Setting Up Multi-Factor Authentication in OverShield®

A Guide for Users and Administrators

Rev. 1.0.0

OVERSHIELD®

by Predictive Monitor

Contents

About this Guide

This document guides OverShield users and administrators through setting up Multi-Factor Authentication (MFA) in OverShield versions 3.5 and later. Before any individual user can set up MFA, it must first be implemented at the company level by the OverShield administrator. For more information about this, refer to the *Administrative Settings* Section at the end of this guide.

Variations

This guide assumes MFA has been deployed as a mandatory requirement with all available options enabled. Some of the procedures and images in this guide may differ from your experience due to variations in the administrative settings. Also, some of the windows and dialog boxes shown in this guide may vary slightly from what you see on-screen.

Getting Started

When MFA is enabled company-wide, each user will be required to set up at least one authentication method the next time they log in to OverShield. The following MFA methods are available:

- Email authentication (via work email)
- SMS authentication (via text)
- Time-based One-Time Password (TOTP) authentication via a 3rd-party authentication app

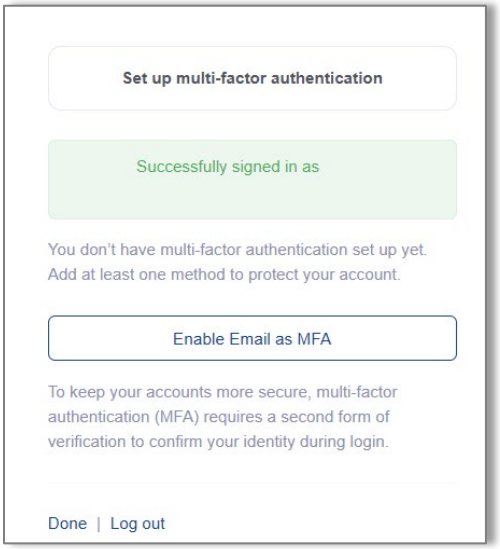
IMPORTANT:

- The email address and/or telephone number used for authentication must match the information in the user's OverShield user profile. If you need to change this information, contact your OverShield administrator.
- If you have any problems during setup, please contact your OverShield Administrator.

Setting Up Authentication Methods

Enabling Email Authentication (Required)

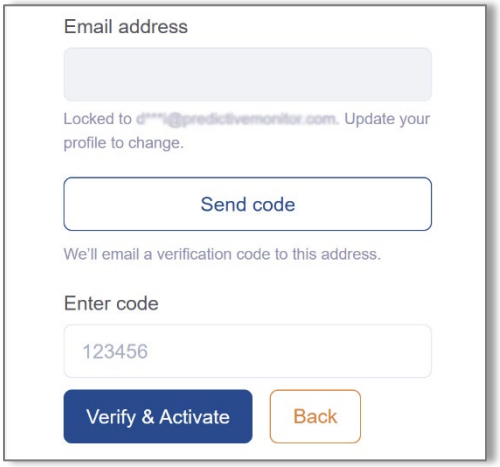
You are required to set up Email as the first authentication method. After that, additional methods can be configured, including text/SMS and your preferred authentication app.



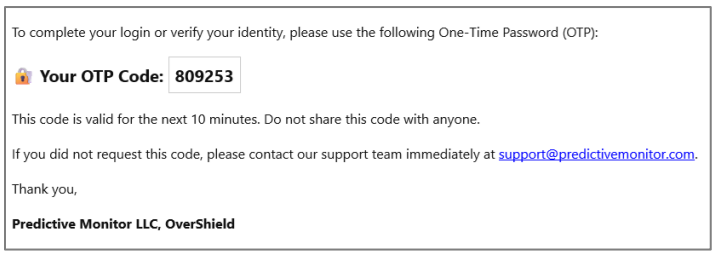
1. Log in to OverShield using your credentials. The **Set up multi-factor authentication** box opens.
2. Click on **Enable Email as MFA.**

   The **Set up Email** box opens.

   If the program has locked in your login email (Look under the Email address field), you can skip step 3 and go to step 4.



