



Conditional Access Policy Documentation

Tenant ID

xxx

Tenant Name

xxx

Generated by

Morten Waltorp Knudsen (mok@2linkIT.net)

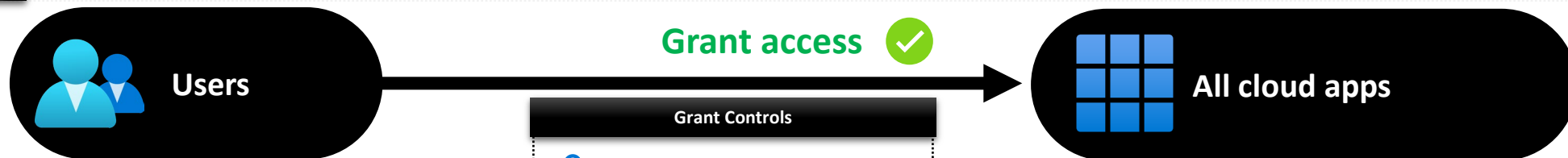
Generated on

04 May 2025

CA000-Prod-Global-AllUsers-AllApps-AnyPlatform-MFA-CatchNoTag

Policy Enabled

Last modified: 2025-04-06



 **Include:**

Users










- All

 **Exclude:**

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA000-Global-AllUsers-AllApps-AnyPlatform-MFA-CatchNoTag-Excluded-Assigned (0)
- Entra-CA-Users-All-Dynamic (19)
- Entra-CA-Admins-All-Dynamic (7)
- Entra-CA-ServiceAccounts-All-Dynamic (4)
- Entra-CA-ADConnect-Accounts-All-Dynamic (2)
- Entra-CA-Shared-Mail-Users-All-Dynamic (2)
- Entra-CA-Shared-Device-Users-All-Dynamic (4)
- Entra-CA-Teams-Rooms-All-Dynamic (0)
- Entra-CA-AppSystem-Test-Users-All-Dynamic (8)
- Entra-CA-Users-NonManaged-All-Dynamic (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

CA001-Prod-Global-AllApps-AnyPlatform-Block-DeniedCountries

Policy Enabled

Last modified: 2025-01-12

 **Risk**
Not configured

 **Device platforms**
Not configured

 **Client apps**
Not configured










 **Filter for devices**
Not configured

 **Locations**
☒ **Include**
- Denied Countries sign-ins










- ☒ **Include:**
Users
- All
- ☐ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA001-Global-AllApps-AnyPlatform-Block-DeniedCountries-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

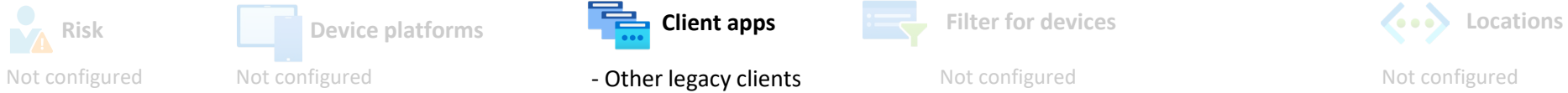
Session Controls

-  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

CA002-Prod-Global-AllApps-AnyPlatform-LegacyAuthentication-OtherClients-Block

Policy Enabled

Last modified: 2025-01-12



Include:

Users

- All



Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)

- Entra-CA-CA002-Global-AllApps-AnyPlatform-LegacyAuthentication-OtherClients-Block-

Excluded-Assigned (1)

Users

- Break Glass Account 0 (Entra ID)

- Break Glass Account 1 (Entra ID)

- Break Glass Account 2 (Entra ID)

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



CA004-Prod-Global-RegisterOrJoin-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



Users

Grant access



Register or join devices

Include:

Users

- All

Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA004-Global-RegisterOrJoin-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)

Users

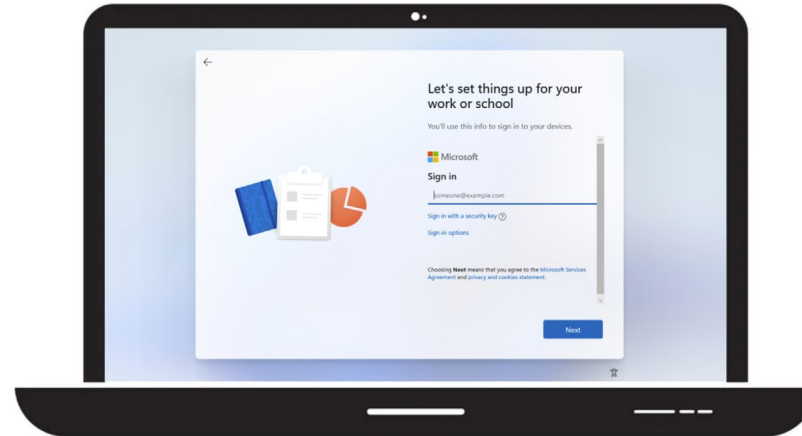
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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



CA005-Prod-Global-DeviceCodeFlow-AllApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-05-01



- ✓ **Include:**
Users
- All
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA005-Global-DeviceCodeFlow-AllApps-AnyPlatform-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

- 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



CA006-Prod-Global-AllApps-AnyPlatform-HighUserRisk-Block

Policy Enabled

Last modified: 2025-01-12



Risk

User risk:
- High



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:
Users
- All

✗ Exclude:
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA006-Global-AllApps-AnyPlatform-HighUserRisk-Block-Excluded-Assigned (2)

Users
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

CA007-Prod-Global-AllApps-AnyPlatform-UnknownPlatforms-Block

Policy Enabled

Last modified: 2025-01-12



- ☒ **Include:**
Users
- All
- ☒ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA007-Global-AllApps-AnyPlatform-UnknownPlatforms-Block-Excluded-Assigned (1)
Users
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

- 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



CA096-Prod-BreakGlassAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-MFA-Allow

Policy Enabled

Last modified: 2025-02-05



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

☒ Include
- All

☐ Exclude
- AllTrusted



Users

☒ Include:

Groups

- Entra-CA-BreakGlassAccounts-Req-MFA-All-Dynamic (1)

Users

- Break Glass Account 0 (Entra ID)

Grant access ☒

Grant Controls



Multifactor authentication



Authentication strength



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



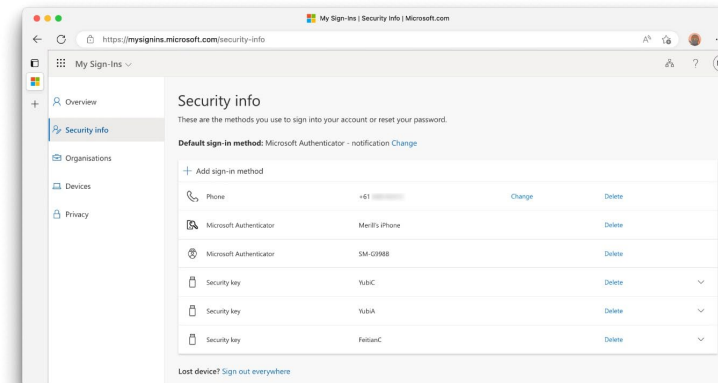
Custom authentication factor



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

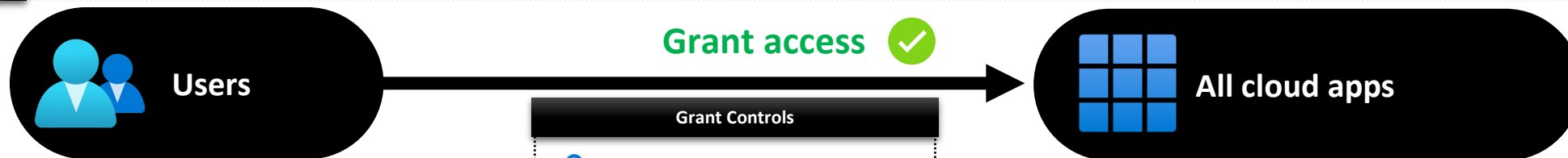



Token protection for session










CA097-Prod-BreakGlassAccounts-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-BreakGlassAccounts-Req-MFA-All-Dynamic (1)
- Users**
- Break Glass Account 0 (Entra ID)

- 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



CA098-Prod-BreakGlassAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

☒ Include
- All

☐ Exclude
- AllTrusted



Users

Grant access



Register security information

☒ Include:

Groups

- Entra-CA-BreakGlassAccounts-Req-FIDO-All-Dynamic (2)

Users

- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant Controls



Multifactor authentication



Auth strength:FIDO Security Key & TAP



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



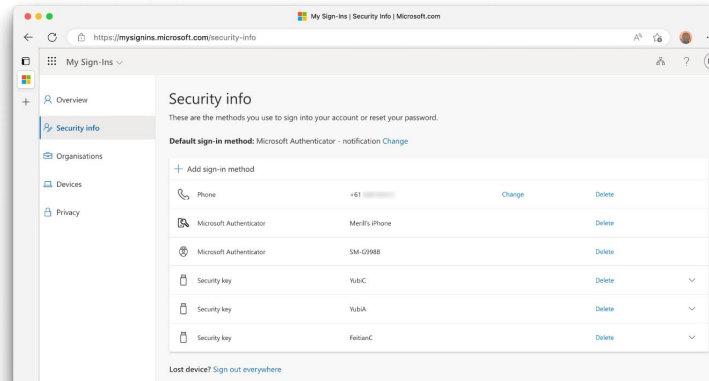
Continuous access evaluation
Strictly enforce location policies



Disable resilience defaults



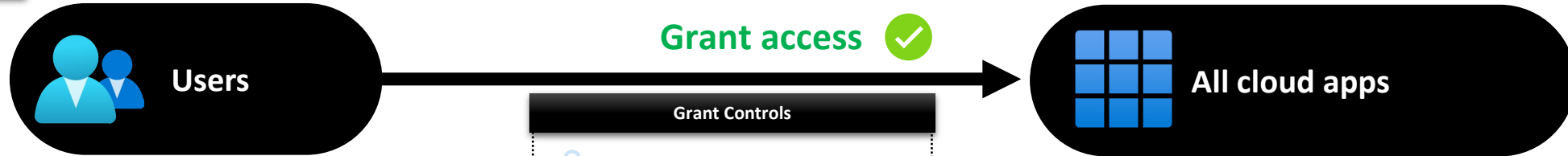
Token protection for session



CA099-Prod-BreakGlassAccounts-AllApps-AnyPlatform-FIDO-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-BreakGlassAccounts-Req-FIDO-All-Dynamic (2)
- Users**
- Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

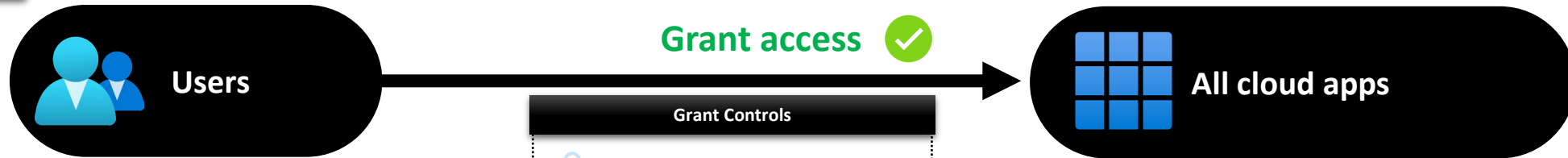
- ✓ **Include:**
- All

- 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

CA100-Prod-Admins-Internal-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Admins-Internal-All-Dynamic (5)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA100-Admins-Internal-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

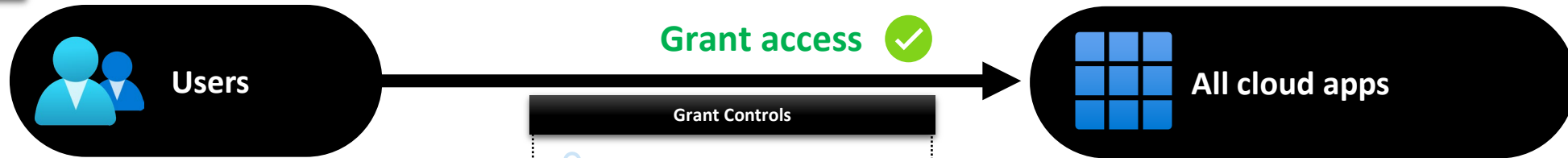
- Include:**
- All



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










CA101-Prod-Admins-Internal-AllApps-AnyPlatform-PersistentBrowser-Enforce


Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-Admins-Internal-All-Dynamic (5)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA101-Admins-Internal-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

CA102-Prod-Admins-Internal-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12

**Risk**
Sign-in risk:

- High
- Medium

**Device platforms**
Not configured

**Client apps**
Not configured

**Filter for devices**
Not configured

**Locations**
Not configured





Users










Grant access 



All cloud apps








-  **Include:**
- Groups**
- Entra-CA-Admins-Internal-Req-MFA-All-Dynamic (4)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA102-Admins-Internal-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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










CA103-Prod-Admins-Internal-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-Admins-Internal-Req-MFA-All-Dynamic (4)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA103-Admins-Internal-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

CA104-Prod-Admins-Internal-RegisterSecurityInfo-AnyPlatform-FIDO-Allow


Policy Enabled


Last modified: 2025-01-12

 Risk
Not configured

 Device platforms
Not configured

 Client apps
Not configured

 Filter for devices
Not configured

 Locations
☒ Include
- AllTrusted



Users










Grant access 

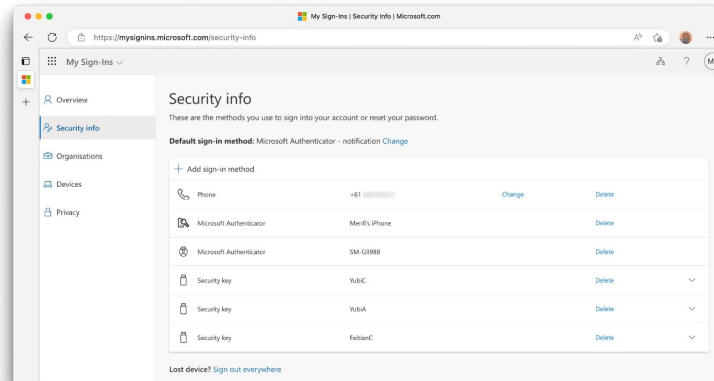


Register security information








- ☒ **Include:**
- Groups**
- Entra-CA-Admins-Internal-Req-FIDO-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA104-Admins-Internal-RegisterSecurityInfo-AnyPlatform-FIDO-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

Grant Controls

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



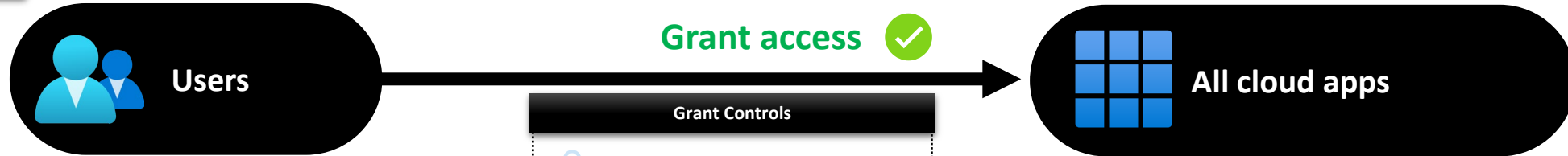
Session Controls

-  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

CA105-Prod-Admins-Internal-AllApps-AnyPlatform-FIDO-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Admins-Internal-Req-FIDO-All-Dynamic (1)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA105-Admins-Internal-AllApps-AnyPlatform-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- Grant Controls**
- Multifactor authentication
 - Auth strength:FIDO Security Key & TAP
 - 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



CA106-Prod-Admins-Internal-AdminPortals-AnyPlatform-FIDO-PAW-Enforce

Policy Enabled

Last modified: 2025-05-03



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Include when
device.extensionAttribute6 -eq
"W365-PAW-Windows-Client-
EntraJoined-Tier0-English" -or
device.extensionAttribute6 -eq
"AutoPilot-PAW-Windows-Client-
EntraJoined-Tier0-English"



Locations

Not configured



Users

Grant access



Microsoft Admin
Portals

Include:

Groups

- Entra-CA-Admins-Internal-Req-FIDO-All-Dynamic
(1)

Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA105-Admins-Internal-AllApps-
AnyPlatform-FIDO-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant Controls

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

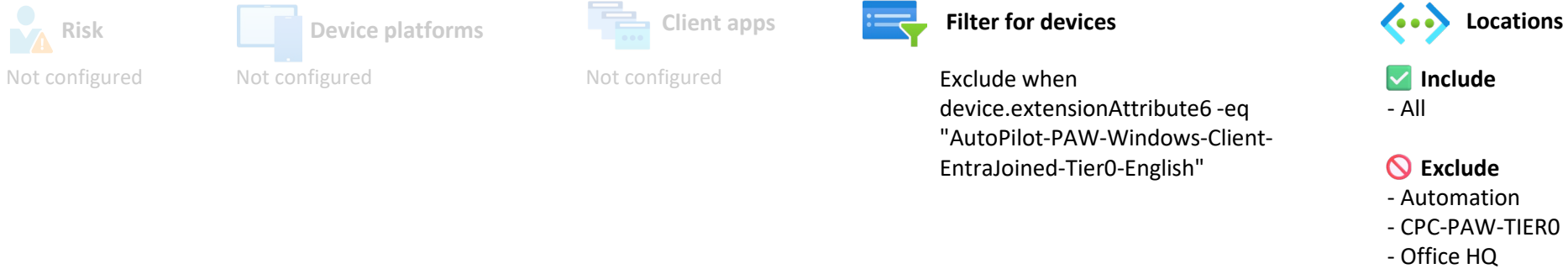
Session Controls

- 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

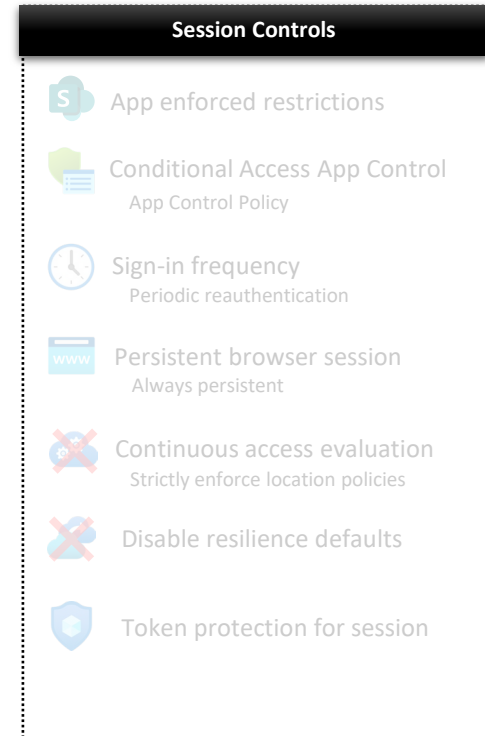
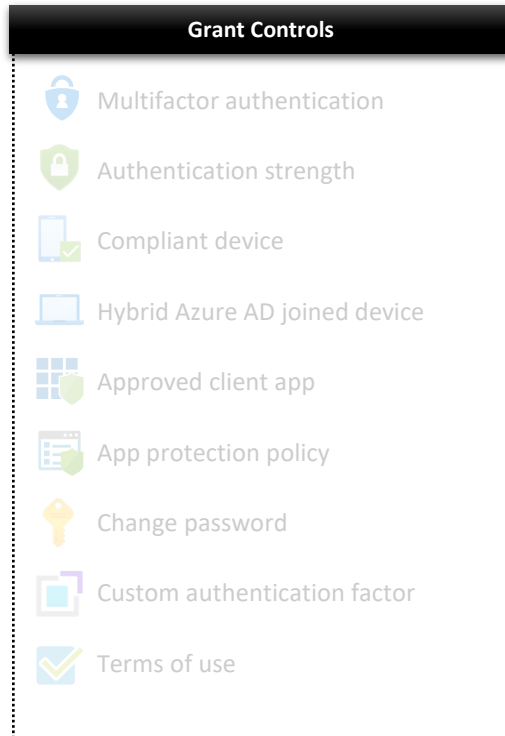
CA107-Prod-Admins-Internal-AdminPortals-AnyPlatform-NonPAWLocations-Block

Policy Enabled

Last modified: 2025-05-03



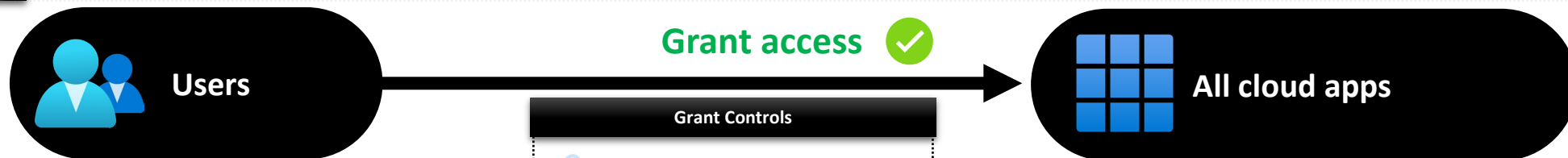
- ☒ **Include:**
 - Groups**
 - Intune-Admins-Internal-All-Dynamic (5)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA600-ServiceAccounts-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA150-Prod-Admins-External-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-Admins-External-All-Dynamic (2)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA150-Admins-External-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

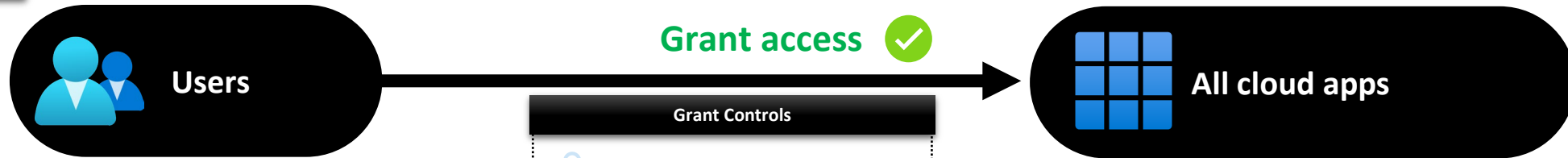
- ✓ **Include:**
- All

- Session Controls**
- App enforced restrictions
 - Conditional Access App Control App Control Policy
 - Sign-in frequency 12 hours
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session

CA151-Prod-Admins-External-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-Admins-External-All-Dynamic (2)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA151-Admins-External-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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



CA152-Prod-Admins-External-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



Risk

Sign-in risk:

- High
- Medium



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Groups

- Entra-CA-Admins-External-Req-MFA-All-Dynamic (2)

✗ Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA152-Admins-External-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant 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

CA153-Prod-Admins-External-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Admins-External-Req-MFA-All-Dynamic (2)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA153-Admins-External-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

CA154-Prod-Admins-External-RegisterSecurityInfo-AnyPlatform-FIDO-Allow

Policy Enabled

Last modified: 2025-01-12



Users

Grant access ✓



Register security information

✓ **Include:**

Groups

- Entra-CA-Admins-External-Req-FIDO-All-Dynamic (0)

✗ **Exclude:**

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA154-Admins-External-RegisterSecurityInfo-AnyPlatform-FIDO-Allow-Excluded-Assigned (0)

Users

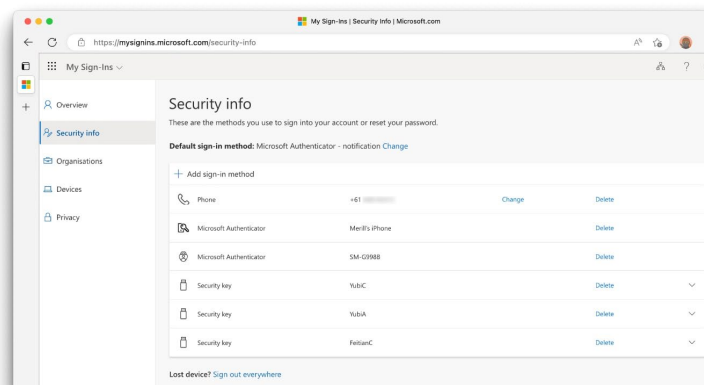
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant Controls

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

Session Controls

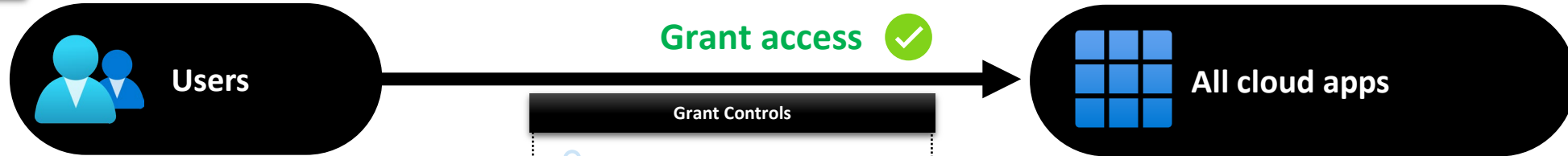
- App enforced restrictions
- Conditional Access App Control App Control Policy
- Sign-in frequency Periodic reauthentication
- Persistent browser session Always persistent
- Continuous access evaluation Strictly enforce location policies
- Disable resilience defaults
- Token protection for session



CA155-Prod-Admins-External-AllApps-AnyPlatform-FIDO-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Admins-External-Req-FIDO-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA155-Admins-External-AllApps-AnyPlatform-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

- Include:**
- All

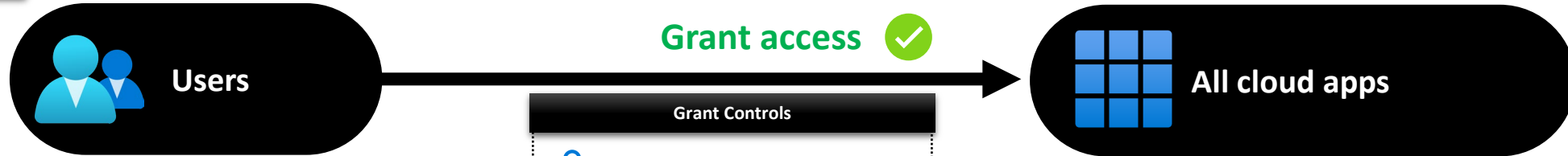
- Session Controls**
- App enforced restrictions
 - Conditional Access App Control App Control Policy
 - Sign-in frequency Periodic reauthentication
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token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



CA200-Prod-Users-Internals-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Users-Internal-Req-MFA-All-Dynamic (13)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA200-Users-Internal-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

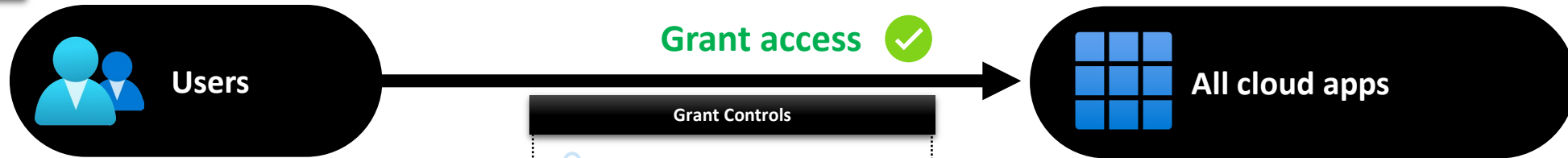
- Include:**
- All

- 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

CA201-Prod-Users-Internal-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled

Last modified: 2025-04-06



- ✓ **Include:**
Groups
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA201-Users-Internal-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

