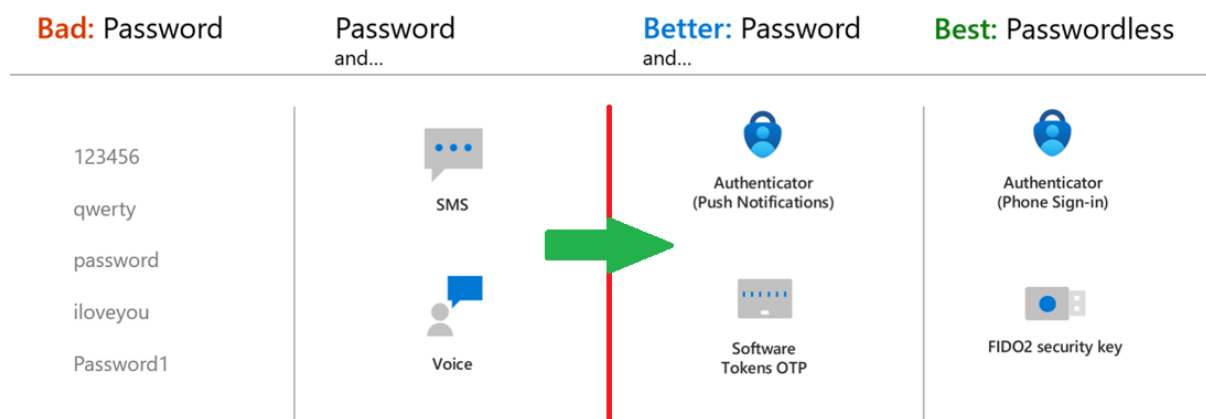


Why Short Message Service/Voice Authentication is Going

Further information on the removal of SMS/voice as an authentication method

Important Update: Removal of SMS/Voice Authentication for All Accounts

As part of our ongoing commitment to strengthening security across the university, and due to upcoming changes from Microsoft, we are retiring SMS and voice call authentication methods for all accounts.



Why This Change Is Necessary

Microsoft currently provide a service through which our SMS and Voice calls are made, this service is being retired shortly, and we need to migrate before this deadline comes into effect. Also, while SMS and voice-based authentication methods are better than having no multi-factor authentication (MFA) at all, they are no longer considered sufficiently secure. These methods are vulnerable to several well-known attacks, including:

- **SIM swapping:** where attackers hijack your phone number to intercept authentication codes
- **SMS interception:** via malware, legacy telecom protocols like SS7, or third-party rerouting services
- **Adversary-in-the-Middle (AiTM) phishing:** attackers use proxy sites to intercept login credentials and SMS-based MFA codes, allowing them to hijack sessions and bypass authentication
- **Physical access:** office phones or shared landlines that are unsecured or accessible to others
- **Voicemail attack:** where attackers use voicemail-to-email forwarding or default PINs to retrieve MFA codes
- **Number porting:** can redirect the calls to the attacker's own number

AI Disclaimer: None used

Because of these risks and the upcoming deadline, SMS and voice MFA have been deprecated by leading security organisations, including guidance from organisations NIST, NCSC, and Microsoft. Modern authentication methods like phishing resistant synced and device-bound passkeys offer significantly stronger protection.

What experience improvements can this lead to?

Other than strengthening security for the university, we also aim to deliver a better user experience in this modern era of cybersecurity

Passwordless

Perhaps our biggest advantage here is the option to enable a passwordless login once you have a passkey set up. It's easy to enable and means that you no longer need to enter your password at sign-in, rather your passkey alone will satisfy the login.

Reliability

We won't be relying solely on your ISP for the method, meaning network delays and patchy reception won't impact authentication as severely. Also, modern methods such as passkeys and Time-based One Time Password (TOTP) continue to work offline, offering more consistent access.

Convenience

Passkeys mean you no longer need to enter in the 6-digit code, you can also set the UC-provided 1Password browser extension to store your passkey, and if available to you, options such as Windows Hello can make the process even easier.

What You Need to Do

If you are currently using SMS or a voice call for MFA, you are required to transition to a more secure authentication method. You can do this through <https://mysignins.microsoft.com/>. Once signed in, go to *Security Info*, click *+ Add sign-in method*, and choose your preferred option (e.g., Authenticator app, TOTP, or Security key).

