

Introduction

The Administrative Office of the U.S. Courts (AO) will implement Multi-Factor Authentication (MFA) for PACER and CM/ECF systems starting May 11, 2025, to enhance security against cyberattacks. MFA is mandatory for CM/ECF users (e.g., attorneys, trustees) by December 31, 2025, and optional for PACER-only users.

Delinea, a leader in Privileged Access Management (PAM) and identity security, offers robust MFA solutions through its Secret Server and Delinea Platform to meet these requirements, ensuring secure access, compliance, and seamless integration with existing systems.

Challenges of the New MFA Requirements



Mandatory MFA for CM/ECF Users:
All users with filing or CM/ECF-level access must enroll in MFA, with phased enforcement starting August 2025.



Third-Party Software Compatibility:
Users must ensure third-party filing software supports MFA to avoid disruptions.



Security Risks:
Password theft via phishing or cyberattacks necessitates strong authentication to protect sensitive court records.



User Experience:
Balancing security with ease of use to prevent delays in filing or accessing records.



Compliance:
Adhering to federal security standards while maintaining operational efficiency.


How Delinea Addresses These Challenges

Delinea’s Secret Server and Delinea Platform provide comprehensive MFA solutions tailored to the needs of federal court systems, ensuring compliance, security, and usability.


Robust MFA Support with Secret Server

Secret Server integrates MFA to secure access to sensitive systems like PACER and CM/ECF, supporting multiple authentication methods to meet diverse user needs.


Supported MFA Providers:
Integrates with Google Authenticator, Microsoft Authenticator, Duo Security, RSA SecurID, and any RADIUS-compliant provider, allowing users to use time-based one-time passwords (TOTP) or push notifications.




RADIUS Integration:
Supports industry-standard RADIUS interfaces, enabling compatibility with existing court IT infrastructure and third-party software.



Backup Options:
Offers out-of-band authentication (e.g., phone calls, SMS) or backup codes for users unable to access their primary MFA method, preventing lockouts during critical filings.



Ease of Enablement:
MFA can be quickly enabled for Secret Server, ensuring rapid deployment to meet the May 2025 rollout.

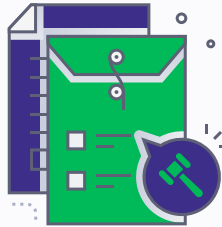


Adaptive MFA with the Delinea Platform

The Delinea Platform provides cloud-based, flexible MFA with adaptive authentication, enhancing security without compromising user experience.

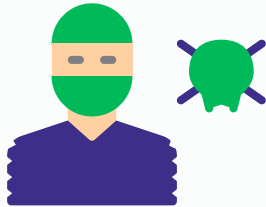
Context-Based Authentication:

Uses contextual factors (e.g., location, device, network) to trigger MFA only when necessary, reducing friction for users logging in from trusted court networks or devices.




Authentication Profiles and Policies:

Allows administrators to create tailored MFA profiles and identity policies, ensuring CM/ECF users meet mandatory requirements while PACER-only users can opt-in as needed.




Delinea Mobile App:

Supports MFA via the Delinea Mobile App, which vaults OATH tokens for secure OTP generation, compatible with court systems requiring compliant authentication.




Federated Authentication:

Supports integration with external identity providers (e.g., Okta, Ping Identity) via SAML or Active Directory with Kerberos/IWA, streamlining access for court staff and third-party vendors.




Seamless Integration with Third-Party Software

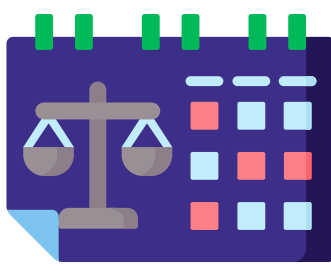
Delinea ensures compatibility with third-party filing software, a critical requirement for PACER and CM/ECF users.



