TokenCore.com

TECHNICAL IMPLEMENTATION GUIDE

Token × Delinea Joint Integration Guide

Phishing-resistant biometric MFA for the Delinea Platform — from administrator login to step-up secret access to audit evidence that names the verified person.

TOKEN

IMPLEMENTATION GUIDE

Contents

00 About This Guide 2
Use cases, solution components, and why it matters

UC 1 Phishing-Resistant MFA at Platform Login 3
Overview · Administrator configuration · End-user enrollment · Verification

UC 2 Step-Up MFA for Sensitive Secret Access 8
Overview · Administrator configuration · Protected checkout · Verification

UC 3 Non-Repudiation for Compliance 12
Overview · Audit evidence · Verification · Control narrative

– Joint Validation Items 15
What TokenCore and Delinea confirm together before Marketplace publication

AUDIENCE

Delinea Platform administrators, TokenCore administrators, IdP administrators, PAM admins, and compliance / GRC teams.

EACH USE CASE INCLUDES

Listing description, architecture, roles and responsibilities, configuration, end-user walkthrough, verification, and references.

SOURCES

Delinea steps follow official Delinea documentation. TokenCore behavior rests on its published FIDO 2.1 / WebAuthn compliance.

00 / INTRODUCTION

About This Guide

This guide covers three joint use cases implementing the **TokenCore biometric FIDO 2.1 authenticator** with the **Delinea Platform**. Configuration steps for Delinea products are taken from official Delinea documentation; TokenCore-side behavior rests on its published FIDO 2.1 / WebAuthn compliance.

The Three Use Cases

USE CASE 1

Phishing-Resistant MFA at Platform Login

Every administrator login to the Delinea Platform requires biometric FIDO2 on the TokenCore device: on-device fingerprint plus BLE proximity.

USE CASE 2

Step-Up MFA for Sensitive Secret Access

Checkout of tier-0 secrets, break-glass accounts, and approval-workflow credentials requires a step-up FIDO2 challenge on the device, replacing the default email code.

USE CASE 3

Non-Repudiation for Compliance

The unified audit trail inherits hardware-biometric and proximity attribution from every TokenCore-authenticated event — evidence for PCI DSS, NIS2, DORA, and cyber-insurance attestations.

Solution Components

COMPONENT	ROLE IN THE SOLUTION
TokenCore device	FIDO 2.1 biometric authenticator in four form factors — Wearable (ring), Portable, Node, and Card. The setup and user experience in this guide are the same across form factors. Fingerprint matching runs on the device, with keys held in an EAL5+ certified secure element. Bluetooth Low Energy confirms physical presence within ~3 feet before authentication begins. Credentials are hardware-bound: non-syncable, non-shareable, non-delegable.
Delinea Platform	Identity security control plane: authentication profiles, identity policies, MFA for secrets, unified audit.
Secret Server (on the Platform)	Vaulting, checkout workflows, secret policies.
Identity Provider	Okta, Microsoft Entra ID, or any OIDC / SAML IdP — the federation layer where TokenCore registers as a FIDO2 authenticator.

WHY THIS MATTERS

PAM-admin credentials, tier-0 secrets, and break-glass accounts are the accounts attackers value most. Push-approvable or OTP-based MFA on those accounts is the vector behind most PAM-related breaches in 2025–26. Hardware-bound biometric FIDO2 removes that vector cryptographically — origin-bound credentials cannot be relayed through AiTM phishing kits, and there is no PIN or code to type on a fake portal.

USE CASE 1 / TOKENCORE + DELINEA PLATFORM

Phishing-Resistant MFA at Platform Login

DESCRIPTION — FOR DELINEA LISTING

The TokenCore device becomes the FIDO2 authentication challenge in Delinea Platform MFA. Every administrator login to the Platform requires on-device fingerprint verification and Bluetooth Low Energy proximity, eliminating credential phishing and MFA push fatigue for the accounts attackers value most. No custom integration code is required — the Delinea Platform accepts FIDO2 / WebAuthn authenticators natively in its authentication profiles.

Architecture

A Delinea Platform authentication profile declares a FIDO2 challenge. When a user attempts to log in, the Platform issues a WebAuthn challenge; the TokenCore device verifies the user's fingerprint on the device, confirms BLE proximity, and signs the challenge with a hardware-bound key — the private half of which never leaves the device. The Platform verifies the assertion and the session proceeds.

01 · PLATFORM
Admin Signs In
Login hits an identity policy with a FIDO2 profile.

→

02 · PLATFORM
WebAuthn Challenge
Platform issues an origin-bound FIDO2 challenge.

→

03 · DEVICE
Fingerprint + Proximity
Match runs on the device; BLE confirms presence.

→

04 · DEVICE
Signed Assertion
Hardware-bound key signs the challenge.

→

05 · PLATFORM
Session Proceeds
Platform verifies the assertion and logs the event.

Roles and Responsibilities

WHO	DOES WHAT
TokenCore administrator	Provisions devices, enrolls user fingerprints on the device (the biometric never leaves the device), distributes hardware, manages lifecycle (lost / replaced devices).
Delinea Platform administrator	Creates the authentication profile with the FIDO2 challenge, enables FIDO2 enrollment in the identity policy, assigns the policy to admin groups.
End user (PAM admin)	Registers the device as a FIDO2 authenticator in their Platform user profile; uses it at every login going forward.
IdP administrator (if federated)	Ensures federated users are still prompted for Platform MFA — see the federated-tenants note on the next page.

USE CASE 1 / CONTINUED

Delinea Platform Administrator — Configuration

Three settings in the Delinea Platform turn the TokenCore device into the login challenge for your PAM administrators.

01

Create the Authentication Profile with a FIDO2 Challenge

Navigate to `Settings > Authentication Profiles > Add Authentication Profile`. Select **FIDO2 authenticator** as an authentication challenge. Save.

