

Microsoft Entra Legacy Risk Policies Retire on 1 October 2026: Migration Playbook

A print-and-follow manual for moving Entra ID Protection user risk and sign-in risk policies to risk-based Conditional Access, with report-only validation and a clean rollback path.

⚠ The legacy risk policies retire on 1 October 2026. There is no automatic migration.

This playbook is designed to be printed. Work through the phases in order, tick the checklists as you go, and keep the completed copy as change evidence. Every screenshot frame carries a shot ID matching the companion shot-list, so screenshots from your own tenant can be dropped in before printing.

Version 1.0 · July 2026 · Steps verified against the Microsoft Entra admin center and Microsoft Learn on 14 July 2026 · Portal UI changes over time: if a step does not match what you see, check the changelog on the last page and the source links in the appendix.
Author: Tiago S. Carvalho · tiagoscarvalho.com · Licence context: Microsoft Entra ID P2 or Entra Suite required.



| Contents

How to use this playbook

Phase 0 — Prerequisites and inventory

Phase 1 — Pre-work: clean up before you migrate

Phase 2 — Create the user risk policy in Conditional Access

Phase 3 — Create the sign-in risk policy in Conditional Access

Phase 4 — Report-only: watch before you enforce

Phase 5 — Enforce, then disable the legacy policies (in that order)

Phase 6 — Validate, document, rollback plan

Appendix A — Passwordless variant

Appendix B — Sources and support path

Sign-off and changelog

| How to use this playbook

Why this migration exists. The user risk and sign-in risk policies configured inside Entra ID Protection (the legacy ones, on the ID Protection dashboard) retire on **1 October 2026**. Microsoft does not migrate them for you. If they are enforcing today and nothing replaces them, the accounts they protect lose risk-based protection on that date. The replacement is risk-based Conditional Access, which is better in every practical way: report-only mode, one console for all access policy, Graph automation, and risk combined with any other condition.

The golden rules baked into these pages:

- User risk and sign-in risk never share one policy. Two conditions, two policies.
- Everything starts in report-only. Nothing enforces until Phase 5.
- The new policies enforce *before* the legacy ones are disabled. No protection gap.
- Break-glass accounts are excluded from every policy, every time.

Time budget: Phases 0 to 3 fit in one focused afternoon. Phase 4 runs passively for as long as it takes to cover your normal work patterns (including at least one full work week). Phases 5 and 6 are one more hour, plus monitoring.

Do not skip Phase 0. The single most common failure in this migration is enforcing risk remediation on users who never registered for Microsoft Entra multifactor authentication. Those users do not self-remediate; they get blocked, and the helpdesk meets the project the hard way.



Phase 0 — Prerequisites and inventory

0.1 Confirm licence and role

- 1 Confirm the tenant holds **Microsoft Entra ID P2** or **Microsoft Entra Suite** licences for the users in scope. Risk-based policies are a P2 feature.
- 2 Confirm the required roles. No single least-privileged role covers every action in this playbook. Use Privileged Identity Management where available and activate only what each phase requires:
 - **Conditional Access Administrator** — create, edit and enable the new Conditional Access policies.
 - **Security Administrator** — read and change the legacy ID Protection policies and perform full ID Protection administration.
 - **Security Reader** or **Security Operator** — review the risk reports; Security Operator is required for actions such as dismissing user risk.
 - **User Administrator** — perform administrator-initiated password resets when required.

A Conditional Access Administrator alone cannot complete the inventory, remediation and legacy-policy shutdown steps in this playbook.

0.2 Find and record the legacy policies

Microsoft Entra admin center (entra.microsoft.com) > ID Protection > Dashboard

- 1 Open the ID Protection dashboard and locate the legacy **User risk policy** and **Sign-in risk policy**.
- 2 For each, record: enforcement state (On/Off), the configured risk level, the assigned users and exclusions, and the configured control. Write them in the table below; the new CA policies must cover at least this scope.

