ManageEngine
Key Manager Plus

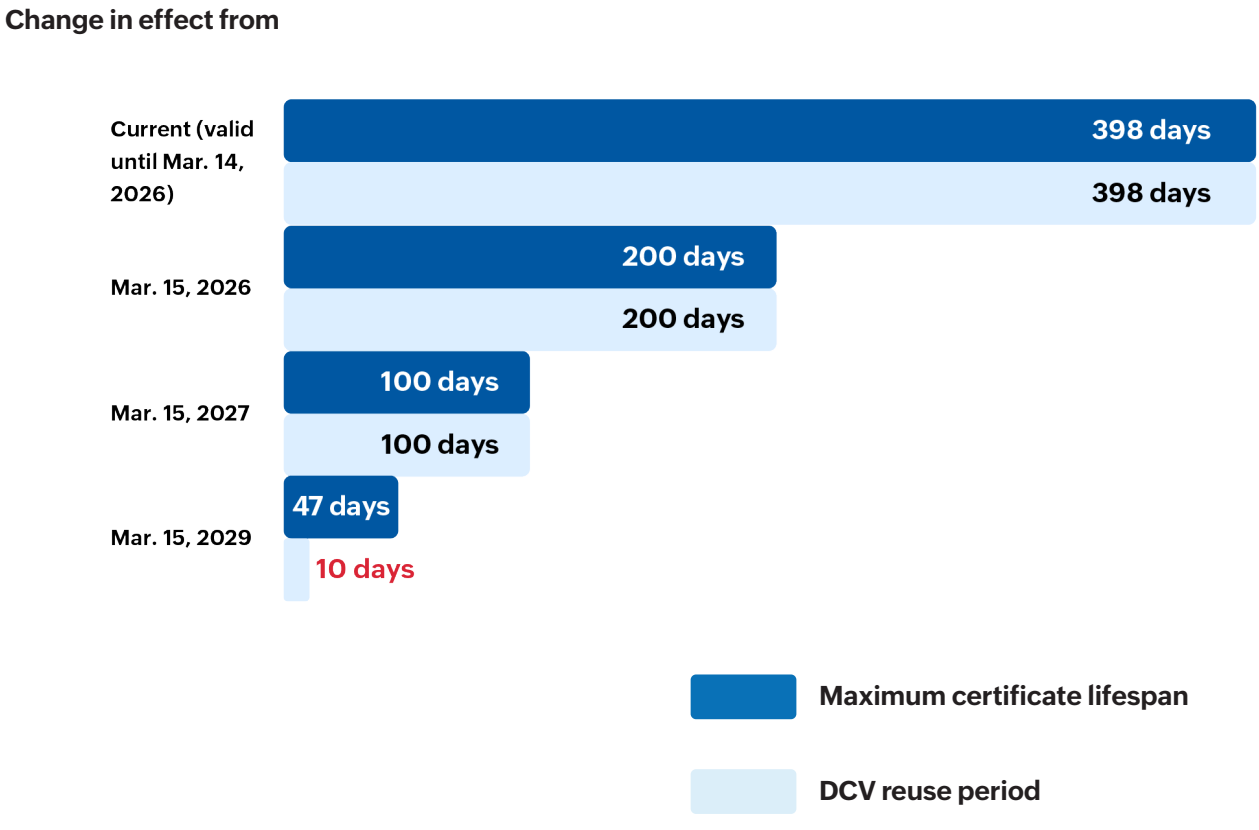
Preparing for the 47-day SSL/TLS certificate life span

Preparing for the 47-day SSL/TLS certificate life span

The digital landscape is shifting beneath our feet. For years, IT and security teams have operated on a comfortable cycle regarding SSL/TLS certificates. We grew used to validity periods spanning multiple years. Then it was reduced to just over one year (398 days). Now, we are approaching the next evolution in digital trust: a shift that will increase certificate renewals from once yearly to almost monthly by 2029, an 88% reduction in validity periods.

Starting March 15, 2026, there will be phased reductions in the maximum lifespan for public SSL/TLS server certificates. In this first phase, the SSL/TLS life cycle will cut down to 200 days. By 2027, it will drop to 100 days. By March of 2029, certificates will be valid for just 47 days. In addition to the shrinking certificate validity, the domain control validation (DCV) reuse period will also drop from 398 days to 10 days by 2029. Read all about this update here.

