



Enterprise trust store management

Manage trust—not just certificates.

Most organizations manage certificates—but not the trust stores that validate them.

DigiCert Trust Lifecycle Manager extends certificate lifecycle management across the full chain of trust.

DigiCert Trust Lifecycle Manager: Enterprise trust store management

Problem statement

Private root and intermediate CAs are not distributed automatically like public trust anchors. When trust stores are unmanaged or inconsistent, certificate validation can fail across servers, applications, containers, cloud workloads, network devices, and endpoints.

As certificate lifecycles shrink and organizations adopt Zero Trust and prepare for post-quantum cryptography (PQC), trust store drift increases the risk of outages, broken mTLS, risky CA rotations, and inconsistent security policy.

Managing certificates alone is no longer enough. Organizations must manage what is trusted, where it is trusted, and how that trust is maintained.

Solution overview

DigiCert Trust Lifecycle Manager extends certificate lifecycle management beyond issued certificates to discover, distribute, govern, and continuously monitor enterprise trust stores.

The solution helps organizations maintain a consistent chain of trust across hybrid, cloud, and on-premises environments while reducing manual work and unnecessary trust exposure.

This enables:

- Centralized visibility into roots, intermediates, and trust stores
- Automated trust bundle distribution and CA rotation
- Policy-driven allowlists, blocklists, and drift remediation
- A stronger foundation for crypto-agility and PQC migration

How it works



Discover

Inventory root and intermediate CAs, trust stores, locations, expiration status, and metadata.



Govern

Define approved roots, trust bundles, assignments, and cryptographic policies.



Distribute

Provision trust bundles through DigiCert agents, sensors, and native connectors.



Monitor

Track trust store health, synchronization, expiration, and policy compliance.



Remediate

Detect and correct drift to restore the approved chain of trust.

Trust management maturity

**Discover & govern**
Create a centralized inventory of enterprise trust anchors and stores.

**Automate distribution**
Synchronize approved roots and intermediates across environments.

**Fully managed trust**
Apply trust policy, reduce attack surface, and remediate drift.

Supported stores and formats

Additional enterprise stores

Microsoft CAPI

IBM DataPower

IBM GSKit

F5 BIG-IP

PKCS#12

PEM

JKS

Value

Key feature	Description	Business value
Root & intermediate discovery	Discovers enterprise trust anchors across environments.	Eliminates blind spots and unmanaged CAs.
Trust store inventory	Identifies trust stores across servers, applications, containers, and appliances.	Provides a unified view of enterprise trust.
Automated distribution	Deploys approved trust bundles using agents and connectors.	Removes manual updates and supports safe CA rotation.
Trust bundle management	Creates reusable bundles for approved roots and intermediates.	Simplifies governance and cross-platform consistency.
Trust store governance	Applies allowlists, blocklists, assignments, and policy.	Reduces attack surfaces and improves compliance.
Drift detection	Monitors trust stores and remediates unauthorized change.	Maintains a consistent chain of trust.
PQC readiness	Inventories trust anchors and cryptographic algorithms.	Accelerates crypto-agility and future migration.

Why DigiCert

Certificate lifecycle management does not end when a certificate is issued—it ends when every system can validate it against the correct chain of trust. DigiCert Trust Lifecycle Manager extends visibility, automation, and policy across the complete trust ecosystem, from root and intermediate governance through trust store distribution and validation.

As machine identities multiply and organizations prepare for shorter certificate lifecycles and post-quantum cryptography, DigiCert helps enterprises manage trust consistently across every environment, creating a resilient, crypto-agile foundation for digital trust.