



Migrate to the Future: Entra Authentication Methods for MFA & SSPR

Legacy policies are retiring — Here's how to modernize before September 2025

Legacy MFA & SSPR Are Retiring in September 2025

- Microsoft will retire all **legacy per-user MFA and SSPR policies**.
- Organizations must migrate to the **Authentication Methods policy** in Microsoft Entra.
- Failure to act can break sign-in and recovery flows.
-  **Deadline:** September 30, 2025



Why Is This Migration So Important?

 **Security:** Legacy policies lack modern controls like Conditional Access.

 **Break Risk:** Apps relying on old policies may **fail** post-retirement.

 **No Support:** Microsoft will **deprecate** updates and support for legacy methods.

 **Unified Experience:** The new Authentication Methods policy **centralizes** MFA, SSPR, and FIDO2 in one place.

Legacy MFA & SSPR Deprecation Timeline: Key Milestones

 September 30, 2025 – Legacy MFA/SSPR policies deprecated

 No new tenants can use legacy policies

 Existing tenants can no longer create or edit old policies

 All organizations must adopt the Authentication Methods policy

 Migration tools available in Microsoft Entra Admin Center

Meet the Future: Microsoft Entra Authentication Methods Policy



CENTRALIZED CONTROL FOR MFA, SSPR, AND PASSWORD LESS METHODS



SUPPORTS MODERN METHODS LIKE FIDO2, MICROSOFT AUTHENTICATOR, SMS, EMAIL



GRANULAR TARGETING WITH CONDITIONAL ACCESS & USER GROUPS



IMPROVED INSIGHTS AND REPORTING ACROSS SIGN-INS



BUILT FOR ZERO TRUST AND FUTURE-READY IDENTITY STRATEGIES

Home > Enriched Microsoft 365 logs > Perparims Cloud Solutions >

Authentication methods | Policies

Perparims Cloud Solutions - Microsoft Entra ID Security

Search < Add external method (Preview) Refresh

Manage

Policies

- >Password protection
- Registration campaign
- Authentication strengths
- Settings

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Authentication method policies

Use authentication methods policies to configure scope for a method, they may use it to authenticate scenarios). [Learn more](#)

Method

Built-In

- Passkey (FIDO2)
- Microsoft Authenticator
- SMS
- Temporary Access Pass
- Hardware OATH tokens (Preview)
- Third-party software OATH tokens
- Voice call
- Email OTP
- Certificate-based authentication
- QR code

Migration Journey: From Legacy to Modern Authentication

- 1** **Review legacy MFA & SSPR settings** in Entra Admin Center 
- 2** **Enable the Authentication Methods policy** (preview or production) 
- 3** **Target test groups first** — apply policy in stages 
- 4** **Verify registration methods & user readiness** 
- 5** **Monitor using Sign-in logs and Authentication Details** 
- 6** **Fully transition and disable legacy policies before September 2025** 

Legacy MFA vs. Authentication Methods Policy

-  Legacy MFA/SSPR
- Separate settings from MFA and SSPR
- No granular user targeting
- Limited modern methods
- Minimal reporting and insights
- Deprecated by Microsoft

Vs.

-  Authentication Methods Policy
- Unified, centralized policy
- Target by groups and Conditional Access
- Supports FIDO2, Authenticator, SMS, etc.
- Rich sign-in logs and registration tracking
- Ongoing feature development and support

 **Tip:** Legacy MFA and SSPR settings can appear active even when not in use — review and disable them to avoid confusion during migration.

Microsoft Authenticator settings

X

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more.](#)

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups

Name	Type	Registration	Authentication mode
All users	Group	Optional	Any

Step-by-Step: Enabling Microsoft Authenticator in the New Policy



Tip: Always test with a small pilot group before enabling methods for your full organization.

