

Imperva Web Application Firewall and DigiCert Trust Lifecycle Manager security solution

Automated TLS/SSL certificate lifecycle management for Imperva WAF

Executive summary

Imperva Web Application Firewall (WAF) protects internet-facing applications while relying on trusted TLS/SSL certificates for secure communications. DigiCert Trust Lifecycle Manager integrates with Imperva WAF to automate certificate issuance, deployment, renewal, and governance, eliminating manual certificate updates and reducing the risk of outages caused by expired certificates.

The challenge

Organizations often manage hundreds of certificates protecting Imperva WAF sites. Manual renewal and deployment introduce operational overhead, increase the risk of expired certificates, and make compliance reporting difficult.

DigiCert and Imperva integrated solution

DigiCert Trust Lifecycle Manager integrates with Imperva WAF using an Admin Web Request (AWR) workflow and Imperva's Custom Certificate API. After certificate enrollment or renewal, Trust Lifecycle Manager executes an automation script that securely uploads the certificate chain and private key to the target Imperva site using authenticated REST API calls.

Solution components

- DigiCert Trust Lifecycle Manager
- DigiCert Trust Lifecycle Manager Agent
- DigiCert ACME Services
- Imperva Web Application Firewall
- Imperva Certificate Management API
- Admin Web Request (AWR) automation workflow

How the integration works

1. TLM requests or renews a certificate.
2. The certificate and private key are securely stored on the TLM Agent.
3. A post-enrollment/post-renewal AWR script is triggered.
4. The script extracts the Site ID, API ID, and API Key supplied as workflow arguments.
5. The certificate chain and private key are encoded in Base64, and the key type (RSA/ECC) is detected automatically.
6. The script authenticates to the Imperva REST API and uploads the certificate bundle.
7. Imperva activates the updated certificate for the protected site.
8. Future renewals repeat automatically with no manual intervention.

Security considerations

API communication is secured using HTTPS and authenticated API credentials, with sensitive values masked in logs. Private keys remain under customer control until securely transmitted to Imperva, and the workflow supports both RSA and ECC certificates while uploading complete certificate chains. Key benefits

- Eliminate outages caused by expired certificates
- Automate issuance, deployment, and renewal
- Centralize certificate governance and visibility
- Reduce operational effort and manual errors
- Support compliance with audit-ready lifecycle reporting
- Scale certificate management across multiple Imperva-protected applications

Joint use cases

- Continuous certificate renewal for internet-facing applications
- Centralized certificate governance for Imperva deployments
- Rapid deployment of newly issued certificates across multiple protected sites

API technical overview

- `PUT /api/prov/v2/sites/{SITE_ID}/customCertificate`

Authentication:

- Imperva Site ID
- Imperva API ID
- Imperva API Key

Supported Platforms:

- DigiCert Trust Lifecycle Manager
- DigiCert Trust Lifecycle Manager Agent v3.x+
- Linux automation hosts
- Imperva WAF

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.

© 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.