+44 345 094 0945
www.waterstons.com

Article

Apr 2022

A practical guide to setting up MFA for Microsoft 365

Multi-factor Authentication (MFA) is an effective way of preventing hackers from accessing your accounts, even if they manage to crack your password.

What is MFA?

It is a security measure that requires two or more methods of proof of identity to access an account.

This could be a combination of:

1. Something you know e.g., a password or PIN
2. Something you have e.g., a mobile device with an authenticator app installed
3. Something you are e.g., a fingerprint, iris or face scan

Proof	You	Hacker
Something you know	✓	✓
Something you have	✓	✗
Something you are	✓	✗
Login successful?	✓	✗

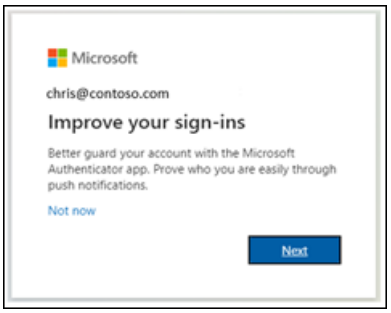
The reason MFA helps to thwart access to accounts is that it ensures that the person logging in is the owner of the account and not a hacker.

Only the owner would have each of the three forms of identification. The hacker may know the password but that's all, so their attempt to access the account will fail.

Enrolling and educating all parties is the hardest part of MFA setup, but thankfully there is a tool to help with enrolment so that you can focus on educating users on how to use MFA.

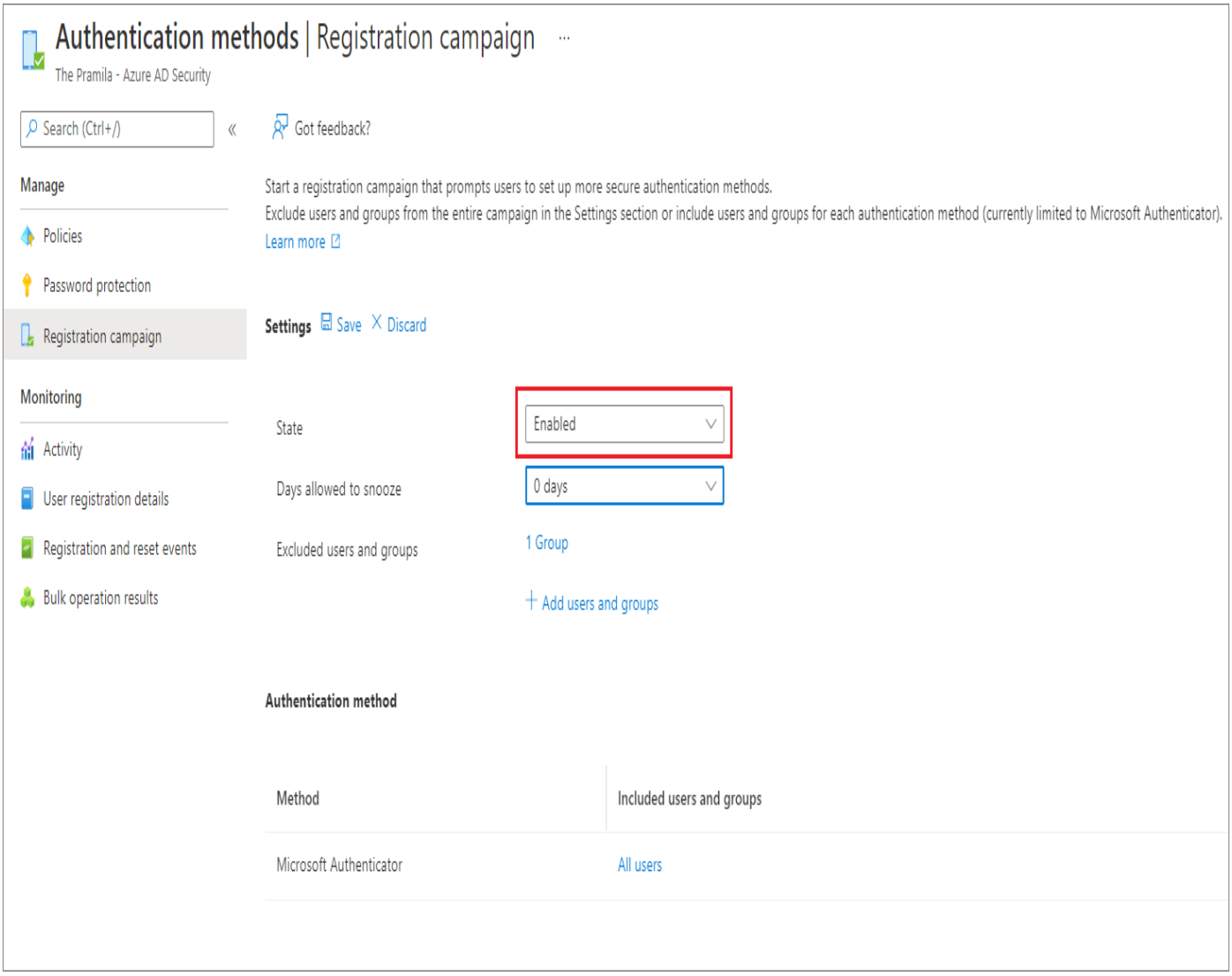
Setting up MFA

You can nudge users to set up the Microsoft Authenticator app when they next sign in, which will result in this popup encouraging them to improve their sign-in experience.



This is achieved through enabling a registration campaign to the users who are required to configure MFA by following these steps:

1. In the Azure AD portal (https://portal.azure.com), click **Security** > **Authentication methods** > **Registration campaign**
2. For **State**, click **Enabled**, select any users or groups to exclude from the registration campaign such as VIP users that you will personally assist.
3. For **Days allows to snooze** choose the number of days in which after users will be required to configure MFA, then click **Save**.



Prompt fatigue

MFA is designed to stop hackers from getting access to your users' accounts, but what if they allow them in anyway?

In a scenario where a hacker has learnt the 'something you know', they have the user's password and are trying to access their account when suddenly they need to do the 'something you have' (tap approve in the Microsoft Authenticator app), using the 'something you are' (by unlocking the phone using their fingerprint).

The user gets a prompt and ignores it because they aren't logging in. Yay, they didn't let the hacker in, phew!

But the hacker doesn't give up.

They still have the 'something you know' so will keep trying, and trying, and trying, meaning the user keeps getting prompt, after prompt, after prompt, until they get fed up and tap that approve button just to make it go away.

Which of course it does; the hacker is in and has full access to that user's files and system - the equivalent of opening the door to a bugler and inviting them in.

This is prompt fatigue, and it's completely preventable by educating your users on the dangers of blindly approving log in attempts and what they can do to stop them. The number 1 tool we have is reporting.

Reporting

The hacker has got the user's password and they are trying to log in. The user gets the prompt, but taps 'deny' as they know they're not trying to access their account.

The attempt has been thwarted, and the user can now report the fraud by tapping the button and sending a report to IT who will then action it.

And what is that action?

The information from the report can help the IT team understand more about the breach, but the important thing is to make sure that the hacker doesn't have correct information.

Changing the password. It's that simple.

MFA is just one area where cloud and security services can protect your users, business and data.

To find out more about how you can protect them, talk to our cloud solutions team today.

For more information on how we can support the future of work in your business, find out more here.