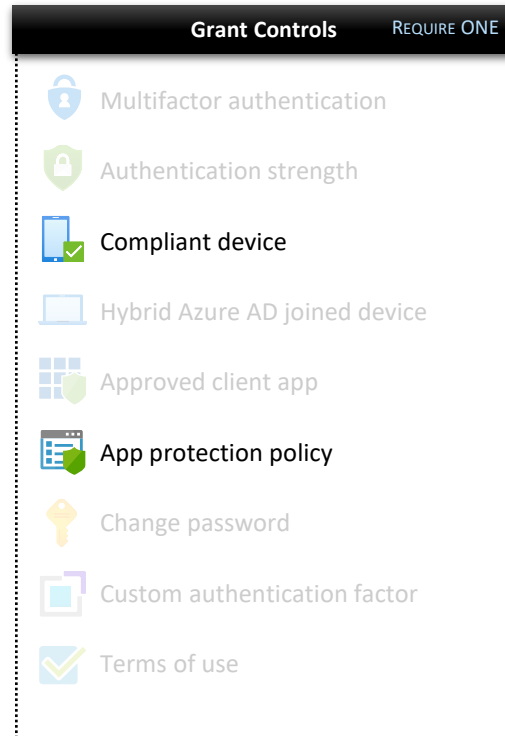


# CAD003-O365: Grant iOS and Android access for All users when Modern Auth Clients and AppProPol or Compliant-v1.3

Last modified: 2025-05-16

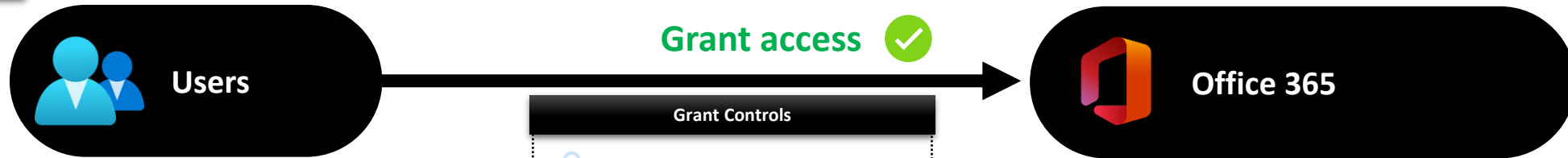


- ✓ **Include:**
  - Users**
    - All
- ✗ **Exclude:**
  - Guest or external users**
    - All external Azure AD organizations
  - Groups**
    - AAD\_UA\_ConAcc-Breakglass (6)
    - AAD\_UA\_CAD003\_Exclude (0)

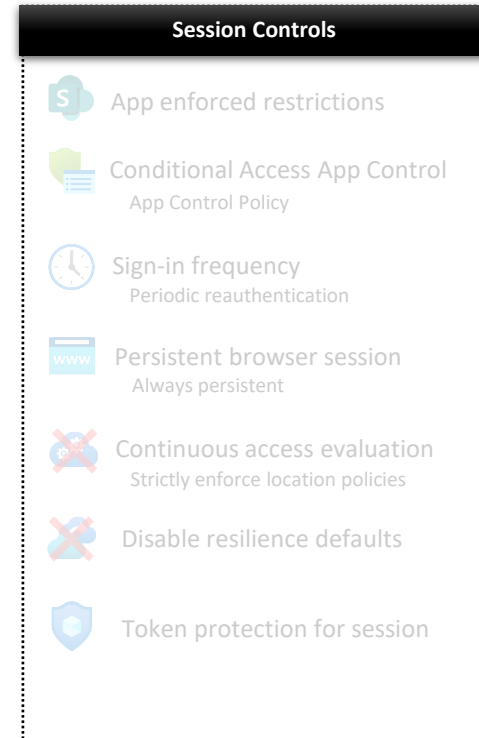
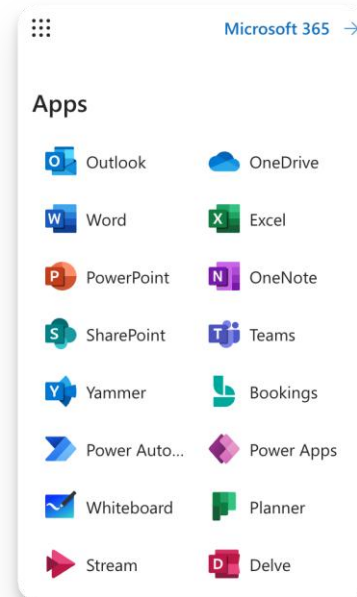
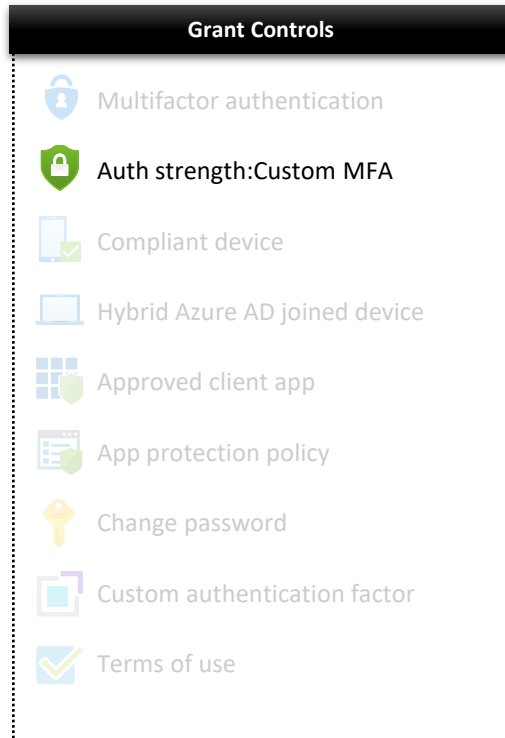


# CAD004-O365: Grant Require MFA for All users when Browser and Non-Compliant-v1.3

Last modified: 2025-01-23



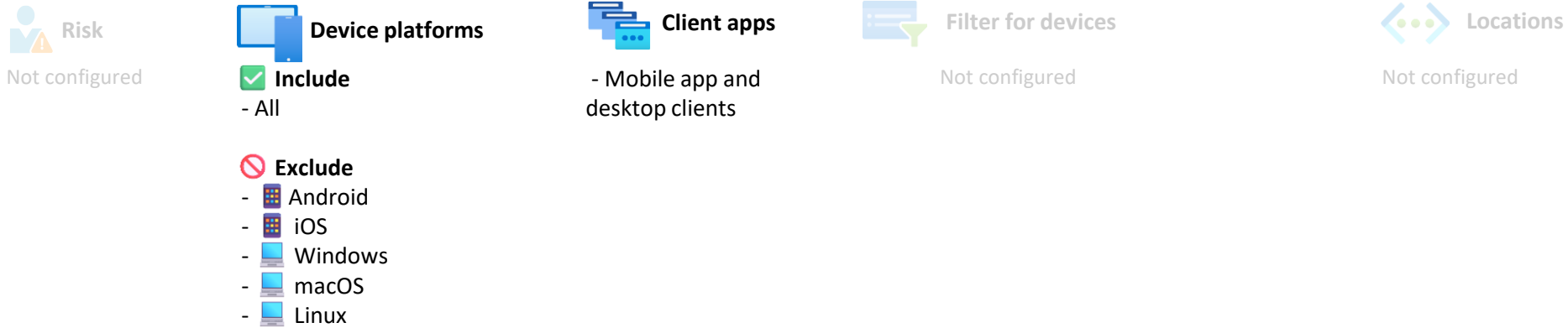
- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_CAD004\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)



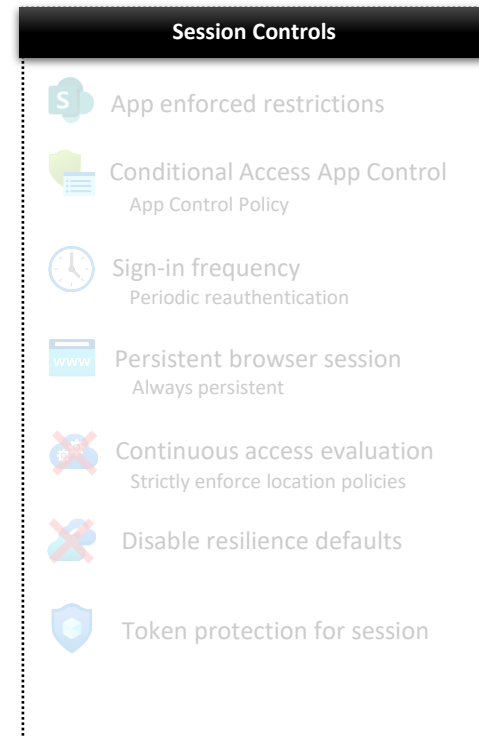
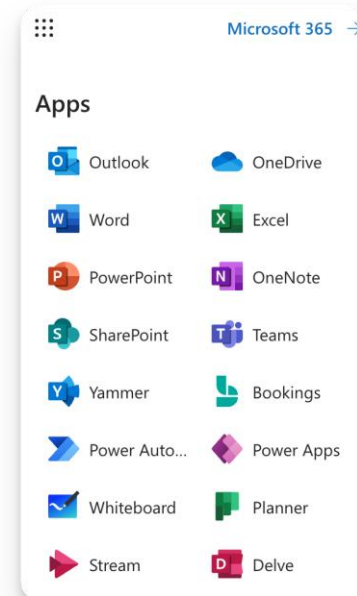
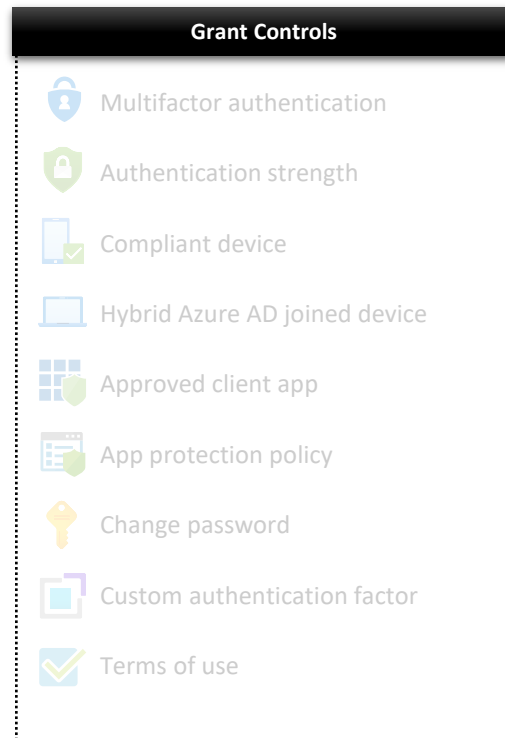