Here's the complete timeline and what it means for your organization:



This represents a significant operational shift, but it's also an opportunity to modernize your PKI infrastructure. Shorter certificate lifespans mean better security. Compromised keys have less time to be exploited, and organizations are forced to adopt automation that eliminates manual errors. The organizations that prepare now will transform this mandate into a competitive advantage. Most importantly, this will also encourage organizations to move away from manual certificate management and prepare them toward a state of crypto agility.

Understanding the impact

First, it's important to be clear about what actually happens on March 15, 2026. The public SSL/TLS server certificates you renew in April, May, and June of 2026 will have a 200-day validity. This means by October 2026, you'll be managing your first wave of 200-day certificate renewals. Ideally, we want enterprises to look at March 15, 2026 as the D-day to prepare for the wave of changes to follow.

What changes immediately:

- Any certificate issued on or after March 15, 2026 will have a maximum validity of 200 days.
- Public certificate authorities (CAs) will no longer issue certificates with 398-day validity.
- Your renewal frequency begins increasing from around once a year to around twice a year.

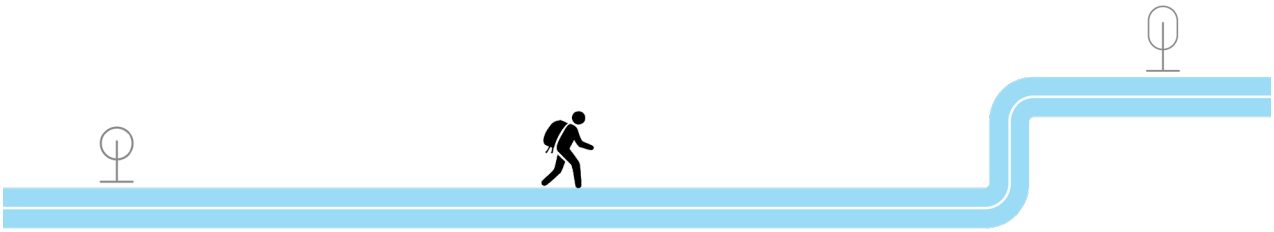
What does not change immediately:

- Certificates issued before March 15, 2026 remain valid until their original expiration date.
- If you have a certificate expiring in July 2026 that was issued in 2025, it stays valid until July 2026.
- Your existing infrastructure continues operating normally.

We have designed this guide to help you navigate this change over the next 90 days. Whether you have already started your preparation or are just now looking at the calendar, this roadmap will help you cross the first deadline (March 15, 2026) with confidence.

Where do you stand right now?

The first step in this process is knowing your starting line. At a high level, organizations typically fall into one of two categories regarding this transition.



I'm already on this journey

You have an inventory and perhaps some automation in place. This guide will help you conduct a comprehensive readiness audit. Use the sections ahead to verify that:

- Your inventory covers all certificate types (public, internal, cloud, containers).
- Automation works reliably end-to-end.
- Your monitoring processes catches issues before they become outages.
- Your team is trained and processes are documented.
- Edge cases have documented fallback procedures.

If you aren't able to verify all these yet, this guide will act as a good refresher. Read through to find improvement areas and evaluate your gaps with our checklist at the end.

I haven’t even started yet

You’re not alone, but time is critical. If you maintain your current manual processes, you’ll face 12 times more renewals per year by 2029. For a portfolio of just 100 certificates, that’s 1,200 renewals annually, which is about five every business day. The good news is that, with focused execution over the next three months, you can build automation that makes this transition seamless. We’ve built this guide to help you throughout this process.

The immediate action plan

In an ideal world, one would prioritize end-to-end automation over everything else. However, if you're short of time, here's a contingency plan that can help you buy some time. Considering the security benefits of the upcoming move, we recommend that you treat this as last-resort and not as your first course of action.

The red zone check

Regardless of which path you're on, you need to identify your immediate risks. Look at your current environment. Identify every certificate that is set to expire between March 15, 2026 and June 2026. These certificates are your highest priority. If they expire after the deadline, their renewal will be subject to the new, shorter validity rules. This could disrupt your operations if your systems are hard-coded to expect a one-year certificate.

