PeopleTray

User Guide | Multi-Factor Authentication (MFA)

Contents

What is MFA?

Multi-Factor Authentication (MFA) adds an extra layer of security when users sign in to PeopleTray. It requires a verification code from a trusted mobile device in addition to the user's usual login credentials.

Overview of MFA for PeopleTray

- MFA is available for Web only (Mobile app support is coming soon).
- Uses Time-Based One-Time Passcodes (TOTP).
- Requires a third-party Authenticator App (e.g. Google Authenticator or Microsoft Authenticator).
- MFA can be enabled or disabled per user by your PeopleTray Administrator.

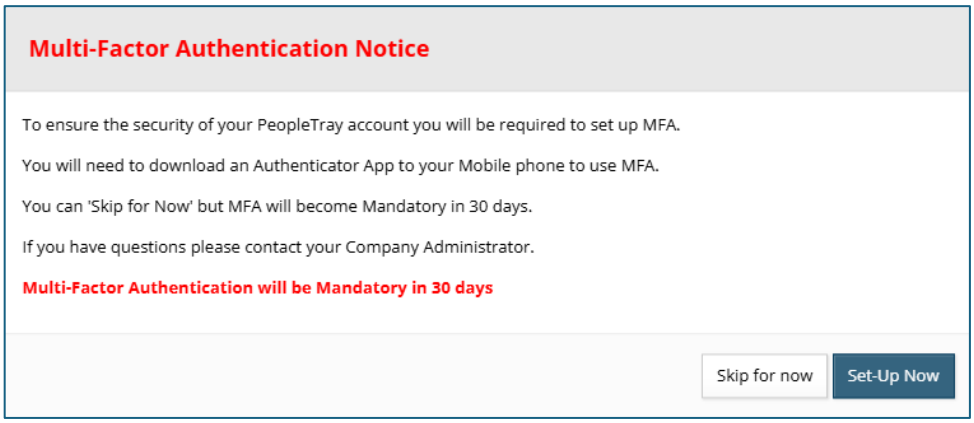
Implementing MFA in Your Organisation

1. Coordinate with PeopleTray Support to enable MFA for your account.
2. Plan your internal rollout – users will need guidance and access to an Authenticator App.
3. PeopleTray can provide a Generic Implementation Plan if needed.

First Time Sign-In once MFA is Enabled

1. Enter your existing PeopleTray credentials and click **Sign me in**.

2. A prompt appears on the homepage: *Multi-Factor Authentication Notice. Set up now or skip for 30 days*.



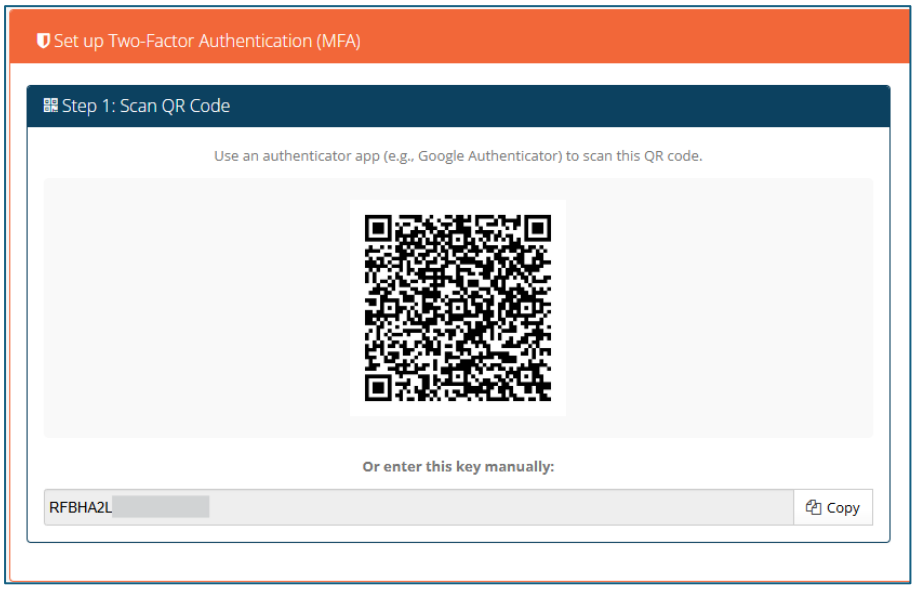
3. Click **Set Up Now** to begin or **Skip for Now** to proceed without setting up (skip option only available for 30 days).

