

Multi-factor authentication (MFA) Setup in Office 365

FAQ

- What is Multi-factor authentication (MFA)?
 - MFA is a secure way to make sure that only you can access your account by asking you to provide a secondary form of authentication along with your password. This secondary factory could be a code sent in a text message, a smart phone app, or even a phone call.
- Will I have to use MFA every time I log in?
 - No, you will only need to use MFA when you are logging in from outside our network.

Setup

- Go to <http://aka.ms/mfasetup>
- **The more options you configure the better** but we at the very least the Authenticator App should be downloaded and configured for push notifications.

The screenshot shows the Microsoft MFA setup interface. At the top, it asks "what's your preferred option?" and states "We'll use this verification option by default." Below this is a dropdown menu set to "Notify me through app". The next section asks "how would you like to respond?" and says "Set up one or more of these options. Learn more". There are three options for phone verification: "Authentication phone" (checked), "Office phone (do not use a Lync phone)" (unchecked), and "Alternate authentication phone" (unchecked). Each phone option has a country/region dropdown and a phone number input field. The "Authentication phone" option is currently selected. Below the phone options, there is a checked option for "Authenticator app or Token" with a "Set up Authenticator app" button. Underneath, there is a list of installed authenticator apps, showing "Authenticator app - SM-G960U" with a "Delete" button. At the bottom, there is a section for "restore multi-factor authentication on previously trusted devices" with a "Restore" button.

- From now on when you log into your email account from outside our network your Authenticator App will ask you if you accept the login activity. A simple press of a button and you are now logged in.