02

Enable FIDO2 Enrollment in the Identity Policy

Navigate to `Access > Identity Policies` > select the policy > `User Security > Authentication Settings > Edit`. Enable **Enable users to enroll FIDO2 authenticators**. Save.

03

Assign the Login Profile

In `Identity Policies` > the policy > `Authentication > Services > Edit`, enable **Enable authentication policy controls**, then select the FIDO2 profile from Step 1 as the **Default authentication profile**. Save.

CRITICAL — AVOID THE ENROLLMENT LOCKOUT

The profile a user is on while enrolling a FIDO2 authenticator must not itself require the FIDO2 challenge, or the user is locked in an authentication loop. This is per official Delinea documentation. Keep the enrollment profile free of the FIDO2 requirement until the user has a registered authenticator.

FEDERATED TENANTS

Disable the identity-policy setting **Platform login via federation satisfies all MFA mechanisms**. Otherwise federated users bypass the FIDO2 challenge entirely because their IdP has already satisfied MFA at the federation layer.

ROLLOUT RECOMMENDATION

Pilot with a small group first (3–5 PAM admins, 1 week). Confirm the login flow, confirm audit event capture, and confirm the lost-device recovery procedure with the TokenCore administrator. Then expand across the full PAM-admin population.

USE CASE 1 / END USER (PAM ADMIN)

Register Your TokenCore Device

Once your Delinea Platform administrator has published the authentication policy, follow the six steps below to register your TokenCore device. The process takes about two minutes.

STEP 1 Open Your Security Settings

Log in to the Delinea Platform. Click your user icon in the top-right corner, then **Account details**. Open the **Security** tab. You will see three verification mechanisms: Password (already configured), Security questions (optional), and **Token Device**. Click the Token Device card to configure it.

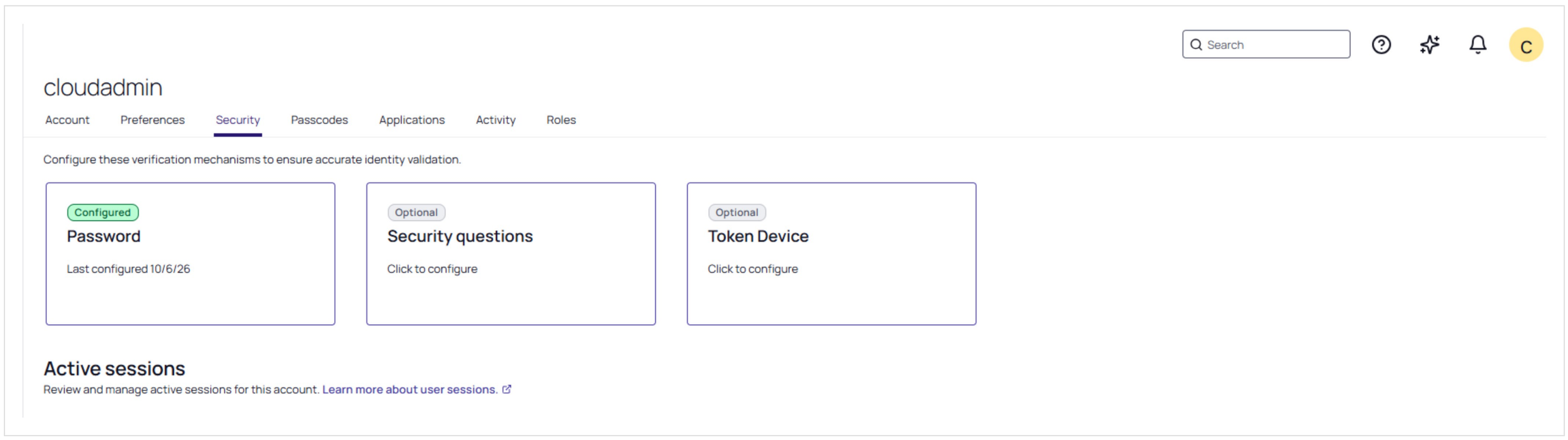


FIGURE 1.1 Delinea Platform Security tab. Click the Token Device card to begin FIDO2 enrollment.

STEP 2

Review the Enrollment Prompt and Get Ready

The Delinea Platform explains its passkey option and confirms that it works with any FIDO2-certified security key. The TokenCore device is FIDO2-certified. Have your TokenCore device ready — on your finger if it is the Wearable, or in hand if it is the Portable or Node — then click **Next**.

