MFA User guide

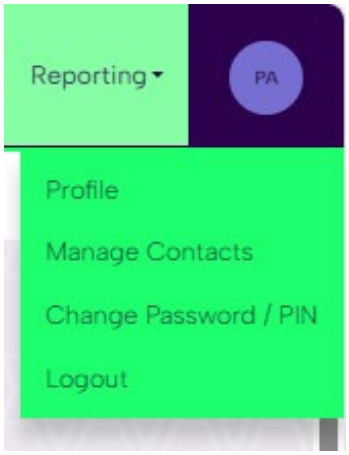
The ARO BOLT portal now has Multi Factor Authentication (MFA) enabled. MFA provides an extra-layer of protection to the sign-in process by asking the individual signing in to provide a security code obtained from an Authenticator mobile application or via their registered email address.

Portal Administrators for each Company Account can opt whether to enable or disable MFA for all contacts in their organisation that have access to the BOLT portal

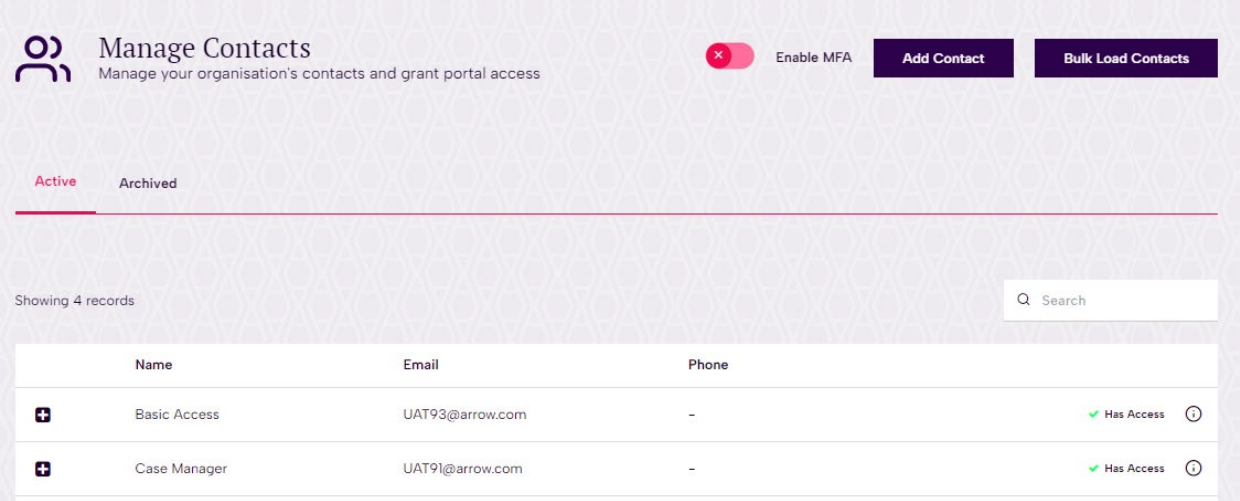
Please note. MFA is a Company-wide settings. It is not possible to only enforce MFA on some users and not others.

Enabling / Disabling MFA as a Portal Admin

On the BOLT home page, click your Avatar in the top right hand corner and select **Manage Contacts**

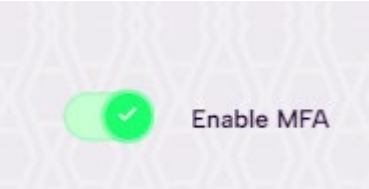


Near the top of the Manage Contacts page you will see the Enable MFA toggle switch. By default MFA is disabled until a Portal Admin for the Account enables this.



To enable MFA click the toggle.

When the icon is a green circle containing a white tick, MFA has been successfully applied to all Contact accounts.



Alternatively click the toggle again, to disable MFA. When the icon is red with a white cross, MFA has been disabled



Registering for MFA

When logging into the Portal again, once MFA has been enabled, the user will be prompted to complete the MFA setup. Each individual needs to complete this process in order to access BOLT, if MFA has been enabled.

Please note – if a Portal Admin disables MFA, then re-enables at a later time, users will be required to repeat this registration process.