Preemptive renewal

If you renew your mission-critical certificates before March 15, 2026, they will still be issued under the current rules. This means you can secure a fresh 398-day certificate one last time. Doing this resets the clock. It gives you a nearly one-year buffer to figure out your long-term automation strategy without the pressure of an immediate outage. This is a strategic move that can buy you valuable time. This way, you do not need to wait for your certificates to expire.

The path to preparedness (in the next 30 days)

You cannot secure what you cannot see. The most common cause of certificate-related outage is a failure of proper inventory management. Your primary goal for the first 30 days is to fix this layer.

1. Complete visibility through discovery

The foundation of certificate automation is knowing exactly what you have. Your certificate inventory acts as your single source of truth. Without it, you're flying blind. Build your inventory in such a way that it acts as the single source of truth for all things certificate management. Regardless of the use case, issuing CA, and deployment environment, your inventory must include clear visibility of every certificate that must be managed.

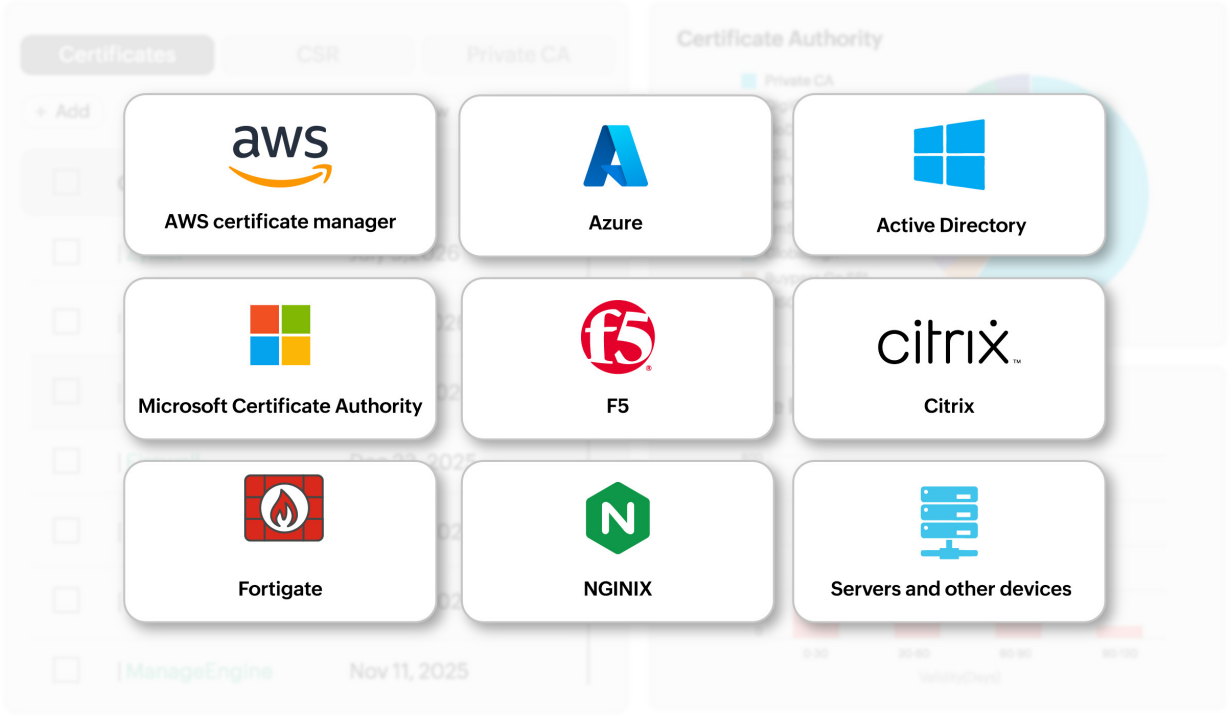
A comprehensive discovery process must capture certificates across:

- **Network scans:**

  Automated scans across your public IP ranges and internal subnets find certificates wherever they exist, including ones you didn't know about.