Home > ID Protection

ID Protection | User risk policy

Search

Dashboard

Risk policy impact analysis

Tutorials

Diagnose and solve problems

Protect

Conditional Access

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky agents

Risky users

Risky workload identities

Risky sign-ins

Risk detections

Settings

Users at risk detected alerts

Weekly digest

Settings

Troubleshooting + Support

New support request

This risk policy is now read-only and will be retired on October 1, 2026. To manage or modify it, migrate it to Conditional Access. Learn more. →

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk

Low and above

Controls

Access

Block access

This view is for Microsoft Entra ID P2 customers to setup user risk policy. Other customers can only disable policies here.

Policy enforcement

Enabled

Disabled

Save

SHOT-01 · A legacy policy as it exists today, retirement banner included. This is the "before" evidence; keep it.

LEGACY POLICY	STATE	RISK LEVEL	USERS / EXCLUSIONS	CONTROL
User risk policy				
Sign-in risk policy				

0.3 Verify the self-remediation prerequisites

- 1 Check MFA registration coverage: users must be registered for Microsoft Entra MFA *before* a policy asks them to remediate. Review the authentication methods registration report and chase the unregistered stragglers now.
- 2 Hybrid tenants only: confirm **password writeback** is enabled, or synced users cannot complete the secure password change that user-risk remediation requires.
- 3 Confirm your **break-glass accounts** exist, are documented, and are genuinely excluded from MFA-dependent policies.



SHOT-02 · Registration coverage before enforcement. Unregistered users become blocked users.

PHASE 0 GATE — ALL BOXES TICKED BEFORE PHASE 1

- ☐ P2 / Entra Suite licensing confirmed for users in scope
- ☐ Required Entra roles identified and activated through PIM for each phase
- ☐ Legacy policy settings recorded in the table above (screenshot taken)
- ☐ MFA registration coverage reviewed; stragglers have a plan
- ☐ Password writeback confirmed (hybrid only)
- ☐ Break-glass accounts documented and tested this quarter

Phase 1 — Pre-work: clean up before you migrate

Turning on risk-based enforcement over a pile of existing risky users creates a bad first day. Investigate and remediate what is already flagged, so the new policies start from a clean slate.

Entra admin center > ID Protection > Report > Risky users / Risky sign-ins

- 1 Open **Risky users**. Triage every user currently at risk: dismiss confirmed false positives, confirm compromise where real, remediate (password reset / session revoke) the rest.
- 2 Open **Risky sign-ins** and repeat the triage for recent detections.
- 3 List the exclusions the new policies will carry: break-glass accounts, and any service accounts still doing interactive sign-ins (flag those for replacement with managed identities; CA scoped to users does not govern service principals anyway).

Home > ID Protection

ID Protection | Risky users

Search

Dashboard

Risk policy impact analysis

Tutorials

Diagnose and solve problems

Protect

Conditional Access

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky agents

Risky users

Risky workload identities

Risky sign-ins

Risk detections

Settings

Users at risk detected alerts

Weekly digest

Settings

Troubleshooting + Support

New support request

Percentage of risky users at each risk level

37

High Risk

Medium Risk

Low Risk

No Risk

New risky users per day

6

4

2

0

07/07

07/08

07/09

07/10

07/11

07/12

07/13

Risky Users

Self Remediation Activity

1 more

Confirm user(s) compromised

Dismiss user(s) risk

Confirm user(s) safe

Reset password

Download

Block user

Refresh

Manage view

Got feedback?

Search

Add filter

Risk level : 2 selected

Risk last updated : None selected

Risk state : 2 selected

Status : Active

Reset filters

Name

Username

Risk state

Risk level

Risk last updated

No Results

SHOT-03 · The clean slate. Enforcement lands on this, not on a backlog.

PHASE 1 GATE

- ☐ Risky users triaged to zero or a known, justified remainder
- ☐ Risky sign-ins triaged
- ☐ Exclusion list written down (break-glass + documented exceptions)



Phase 2 — Create the user risk policy in Conditional Access

Feature-status check. Microsoft announced passwordless self-remediation and the Require risk remediation control as Public Preview in November 2025. As of 14 July 2026, the current implementation documentation presents the control without a visible preview badge, but no separate General Availability announcement was identified. Treat the passwordless self-remediation capability as preview unless Microsoft confirms GA through updated release notes, product documentation or your Microsoft account team.

If your organisation does not permit preview features, use the established High user risk + Require password change pattern for password-based users and retain an explicitly tested administrator-led remediation design for passwordless users.