As prompted on screen the first step is download a mobile application (to the users smartphone) that supports Time-based One-Time Password.

NB: Technically, the smart-phone used does not need to be one provided to the user by your organisation. If the user opts to, and if in line with your Mobile Device Usage/Access

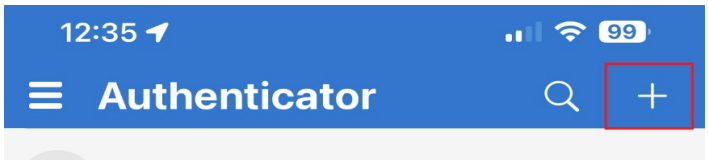
Management policy, personal devices can be used.
For the purpose of this user guide, ARO are demonstrating use of the Microsoft Authenticator mobile application.



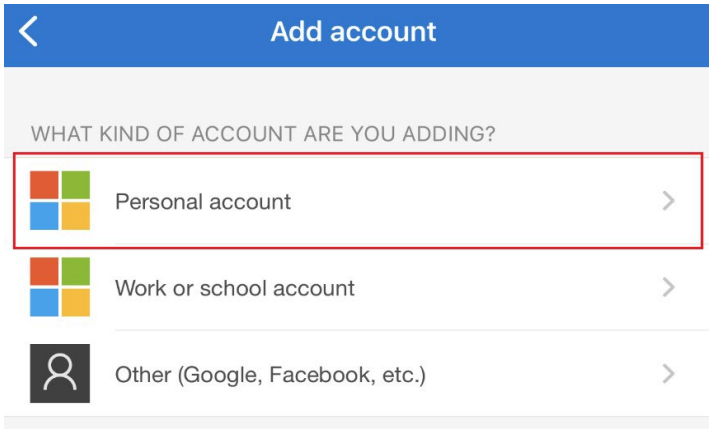
This can be downloaded from the Google play store or Apple App store (depending on the Mobile operating system).

Instructions vary for different Authenticator applications.

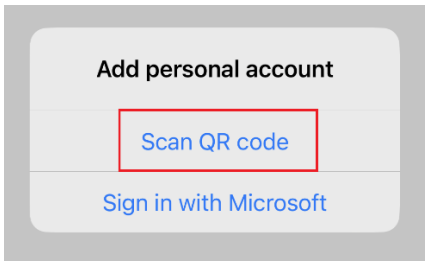
Once downloaded, open Microsoft Authenticator app and press the + in the top right hand corner



On the following screen, select Personal account



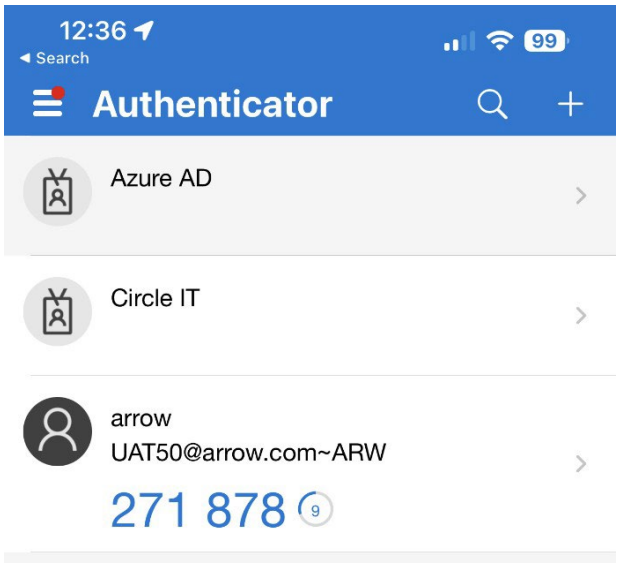
On the pop-up box that appears, press Scan QR Code.



The user device's camera will be enabled. The user should then scan the QR code on the MFA setup screen. If this process has completed successfully the user will be returned to the home page of the Authenticator application.