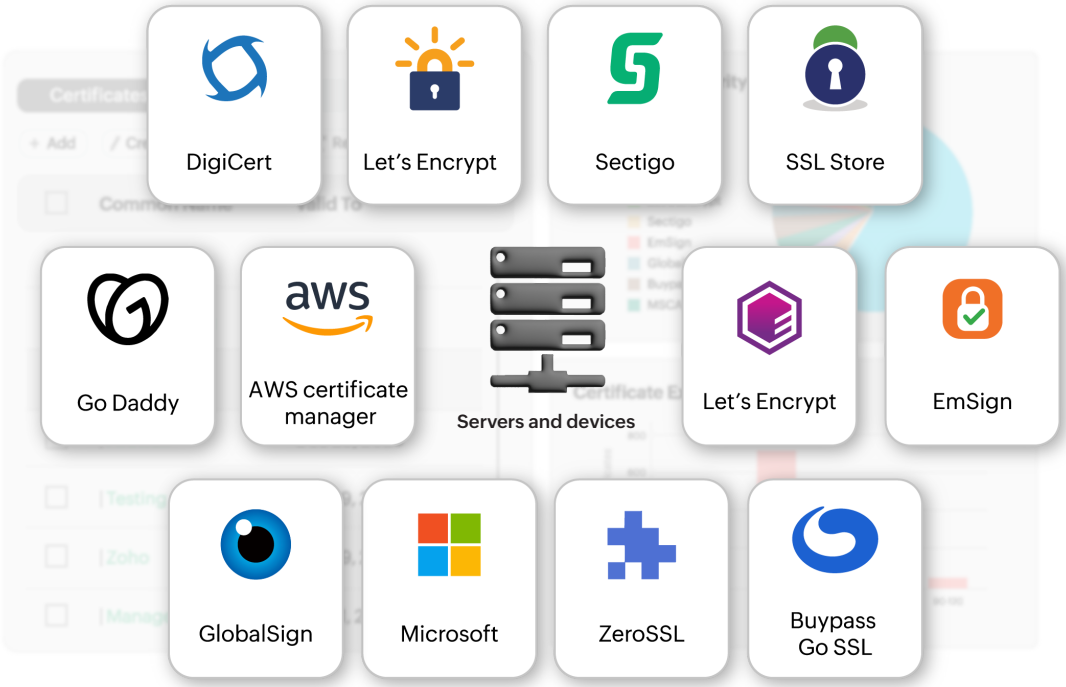
- **Cloud environments:**

  Connect to AWS, Azure, GCP, and other cloud accounts. Cloud-native certificates issued through services like AWS Certificate Manager or Azure Key Vault must be tracked centrally.



- **CAs:**

  Import data directly from the CAs you use (DigiCert, Sectigo, Let's Encrypt, etc.). This gives you a complete list of everything you've purchased.



Discovery tools and methods

Rather than managing certificates manually across scattered tools and spreadsheets, a CLM platform provides centralized visibility and control. A certificate life cycle management (CLM) solution like Key Manager Plus automates discovery across all these sources, continuously updating your inventory as certificates are added, renewed, or removed.

What must your inventory include?

For each certificate, ensure you track the following:

- Common names and Subject Alternative Names (SANs)
- Issuing CA and certificate type
- Expiration date and days remaining
- Installation location (servers, load balancers, cloud services)
- Owner/responsible team
- Automation status (automated, manual, in progress)
- Business criticality

Your output should be a live inventory showing all certificates with their status, not a static spreadsheet. This becomes your operational dashboard for everything that follows. Your certificate management solution must have you covered.

Note:
The discovery will produce a comprehensive certificate dump, but this isn't the endgame. Once you have your data, you must audit it. Focus on identifying the active certificates and remove certificates that are no longer in use. For example, this can be certificates assigned to applications or services that no longer exist. After a thorough assessment, you can safely remove these from your view to reduce noise.