4. A countdown warning will display the number of days remaining before MFA setup becomes mandatory.

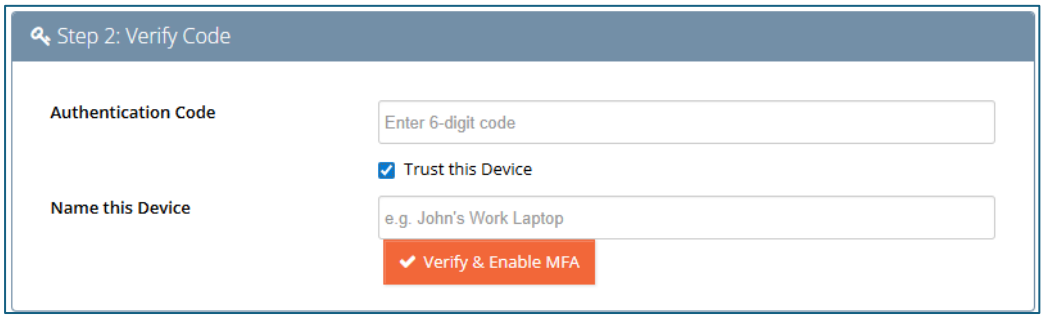
Setting Up MFA

After clicking 'Set-Up Now' you will be taken to the setup page.

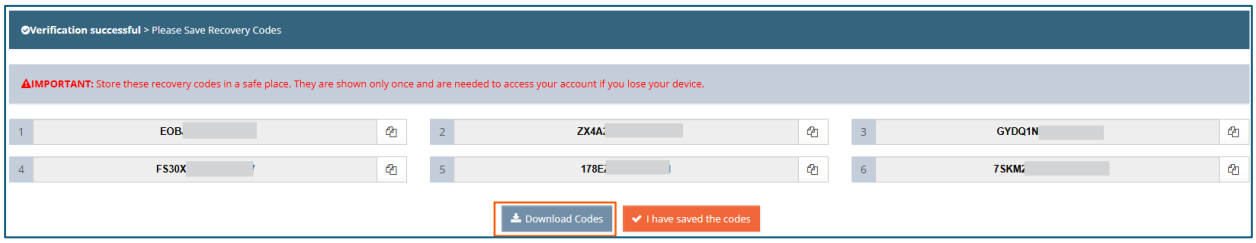
1. Open your Authenticator App on your mobile device and **scan the QR code** displayed on your PeopleTray screen. If needed, enter the setup key manually.



5. Enter the **6-digit code** from the Authenticator App on your mobile device.
6. Optional: Check **Trust this device** and name it. Trusted devices reduce the need to re-enter verification codes for 30 days.
7. Click **Verify & Enable MFA**.