# CAD005-O365: Block access for unsupported device platforms for All users when Modern Auth Clients-v1.1

Last modified: 2023-08-01



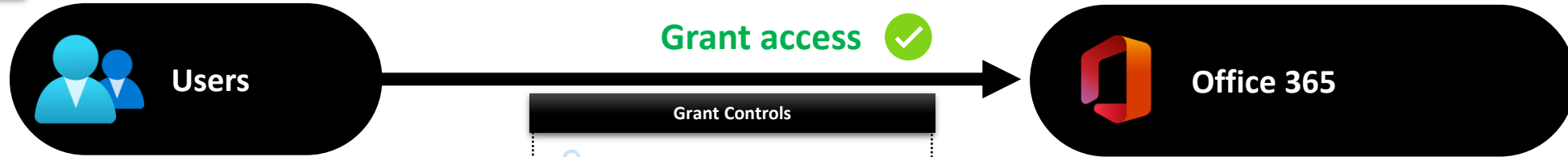
- ☒ **Include:**  
**Users**
  - All
- ☐ **Exclude:**  
**Groups**
  - AAD\_UA\_ConAcc-Breakglass (6)
  - AAD\_UA\_CAD005\_Exclude (1)





# CAD006-O365: Session block download on unmanaged device for All users when Browser and Modern App Clients and Non-Compliant-v1.5

Last modified: 2023-08-01



**Include:**

**Users**

- All



**Exclude:**

**Groups**

- AAD\_UA\_ConAcc-Breakglass (6)

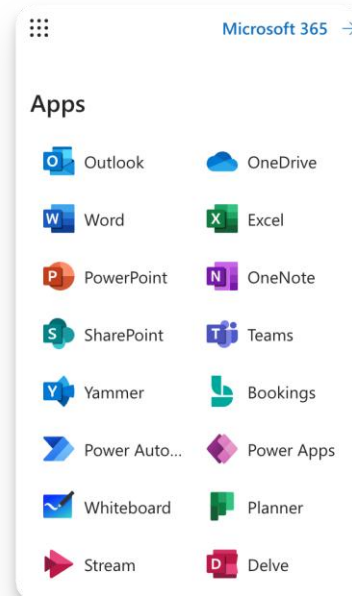
- AAD\_UA\_CAD006\_Exclude (0)

## Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use



Office 365



## Session Controls

- App enforced restrictions
- Conditional Access App Control  
App Control Policy
- Sign-in frequency  
Periodic reauthentication
- Persistent browser session  
Always persistent
- Continuous access evaluation  
Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAD007-O365: Session set Sign-in Frequency for Apps for All users when Modern Auth Clients and Non-Compliant-v1.2

Last modified: 2023-03-22



Risk

Not configured



Device platforms

✓ Include

- Android
- iOS



Client apps

- Mobile app and desktop clients



Filter for devices

Exclude when  
device.isCompliant -eq True -or  
device.trustType -eq "ServerAD"



Locations

Not configured



Users

✓ Include:

Users

- All

✗ Exclude:

Groups

- AAD\_UA\_CAD007\_Exclude (0)
- AAD\_UA\_ConAcc-Breakglass (6)

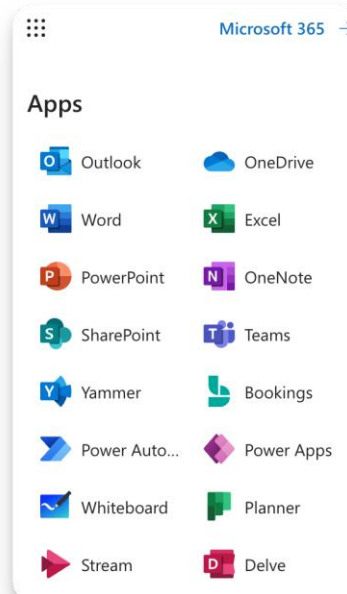
Grant access ✓



Office 365

Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use



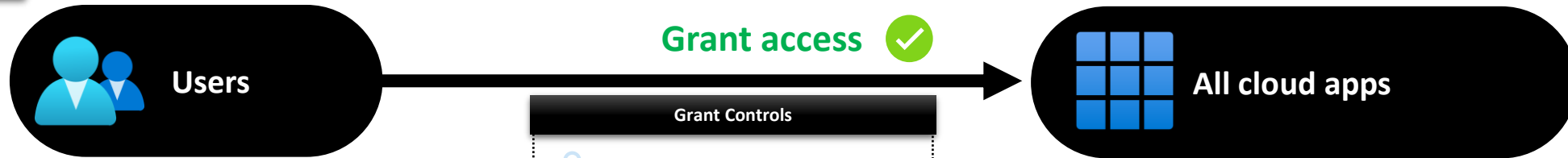
Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency 7 days
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session

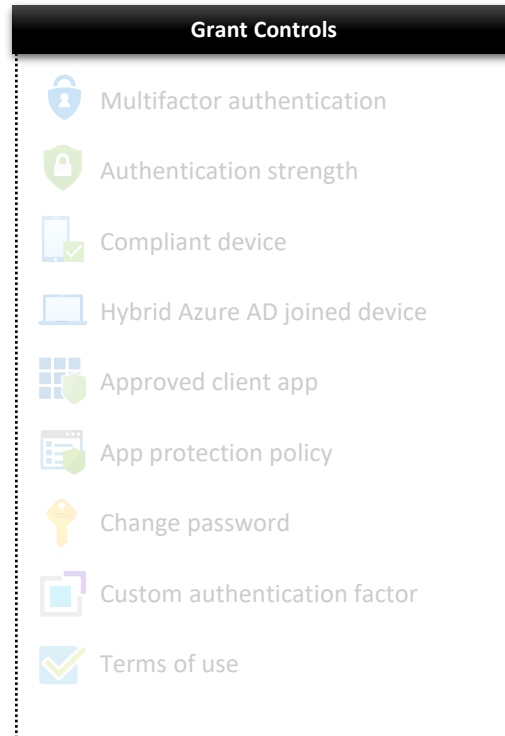


# CAD008-All: Session set Sign-in Frequency for All users when Browser and Non-Compliant-v1.1

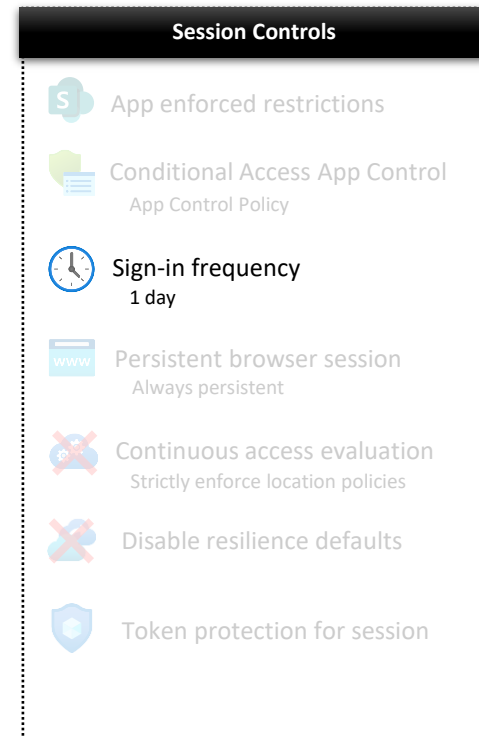
Last modified: 2022-12-29



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_CAD008\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)



- ✓ **Include:**  
- All





# CAD009-All: Session disable browser persistence for All users when Browser and Non-Compliant-v1.2

Last modified: 2023-03-22



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser



Filter for devices

Exclude when  
device.isCompliant -eq True -or  
device.trustType -eq "ServerAD"



Locations

Not configured

Conditions



Users

✓ Include:

Users

- All

✗ Exclude:

Groups

- AAD\_UA\_CAD009\_Exclude (0)

- AAD\_UA\_ConAcc-Breakglass (6)

Grant access ✓

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



All cloud apps

✓ Include:

- All

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Never persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session



# CAD010-RJD: Require MFA for device join or registration when Browser and Modern Auth Clients- v1.1

Last modified: 2024-02-02



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Users

- All

✗ Exclude:

Groups

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAD010\_Exclude (1)