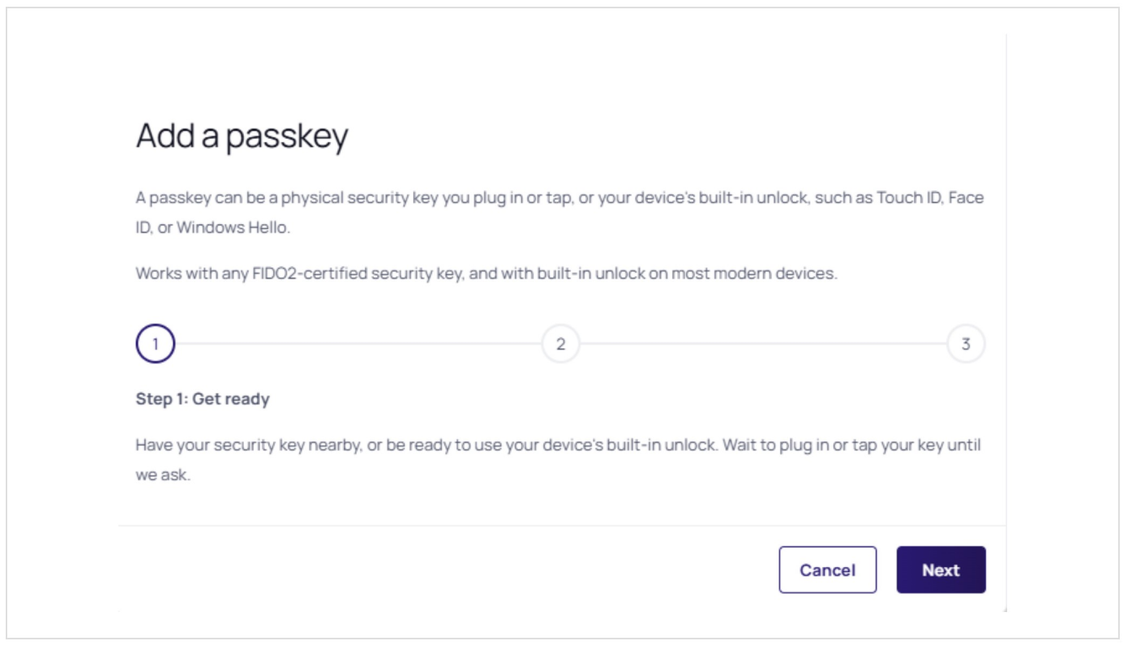


FIGURE 1.2 Step 1 of 3: the pre-enrollment confirmation screen.

STEP 3

Name Your Authenticator

Give the authenticator a friendly name so you can recognize it later in your account's device list. Use a label that matches the device you were issued — for example **Token Wearable**, **Token Portable**, or **Token Node**. This is only a display label; it does not change how the authenticator works. Click **Next**.

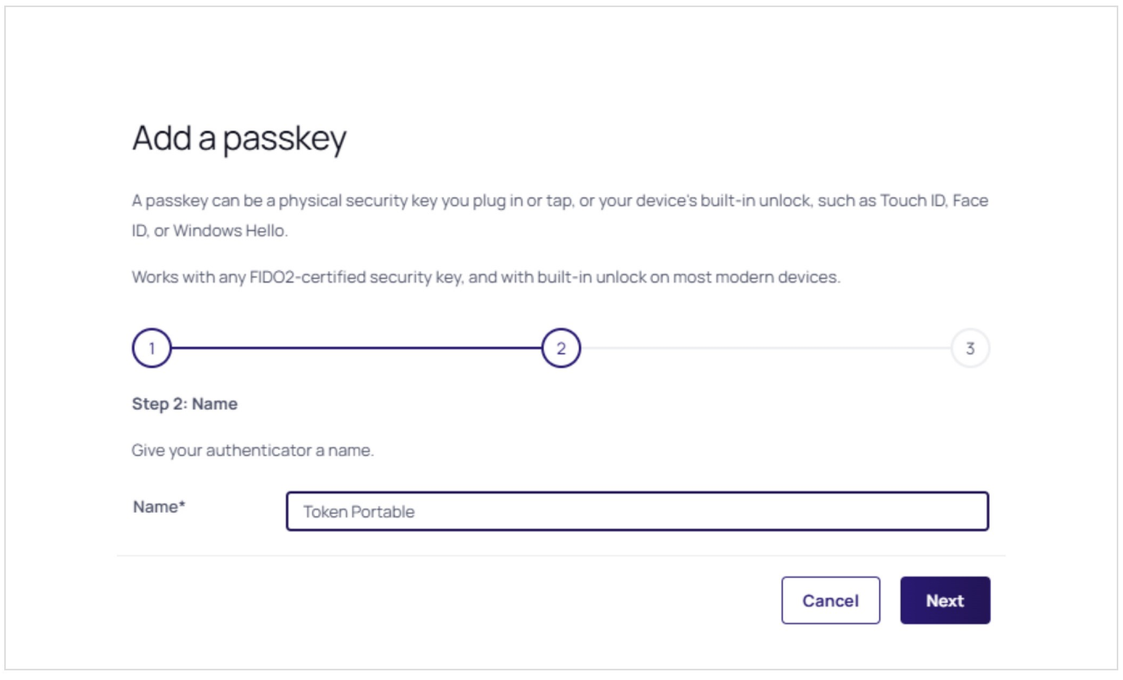


FIGURE 1.3 Step 2 of 3: name your authenticator.

USE CASE 1 / END USER / CONTINUED

Bind the Credential to Your Device

STEP 4

Choose “Security Key” in the Windows Security Dialog

Windows will offer several places to save the new credential. For the TokenCore device, choose **Security key**. Do not choose “This Windows device”, “Microsoft Password Manager”, or “iPhone, iPad, or Android device” — those save the credential into Windows Hello or a password manager instead of onto your TokenCore device.