2. Prioritize with a strategic matrix (day 31–75)

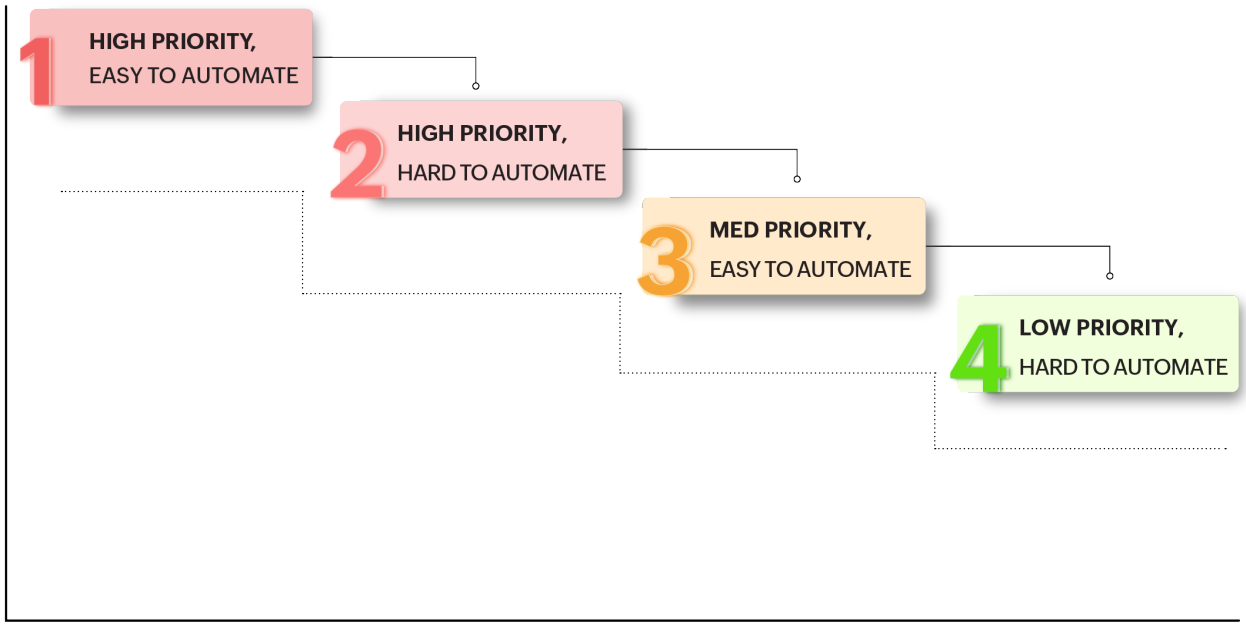
Once you have complete visibility, you need to triage your workload. Attempting to automate everything simultaneously leads to overwhelm and failure. Instead, use a priority matrix based on two factors:

Business impact :

How critical is this certificate to operations?

Ease of automation:

How readily can this certificate be automated?



1 Priority 1:

Certificates that hold the highest criticality and have modern automation workflows available should take the first priority. Think of your standard web servers like Nginx, Apache, or IIS. They power critical websites, but they also support automation protocols like ACME natively. Prioritize these for immediate automation. These low-hanging fruits are important quick wins.

2 Priority 2:

Once you're done addressing them, focus on the highly critical certificates that are hard to automate. These are critical systems like older load balancers, hardware appliances, legacy modules, or legacy applications with certificates that do not support modern automation. This is your legacy challenge and requires human intervention. Devices that previously failed to support automation capabilities may have incorporated support recently. Use this time to validate if automation is already possible. If not, you should start conversations with these vendors to ask about their roadmap for automation support.

If you're certain that automation isn't an option, set up a playbook to address the certificate renewal process. Write a step-by-step manual renewal guide for this specific use case and assign specific owners to oversee the entire process. The owner and the corresponding stakeholders must be thoroughly trained on it.

3 Priority 3:

When you're done with high-priority certificates, focus on the easy-to-automate low-priority certificates. These might be internal developer or test environments and can act as excellent testing grounds. Use them to refine your automation scripts before rolling them out to production.

4 Priority 4:

Finally, focus on the low-impact, internal legacy tools that have the lowest priority. If possible, consider deprecating these systems. If they must stay, accept that they will require manual management, but they should not distract your focus from the high-priority certificates.

Note:
Please remember that every organization is different. The examples we list below are common scenarios, but they are just examples. You must map your own priority based strictly on what you found during your discovery phase. A system that is low priority for one company might be mission-critical for yours.

Things to remember

Before you implement these changes, ensure you're asking yourself these important questions:

Does this really warrant a public certificate?

Before you map your certificates to the matrix, pause to ask a critical question. Does this service actually need a public certificate? The incoming mandate specifically targets public SSL/TLS server certificates. If you are using a public certificate to secure an internal intranet site, a testing server, or a backend database, you might be creating unnecessary work for yourself.

In the past, your organization might have defaulted to public certificates because setting up a private CA was too complex. However, your infrastructure has likely scaled since then. Now is the perfect time to consider switching these internal use cases to a private CA or self-signed certificates. Doing so removes them from the scope of the 47-day mandate entirely and gives you full control over their validity periods.