Never combine user risk and sign-in risk in the same policy. This phase builds the user-risk policy; Phase 3 builds its sign-in sibling. Two policies, always.

Entra admin center > Entra ID > Conditional Access > New policy

- 1 Select **New policy** and name it to your standard. Suggested: `CA-Risk-UserRisk-High-RequireRemediation`.
- 2 Under **Assignments > Users or workload identities**:
 - **Include:** All users.
 - **Exclude:** emergency access accounts, Guest or external users because Require risk remediation isn't supported for them, and any documented nonhuman user accounts that can't complete interactive remediation. Select Done.

Handle guest and external user risk through a separate, explicitly tested policy or an administrator-led remediation process. Do not leave them implicitly covered by a control they can't complete.
- 3 Under **Target resources > Include**, select **All resources (formerly 'All cloud apps')**.
- 4 Under **Conditions > User risk**, set **Configure** to **Yes** and select **High**. (Microsoft's recommendation; adjust only with a written reason.) Select Done.
- 5 Under **Access controls > Grant**, select **Grant access > Require risk remediation**. Note what happens automatically:
 - **Require authentication strength** is auto-selected; choose the strength appropriate for your organisation.
 - **Sign-in frequency - Every time** is auto-applied as a mandatory session control.
- 6 Confirm the summary, set **Enable policy** to **Report-only**, and select **Create**.



Home > Conditional Access | Policies

New

Conditional Access policy

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

Name *
CA-Risk-UserRisk-High-RequireRemediation

Assignments
Users or agents
All users included and specific users excluded
Select users and groups must be configured

Target resources
No target resources selected

Network
Not configured

Conditions
0 conditions selected

Access controls
Grant
0 controls selected
Session
0 controls selected

Enable policy
Report-only On Off
Create

Control access based on who the policy will apply to, such as users and groups, agents, workload identities, directory roles, or external guests. [Learn more](#)

What does this policy apply to?
Include Exclude
Select the users and groups to exempt from the policy
Guest or external users
Directory roles
Users and groups
Select excluded users and groups
0 users and groups selected
Select at least one user or group
User-based policies apply when users access resources directly or through agents acting on the user's behalf

Select excluded users and groups

Try changing or adding filters if you don't see what you're looking for.

Search
admin
9 results found

All Users Groups

	Name	Type	Details
☐	D	Group	
☒	GA Global admin	User	
☐	BA	Group	
☐	AA	User	
☐	A	Group	
☐	BA	Group	
☐	DA	Group	
☐	I	Group	
☐	JA	Group	

Selected (1)
Reset
GA Global admin

Select

SHOT-04 · Assignments with the exclusion in place. The exclusion is the point of the screenshot.

Home > Conditional Access | Policies

New

Conditional Access policy

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

Name *
CA-Risk-UserRisk-High-RequireRemediation

Assignments
Users or agents
0 users or agents selected

Target resources
No target resources selected

Network
Not configured

Conditions
0 conditions selected

Access controls
Grant
0 controls selected
Session
0 controls selected

Enable policy
Report-only On Off
Create

Control access based on signals such as risk, device and location. [Learn more](#)

User risk
User risk level is the likelihood that the user account is compromised.
Not configured

Sign-in risk
Sign-in risk level is the likelihood that the sign-in session is compromised.
Not configured

Insider risk
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Filter for devices
Not configured

Authentication flows
Not configured

User risk

Configure
Yes No

Configure user risk levels needed for policy to be enforced
High
Medium
Low

Done

SHOT-05 · The user-risk condition. Only user risk; sign-in risk stays Not configured here.



Home > Conditional Access | Policies

New

Conditional Access policy

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

Name *

CA-Risk-UserRisk-High-RequireRemediation✓

Assignments

Users or agents

All users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network

Not configured

Conditions

0 conditions selected

Access controls

Grant *

0 controls selected

Session *

0 controls selected

Enable policy

Report-only On Off

Create

Grant

Control access enforcement to block or grant access. [Learn more >](#)

Block access

Grant access

Require multifactor authentication

Require authentication strength

Multifactor authentication...