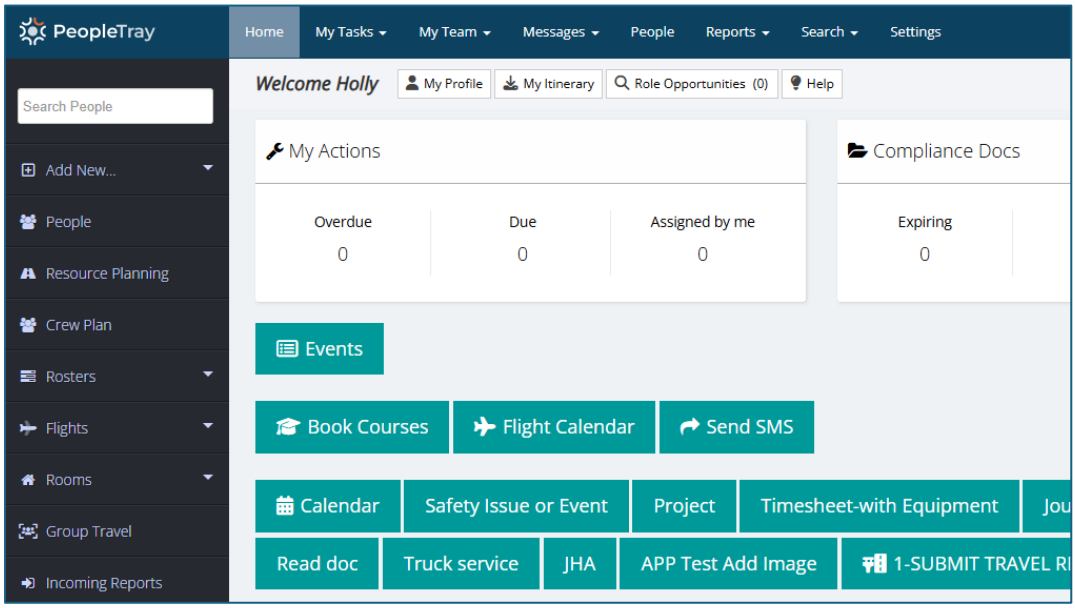


8. Six one-time recovery codes are displayed. These codes allow access if your device is lost. **Save them immediately**:
    - Download
    - Copy/paste into a secure file
    - Print and store safely



9. Click **I have saved the codes** to complete setup.

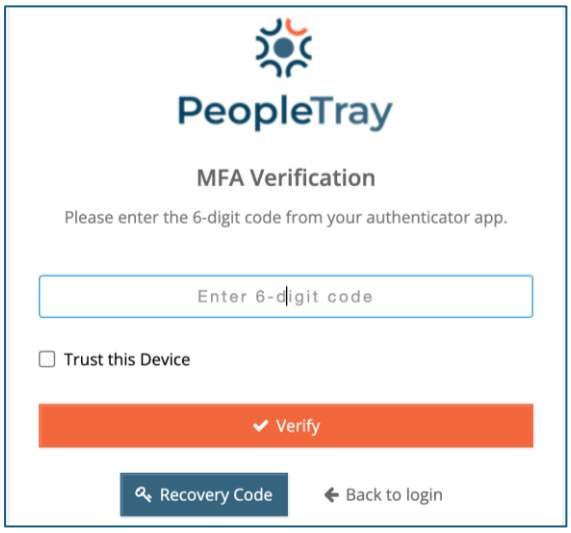
10. You will now be logged in to PeopleTray.



Logging In After MFA Is Set Up

1. Enter your usual PeopleTray login credentials and click **Sign me in**.

2. The MFA Verification Screen will display. Enter the **current 6-digit code** from the Authenticator app on your mobile device.
3. If not already done, you can choose to **trust this device** to simplify future logins.
4. Click **Verify**.



If You Lose Access to Your MFA Device

1. Enter your usual PeopleTray login credentials and click **Sign me in**.

2. The MFA Verification Screen will display. Click **Recovery Code**.

3. Enter one of your **saved recovery codes** and then click **Verify Recovery Code** to log in.

If You Lose Your Recovery Codes

If you have lost both your device and recovery codes, you can request your Administrator to reset your MFA. PeopleTray Support cannot reset MFA for individual users.

