



# Automated Certificate Management and App Security Integration



SOLUTION BRIEF

# DigiCert and F5: Automated, Policy-Driven Integration

## Problem statement

Modern application environments rely on F5 platforms to deliver and secure digital experiences across on-premises, hybrid, and multi-cloud infrastructures. Yet managing TLS/SSL certificates manually within these complex ecosystems creates risk, delay, and compliance gaps.

Certificates can expire without visibility, be provisioned inconsistently across virtual servers, 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.

Organizations need an automated, policy-driven integration that connects F5's advanced application delivery and security capabilities with DigiCert's enterprise-grade digital trust platform.

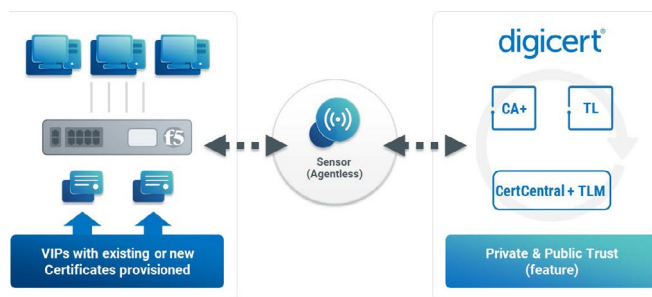
## Product integration

The DigiCert Trust Lifecycle Manager and F5 Application Delivery and Security Platform integration deliver complete automation for the certificate lifecycle—from discovery and issuance to renewal, re-issuance, and deployment—directly on elements F5 application delivery and security platform like BIG-IP load balancers.

Through Trust Lifecycle Manager's native F5 connector, administrators can centrally configure, monitor, and automate certificates across multiple BIG-IP instances, reducing manual intervention and ensuring adherence to organizational security policies.

This automation enables:

- Continuous compliance with evolving validity and cryptographic requirements
- Seamless deployment of new or renewed certificates to BIG-IP SSL profiles
- Built-in support for auto-renewal, scheduled updates, and rollback safety

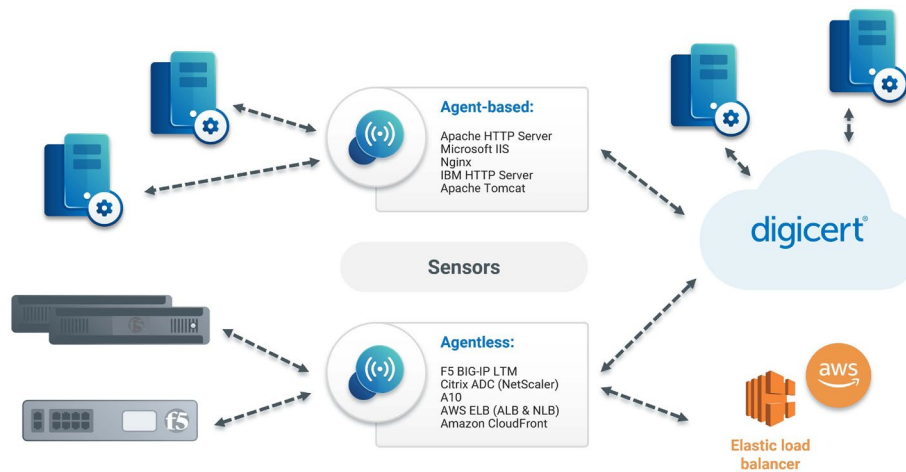


## How it works

Trust Lifecycle Manager discovers all certificates across connected F5 devices and maps them to their respective virtual servers. Centralized policies govern key strength, algorithms, and validity, ensuring every certificate meets compliance standards.

- Connector Setup: Administrators configure an F5 connector in Trust Lifecycle Manager using secure Sensor communication
- Certificate Discovery: Trust Lifecycle Manager scans F5 devices to identify and map certificates to Virtual Servers (VIPs)
- Policy Governance: Enforces centralized policies for validity, key strength, and algorithm compliance.
- Automation Execution: Automatically reissues and deploys expiring certificates to F5 TLS/SSL profiles
- Verification & Rollback: Activates new certificates seamlessly while retaining old ones for fallback
- Visibility & Audit: Logs every certificate event in Trust Lifecycle Manager for traceability and compliance





## Value

Key Feature	Description	Data Points
Automated Certificate Management	End-to-end automation of issuance, deployment, and renewal on F5 load balancers.	Eliminates manual errors, outages, and ticket backlog.
Centralized Visibility & Governance	Unified view of all F5 certificates, VIPs, and profiles from Trust Lifecycle Manager's dashboard.	Simplifies oversight and enforces policy consistency.
Scalable Deployment	Supports global, multi-tenant F5 deployments across data centers and clouds.	Provides consistent governance for large-scale operations.
Enhanced Auditing & Reporting	Logs every certificate action with full metadata for audit trails.	Accelerates compliance with PCIDSS, ISO 27001, NIST 800-57.
Connector-Based Integration	Secure F5 connector communicates via DigiCert Sensor; supports multiple appliances.	Streamlines integration without altering F5 configurations.

## 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](https://www.digicert.com).

© 2025 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.