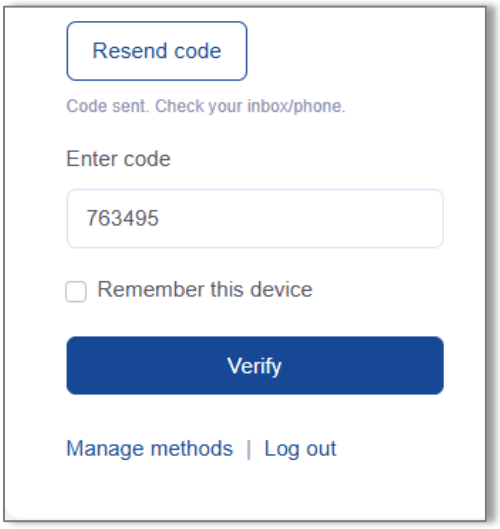
3. Enter the email address used to log in to OverShield.
4. Click the **Send code** button and check your email for the One-Time Password (OTP) code.



   The authentication code is valid for 10 minutes.

   If you do not receive this email within 1-2 minutes:

   - Check your Junk Email folder.
   - Click the **Resend code** button.

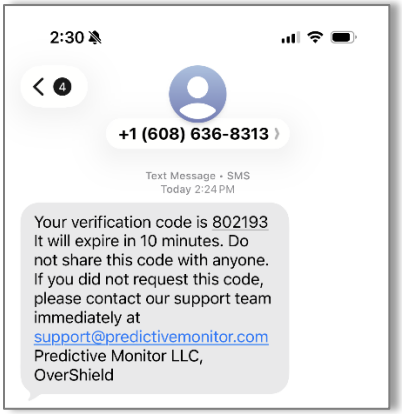


5. Enter the OTP code in the **Enter code** field and click the **Verify & Activate** button.
   - Do not share this code with anyone.

   If authentication is successful, the OverShield application opens.

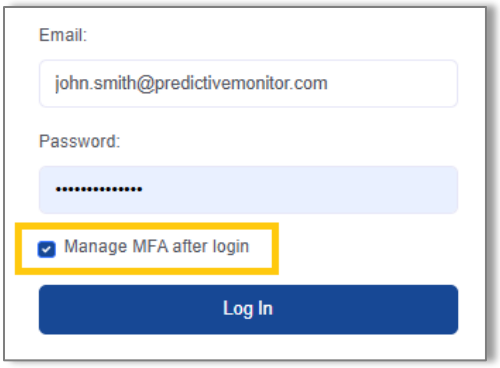
Enabling SMS (Text) Authentication

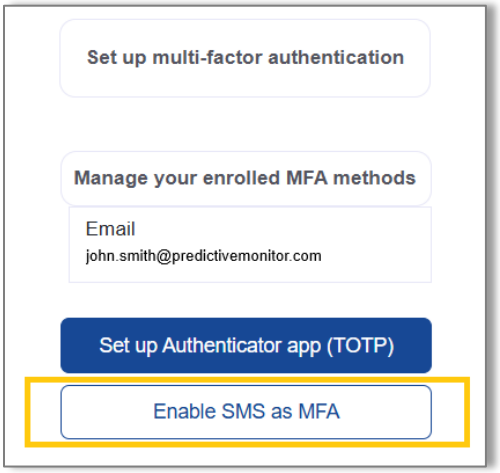
1. If you are currently logged into OverShield, sign out.
2. Check the **Manage MFA after login** box and click the **Log In** button.
3. Authenticate as usual.
   After successful authentication, the **Set up multi-factor authentication** box appears.
4. Click the **Enable SMS as MFA** button.
5. The **Set up SMS** box opens, prefilled with the phone number from your OverShield User Profile.
6. Confirm that the phone number is correct and click the **Send code** button.
7. Check your cell phone for a text message containing your OTP token and enter that number in the **Enter code** field.

