



# Multi-Factor Authentication (MFA) mini-guide

[www.qunote.com](http://www.qunote.com)



# Strengthening Your Security with Multi-Factor Authentication



# ENABLING MFA

To enable MFA, please follow these steps:

1. Users must have access to the **registered email address** associated with their Qunote account.
2. Navigate to **Admin section > Users > User settings**.
3. By default, MFA is disabled at account level.
4. To enable MFA at account level, select **Enable Account Multi-Factor Authentication (MFA) > Yes**.

5. Users with **edit user permissions** can disable MFA on a user level by selecting **Allow MFA to be disabled for individual users > Yes**.

**Note:** it is recommended to keep this setting off, unless MFA needs to be temporarily disabled for a specific user.

Admin / User settings

## User settings

Include inactive users in Team Management  Yes  No

Include inactive users in filters  Yes  No

Include inactive users in reports  Yes  No

Enable account Multi-Factor Authentication (MFA)  Yes  No

Allow MFA to be disabled for individual users  Yes  No

MFA timeout interval  hours

Admin / User settings

## User settings

Include inactive users in Team Management  Yes  No

Include inactive users in filters  Yes  No

Include inactive users in reports  Yes  No

Enable account Multi-Factor Authentication (MFA)  Yes  No

Allow MFA to be disabled for individual users  Yes  No

MFA timeout interval  hours

6. To action go to **Users > Edit user > Login credentials accordion > MFA enabled > No**.

The screenshot shows the 'Login credentials' form. It includes fields for 'Username' and 'Password', and a 'Confirm Password' field. There are radio buttons for 'Active' (Yes/No) and 'MFA Enabled' (Yes/No). The 'MFA Enabled' 'Yes' radio button is selected. A 'Team management' button is at the bottom.

7. In **Admin > User settings**, you can configure the MFA timeout interval, ranging from 1 to 12 hours.

The screenshot shows the 'User settings' page. It has a breadcrumb 'Admin / User settings'. The page lists several settings with radio buttons: 'Include inactive users in Team Management' (Yes selected), 'Include inactive users in filters' (Yes selected), 'Include inactive users in reports' (Yes selected), 'Enable account Multi-Factor Authentication (MFA)' (Yes selected), and 'Allow MFA to be disabled for individual users' (No selected). The 'MFA timeout interval' is set to '10 hours' and is highlighted with a blue box.

**Note:** MFA does not take effect immediately and will be enabled the next time you log into the account.

## MFA LOGIN PROCESS

Once MFA is enabled, follow these steps to access your account:

1. Enter your **Qunote login credentials** as usual.
2. You will be prompted to enter a **verification code**.
3. The code will be sent to your **registered email** and is **valid for 5 minutes**.
4. Enter the code in the MFA field and click **Continue**.
5. If you do not receive the email, click **Resend Code**.

## MFA TIMEOUT INTERVAL

After logging in, MFA will be required again based on inactivity:

- By default, **MFA prompts after 6 hours of inactivity**.
- Administrators can adjust the **MFA timeout interval** between **1 to 12 hours**.

## MFA ACCOUNT RECOVERY

In the event you lose access to your registered email, take steps to regain access. If this is not possible, contact Qunote Support for assistance.



[www.qunote.com](http://www.qunote.com)

 [youtube.com/@qunote3](https://youtube.com/@qunote3)

 [x.com/qunotetweets](https://x.com/qunotetweets)

 [linkedin.com/company/qunote](https://linkedin.com/company/qunote)

© 2025 Qunote, Cage Farm Studio, Stowting, Kent, TN25 6BE

25030QUNO // Qunote MFA mini-guide



Cert No. 16451  
ISO 27001