- 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

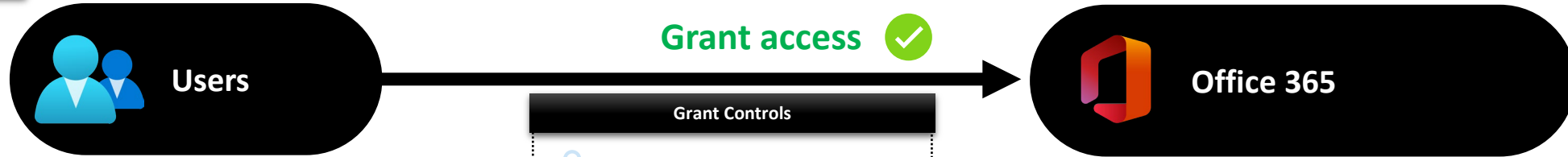
- ✓ **Include:**
- All

- 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

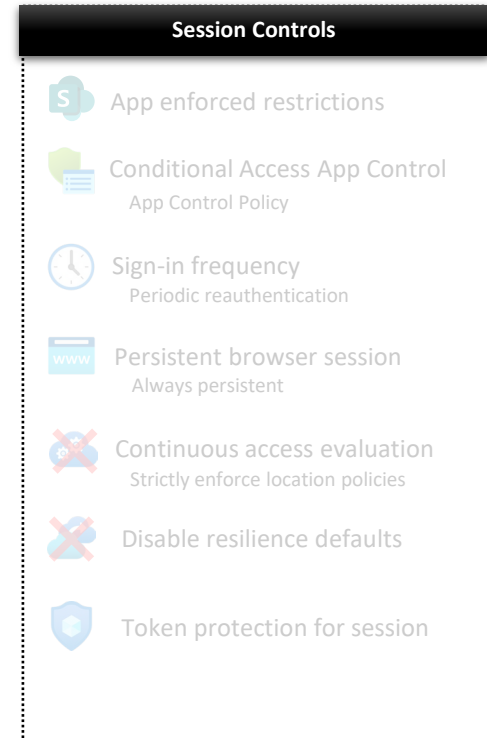
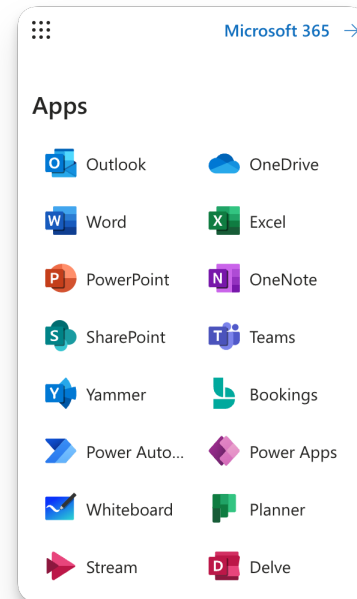
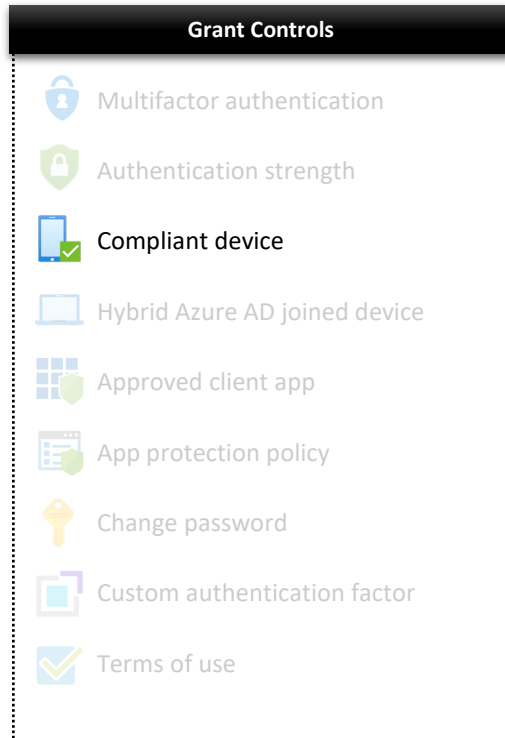
CA202-Prod-Users-Internal-Office365-Windows-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20



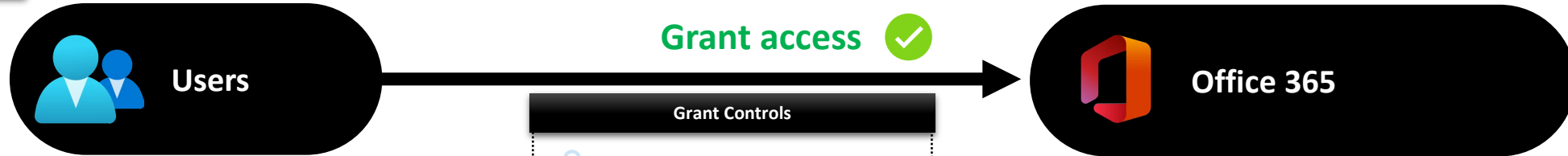
- Include:**
 - Groups**
 - Entra-CA-Users-Internal-All-Dynamic (13)
- Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA202-Users-Internal-Office365-Windows-CompliantDevice-Enforce-Excluded-Assigned (7)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



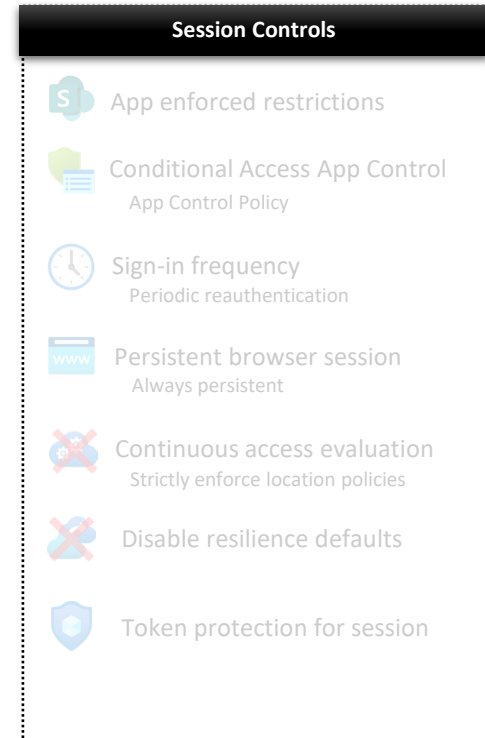
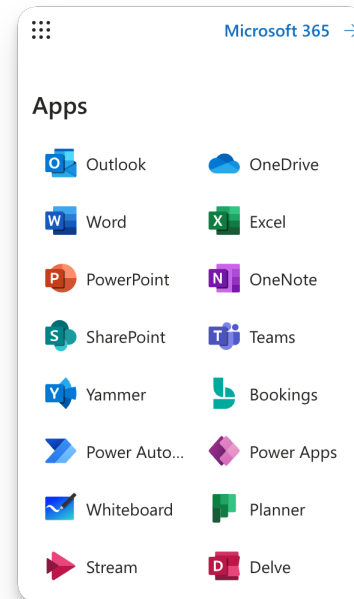
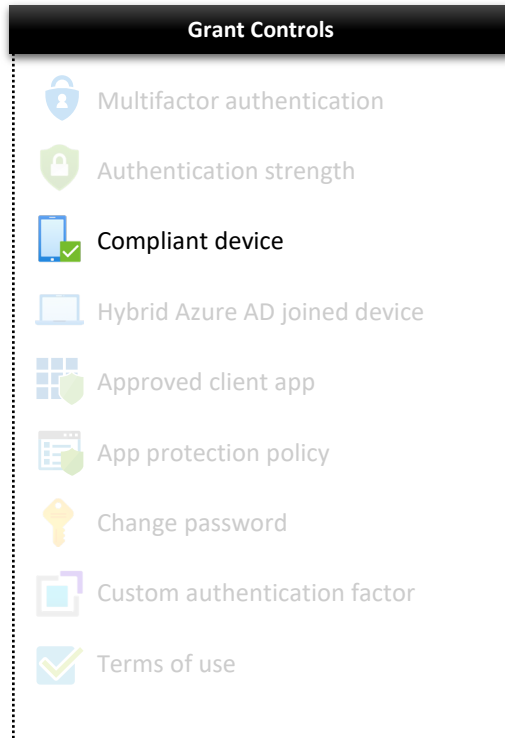
CA203-Prod-Users-Internal-Office365-MacOS-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA203-Users-Internal-Office365-MacOS-CompliantDevice-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)





CA204-Demo-Users-Internal-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-05-03



Risk

Not configured



Device platforms



Include

- Windows
- macOS



Client apps

Not configured



Filter for devices

Include when
device.trustType -ne "AzureAD" -
and device.trustType -ne
"ServerAD"



Locations

Not configured



Users



Include:

Users

- Demo Security



Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA204-Users-Internal-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce-Excluded-Assigned (3)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant 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
Every time



Persistent browser session
Always persistent



Continuous access evaluation
Strictly enforce location policies



Disable resilience defaults



Token protection for session



CA204-Prod-Users-Internal-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-03-17



Risk

Not configured



Device platforms



Include

- Windows
- macOS



Client apps

Not configured



Filter for devices

Include when
device.trustType -ne "AzureAD" -
and device.trustType -ne
"ServerAD"



Locations

Not configured



Users



Include:

Groups

- Entra-CA-Users-Internal-All-Dynamic (13)



Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA204-Users-Internal-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce-Excluded-Assigned (3)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant 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
1 day



Persistent browser session
Always persistent



Continuous access evaluation
Strictly enforce location policies



Disable resilience defaults



Token protection for session

CA205-Prod-Users-Internal-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12

**Risk**
Sign-in risk:

- High
- Medium

**Device platforms**
Not configured

**Client apps**
Not configured

**Filter for devices**
Not configured

**Locations**
Not configured





Users










Grant access 



All cloud apps








-  **Include:**
- Groups**
- Entra-CA-Users-Internal-Req-MFA-All-Dynamic (13)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA205-Users-Internal-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

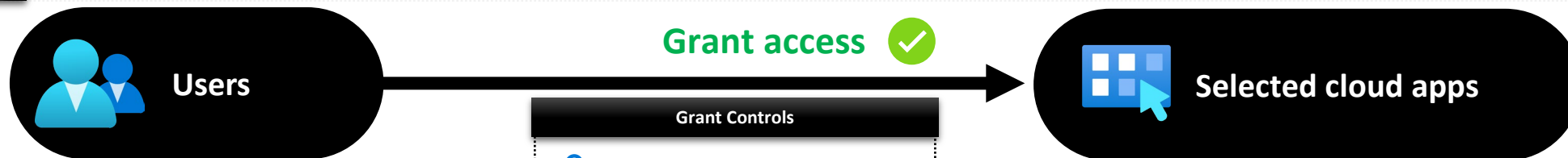
Session Controls

-  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

CA206-Prod-Users-Internal-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Req-MFA-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA206-Users-Internal-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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:**
- 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



CA207-Prod-Users-Internal-Office365-AnyPlatform-Unmanaged-AppEnforcedRestrictions-BlockDownload

Policy Enabled

Last modified: 2025-01-20



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Include when
device.trustType -eq "Workplace"



Locations

Not configured



Users

Grant access



Office 365

Include:

Groups

- Entra-CA-Users-Internal-All-Dynamic (13)

Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)

- Entra-CA-CA207-Users-Internal-Office365-AnyPlatform-Unmanaged-

AppEnforcedRestrictions-BlockDownload-

Excluded-Assigned (1)

Users

- Break Glass Account 0 (Entra ID)

- Break Glass Account 1 (Entra ID)

- Break Glass Account 2 (Entra ID)

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
Block downloads



Sign-in frequency
Periodic reauthentication



Persistent browser session
Always persistent



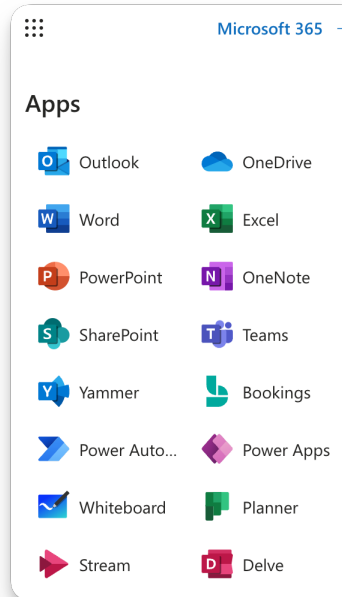
Continuous access evaluation
Strictly enforce location policies



Disable resilience defaults



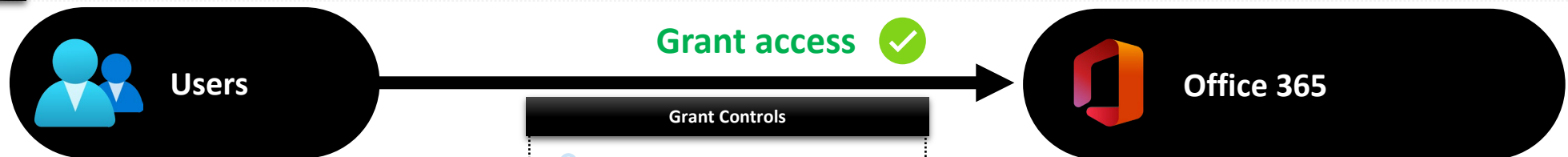
Token protection for session



CA208-Pilot1-Users-Internal-Office365-iOSAndroid-Unmanaged-RequireAppProtection

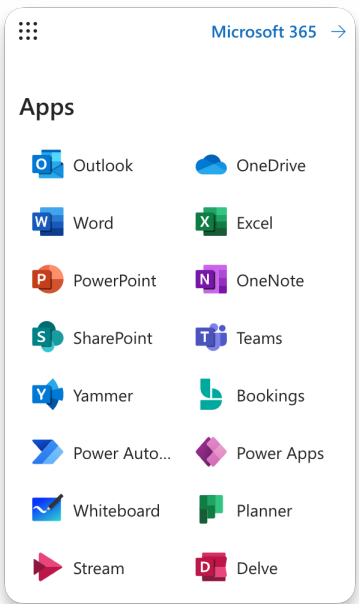
Policy Enabled

Last modified: 2025-03-17



- ✓ **Include:**
Groups
- Entra-CA-CA208-SpecialTest (0)
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA208-Users-Internal-Office365-iOSAndroid-Unmanaged-RequireAppProtection-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

- 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

CA209-Prod-Users-Internal-SelectedApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-04-06



- ✓ **Include:**
 - Groups**
 - Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA209-Users-Internal-SelectedApps-AnyPlatform-Block-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

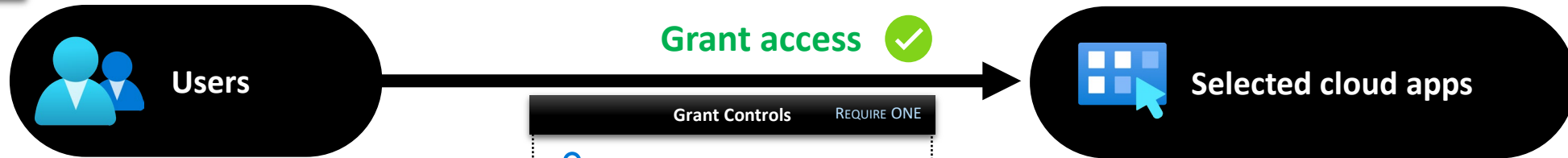
- Grant Controls**
- Multifactor authentication
 - Authentication strength
 - Compliant device
 - Hybrid Azure AD joined device
 - Approved client app
 - App protection policy
 - Change password
 - Custom authentication factor
 - Terms of use

- 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

CA210-Prod-Users-Internal-EntraGSA-Windows-MFACompliant-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Req-MFA-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA210-Users-Internal-EntraGSA-Windows-MFACompliant-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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:**
- Microsoft apps with Global Secure Access
 - Internet resources with Global Secure Access

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

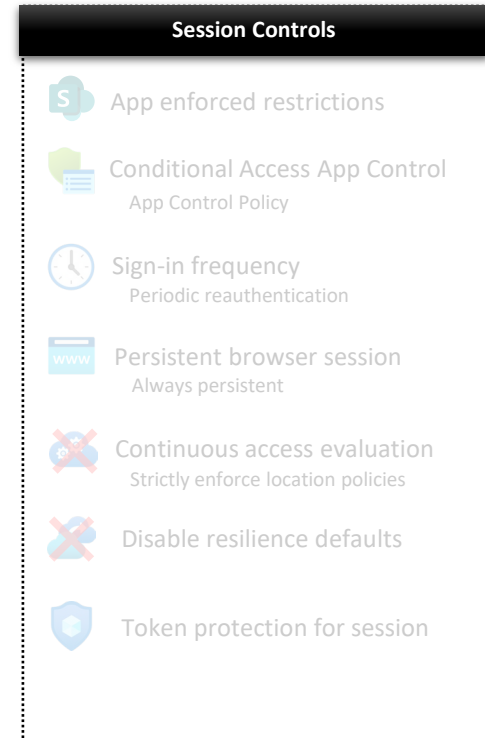
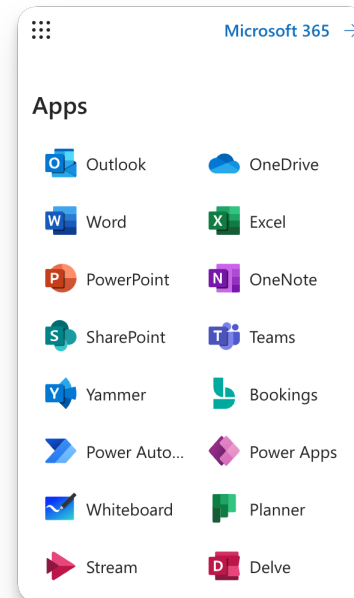
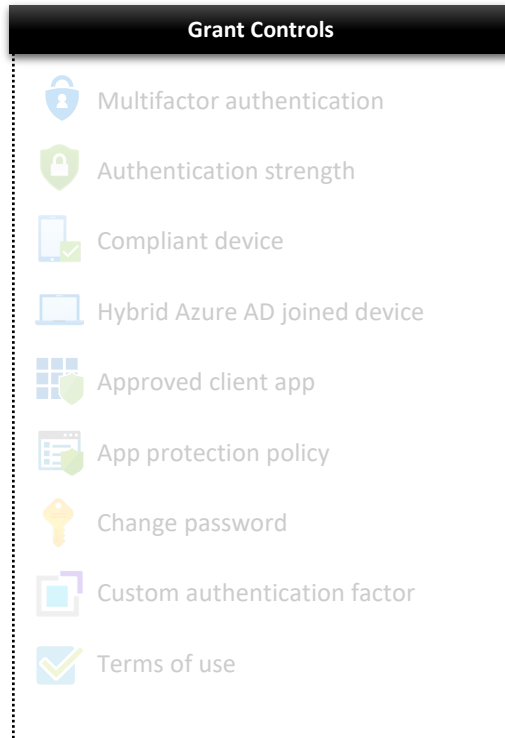
CA211-Prod-Users-Internal-Office365-InsiderRiskElevated-Block

Policy Enabled

Last modified: 2025-01-12



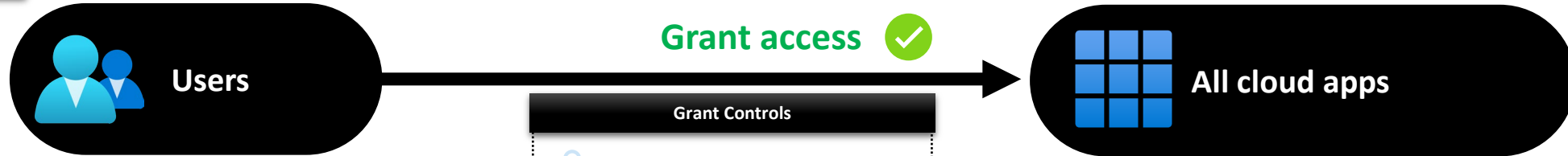
- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA211-Users-Internal-Office365-InsiderRiskElevated-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA212-Prod-Users-Internal-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-03-16



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA212-Users-Internal-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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 30 days
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session

CA250-Prod-Users-Internal-Developers-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



- Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-Req-MFA-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA250-Users-Internal-Developers-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

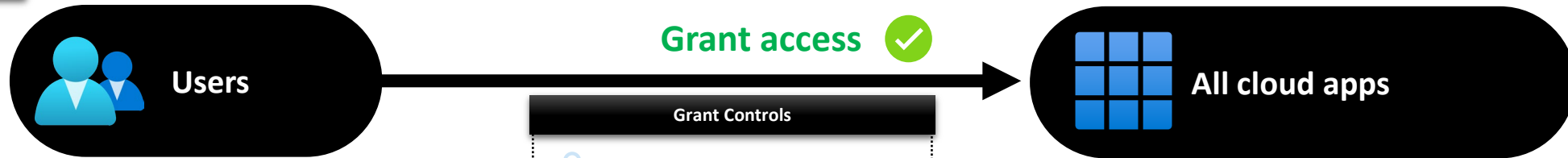
- Include:**
- All

- 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

CA251-Prod-Users-Internal-Developers-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled

Last modified: 2025-01-15



- Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA251-Users-Internal-Developers-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

CA252-Prod-Users-Internal-Developers-Office365-Windows-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20

Risk Not configured

Device platforms ☒ **Include**
- All

☐ **Exclude**
- Android
- iOS
- macOS
- Linux

Client apps Not configured

Filter for devices Not configured

Locations Not configured



Users

Grant access ☒



Office 365

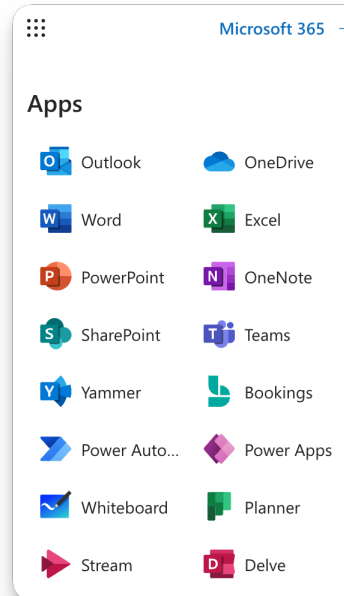
- ☒ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA252-Users-Internal-Developers-Office365-Windows-CompliantDevice-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

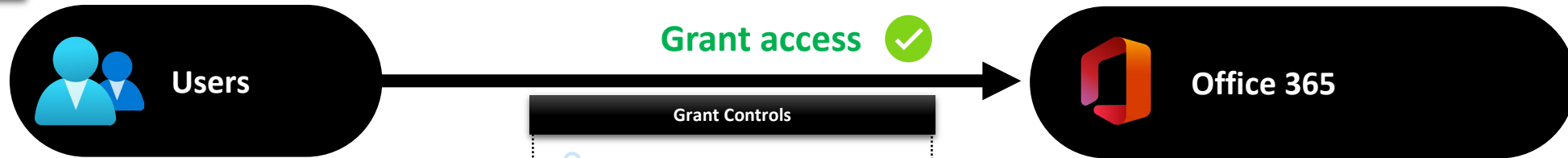
- ☐ App enforced restrictions
- ☐ Conditional Access App Control App Control Policy
- ☐ Sign-in frequency Periodic reauthentication
- ☐ Persistent browser session Always persistent
- ☐ Continuous access evaluation Strictly enforce location policies
- ☐ Disable resilience defaults
- ☐ Token protection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



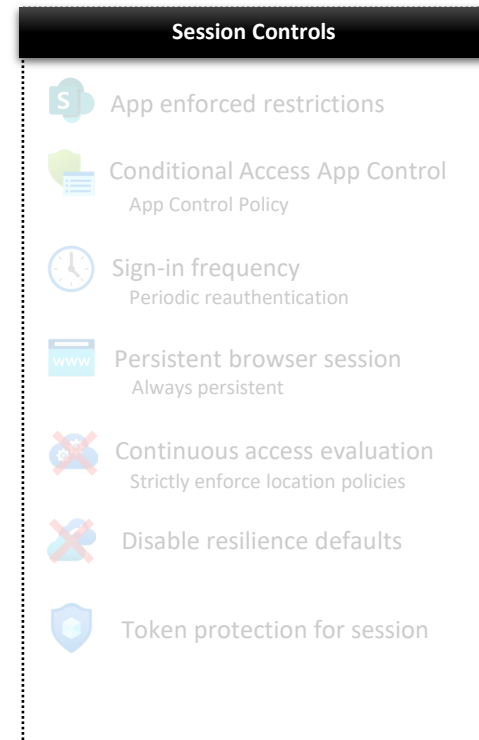
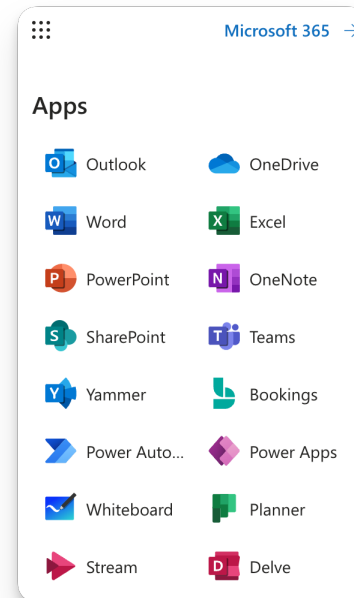
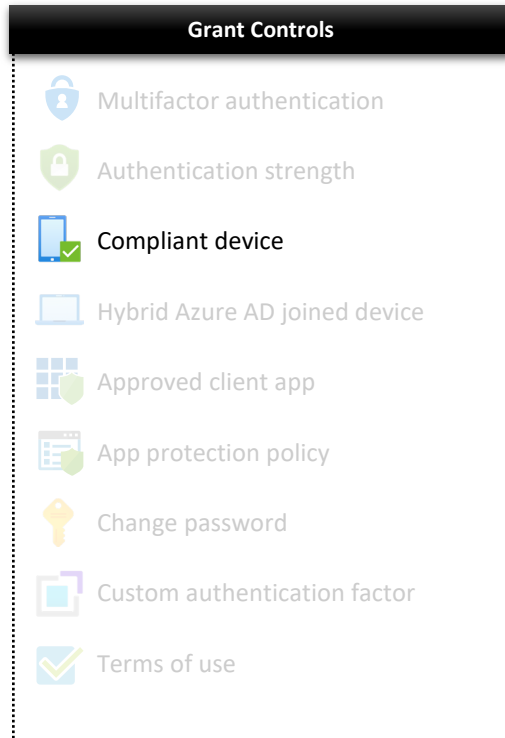
CA253-Prod-Users-Internal-Developers-Office365-MacOS-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20



- ✓ Include:
- Groups**
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ Exclude:
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA253-Users-Internal-Developers-Office365-MacOS-CompliantDevice-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA254-Prod-Users-Internal-Developers-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-15

 **Risk**
Not configured

 **Device platforms**
☒ **Include**

-  Windows
-  macOS

 **Client apps**
Not configured










 **Filter for devices**
Not configured

 **Locations**
Not configured










- ☒ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA254-Users-Internal-Developers-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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
1 day
-  Persistent browser session
Always persistent
-  Continuous access evaluation
Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session



CA255-Prod-Users-Internal-Developers-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



Risk

Sign-in risk:

- High
- Medium



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Groups

- Entra-CA-Users-Internal-Developers-Req-MFA-All-Dynamic (0)

✗ Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA255-Users-Internal-Developers-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant 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



CA256-Prod-Users-Internal-Developers-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

Grant access



Selected cloud apps

Include:

Groups

- Entra-CA-Users-Internal-Developers-Req-MFA-All-Dynamic (0)

Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA256-Users-Internal-Developers-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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:

- 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



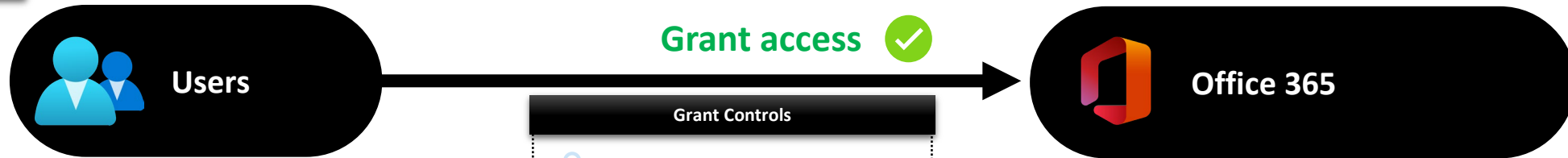
Token protection for session



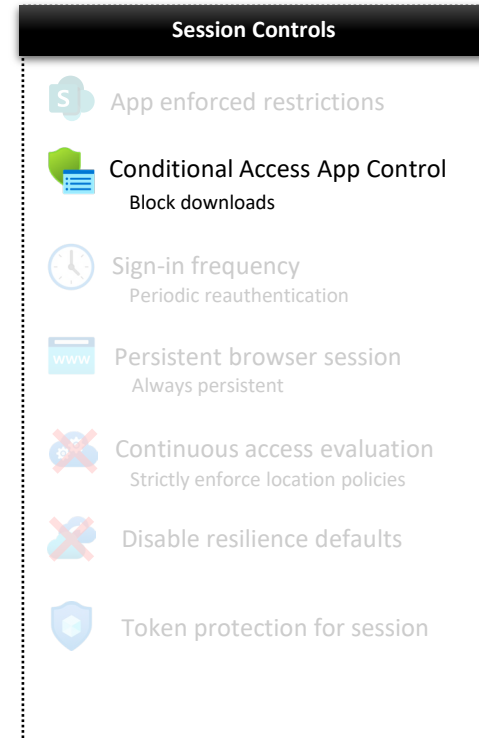
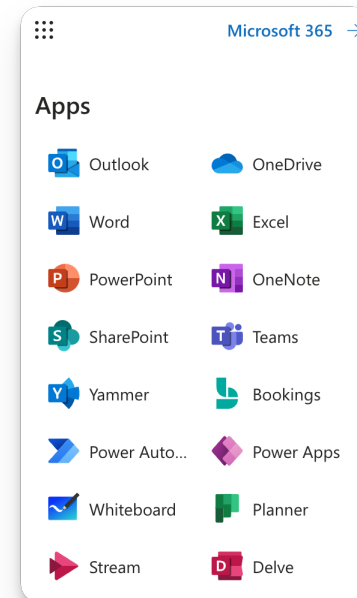
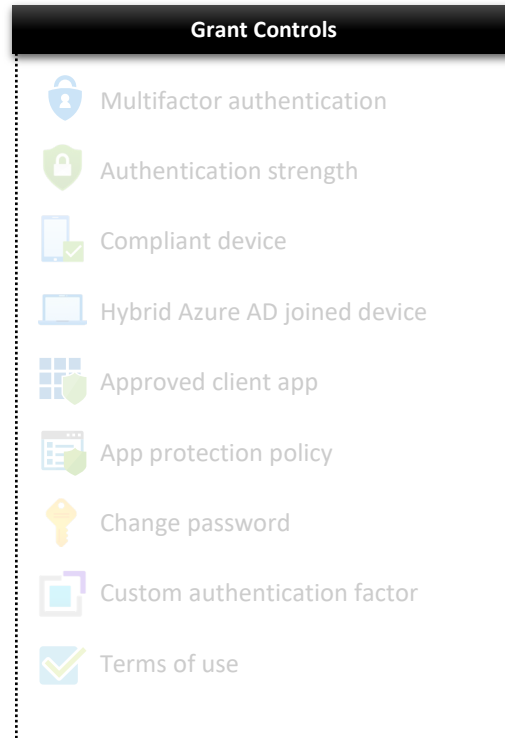
CA257-Prod-Users-Internal-Developers-Office365-AnyPlatform-Unmanaged-AppEnforcedRestrictions-BlockDownload

