# DigiCert Trust Lifecycle Manager with Delinea Secret Server and the Delinea Platform

## Automated Certificate Management and PKI Resilience

DigiCert® Trust Lifecycle Manager retrieves secrets from Delinea Secret Server and the Delinea Platform to authenticate supported integrations across the certificate management environment.

### The challenge of securing access as certificate operations scale

Enterprises depend on privileged credentials to administer servers, network appliances, and cloud services, many of which belong to non-human identities such as service accounts and API keys. The challenge is that most organizations often don't understand why a non-human identity took a privileged action.

Delinea Secret Server and the Delinea Platform secure both human and machine identities through centralized authorization. Non-human identities are vaulted, automatically rotated, and audited, so secrets are not left sitting in scripts, pipelines, or tool configurations. Those servers, network appliances, and cloud services also depend on digital certificates to establish trusted connections.

Certificate discovery, renewal, and deployment introduce another set of operational responsibilities. Manual handoffs between certificate administrators and privileged access teams increase effort and create opportunities for error. An expired certificate can interrupt an otherwise healthy service, while inconsistent processes make certificate policies harder to enforce.



Organizations need certificate automation that works with their established secrets management practices. Connecting these capabilities helps teams scale operations while maintaining control over privileged access.

## The solution for certificate automation with governed credentials

Trust Lifecycle Manager brings certificate discovery, inventory, policy, and automation into a unified management environment. Its Delinea connector supports standalone Secret Server and the Delinea Platform, allowing teams to use vaulted credentials for other Trust Lifecycle Manager integrations.

Delinea vaults, rotates, and audits the credentials those integrations rely on, while Trust Lifecycle Manager orchestrates certificate operations on supported systems. That covers two kinds of non-human identity: the certificates machines use to establish trust, and the service accounts and credentials used to deploy them. This combination helps security and infrastructure teams coordinate their responsibilities and extend automation across their existing environment.

## Operational resilience through certificate automation



### Reduce certificate outage risk

Use discovery, monitoring, and automated renewals to address expiration and configuration issues before they disrupt services.



### Strengthen certificate governance

Centralize inventory and policies to improve visibility across certificate authorities and infrastructure.



### Lower administrative effort

Automate certificate requests, installation, and renewal on supported targets, reducing repetitive work and manual errors.

## Business value

Together, Trust Lifecycle Manager and Delinea help organizations:



### Protect privileged credentials

Apply secure vault access controls and password management practices to the service accounts and other non-human identities that operations rely on, including certificate automation.



### Improve service continuity

Reduce exposure to certificate expiration through repeatable renewal and deployment workflows.



### Rotate without breaking automation

Credentials rotated in Delinea apply automatically wherever Trust Lifecycle Manager references them, so certificate workflows keep running.



### Support compliance efforts

Combine certificate visibility and policy management with Delinea's privileged account controls and audit trails, so access to the credentials behind certificate operations can be audited and verified.



### Scale with less manual work

Allow certificate teams to expand automation while privileged access teams govern the credentials needed to administer resources.

## How it works

Enable the secrets manager feature and deploy an active DigiCert sensor with HTTPS access to Delinea on port 443. Multiple sensors provide automatic failover.

### Connect your deployment

For standalone Secret Server, use a dedicated application account with minimum secret permissions and OAuth2 API access. For the Delinea Platform, configure a Platform service user, Client ID, client secret, vault access, and a dedicated Secret Server service account within the vault.

### Configure authentication

Add the Delinea connector, choose its business unit and managing sensors, and supply the deployment URL and authentication details. Select it for other connectors and reference secrets using Secret ID or SecretID/FieldSlug; the default field is password.

### Maintain current access

Credential updates in Delinea automatically apply wherever referenced in Trust Lifecycle Manager. Connectivity or authentication failures flag affected connectors as Action Needed and associated automation flows as Failed, with error details.

### Learn more

For configuration requirements and deployment details, see the DigiCert-Delinea connector documentation.



## 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.

## About Delinea

Delinea is the identity security platform that continuously controls what AI agents, humans, and machines can do, and for how long. It extends privileged access management from the point of access to the moment of action, using just-in-time authorization to reduce standing privilege across on-premises, multi-cloud, and short-lived infrastructure. The platform provides visibility across every identity type, understands the risk each one carries, and preserves context to make access decisions auditable and defensible. Over 9,000 organizations, including two-thirds of the Fortune 100, rely on Delinea. Learn more at www.delinea.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.