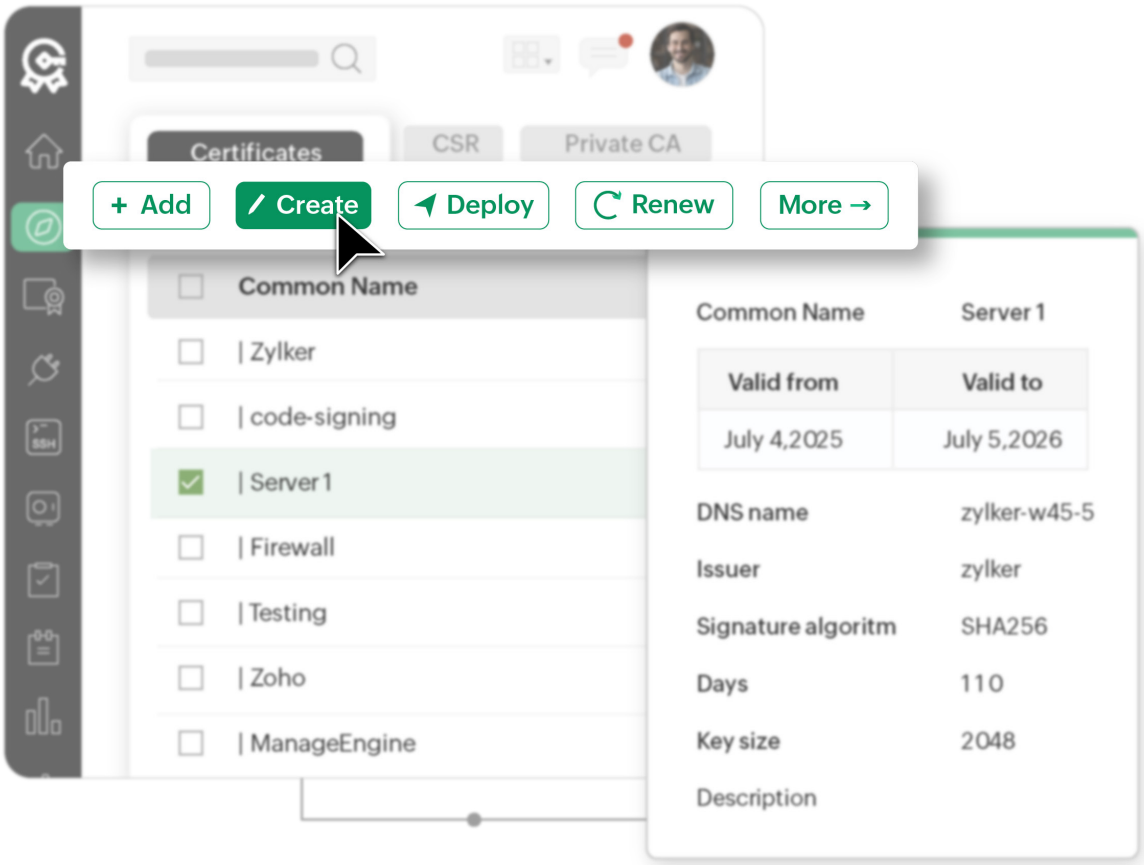
Is my alerting mechanism up to date?

In a 398-day world, getting an alert 90 days before expiration made sense. In a 47-day world, a 90-day alert is pointless. Adjust your alerts to notify you 20 or 30 days before expiration to keep your team focused. Here's an easy way to align your notifications according to the upcoming change timeline:

Certificate validity period	Alert 1 (days before expiration)	Alert 2 (days before expiration)	Alert 3 (days before expiration)
398 days (current)	90 days	30 days	7 days
200 days (starting Mar. 2026)	60 days	30 days	7 days
100 days (by Mar. 2027)	30 days	14 days	3 days
47 days (by Mar. 2029) 90 days	14 days	7 days	2 days

Does my certificate management platform handle end-to-end automation?

A certificate management solution will be at the heart of this whole project. If your current CLM application cannot help you with the automation process, it might be best to revisit your strategy. For example, you need a CA-agnostic certificate management platform like Key Manager Plus that can automate the entire certificate life cycle, right from discovery and monitoring to issuance, renewal, and deployment.