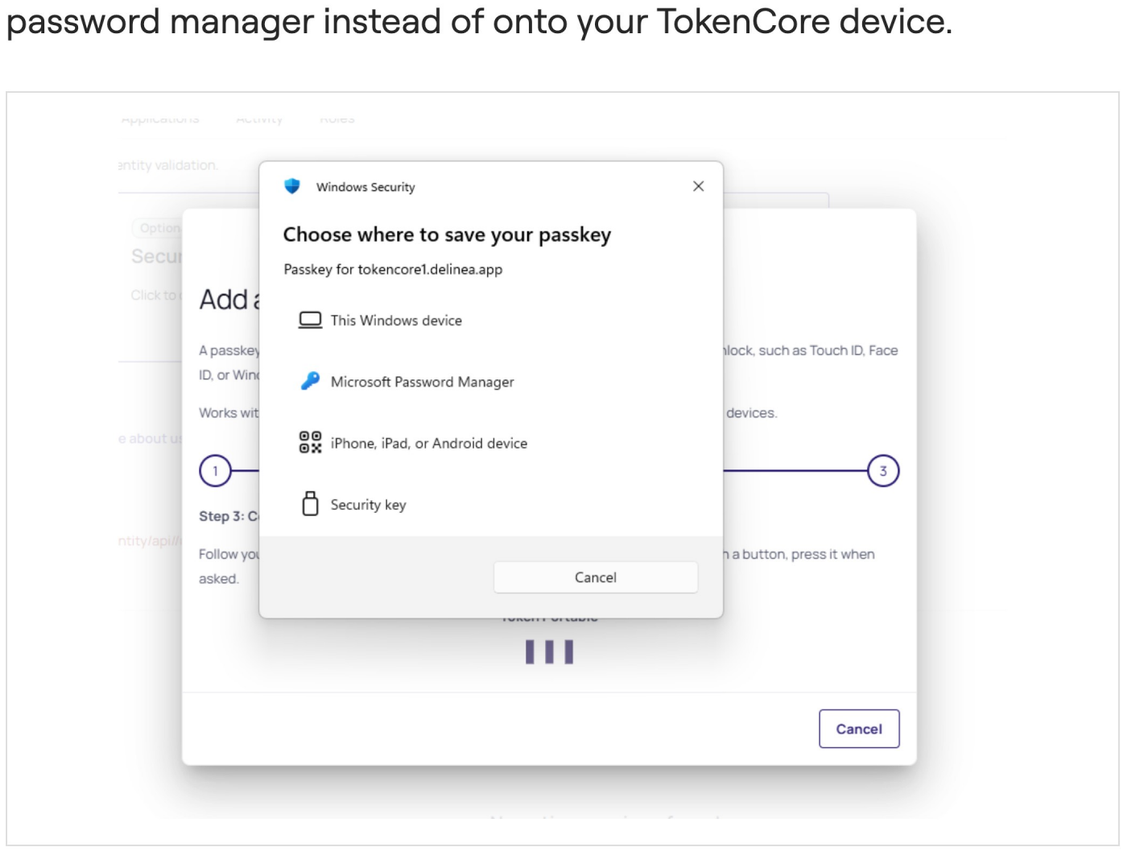


FIGURE 1.4 Windows Security dialog: choose Security key to bind the credential to your TokenCore device.

STEP 5

Complete the Fingerprint Ceremony on the Device

Windows will prompt you to present your TokenCore device — tap it to the reader, hold it in NFC range, or insert it in a USB port, depending on your form factor and workstation. Place your enrolled finger on the device. The device verifies the fingerprint and signs the WebAuthn challenge; the biometric never leaves the device — the signature does. The Delinea Platform confirms success.

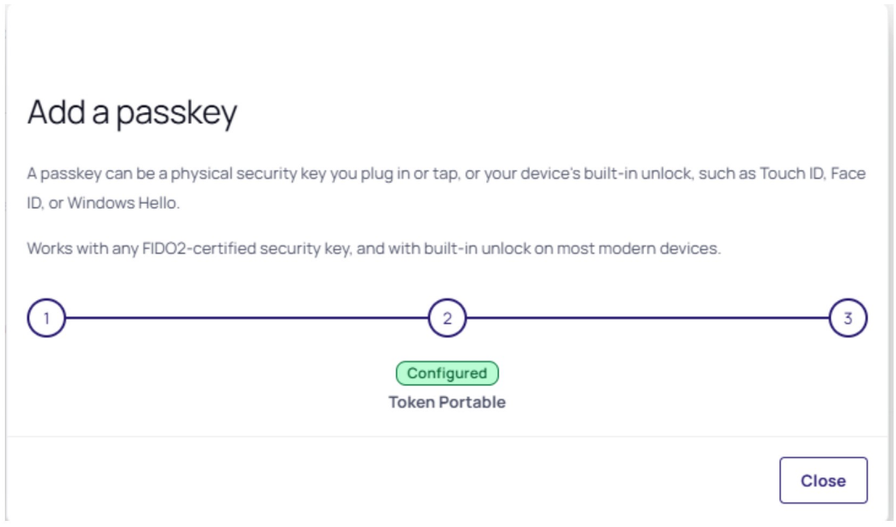


FIGURE 1.5 Step 3 of 3: enrollment complete.

STEP 6 Confirm the Final State in Your Security Tab

Return to your Security tab. The Token Device card now shows **Configured** with “Configured successfully”. You are done — every Platform login going forward will prompt for your TokenCore device.

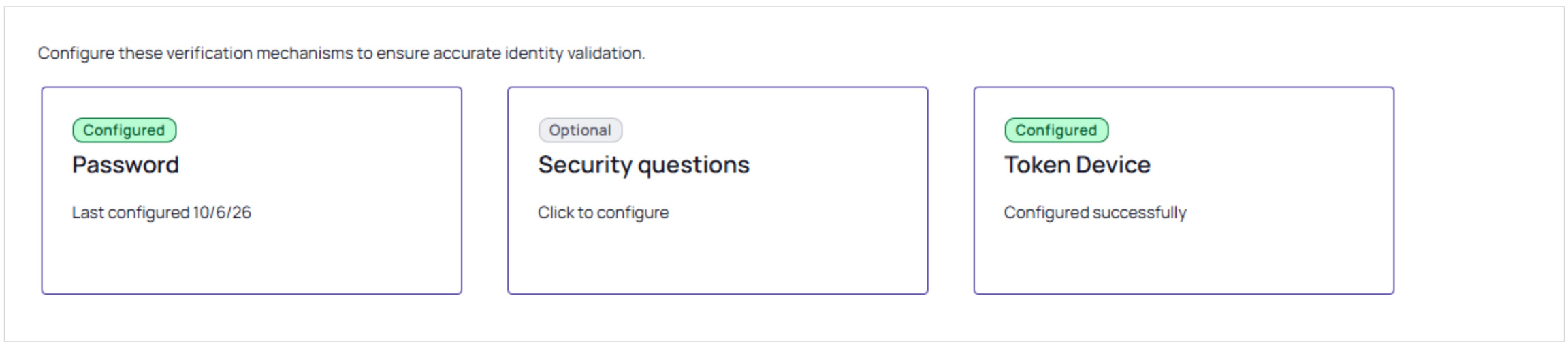


FIGURE 1.6 Final state: Token Device is Configured.

