

# THE INSIGHTS








Author: [Mick McLean](#) | Published: 14th December, 2023

## Welcome to your December update

We know it's difficult to keep up with the number of changes and releases that come from Microsoft.

That's why every month we highlight the latest updates that are important to your business.

## Contents

-  Conditional Access policies will be added to Microsoft managed tenants **P. 2**
-  Microsoft Entra ID now supports more device-bound passkeys **P. 3**
-  Authenticator prompts that pose a risk will now be suppressed **P. 3**
-  SharePoint archiving is now easier in the admin centre **P. 4**
-  Users are being encouraged to create channels instead of teams **P. 4**

## Conditional Access policies will be added to Microsoft managed tenants

Probably the most important update to be released, Microsoft are creating new Conditional Access policies in your tenant.

[Conditional Access](#) minimises the risk of unauthorised access to resources and this update shows Microsoft's ongoing commitment to enforcing [Zero Trust](#) security measures like [multifactor authentication](#) (MFA).

Studies conducted by Microsoft have shown that [MFA reduces the risk of an account being taken over by over 99%](#), and its Microsoft's goal to have 100% MFA across their customers.

These policies will be created in report-only mode, which means that they won't block any access, but they will generate reports on how they'll affect users when they're switched to the 'on' state. After the policies have been created in your tenant, you'll have 90 days to evaluate and configure them.

Then, if you haven't already moved them to the 'on' or 'off' state, they'll be automatically moved to 'on'. Once the policies are enabled, users covered by them will need to have multifactor authentication.

This is being rolled out as of November/ December 2023, so you will need to review these policies early in the new year.



You can learn more about using Microsoft to apply zero trust principles to your security strategy in our on-demand webinar [Key principles of Microsoft Zero Trust](#).

Or, you can book a more [detailed consultation](#) with one of our experts to discuss how this will affect your organisation, security strategy, Microsoft environment and user experience.



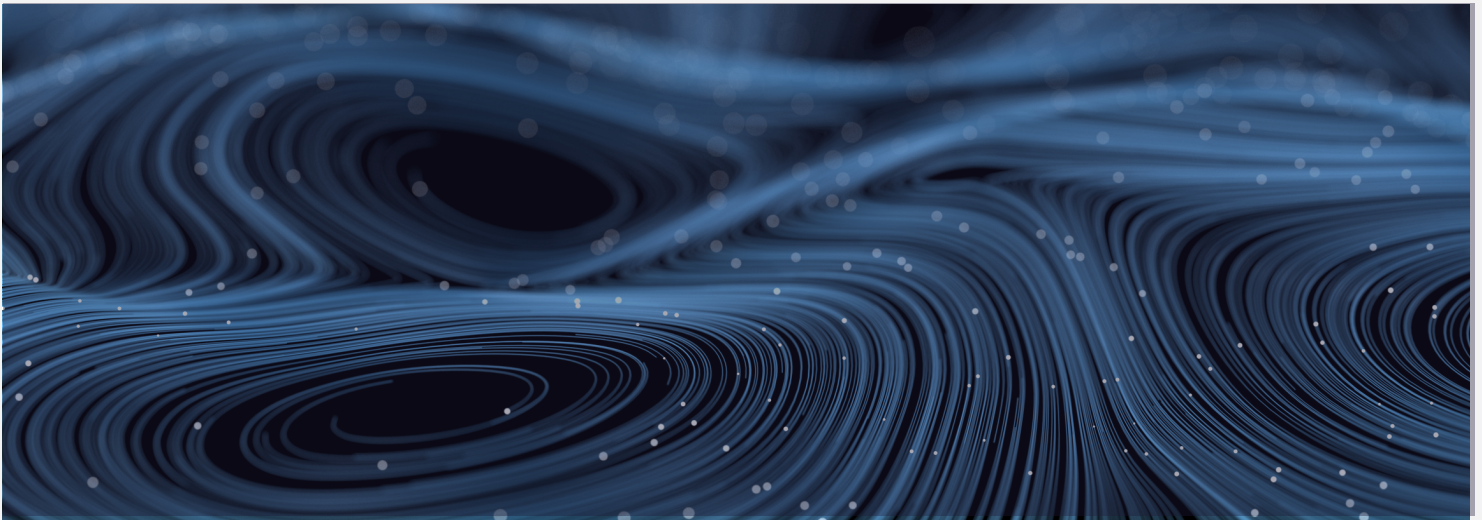
## Microsoft Entra ID now supports more device-bound passkeys

Another push by Microsoft to increase the use of MFA technologies across their customers, Microsoft Entra ID will now support device-bound passkeys stored on computers and mobile devices as an authentication method.

