



Adding Authenticator as Default Factor

Updated Winter 2024

Information Technology Services

helpdesk@clarku.edu

What is multi-factor authentication?

To learn more about MFA, please [click here to view a short video](#).

Why make Microsoft Authenticator my default factor?

All major information security organizations recommend using a modern authentication app (such as Microsoft Authenticator) for MFA, instead of SMS, calls, or secondary emails. Authenticator apps are more secure from SIM cloning, interception and social behavior phishing. Additionally, they allow users more flexibility when travelling away from their primary phone number and when offline.

Therefore, ITS strongly recommends using Microsoft Authenticator.

What do I need?

These instructions are for users who already have MFA set up with SMS, to switch to using Authenticator as your primary MFA factor.

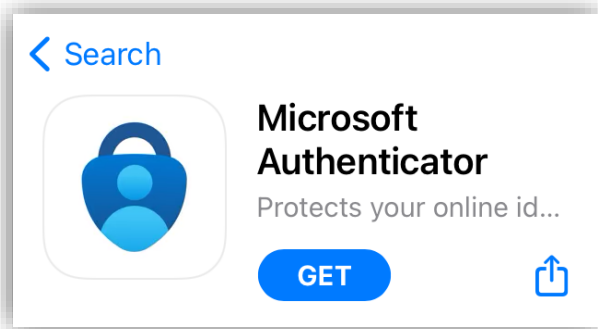
If you are setting up MFA for the first time, please visit this page for better instructions:

To add Microsoft Authenticator as your primary MFA factor, you'll need:

- Your smartphone with access to your SMS
- Internet access

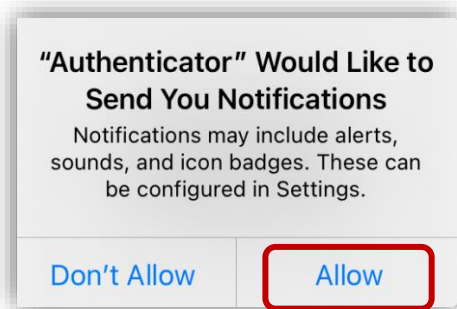
Set-Up Microsoft Authenticator App

1. Download the Microsoft Authenticator app to your smartphone using either the [Play Store](#) (for Android devices) or the [App Store](#) (for iOS devices).



Check that the app you download was published by Microsoft corporation.

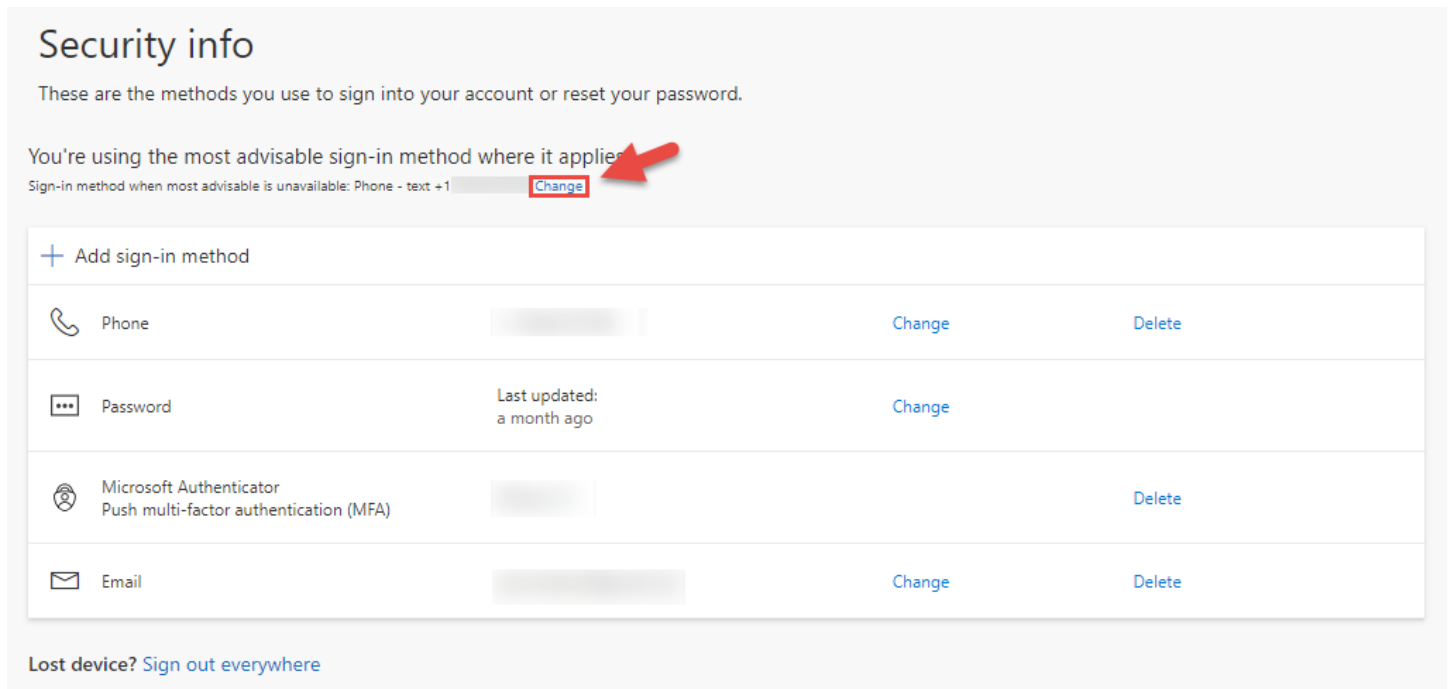
2. Once the Authenticator app is downloaded to your smartphone, tap the app to open it.
3. The app will ask to send you notifications: these notifications will help you authenticate your account moving forward. Tap *Allow*.



4. If necessary, click the Plus icon to add a new account.
5. Tap *Add work or school account*, then tap *Sign in*.
6. Log in using your Clark University email address and password.
7. Follow the prompts to authenticate as usual with SMS
8. The Authenticator App is now set up.

Set Authenticator as your Default Factor

1. Navigate to <https://mysignins.microsoft.com/security-info>
2. Log in with your Clark account information, authenticating with SMS as usual if prompted.
3. Click “Change” for the Sign-in method when most advisable is unavailable.



The screenshot shows the 'Security info' page in a Microsoft account settings interface. At the top, it says 'Security info' and 'These are the methods you use to sign into your account or reset your password.' Below that, it states 'You're using the most advisable sign-in method where it applies' with a red arrow pointing to a 'Change' button next to the 'Phone' method. The 'Phone' method is currently selected as the most advisable. Below this, there is a list of sign-in methods: 'Phone', 'Password', 'Microsoft Authenticator', and 'Email'. Each method has a 'Change' or 'Delete' button. The 'Password' method is noted as 'Last updated: a month ago'. At the bottom, there is a link for 'Lost device? Sign out everywhere'.

Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies

Sign-in method when most advisable is unavailable: Phone - text +1 [Change]

+ Add sign-in method

Phone	[Redacted]	Change	Delete
Password	Last updated: a month ago	Change	
Microsoft Authenticator Push multi-factor authentication (MFA)	[Redacted]		Delete
Email	[Redacted]	Change	Delete

Lost device? [Sign out everywhere](#)

4. Choose App based authentication – notification
5. Click Confirm