Administrator Tools:

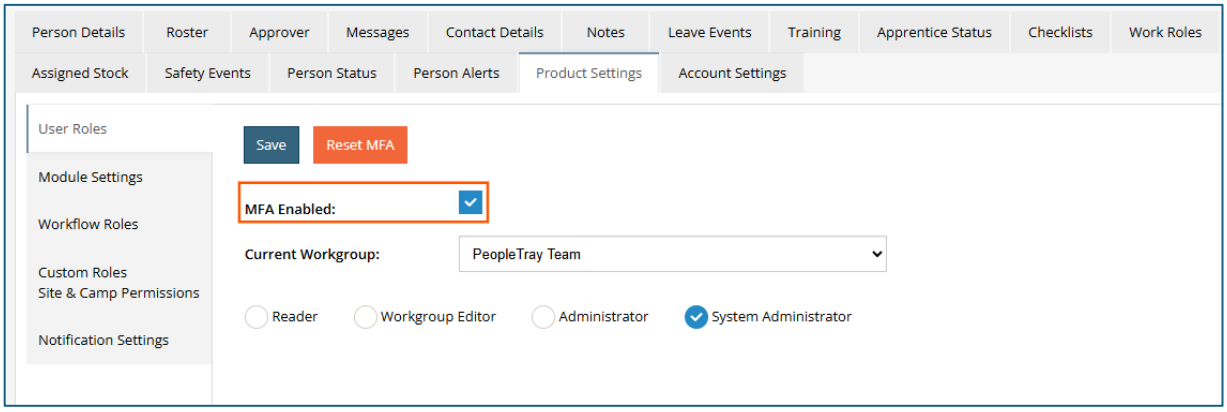
Disable MFA for a User

It may be decided by your Organisation that some users will not be required to use MFA. This can only be actioned by your Organisation's PeopleTray Administrator.

Note: PeopleTray Support does not have the authority to enable or disable MFA.

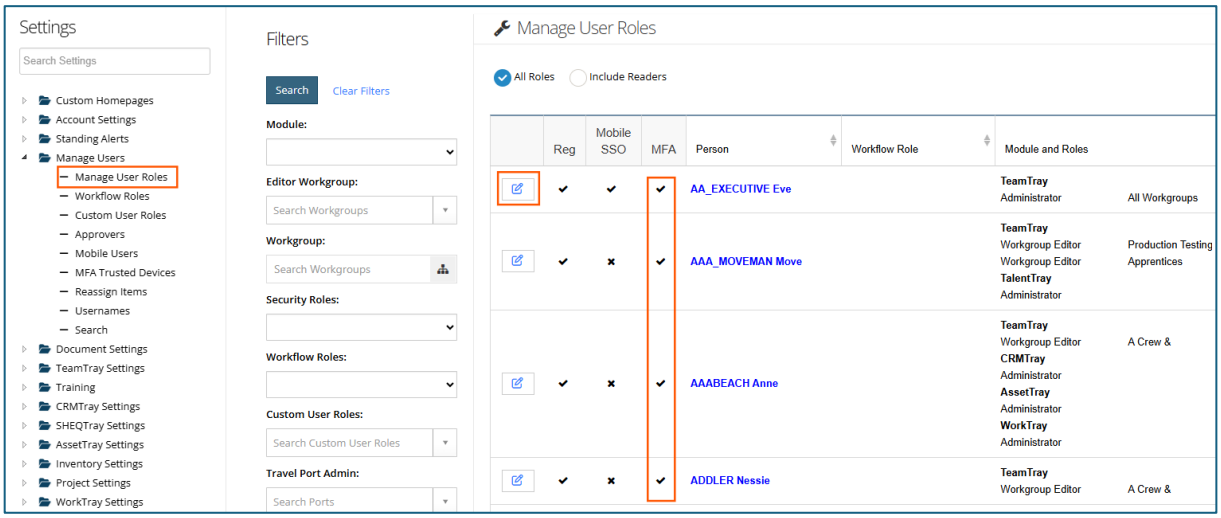
1. **Disable for Single User:**

   Navigate to the User's Profile > Product Settings tab > User Roles tab > Uncheck 'MFA Enabled'