We recommend the following options:

- **Passkey in Microsoft Authenticator** (available on iOS and Android)
 - Officially supported by the UC Service Desk
 - Enables passwordless login
 - Requires Android 10 or iOS 16+
 - Allows the use of biometrics (face, fingerprint)
 - Strong phishing resistance
- **Physical passkey** (YubiKey 5 NFC, 5C NFC, and 5C Nano)
 - Strong phishing-resistant authentication
 - Works offline and doesn't require a mobile device
- **Passkey in 1Password**
 - Allows for a seamless login via the browser extension
 - Works across many platforms including web browsers
 - No separate device needed

Questions or Support

We understand that changes to authentication can be disruptive, and we're here to help. If you have any questions or need assistance updating your MFA method, please contact the UC Service Desk on 0508 824 843, or raise an MFA support request via [ServiceNow](#).

FAQ

When do I need to switch from SMS/voice MFA?

By December 2026 however we recommend changing as soon as you can

How do I know which MFA method I'm currently using?

Check your current method via the Microsoft Account Security Info page on <https://mysignins.microsoft.com/security-info>

What kind of devices can I use?

Microsoft Authenticator works on most smartphones and tablets running Android 10 or iOS 16 and above. If you have the option on a Windows computer, Windows Hello can use your computers biometrics capability or a PIN to allow for not only logging into your PC but to apps as well. Those on Apple based devices can use the Apple Passwords / iCloud Keychain to store passkeys and TOTP codes.

Otherwise, if you prefer other authentication apps (like TOTP-based ones), they're widely compatible across platforms including desktops, Linux systems, and even web browsers. This flexibility ensures you can choose a method that suits your device and workflow

Can I use more than one MFA method?

Yes! Having a backup method (e.g., Passkey in Microsoft Authenticator + 1Password) is recommended in case your primary method becomes unavailable

I don't want to use my smartphone for authentication, or I don't have a smartphone

No problem at all! You're welcome to use any passkey or TOTP-based authentication method that works on your preferred device. If you're using a UC-managed laptop, keep in mind that some apps may not be installable due to system restrictions. In that case, we recommend choosing a browser-based or portable authenticator that doesn't require installation

Using something physical that's separate from my UC device would be a better fit for me

We've got you covered! UC supports the use of YubiKeys, which are physical USB or NFC-based passkeys offering strong phishing-resistant authentication.

If you already own a YubiKey, please ensure it's one of the supported models: YubiKey 5 NFC, 5C NFC, or 5C Nano.

I tried to update my default method but it's not allowing me to change to the method I want

If you're having trouble changing your default MFA method, please contact the UC Service Desk or raise an MFA support ticket via [ServiceNow](#). Our team will help resolve the issue and ensure you're set up with the method that works best for you.

How do I set up a Passkey in Microsoft Authenticator?

Step 1. Download and install the Microsoft Authenticator app

Visit the [Apple app store](#) or [Google play store](#) on your device and install the Microsoft Authenticator app. Alternatively, visit aka.ms/authapp and download the Microsoft Authenticator app.

Step 2. Add your account to the app

1. On your desktop, visit <https://aka.ms/mysecurityinfo>
2. Select *Add Method > Passkey in Authenticator app*
3. Follow the wizard experience to setup the app

Scan the QR Code in the app. For more information, see [this guidance](#).

Congratulations! You are now setup with the Microsoft Authenticator app to use your passkey.

How do I set up a Passkey in 1Password?

Step 1. Ensure you have the browser extension installed on your browser of choice

If you don't have it already, you can find the page to download on <https://1password.com/downloads/browser-extension>

Step 2. Follow the instructions provided by 1Password

These instructions can be found on <https://passkeys.directory/details/microsoft/>, they also provide instructions on how to set up passkeys for other websites and services

References

For further reading and official guidance, see the references below:

NZ National Cyber Security Centre - [Multi-factor authentication and verification](#)

NZ Information Security Manual - [ISM Document | New Zealand Information Security Manual](#)

Microsoft – [Recommendation to migrate to Microsoft authenticator - Microsoft Entra ID | Microsoft Learn](#)

U.S. National Institute of Standards and Technology - [NIST Special Publication 800-63B](#)

U.S. Cybersecurity and Infrastructure Security Agency - [Implementing Phishing-Resistant MFA](#)

AI Disclaimer: None used