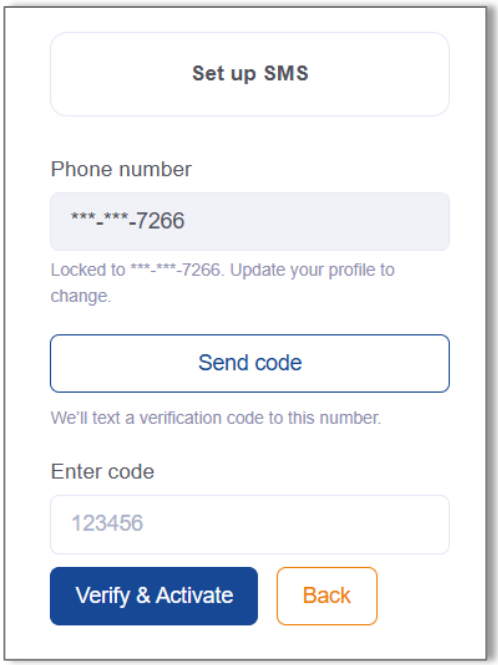


8. After successful authentication, OverShield opens as usual.

The next time you log in to OverShield, **Text message** will be available as a verification method.



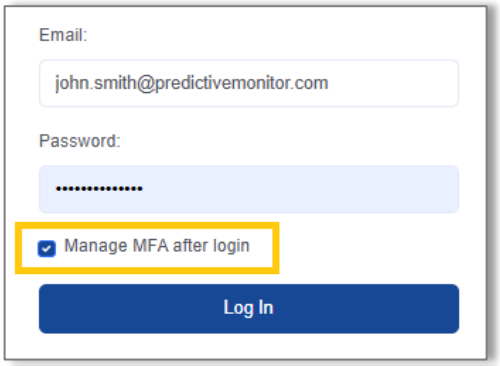


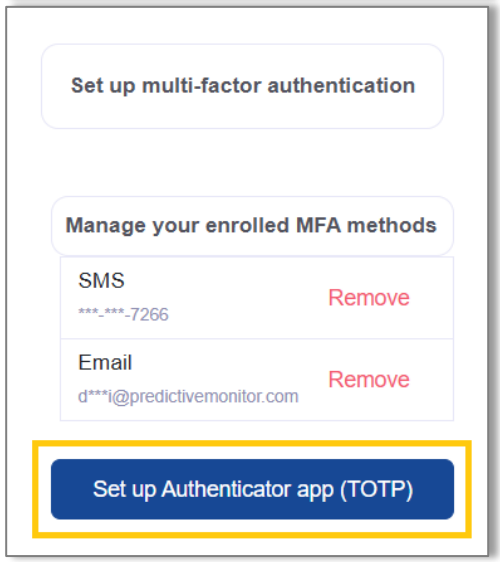


Enabling a Time-based One-Time Password (TOTP)

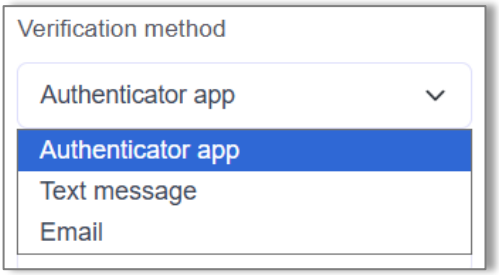
This method allows you to use your favorite authentication app to verify your identity.

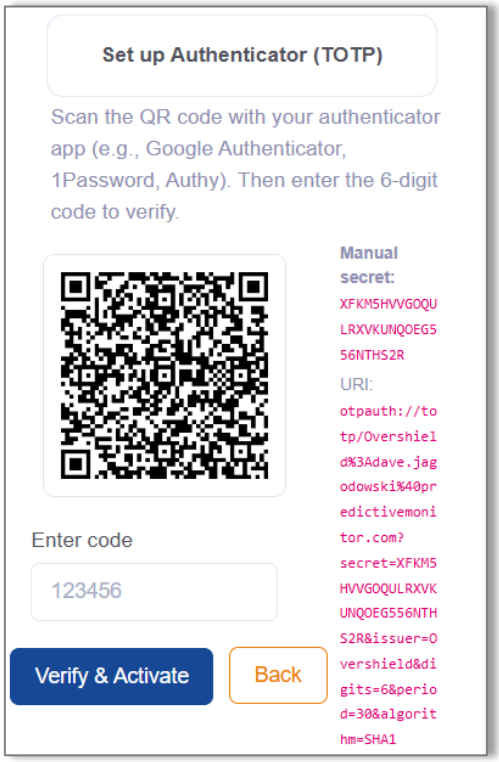
1. If you are currently logged into OverShield, sign out.
2. Check the **Manage MFA after login** box and click the **Log In** button.
3. Authenticate as usual. The **Set up multi-factor authentication** box appears.
4. Click the **Set up Authenticator app (TOTP)** button.
5. The **Set up Authenticator** box opens, prefilled with the information from your User Profile.
6. On your phone/device, open your preferred authenticator app and scan the QR code. (Google Authenticator, Microsoft Authenticator, Authy, etc.)
7. Enter the code generated by the app into the **Enter code** box and click the **Verify & Activate** button.
8. After successful authentication, OverShield opens as usual.