Grant access ✓

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



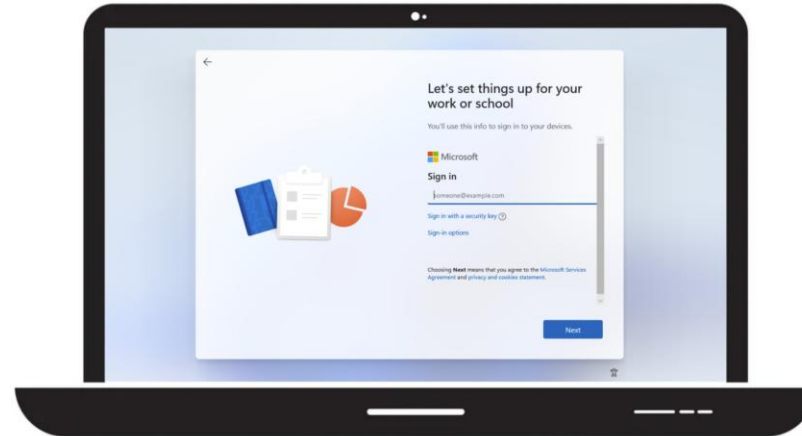
Custom authentication factor



Terms of use



Register or join devices



Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



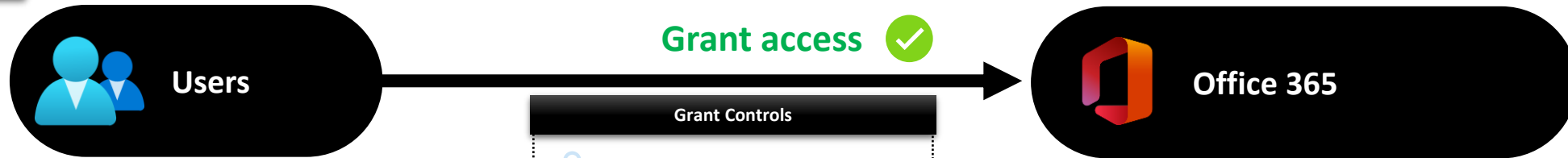
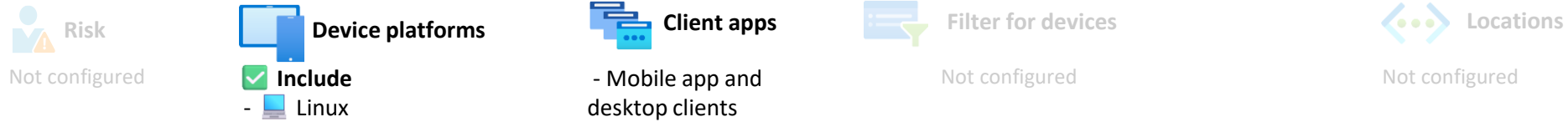
Disable resilience defaults



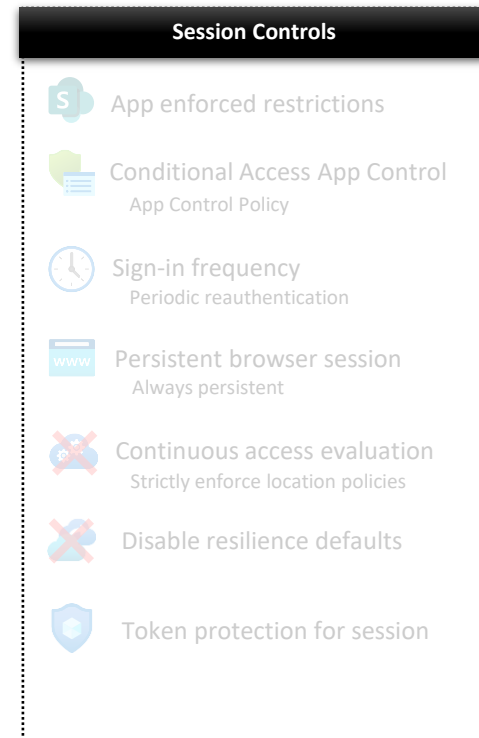
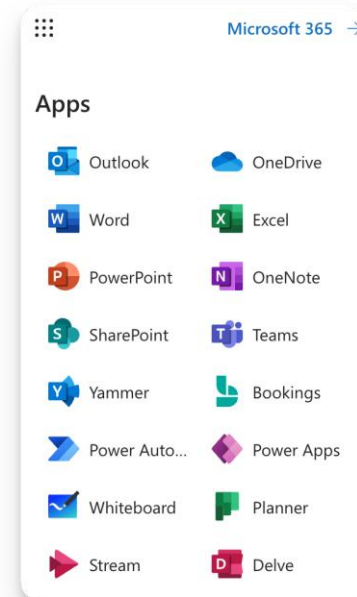
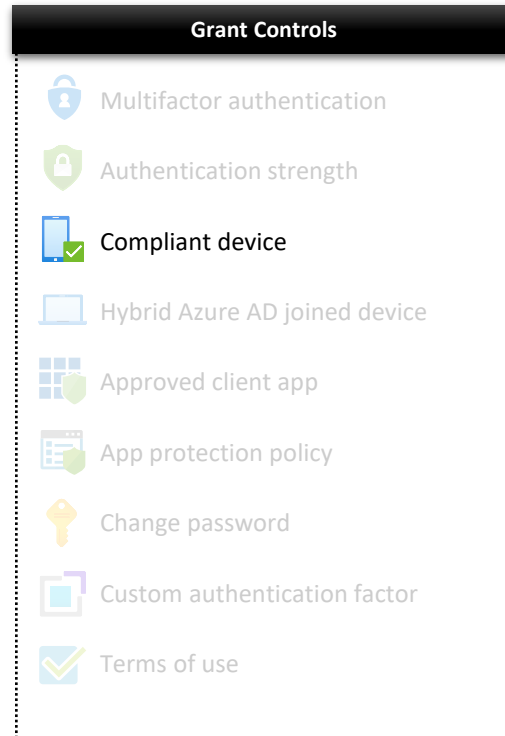
Token protection for session

# CAD011-O365: Grant Linux access for All users when Modern Auth Clients and Compliant-v1.0

Last modified: 2022-10-24




- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAD001\_Exclude (1)
- Users**  
- GuestsOrExternalUsers





# CAD012-All: Grant access for Admin users when Browser and Modern Auth Clients and Compliant-v1.1


Last modified: 2024-11-18


Conditions

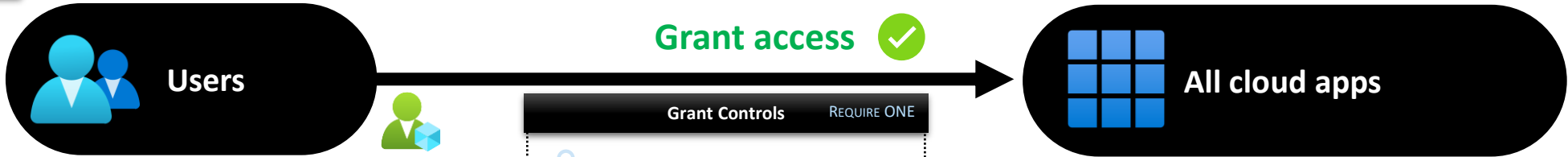
**Risk**  
Not configured

**Device platforms**  
Not configured

**Client apps**  
- Browser  
- Mobile app and desktop clients


**Filter for devices**  
Not configured


**Locations**  
Not configured





- ☒ **Include:**
- Directory roles**
- Application Administrator
  - Application Developer
  - Authentication Administrator
  - Authentication Extensibility Administrator
  - B2C IEF Keyset Administrator
  - Billing Administrator
  - Cloud Application Administrator
  - Cloud Device Administrator
  - Compliance Administrator
  - Conditional Access Administrator
  - Directory Writers
  - Exchange Administrator
  - Global Reader
  - Global Administrator
  - Helpdesk Administrator
  - Hybrid Identity Administrator
  - Intune Administrator


**Grant Controls** REQUIRE ONE


 Multifactor authentication


 Authentication strength


 Compliant device


 Hybrid Azure AD joined device

 Approved client app

 App protection policy


 Change password


 Custom authentication factor


 Terms of use


- ☒ **Include:**
- All


**Session Controls**


 App enforced restrictions


 Conditional Access App Control App Control Policy

 Sign-in frequency Periodic reauthentication

 Persistent browser session Always persistent

 Continuous access evaluation Strictly enforce location policies

 Disable resilience defaults

 Token protection for session



# CAD013-Selected: Grant access for All users when Browser and Modern Auth Clients and Compliant-v1.0

Last modified: 2025-08-08

Conditions



Risk

Not configured



Device platforms

✓ Include  
- All



Client apps

- Browser  
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:  
Users  
- All

✗ Exclude:  
Groups  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAD013\_Exclude (0)

Grant access



Selected cloud apps

✓ Include:  
- Edge Sync  
- Azure DevOps  
- Dynamics 365 Business Central  
- Windows Azure Service Management API

Grant Controls REQUIRE ONE

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAD014-O365: Require App Protection Policy for Edge on Windows for All users when Browser and Non-Compliant-v1.0

Last modified: 2024-10-14

Conditions



Risk

Not configured



Device platforms



Include

- Windows



Client apps

- Browser



Filter for devices

Exclude when  
device.isCompliant -eq True -or  
device.trustType -eq "ServerAD"



Locations

Not configured



Users

Grant access



Office 365



Include:

Groups

- AAD\_UA\_CAD014\_Include (0)



Exclude:

Groups

- AAD\_UA\_CAD014\_Exclude (0)
- AAD\_UA\_ConAcc-Breakglass (6)

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session

Microsoft 365 →

Apps

Outlook	OneDrive
Word	Excel
PowerPoint	OneNote
SharePoint	Teams
Yammer	Bookings
Power Auto...	Power Apps
Whiteboard	Planner
Stream	Delve



# CAD015-All: Grant access for All users when Browser and Modern Auth Clients and Compliant on Windows and macOS-v1.0

Last modified: 2025-03-04



Risk

Not configured



Device platforms



Include

- Windows
- macOS



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users



Include:

Groups

- AAD\_UA\_CAD015\_Include (1)



Exclude:

Groups

- AAD\_UA\_ConAcc-Breakglass (6)
- AAD\_UA\_CAD015\_Exclude (0)

Grant access

Grant Controls REQUIRE ONE



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



All cloud apps



Include:

- All

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session

Conditions





# CAD016-EXO\_SPO\_CloudPC: Require token protection when Modern Auth Clients on Windows- v1.2

Last modified: 2025-05-08



Risk

Not configured



Device platforms



**Include**

- Windows



Client apps

- Mobile app and  
desktop clients



Filter for devices

Not configured



Locations

Not configured



Users



**Include:**

**Groups**

- AAD\_UA\_CAD016\_Include (0)



**Exclude:**

**Guest or external users**

**All external Azure AD organizations**

**Groups**

- AAD\_UA\_CAD016\_Exclude (0)

- AAD\_UA\_ConAcc-Breakglass (6)

**Grant access**



Selected cloud apps

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



**Include:**

- Azure Virtual Desktop  
- Windows 365  
- Windows Cloud Login  
- Office 365 Exchange Online  
- Office 365 SharePoint Online

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session



# CAD017-Selected: Grant iOS and Android access for All users when Modern Auth Clients and AppProPol or Compliant-v1.1

Last modified: 2025-10-18

Conditions



Risk

Not configured



Device platforms



Include

- Android
- iOS



Client apps

- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users



Include:

Groups

- AAD\_UA\_CAD017\_Include (0)



Exclude:

Guest or external users

All external Azure AD organizations

Groups

- AAD\_UA\_ConAcc-Breakglass (6)
- AAD\_UA\_CAD017\_Exclude (0)

Grant access



Azure Active Directory

Grant Controls

REQUIRE ONE



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults

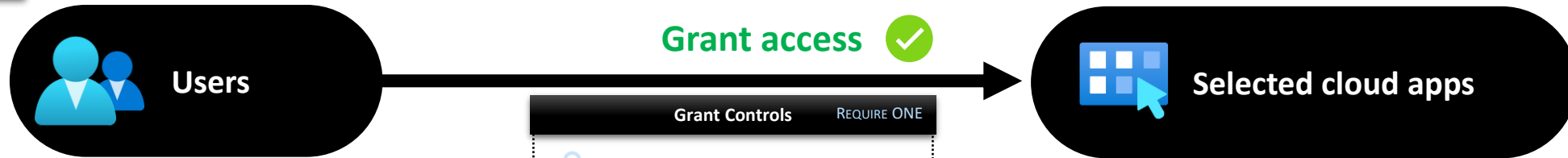
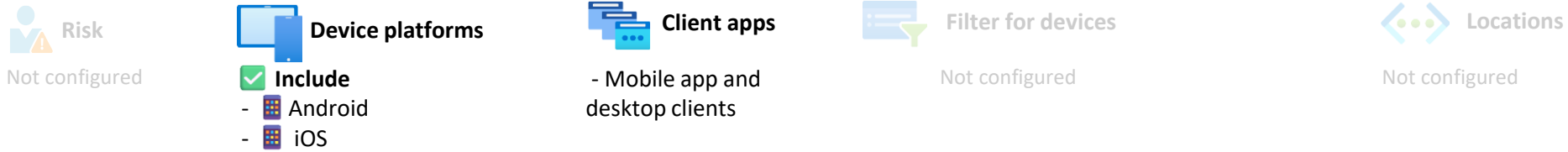


Token protection for session

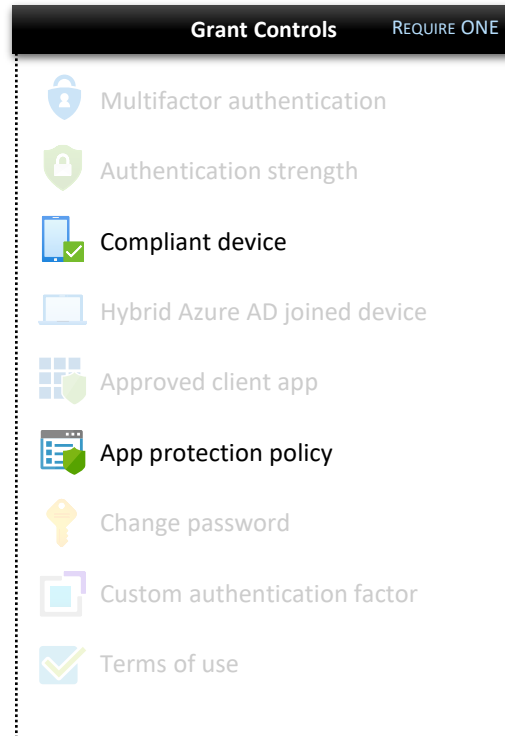


# CAD018-CloudPC: Grant iOS and Android access for All users when Modern Auth Clients and AppProPol or Compliant-v1.0

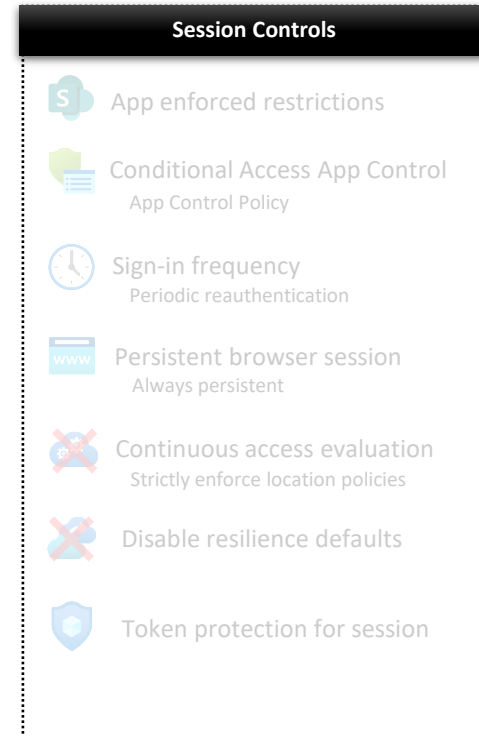
Last modified: 2025-09-01



- ✓ **Include:**
  - Users**
    - All
- ✗ **Exclude:**
  - Guest or external users**
    - All external Azure AD organizations
  - Groups**
    - AAD\_UA\_ConAcc-Breakglass (6)
    - AAD\_UA\_CAD018\_Exclude (0)

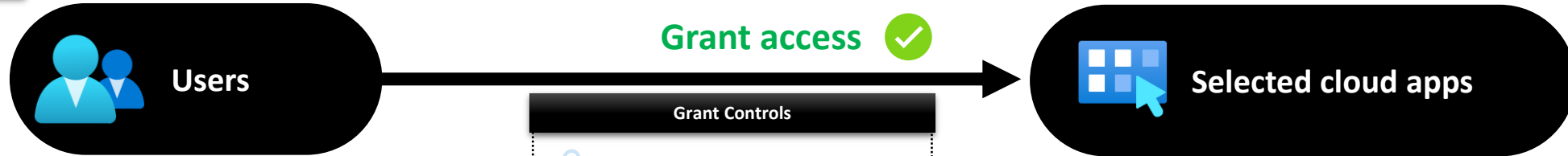


- ✓ **Include:**
  - Azure Virtual Desktop
  - Microsoft Remote Desktop
  - Windows 365
  - Windows Cloud Login



# CAD019-Intune: Require MFA and set sign-in frequency to every time-v1.0

Last modified: 2025-10-11



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_CAD019\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)

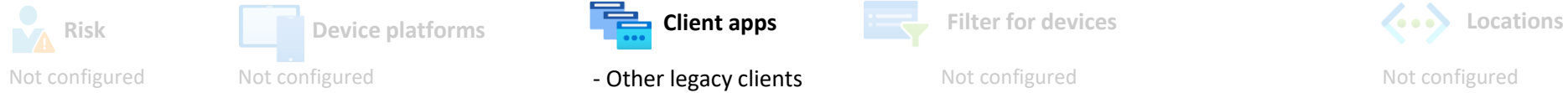
- Grant Controls**
- Multifactor authentication
  - Auth strength: Multifactor authentication
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- ✓ **Include:**  
- Microsoft Intune Enrollment

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency  
Every time
  - Persistent browser session  
Always persistent
  - Continuous access evaluation  
Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session

# CAP001-All: Block Legacy Authentication for All users when OtherClients-v1.0

Last modified: 2022-12-29



✓ **Include:**

**Users**

- All










✗ **Exclude:**

**Groups**

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAP001\_Exclude (0)








## Grant Controls

-  Multifactor authentication
-  Authentication strength
-  Compliant device
-  Hybrid Azure AD joined device
-  Approved client app
-  App protection policy
-  Change password
-  Custom authentication factor
-  Terms of use

