IdentitySecurity.net

PACER MFA STARTER KIT

Securing Legal Access

Empower Your Court System Access with Multi-Factor Authentication Essentials

A Step-by-Step Guide

Time-based One-Time Password (TOTP) authentication enhances security by requiring users to provide a dynamic, time-sensitive code along with their credentials. Integrating TOTP with your Secret Server allows for robust multi-factor authentication (MFA) on stored secrets, providing an additional security layer. This article walks you through the essential steps to enable TOTP for a secret, configure it properly, and follow best practices to maintain security integrity.

Step 1: Configure the Secret Template for TOTP

Before enabling TOTP on individual secrets, the underlying secret template must support TOTP functionality.

Access the Secret Templates:

Navigate to Admin > Secret Templates within the Secret Server interface.

Select or Create a Template:

Choose an existing secret template (e.g., “Web Password”) or create a new one tailored to your needs.

Add a One-Time Password (OTP) Field:

Modify the template by adding an OTP field designed to store and generate TOTP codes.

Configure TOTP Settings:

Define the TOTP parameters, including the hashing algorithm (such as SHA-1, SHA-256), the period (time interval, typically 30 seconds), and the number of digits for the OTP code (commonly 6).

Save the Template:

Confirm and save your changes to ensure the template supports TOTP generation.

Step 2: Create or Edit a Secret with TOTP Enabled

Once the template supports TOTP, apply it to the actual secrets.

Navigate to Secrets:

Go to Secrets > All Secrets.

Create or Modify a Secret:

Use the TOTP-enabled secret template to create a new secret or edit an existing one.

Enter the TOTP Secret Key:

Input the secret key provided by your external authentication system (e.g., Google Authenticator or an enterprise MFA solution).

Enable TOTP Generation:

If available, activate the option to generate TOTP codes within the Secret Server.

Save the Secret:

Finalize by saving your secret with the TOTP configurations.

For more content like and follow me: @bertblevins

Step 3: Generate and Use TOTP Codes

After setup, generate OTPs to authenticate or autofill login credentials.

01. Open the Secret:
Access the saved secret in Secret Server.

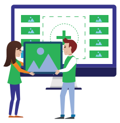
02. Generate One-Time Password:
Click the option to Generate One-Time Password to produce the current TOTP code.

03. Copy and Use the Code:
Use the displayed TOTP code to authenticate on your target system.

04. Utilize Web Password Filler (WPF) if Available:
If integrated, WPF can autofill credentials and TOTP codes for seamless login experiences.

Step 4: (Optional) Configure Secret Server as a TOTP Generator

Secret Server can act as a TOTP generator for enhanced control.



Confirm
the secret template's TOTP settings are active.

Enable TOTP
generation in the secret's configuration settings.

Test code generation
with the target application to ensure compatibility.

Step 5: Securely Store Backup Codes

Backup codes act as fallback authentication in case TOTP devices are unavailable.

01. Store backup codes encrypted within Secret Server to prevent unauthorized access.

02. Treat each backup code as a one-time use credential to bypass TOTP when necessary.

Step 6: Test the TOTP Setup Thoroughly

Validation is critical to ensure a smooth user experience.

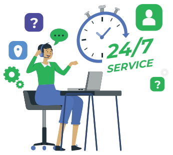
Test
user login procedures requiring TOTP codes.

Confirm
that TOTP codes generated by Secret Server or external systems are accepted by the target systems.

Verify
that autofill functionality via WPF works as expected if implemented.

Step 7: Follow Best Practices for TOTP Management

Maintaining security over TOTP implementations involves ongoing diligence.



Protect TOTP Keys and Backup Codes:

Store all sensitive keys and backup codes securely, using encryption and strict access controls.

Align Hashing Algorithms:

Ensure the hashing algorithm set in Secret Server matches that of your external authentication system for seamless code validation.

Conduct Regular Audits

Review TOTP usage logs periodically to detect unauthorized or suspicious activity.

Enable MFA on High-Security Secrets:

Prioritize enabling TOTP and other MFA methods on credentials with elevated privileges.

Plan Backup Code Recovery:

Establish clear protocols for distributing, revoking, and regenerating backup codes to minimize disruption.

