

OVERVIEW

This guide provides instructions for setting up and using Multi-Factor Authentication (MFA) within the eLANY Electronic Filing System (EEFS/AEROS). MFA adds an extra layer of security by requiring users to provide two forms of verification: Their unique EEFS/AEROS password and a code sent to an email or authentication app (e.g., Microsoft or Google Authenticators).

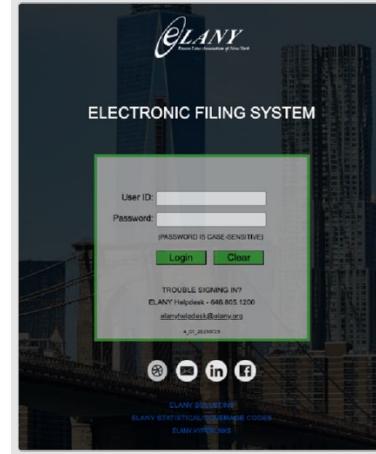
Table of Contents

Initial MFA Setup.....	Page 1
Log into EEFS/AEROS with MFA Enabled	Page 3
Change MFA Settings	Page 4
Best Practices and System Requirements	Page 5

INITIAL MFA SETUP

There are two forms of MFA configuration: Email and Authenticator Applications (Apps, e.g., Microsoft or Google Authenticators). Each user can elect their preference.

1. Login to EEFS/AEROS



2. Navigate to the My Profile page if not automatically redirected.

Choose the Security option at the top of the screen and then choose My Profile on the left.

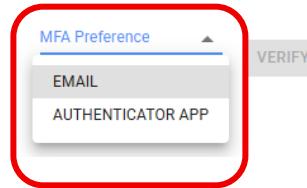


3. Enter an email account

Email is required even if an authenticator application will be used.

4. Select your MFA preference (email or authenticator app).

Options include email or authenticator app.



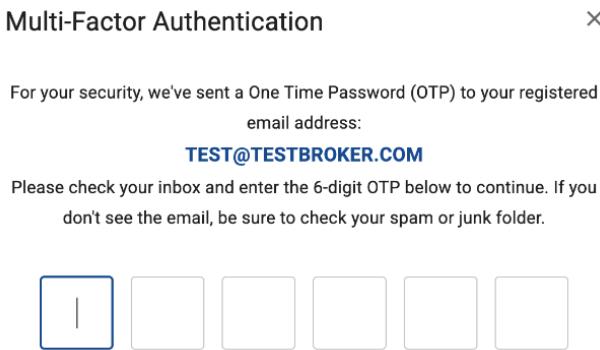
5. Verify your MFA preference.

Click the Verify button

If MFA preference is EMAIL:

An email with a verification code will be sent to the email entered for "MFA email address," and an MFA pop-up screen will display.

Review your email for the One Time Password (OTP) and enter the OTP in the pop-up screen.
(OTP expires after 20 minutes)



If MFA preference is AUTHENTICATOR APP:

Follow the instructions on the QR Code pop-up screen to scan the QR code using your authenticator app.

Enter the One Time Password (OTP) generated by your authenticator app into the text input field on the QR Code Dialog popup screen.



6. Confirm MFA setup success

Green checkmark indicates success.



If Validation Fails

- Re-enter the One Time Passcode (OTP) in the same pop-up screen, OR
- Close the pop-up screen, and click "Verify" again to generate a new OTP

7. For MFA to take effect, please log out and then log back into EEFS/AEROS.

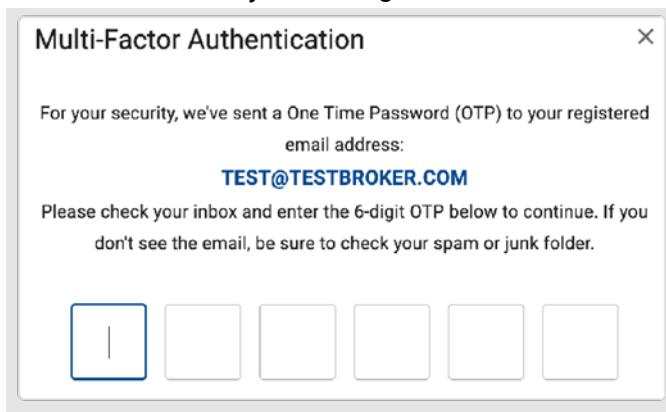
LOGGING IN WITH MFA ENABLED

Standard Login Process

1. Launch the ELANY Electronic Filing System ([EEFS/AEROS](#)) system.
2. Enter your username and password as usual
3. Click the "Login" button
4. MFA Verification Dialog appears prompting for your One Time Password (OTP)