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more >](#)

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device

Require approved client app

See list of approved client apps

Require app protection policy

See list of policy protected client apps

Require risk remediation

"Require risk remediation" can only be used when policy is assigned to "All resources (formerly 'All cloud apps')". This option requires multifactor authentication or authentication strengths controls. Other controls cannot be used. This option also requires the Session control. [Learn more >](#)

Select

SHOT-06

Require risk remediation plus the auto-applied controls.

Enable policy

Report-only On Off

It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy.

Create

SHOT-07

Report-only. The whole rollout discipline in one toggle.

PHASE 2 GATE

- ☐ Policy created and named to standard
- ☐ Break-glass excluded
- ☐ Guest and external users excluded from Require risk remediation
- ☐ Nonhuman accounts reviewed and excluded or replaced
- ☐ User risk = High; sign-in risk NOT configured in this policy
- ☐ Require risk remediation + auto controls confirmed
- ☐ State = Report-only

Phase 3 — Create the sign-in risk policy in Conditional Access

Entra admin center > Entra ID > Conditional Access > New policy

- 1 Select **New policy**. Suggested name: `CA-Risk-SignInRisk-MedHigh-RequireMFA`.
- 2 Under **Assignments** > **Users or workload identities**:
 - **Include**: All users.
 - **Exclude**: emergency access accounts and any documented nonhuman user accounts that can't complete interactive multifactor authentication. Decide explicitly how guest and external users are handled, based on your cross-tenant MFA trust configuration, and test that population separately. Select Done.
- 3 Under **Cloud apps or actions** > **Include**, select **All resources (formerly 'All cloud apps')**.
- 4 Under **Conditions** > **Sign-in risk**, set **Configure** to **Yes** and select **High** and **Medium**. Select Done.
- 5 Under **Access controls** > **Grant**, select **Grant access** > **Require authentication strength** and pick the built-in **Multifactor authentication** strength. Select Select.
- 6 Under **Session**, select **Sign-in frequency**, ensure **Every time** is selected, then Select. (A successful strong authentication is the only way a user self-remediates sign-in risk; every-time frequency makes sure the prompt actually happens.)
- 7 Confirm the summary, set **Enable policy** to **Report-only**, and select **Create**.

SHOT-08 · The sign-in risk condition, Medium + High per Microsoft's recommendation.

Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication

⚠

"Require authentication strength" cannot be used with "Require multifactor authentication".
[Learn more](#)

☒ Require authentication strength

Multifactor authentication

ℹ

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users.
[Learn more](#)

☐ Require device to be marked as compliant

☐ Require Microsoft Entra hybrid joined device

☐ Require approved client app
[See list of approved client apps](#)

SHOT-09 · Authentication strength as the grant control.

Home > Conditional Access | Policies

New

Conditional Access policy

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

Name *

CA-Risk-SigninRisk-MedHigh-RequireMFA

Assignments

Users or agents

0 users or agents selected

Target resources

No target resources selected

Network

Not configured

Conditions

0 conditions selected

Access controls

Grant *

0 controls selected

Session *

0 controls selected

Enable policy

Report only

OnOff

⚠

It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy.

Create

Session

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

☐ Use app enforced restrictions

ℹ

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app-enforced restrictions. [Learn more](#)

☐ Use Conditional Access App Control

☒ Sign-in frequency

☐ Periodic reauthentication

☒ Every time (5 minute tolerance)

☐ Persistent browser session

☐ Customise continuous access evaluation

☐ Disable resilience defaults

☐ Require token protection for sign-in sessions (Generally available for Windows. Preview for MacOS, iOS)

☐ Use Global Secure Access security profile

ℹ

This option only works with Global Secure Access resources.

Select

SHOT-10 · Every time. Without it, a stale session can outlive the risk.

PHASE 3 GATE

- ☐ Second policy created; user risk NOT configured in it
- ☐ Guest and external user handling decided and tested
- ☐ Sign-in risk = Medium + High
- ☐ Auth strength = Multifactor authentication
- ☐ Sign-in frequency = Every time
- ☐ State = Report-only



Phase 4 — Report-only: watch before you enforce

Both policies now evaluate every sign-in and record what they *would* have done, without touching anyone. This phase is where surprises surface for free.

