Security Hardening

Productie-minimum voor HTTPS, sessies, 2FA en vault

Product	CertiForge (SaaS, OnPrem en Dedicated)
Document	Versie 1.1 · 21 september 2026 · Nederlands
Doelgroep	Security- en systeembeheerder
Uitgever	AppForge.NL · https://www.appforge.nl · hello@appforge.nl

> **Leeswijzer.** Dit is het productie-minimum. CertiForge vervangt IIS-TLS-bindingen nooit automatisch. Private keys horen in de vault, niet in tickets of chat.

1. Verplichte instellingen

```
APP_ENV=production
APP_DEBUG=false
APP_URL=https://certiforge.jouwdomein.internal
SESSION_ENCRYPT=true
SESSION_SECURE_COOKIE=true
SESSION_LIFETIME=30
CERTIFORGE_FORCE_HTTPS=true
CERTIFORGE_PRIVILEGED_REQUIRE_2FA=true
CERTIFORGE_REQUIRE_REAUTH=true
CERTIFORGE_PKI_ALLOW_MOCK=false
CERTIFORGE_REGISTRATION=false
```

- `VAULT_KEY` is niet gelijk aan `APP_KEY`
- Install-token minimaal 16 tekens; daarna installer-API blokkeren
- HSTS aan

2. Wat de applicatie al afdwingt

- Tenant-isolatie
- CSRF op webformulieren
- SSRF-guards op scanner en discovery
- Parameterized queries
- Geen shell-from-server
- Agent HMAC + nonce / replay-bescherming
- Rate limits

- Audit zonder secrets
- Encrypted vault

3. Accounts

- 2FA voor bevoorrechte rollen
- Korte sessie en herauthenticatie bij uitrol, restore en revoke
- Vier-ogen voor productie-uitrol
- Break-glass lokaal houden, niet hetzelfde wachtwoord hergebruiken

4. Netwerk

- Agent: alleen outbound 443, geen inbound Agent-poort
- Licentieserver: uitgaande HTTPS naar `license.appforge.nl` (on-premises/dedicated)
- Interne hostnamen (.local / .internal) zijn toegestaan voor de app zelf

> Zet `APP_DEBUG=true` nooit aan in productie. Dat kan stack traces en paden lekken.

AppForge.NL · hello@appforge.nl · https://www.appforge.nl

Document: CertiForge Security Hardening · versie 1.1 · 21 september 2026 · geen secrets in dit document.