digicert® x net>scaler™

Seamless Certificate Automation at Scale with NetScaler and DigiCert

Seamless Certificate Automation at Scale with NetScaler and DigiCert

Problem statement

The TLS/SSL certificate ecosystem is undergoing a major shift. To improve internet security and reduce the window of exposure if a certificate is misissued or a key is compromised, certificate lifetimes are being shortened across the industry, reduced from 398 days to 47 days. At the same time, significant changes to the cryptographic protocols used in TLS/SSL will be implemented and mandated in the late 2020s. These changes are being driven by browser vendors, certificate authorities, and industry bodies like the CA/Browser Forum, reflecting a push toward stronger cryptographic agility and faster adoption of new standards.

This creates three key challenges for enterprises:

- Frequent renewals increase administrative burden

- Manual processes are time-consuming and error-prone (CSR generation, certificate uploads, binding to vServers)

- Missed expirations are a leading cause of outages, leading to customer-facing downtime and reputational damage

> Organizations have, on average, 256,000 certificates. 53% of those organizations have insufficient PKI staff. — Gartner

The Solution

Part 1: Zero-touch certificate management: Automated Deployment of Certificates

NetScaler has introduced Zero-Touch Certificate Management (ZTCM) to address these challenges.

- Automatic lifecycle handling: Once certificates and keys are uploaded to the Console's repository, onboarded NetScaler appliances fetch, validate, and deploy the correct certificates automatically.

- Hands-free renewals: No binding required. Certificates are continuously fetched and updated across all NetScaler deployments.

- Seamless experience: The correct certificate is served dynamically at handshake based on SNI, removing the need for admins to configure bindings manually.

Result: Administrators save time, eliminate repetitive errors, and ensure continuous availability of secure services.

Part 2: Automated certificate renewal powered by DigiCert and ACME

With DigiCert's leadership in digital trust, customers gain not only automation but confidence that their certificates meet worldwide compliance and security standards.

NetScaler Zero-Touch Certificate Management (ZTCM) integrates the ACME protocol for full end-to-end automation, solving the renewal problem.

- Standards-based automation: Through direct integration with DigiCert, NetScaler ZTCM extends into full end-to-end automation, from issuance through renewal.

- Automated domain validation: Console (via acme.sh) supports DNS-01, automatically validating domain control through supported DNS providers.

ZTCM ACME support ensures enterprises with hundreds or thousands of SSL-enabled vServers stay secure with minimal overhead.

Automated Certificate Renewal Powered by DigiCert® Trust Lifecycle Manager

DigiCert Trust Lifecycle Manager is the heart of a modern, scalable PKI. It detects and catalogs TLS/SSL certificates anywhere on the network and automates their management and policy enforcement. This solves the renewal problem and many others that enterprises face.

DigiCert Trust Lifecycle Manager can manage certificates through open standards, such as ACME (Automated Certificate Management Environment), which NetScaler products support, and proprietary interfaces required by many others. Once automation is configured, administrators can set it to satisfy the frequent renewal requirements coming.

Business Value

From an executive standpoint, ACME + Zero-Touch in NetScaler Console provides:

- Risk Reduction: Automated renewals prevent costly outages and compliance gaps caused by expired certificates.

- Operational Efficiency: Significantly reduces manual effort and human error in certificate lifecycle management.

- Agility at Scale: Supports rapid certificate turnover required by industry changes (47-day validity and beyond).

- Governance & Compliance: Centralized dashboard, monitoring, and auditability align with enterprise security mandates.

- Strategic Advantage: By automating foundational security processes, IT teams can focus on innovation and delivering business outcomes.

Use Case	Description	Benefits
Enterprise Web Applications	Prevent downtime and expired-certificate incidents for public websites and APIs	Avoid costly outages and reputational damage
Hybrid & Multi-Cloud Deployments	Centrally manage certificates across AWS, Azure, and on-premises appliances	Consolidate management for savings and efficiency
High-Scale Deployments	Large enterprises with thousands of TLS/SSL VIPs gain the most value through automation	Make maintenance of important infrastructure reliable and low-cost
VDI & Secure Access	Support for virtual desktop needs, such as authentication, enumeration, and session initiation	Automation of a high-volume and difficult admin task
DigiCert-First Automation	Enterprises standardizing on DigiCert as their public certificate authority can now automate issuance, deployment, and renewal in one integrated flow — no manual intervention required	Use one console to manage all public and private certificates enterprise-wide
Compliance Without Complexity	Organizations with stringent compliance needs can pair DigiCert's advanced validation and reporting with NetScaler's centralized dashboard for audit-ready operations	Audit-readiness through consistent application of company and regulatory policy across your PKI

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.