[Entra admin center](#) › [Entra ID](#) › [Conditional Access](#) › [Insights and reporting](#) | [Sign-in logs](#) › (a sign-in) › **Report-only tab**

- 1 Let the policies run in report-only long enough to cover normal work patterns, including at least one full work week (month-end or shift patterns may justify longer).
- 2 **Prerequisite check:** the insights workbook requires an Azure subscription with a Log Analytics workspace and Entra diagnostic settings streaming sign-in logs to it. Without the required Log Analytics integration and permissions, the workbook won't populate and can return configuration or authorization errors. The no-cost fallback: filter **Sign-in logs** by date range and read the Report-only tab per sign-in, or open each policy and use its impact summary. Same answers, more clicks.
- 3 Review the Conditional Access insights workbook filtered to the two new policies. Questions to answer:
 - Who *would* have been prompted or blocked, and does the list make sense?
 - Any service or shared accounts appearing? They need the managed-identity conversation, not an exclusion-forever.
 - Any user who would fail remediation because they are still unregistered for MFA?
- 4 Spot-check individual sign-ins: open a sign-in log entry and read the **Report-only** tab to see each policy's would-be result.
- 5 Fix what surfaced (register users, adjust exclusions with written justification) and, if anything material changed, extend the observation window.

SHOT-11 · Evidence to capture in your own tenant during the report-only window: the impact view (insights workbook where Log Analytics is configured; filtered sign-in logs otherwise).



Activity Details: Sign-ins



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

Search

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓	
CA-Risk-SignInRisk-MedHigh...		Sign-in frequency	Report-only: Not applied	...
CA-Risk-UserRisk-High-Requir...	AdaptiveRiskRemediation	Sign-in frequency	Report-only: Not applied	...

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

SHOT-12 · Ground truth for one sign-in. Spot-checks catch what dashboards average away. "Not applied" here means the sign-in carried no risk; the policies evaluated it and stood down.

PHASE 4 GATE — THE ENFORCEMENT DECISION

- ☐ Observation window covered normal work patterns (min. one full work week)
- ☐ Insights reviewed; would-be impact understood and acceptable
- ☐ MFA registration gaps closed for affected users
- ☐ Exceptions documented with owner and review date

Phase 5 — Enforce, then disable the legacy policies (in that order)

Order matters. Enable the Conditional Access policies first; only then disable the legacy ID Protection policies. Reversing the order opens a window with no risk protection at all. Do both steps in the same session, with the sign-in logs open.

5.1 Enable the CA policies

Entra admin center > Entra ID > Conditional Access > Policies

- 1 Open the user-risk policy, move **Enable policy** from **Report-only** to **On**, save.
- 2 Open the sign-in-risk policy, do the same.
- 3 Watch the sign-in logs for the first hour. The expected experience: risky sign-ins get an MFA prompt; high-risk users get the remediation flow. The unexpected experience is why you are watching.

Home > Conditional Access

Conditional Access | Policies

Overview Policies Deleted Policies Phased rollout Insights and reporting Diagnose and solve problems Manage Named locations Custom controls (Preview) Terms of use VPN connectivity Authentication contexts Authentication strengths Classic policies Monitoring Sign-in logs Audit logs Troubleshooting + Support New support request

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

2 out of 2 policies found

Policy name	Created by	State	Alert	Creation date	Modified date
CA-Risk-SignInRisk-MedHigh-RequireMFA	USER	On		7/14/2026, 2:01:08 ...	7/15/2026, 8:33:35 ...
CA-Risk-UserRisk-High-RequireRemediation	USER	On		7/14/2026, 2:04:05 ...	7/15/2026, 8:34:16 ...

SHOT-13 · Enforcement live: both risk policies On. This is change evidence; keep it.

5.2 Disable the legacy policies

Entra admin center > ID Protection > Dashboard > User risk policy / Sign-in risk policy

- 1 Open the legacy **User risk policy** and set **Enforce policy** to **Disabled**.
- 2 Repeat for the legacy **Sign-in risk policy**.

- 3 Do not delete anything. Disabled legacy policies are your rollback lever until the retirement date makes them irrelevant.

Home

User risk policy

This risk policy is now read-only and will be retired on October 1, 2026. To manage or modify it, migrate it to Conditional Access. Learn more.