✓ **Include:**

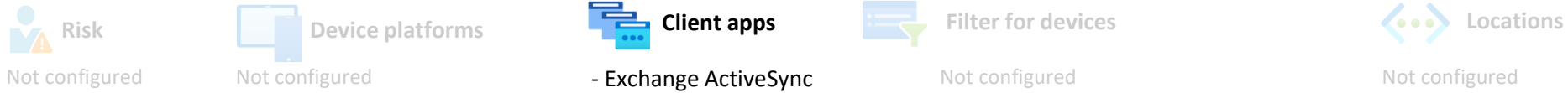
- All

## Session Controls

-  App enforced restrictions
-  Conditional Access App Control App Control Policy
-  Sign-in frequency Periodic reauthentication
-  Persistent browser session Always persistent
-  Continuous access evaluation Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session

# CAP002-All: Block Exchange ActiveSync Clients for All users-v1.1

Last modified: 2025-08-13



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_CAP002\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)

- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- ✓ **Include:**  
- All

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency  
Periodic reauthentication
  - Persistent browser session  
Always persistent
  - Continuous access evaluation  
Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session



# CAP003-All: Block device code authentication flow-v1.0

Policy Enabled

Last modified: 2025-03-04



- Include:**  
**Users**  
- All
- Exclude:**  
**Groups**  
- AAD\_UA\_CAP003\_Exclude (2)  
- AAD\_UA\_ConAcc-Breakglass (6)

- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- Include:**  
- All

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency  
Periodic reauthentication
  - Persistent browser session  
Always persistent
  - Continuous access evaluation  
Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session

# CAP004-All: Block authentication transfer-v1.0

Last modified: 2025-03-04

**Risk** Not configured

**Device platforms** Not configured

**Client apps** Not configured

**Filter for devices** Not configured

**Locations** Not configured



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAP004\_Exclude (0)

- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

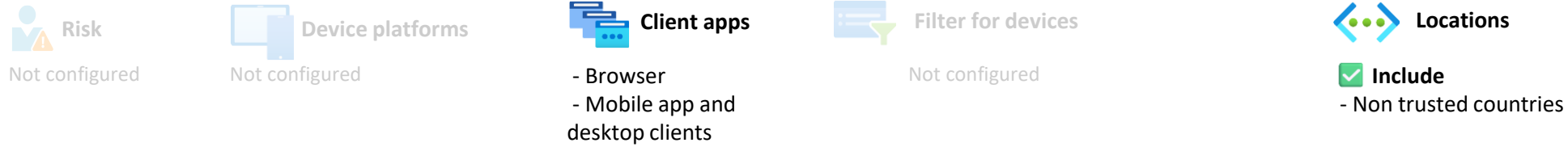
- ✓ **Include:**  
- All

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control  
App Control Policy
  - Sign-in frequency  
Periodic reauthentication
  - Persistent browser session  
Always persistent
  - Continuous access evaluation  
Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session

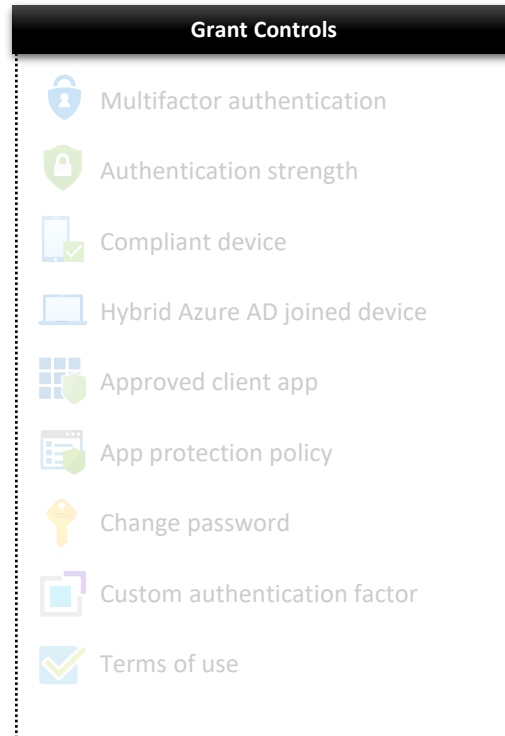


# CAL001-All: Block specified locations for All users when Browser and Modern Auth Clients-v1.1

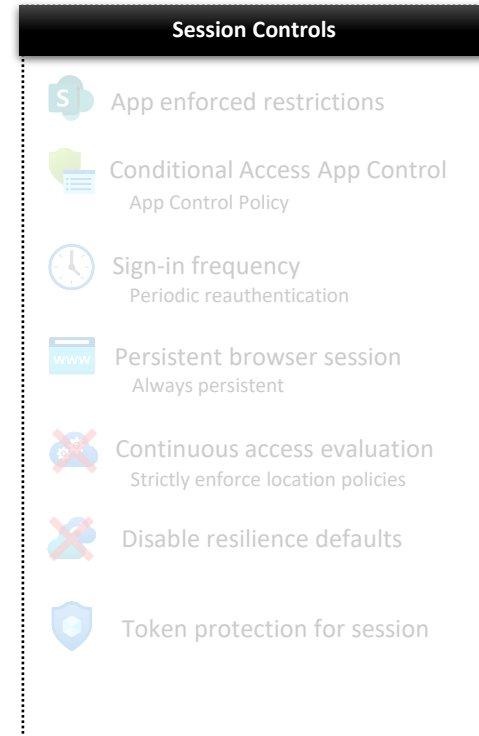
Last modified: 2023-08-01



- ✓ **Include:**  
**Users**
  - All
- ✗ **Exclude:**  
**Groups**
  - AAD\_UA\_CAL001\_Exclude (0)
  - AAD\_UA\_ConAcc-Breakglass (6)



- ✓ **Include:**
  - All





# CAL002-RSI: Require MFA registration from trusted locations only for All users when Browser and Modern Auth Clients-v1.4

Last modified: 2024-08-20



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

- ☒ **Include**
  - All
- ☐ **Exclude**
  - AllTrusted



Users

- ☒ **Include:**
  - Users
  - All

- ☐ **Exclude:**
  - Guest or external users
  - All external Azure AD organizations
- Groups**
  - AAD\_UA\_CAL002\_Exclude (0)
  - AAD\_UA\_ConAcc-Breakglass (6)

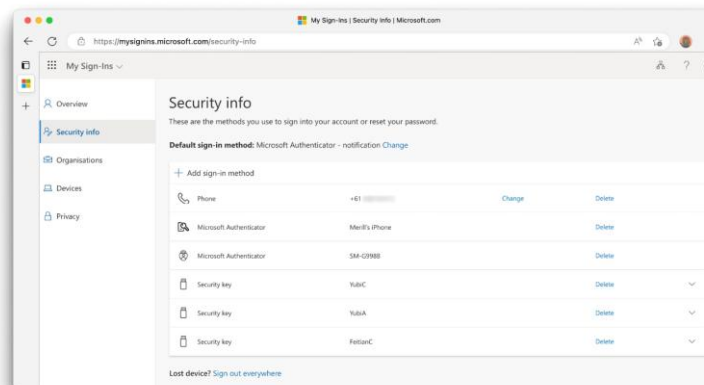
Grant access

Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use



Register security information



Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAL003-All: Block Access for Specified Service Accounts except from Provided Trusted Locations when Browser and Modern Auth Clients-v1.1

Last modified: 2025-10-18



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

☒ **Include**  
- All

☐ **Exclude**  
- AllTrusted



Users

☒ **Include:**  
**Users**  
- None

**Block access**



All cloud apps

☒ **Include:**  
- All

## Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

## Session Controls

- App enforced restrictions
- Conditional Access App Control  
App Control Policy
- Sign-in frequency  
Periodic reauthentication
- Persistent browser session  
Always persistent
- Continuous access evaluation  
Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAL004-All: Block access for Admins from non-trusted locations when Browser and Modern Auth Clients-v1.2

Last modified: 2024-12-05

Conditions



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

- ☒ **Include**
  - All
- ☐ **Exclude**
  - AllTrusted



Users



**Block access**



All cloud apps

☒ **Include:**

**Directory roles**

- Application Administrator
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Billing Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Compliance Administrator
- Conditional Access Administrator
- Directory Writers
- Exchange Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator

Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

☒ **Include:**

- All

Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAL005-Selected: Grant access for All users on less-trusted locations when Browser and Modern Auth Clients and Compliant-v1.0

Last modified: 2025-08-13

Conditions



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

- ✓ Include
- Less trusted countries



Users

- ✓ Include:  
Users  
- All
- ✗ Exclude:  
Groups  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAL005\_Exclude (0)

Grant access ✓

Grant Controls REQUIRE ONE

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use



All cloud apps

- ✓ Include:  
- All
- ✗ Exclude:  
- Office365

Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- ✗ Continuous access evaluation Strictly enforce location policies
- ✗ Disable resilience defaults
- Token protection for session



# CAL006-All: Only Allow Access from specified locations for specific accounts when Browser and Modern Auth Clients-v1.0

Last modified: 2025-03-04



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

☒ Include

- All

☐ Exclude

- United States



Users

☒ Include:

Groups

- AAD\_UA\_CAL006\_Include (1)

☐ Exclude:

Groups

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAL006\_Exclude (0)

Block access



All cloud apps

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

☒ Include:

- All

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



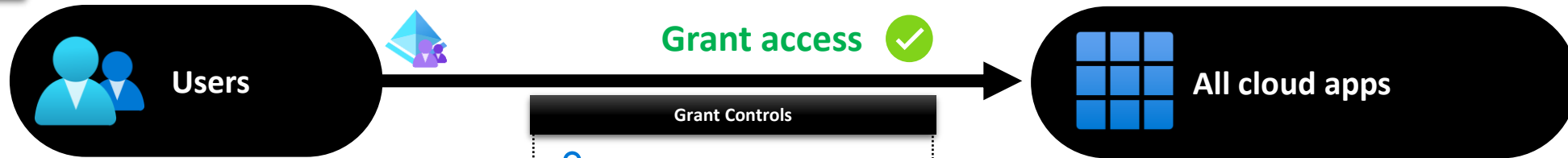
Disable resilience defaults



Token protection for session

# CAU001-All: Grant Require MFA for guests when Browser and Modern Auth Clients-v1.1

Last modified: 2025-10-11



✓ **Include:**  
**Guest or external users**  
**All external Azure AD organizations**

✗ **Exclude:**  
**Groups**

- AAD\_UA\_CAU001\_Exclude (0)
- AAD\_UA\_ConAcc-Breakglass (6)

Grant Controls	
	Multifactor authentication
	Authentication strength
	Compliant device
	Hybrid Azure AD joined device
	Approved client app
	App protection policy
	Change password
	Custom authentication factor
	Terms of use

✓ **Include:**

- All

✗ **Exclude:**

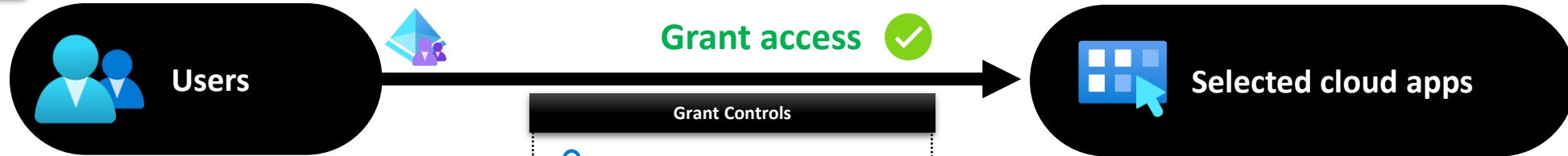
- Microsoft Rights Management Services

Session Controls	
	App enforced restrictions
	Conditional Access App Control App Control Policy
	Sign-in frequency Periodic reauthentication
	Persistent browser session Always persistent
	Continuous access evaluation Strictly enforce location policies
	Disable resilience defaults
	Token protection for session



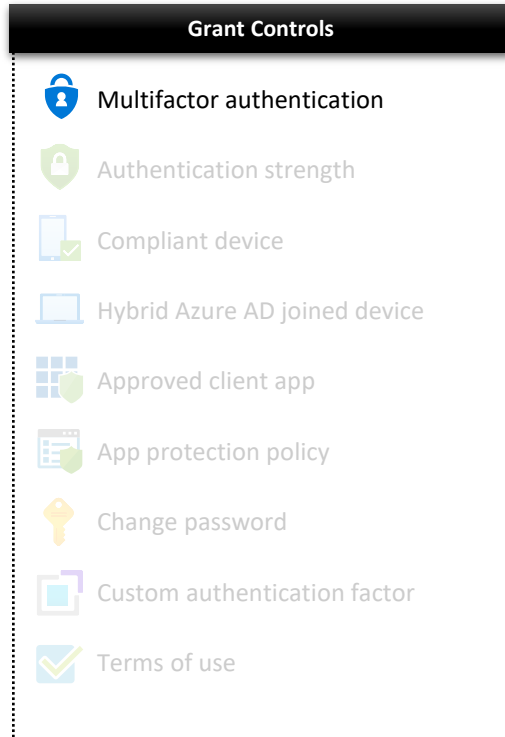
# CAU001A-Windows Azure Active Directory: Grant Require MFA for guests when Browser and Modern Auth Clients-v1.0

Last modified: 2025-10-11

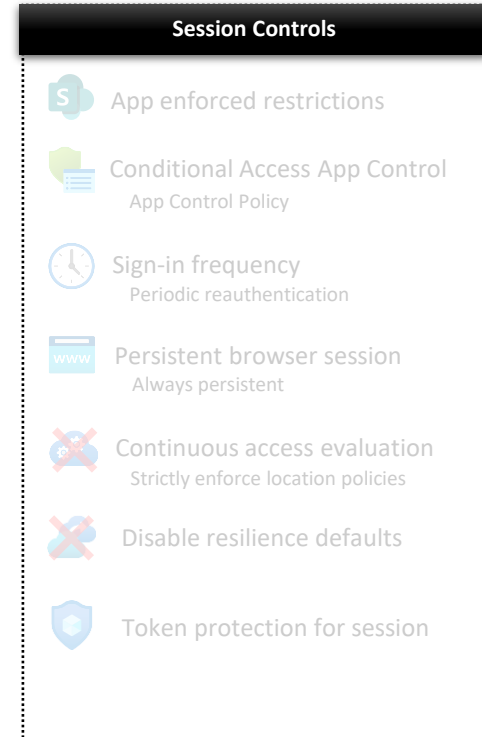


- ✓ **Include:**  
**Guest or external users**  
**All external Azure AD organizations**

- ✗ **Exclude:**  
**Groups**
  - AAD\_UA\_CAU001\_Exclude (0)
  - AAD\_UA\_ConAcc-Breakglass (6)



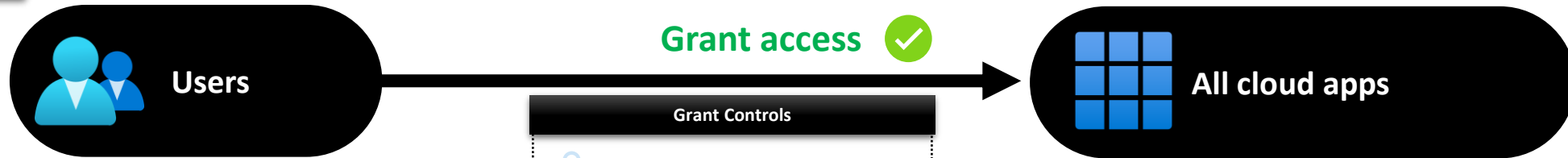
- ✓ **Include:**  
- Windows Azure Active Directory





# CAU002-All: Grant Require MFA for All users when Browser and Modern Auth Clients-v1.5

Last modified: 2025-09-04



 **Include:**

**Users**

- All

 **Exclude:**










**Guest or external users**

**All external Azure AD organizations**

**Directory roles**

- Application Administrator
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Device Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Directory Writers
- Global Administrator
- Global Reader








## Grant Controls

-  Multifactor authentication
-  Auth strength: Multifactor authentication
-  Compliant device
-  Hybrid Azure AD joined device
-  Approved client app
-  App protection policy
-  Change password
-  Custom authentication factor
-  Terms of use

 **Include:**

- All

## Session Controls

-  App enforced restrictions
-  Conditional Access App Control App Control Policy
-  Sign-in frequency Periodic reauthentication
-  Persistent browser session Always persistent
-  Continuous access evaluation Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session



# CAU003-Selected: Block unapproved apps for guests when Browser and Modern Auth Clients-v1.0

Last modified: 2024-09-24

Risk  
Not configured

Device platforms  
Not configured

Client apps  
- Browser  
- Mobile app and desktop clients

Filter for devices  
Not configured

Locations  
Not configured



✓ **Include:**  
Guest or external users  
All external Azure AD organizations

✗ **Exclude:**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAU003\_Exclude (0)

Grant Controls

Multifactor authentication  
 Authentication strength  
 Compliant device  
 Hybrid Azure AD joined device  
 Approved client app  
 App protection policy  
 Change password  
 Custom authentication factor  
 Terms of use

✓ **Include:**  
- Portfolios

Session Controls

App enforced restrictions  
 Conditional Access App Control App Control Policy  
 Sign-in frequency  
Periodic reauthentication  
 Persistent browser session  
Always persistent  
 Continuous access evaluation  
Strictly enforce location policies  
 Disable resilience defaults  
 Token protection for session



# CAU004-Selected: Session route through MDCA for All users when Browser on Non-Compliant- v1.2

Last modified: 2025-05-28



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser



Filter for devices

Exclude when  
device.isCompliant -eq True -or  
device.trustType -eq "ServerAD"



Locations

Not configured

Grant access



Users

Include:

Users

- All

Exclude:

Guest or external users

All external Azure AD organizations

Groups

- AAD\_UA\_CAU004\_Exclude (0)

- AAD\_UA\_ConAcc-Breakglass (6)

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



Selected cloud apps

Include:

- Sessionize.com

- Office365

Session Controls



App enforced restrictions



Conditional Access App Control  
Use custom policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



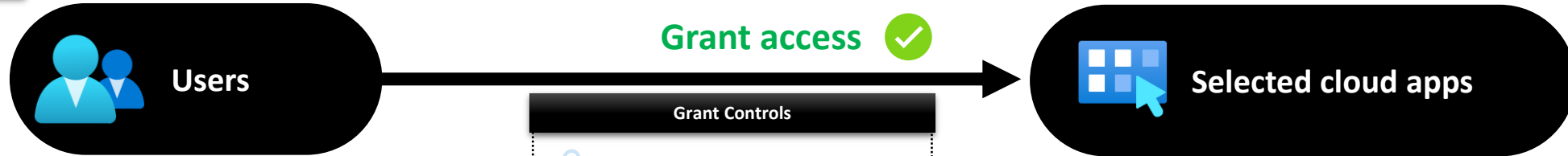
Disable resilience defaults



Token protection for session

# CAU005-Selected: Session route through MDCA for All users when Browser on Compliant-v1.1

Last modified: 2023-10-06



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAU005\_Exclude (0)

- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- ✓ **Include:**  
- Portfolios

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control  
Monitor cloud apps
  - Sign-in frequency  
Periodic reauthentication
  - Persistent browser session  
Always persistent
  - Continuous access evaluation  
Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session



# CAU006-All: Grant access for Medium and High Risk Sign-in for All Users when Browser and Modern Auth Clients require MFA-v1.4

Last modified: 2025-10-08



**Risk**

**Sign-in risk:**

- High
- Medium



**Device platforms**

Not configured



**Client apps**

- Browser
- Mobile app and desktop clients



**Filter for devices**

Not configured



**Locations**

Not configured



**Users**

✓ **Include:**

**Users**

- All

✗ **Exclude:**

**Groups**

- AAD\_UA\_ConAcc-Breakglass (6)
- AAD\_UA\_CAU006\_Exclude (0)

**Grant access** ✓

**Grant Controls**



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



**All cloud apps**

✓ **Include:**

- All

**Session Controls**



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Every time



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session



# CAU007-All: Grant access for Medium and High Risk Users for All Users when Browser and Modern Auth Clients require PWD reset-v1.3

Last modified: 2025-03-04



Risk

User risk:

- High
- Medium



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Users

- All

✗ Exclude:

Guest or external users

All external Azure AD organizations

Groups

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAU007\_Exclude (0)

Grant access



All cloud apps

Grant Controls

REQUIRE ALL



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

✓ Include:

- All

Session Controls



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Every time



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session



# CAU008-All: Grant Require Phishing Resistant MFA for Admins when Browser and Modern Auth Clients-v1.4

Last modified: 2025-03-04



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users



Grant access



All cloud apps

Include:

## Directory roles

- Application Administrator
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Billing Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Compliance Administrator
- Conditional Access Administrator
- Directory Writers
- Exchange Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator

## Grant Controls

- Multifactor authentication
- Auth strength:Phishing-resistant MFA
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

Include:

- All

## Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAU009-Management: Grant Require MFA for Admin Portals for All Users when Browser and Modern Auth Clients-v1.2

Last modified: 2023-08-28



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Users

- All

✗ Exclude:

Groups

- AAD\_UA\_CAU009\_Exclude (1)
- AAD\_UA\_ConAcc-Breakglass (6)

Grant access ✓



Selected cloud apps

Grant Controls

- Multifactor authentication
- Auth strength:Multifactor authentication
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

✓ Include:

- MicrosoftAdminPortals
- Windows Azure Service Management API

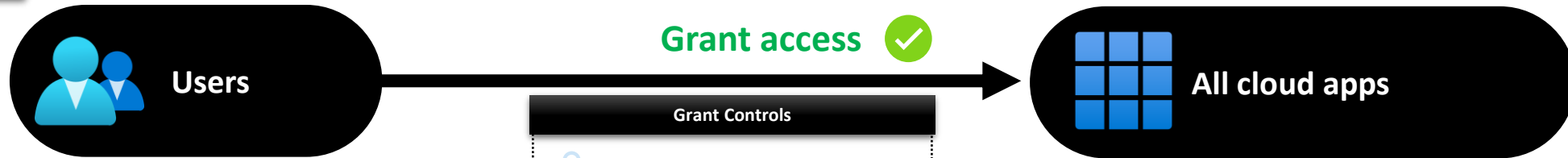
Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAU010-All: Grant Require ToU for All Users when Browser and Modern Auth Clients-v1.2

Last modified: 2025-08-01



- ✓ **Include:**  
**Users**  
- All
- ✗ **Exclude:**  
**Guest or external users**  
**All external Azure AD organizations**  
**Groups**  
- AAD\_UA\_CAU010\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)

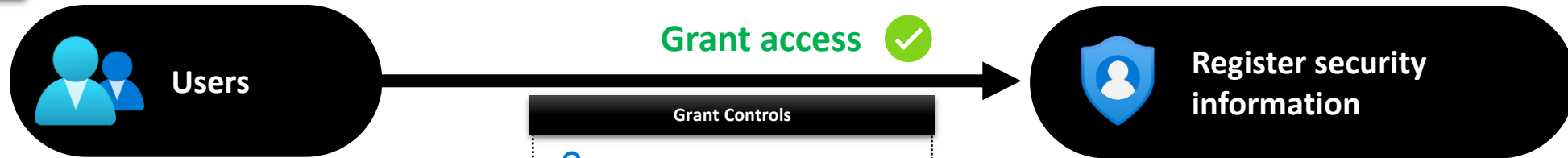
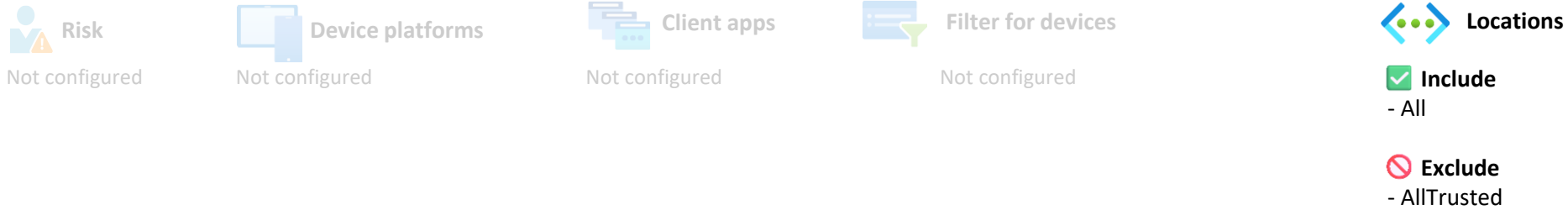
- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - ✓ Integration Terms Of Use

- ✓ **Include:**  
- All
- ✗ **Exclude:**  
- Microsoft Intune  
- Microsoft Intune Enrollment

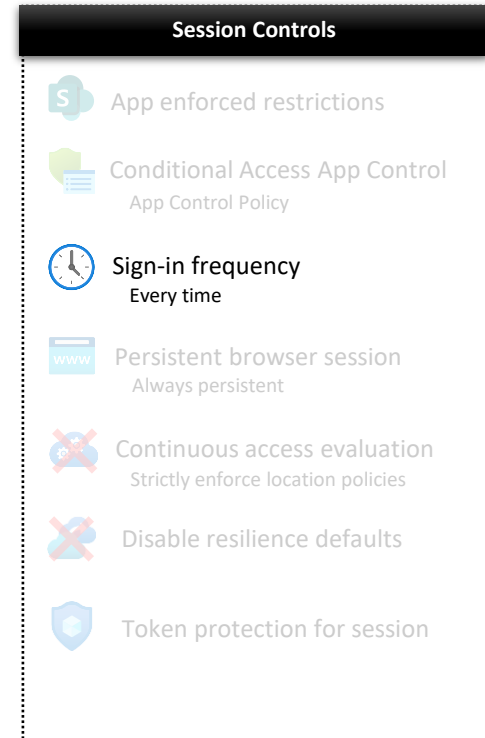
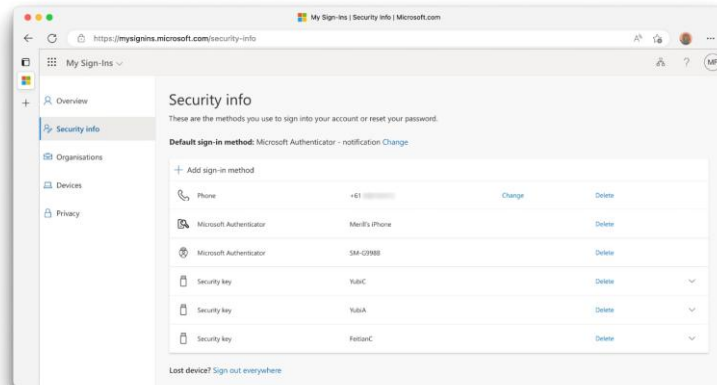
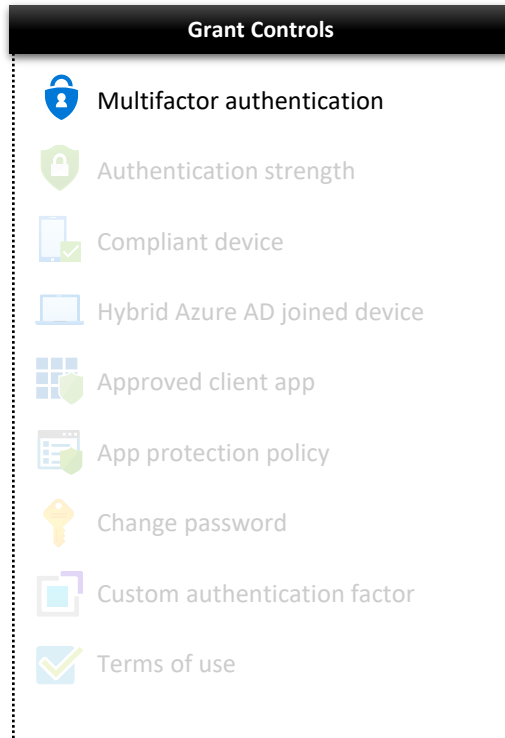
- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency Periodic reauthentication
  - Persistent browser session Always persistent
  - ✗ Continuous access evaluation Strictly enforce location policies
  - ✗ Disable resilience defaults
  - Token protection for session