USE CASE 1 / VERIFY

Verification

TEST	EXPECTED RESULT
Test with the device present	Sign out and sign back in. The Platform must prompt for the FIDO2 challenge, and the TokenCore device must complete it with fingerprint + proximity.
Test without the device	Attempt to sign in without your TokenCore device present (or out of BLE range). Authentication must fail.
Review the Platform audit log	The Delinea administrator checks the login event in Platform audit — it should show the FIDO2 challenge completion for your account.

Deployment Checklist

DELINEA PLATFORM ADMINISTRATOR

- [ ] Authentication profile with FIDO2 challenge created
- [ ] FIDO2 enrollment enabled in the identity policy
- [ ] FIDO2 profile set as the default login profile
- [ ] Enrollment profile does not require FIDO2
- [ ] Federated tenants: “federation satisfies all MFA mechanisms” disabled

TOKENCORE ADMINISTRATOR + END USER

- [ ] Devices provisioned and fingerprints enrolled on the device
- [ ] Pilot group of 3–5 PAM admins identified
- [ ] Device registered as “Security key”, not Windows Hello
- [ ] Token Device shows Configured in the Security tab
- [ ] Lost-device recovery procedure confirmed

References

Hardware security keys	docs.delinea.com
Authentication profiles	docs.delinea.com
Authentication policies	docs.delinea.com
Yubico integration (reference)	docs.delinea.com

USE CASE 2 / TOKENCORE + SECRET SERVER ON THE DELINEA PLATFORM

Step-Up MFA for Sensitive Secret Access

DESCRIPTION — FOR DELINEA LISTING

MFA on Secret Access (Platform-exclusive) adds a step-up challenge when a user checks out designated secrets — tier-0 credentials, break-glass accounts, approval workflows. Replacing the default email challenge with FIDO2 means the TokenCore device, and the physically present verified person using it, gates the crown jewels. Enable per-secret, per secret policy, or in bulk; swap the default email step-up profile for a FIDO2 profile and every protected checkout requires biometric + proximity.

Architecture

A secret (or a secret policy covering a folder) carries a **Require Multi-factor Authentication** flag. When a user attempts to view or modify that secret, the Platform issues a step-up FIDO2 challenge using the designated MFA profile. The TokenCore device completes the WebAuthn ceremony and the secret is released. A tunable pass-through window lets administrators balance friction against risk.

01 · SECRET SERVER
Open a Secret
User views or modifies a flagged secret.

→

02 · PLATFORM
FIDO2 Step-Up
Challenge issued from the designated MFA profile.

→

03 · DEVICE
Fingerprint + Proximity
Match runs on the device; BLE confirms presence.

→

04 · DEVICE
Signed Assertion
WebAuthn ceremony completes on the device.

→

05 · PLATFORM
Secret Released
Pass-through window sets when to re-challenge.

Roles and Responsibilities

WHO	DOES WHAT
Delinea Platform administrator	Enables MFA on target secrets (individually, via secret policy, or bulk); sets the step-up MFA profile to one containing FIDO2; tunes the challenge pass-through duration.
Vault owner / secret owner	Identifies tier-0 and break-glass secrets that warrant hardware-biometric step-up; manages the inventory of MFA-protected secrets.
End user	Completes the FIDO2 challenge with the TokenCore device at checkout — the biometric and proximity ceremony that gates the credential.
TokenCore administrator	Provisions devices and supports enrollment (shared with Use Case 1 — a device enrolled for Platform login is already usable for step-up).

USE CASE 2 / CONTINUED

Delinea Platform Administrator — Configuration

01 Enable MFA on Target Secrets

Choose the enablement scope that fits your deployment:

PER-SECRET

`Secret Server > All Secrets` → select secret → **Security** tab → `Multi-factor Authentication > Edit` → **Require Multi-factor Authentication** → Save.

AT SCALE BY POLICY

`Secret Policy` → policy → **Security** tab → **Edit** → set **Require Multi-factor Authentication = Yes** → Save. All secrets in folders under the policy inherit it.

BULK

`All Secrets` → select secrets → **Bulk Actions** → **Change Security Options** → Enable Multi-factor Authentication.

02 Replace the Default Step-Up Profile with a FIDO2 Profile

Navigate to `Settings > Administration (Secret Server) > Security MFA Authentication > Edit`. Select the MFA profile containing the FIDO2 challenge (the same profile family you built in Use Case 1). Save. This swap replaces the default email step-up with a hardware-biometric step-up for every MFA-protected secret.

03 Tune the Challenge Pass-Through Duration

Match the re-challenge window to your risk model.

DEFAULT

30 minutes

Users are not re-challenged for that window within an active session.

TIER-0 / BREAK-GLASS

No pass-through

Forces MFA every time, with up to 5 minutes of caching for operational workflows.

PLANNING NOTES

MFA-enabled secrets are **not available in the Secret Server mobile application**. Exporting secrets prompts MFA if any selected secret has MFA enabled. Secret Server Cloud accesses MFA-protected secrets only when authenticated through the Platform.

USE CASE 2 / END USER

What a Protected Secret Checkout Looks Like

The end-user experience when checking out a secret flagged for MFA step-up. The TokenCore device completes the challenge; the audit log shows which verified individual accessed the credential.