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk

Low and above

Controls

Access

Block access

Policy enforcement

Enabled Disabled

Save

SHOT-14 · The legacy policy standing down: retirement banner above, enforcement Disabled below. The "after" evidence to pair with SHOT-01.

PHASE 5 GATE

- ☐ Both CA policies On (CA first, always)
- ☐ First-hour sign-in logs reviewed; no unexpected blocks
- ☐ Both legacy policies Disabled (not deleted)
- ☐ Helpdesk briefed: what the remediation prompt looks like, what to do when a user calls



Phase 6 — Validate, document, rollback plan

6.1 Validation within the first week

- 1 Confirm at least one real medium- or high-risk sign-in was challenged and self-remediated. If no suitable event occurs naturally, use a dedicated test account and follow Microsoft's Simulate risk detections guidance. Tor Browser can be used to simulate an anonymous-IP detection, but a VPN alone doesn't reliably generate sign-in risk. Never test with a production administrator or emergency access account.
- 2 Review helpdesk tickets tagged to the change. Most surprises trace back to registration gaps, authentication-strength mismatches, conflicting Conditional Access policies or exclusions that were never formally documented.
- 3 Re-run the insights workbook in enforcement mode and file the export with this playbook.

6.2 Rollback plan (write it before you need it)

SCENARIO	ACTION
Widespread false-positive prompts	Move the affected CA policy back to Report-only ; re-enable the corresponding legacy policy if before 1 Oct 2026; investigate levels/exclusions; re-run Phase 4.
Specific user locked out	Admin-remediate in ID Protection (dismiss/confirm + reset), register MFA, unblock; no policy change for one user.
Break-glass locked out (should be impossible)	Exclusion failed: this is the drill you tested in Phase 0. Use the second break-glass account, fix the exclusion, write the post-mortem.

6.3 Evidence pack

Staple (physically or digitally) into the change record: SHOT-01 and SHOT-14 (before/after), the Phase 0 table, the Phase 4 insights export, this playbook with ticked gates, and the sign-off below. For organisations in scope of NIS2, this evidence pack can support the documentation of access-control and multifactor-authentication measures associated with Article 21. It is one piece of the organisation's wider cybersecurity risk-management evidence and does not, by itself, demonstrate NIS2 compliance.

Appendix A — Passwordless variant

If a population signs in passwordless, create a *separate* sign-in-risk policy targeted at that group: same conditions (sign-in risk Medium + High), but the grant control uses the built-in **Passwordless MFA** or **Phishing-resistant MFA** authentication strength, matching what those users actually hold; session control stays Sign-in frequency: Every time.

For user risk, the Require risk remediation control uses a Microsoft-managed flow based on the detected threat and the user's authentication method. For passwordless authentication scenarios where the active risk doesn't involve a compromised password, Microsoft Entra revokes the affected sessions and requires the user to authenticate again using the selected authentication strength. Validate the complete



remediation experience in report-only mode and with dedicated test accounts before production enforcement.

Appendix B — Sources and support path

- Microsoft Learn: Configure and enable risk policies — steps and recommendations mirrored by this playbook, including the migration section, the 1 October 2026 retirement warning and the support path; verified 14 July 2026.
- Microsoft Learn: ID Protection risk-based access policies — Require risk remediation behaviour and guest/external limitations.
- Microsoft Entra release archive — Public Preview announcement for passwordless self-remediation, November 2025.
- Microsoft Learn: Conditional Access insights and reporting workbook — Log Analytics prerequisites and report-only review.
- Microsoft Learn: Simulate risk detections — safe test patterns for anonymous IP and unfamiliar sign-in properties.
- EUR-Lex: Directive (EU) 2022/2555 (NIS2) — Article 21 context for the evidence-pack note.
- Stuck? Microsoft support path: Entra admin center > New support request > "Migrate legacy ID Protection policy" > service type Microsoft Entra Sign-in and Multifactor Authentication > problem type Identity Protection > Configure risk policies.

Sign-off

ROLE	NAME	DATE	SIGNATURE
Implemented by			
Reviewed by			
Change approved by			

Changelog

VERSION	DATE	CHANGES
1.0	July 2026	First edition. Steps verified against the Entra admin center and Microsoft Learn on 14 July 2026.