The user will see their BOLT account added to the home page, with a 6-digit code that

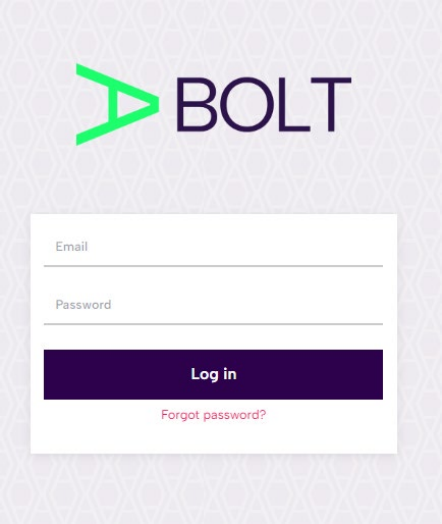
refreshes every 30 seconds



Once the user has reached this stage, their MFA setup is complete

Logging on with MFA enabled

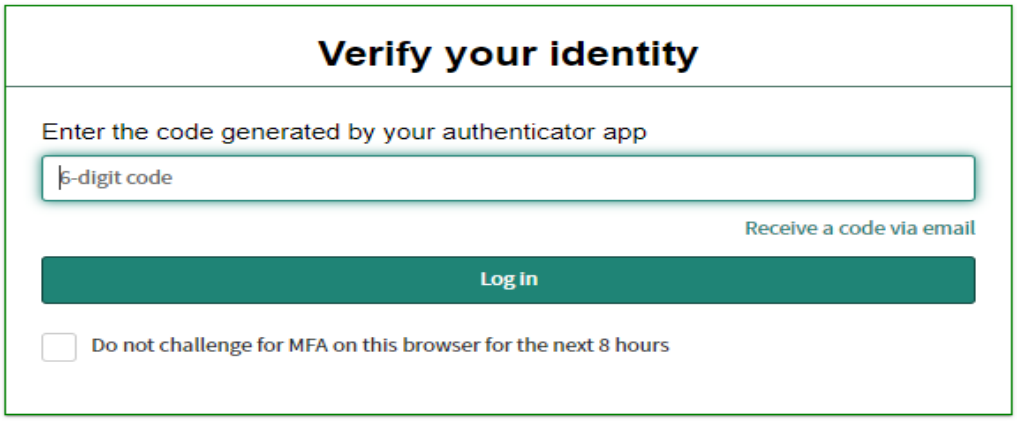
From the BOLT login screen (https://BOLT.aro.tech)
Enter your user credentials



Click Log in
If the credentials are correct the user will be prompted with the Verify your identity screen.

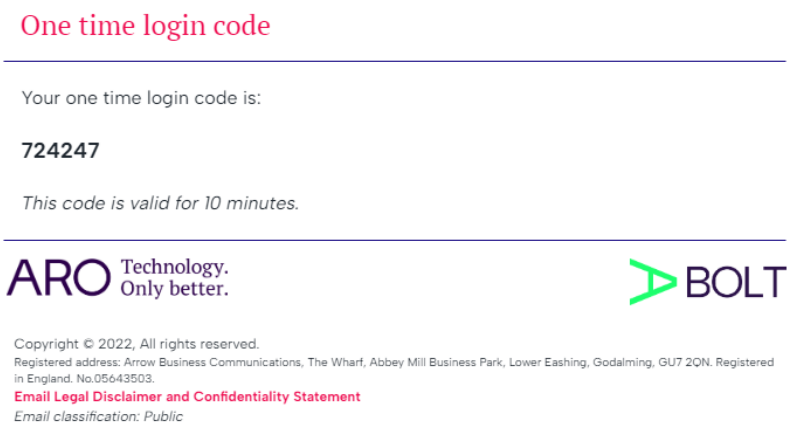
The user should access the Authenticator application they have chosen and enter the 6 digit code presented within the application.

Click log-in. If the code is correct, the BOLT home page will be presented.



Alternatively, the user can click Receive a code via email to receive a 6 digit code to the email associated to their BOLT account.

The email is sent from popx@service-now.com and appears as:



If the user enters the code into the Verify your identity page, within 10 minutes, they will be presented with the BOLT home page

Resetting MFA

If a customer needs to reset their MFA, this can be done by Portal Admins via 'Manage Contacts'.



For more information or assistance, please contact the ARO Customer Service team via BOLT or call on 0330 440 4444