STEP 1 Open the Secret in Secret Server

In Secret Server, navigate to **All secrets** (or any folder containing MFA-protected secrets). Open the target secret — for example, an Active Directory privileged account, a break-glass credential, or a vaulted database password.

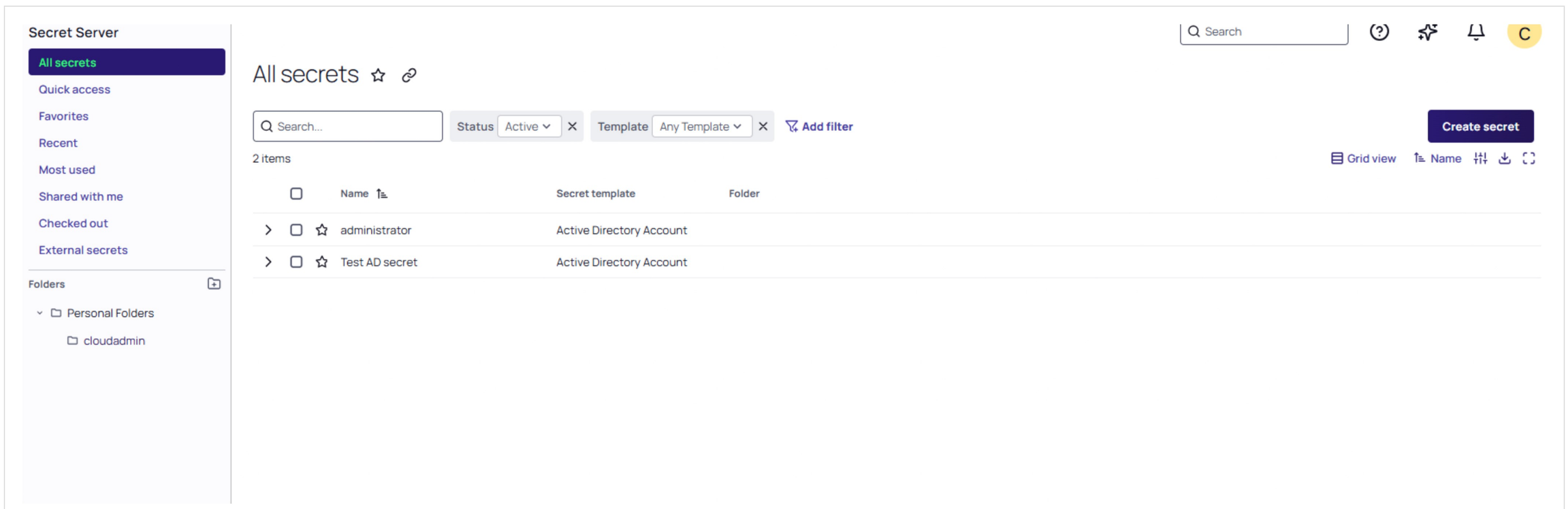


FIGURE 3.1 Secret Server All Secrets list. MFA-protected secrets open to a step-up challenge rather than directly revealing the credential.

STEP 2 Receive the MFA Step-Up Prompt

Instead of revealing the secret, the Platform shows a **Multifactor authentication required** prompt: “You must complete your Multifactor Challenge to view this Secret.” Click **Challenge** to begin the step-up ceremony.

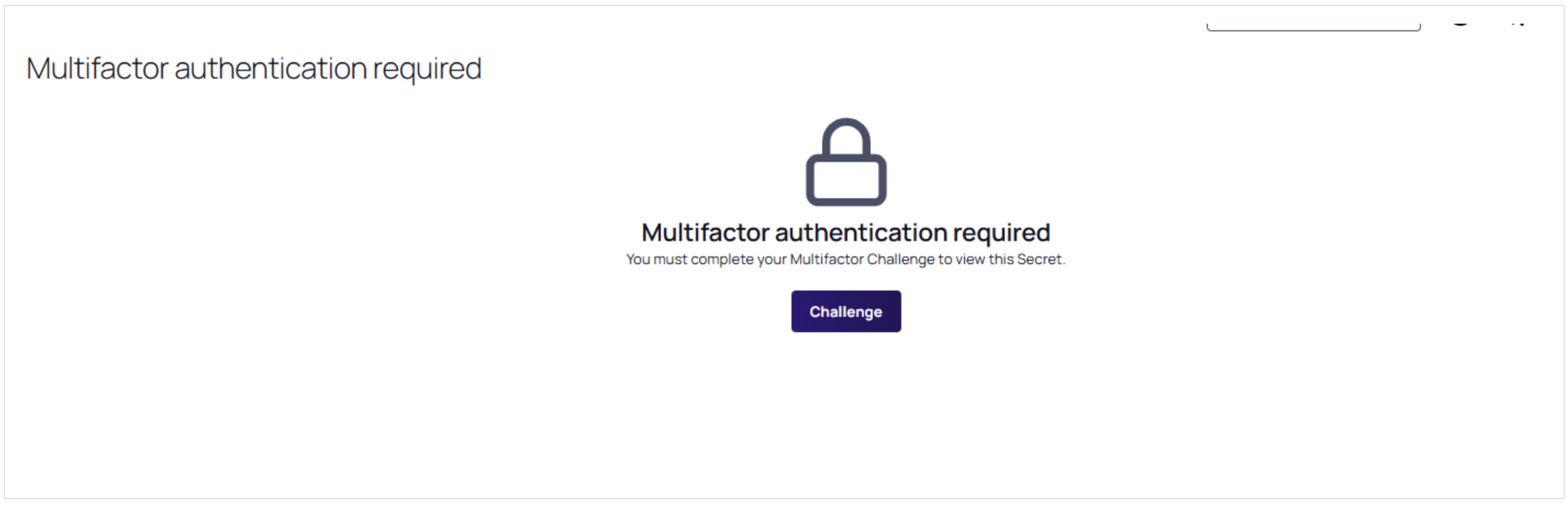


FIGURE 3.2 Multifactor authentication required on secret access. Click Challenge to begin the step-up.