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA257-Users-Internal-Developers-Office365-AnyPlatform-Unmanaged-AppEnforcedRestrictions-BlockDownload-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)





CA258-Prod-Users-Internal-Developers-Office365-iOSAndroid-Unmanaged-RequireAppProtection

Policy Enabled

Last modified: 2025-01-15



Users

Grant access ✓

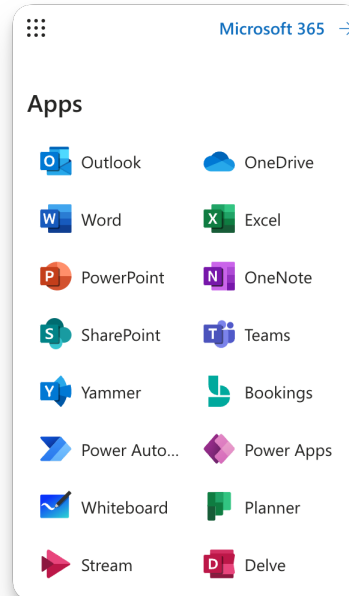


Office 365

- ✓ **Include:**
Groups
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA258-Users-Internal-Developers-Office365-iOSAndroid-Unmanaged-RequireAppProtection-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

CA259-Prod-Users-Internal-Developers-SelectedApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA259-Users-Internal-Developers-SelectedApps-AnyPlatform-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

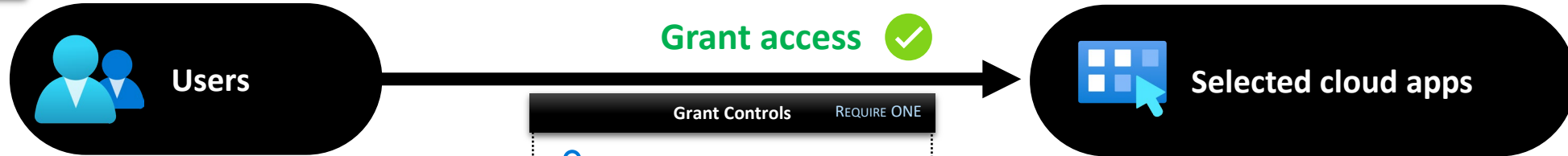
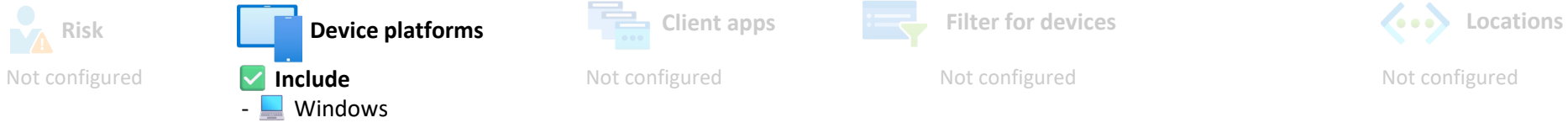
- Grant Controls**
- Multifactor authentication
 - Authentication strength
 - Compliant device
 - Hybrid Azure AD joined device
 - Approved client app
 - App protection policy
 - Change password
 - Custom authentication factor
 - Terms of use

- 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

CA260-Prod-Users-Internal-Developers-EntraGSA-Windows-MFACompliant-Enforce

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Req-MFA-All-Dynamic (13)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA260-Users-Internal-Developers-EntraGSA-Windows-MFACompliant-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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:**
- Microsoft apps with Global Secure Access
 - Internet resources with Global Secure Access

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

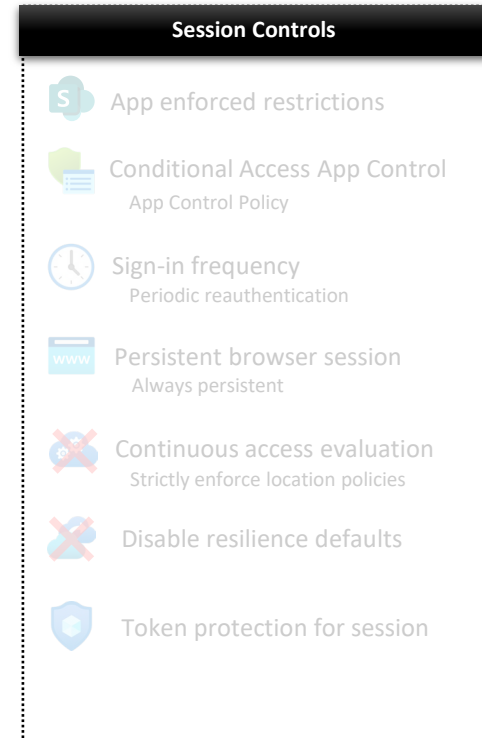
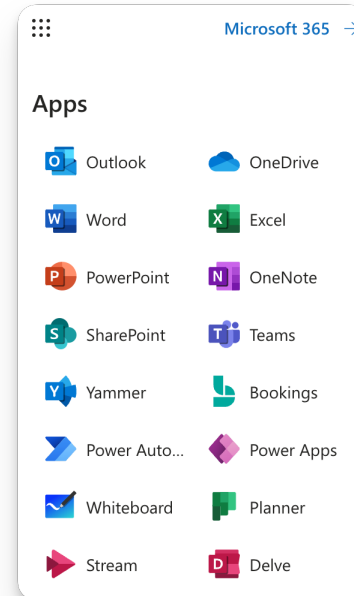
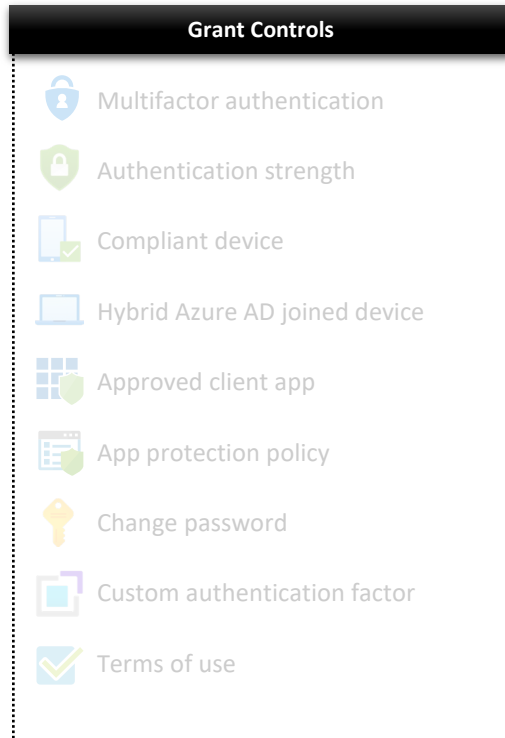
CA261-Prod-Users-Internal-Developers-Office365-InsiderRiskElevated-Block

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA261-Users-Internal-Developers-Office365-InsiderRiskElevated-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA262-Prod-Users-Internal-Developers-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-Internal-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA262-Users-Internal-Developers-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

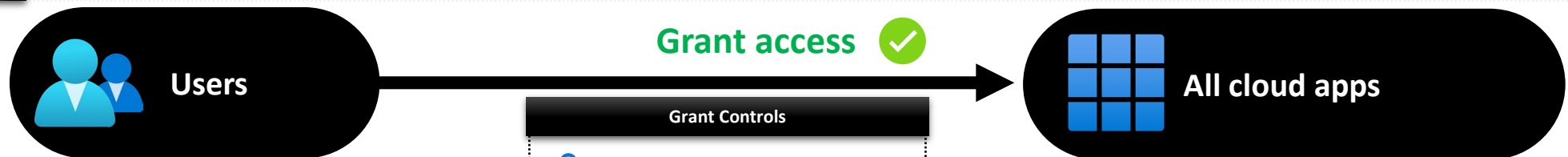
- ✓ **Include:**
- All



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










CA300-Prod-Users-External-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-Users-External-Req-MFA-All-Dynamic (6)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA300-Users-External-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

CA301-Prod-Users-External-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12

 **Risk**
Sign-in risk:

- High
- Medium

 **Device platforms**
Not configured

 **Client apps**
Not configured










 **Filter for devices**
Not configured

 **Locations**
Not configured










- ✓ **Include:**
- Groups**
- Entra-CA-Users-External-Req-MFA-All-Dynamic (6)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA301-Users-External-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

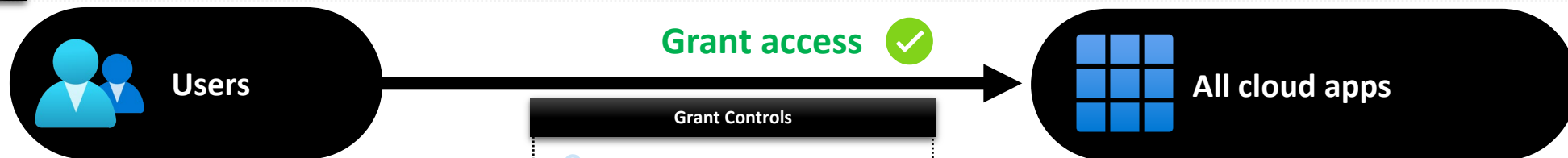
Session Controls

-  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

CA302-Prod-Users-External-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Users-External-All-Dynamic (6)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA302-Users-External-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

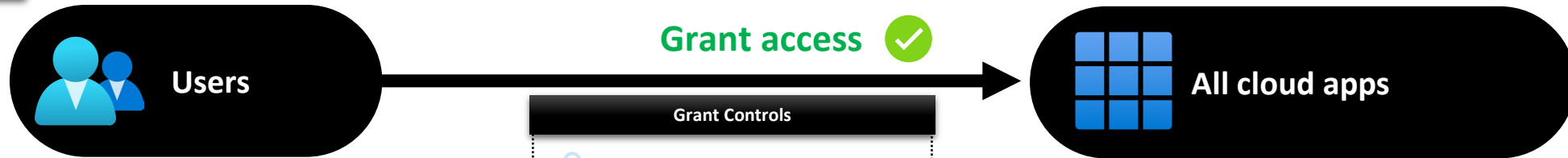
- Include:**
- All



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










CA303-Prod-Users-External-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-Users-External-All-Dynamic (6)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA303-Users-External-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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



CA304-Prod-Users-External-SelectedApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-01-22



Users

Block access 



Azure Active Directory

 **Include:**

Groups

- Entra-CA-Users-External-All-Dynamic (6)

 **Exclude:**










Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA304-Users-External-SelectedApps-AnyPlatform-Block-Excluded-Assigned (0)








Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

CA350-Prod-Users-External-Developers-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



- Include:**
- Groups**
- Entra-CA-Users-External-Developers-Req-MFA-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA350-Users-External-Developers-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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



CA351-Prod-Users-External-Developers-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled

Last modified: 2025-01-15



Users

Grant access



All cloud apps

- Include:**
- Groups**
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA351-Users-External-Developers-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

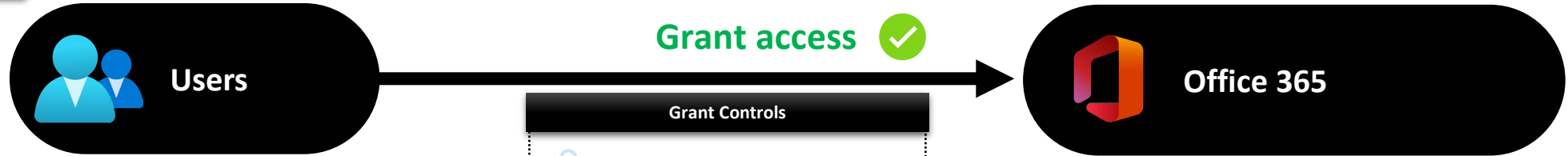
Session Controls

- 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

CA352-Prod-Users-External-Developers-Office365-Windows-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20



- ☒ **Include:**
Groups
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- ☒ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA352-Users-External-Developers-Office365-Windows-CompliantDevice-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

Microsoft 365 →

Apps

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

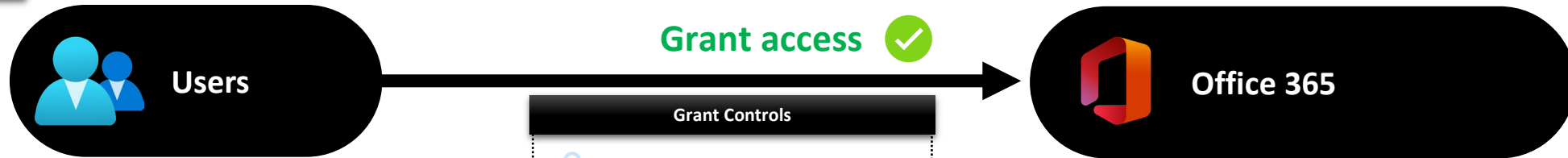
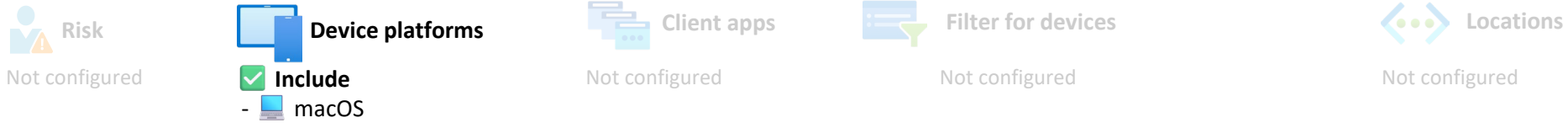
Session Controls

- 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

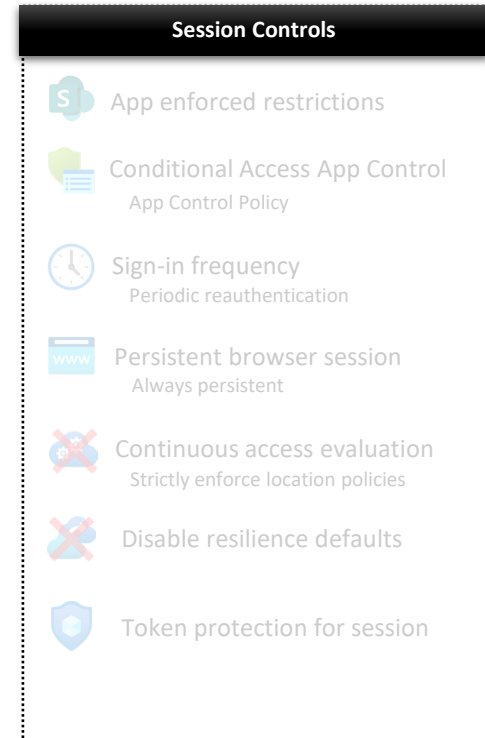
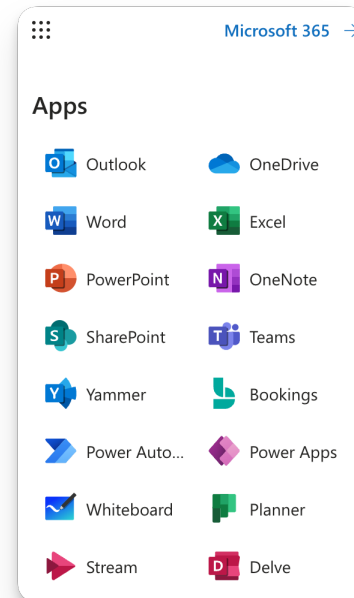
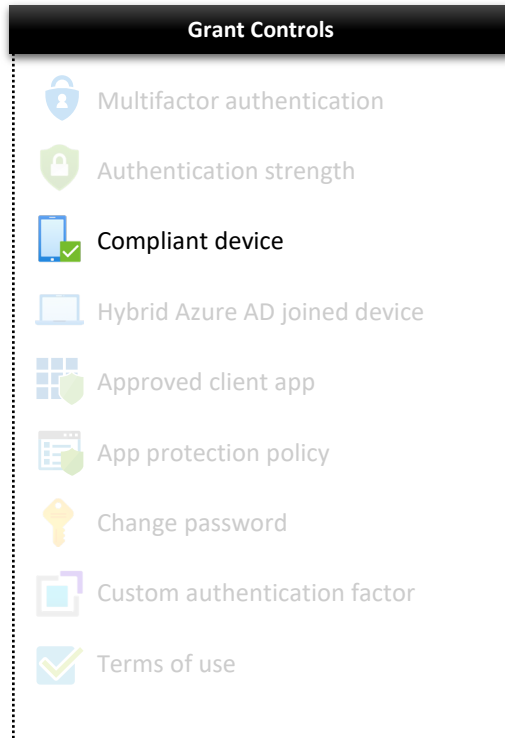
CA353-Prod-Users-External-Developers-Office365-MacOS-CompliantDevice-Enforce

Policy Enabled

Last modified: 2025-01-20



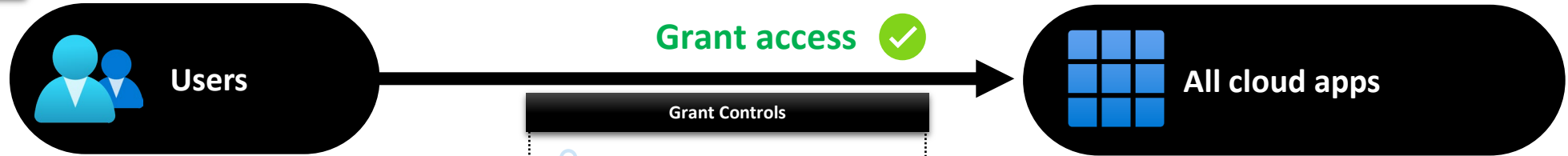
- ✓ **Include:**
Groups
- Entra-CA-Users-Internal-All-Dynamic (13)
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA353-Users-External-Developers-Office365-MacOS-CompliantDevice-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)



CA354-Prod-Users-External-Developers-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-04-06



- ✓ **Include:**
Groups
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- ✗ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA354-Users-External-Developers-AllApps-WindowsMacOS-UnmanagedDevices-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

- 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 1 day
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session



CA355-Prod-Users-External-Developers-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



Risk

Sign-in risk:

- High
- Medium



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

✓ Include:

Groups

- Entra-CA-Users-External-Developers-Req-MFA-All-Dynamic (0)

✗ Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA355-Users-External-Developers-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant 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



CA356-Prod-Users-External-Developers-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-03-16



Users

Grant access



Selected cloud apps

- Include:**
- Groups**
- Entra-CA-Users-External-Developers-Req-MFA-All-Dynamic (0)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA356-Users-External-Developers-MicrosoftIntuneEnrollment-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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:**
- 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



CA357-Prod-Users-External-Developers-Office365-AnyPlatform-Unmanaged-AppEnforcedRestrictions-BlockDownload

Policy Enabled

Last modified: 2025-01-15



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

Grant access 



Office 365

 Include:

Groups

- Entra-CA-Users-External-Developers-All-Dynamic (0)

 Exclude:










Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA357-Users-External-Developers-Office365-AnyPlatform-Unmanaged-AppEnforcedRestrictions-BlockDownload-Excluded-Assigned (0)








Users

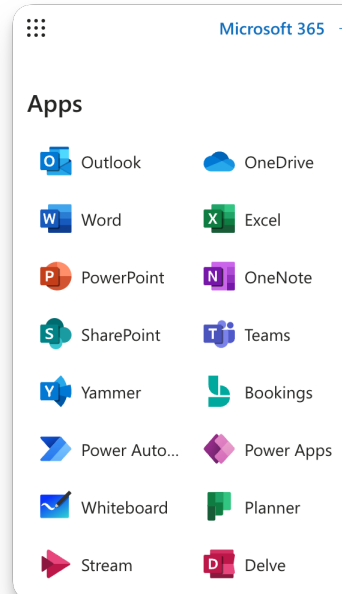
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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
Block downloads
-  Sign-in frequency
Periodic reauthentication
-  Persistent browser session
Always persistent
-  Continuous access evaluation
Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session





CA358-Prod-Users-External-Developers-Office365-iOSAndroid-Unmanaged-RequireAppProtection

Policy Enabled

Last modified: 2025-01-15



Users

Grant access ✓



Office 365

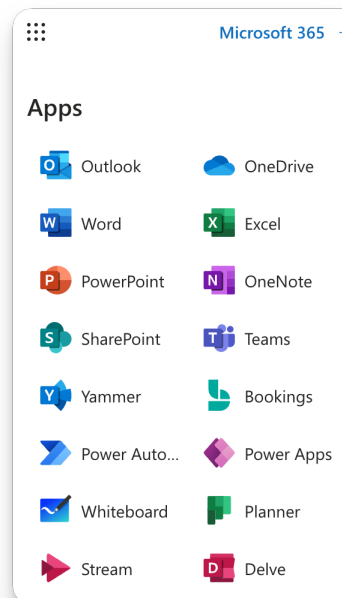
- ✓ **Include:**
- Groups**
 - Entra-CA-Users-External-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA358-Users-External-Developers-Office365-iOSAndroid-Unmanaged-RequireAppProtection-Excluded-Assigned (0)
- Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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



CA359-Prod-Users-External-Developers-SelectedApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA359-Users-External-Developers-SelectedApps-AnyPlatform-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

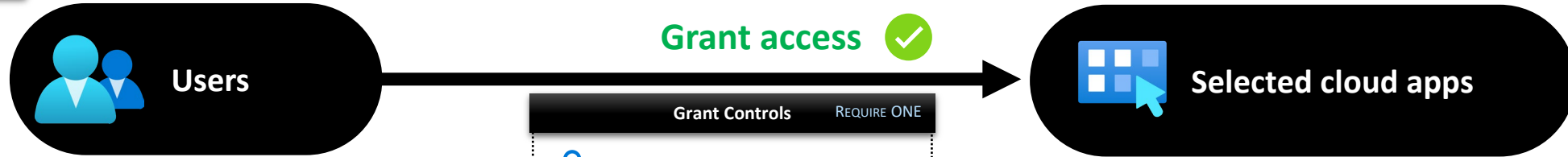
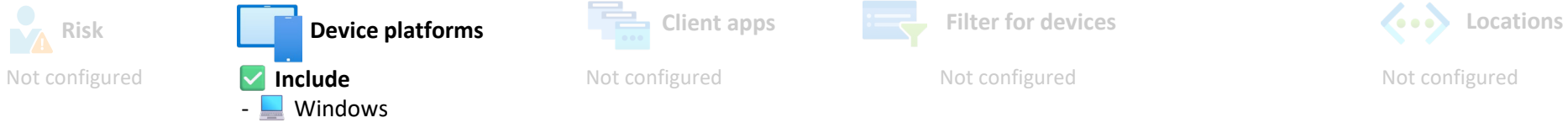
- Grant Controls**
- Multifactor authentication
 - Authentication strength
 - Compliant device
 - Hybrid Azure AD joined device
 - Approved client app
 - App protection policy
 - Change password
 - Custom authentication factor
 - Terms of use

- 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

CA360-Prod-Users-External-Developers-EntraGSA-Windows-MFACompliant-Enforce

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-External-Req-MFA-All-Dynamic (6)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA360-Users-External-Developers-EntraGSA-Windows-MFACompliant-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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:**
- Microsoft apps with Global Secure Access
 - Internet resources with Global Secure Access

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

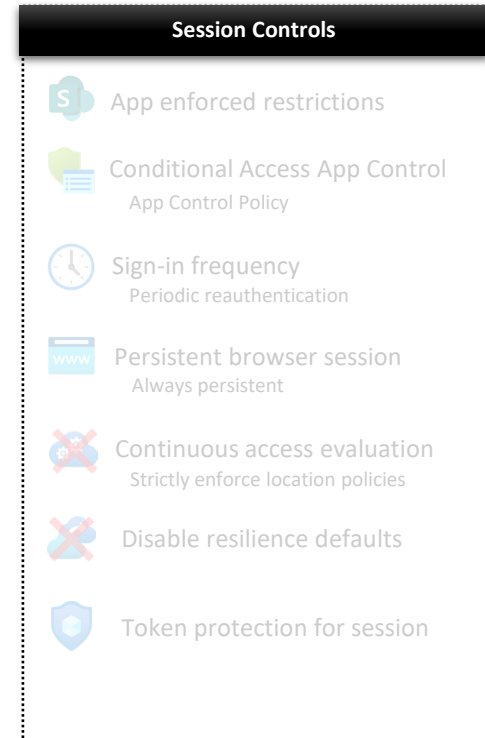
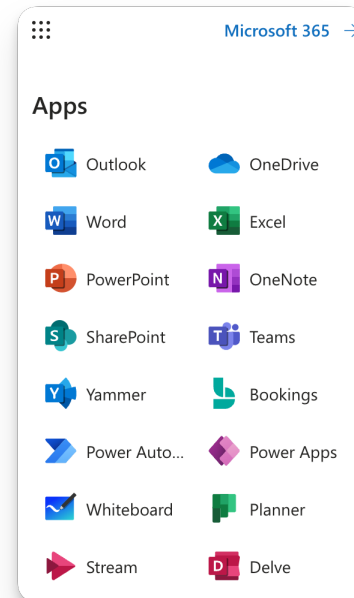
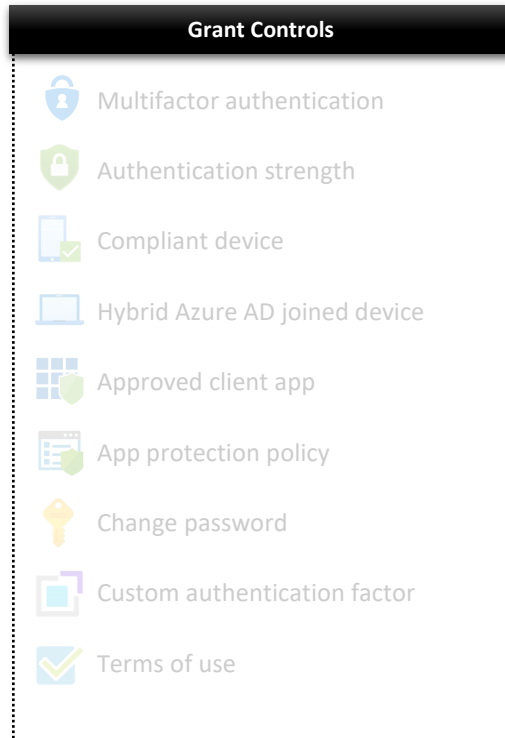
CA361-Prod-Users-External-Developers-Office365-InsiderRiskElevated-Block

Policy Enabled

Last modified: 2025-01-15



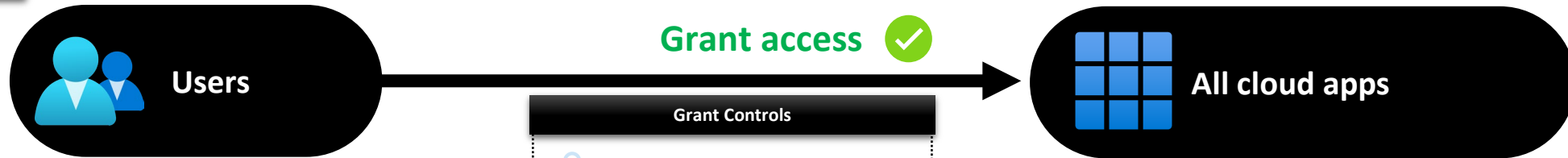
- ✓ **Include:**
- Groups**
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA361-Users-External-Developers-Office365-InsiderRiskElevated-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA362-Prod-Users-External-Developers-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-15



- ✓ **Include:**
- Groups**
- Entra-CA-Users-External-Developers-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA362-Users-External-Developers-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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 1 day
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session



CA400-Prod-Guests-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

Grant access



All cloud apps

Include:

Groups

- Entra-CA-Guests-Req-MFA-All-Dynamic (0)

Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)

- Entra-CA-CA400-Guests-AllApps-AnyPlatform-MFA-Enforce-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)

- Break Glass Account 1 (Entra ID)

- Break Glass Account 2 (Entra ID)

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

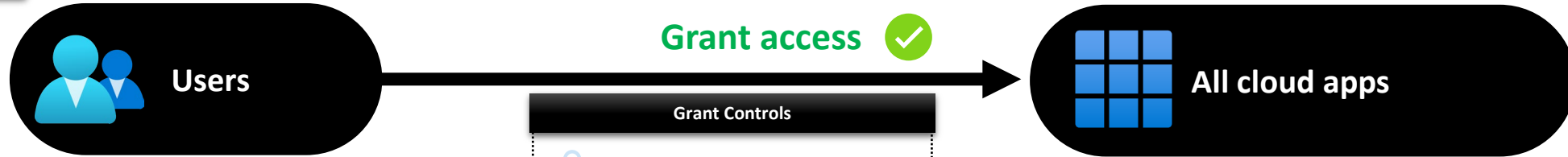


Token protection for session

CA401-Prod-Guests-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-12



- ✓ **Include:**
- Groups**
- Entra-CA-Guests-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA401-Guests-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

