

🔍 Filter by title

Microsoft Entra ID Protection Documentation

> Overview

> Concepts

▾ How-to guides

Deploy Microsoft Entra ID Protection

Configure notifications

▾ Policy configuration

Configure the MFA registration policy

Configure risk policies

Simulate risk detections

> Investigate and remediate

Provide feedback on risk detections

Impact analysis workbook

> Reference

> Resources

Learn / Microsoft Entra / Microsoft Entra ID Protection /

⊕ ✎ ⋮

How To: Configure the multifactor authentication registration policy

Article • 05/06/2024 • 4 contributors

👍 Feedback

In this article

- Policy configuration
- User experience
- Related content

Microsoft helps you manage the deployment of multifactor authentication (MFA) by configuring the Microsoft Entra ID Protection policy to require MFA registration no matter what modern authentication app you're signing in to. Multifactor authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins. In order for users to be able to respond to MFA prompts, they must first register authentication methods, like the Microsoft Authenticator app.

We recommend that you require multifactor authentication for all user sign-ins. [Based on our studies](#) [↗], your account is more than 99% less likely to be compromised if you use MFA. Even if you don't require MFA all the time this policy ensures your users are ready when the time comes to do MFA.

For more information, see the article [Common Conditional Access policy: Require MFA for all users](#).

Policy configuration

- Sign in to the [Microsoft Entra admin center](#) [↗] as at least a [Security Administrator](#).
- Browse to **Protection > Identity Protection > Multifactor authentication registration policy**.
 - Under **Assignments > Users**.
 - Under **Include**, select **All users** or **Select individuals and groups** if limiting your rollout.
 - Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
- Set **Policy enforcement** to **Enabled**.
- Select **Save**.

User experience

Microsoft Entra ID Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they're required to register before they can complete the sign-in process.

For an overview of the related user experience, see:

- [Sign-in experiences with Microsoft Entra ID Protection](#).

Related content

- [Enable sign-in and user risk policies](#)
- [Enable Microsoft Entra self-service password reset](#)
- [Enable Microsoft Entra multifactor authentication](#)

Feedback

📄 Download PDF

Page 1 of 2

Was this page helpful?

Yes

No

[Provide product feedback](#)

Additional resources





Training

Module
[Secure Microsoft Entra users with multifactor authentication - Training](#)

Learn how to use multifactor authentication with Microsoft Entra ID to harden your user accounts.

Certification
[Microsoft Certified: Identity and Access Administrator Associate - Certifications](#)

Demonstrate the features of Microsoft Entra ID to modernize identity solutions, implement hybrid solutions, and implement identity governance.

 English (United States)  Your Privacy Choices  Theme 

[Manage cookies](#) [Previous Versions](#) [Blog](#) [Contribute](#) [Privacy](#) [Terms of Use](#) [Trademarks](#) [© Microsoft 2024](#)