STEP 3

Complete the FIDO2 Challenge on the TokenCore Device

The Platform issues an authentication challenge bound to your identity. The Authentication Challenge dialog confirms the username (for example, `cloudadmin@tokencore1`). Place your enrolled finger on the TokenCore device — the device verifies the fingerprint and confirms BLE proximity before signing the WebAuthn assertion. The Platform verifies the assertion and releases the secret.

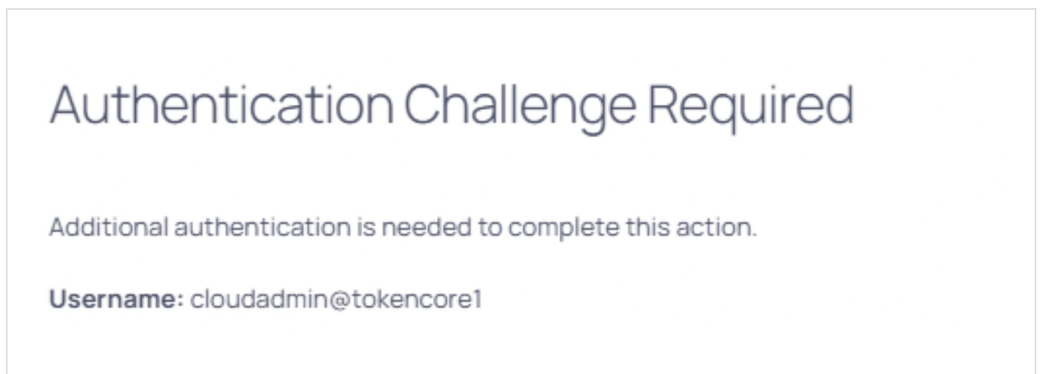


FIGURE 3.3 Authentication Challenge dialog. The TokenCore device completes the FIDO2 ceremony and the secret becomes available.

Verification

TEST	EXPECTED RESULT
Check out a protected secret	The FIDO2 step-up prompt must appear and be satisfiable only with the TokenCore device in BLE proximity.
Modify a protected secret	An MFA challenge must precede the change (not only reads).
Review the audit log	Confirm the audit shows the step-up completion attributed to the individual, not just the account.

References

MFA for secrets — docs.delinea.com

Authentication profiles — docs.delinea.com

USE CASE 3 / TOKENCORE + DELINEA PLATFORM UNIFIED AUDITING

Non-Repudiation for Compliance

DESCRIPTION — FOR DELINEA LISTING

Every flow in Use Cases 1 and 2 lands in the Delinea Platform's unified audit trail. Because the TokenCore authenticator is biometrically bound to one human and requires physical presence, audit evidence upgrades from “this account acted” to “this verified, present person acted” — the answer auditors want for PCI DSS, NIS2, DORA, and cyber-insurance attestations. No additional configuration is required beyond Use Cases 1 and 2; attribution and non-repudiation are intrinsic properties of hardware-bound FIDO2.

Architecture

The Platform's unified audit records every MFA event, secret access event, and session activity. When the authentication factor is a biometrically bound, non-syncable, non-transferable hardware device, each audit entry carries individual attribution by construction. Logs stream to your SIEM through the standard Platform audit pipeline.

SHARED OR PHISHABLE FACTOR	TOKENCORE + DELINEA AUDIT
“This account acted.”	“This verified, present person acted.”

Roles and Responsibilities

WHO	DOES WHAT
Delinea Platform administrator	Ensures MFA is enforced on the flows in Use Cases 1 and 2; configures audit retention and SIEM export per the audit pipeline.
Compliance / GRC team	Maps device-verified MFA events to control requirements (PCI DSS 8.4 / 8.5, NIS2 access-control measures, DORA ICT requirements); defines evidence packages for audit.
Auditor (consumer)	Reviews reports where privileged actions carry individual, biometric-verified attribution — not shared-account traces.
TokenCore administrator	Documents device lifecycle (enrollment, revocation on loss, replacement) for inclusion in the evidence package.

CONFIGURATION — NOTHING NEW TO CONFIGURE

If Use Cases 1 and 2 are in place, the audit record is already produced. The Platform's unified audit records every MFA event, secret access event, and session activity automatically. Point your SIEM at the Platform audit pipeline, and the device-verified attribution comes with it.

USE CASE 3 / CONTINUED

What the Audit Evidence Looks Like

In the Platform's `Insights > Audit logs` view, filter by **Level: Privileged activity** over the relevant window. Each entry carries a service (Secret Server, Identity, Remote Access), a privileged-activity classification, and the action — including the specific secret viewed or modified, the MFA challenge event, and the initiating identity. Clicking an event opens the event-details pane with level, event type, and the initiating user.