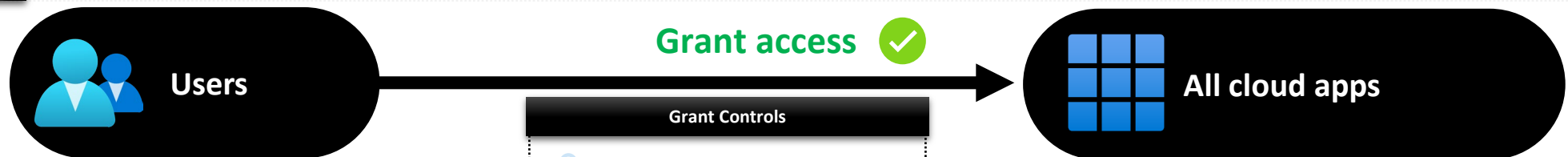
- ✓ **Include:**
- All

- Session Controls**
- App enforced restrictions
 - Conditional Access App Control App Control Policy
 - Sign-in frequency 1 day
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session

CA402-Prod-Guests-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled

Last modified: 2025-01-12



 **Include:**

Groups

- Entra-CA-Guests-All-Dynamic (0)

 **Exclude:**

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)

- Entra-CA-CA402-Guests-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)










Users

- Break Glass Account 0 (Entra ID)

- Break Glass Account 1 (Entra ID)

- Break Glass Account 2 (Entra ID)








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

CA403-Prod-Guests-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce

Policy Enabled

Last modified: 2025-01-12

**Risk**
Sign-in risk:

- High
- Medium

**Device platforms**
Not configured

**Client apps**
Not configured










**Filter for devices**
Not configured

**Locations**
Not configured










- ✓ **Include:**
- Groups**
- Entra-CA-Guests-Req-MFA-All-Dynamic (0)
- ✗ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA403-Guests-AllApps-AnyPlatform-MediumHighSigninRisk-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

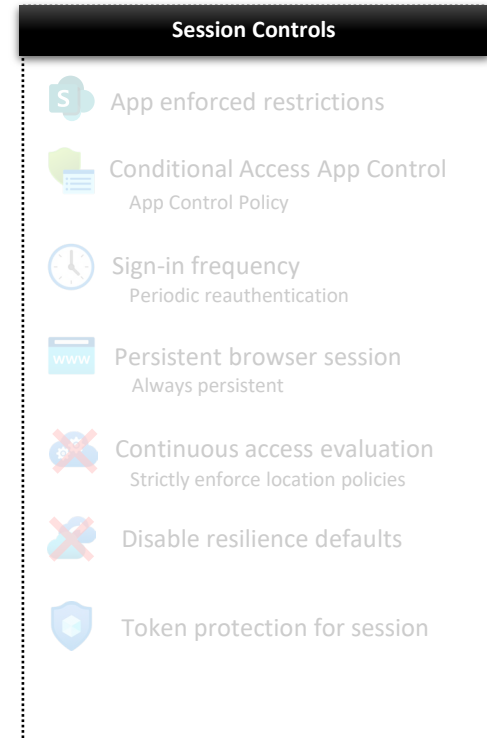
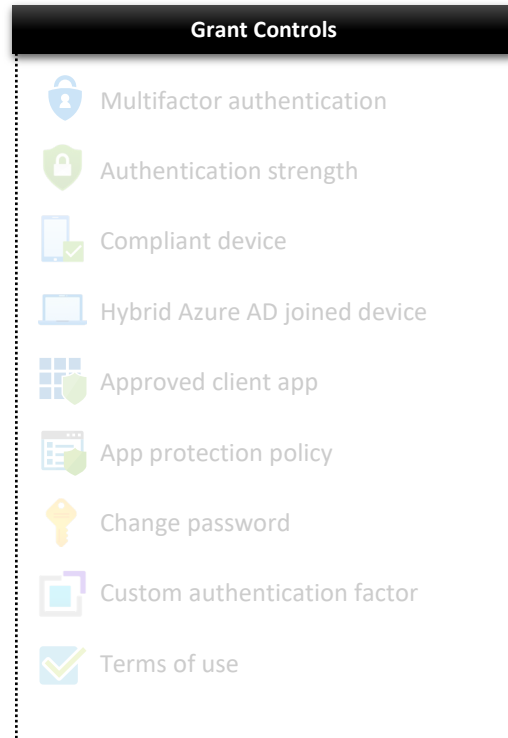
CA404-Prod-Guests-SelectedApps-AnyPlatform-Block

Policy Enabled

Last modified: 2025-04-06



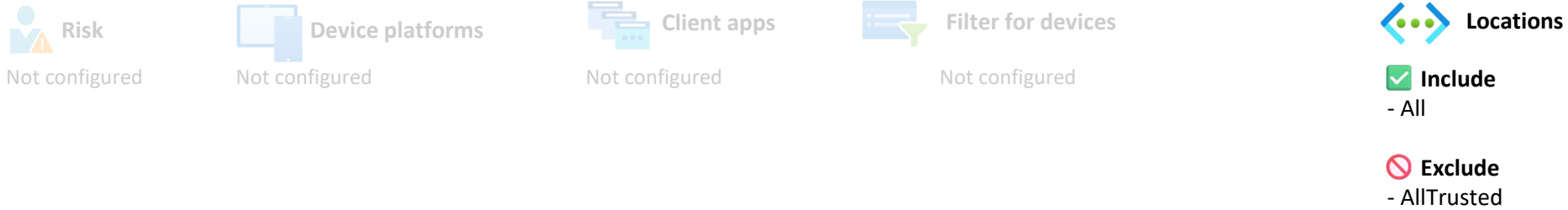
-  **Include:**
- Groups**
- Entra-CA-Guests-All-Dynamic (0)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA404-Guests-SelectedApps-AnyPlatform-Block-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA500-Prod-Shared-Device-Users-AllApps-AnyPlatform-NonTrustedLocations-Block

Policy Enabled

Last modified: 2025-01-29



- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Device-Users-All-Dynamic (4)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA500-Shared-Device-Users-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

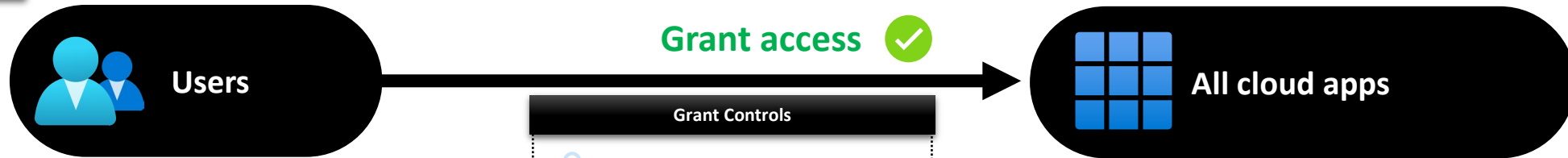
- ☒ **Include:**
 - All

- 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

CA501-Prod-Shared-Device-Users-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-01-12



- Include:**
- Groups**
- Entra-CA-Shared-Device-Users-All-Dynamic (4)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA501-Shared-Device-Users-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

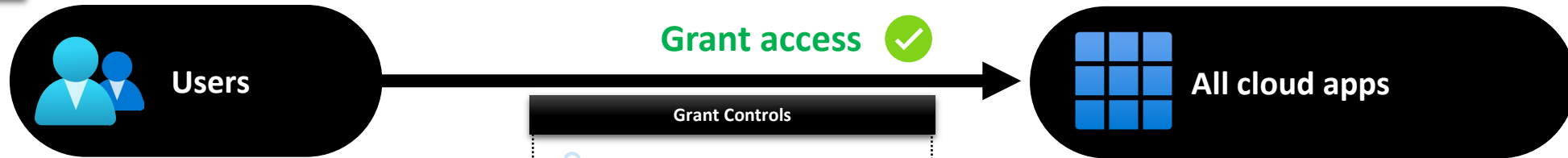
- Include:**
- All



- Session Controls**
- App enforced restrictions
 - Conditional Access App Control App Control Policy
 - Sign-in frequency 1 day
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session










CA502-Prod-Shared-Device-Users-AllApps-AnyPlatform-PersistentBrowser-Enforce

Policy Enabled








Last modified: 2025-01-12



-  **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-All-Dynamic (4)
-  **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA502-Shared-Device-Users-AllApps-AnyPlatform-PersistentBrowser-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

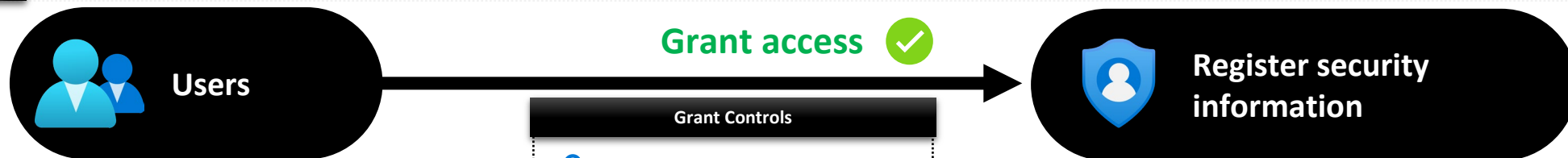
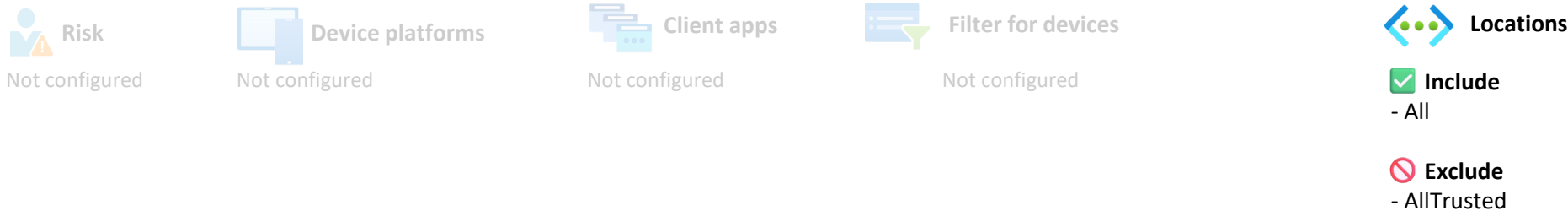
-  **Include:**
- All

- 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

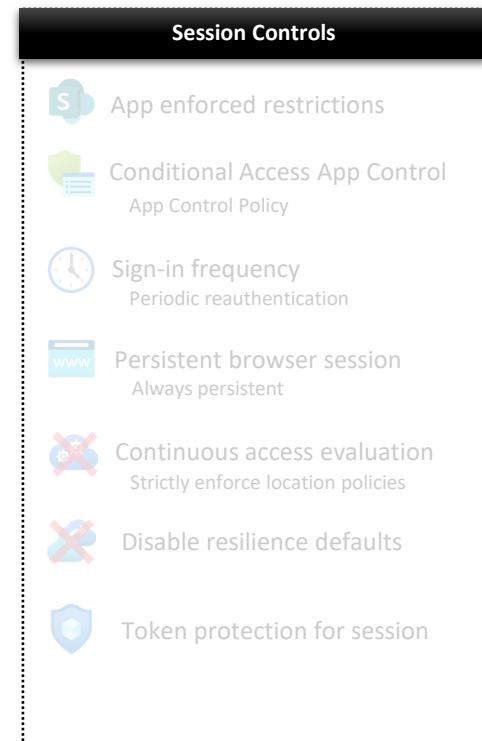
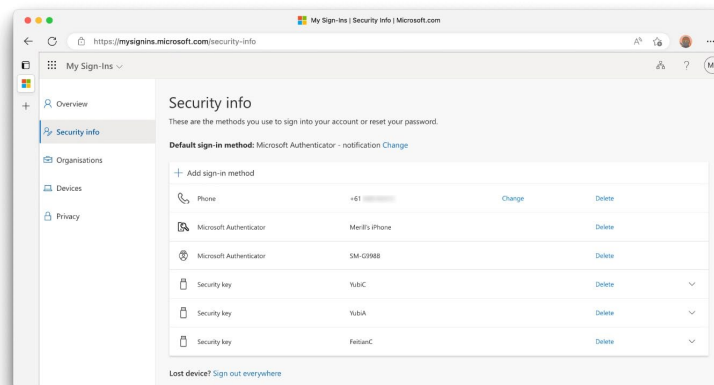
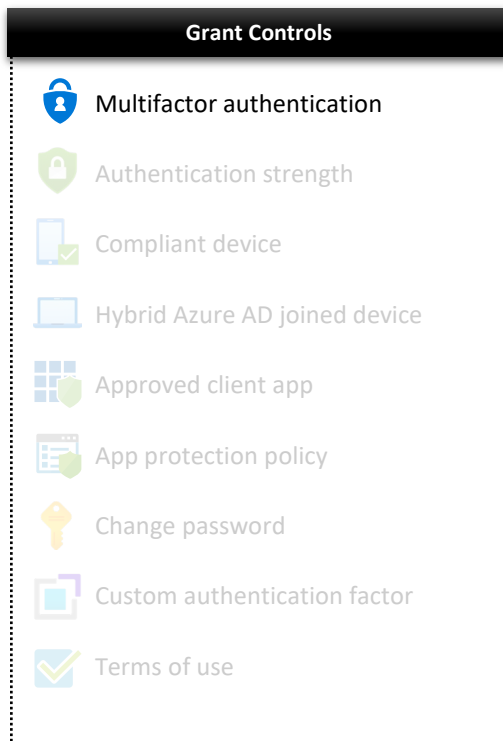
CA503-Prod-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA503-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA504-Prod-Shared-Device-Users-AllApps-TrustedLocations-Pwd-Enforce

Policy Enabled

Last modified: 2025-02-05

 Risk
Not configured

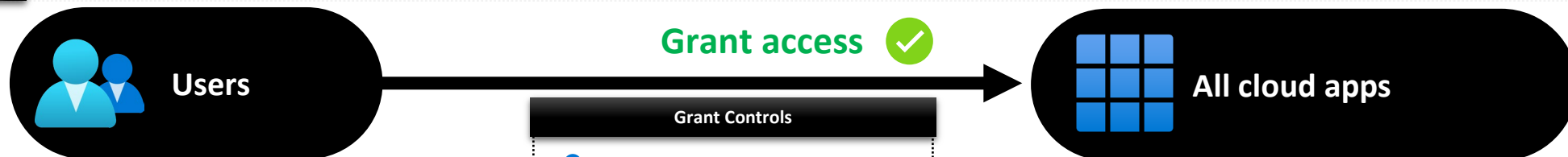
 Device platforms
Not configured

 Client apps
Not configured

 Filter for devices
Not configured


 Locations
☒ Include
- All


☐ Exclude
- AllTrusted





- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA504-Shared-Device-Users-AllApps-TrustedLocations-Pwd-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)


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

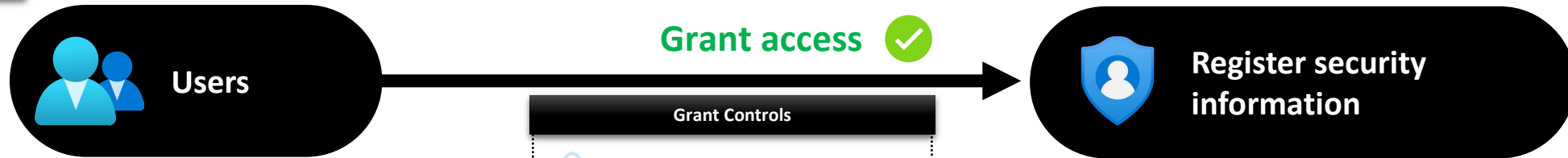
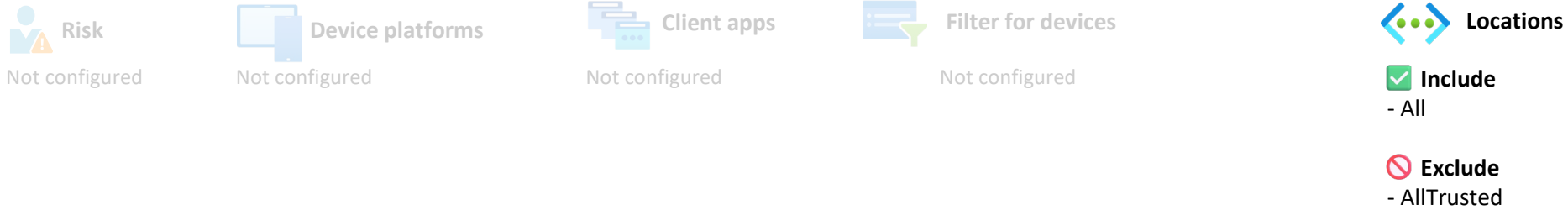
 Disable resilience defaults

 Token protection for session

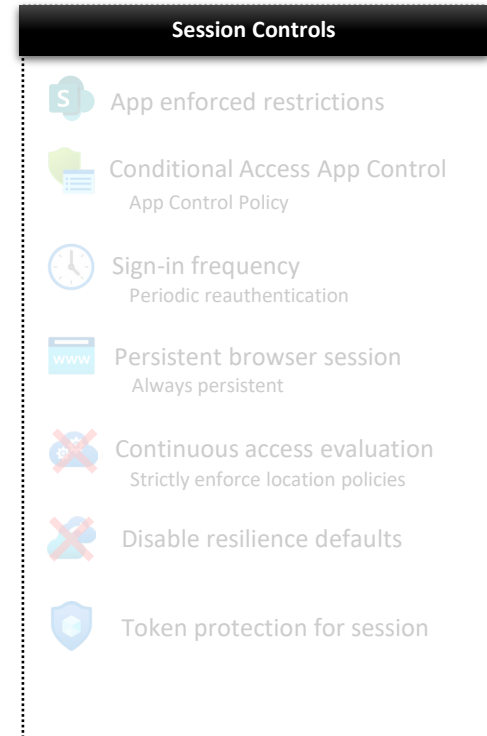
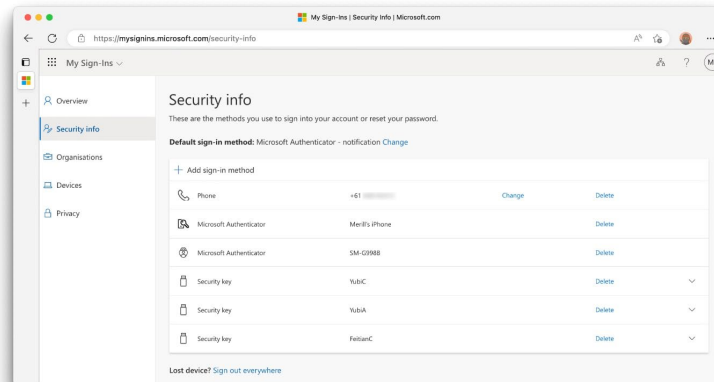
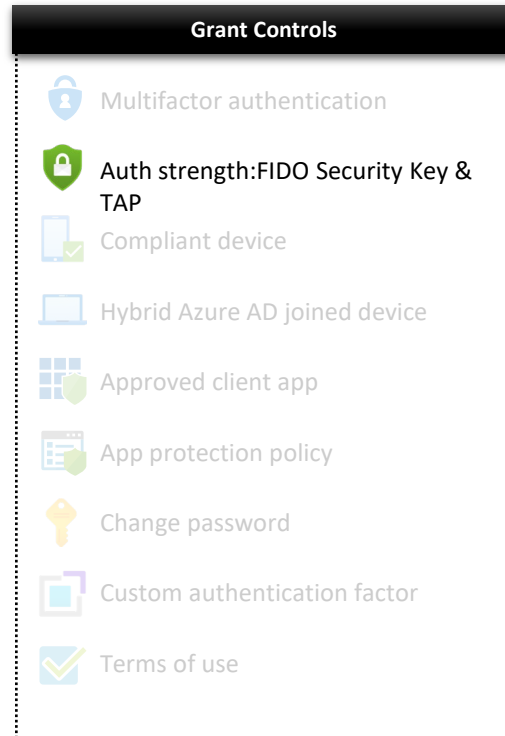
CA505-Prod-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05



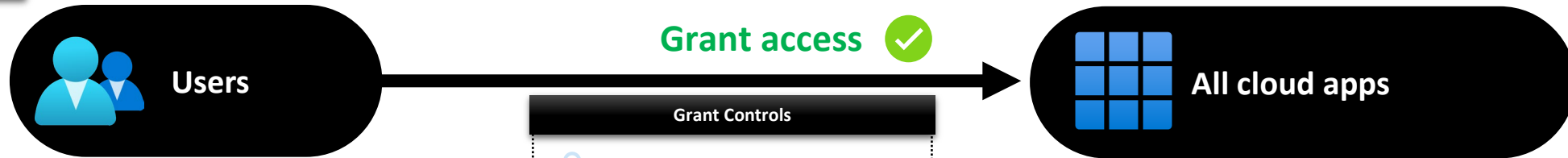
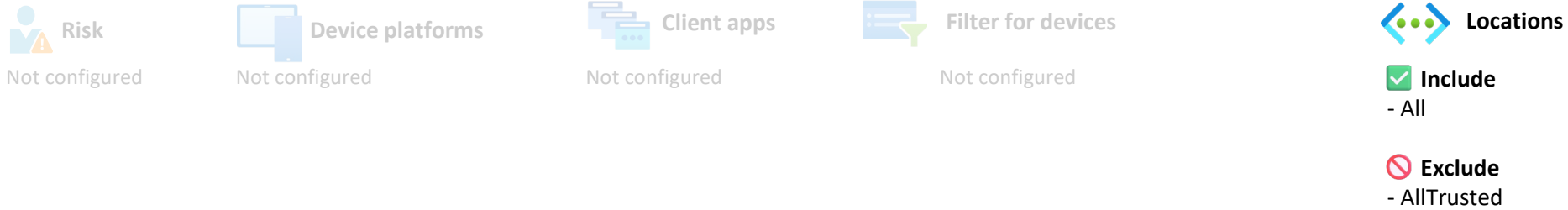
- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Device-Users-Req-FIDO-All-Dynamic (1)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA505-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA506-Prod-Shared-Device-Users-AllApps-TrustedLocations-FIDO-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-FIDO-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA506-Shared-Device-Users-AllApps-TrustedLocations-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

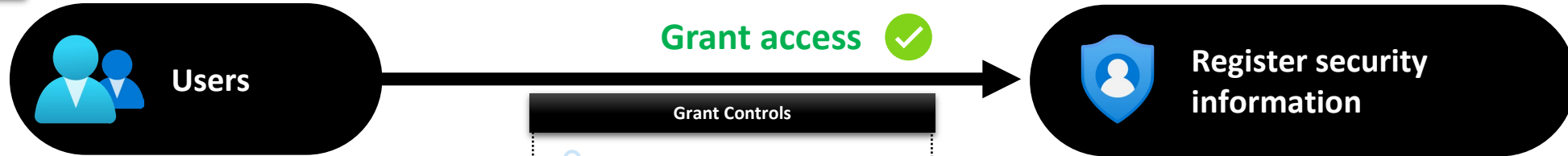
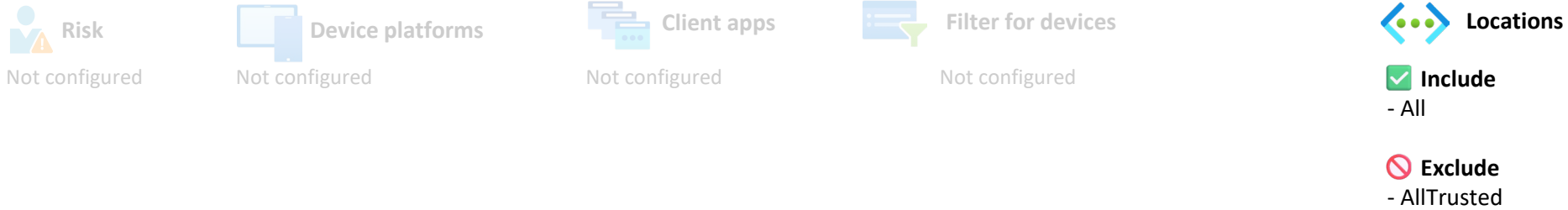
- ☒ **Include:**
- All

- 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

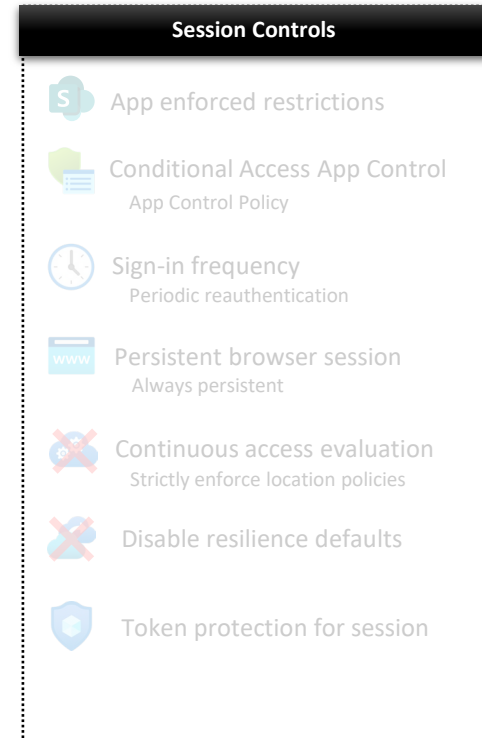
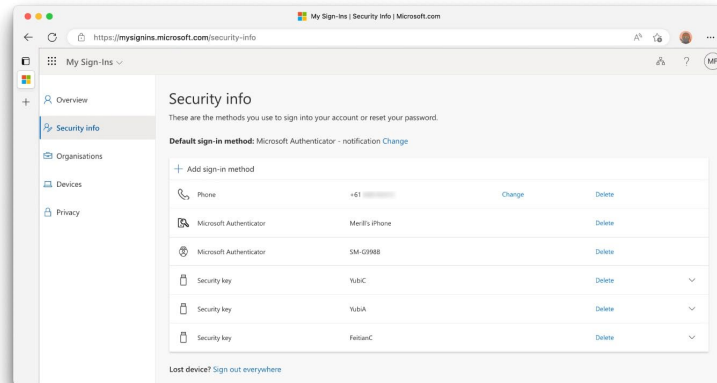
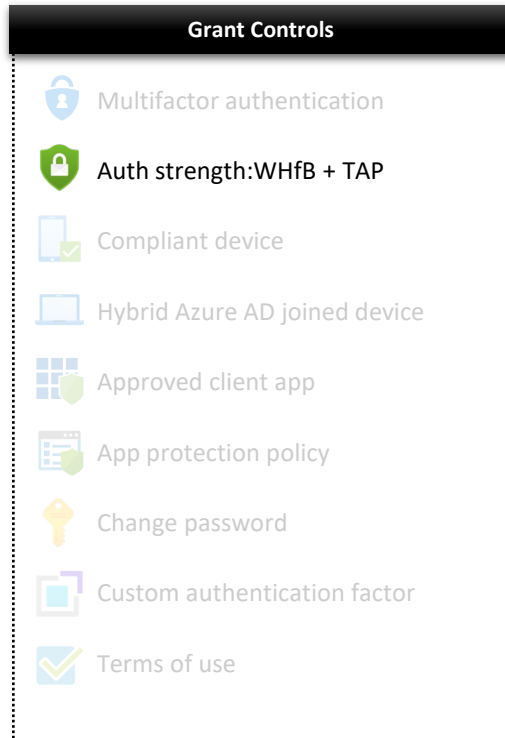
CA507-Prod-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-WHfB-Allow

Policy Enabled

Last modified: 2025-02-05



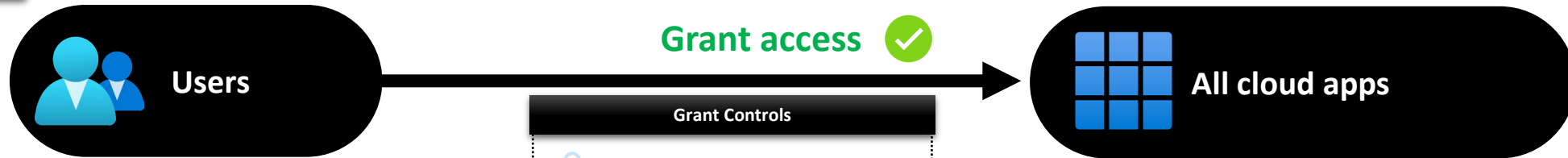
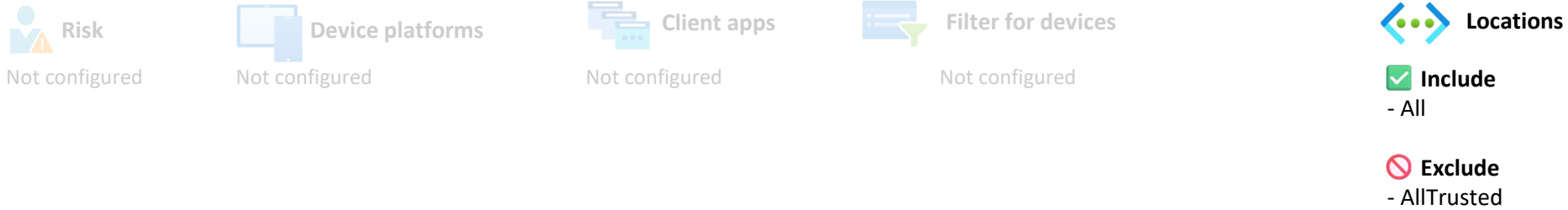
- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Device-Users-Req-WHfB-All-Dynamic (2)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA507-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-WHfB-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