# CAU012-RSI: Combined Security Info Registration with TAP-v1.1

Last modified: 2025-02-26



- ☒ **Include:**  
**Users**  
- All
- ☐ **Exclude:**  
**Groups**  
- AAD\_UA\_CAU012\_Exclude (0)  
- AAD\_UA\_ConAcc-Breakglass (6)





# CAU013-All: Grant Require phishing resistant MFA for All users when Browser and Modern Auth Clients-v1.0

Last modified: 2024-10-07

Conditions

- Risk  
Not configured
- Device platforms  
Not configured
- Client apps  
- Browser  
- Mobile app and desktop clients
- Filter for devices  
Not configured
- Locations  
Not configured



- Include:**  
**Groups**  
- AAD\_UA\_CAU013\_Include (0)
- Exclude:**  
**Groups**  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAU013\_Exclude (0)

- Grant Controls
- Multifactor authentication
- Auth strength: Phishing-resistant MFA
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

- Include:**  
- All
- Exclude:**  
- Windows Store for Business

- Session Controls
- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency  
Periodic reauthentication
- Persistent browser session  
Always persistent
- Continuous access evaluation  
Strictly enforce location policies
- Disable resilience defaults
- Token protection for session

# CAU014-All: Block Managed Identity when Sign in Risk is Medium or High-v1.0

Last modified: 2024-10-14

 **Risk**  
Service principal risk:

- High
- Medium

 **Device platforms**  
Not configured

 **Client apps**  
Not configured

 **Filter for devices**  
Not configured

 **Locations**  
Not configured

 **Workload identity**










- ✓ **Include:**
- Simeon Cloud Sync

**Block access** 








 **All cloud apps**

- ✓ **Include:**
- All

## Grant Controls

-  Multifactor authentication
-  Authentication strength
-  Compliant device
-  Hybrid Azure AD joined device
-  Approved client app
-  App protection policy
-  Change password
-  Custom authentication factor
-  Terms of use

## Session Controls

-  App enforced restrictions
-  Conditional Access App Control App Control Policy
-  Sign-in frequency Periodic reauthentication
-  Persistent browser session Always persistent
-  Continuous access evaluation Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session



# CAU015-All: Block access for High Risk Sign-in for All Users when Browser and Modern Auth Clients-v1.0

Last modified: 2025-10-06

Conditions



**Risk**

**Sign-in risk:**  
- High



**Device platforms**

Not configured



**Client apps**

- Browser  
- Mobile app and desktop clients



**Filter for devices**

Not configured



**Locations**

Not configured



**Users**

✓ **Include:**

**Groups**

- AAD\_UA\_CAU015\_Include (0)

✗ **Exclude:**

**Guest or external users**

**All external Azure AD organizations**

**Groups**

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAU015\_Exclude (0)

**Block access** ✗



**All cloud apps**

**Grant Controls**



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

✓ **Include:**

- All

**Session Controls**



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



Disable resilience defaults



Token protection for session



# CAU016-All: Block access for High Risk Users for All Users when Browser and Modern Auth Clients-v1.0

Last modified: 2024-10-14



**Risk**

**User risk:**  
- High



**Device platforms**

Not configured



**Client apps**

Not configured



**Filter for devices**

Not configured



**Locations**

Not configured



**Users**



**Include:**

**Groups**

- AAD\_UA\_CAU016\_Include (0)



**Exclude:**

**Guest or external users**

**All external Azure AD organizations**

**Groups**

- AAD\_UA\_ConAcc-Breakglass (6)

- AAD\_UA\_CAU016\_Exclude (0)

**Block access**



**All cloud apps**

**Grant Controls**



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use



**Include:**

- All

**Session Controls**



App enforced restrictions



Conditional Access App Control  
App Control Policy



Sign-in frequency  
Periodic reauthentication



Persistent browser session  
Always persistent



Continuous access evaluation  
Strictly enforce location policies



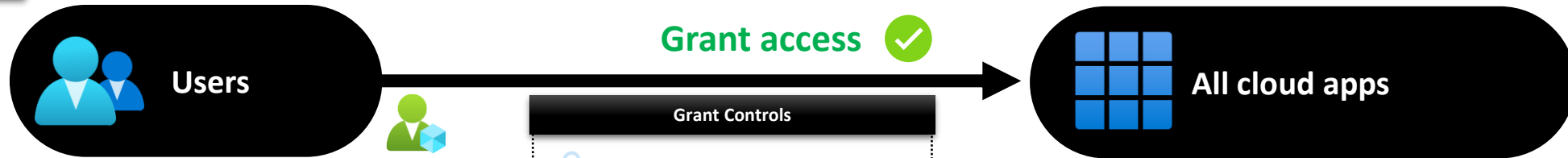
Disable resilience defaults



Token protection for session

# CAU017-All: Session set Sign-in Frequency for Admins when Browser-v1.0

Last modified: 2025-10-16



- ✓ **Include:**
- Directory roles**
- Application Administrator
  - Application Developer
  - Authentication Administrator
  - Authentication Extensibility Administrator
  - B2C IEF Keyset Administrator
  - Billing Administrator
  - Cloud Application Administrator
  - Cloud Device Administrator
  - Compliance Administrator
  - Conditional Access Administrator
  - Directory Writers
  - Exchange Administrator
  - Global Administrator
  - Global Reader
  - Helpdesk Administrator
  - Hybrid Identity Administrator
  - Intune Administrator

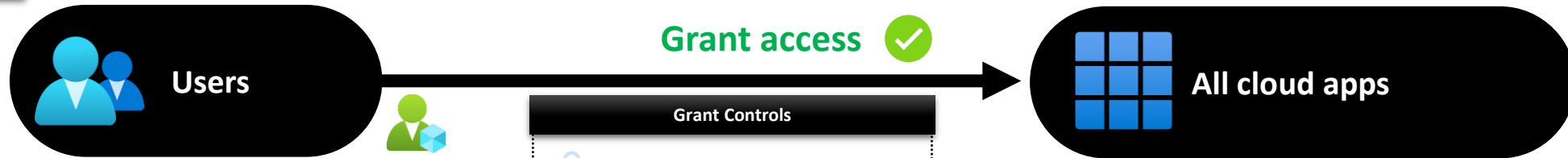
- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- ✓ **Include:**
- All

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency 10 hours
  - Persistent browser session Always persistent
  - Continuous access evaluation Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session

# CAU018-All: Session disable browser persistence for Admins when Browser-v1.0

Last modified: 2025-10-16



- ✓ **Include:**
- Directory roles**
- Application Administrator
  - Application Developer
  - Authentication Administrator
  - Authentication Extensibility Administrator
  - B2C IEF Keyset Administrator
  - Billing Administrator
  - Cloud Application Administrator
  - Cloud Device Administrator
  - Compliance Administrator
  - Conditional Access Administrator
  - Directory Writers
  - Exchange Administrator
  - Global Administrator
  - Global Reader
  - Helpdesk Administrator
  - Hybrid Identity Administrator
  - Intune Administrator

- Grant Controls**
- Multifactor authentication
  - Authentication strength
  - Compliant device
  - Hybrid Azure AD joined device
  - Approved client app
  - App protection policy
  - Change password
  - Custom authentication factor
  - Terms of use

- ✓ **Include:**
- All

- Session Controls**
- App enforced restrictions
  - Conditional Access App Control App Control Policy
  - Sign-in frequency Periodic reauthentication
  - Persistent browser session Never persistent
  - Continuous access evaluation Strictly enforce location policies
  - Disable resilience defaults
  - Token protection for session





# CAU019-Selected: Only allow approved apps for guests when Browser and Modern Auth Clients- v1.0

Last modified: 2025-10-17



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured

Conditions



Users



Block access



All cloud apps

- ✓ **Include:**  
Guest or external users  
All external Azure AD organizations

- ✗ **Exclude:**  
Groups  
- AAD\_UA\_ConAcc-Breakglass (6)  
- AAD\_UA\_CAU019\_Exclude (0)

Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

- ✓ **Include:**  
- All
- ✗ **Exclude:**  
- Windows Azure Active Directory  
- Microsoft Approval Management  
- AADReporting  
- Azure Credential Configuration Endpoint Service  
- Microsoft App Access Panel  
- My Signins  
- Microsoft Invitation Acceptance Portal  
- My Profile  
- My Apps  
- Office365

Session Controls

- App enforced restrictions
- Conditional Access App Control  
App Control Policy
- Sign-in frequency  
Periodic reauthentication
- Persistent browser session  
Always persistent
- Continuous access evaluation  
Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



# CAU011-All: Block access for All users except licensed when Browser and Modern Auth Clients- v1.0

Last modified: 2022-09-18



Risk

Not configured



Device platforms

Not configured



Client apps

- Browser
- Mobile app and desktop clients



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Users

- All

✗ Exclude:

Directory roles

- License Administrator
- Global Administrator

Groups

- AAD\_UA\_CAU011\_Exclude (1)
- AAD\_UA\_ConAcc-Breakglass (6)
- AAD\_UG\_ModernWorkplace (7)

Users

- GuestsOrExternalUsers

Block access



All cloud apps

Grant Controls

- Multifactor authentication
- Authentication strength
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

✓ Include:

- All

Session Controls

- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session