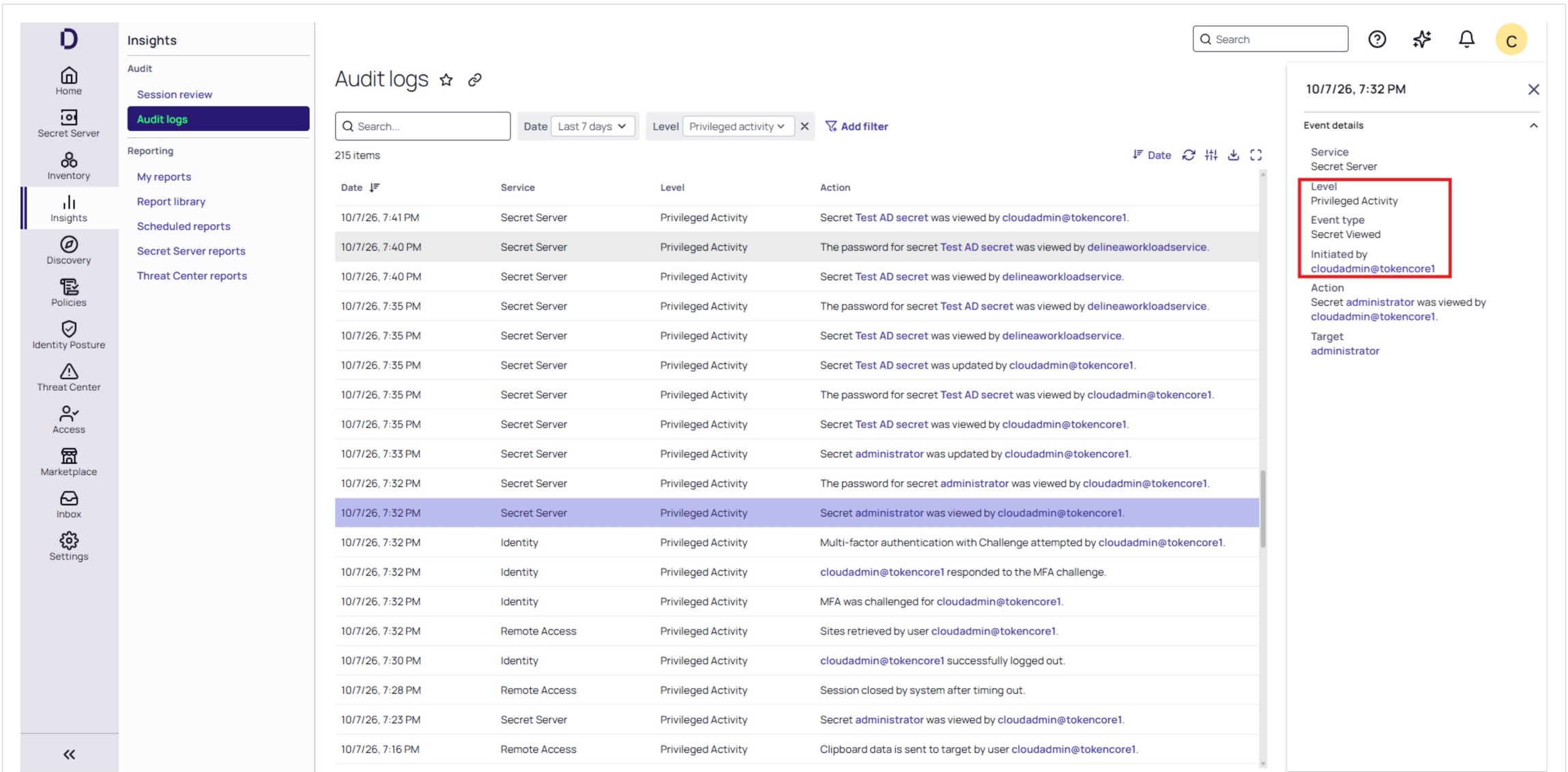


FIGURE 4.1 Platform Insights > Audit logs filtered to Privileged Activity. Secret-viewed events, MFA challenges, and session activity all carry per-user attribution. The side panel surfaces level, event type, and initiating user for forensics.

Verification

TEST	EXPECTED RESULT
Pull an audit report for a pilot user	Confirm login, elevation, and secret-checkout events are attributable to that individual via the device-verified MFA challenge.
Shared-account resolution	Where shared vaulted accounts are in use, confirm audit shows the mapped individual identity who completed the MFA challenge, not the shared account.
End-to-end correlation	Pick one high-value event (for example, a tier-0 secret view). Trace from the authentication challenge through the step-up challenge to the view event — every link should name the same verified user and preserve timestamps.

USE CASE 3 / FOR THE COMPLIANCE EVIDENCE PACKAGE

Control Narrative

Six properties of a TokenCore-authenticated event that compliance and GRC teams can cite when mapping Delinea audit records to control requirements.

01

Factor Strength

Hardware FIDO 2.1 authenticator with an EAL5+ certified secure element. The private key never leaves the device.

02

Biometric Binding

Fingerprint matched on the device. The biometric never leaves the device — the signature does. One device = one enrolled person.

03

Physical Presence

Bluetooth Low Energy confirms the user is within ~3 feet before authentication begins.

04

Phishing Resistance

Origin-bound WebAuthn credentials cannot be relayed through AiTM proxies; there is no code to type on a fake portal.

05

Non-Transferability

Credentials are hardware-bound. They cannot be synced, shared, or delegated. Lost or replaced devices are revocable via the standard Delinea user-authenticator revocation path.

06

Individual Attribution

The Platform audit record names the device-verified individual, including on shared-account access via MFA Redirection where configured.

References

MFA Redirection	docs.delinea.com
Adaptive MFA for PAM (solution brief)	delinea.com

BEFORE MARKETPLACE PUBLICATION

Joint Validation Items

The Delinea configuration in this guide follows official documentation. The TokenCore-side behavior rests on its published FIDO 2.1 / WebAuthn compliance and should be validated jointly before publication to the Delinea Marketplace.

01	Confirm the TokenCore device (all three form factors: Wearable, Portable, Node) completes WebAuthn ceremonies in the browsers used for Platform login and secret step-up.
02	Confirm device enrollment works in the Delinea Platform user profile (Security > FIDO2) and in step-up MFA flows for Secret Server.
03	Validate BLE proximity behavior on managed and unmanaged workstations.
04	Validate audit attribution end-to-end for both direct and MFA-Redirection (shared account) flows.