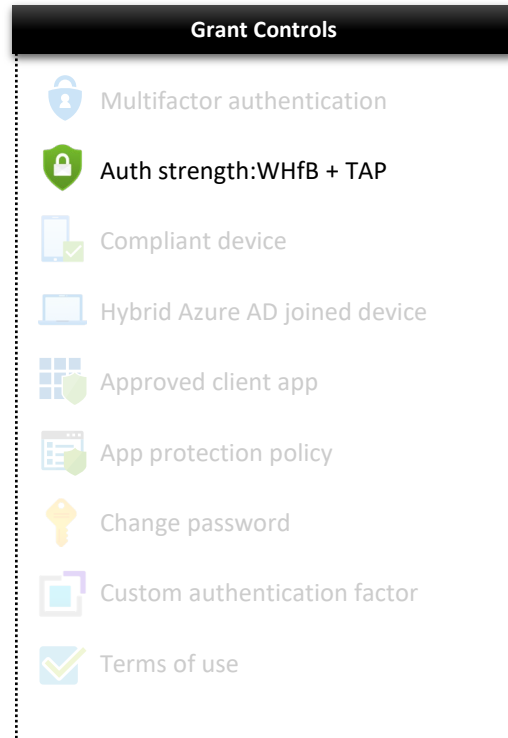
CA508-Prod-Shared-Device-Users-AllApps-TrustedLocations-WHfB-Enforce

Policy Enabled

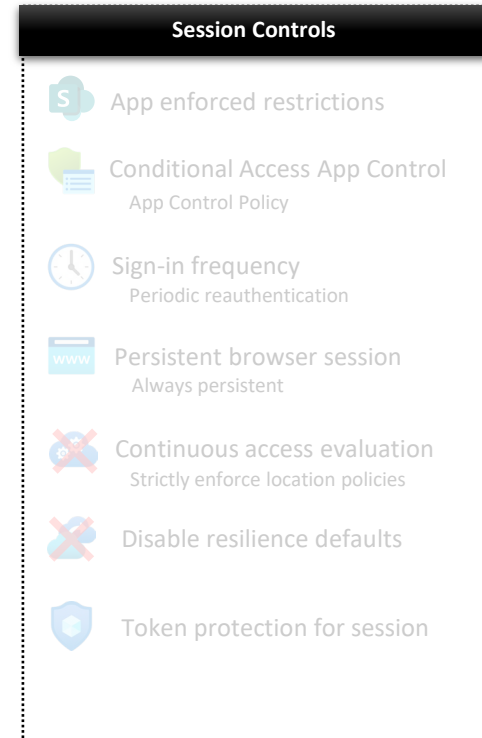
Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-WHfB-All-Dynamic (2)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA508-Shared-Device-Users-AllApps-TrustedLocations-WHfB-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



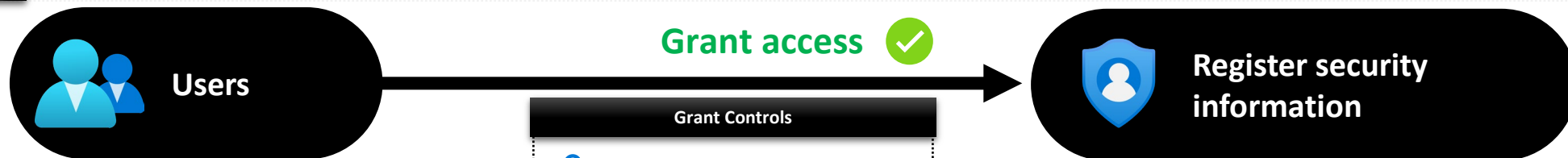
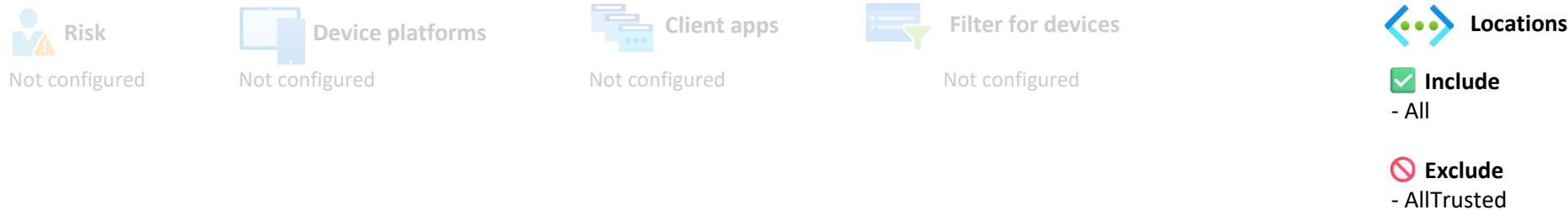
- ☒ **Include:**
- All



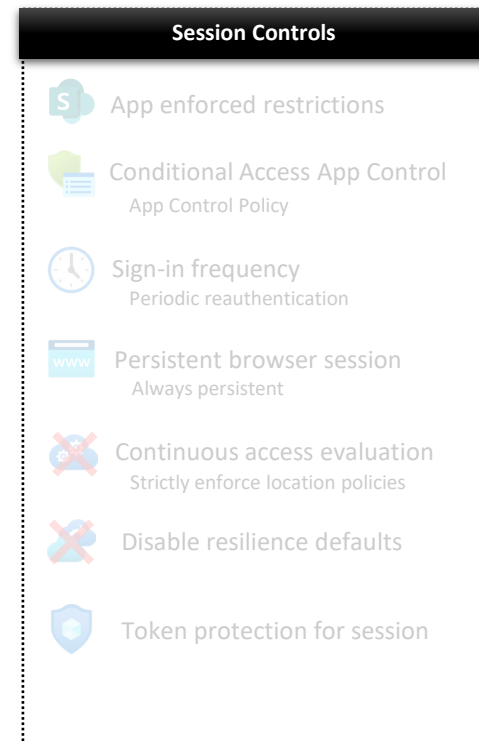
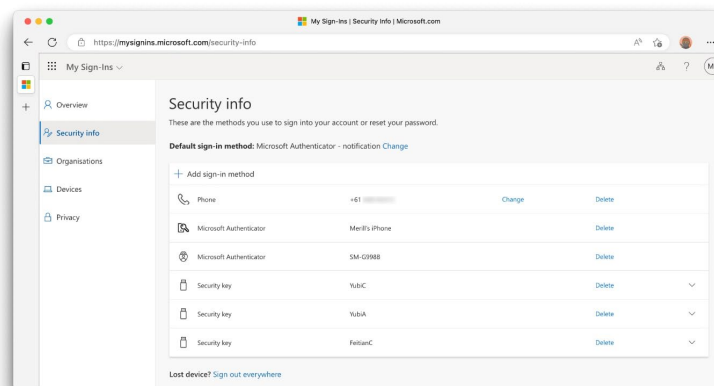
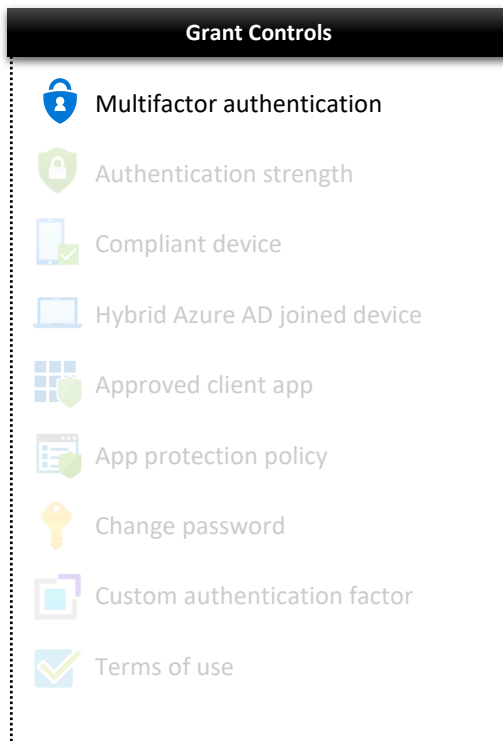
CA509-Prod-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow

Policy Enabled

Last modified: 2025-02-05



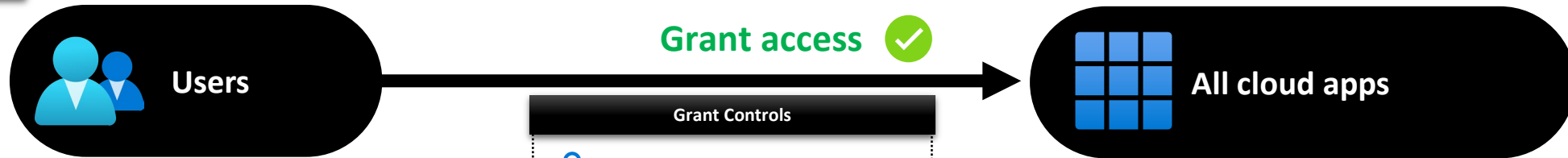
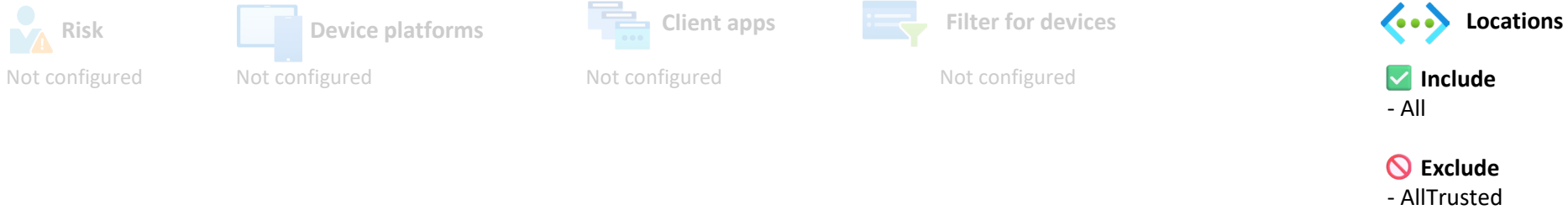
- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA509-Shared-Device-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



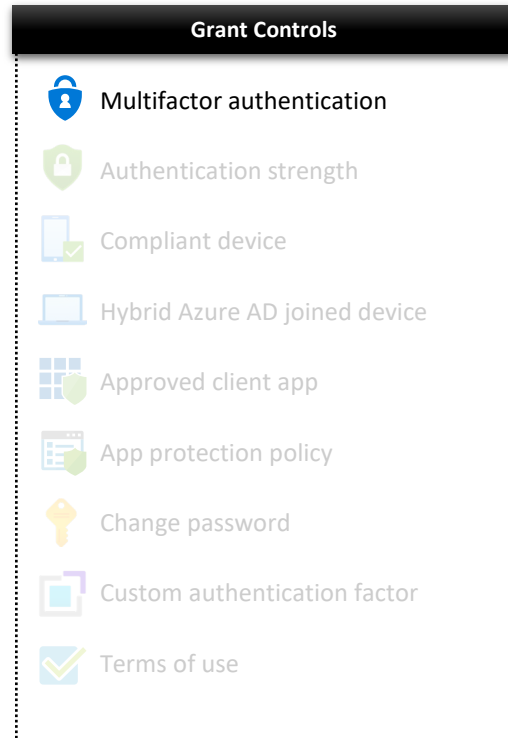
CA510-Prod-Shared-Device-Users-AllApps-TrustedLocations-MFA-Enforce

Policy Enabled

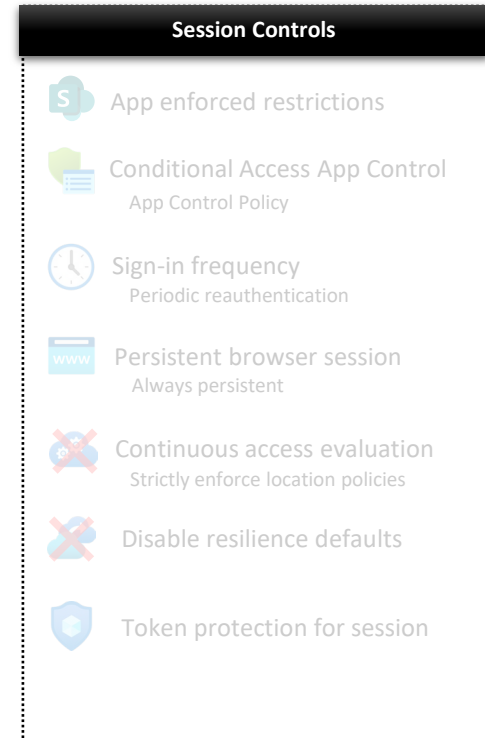
Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Device-Users-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA510-Shared-Device-Users-AllApps-TrustedLocations-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



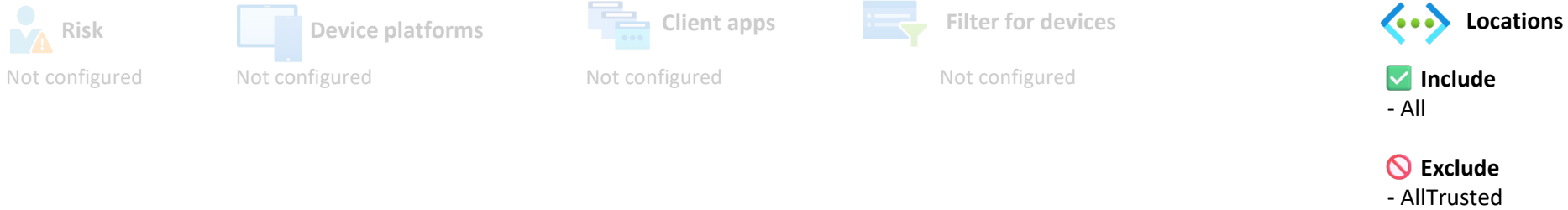
- ☒ **Include:**
- All



CA540-Prod-Teams-Rooms-AllApps-AnyPlatform-NonTrustedLocations-Block

Policy Enabled

Last modified: 2025-01-29



- ☒ **Include:**
 - Groups**
 - Entra-CA-Teams-Rooms-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA540-Teams-Rooms-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

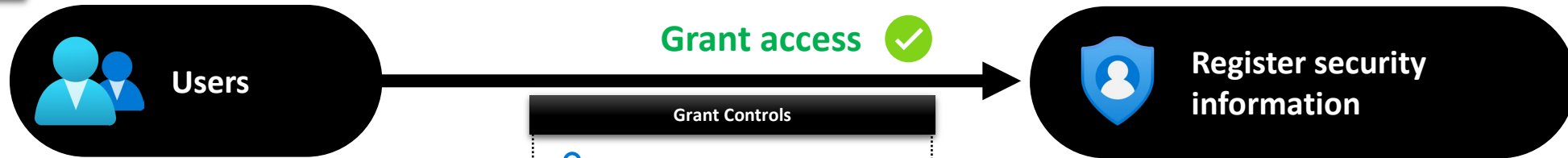
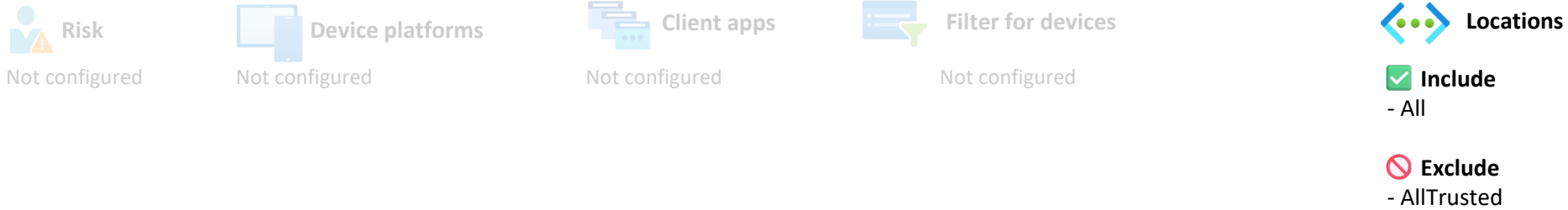
- ☒ **Include:**
 - All

- 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

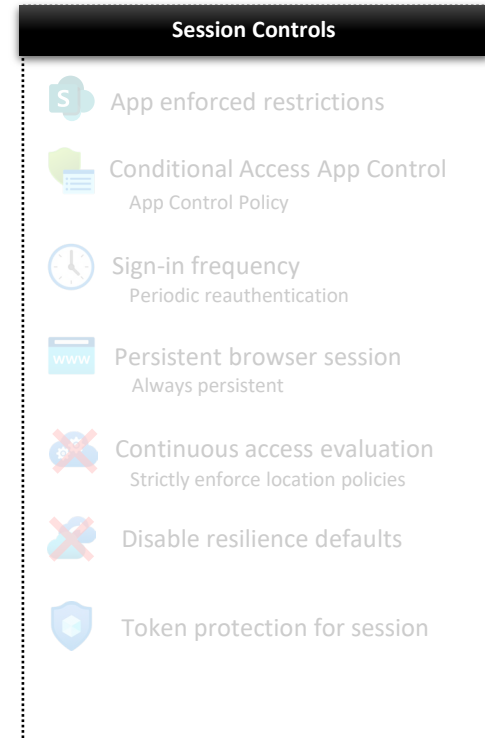
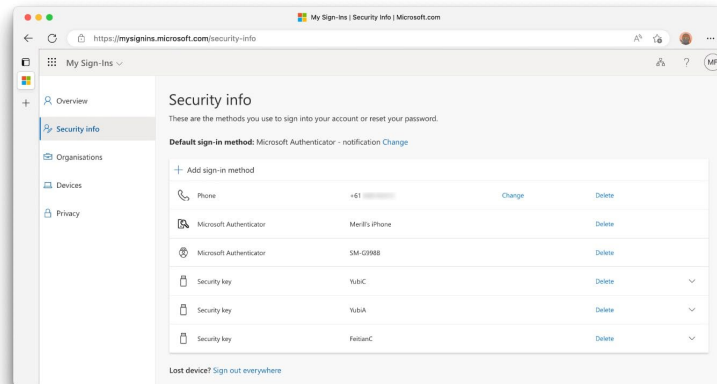
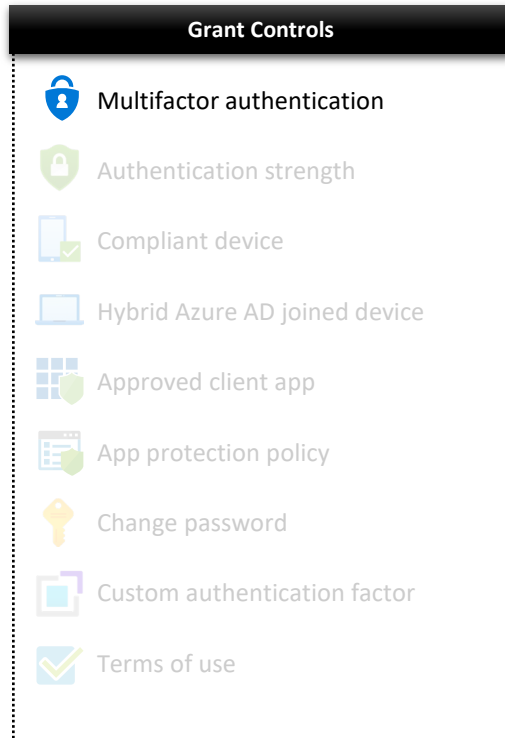
CA542-Prod-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-Pwd-Allow

Policy Enabled

Last modified: 2025-02-05



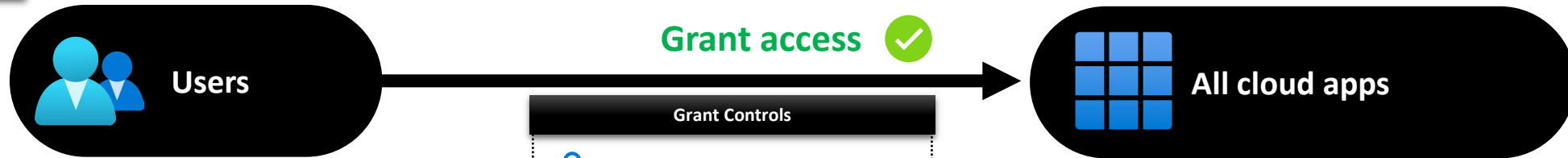
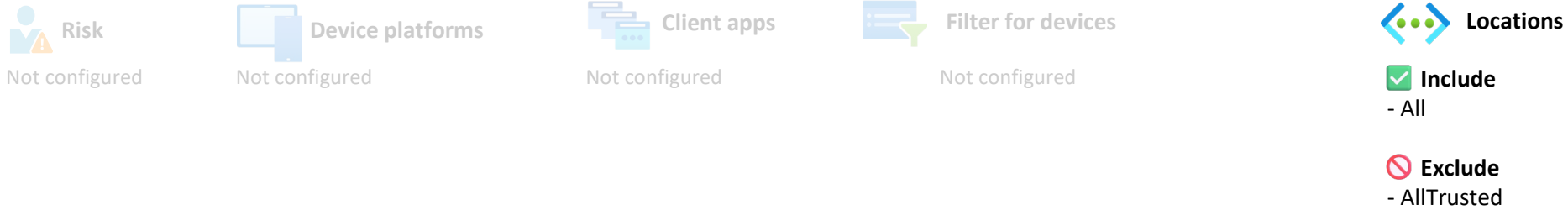
- ☒ **Include:**
 - Groups**
 - Entra-CA-Teams-Rooms-Req-Pwd-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA542-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-Pwd-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



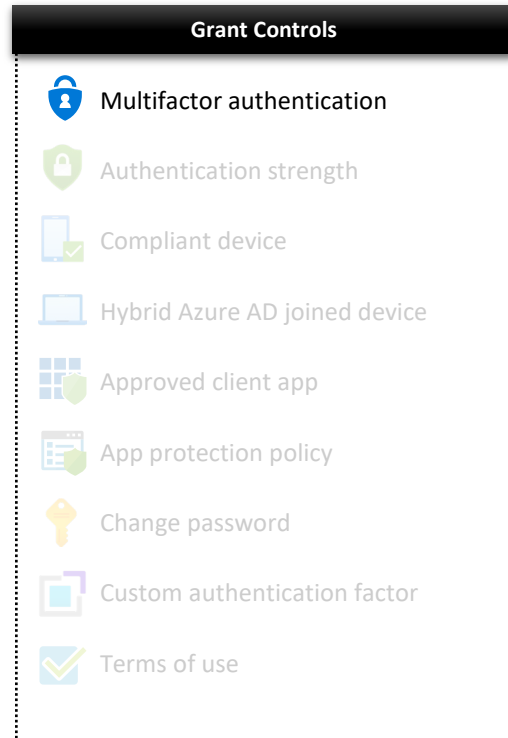
CA543-Prod-Teams-Rooms-AllApps-TrustedLocations-Pwd-Enforce

Policy Enabled

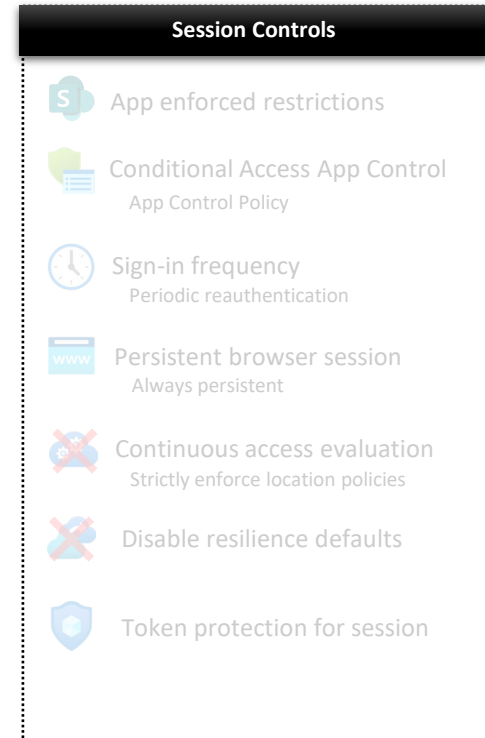
Last modified: 2025-02-05



- ☒ **Include:**
Groups
- Entra-CA-Teams-Rooms-Req-Pwd-All-Dynamic (0)
- ☐ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA543-Teams-Rooms-AllApps-TrustedLocations-Pwd-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)



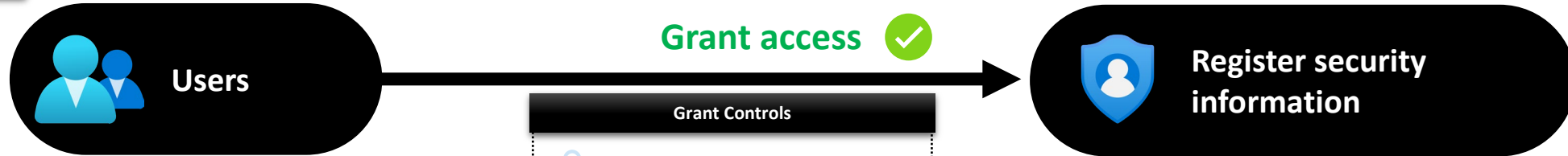
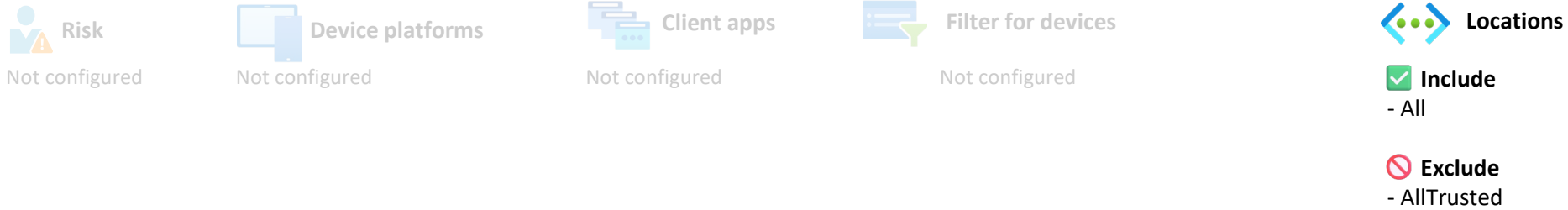
- ☒ **Include:**
- All



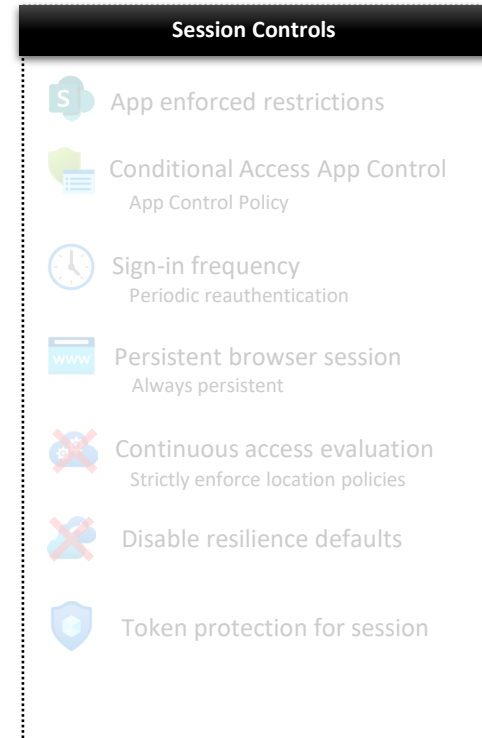
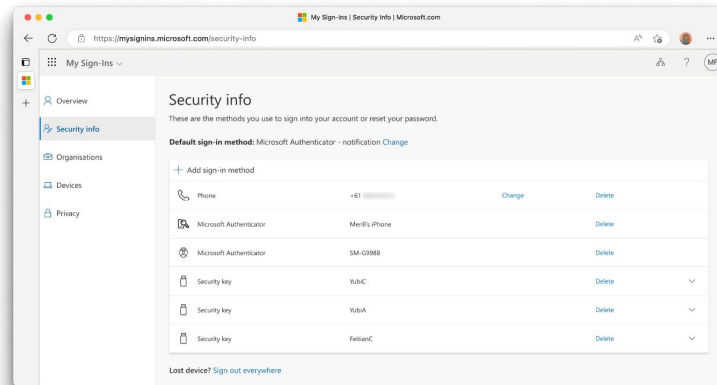
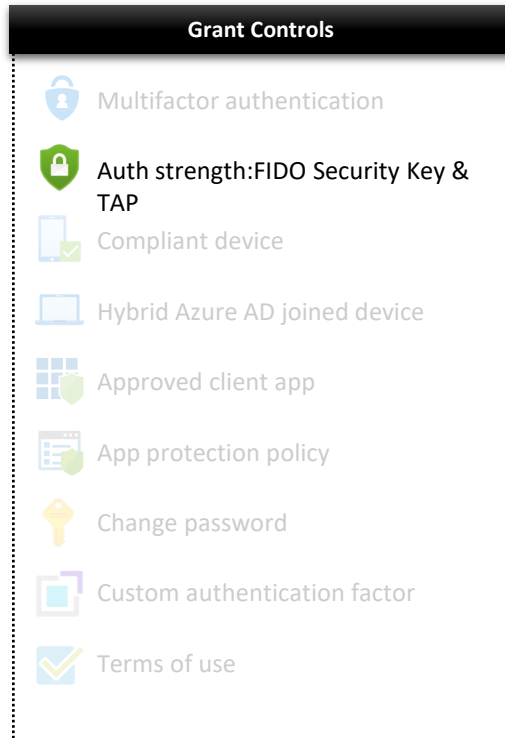
CA544-Prod-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05