Conclusion

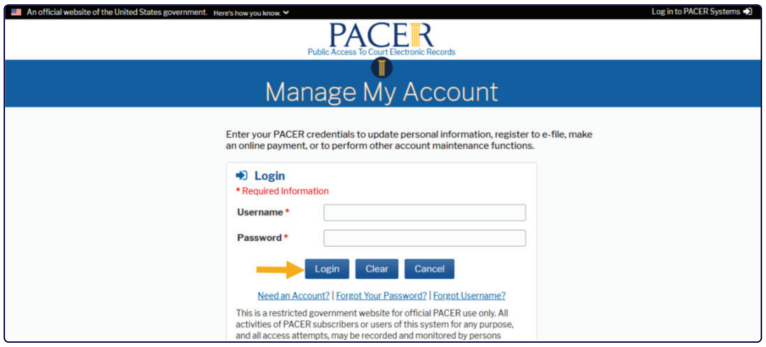
Implementing TOTP within your Secret Server environment significantly strengthens your security posture by adding a dynamic authentication layer for sensitive credentials. Following the outlined steps—from template configuration to rigorous testing and adherence to best practices—ensures a reliable, secure, and user-friendly MFA experience. Proper management of TOTP keys, backup codes, and regular auditing will help maintain the integrity of your authentication process and safeguard your critical assets.

How to Enroll in Multifactor Authentication (MFA)

Using Authentication Apps for PACER

Multifactor Authentication (MFA) adds an essential layer of security beyond passwords by requiring a secondary verification step to access accounts. For PACER (Public Access to Court Electronic Records) users, MFA is now available and mandatory for certain user types to protect sensitive legal information and prevent cyberattacks such as password theft.

This article provides a clear, step-by-step guide to enrolling in MFA using authentication apps with your PACER account, as well as managing your MFA settings including adding and deleting authentication apps.


An official website of the United States government. Here's how you know.
Log in to PACER Systems
PACER
Public Access To Court Electronic Records

Manage My Account

Enter your PACER credentials to update personal information, register to e-file, make an online payment, or to perform other account maintenance functions.

Login
* Required Information
Username *
Password *

Login
Clear
Cancel
Need an Account? | Forgot Your Password? | Forgot Username?

This is a restricted government website for official PACER use only. All activities of PACER subscribers or users of this system for any purpose, and all access attempts, may be recorded and monitored by persons

Fig 1: Manage My Account login page

Why Use MFA with PACER?

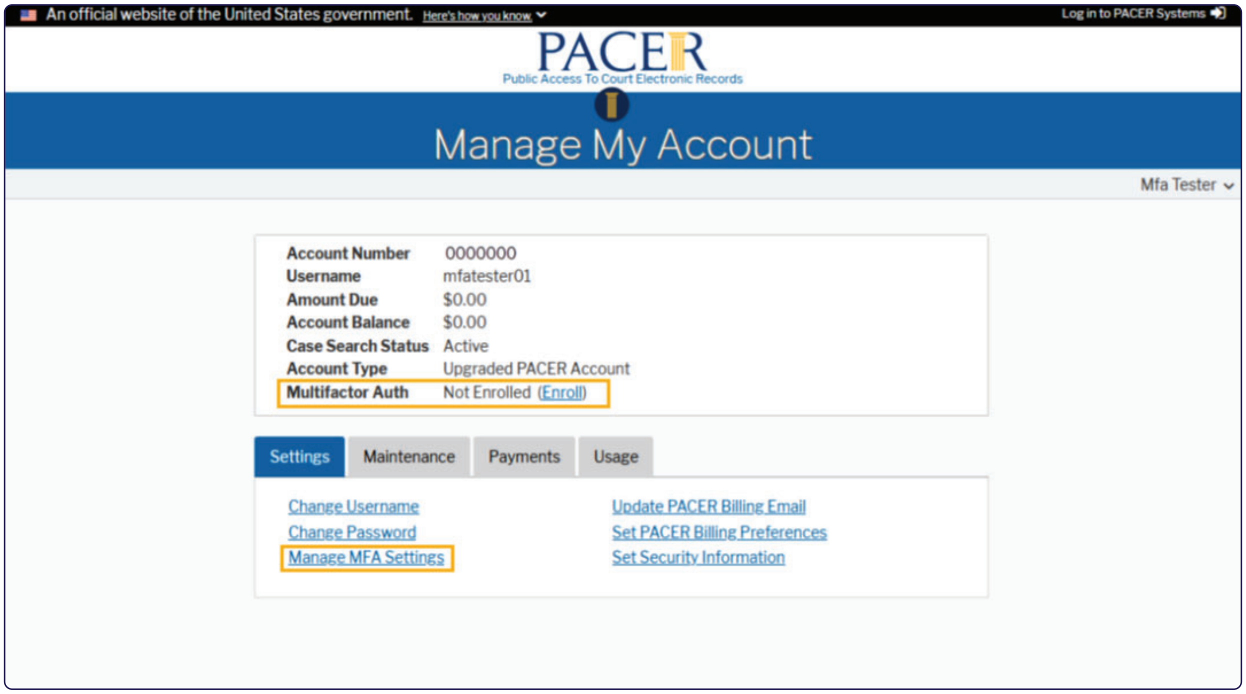
Passwords alone can be vulnerable to hacking or phishing attempts. By requiring a one-time passcode generated on an authentication app, MFA ensures that even if your password is compromised, unauthorized access is still prevented. This added security is critical for PACER users who handle confidential court documents or perform filings.

