**Delinea:**
Offboarding Legal Resource

Delinea

# Responsibilities

## IT/Security Administrator:

Executes the deactivation process in Secret Server, verifies audit logs, and coordinates with the firm's PACER account manager.

## Human Resources (HR):

Notifies IT of the attorney's departure and provides relevant details (e.g., employee ID, departure date).


## Legal Department:

Ensures compliance with court requirements for PACER account updates, if applicable.

# Prerequisites

**01.** Access to Delinea Secret Server with administrative privileges.

**02.** Confirmation of the attorney's departure from HR.

**03.** Identification of the specific PACER web password secret associated with the attorney (e.g., secret name, folder, or ID).

**04.** Access to PACER's Manage My Account portal for updating contact information, if required.

# Procedure

## Step 1: Verify Attorney Departure

**01. HR Notification:**

HR confirms the attorney's departure, including the effective date and any relevant details (e.g., whether cases are transferring with the attorney).

**02. PACER Account Check:**

Verify whether the PACER account is individual or firm-shared:

- If individual, the attorney may retain the account but must update contact information in PACER's Manage My Account portal.
- If firm-shared, proceed with deactivation of the secret in Secret Server.

**Delinea:**
Offboarding Legal Resource

Delinea

## Step 2: Locate the PACER Web Password Secret

Log in to Delinea Secret Server using administrative credentials.

Navigate to the All Secrets page or the specific folder where PACER secrets are stored (e.g., “Legal/PACER Accounts”).

Search for the secret by name (e.g., “PACER_AttorneyName” or “domain/attorney_ username”) or filter by the web password template.

Confirm the secret’s details, including:
- Username associated with the PACER account.
- Folder permissions.
- Audit history to verify recent access.

## Step 3: Check Out and Restrict Access

**01.** If the secret is configured for checkout, ensure it is not currently checked out by another user. If it is, coordinate with the user or an unlimited administrator to release it.

**02.** Modify folder or secret permissions to remove the departing attorney’s access:
- Navigate to the secret’s folder or the secret itself.
- Update role-based access control (RBAC) to revoke permissions for the attorney’s Active Directory (AD) account or Secret Server user account.
- If using a hybrid group structure, confirm the attorney’s AD account is disabled to automatically deprovision access.

## Step 4: Deactivate or Rotate the Password

### Option 1: Deactivate the Secret (if the PACER account is no longer needed):

- Open the secret’s configuration page.
- Disable the secret by selecting “Deactivate” or archiving it to prevent further use.
- Document the deactivation in the audit log with a note (e.g., “Deactivated due to attorney departure on [date]”).

### Option 2: Rotate the Password (if the PACER account is shared and will remain active):

- Enable Remote Password Changing (RPC) if not already configured, or manually trigger a password rotation:
  - Go to the secret’s Security tab and select “Generate” to create a new password meeting PACER’s requirements (e.g., strong password, max 1024 characters).
  - Update the PACER account with the new password via the Manage My Account portal or coordinate with the firm’s PACER account manager.
- Verify the rotation in the audit log and ensure the new password is not shared with the departing attorney.

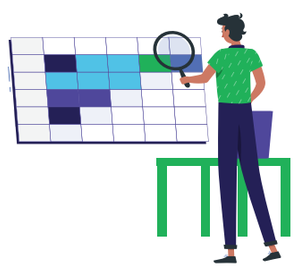
## Step 5: Update PACER Account Details

**01.** If the PACER account is firm-managed, log in to PACER’s Manage My Account portal:
- Update email notification settings to remove the attorney’s email from CM/ECF noticing or duplicate receipt lists (up to five support staff or 255 characters).
- Submit a change of address to the clerk’s office if cases are not transferring with the attorney.

**02.** If MFA is enabled (mandatory for CM/ECF users by December 31, 2025), ensure the attorney’s MFA tokens (e.g., Google Authenticator, Delinea Mobile App) are removed from Secret Server’s MFA configuration.

For more content like and follow me:  @bertblevins

## Step 6: Audit and Report



Review the secret's audit log to confirm no unauthorized access occurred before or during offboarding.

Generate a report in Secret Server to document the deactivation or password rotation event:

- Navigate to Reports and select a relevant audit report (e.g., "Secret Access History").
- Export the report for compliance records.

If session recording was enabled for the secret, archive or offboard recordings to the firm's storage, as per compliance requirements (4TB limit for standard service).

## Step 7: Notify Stakeholders

Inform HR and the legal department that the secret has been deactivated or rotated.

If the PACER account is individual and transferring with the attorney, remind them to update their contact information and reactivate the account if inactive (e.g., after two years of non-use).


Document the offboarding process in the firm's internal records for compliance audits.

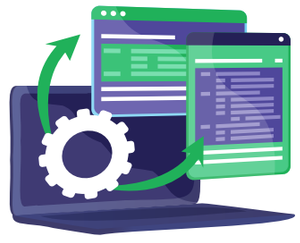
## Best Practices

### Automate User Deprovisioning:

Sync Secret Server with Active Directory to automatically disable user access when the attorney's AD account is disabled.

### Minimize Session Recording:

Only enable session recording for high-risk secrets to reduce infrastructure overhead.



### Secure Shared Accounts:

If the PACER account is shared, rotate passwords immediately upon the attorney's departure to prevent unauthorized access.

### Compliance:

Ensure all actions comply with federal cybersecurity standards, especially for PACER's MFA requirements starting May 11, 2025.