- 1 Go to Microsoft Entra Admin Center → Protection → Authentication Methods
- 2 Select “Microsoft Authenticator” from the Built-in methods list
- 3 Toggle "Enable" to On
- 4 Choose target: All Users or Select Groups
- 5 (Optional) Adjust registration & authentication mode
- 6 Click Save — policy is now live for targeted users

Configure Microsoft Authenticator for Enhanced Security

- Allow or block Microsoft Authenticator OTP
- Require number matching for push approvals (enabled by default)
- Choose notification types: app name, geo-location, etc.
- Target specific groups for customized experiences
- Align settings with your organization's MFA policy

Home > Enriched Microsoft 365 logs > Perparims Cloud Solutions > Authentication methods | Policies >

Microsoft Authenticator settings ...

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The feature is currently in preview.

Enable and Target [Configure](#)

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Enable and Target' tab.

GENERAL

Allow use of Microsoft Authenticator OTP [Yes](#) [No](#)

Require number matching for push notifications

Note: This feature has been enabled for all users of the Microsoft Authenticator. [Learn more](#)

Status [Enabled](#)

Target [Include](#)

All users

Select group

Show application name in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status [Microsoft managed](#)

Target [Include](#) [Exclude](#)

All users

Select group

Show geographic location in push and passwordless notifications

[Save](#) [Discard](#)

Home > Enriched Microsoft 365 logs > Perparims Cloud Solutions > Authentication methods | Policies >

Microsoft Authenticator settings ...

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status [Microsoft managed](#)

Target [Include](#) [Exclude](#)

All users

Select group

Show geographic location in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status [Microsoft managed](#)

Target [Include](#) [Exclude](#)

All users

Select group

Microsoft Authenticator on companion applications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status [Microsoft managed](#)

Target [Include](#) [Exclude](#)

All users

Select group

[Save](#) [Discard](#)

Tip: Enforcing number matching significantly reduces MFA fatigue and phishing risks.

Authentication Methods	UserManagement	User registered security ...	Success	User registered Authenticator App with N...
Authentication Methods	UserManagement	User started security inf...	Success	User started the registration for Authentic...
Core Directory	UserManagement	Update user	Success	

User successfully registered Microsoft Authenticator with push notifications

Monitor and Validate Authentication Activity

- Use Sign-in logs to track user access, success, and failure reasons
- Validate that users are registering Authenticator methods successfully
- Monitor Conditional Access policies (Report-only mode available)
- Identify sign-in interruptions or blocked legacy authentication
- Export data or connect to Sentinel for deeper analytics

Tip: Conditional Access in report-only mode is a great way to simulate and test your MFA strategy without impacting users.

Copilot

Activity Details: Sign-ins

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

Search

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓
Block Legacy Authentication	Block		Report-only: Failure
Require MFA for All Users	Require multifactor authentica...		Report-only: User action requir...
Require MFA for Admins	Require multifactor authentica...		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.

Conditional Access policies set to Report-only mode for safe testing

User ↑↓	Application ↑↓	Status	Sign-in error code
Perparim Abdullahu	Azure Portal	Success	0
Sophia Davis	Azure Portal	Success	0
Sophia Davis	Azure Portal	Interrupted	50140
Sophia Davis	Azure Portal	Success	0
Sophia Davis	Azure Portal	Interrupted	50140
Sophia Davis	Azure Portal	Interrupted	50055
Sophia Davis	Azure Portal	Failure	50126
Sophia Davis	Azure Portal	Failure	50126
Sophia Davis	Azure Portal	Failure	50126

Secure the Future: Move Beyond Legacy Authentication Today

Ready to lead your organization forward?

Start your migration now and embrace secure, modern identity management with Microsoft Entra.



Legacy MFA & SSPR policies are being deprecated by September 2025



Microsoft Entra Authentication Methods Policy is the future



Offers centralized control, flexible targeting, and modern methods



Real-time monitoring ensures visibility, accountability, and security



Start migrating early — test, measure, and empower your users

Tip: Identity is the new perimeter — modernize it before the deadline forces your hand.

Real Labs. Real Identity. Real Security.



#PerparimLabs | #MicrosoftEntra | #ModernAuth |
#SC300 | #IdentityGovernance