digicert® x BeyondTrust

DigiCert Trust Lifecycle Manager + BeyondTrust Password Safe

SOLUTION BRIEF

Automated Certificate Management and PKI Resilience

The Challenge:

Shorter Lifecycles, Higher Risk, Changing Standards

Enterprises require the highest level of authentication to protect sensitive resources such as DNS, database servers, and network infrastructure. BeyondTrust Password Safe plays a critical role by discovering, categorizing, and safeguarding privileged account credentials that secure these resources.

These systems also rely on digital certificates to ensure secure communication across internal and external networks. Managing these certificates often involves multiple tools and teams, which can make coordination complex. While Password Safe excels at protecting privileged credentials, certificate management typically falls under separate processes. When handled manually or across disparate systems, this can introduce inefficiencies and potential compliance challenges, highlighting the importance of streamlined, integrated approaches to certificate lifecycle management.

Certificates can expire without visibility, be provisioned inconsistently across physical and virtual devices, or fail to comply with new short-lived validity policies. This exposes critical applications to outages and security incidents—especially as certificate lifetimes shrink to 47 days and cryptographic standards rapidly evolve to support advances such as post-quantum cryptography (PQC).

Organizations need an automated, policy-driven integration that connects Password Safe's advanced secrets management capabilities with DigiCert's enterprise-grade certificate lifecycle management solution, Trust Lifecycle Manager.

The Solution:

Automating PKI with Zero Credential Exposure

The BeyondTrust Connector provides DigiCert Trust Lifecycle Manager secure, API-based access to the credentials stored in Password Safe, enabling it to automate the entire certificate lifecycle—from discovery and issuance to renewal, reissuance, and deployment—while Password Safe maintains secure credentials for the resources under management.

The connector allows administrators to centrally discover, configure, monitor, and automate certificate delivery to privileged devices and services across the enterprise, reducing manual intervention and ensuring compliance with organizational security policies.

Many TLM discovery, delivery, and automation workflows require privileged credentials, but customers are not comfortable storing these secrets locally inside TLM. Integration with Password Safe enables these workflows to run securely by keeping all high-value credentials in a customer-governed vault, ensuring TLM never stores or exposes static passwords.

Get Operational Resilience Through Certificate Automation

- Continuous compliance as certificate validity and cryptographic standards evolve
- Automated certificate deployment for resources that use protected credentials
- Reduced risk through built-in auto-renewal, scheduled updates, and safe rollback options

How It Works

- To securely establish and manage a connection to your Password Safe instance, you must have at least one active DigiCert sensor.
- For high availability, we recommend using multiple sensors. This provides fault tolerance—if one sensor becomes unavailable, the connector automatically switches to another sensor without interruption.
- After the Password Safe connection is established, you can select it when configuring authentication in Trust Lifecycle Manager for supported resources, such as F5 appliances and AWS Certificate Manager (ACM). For more information, see the DigiCert documentation for the BeyondTrust connector and to Deploy and Manage DigiCert Sensors.

Business Value

Together, Trust Lifecycle Manager and Password Safe:

- Eliminate hard-coded or locally stored credentials
- Allow multiple teams to retrieve current secrets just-in-time for certificate management operations
- Prevent certificate-related outages by automatically renewing appliance, web console, and connector certificates—essential with upcoming 47-day TLS lifetimes
- Provision short-lived client certificates for administrators, services, and connectors using policy-driven rotation
- Maintain a unified, auditable certificate inventory across your PAM infrastructure for stronger Zero Trust controls, faster incident response via instant revocation, and improved compliance
- Reduce downtime by eliminating service disruptions due to misconfigured or expired certificates
- Lower administrative overhead through automated renewals and deployment
- Centralize visibility into certificate usage across environments
- Improve security posture with trusted, compliant certificates with increased cryptographic agility

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.