2. **Disable for Multiple Users:**

   Navigate to: Settings > Manage Users > Manage User Roles > Edit > Uncheck 'MFA Enabled'



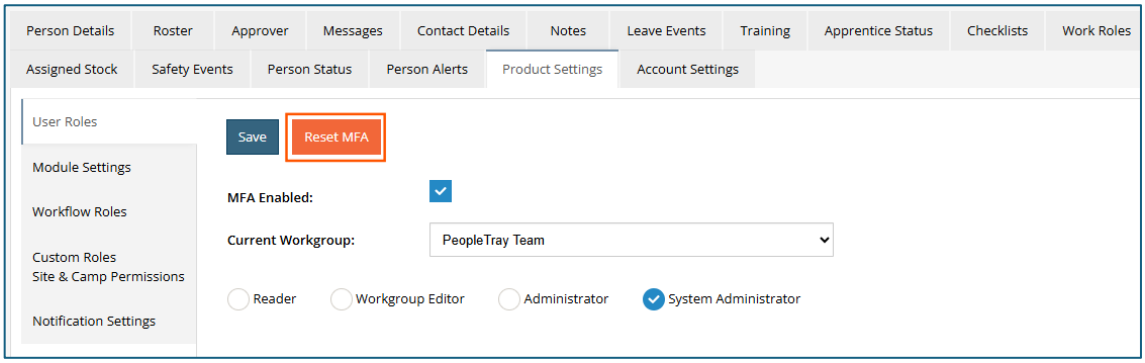
Reset MFA for a User

If a user loses their device and recovery codes, the PeopleTray Administrator for your Organisation can reset the MFA status on the user's profile. This will prompt the user to go through the MFA setup process again.

Note: PeopleTray Support does not have the authority to reset MFA for a user.

1. **Reset MFA for a User:**

   Navigate to the User's Profile > Product Settings tab > User Roles tab > Choose 'Reset MFA'



Manage Trusted Devices

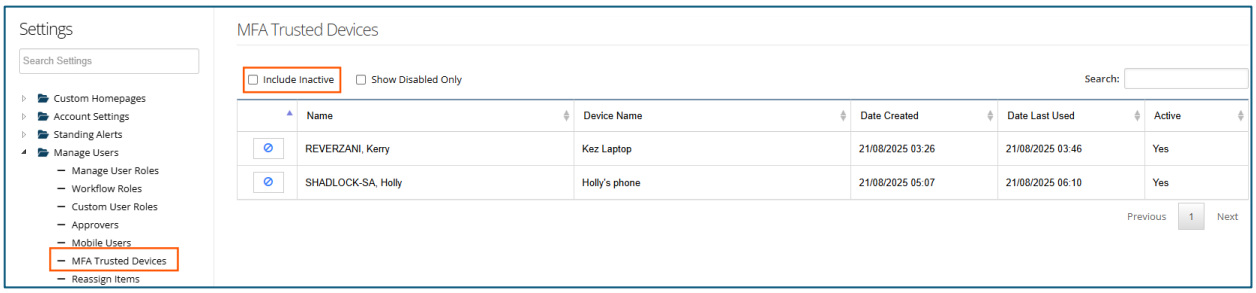
Trusted devices are those registered by a user during their MFA setup. Once a device is marked as trusted, the user will only need to enter a new verification code from their Authenticator App every 30 days.

Note: It is important to disable a trusted device if it is lost or stolen.