The next time you log in to OverShield, **Authenticator App** will be available as a verification method.

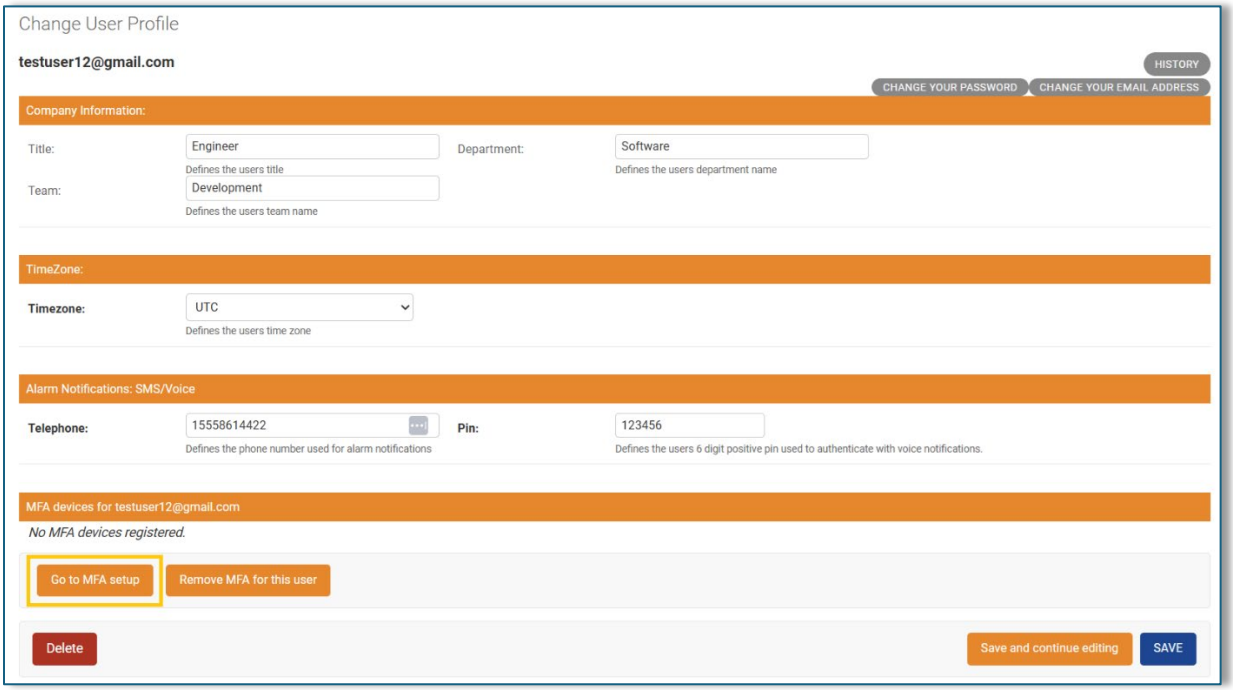




Accessing MFA Settings Within OverShield

Use this procedure to access the MFA Setup page without having to log out of OverShield.