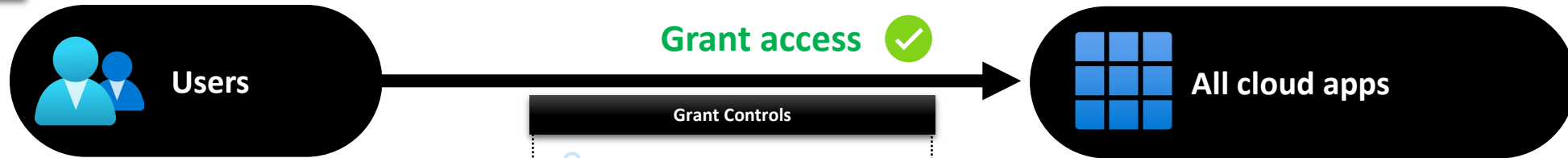
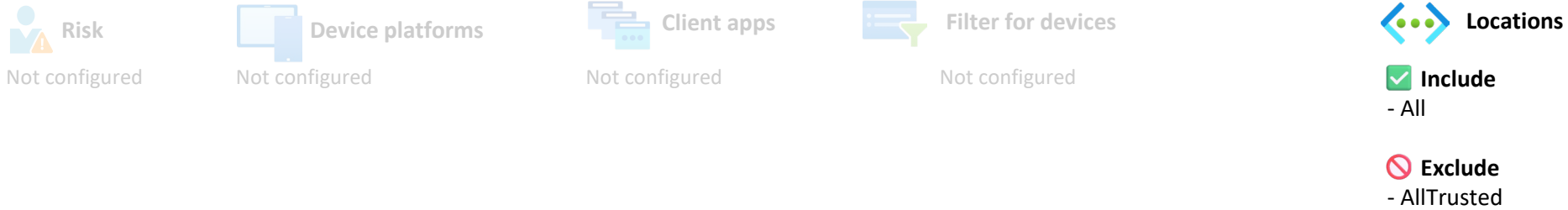
- ☒ **Include:**
- Groups**
- Entra-CA-Teams-Rooms-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA544-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-FIDO-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA545-Prod-Teams-Rooms-AllApps-TrustedLocations-FIDO-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Teams-Rooms-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA545-Teams-Rooms-AllApps-TrustedLocations-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

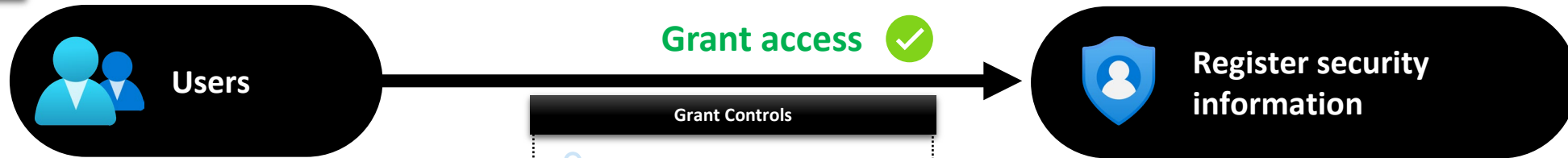
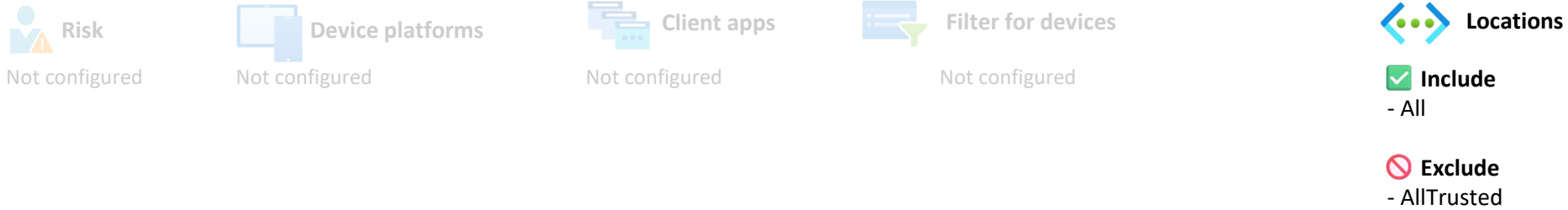
- ☒ **Include:**
- All

- 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

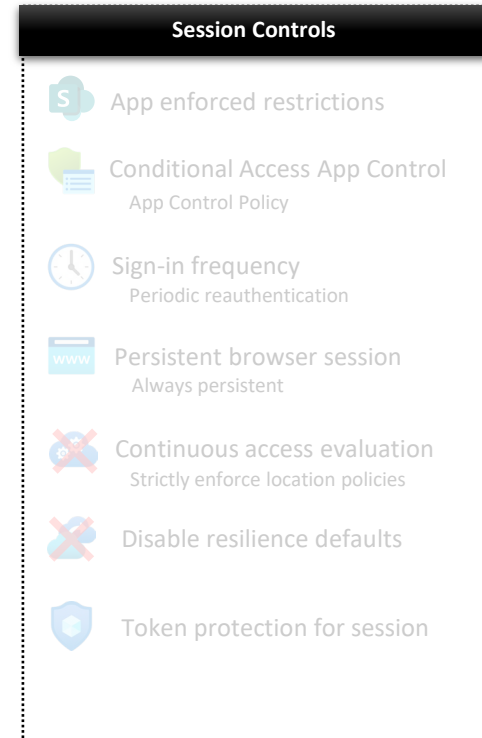
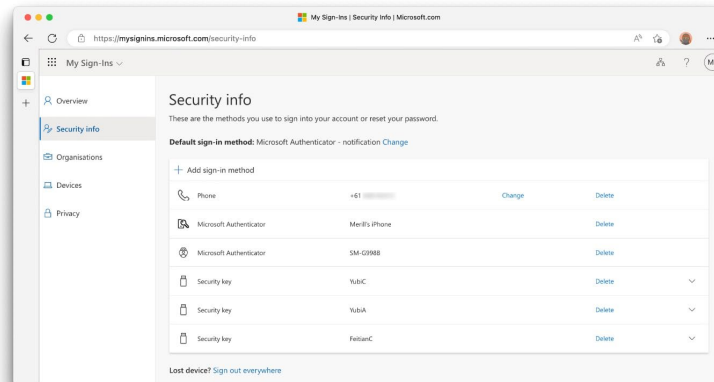
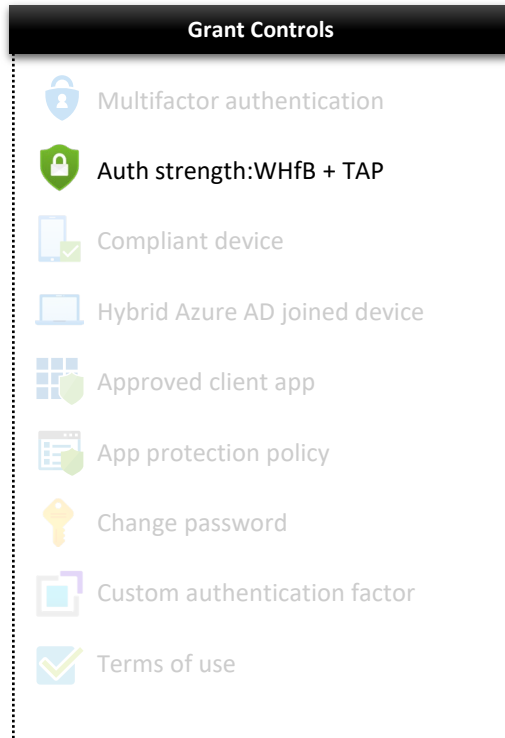
CA546-Prod-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-WHfB-Allow

Policy Enabled

Last modified: 2025-02-05



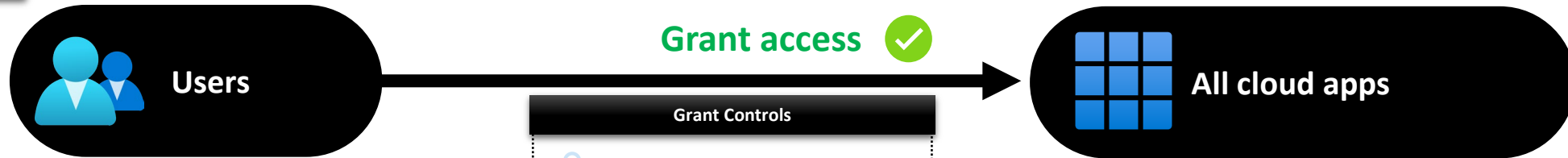
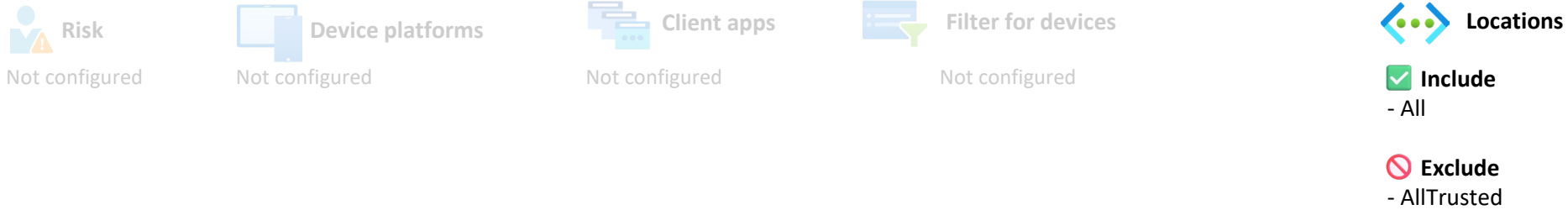
- ☒ **Include:**
 - Groups**
 - Entra-CA-Teams-Rooms-Req-WHfB-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA546-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-WHfB-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA547-Prod-Teams-Rooms-AllApps-TrustedLocations-WHfB-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Teams-Rooms-Req-WHfB-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA547-Teams-Rooms-AllApps-TrustedLocations-WHfB-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- Grant Controls**
- Multifactor authentication
 - Auth strength: WHfB + TAP
 - 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


CA548-Prod-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-MFA-Allow


Policy Enabled


Last modified: 2025-02-05

 **Risk**
Not configured

 **Device platforms**
Not configured

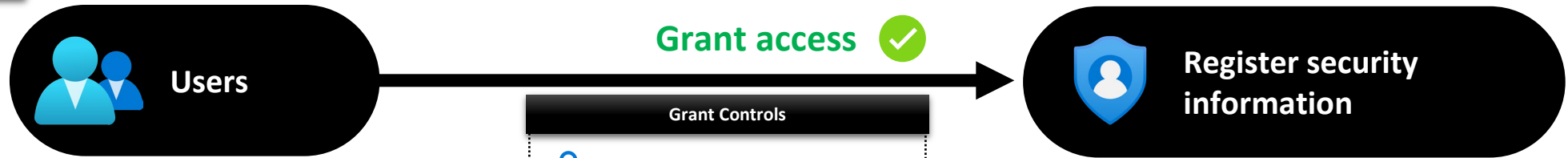
 **Client apps**
Not configured

 **Filter for devices**
Not configured

 **Locations**
☒ **Include**
- All










☐ **Exclude**
- AllTrusted

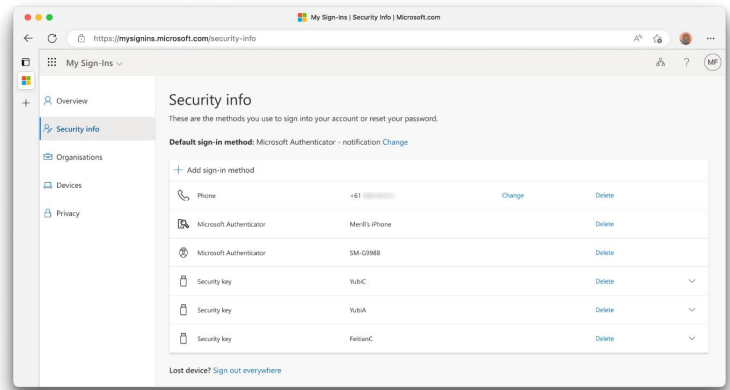
Conditions










- ☒ **Include:**
- Groups**
- Entra-CA-Teams-Rooms-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA548-Teams-Rooms-RegisterSecurityInfo-TrustedLocations-MFA-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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



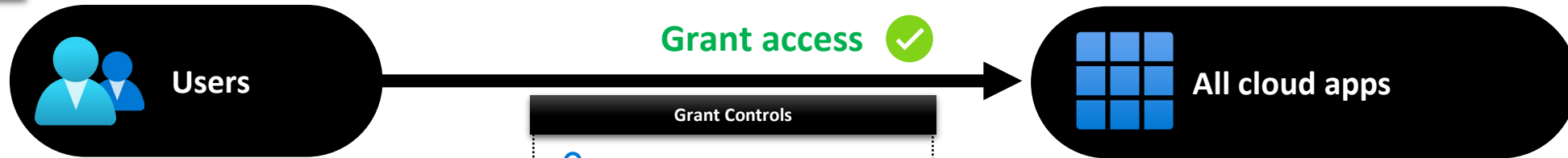
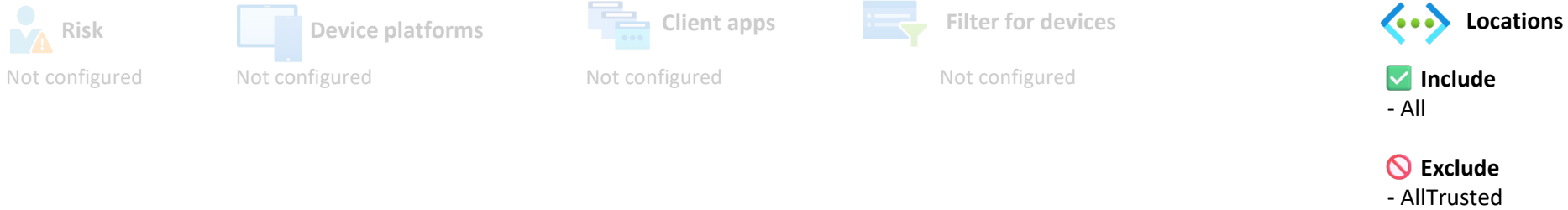
Session Controls

-  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

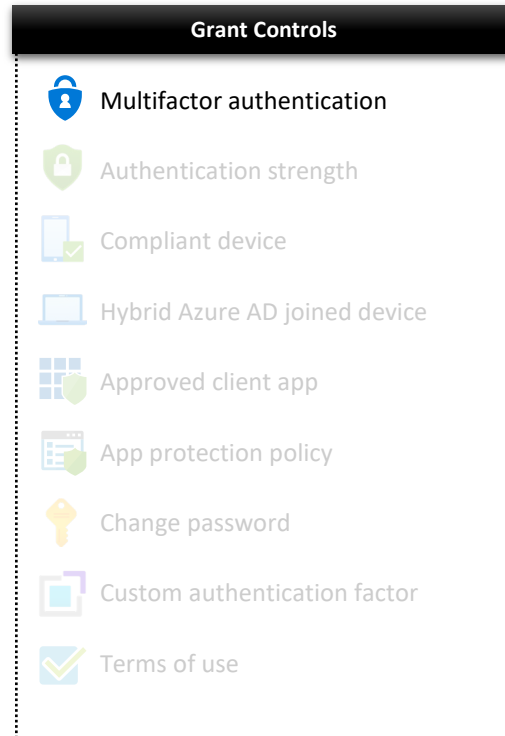
CA549-Prod-Teams-Rooms-AllApps-TrustedLocations-MFA-Enforce

Policy Enabled

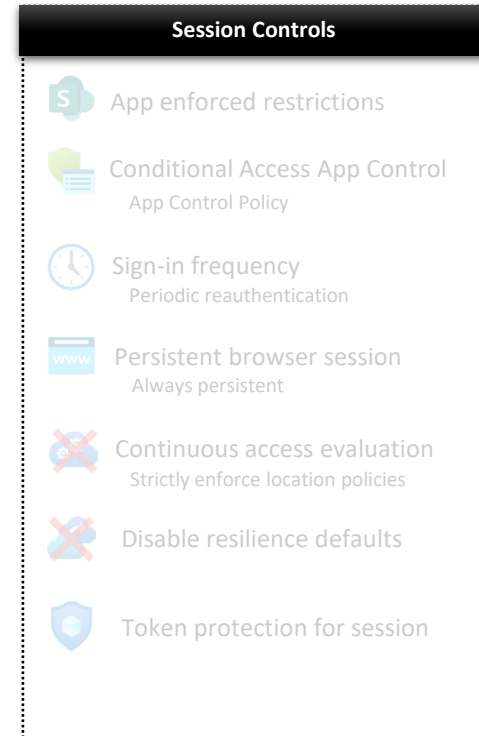
Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Teams-Rooms-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA549-Teams-Rooms-AllApps-TrustedLocations-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



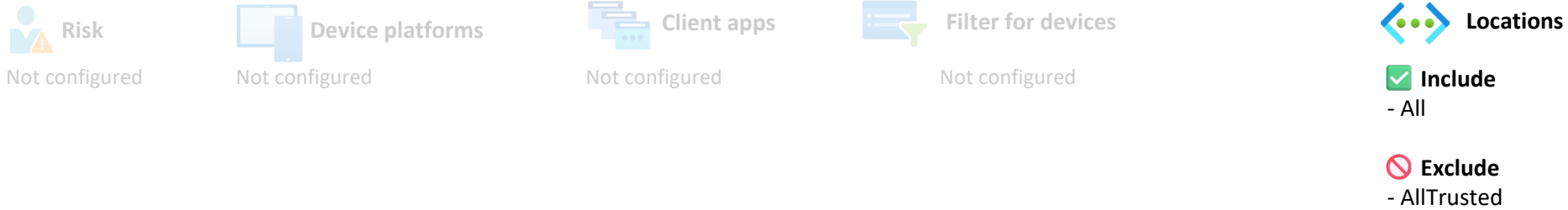
- ☒ **Include:**
- All



CA550-Prod-Shared-Mail-Users-AllApps-AnyPlatform-NonTrustedLocations-Block

Policy Enabled

Last modified: 2025-01-29



- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Mail-Users-All-Dynamic (2)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA550-Shared-Mail-Users-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (2)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

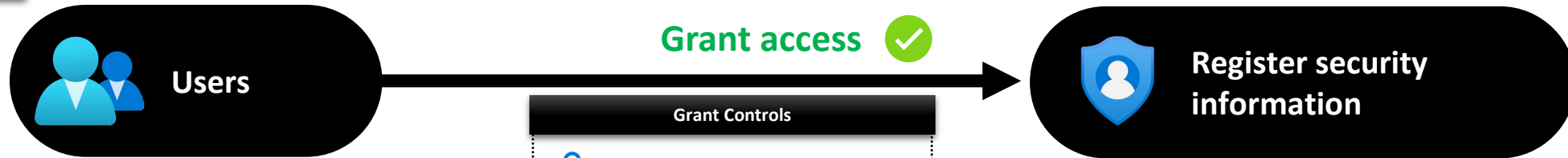
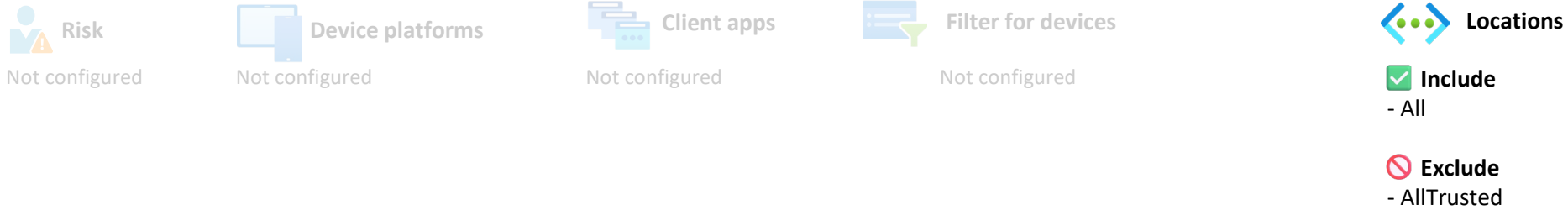
- ☒ **Include:**
 - All

- 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

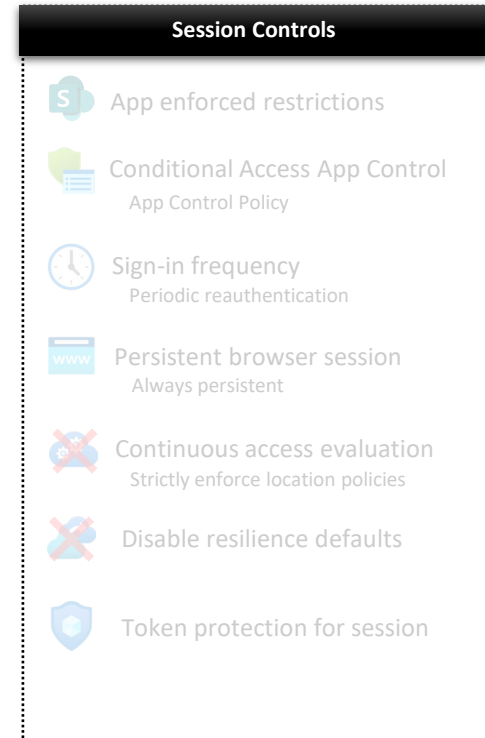
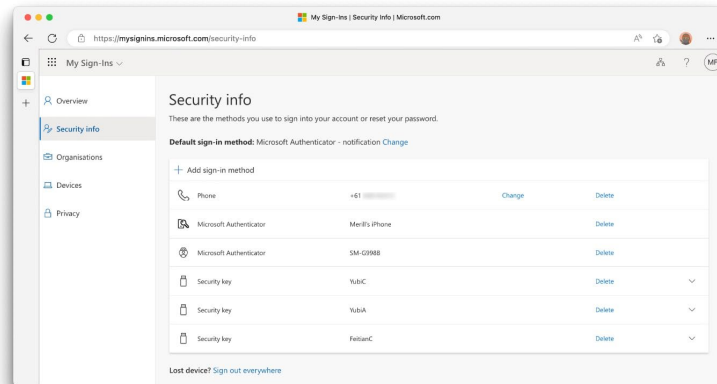
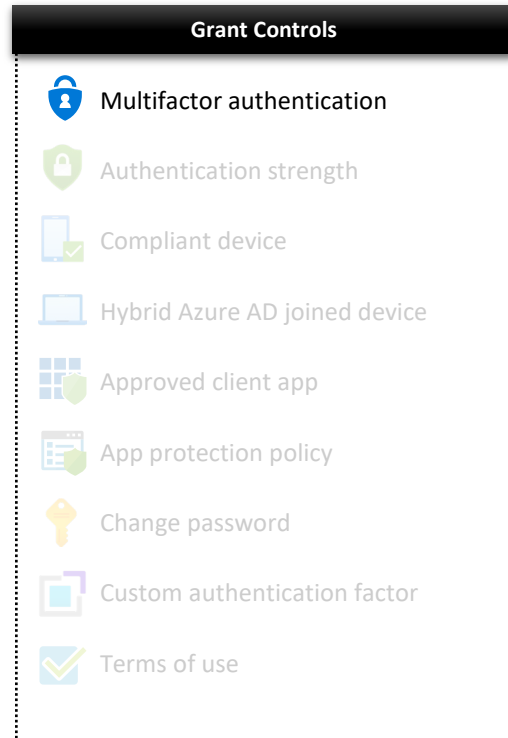
CA551-Prod-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow

Policy Enabled

Last modified: 2025-02-05




- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Mail-Users-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA551-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)





CA552-Prod-Shared-Mail-Users-AllApps-TrustedLocations-Pwd-Enforce


Policy Enabled


Last modified: 2025-02-05

**Risk**
Not configured

**Device platforms**
Not configured

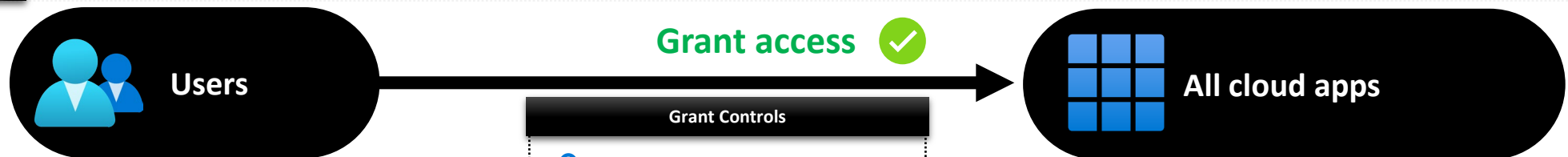
**Client apps**
Not configured

**Filter for devices**
Not configured










**Locations**
☒ **Include**
- All








☐ **Exclude**
- AllTrusted

Conditions



- ☒ **Include:**
Groups
 - Entra-CA-Shared-Mail-Users-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
Groups
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA552-Shared-Mail-Users-AllApps-TrustedLocations-Pwd-Enforce-Excluded-Assigned (1)
- Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

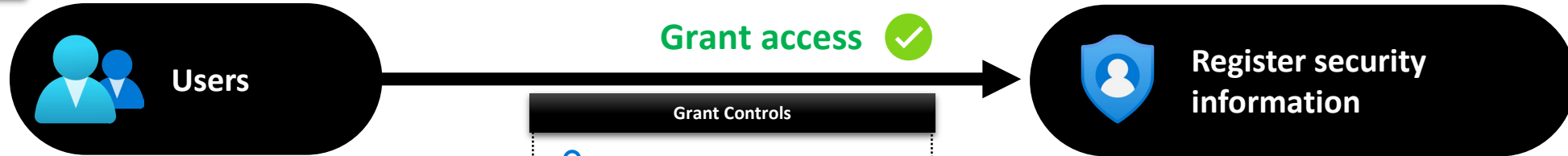
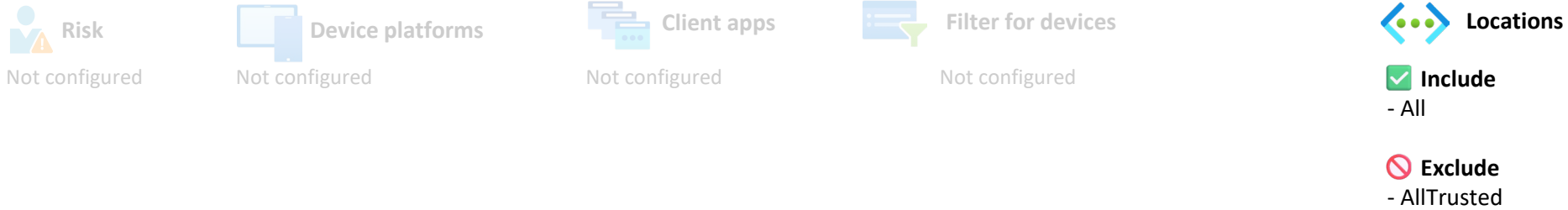
- Session Controls
-  App enforced restrictions
 -  Conditional Access App Control
App Control Policy
 -  Sign-in frequency
Periodic reauthentication
 -  Persistent browser session
Always persistent
 -  Continuous access evaluation
Strictly enforce location policies
 -  Disable resilience defaults
 -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