1. **View Trusted Devices:**

   Navigate to Settings > Manage Users > MFA Trusted Devices

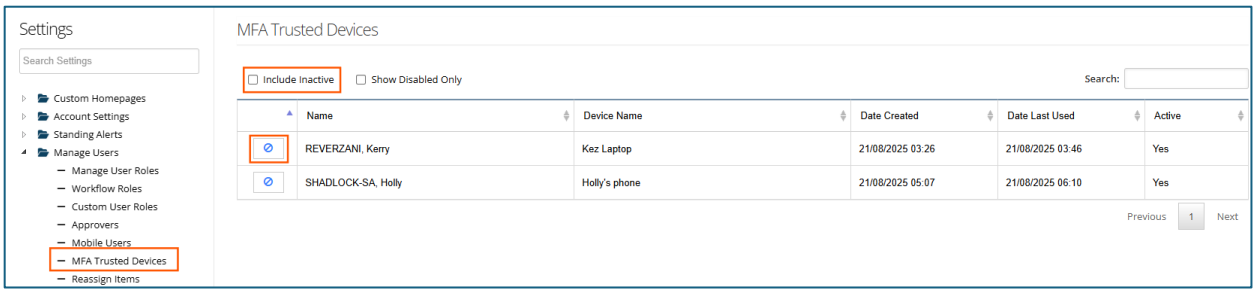
   Optional: Tick 'Include Inactive' to display inactive Profiles with a trusted device



2. **Disable Trusted Devices:**

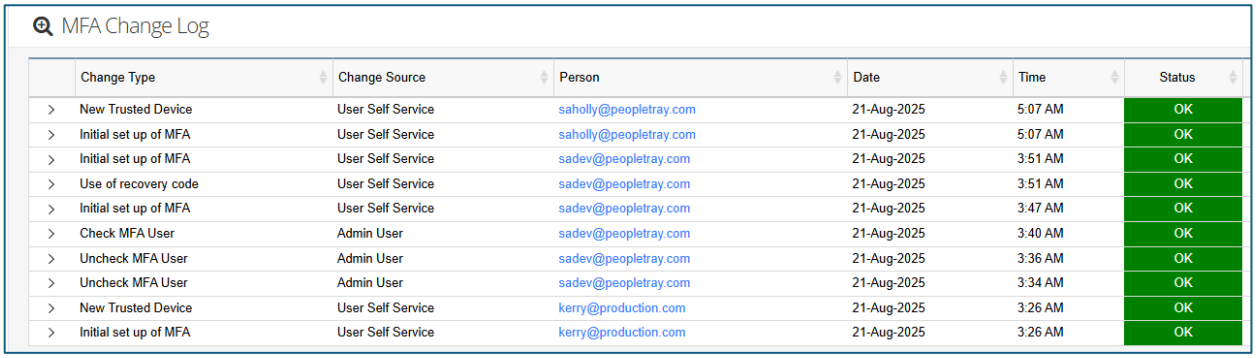
   Navigate to Settings > Manage Users > MFA Trusted Devices

   Use the Search bar to search for a device, and then click 'Disable' next to the required device if it is lost or stolen



MFA Change Logs

Track MFA-related changes via TeamTray > Change Logs > MFA Change Log:



Change Type	Change Source	Person	Date	Time	Status
New Trusted Device	User Self Service	saholly@peopletray.com	21-Aug-2025	5:07 AM	OK
Initial set up of MFA	User Self Service	saholly@peopletray.com	21-Aug-2025	5:07 AM	OK
Initial set up of MFA	User Self Service	sadev@peopletray.com	21-Aug-2025	3:51 AM	OK
Use of recovery code	User Self Service	sadev@peopletray.com	21-Aug-2025	3:51 AM	OK
Initial set up of MFA	User Self Service	sadev@peopletray.com	21-Aug-2025	3:47 AM	OK
Check MFA User	Admin User	sadev@peopletray.com	21-Aug-2025	3:40 AM	OK
Uncheck MFA User	Admin User	sadev@peopletray.com	21-Aug-2025	3:36 AM	OK
Uncheck MFA User	Admin User	sadev@peopletray.com	21-Aug-2025	3:34 AM	OK
New Trusted Device	User Self Service	kerry@production.com	21-Aug-2025	3:26 AM	OK
Initial set up of MFA	User Self Service	kerry@production.com	21-Aug-2025	3:26 AM	OK