Standards Compliance:
Adheres to standards like RADIUS and OATH, ensuring interoperability with court-approved software and testing environments (e.g., PACER QA environment).




API Support:
Provides APIs for custom integrations, allowing third-party developers to incorporate Delinea MFA into existing workflows, minimizing disruptions.




Testing and Validation:
Users can test MFA compatibility in a controlled environment, aligning with the AO's recommendation to use the PACER QA environment.

Enhanced Security for Privileged Access


PACER and CM/ECF handle sensitive legal data, making privileged account security paramount. Delinea's PAM capabilities protect these accounts.



Privileged Access Management:
Secret Server secures privileged accounts (e.g., administrative or shared accounts) with MFA at login, privilege elevation, or password checkout, reducing unauthorized access risks.




Behavior-Based Access Control:
Applies MFA based on risk ratings, adding security for high-risk actions like accessing sensitive case files or modifying records.



Continuous Monitoring:
Integrates with SIEM systems for real-time threat detection, ensuring compliance with federal cybersecurity standards.

For more content like and follow me:



@bertblevins

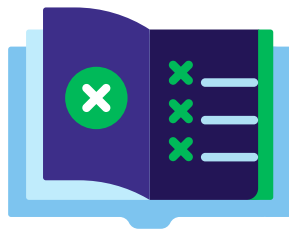
User-Friendly Experience

Delinea balances security with usability to support court staff and public users.



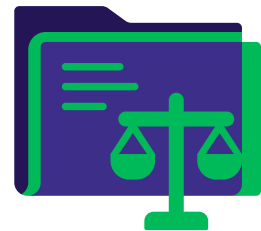
Single Sign-On (SSO) Integration:

Combines MFA with SSO to reduce password fatigue, allowing users to access multiple court systems with one set of credentials.



Training and Support:

Provides documentation and training resources to educate users on MFA setup and usage, addressing the AO’s emphasis on early enrollment.



Backup Authentication:

Ensures alternative methods (e.g., backup codes, secondary devices) prevent lockouts, critical for meeting filing deadlines.

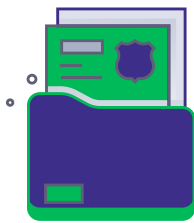
Compliance with Federal Standards

Delinea aligns with federal regulations and security best practices.



Single Sign-On (SSO) Integration:

Supports standards like NIST, HIPAA, and PCI, which align with federal court security requirements.



Audit and Reporting:

Offers comprehensive logs and reports for MFA usage, enabling courts to demonstrate compliance during audits.



Secure Remote Access:

Ensures MFA for remote access complies with guidelines like IRS Publication 1075, relevant for court systems handling sensitive data.

Implementation Recommendations

To leverage Delinea for PACER and CM/ECF MFA compliance:



Deploy Secret Server for CM/ECF Users:

Enable MFA with Google Authenticator or Duo Security for mandatory users, integrating with RADIUS for compatibility.



Use Delinea Platform for Adaptive MFA:

Configure context-based policies for PACER-only users to encourage voluntary enrollment without disrupting workflows.



Test in QA Environment:

Validate third-party software compatibility in the PACER QA environment using Delinea’s API and RADIUS support.



Train Users Early:

Provide training sessions before May 11, 2025, to ensure smooth adoption, especially for CM/ECF users facing mandatory enrollment.



Monitor and Audit:

Use Secret Server’s monitoring and reporting tools to track MFA usage and ensure compliance by December 31, 2025.

Conclusion

Delinea’s Secret Server and Delinea Platform offer a comprehensive solution to meet the AO’s MFA requirements for PACER and CM/ECF. By providing robust, flexible, and user-friendly MFA, seamless third-party integration, and compliance with federal standards, Delinea ensures secure access to sensitive court systems while minimizing disruptions. Courts can rely on Delinea to protect against cyberattacks, streamline authentication, and support a smooth transition to MFA by the 2025 deadline.