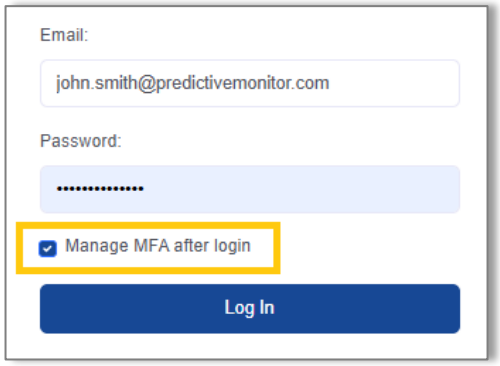
1. From the main OverShield screen, select **Logs > System > User Profiles** from the sidebar.
2. Select your name from the list.
   The Change User Profile window opens.



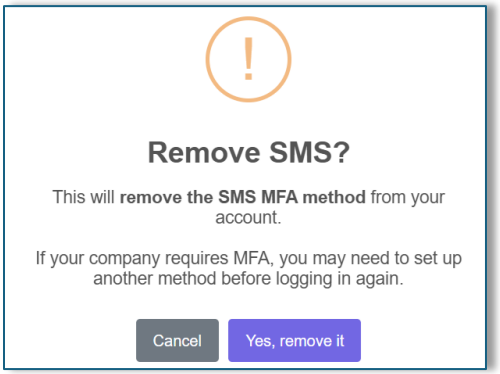
3. Scroll down to the MFA devices for [user] section.
4. Take the desired action to edit your MFA options.
   - To add or remove an MFA method, click the **Go to MFA setup** button.
   - To remove all of your MFA methods simultaneously, click on the **Remove MFA for this user** button and confirm the decision.

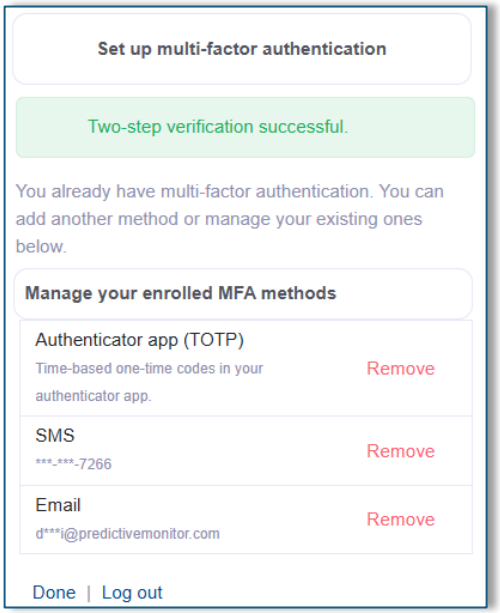
Removing an Authentication Method

Use this procedure to remove one or more authentication options. You must maintain at least one type of authentication.



1. If you are currently logged into OverShield, sign out.
2. Check the **Manage MFA after login** box and click the **Log In** button.
3. Authenticate as usual. The **Set up multi-factor authentication** box appears.
4. Select which authentication method you want to remove and click on the word **Remove**.
5. You are prompted to confirm your decision to remove this MFA method.





6. Click on **Yes, remove it** to proceed with the operation, or click **Cancel** to end this process.

   Note: Be aware that your ability to add or remove certain MFA methods could be overridden by company-wide administrative settings.

7. Click **Done** at the bottom of the box to continue to OverShield, or if you are finished, click **Log out**.

Note: Administrators can remove all authentication methods from any individual account.

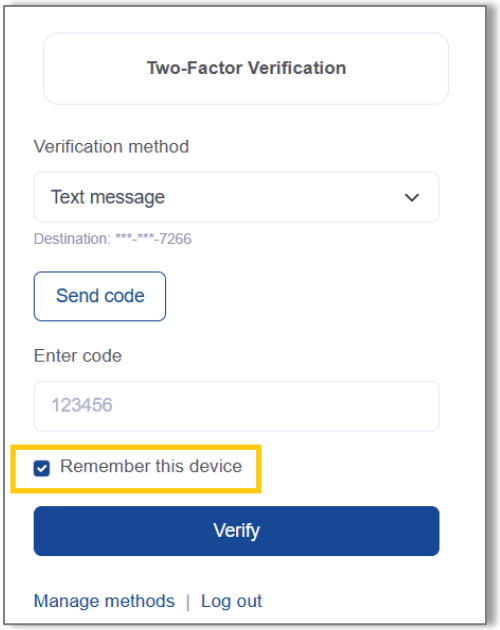
Bypassing Authentication

If you do not want to authenticate on your current device every time you log in to OverShield, you can disable authentication for a period of 1– 4 weeks as predetermined by the administrative MFA Policy settings.