Step 1: Access Your PACER Account Settings

Navigate
to https://pacer.uscourts.gov/.

Click Log in to...
in the top-right corner, then select Manage PACER Account.

Enter your PACER
username and password, then click Login.



An official website of the United States government. Here's how you know
Log in to PACER Systems
PACER
Public Access To Court Electronic Records
Manage My Account
Mfa Tester

Account Number	0000000
Username	mfatester01
Amount Due	$0.00
Account Balance	$0.00
Case Search Status	Active
Account Type	Upgraded PACER Account
Multifactor Auth	Not Enrolled (Enroll)

Settings
Maintenance
Payments
Usage
Change Username
Change Password
Manage MFA Settings
Update PACER Billing Email
Set PACER Billing Preferences
Set Security Information

Fig 2: Manage My Account landing page

Step 2: Begin MFA Enrollment

01. On your account landing page, find the Multifactor Auth section.

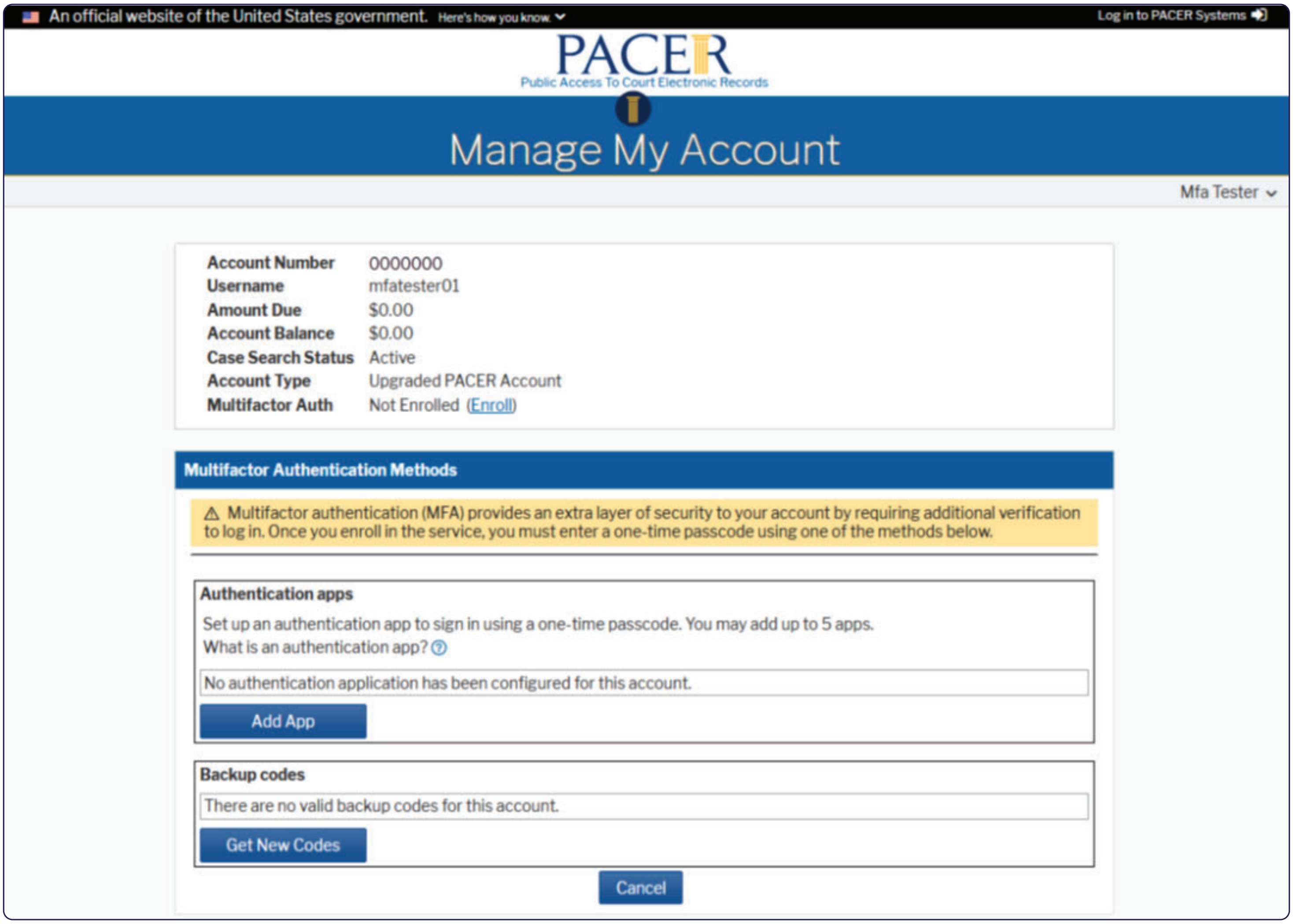
02. Click the Enroll link or go to Manage MFA Settings under the Settings tab.