3. The last-mile (day 76–90)

As March 15, 2026 approaches, treat it like a major production release. Even with robust automation in place, the transition to 200-day maximum validity is a significant change and requires active management. Here's what you can have the team do during the last two weeks:

- ☑ Start by briefing all stakeholders on the transition timeline.
- ☑ Review all certificates expiring within 60 days of March 15, 2026.
- ☑ Verify automation is functioning for all high-priority certificates. This is also the time when you test emergency manual renewal procedures for these certificates. Should your workflow fail for any reason, this should bail you out.
- ☑ Confirm that you have the playbooks in place for certificates that still need manual intervention. Verify that renewal alerts are scheduled well in advance and the workflow is configured to notify all stakeholders.
- ☑ Set up alerts with multiple notification channels (email, ticketing system, and official communication channels).
- ☑ If you need more time to adapt to this change, create a preemptive renewal list and begin executing renewals for your top 50 mission-critical certificates that must be renewed before year-end with 398-day validity.

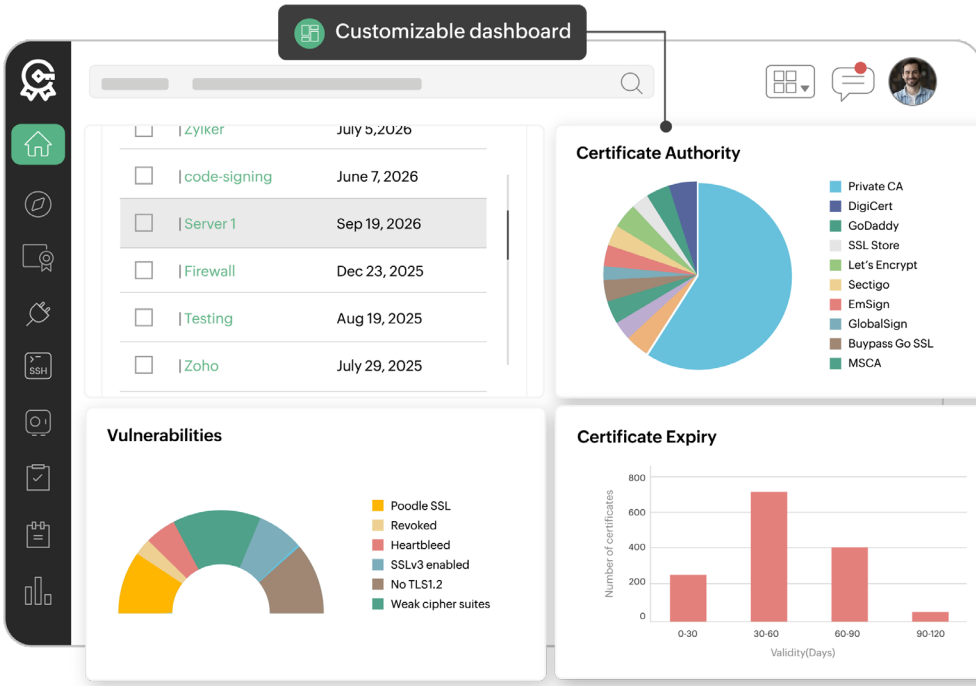
Building crypto-agility

The 47-day certificate mandate is one milestone in a longer journey toward cryptographic agility. Crypto agility is the ability to rapidly adapt your cryptographic infrastructure in response to emerging threats or technological advances, and this will play a crucial role in migrating to a post-quantum cryptographic world.

Quantum computers pose an existential threat to current encryption algorithms. NIST has published post-quantum cryptography standards, and the industry will transition to quantum-resistant algorithms over the next five to 10 years. When critical vulnerabilities emerge (like Heartbleed, Spectre, or future unknown threats), crypto-agile organizations can rapidly rotate certificates and keys across their entire infrastructure and adapt seamlessly. The infrastructure you're building for 47-day certificates creates the foundation for crypto agility.

Champion the transition with Key Manager Plus

As you navigate the transition to short-lived certificates, the right platform makes all the difference. Key Manager Plus provides the automation infrastructure you need: comprehensive discovery across all environments, automated renewal workflows, and seamless deployment to any platform, all CA-agnostic and fully integrated. Organizations can deploy complete certificate life cycle management in weeks, giving you automation that's operational well before the March 2026 deadline.



Talk to us

Schedule a demo with an expert

Thousands of organizations worldwide rely on Key Manager Plus to automate their certificate life cycle management.

ManageEngine
Key Manager Plus