Cloudflare and DigiCert Security Integration

Automated TLS/SSL certificate lifecycle management for Cloudflare WAF

Executive summary

Modern web applications depend on continuous availability, strong encryption, and secure traffic inspection to protect customer interactions and business-critical services. Cloudflare Web Application Firewall (WAF) provides advanced application security, DDoS protection, TLS/SSL termination, and edge delivery capabilities for internet-facing applications. Because these services rely on TLS/SSL certificates, maintaining valid and trusted certificates is essential to uninterrupted application delivery and security.

DigiCert and Cloudflare deliver an integrated solution that automates TLS/SSL certificate lifecycle management for Cloudflare WAF environments. By combining DigiCert Trust Lifecycle Manager with Cloudflare's Custom Certificate APIs, organizations can eliminate manual certificate deployment processes, reduce operational risk, prevent outages caused by expired certificates, and maintain continuous compliance across distributed application environments.

The challenge

TLS/SSL certificates are foundational to Cloudflare WAF operations, enabling encrypted communication, authentication, and secure application delivery. These certificates are critical for protecting customer-facing applications and maintaining digital trust.

Managing certificates across Cloudflare environments introduces operational and security challenges including limited visibility into deployed certificates, missed renewals, manual deployment processes, scaling complexity, and compliance gaps.

DigiCert and Cloudflare integrated solution

DigiCert Trust Lifecycle Manager integrates with Cloudflare WAF to provide automated, centralized TLS/SSL certificate lifecycle management. The integration automates certificate issuance, deployment, renewal, and governance using Trust Lifecycle Manager automation workflows, ACME-based certificate issuance, and Cloudflare REST APIs.

This integration enables organizations to maintain valid and trusted certificates without manual intervention while reducing operational complexity and improving security posture.

Integration components

Product	Solution
DigiCert Trust Lifecycle Manager	Enterprise platform for managing, automating, and governing machine identities and TLS/SSL certificates
Trust Lifecycle Manager Agent	Automation component that executes certificate lifecycle workflows and integrates with Cloudflare APIs
DigiCert ACME Services	Automated certificate issuance and renewal services supporting secure certificate provisioning workflows
Cloudflare WAF	Cloud-native web application firewall and edge security platform
Cloudflare Custom Certificate API	REST API used to securely upload and manage externally issued certificates within Cloudflare zones

How the integration works

The integration uses secure API-based communication and automated workflows to eliminate manual certificate handling.

Key capabilities include:

- Automated certificate enrollment
- Secure certificate deployment
- Automated renewal and redeployment
- Centralized visibility
- Policy enforcement
- Audit and compliance reporting
- Flexible deployment workflows

The integration supports both Certbot post-hook automation workflows and DigiCert Trust Lifecycle Manager Admin Web Request scripting workflows.

Integration workflow

1. Trust Lifecycle Manager requests a certificate using ACME services
2. Certificate and private key are stored securely on the Trust Lifecycle Manager Agent host
3. A post-enrollment or post-renewal automation script is triggered
4. The automation script authenticates to Cloudflare using API credentials
5. The certificate and private key are uploaded to Cloudflare using the Custom Certificate API
6. Cloudflare activates the updated certificate for the configured zone
7. Future renewals repeat automatically without manual intervention

Security considerations

Security features include HTTPS encryption for API communication, scoped Cloudflare API Tokens, masking of sensitive credentials in logs, and secure private key handling. The integration also supports centralized governance and policy enforcement through Trust Lifecycle Manager.

Key benefits

- Eliminate outages caused by expired certificates
- Automate certificate issuance, deployment, and renewal workflows
- Reduce operational overhead
- Improve visibility into deployed certificates
- Strengthen security posture
- Maintain compliance with audit-ready reporting
- Scale certificate management across distributed environments

Joint use cases

Continuous application availability

Automatically renew and deploy TLS/SSL certificates to ensure uninterrupted application delivery.

Secure edge application delivery

Enable automated certificate management for applications protected by Cloudflare WAF.

Scalable multi-zone certificate management

Centralize lifecycle management for certificates deployed across multiple Cloudflare zones.

Technical overview

APIs Used:

/client/v4/zones/{ZONE_ID}/custom_certificates

Authentication Requirements:

- Cloudflare Zone ID
- Cloudflare API Token with Custom Certificate permissions

Supported Platforms:

- DigiCert Trust Lifecycle Manager
- DigiCert Trust Lifecycle Manager Agent v3.x+
- Linux-based automation hosts
- Cloudflare WAF and Custom Certificate services

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, and AI content, agents, and models. Learn why more than 125,000 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 Cloudflare

Cloudflare, Inc. (NYSE: NET) is the leading connectivity cloud company on a mission to help build a better Internet. It empowers organizations to make their employees, applications and networks faster and more secure everywhere, while reducing complexity and cost. Cloudflare's connectivity cloud delivers the most full-featured, unified platform of cloud-native products and developer tools, so any organization can gain the control they need to work, develop, and accelerate their business.

Powered by one of the world's largest and most interconnected networks, Cloudflare blocks billions of threats online for its customers every day. It is trusted by millions of organizations – from the largest brands to entrepreneurs and small businesses to nonprofits, humanitarian groups, and governments.