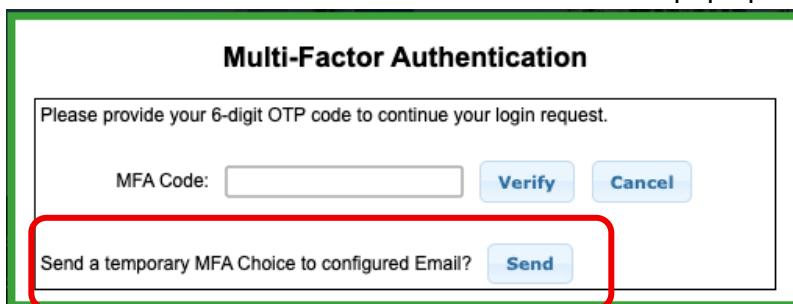
EMAIL MFA Users:

1. System automatically sends OTP to your registered MFA email address
2. Check your email for the OTP code (OTP expires after 20 minutes)
3. Enter the OTP in the MFA Code of the pop-up window and click the Verify button
4. If incorrect: Re-enter the OTP and click the Verify button
5. To generate a new OTP: Click the X in the upper right corner to close the MFA pop-up screen, then click the Verify button again on the EEFS/AEROS screen.



AUTHENTICATOR APP MFA users:

1. Open your authenticator app
2. Locate the OTP code for your User Profile portal account
3. Enter the OTP in the MFA Code of the pop-up window and click the Verify button
4. If incorrect: Re-enter the OTP and click the Verify button
5. Backup option: Click "Send OTP via Email"
 - a. System will send OTP to your registered MFA email address (OTP expires after 20 minutes)
 - b. Enter the email OTP in the MFA Code of the pop-up window and click the Verify button.



CHANGE MFA SETTINGS

MFA preferences can be changed after setup and validation. This includes converting between email and authenticator apps or changing the MFA email address.

1. Navigate to the My Profile page

Choose the Security option at the top of the screen and then choose My Profile on the left.

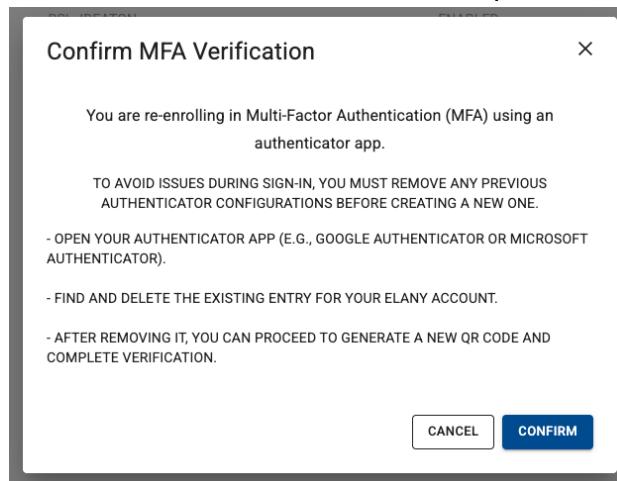


2. Modify the MFA settings and click the Verify button

A screenshot of a form for modifying MFA settings. On the left, there is a field labeled 'MFA Email Address' with the placeholder 'Please enter an MFA email'. On the right, there is a dropdown menu labeled 'MFA Preference' with the placeholder 'Please select an MFA preference'. Below the dropdown is a 'VERIFY' button.

3. Confirm the change.

The confirmation screen contains helpful information when re-enrolling in MFA.



4. Follow the verification process steps (same as steps 5 and 6 from the Initial MFA Setup)

BEST PRACTICES and SYSTEM REQUIREMENTS

System Requirements

- **JavaScript must be enabled** in browsers for the EEFS/AEROS MFA system to function properly
- **Supported browsers:** Chrome, Firefox, Safari, and Edge (latest versions recommended)
- **Access during login to the email accounts and / or authenticator apps** used for the MFA setup
- **MFA Code expirations** - Email codes will expire in 20 minutes; Authenticator app codes expire per authenticator setting.

Best Practices

- **Keep your MFA email address current;** update your profile immediately if your MFA email changes.
- **Clear browser cache regularly** – This resolves many common login and verification issues.
- **Authenticator Apps** – Delete old EEFS accounts before adding new ones
- **Backup authentication is possible** if using an Authentication app (backup to email).
- **Do not share usernames, passwords, or MFA codes.**
- **Logout completely** when finished with your EEFS/AEROS session, especially on shared computers.

For questions, please contact ELANYHelpdesk@elany.org.