Unlike traditional MFA methods that send notifications and prompts, device-bound passkeys can't be spoofed, so employees can't be tricked into granting unauthorised access.

This is being rolled in January 2024 and is in addition to the existing support for FIDO2 security keys. This will enable your employees to perform phishing-resistant authentication using the devices that they already have.

This is a rising trend in security as it defends against more [sophisticated phishing attacks](#) for organisations with highly sensitive data that are prime targets for cyber criminals.



## Authenticator prompts that pose a risk will now be suppressed

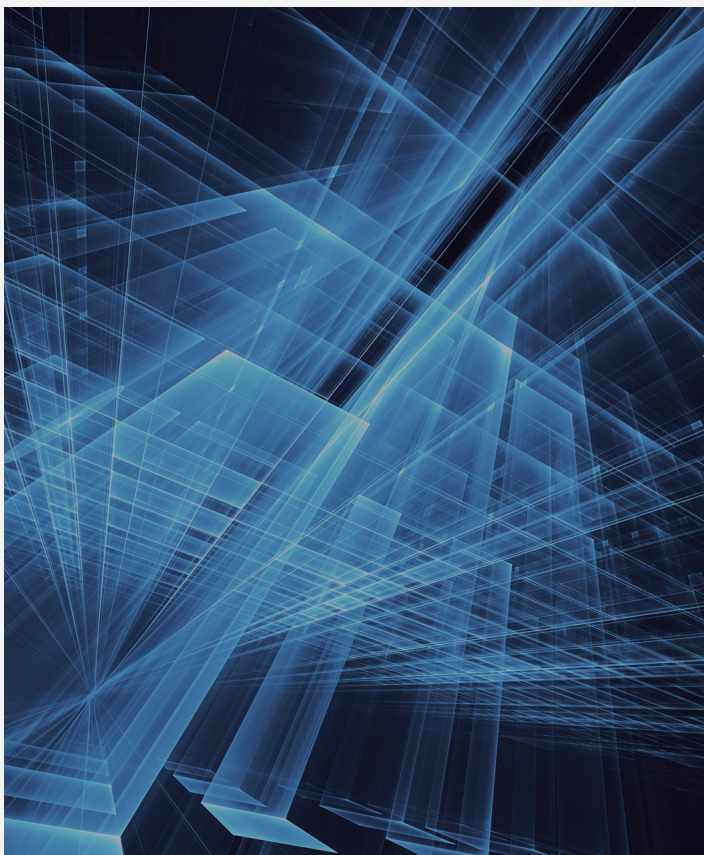
In the third of Microsoft's contextual access updates, they will now suppress Authenticator notifications when a request displays potential risks, such as when it originates from an unfamiliar location or is exhibiting other anomalies.

Notifications will still be stored and accessible within the app, but suppressing the prompt but a break in the chain for employees, making them stop and think before they approve access requests.



While this is a significant step in reducing human error you should still provide [ongoing training](#) to help employees understand their roles and responsibilities in maintaining a secure environment.

To further explore the right MFA solution for your organisation, book a [free consultation](#) with our security experts.



## SharePoint archiving is now easier in the admin centre

To help ease the management of [SharePoint](#) and data sprawl, Sharepoint and global admins can now choose inactive sites in the SharePoint admin centre (and via PowerShell) to archive them.

Admins can select one or more sites in the 'active sites' page and archive them using the command bar.

When archived, the storage occupied by the site is deducted from active storage and charged as a part of archived storage, which is charged based on consumption.

This will help admins more easily manage their Microsoft environment and ongoing spend.

## Users are being encouraged to create channels instead of teams

Further helping customers to combat SharePoint and data sprawl, Microsoft are now encouraging users to create 'channels' instead of 'teams'. This will minimise the number of SharePoint sites inadvertently being created, helping to reduce the complexity and management of your Microsoft estate.

Users will now be able to create a [team](#) or channel from the top "+" button. The "create channel" option has been lifted to the top of the screen, promoting this as the easier option and reducing team proliferation.



Managing the proliferation of data across teams and SharePoint sites is a common challenge for enterprises. We recommend booking a more [detailed consultation](#) with one of our experts to discuss best practice governance of your Microsoft estate.