To bypass authentication:

1. If you are currently logged into OverShield, sign out.
2. Click the **Log In** button.
3. Authenticate as usual, checking the **Remember this device** box.
4. Click the Verify button to complete authentication.

   The next time you log in to OverShield, you will not be required to authenticate.

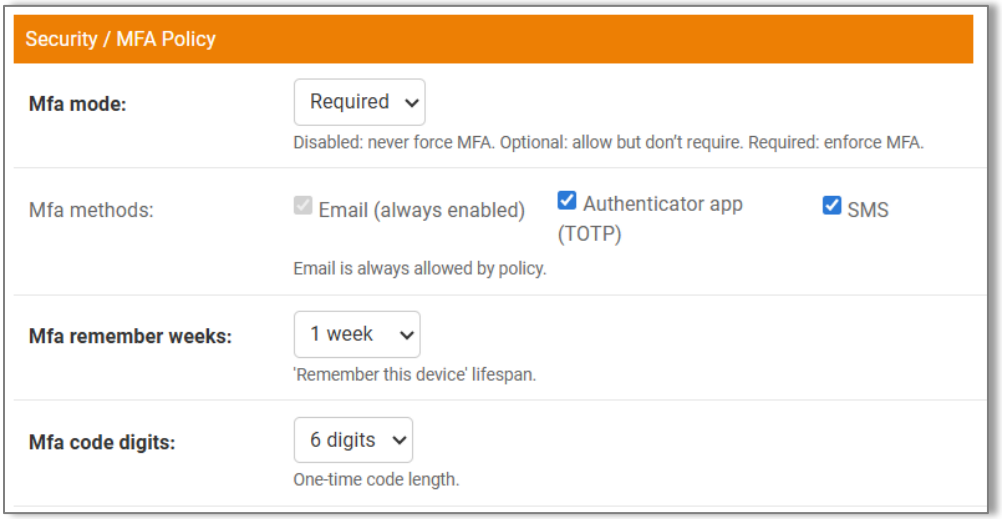


Administrative Settings

Setting Authentication Policy for a Company

Only OverShield administrators can set the company-wide MFA, which applies to all users.

1. Navigate to the **Change Company Definition** page (**Logs > All**) and select **Companies** from the sidebar.
2. In the Company Definition List, click on the company name you want to edit.
3. In the Change Company Definition window, scroll down to the **Security / MFA Policy** section and make the desired selections.



MFA mode

Disabled	No multi-factor authentication will be in place.
Optional	MFA is enforced only if it has been set up for the user; otherwise, it is bypassed.
Required	MFA is mandatory for all users

MFA methods

Email	Enables authentication via Email. This option cannot be disabled.
Authenticator app (TOTP)	Allow the user to authenticate using a 3rd-party authentication app such as Microsoft Authenticator, Google Authenticator, or Authy.
SMS	Allow the user to authenticate via text message. (SMS = Short Message Service)

MFA remember weeks

This specifies how long OverShield will remember a device when the user checks the **Remember this device** checkbox during login. Choose **one**, **two**, **three**, or **four** weeks.