Step 3: Add an Authentication App

Click Add App
to begin linking an authentication app to your PACER account.

To verify
your authorization, PACER will send a security code to your registered email.

Retrieve
the code from your inbox (or junk folder if you don't see it) and enter it on the website, then submit.



An official website of the United States government. Here's how you know
Log in to PACER Systems
PACER
Public Access To Court Electronic Records

Manage My Account

Account Number	0000000
Username	mfatester01
Amount Due	$0.00
Account Balance	$0.00
Case Search Status	Active
Account Type	Upgraded PACER Account
Multifactor Auth	Not Enrolled (Enroll)

Multifactor Authentication Methods

⚠ Multifactor authentication (MFA) provides an extra layer of security to your account by requiring additional verification to log in. Once you enroll in the service, you must enter a one-time passcode using one of the methods below.

Authentication apps

Set up an authentication app to sign in using a one-time passcode. You may add up to 5 apps.
What is an authentication app? ?

No authentication application has been configured for this account.

Backup codes

There are no valid backup codes for this account.

Fig 3: Multifactor Authentication Methods page – Authentication apps section

Step 4: Configure Your Authentication App

01. Assign a nickname for your app in PACER (e.g., "My Phone").

02. Open your authentication app on your device.

03. Use the app's "+" or "Add Account" feature to scan the QR code shown by PACER or enter the provided code manually.

04. After adding the PACER account, return to the PACER site and click Next.

Step 5: Verify the Authentication Setup

Your authentication app will display a one-time passcode.

Enter this passcode in the PACER website's Enter Code field and click Next.

Important: Click the Next button instead of pressing Enter to proceed correctly.

You will then receive confirmation that your authentication app has been successfully enrolled.

Managing Multiple Authentication Apps

You can link up to five authentication apps to your PACER account. This flexibility allows you to add devices for other authorized users, such as a paralegal or assistant, ensuring multiple people can access the account securely.

Deleting an Authentication App

If you need to remove an authentication app:

01. Go to the Authentication Apps section in your MFA settings.

02. Click the Delete link next to the app you want to remove.

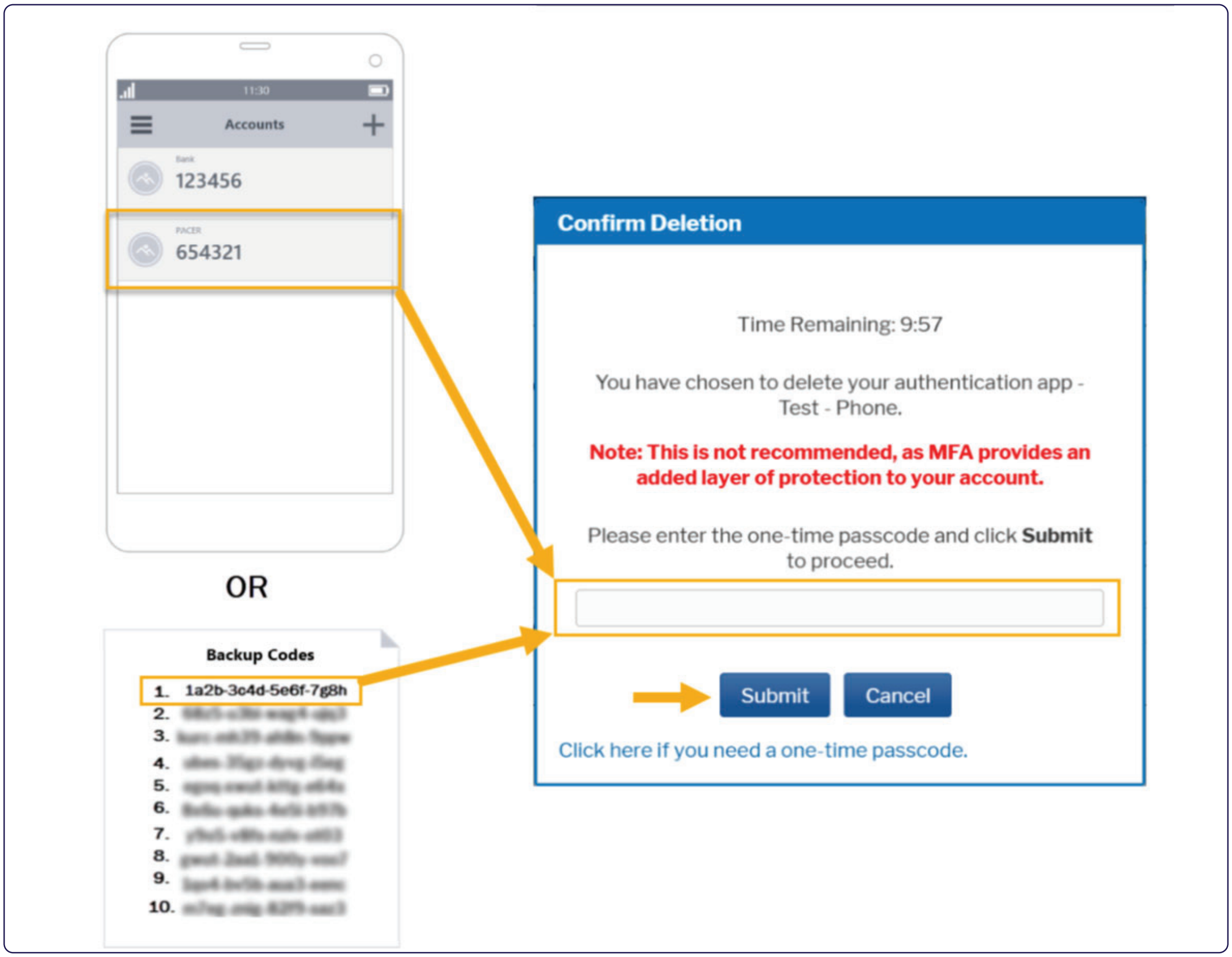
03. Enter either a backup code or a current passcode from the app being deleted, then submit.

04. Once deleted, the app's passcodes will no longer work for your PACER account.

Note:
If you are required to use MFA, you cannot delete all authentication apps without having backup codes available.

Backup Codes: Your MFA Safety Net

Backup codes allow access if your authentication app is unavailable (e.g., lost device). PACER provides an option to generate and store these codes. Treat backup codes as single-use credentials and store them securely.



Confirm Deletion

Time Remaining: 9:57

You have chosen to delete your authentication app - Test - Phone.

Note: This is not recommended, as MFA provides an added layer of protection to your account.

Please enter the one-time passcode and click **Submit** to proceed.

Fig 4: Confirm Deletion dialog box and illustrations of a generic authentication app display and list of backup codes

Conclusion

Enrolling in MFA with an authentication app is a straightforward but crucial step for securing your PACER account. It helps protect sensitive court information with an additional verification factor that is dynamically generated and time-limited. By following the steps above, you can quickly set up, manage, and delete authentication apps as needed. Remember to keep backup codes safe to avoid being locked out of your account.