- ☒ **Include:**
- All

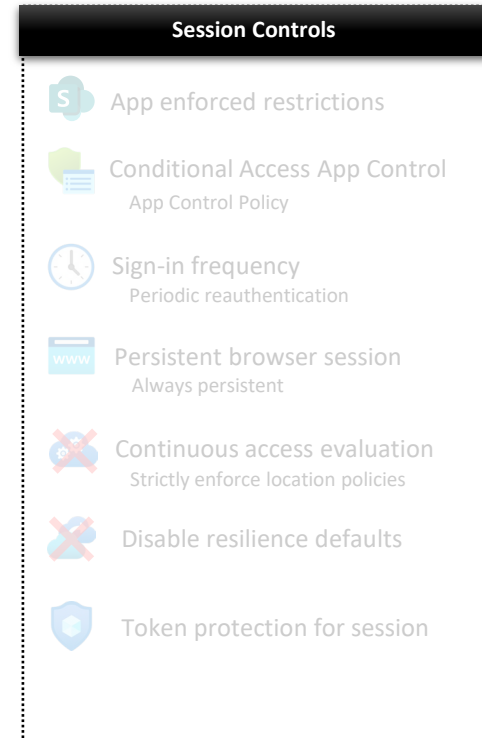
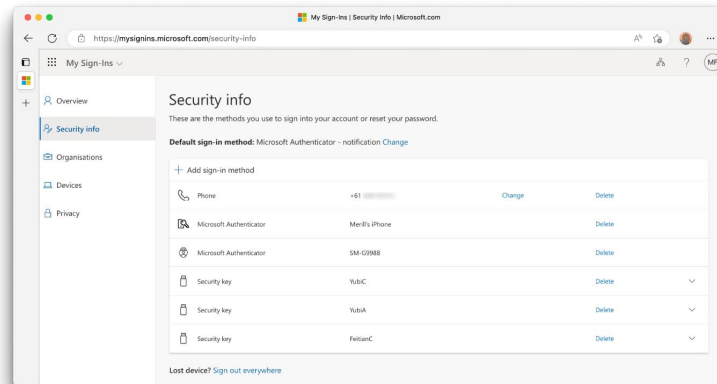
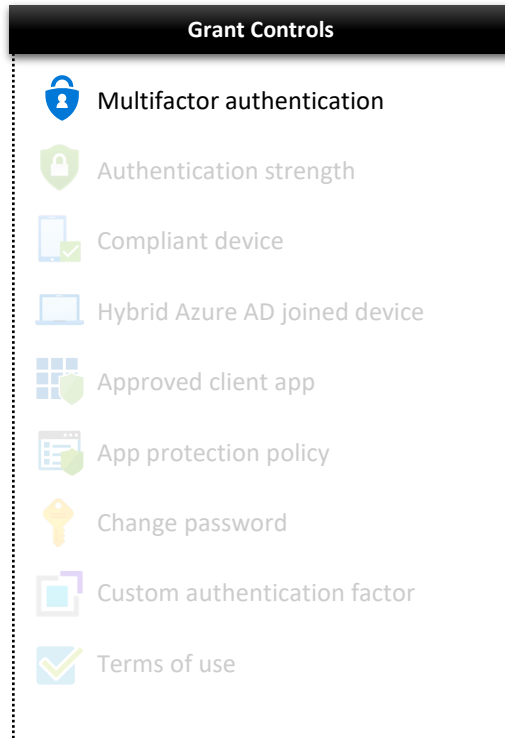
CA553-Prod-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow

Policy Enabled

Last modified: 2025-02-05



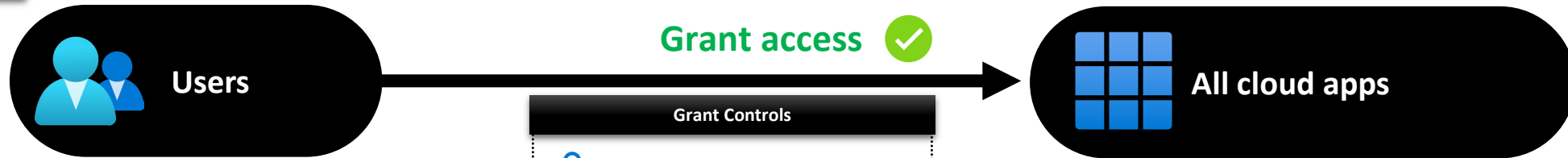
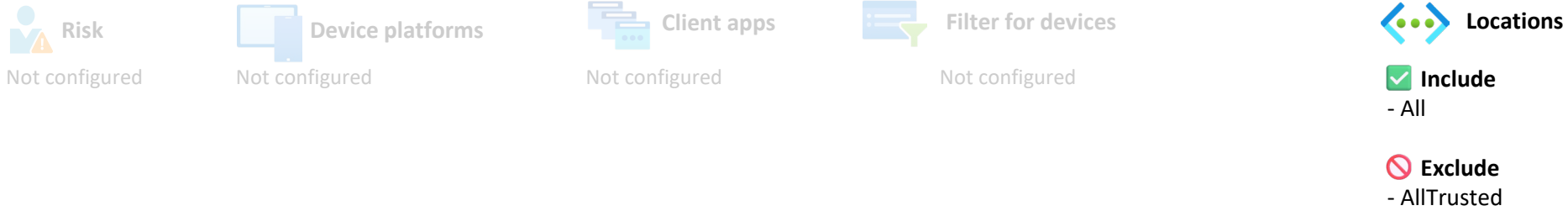
- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Mail-Users-Req-MFA-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA553-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



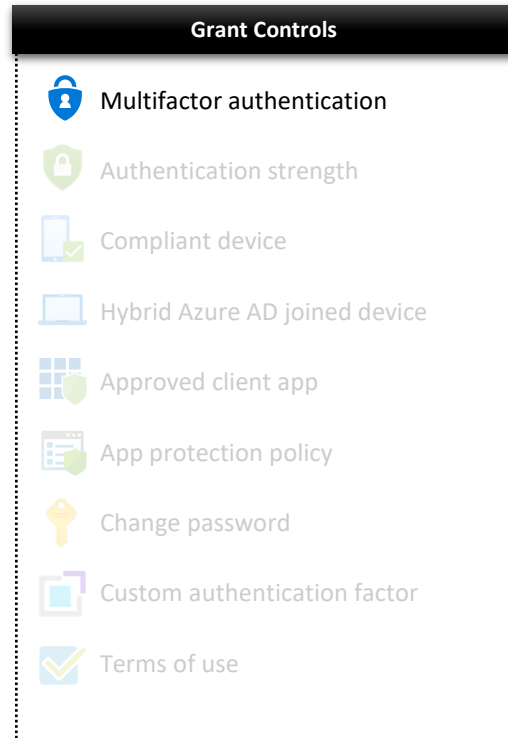
CA554-Prod-Shared-Mail-Users-AllApps-TrustedLocations-MFA-Enforce

Policy Enabled

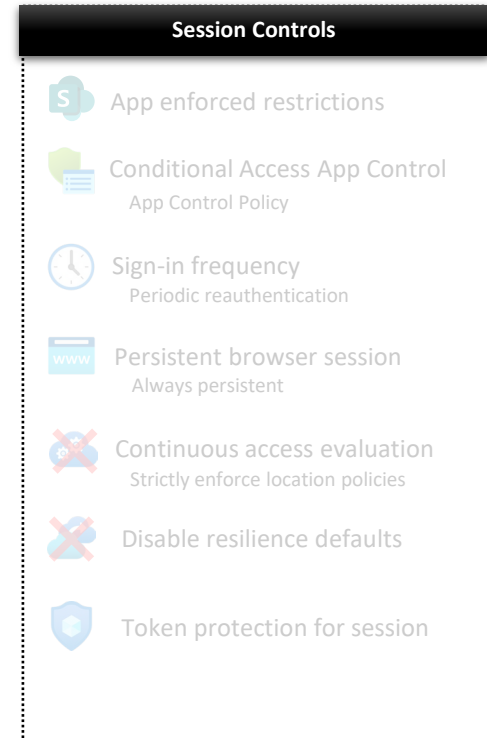
Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Mail-Users-Req-MFA-All-Dynamic (1)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA554-Shared-Mail-Users-AllApps-TrustedLocations-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



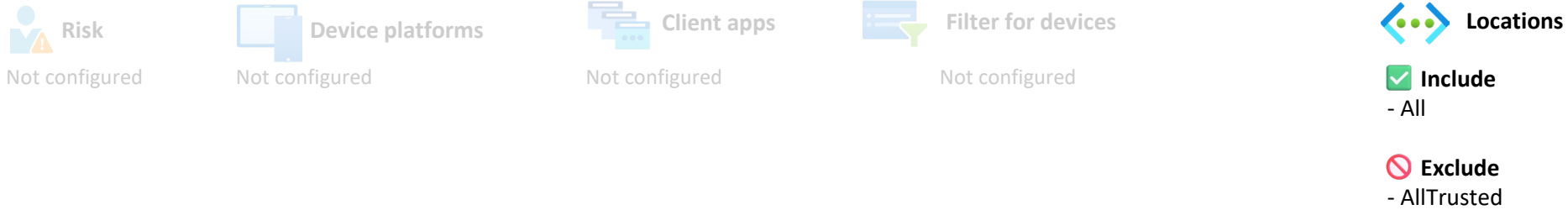
- ☒ **Include:**
- All



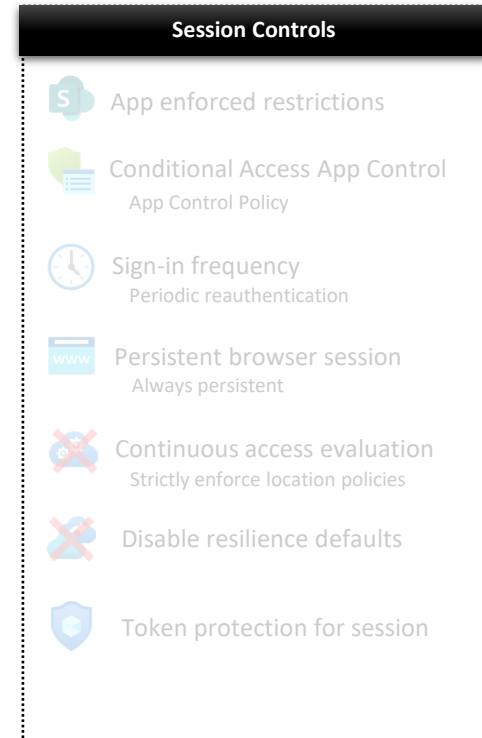
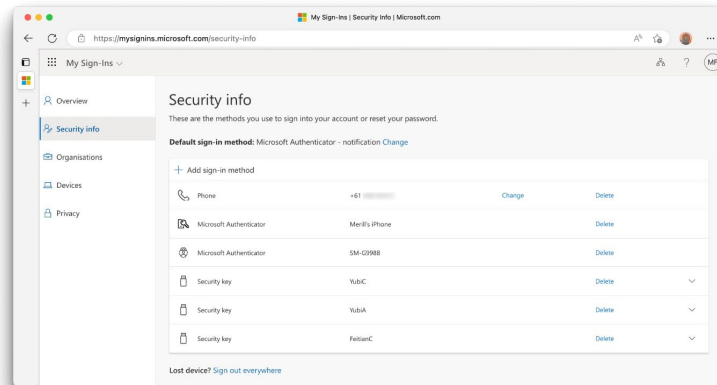
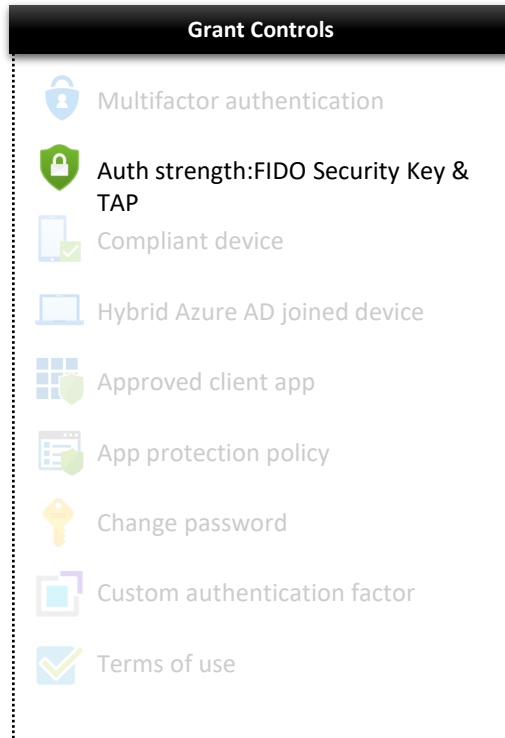
CA555-Prod-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05



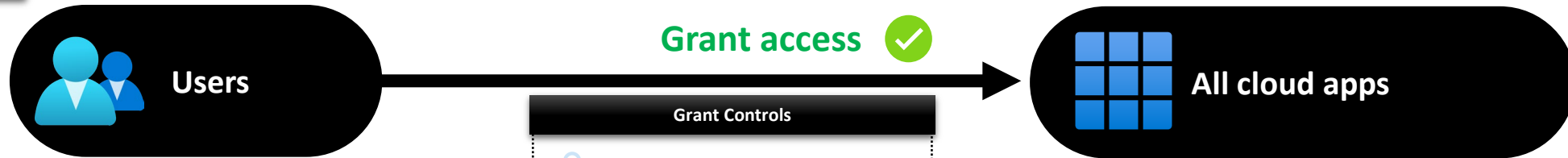
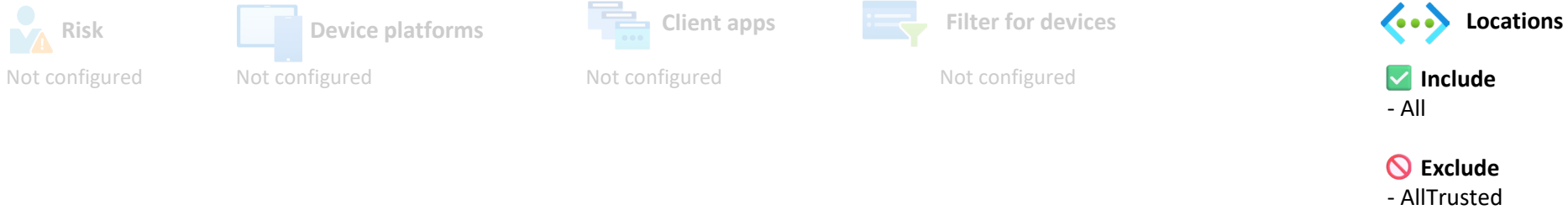
- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Mail-Users-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA555-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA556-Prod-Shared-Mail-Users-AllApps-TrustedLocations-FIDO-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Mail-Users-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA556-Shared-Mail-Users-AllApps-TrustedLocations-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

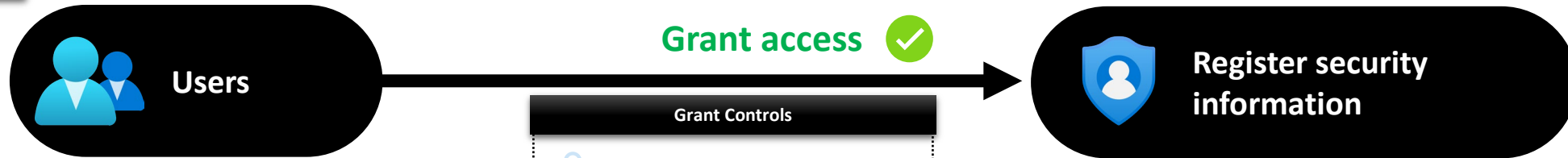
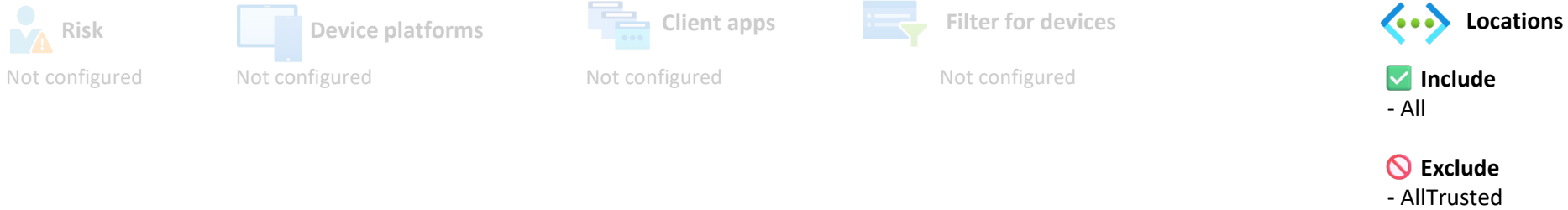
- ☒ **Include:**
- All

- 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

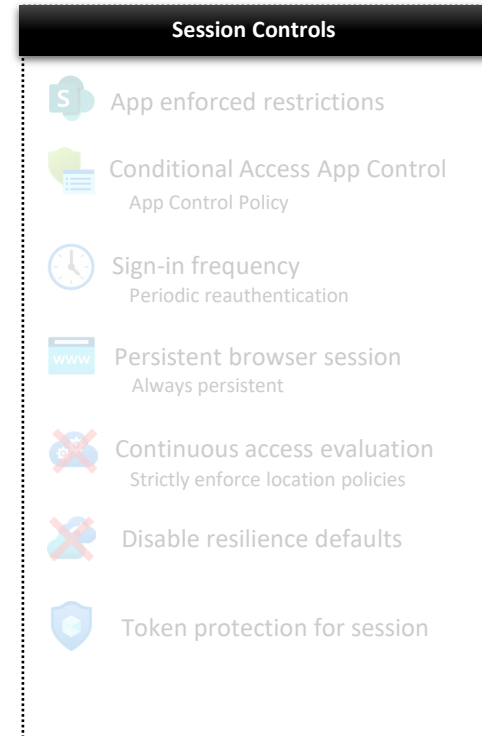
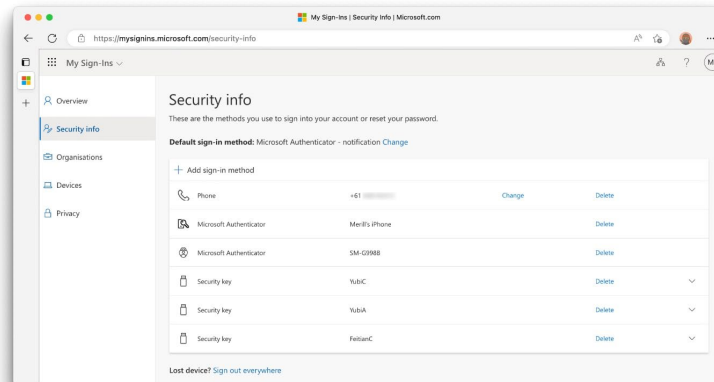
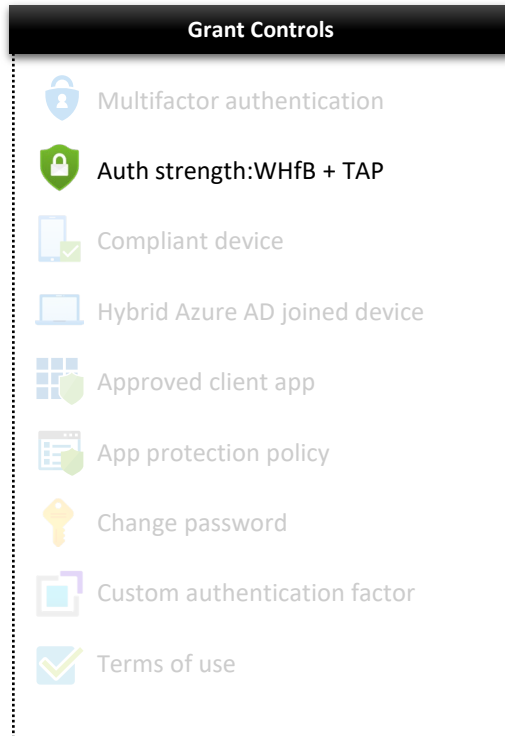
CA557-Prod-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-WHfB-Allow

Policy Enabled

Last modified: 2025-02-05



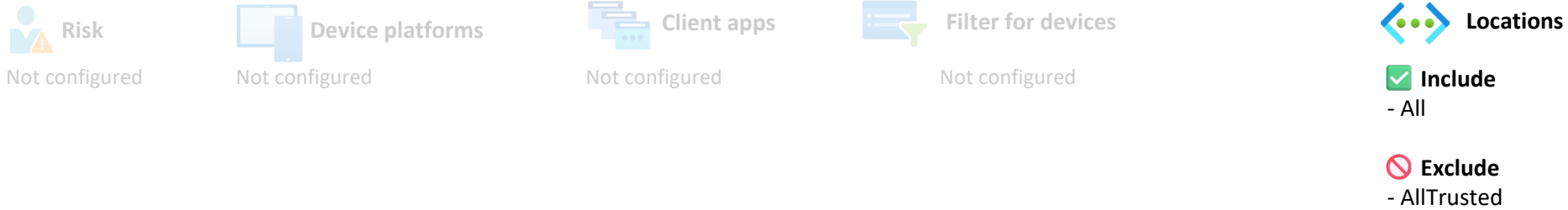
- ☒ **Include:**
 - Groups**
 - Entra-CA-Shared-Mail-Users-Req-WHfB-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA557-Shared-Mail-Users-RegisterSecurityInfo-TrustedLocations-WHfB-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA558-Prod-Shared-Mail-Users-AllApps-TrustedLocations-WHfB-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-Shared-Mail-Users-Req-WHfB-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA558-Shared-Mail-Users-AllApps-TrustedLocations-WHfB-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

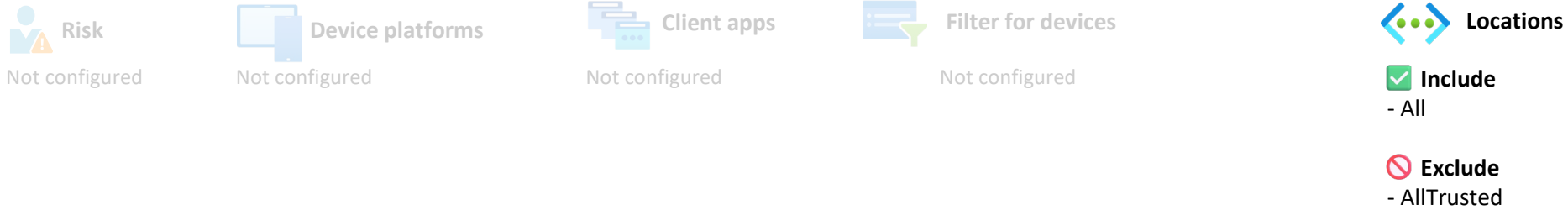
- ☒ **Include:**
- All

- 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

CA600-Prod-ServiceAccounts-AllApps-AnyPlatform-NonTrustedLocations-Block

Policy Enabled

Last modified: 2025-01-29



- ☒ **Include:**
 - Groups**
 - Entra-CA-ServiceAccounts-All-Dynamic (4)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA600-ServiceAccounts-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

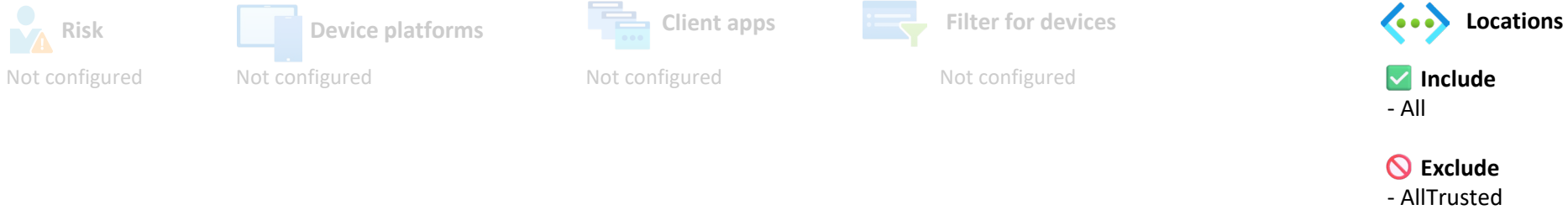
- Session Controls**
- ☐ App enforced restrictions
 - ☐ Conditional Access App Control
App Control Policy
 - ☐ Sign-in frequency
Periodic reauthentication
 - ☐ Persistent browser session
Always persistent
 - ☐ Continuous access evaluation
Strictly enforce location policies
 - ☐ Disable resilience defaults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



CA601-Prod-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-Pwd-Allow

Policy Enabled

Last modified: 2025-02-05



Users

Grant access ☒



Register security information

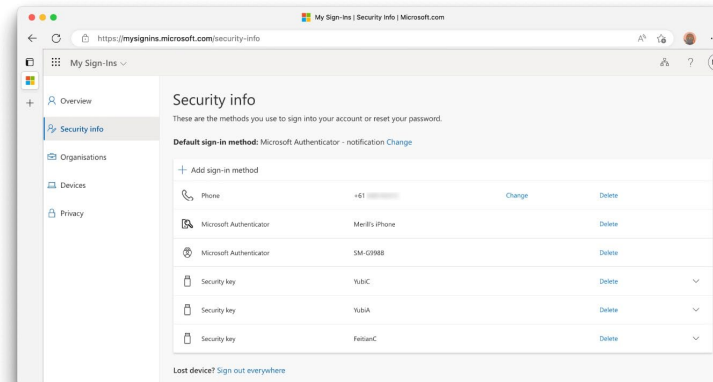
- ☒ **Include:**
 - Groups**
 - Entra-CA-ServiceAccounts-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA601-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-Pwd-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

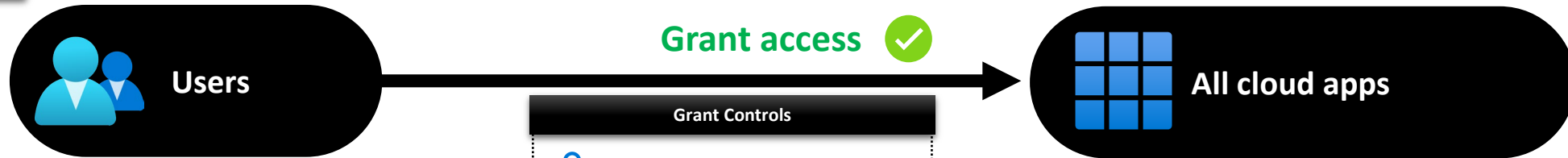
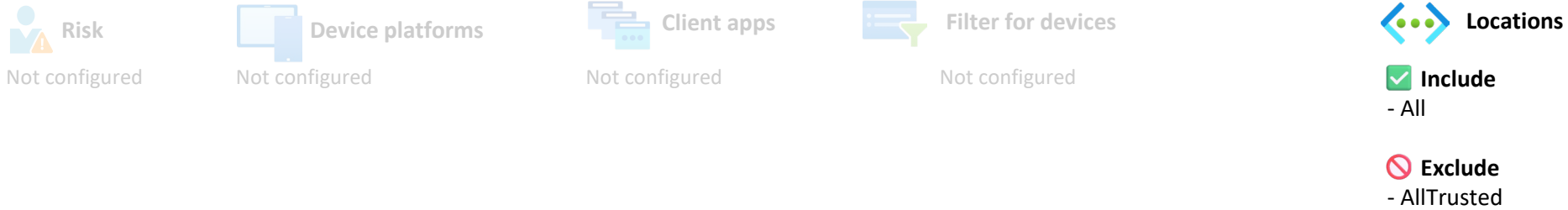
- ☐ App enforced restrictions
- ☐ Conditional Access App Control App Control Policy
- ☐ Sign-in frequency Periodic reauthentication
- ☐ Persistent browser session Always persistent
- ☐ Continuous access evaluation Strictly enforce location policies
- ☐ Disable resilience defaults
- ☐ Token protection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



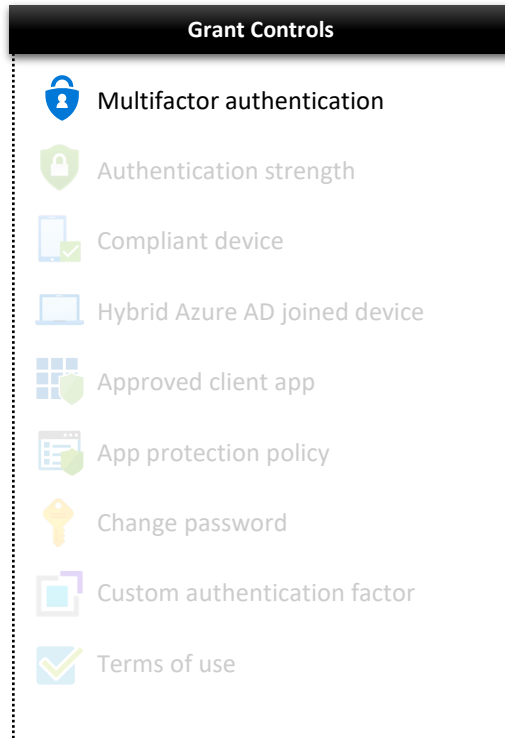
CA602-Prod-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-Pwd-Enforce

Policy Enabled

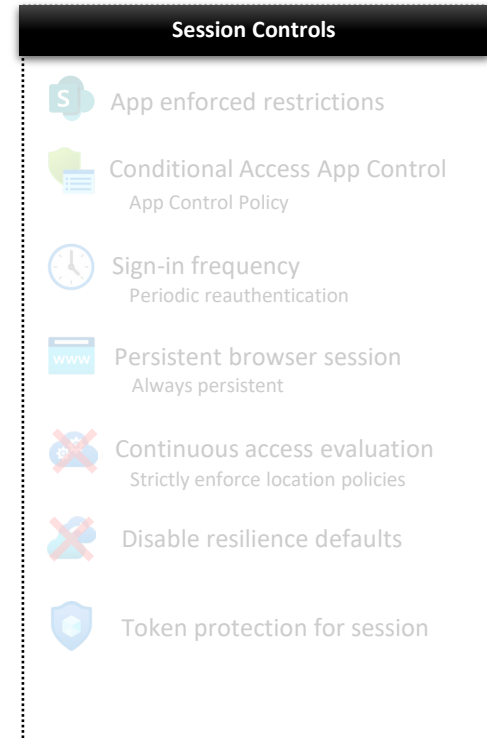
Last modified: 2025-02-05



- ☒ **Include:**
Groups
- Entra-CA-ServiceAccounts-Req-Pwd-All-Dynamic (1)
- ☐ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA602-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-Pwd-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)



- ☒ **Include:**
- All





CA603-Prod-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05



Risk

Not configured



Device platforms

Not configured



Client apps

Not configured



Filter for devices

Not configured



Locations

☒ Include
- All

☐ Exclude
- AllTrusted



Users

Grant access



Register security information

☒ Include:

Groups

- Entra-CA-ServiceAccounts-Req-FIDO-All-Dynamic (3)

☐ Exclude:

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA603-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-FIDO-Allow-Excluded-Assigned (0)

Users

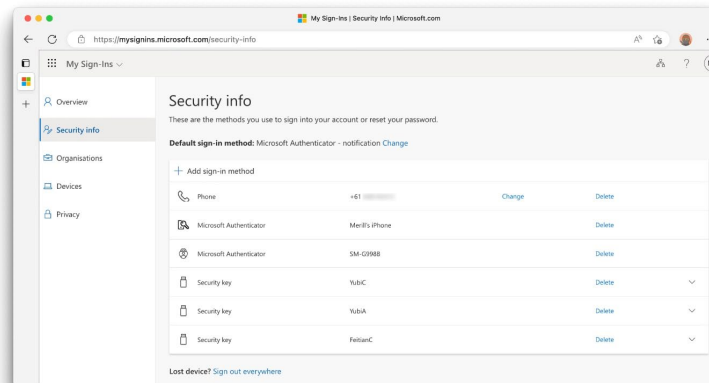
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

Grant Controls

- Multifactor authentication
- Auth strength: FIDO Security Key & TAP
- 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





CA604-Prod-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-FIDO-Enforce


Policy Enabled


Last modified: 2025-02-05

 **Risk**
Not configured

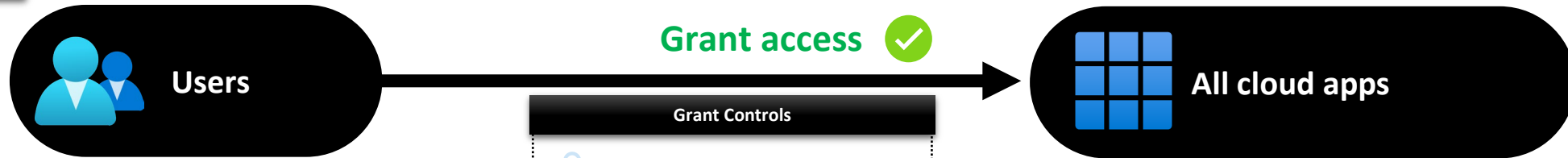
 **Device platforms**
Not configured

 **Client apps**
Not configured

 **Filter for devices**
Not configured










 **Locations**
☒ **Include**
- All

☐ **Exclude**
- AllTrusted










- ☒ **Include:**
- Groups**
- Entra-CA-ServiceAccounts-Req-FIDO-All-Dynamic (3)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA604-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

Grant Controls

-  Multifactor authentication
-  Auth strength:FIDO Security Key & TAP
-  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

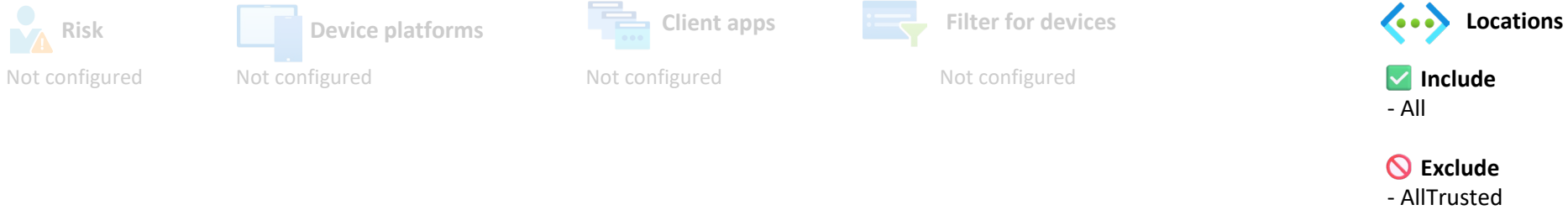
-  App enforced restrictions
-  Conditional Access App Control App Control Policy
-  Sign-in frequency Periodic reauthentication
-  Persistent browser session Always persistent
-  Continuous access evaluation Strictly enforce location policies
-  Disable resilience defaults
-  Token protection for session



CA605-Prod-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-MFA-Allow

Policy Enabled

Last modified: 2025-02-05



Users

Grant access ☒



Register security information

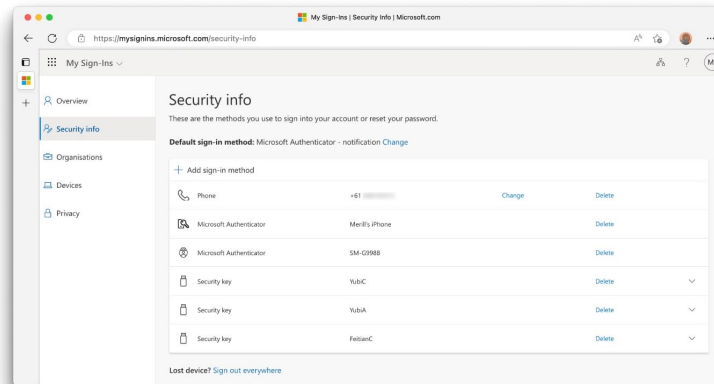
- ☒ **Include:**
 - Groups**
 - Entra-CA-ServiceAccounts-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA605-ServiceAccounts-RegisterSecurityInfo-AnyPlatform-TrustedLocations-MFA-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

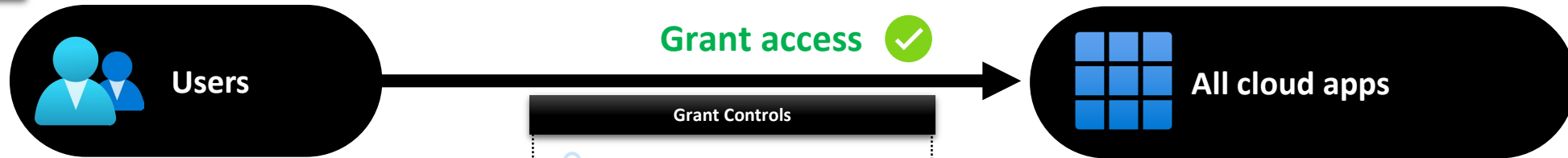
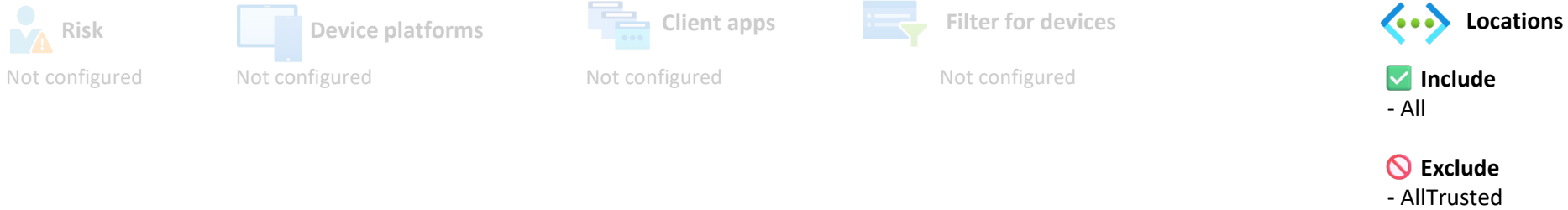
- ☐ App enforced restrictions
- ☐ Conditional Access App Control App Control Policy
- ☐ Sign-in frequency Periodic reauthentication
- ☐ Persistent browser session Always persistent
- ☐ Continuous access evaluation Strictly enforce location policies
- ☐ Disable resilience defaults
- ☐ Token protection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



CA606-Prod-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-MFA-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-ServiceAccounts-Req-MFA-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA606-ServiceAccounts-AllApps-AnyPlatform-TrustedLocations-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- Grant Controls**
- ☒ Multifactor authentication
 - ☒ Auth strength:WHfB + TAP
 - ☒ 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


CA607-BCLogicAppConnector-ServiceAccount-BusinessCentral-AnyPlatform-AzWELogicAppNetwork-Block

Policy Enabled


Last modified: 2025-05-04


Conditions

**Risk**
Not configured

**Device platforms**
Not configured

**Client apps**
Not configured

**Filter for devices**
Not configured

**Locations**


☒ **Include**
- All

☐ **Exclude**
- Azure.Network.ServiceTag.LogicApps.WestEurope




- ☒ **Include:**
Users
- LogicApp Connector Service Account, Azure WestEurope [DEMO]


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:**
- Dynamics 365 Business Central


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





CA700-Prod-WorkloadIdentities-Automation-2LINKIT-AnyPlatform-NonTrustedLocations-Block


Policy Enabled


Last modified: 2025-04-07

**Risk**
Not configured

**Device platforms**
Not configured

**Client apps**
Not configured

**Filter for devices**
Not configured

**Locations**
☒ **Include**
- All

☐ **Exclude**
- Automation



Workload identity

- ☒ **Include:**
- 2LINKIT - Automation - Resource Onboarding
 - 2LINKIT - Automation - KeyVault Lookup
 - 2LINKIT - Automation - O365
 - 2LINKIT - Automation - Azure










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


CA750-Prod-AppSystem-Test-Users-AllApps-AnyPlatform-NonTrustedLocations-Block


Policy Enabled


Last modified: 2025-01-29

 **Risk**
Not configured

 **Device platforms**
Not configured

 **Client apps**
Not configured

 **Filter for devices**
Not configured










 **Locations**
☒ **Include**
- All

☐ **Exclude**
- AllTrusted










- ☒ **Include:**
Groups
- Entra-CA-AppSystem-Test-Users-All-Dynamic (8)
- ☐ **Exclude:**
Groups
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA750-AppSystem-Test-Users-AllApps-AnyPlatform-NonTrustedLocations-Block-Excluded-Assigned (3)
- Users**
- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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

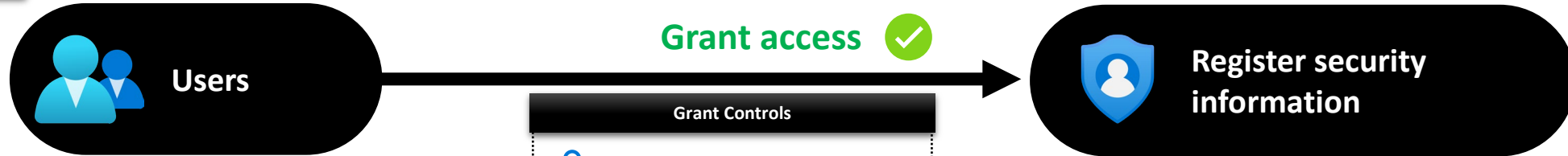
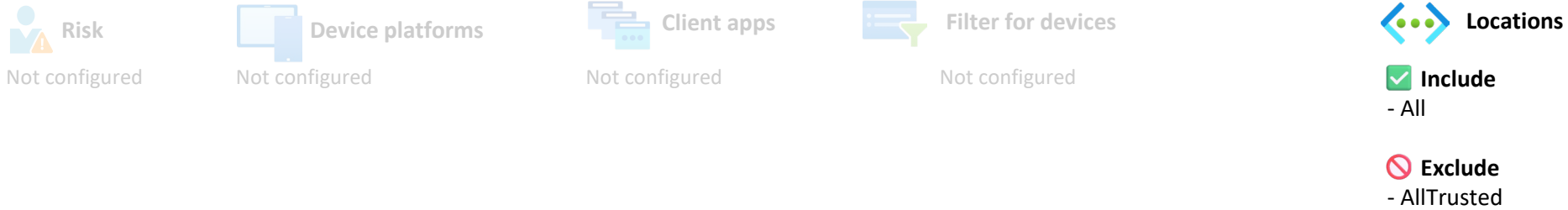
Session Controls

-  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

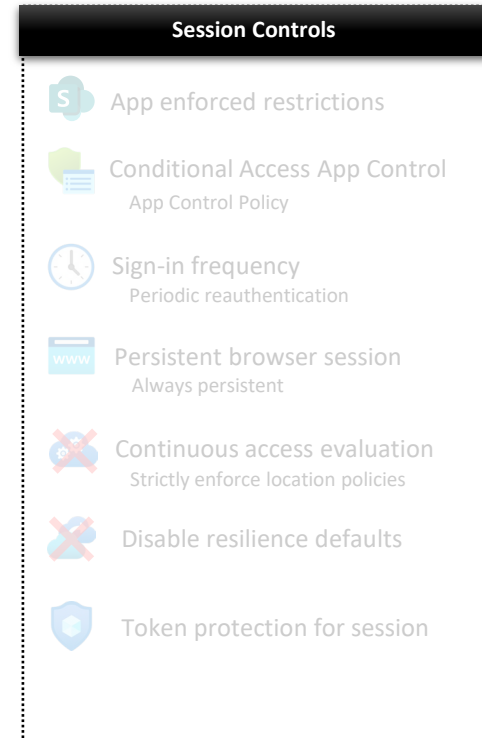
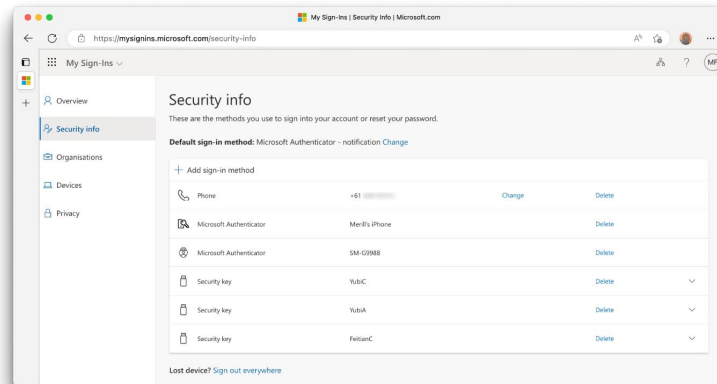
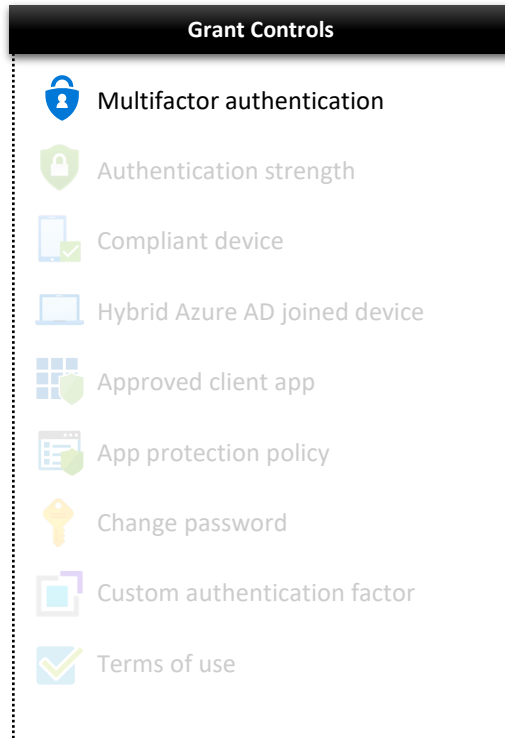
CA751-Prod-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow

Policy Enabled

Last modified: 2025-02-05



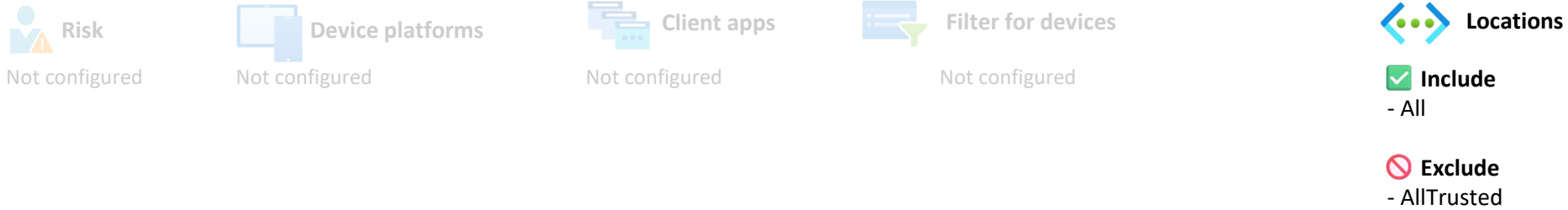
- ☒ **Include:**
 - Groups**
 - Entra-CA-AppSystem-Test-Users-Req-Pwd-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA751-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-Pwd-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)



CA752-Prod-AppSystem-Test-Users-AllApps-TrustedLocations-Pwd-Enforce

Policy Enabled

Last modified: 2025-02-05



- ☒ **Include:**
- Groups**
- Entra-CA-AppSystem-Test-Users-Req-Pwd-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA752-AppSystem-Test-Users-AllApps-TrustedLocations-Pwd-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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


CA753-Prod-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow


Policy Enabled


Last modified: 2025-02-05

 **Risk**
Not configured

 **Device platforms**
Not configured

 **Client apps**
Not configured

 **Filter for devices**
Not configured

 **Locations**
☒ **Include**
- All










☐ **Exclude**
- AllTrusted

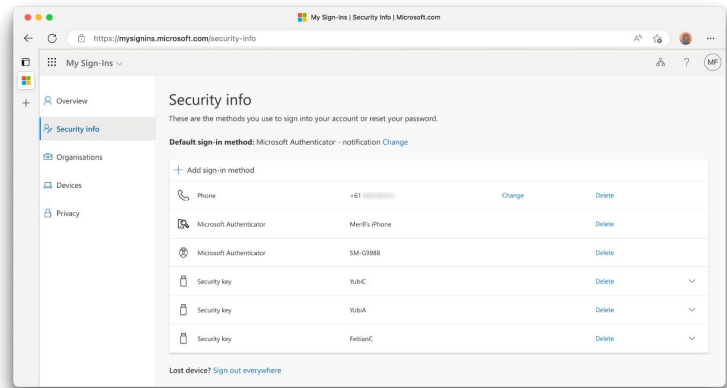
Conditions










- ☒ **Include:**
- Groups**
- Entra-CA-AppSystem-Test-Users-Req-MFA-All-Dynamic (8)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA753-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-MFA-Allow-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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


CA754-Prod-AppSystem-Test-Users-AllApps-TrustedLocations-MFA-Enforce


Policy Enabled


Last modified: 2025-02-05

 **Risk**
Not configured

 **Device platforms**
Not configured

 **Client apps**
Not configured

 **Filter for devices**
Not configured










 **Locations**
☒ **Include**
- All

☐ **Exclude**
- AllTrusted










- ☒ **Include:**
- Groups**
- Entra-CA-AppSystem-Test-Users-Req-MFA-All-Dynamic (8)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA754-AppSystem-Test-Users-AllApps-TrustedLocations-MFA-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

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

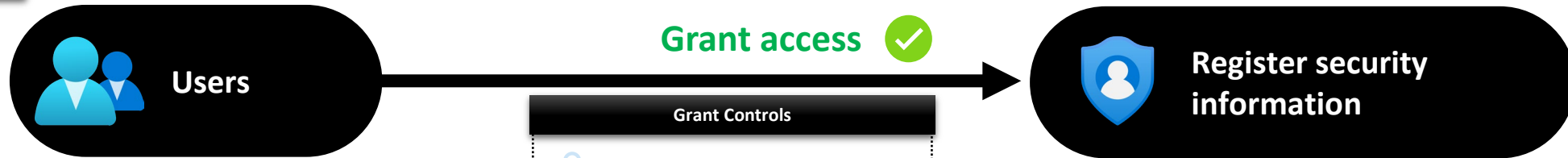
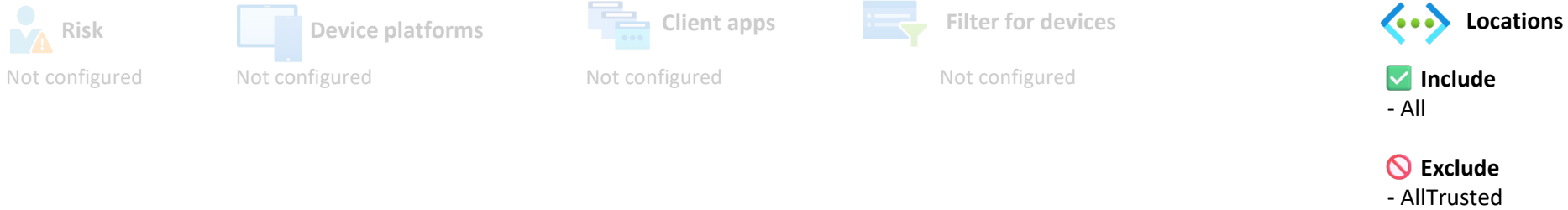
Session Controls

-  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

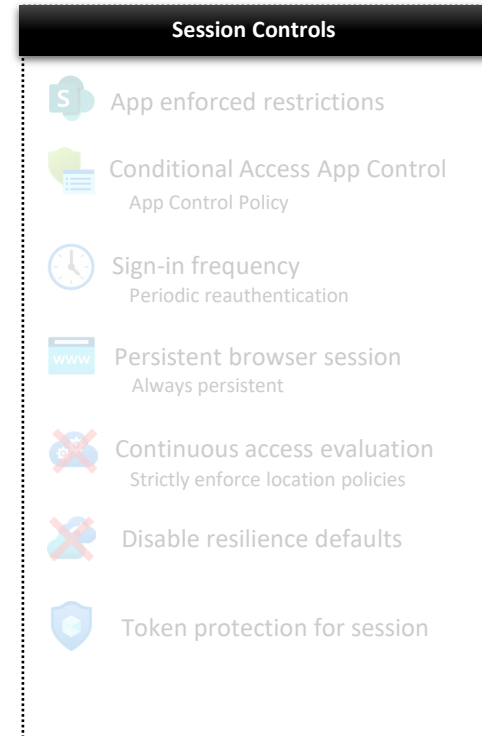
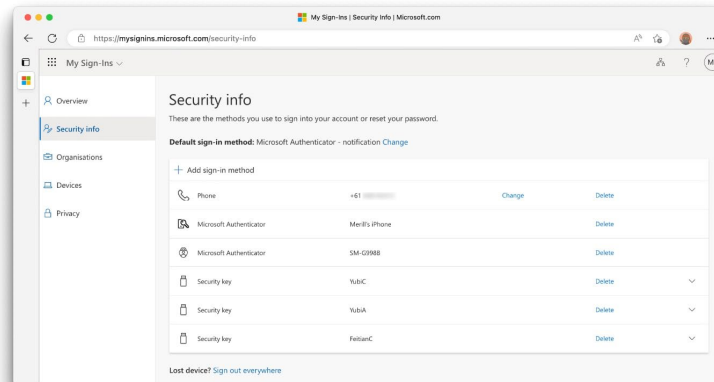
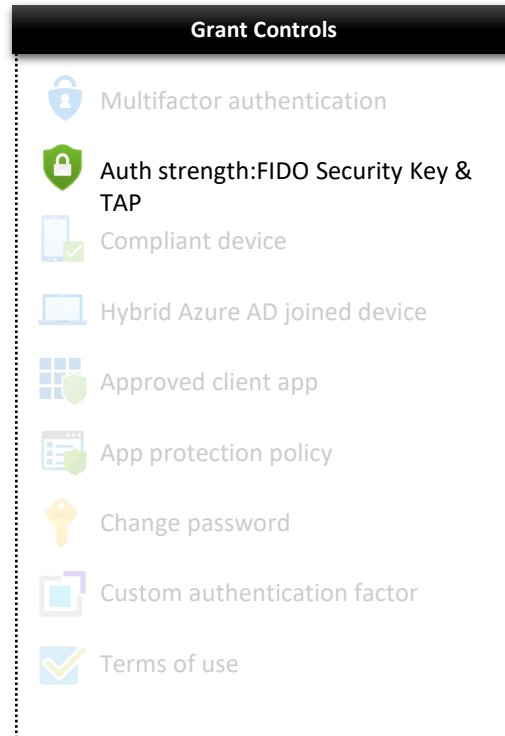
CA755-Prod-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow

Policy Enabled

Last modified: 2025-02-05




- ☒ **Include:**
 - Groups**
 - Entra-CA-AppSystem-Test-Users-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
 - Groups**
 - Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA755-AppSystem-Test-Users-RegisterSecurityInfo-TrustedLocations-FIDO-Allow-Excluded-Assigned (0)
 - Users**
 - Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)





CA756-Prod-AppSystem-Test-Users-AllApps-TrustedLocations-FIDO-Enforce


Policy Enabled


Last modified: 2025-02-05

**Risk**
Not configured

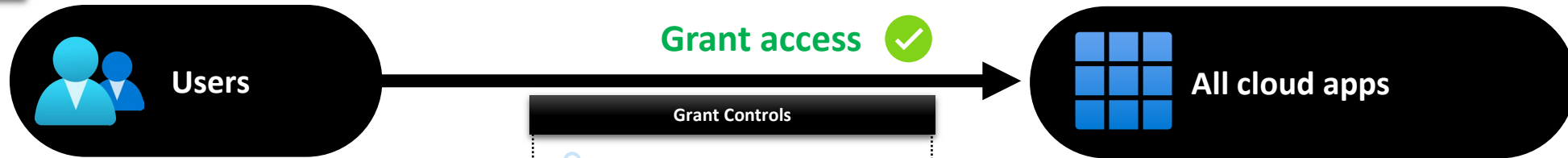
**Device platforms**
Not configured

**Client apps**
Not configured

**Filter for devices**
Not configured










**Locations**
☒ **Include**
- All

☐ **Exclude**
- AllTrusted










- ☒ **Include:**
- Groups**
- Entra-CA-AppSystem-Test-Users-Req-FIDO-All-Dynamic (0)
- ☐ **Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA756-AppSystem-Test-Users-AllApps-TrustedLocations-FIDO-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

Grant Controls

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

- ☒ **Include:**
- All

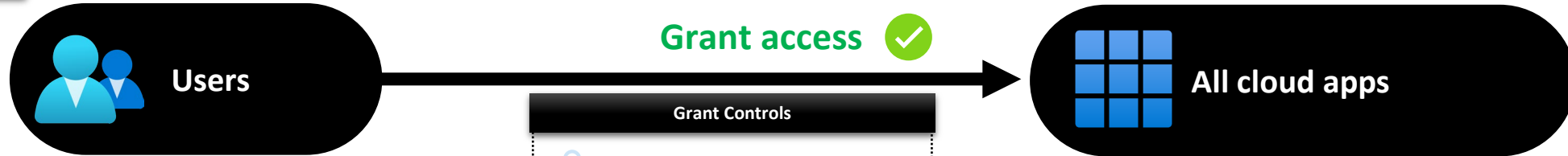
Session Controls

-  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

CA799-Prod-AppSystem-Test-Users-AllApps-AnyPlatform-SigninFrequency-Enforce

Policy Enabled

Last modified: 2025-05-03



- Include:**
- Groups**
- Entra-CA-AppSystem-Test-Users-All-Dynamic (8)
- Exclude:**
- Groups**
- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
 - Entra-CA-CA799-AppSystem-Test-Users-AllApps-AnyPlatform-SigninFrequency-Enforce-Excluded-Assigned (0)
- Users**
- Break Glass Account 0 (Entra ID)
 - Break Glass Account 1 (Entra ID)
 - Break Glass Account 2 (Entra ID)

- 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

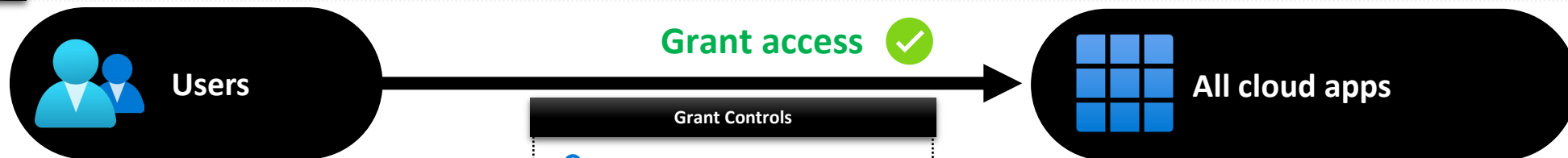
- Include:**
- All

- Session Controls**
- App enforced restrictions
 - Conditional Access App Control App Control Policy
 - Sign-in frequency 60 days
 - Persistent browser session Always persistent
 - Continuous access evaluation Strictly enforce location policies
 - Disable resilience defaults
 - Token protection for session

CA800-Prod-Users-NonManaged-AllApps-AnyPlatform-MFA-Enforce

Policy Enabled

Last modified: 2025-04-06



 **Include:**

Groups

- Entra-CA-Users-NonManaged-Req-MFA-All-Dynamic (3)

 **Exclude:**










Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)








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



CA003-Prod-Global-AllApps-AnyPlatform-LegacyAuthentication-ExchangeActiveSyncClients-Block

Policy Report-only

Last modified: 2025-04-06

- Risk**
Not configured
- Device platforms**
Not configured
- Client apps**
- Exchange ActiveSync clients
- Filter for devices**
Not configured
- Locations**
Not configured



Users

✓ **Include:**

Users

- All

✗ **Exclude:**

Groups

- Entra-CA-BreakGlassAccounts-All-Dynamic (3)
- Entra-CA-CA003-Global-AllApps-AnyPlatform-LegacyAuthentication-ExchangeActiveSyncClients-Block-Excluded-Assigned (0)

Users

- Break Glass Account 0 (Entra ID)
- Break Glass Account 1 (Entra ID)
- Break Glass Account 2 (Entra ID)

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