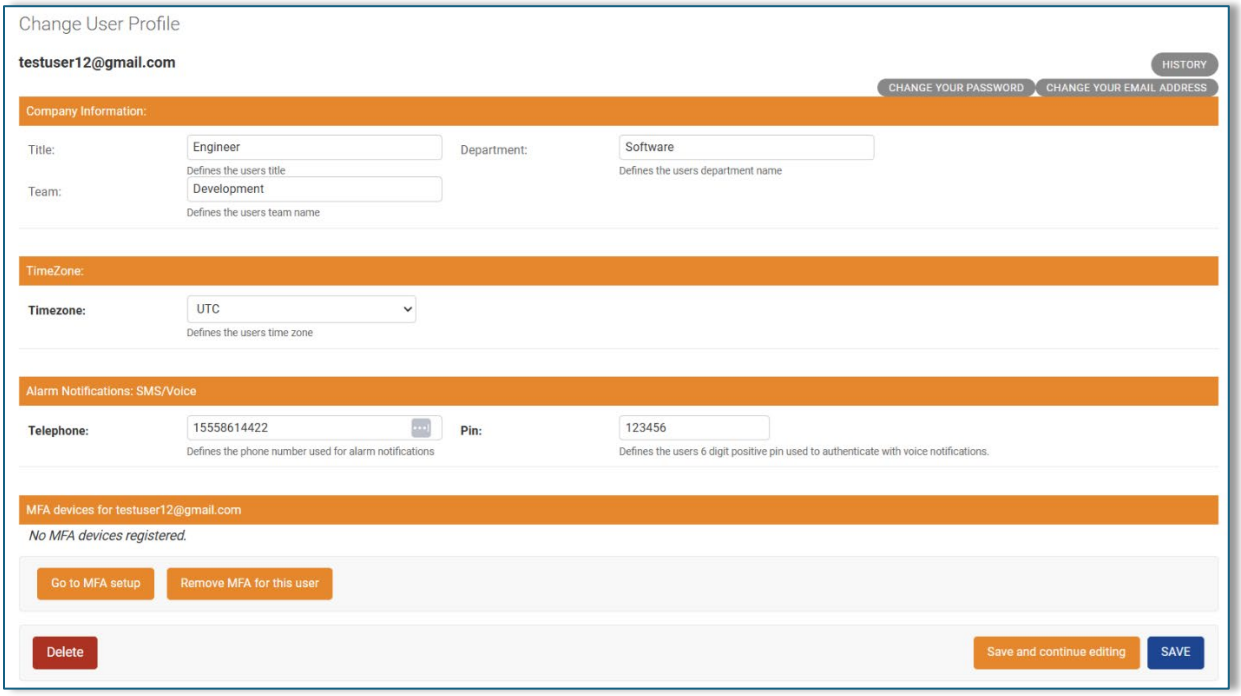
MFA code digits

This specifies the number of digits used for SMS and Email authentication codes. Options are **6 digits** and **8 digits**.

Changing Phone Numbers and Emails

If changes are needed to a phone number or an Email address, do the following:

5. From the main OverShield screen, select **Logs > System > User Profiles** from the sidebar.
6. From the list of names, select the user whose information you want to edit.



When users set up SMS or Email authentication, their phone and email information automatically prefills with the information from their User Profile. This information can only be changed by an OverShield administrator using the following procedures:

To change a user's email address:

1. Navigate to the Change User Profile window. (**Logs > System > User Profiles**) and select the user you want to edit.

   The Change User Profile window opens.

2. In the upper right section of the window, click on the **CHANGE YOUR EMAIL ADDRESS** button.

3. Enter the new email address, confirm it, and click the **Save Email** button.
4. Click the **SAVE** button at the bottom of the Change User Profile window.

To change a user's phone number:

1. Navigate to the Change User Profile window. (**Logs > System > User Profiles**) and select the user you want to edit.

   The Change User Profile window opens.

2. Scroll down to the **Alarm Notifications: SMS/Voice** section.
3. In the **Telephone** field, enter the new phone number using an 11-digit format.
   For example: 15554971516
4. Click the **SAVE** button at the bottom of the Change User Profile window.

Removing MFA From A Single User

As an administrator, you can remove MFA for individual users. This instantly removes all of the MFA methods the user has set up.

Note: Users can also remove their own MFA methods.

1. Navigate to the Change User Profile window. (**Logs > System > User Profiles**) and select the user you want to edit.

   The Change User Profile window opens.

2. Scroll down to the **MFA devices for [user]** section, which shows the types of MFA that are currently active for that user.
3. Click on the **Remove MFA for this user** button.
4. To confirm removal, click on the **Yes, remove MFA** button. To end this action without removing MFA, click **Cancel**.
5. Click the **SAVE** button at the bottom of the Change User Profile window.

20 Cotton Road, Suite 201
Nashua, NH 03063

Phone: (603) 691-3374

E-mail: info@predictivemonitor.com

Follow us on LinkedIn