DigiCert PKI Platform 8 End of Life (EOL) on March 31, 2027 – Frequently Asked Questions

BACKGROUND

Why will DigiCert End of Life PKI Platform 8 on March 31, 2027?

As a current PKI Platform 8 customer, you were previously upgraded to Trust Lifecycle Manager in DigiCert ONE, our enterprise-grade, fully modernized digital security solution offering comprehensive automation, scalability, security, and flexibility. Go-forward issuance and certificate lifecycle management will be in Trust Lifecycle Manager, so we have made the decision to refocus resources and innovation on this exciting new offering.

How does moving to Trust Lifecycle Manager and DigiCert ONE benefit my organization?

In addition to Trust Lifecycle Manager's robust, fully automated, CA-agnostic certificate management and PKI services, the full DigiCert ONE platform contains myriad benefits currently unavailable on PKI Platform 8, including:

- Secure software and policy governance capabilities
- Tailored DNS solutions
- End-to-end device security
- Support for a wide array of third-party integrations, including automation protocols, certificate authorities, DNS providers, and authentication systems

What does "End of Life" mean for PKI Platform 8, technically speaking?

- On March 31, 2027, we will end support of the platform, including updates, maintenance, and patches.
- All PKI Platform 8 customer accounts will be deactivated.
- Your users will no longer have access to the PKI Platform 8 platform by either UI or API.

SEAMLESS TRANSITION AND ACCESS TO CERTIFICATES

How can my organization ensure our current valid certificates in PKI Platform 8 are mapped to Trust Lifecycle Manager with seamless access and management after March 31, 2027?

Your team has a couple of options:

1. You can issue new certificates in Trust Lifecycle Manager, with full feature parity, using the Trust Lifecycle Manager console and automation solution, or via API.
    - Once your new certificates are issued in Trust Lifecycle Manager, you can optionally revoke the original certificates in PKI Platform 8 via console or API.
    - If you have a large number of certificates, your assigned DigiCert support expert can revoke them in PKI Platform 8 on your behalf.
2. You can import your PKI Platform 8 certificates to Trust Lifecycle Manager using the PKI Platform 8 connector. *This option allows you to continue managing your current PKI Platform 8 certificates from your Trust Lifecycle Manager account, including revocations, suspension of privately trusted certificates, and recovery of escrowed certificates.*

What about our public S/MIME certificates that are still valid in PKI Platform 8 after March 31, 2027?

- If they are escrowed, you can bring them to Trust Lifecycle Manager using the PKI Platform 8 connector.
- If they are not escrowed, there is no need to manage them in Trust Lifecycle Manager—you can let them expire in PKI Platform 8 and issue new public S/MIME certificates from Trust Lifecycle Manager (via your validated CertCentral account).

What happens if we don't revoke our current certificates in PKI Platform 8 after issuing them in, or importing them to, Trust Lifecycle Manager?

Nothing. You can keep the certificates in both accounts if you wish.

ADMINISTRATION FEATURES FOR EXISTING CERTIFICATES

How will revocation and validation services work during and after PKI Platform 8 end of life?

- Validation (OCSP and CRL) services are hosted in DigiCert ONE and available with your Trust Lifecycle Manager account for any certificates issued there. They will also continue to work for your existing PKI Platform 8 certificates during and after the platform's end of life, regardless of whether you import them to Trust Lifecycle Manager.
- Revocation services for your *existing certificates in PKI Platform 8* are available only by using the PKI Platform 8 connector and importing your valid certificates to Trust Lifecycle Manager.

How will automated renewals work for certificates that remain valid after PKI Platform 8 end of life?

- For web-based flows, you can configure the renewal email template in PKI Platform 8 to point to a Trust Lifecycle Manager URL as the destination to enroll for a new certificate.
- For API integrations, whether from third-parties or yourself, you will need to issue a new certificate from Trust Lifecycle Manager.