

The Top 10 PKI Metrics You Need to Track

Get the metrics you need to analyze the health of every machine identity.





Contents

INTRODUCTION3

THE TOP 10 PKI METRICS..... 4

BRINGING IT TOGETHER WITH KEYFACTOR DASHBOARDS15

IT'S TIME FOR BETTER REPORTING.....18

Introduction

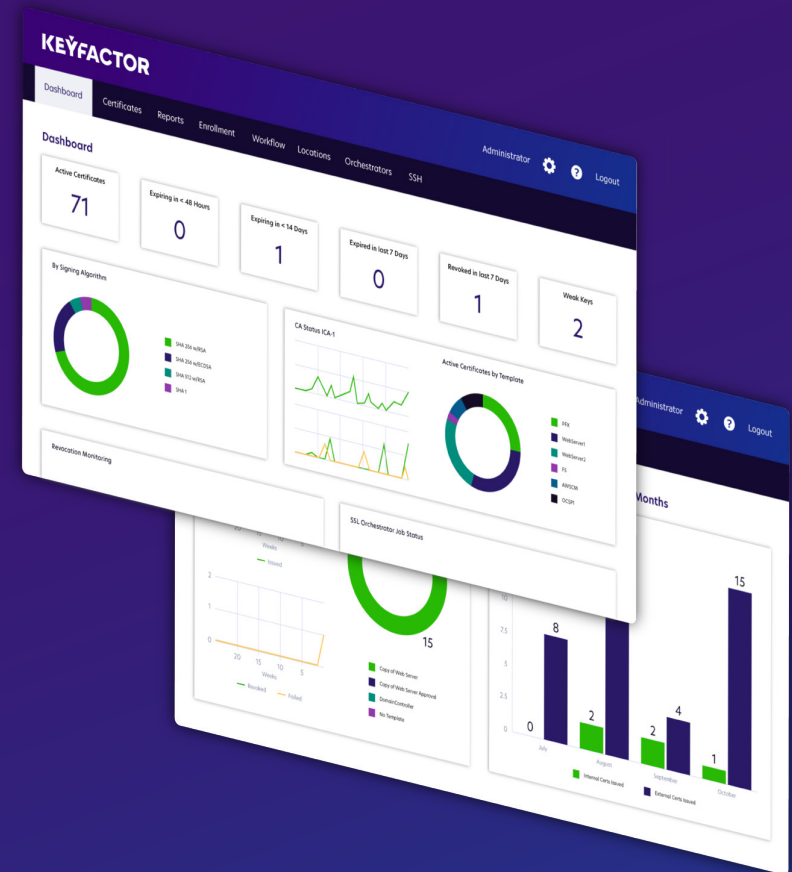
If you're running public key infrastructure (PKI) operations in your enterprise, or you're responsible for managing thousands of keys and certificates, this eBook is for you.

Let's be real. There's a lot to consider when it comes to the state of PKI and machine identities.

Getting an accurate inventory of every key and certificate is the place to start, but that is really just the tip of the iceberg. There's no shortage of reporting metrics you can track, but if you're like most organizations with limited time and resources, you need to focus on what counts.

That's why we've narrowed down the top 10 must-have metrics you need to track to manage cryptography in your enterprise effectively.

This guide will help you and your team create a baseline to avoid preventable outages, security risks, and frustrations caused by unknown or untracked machine identities.





The Top 10 PKI Metrics

#1: Expiration Status

Who needs to know?

- ▶ App Owners
- ▶ Managers
- ▶ PKI Admins

Why should you care?

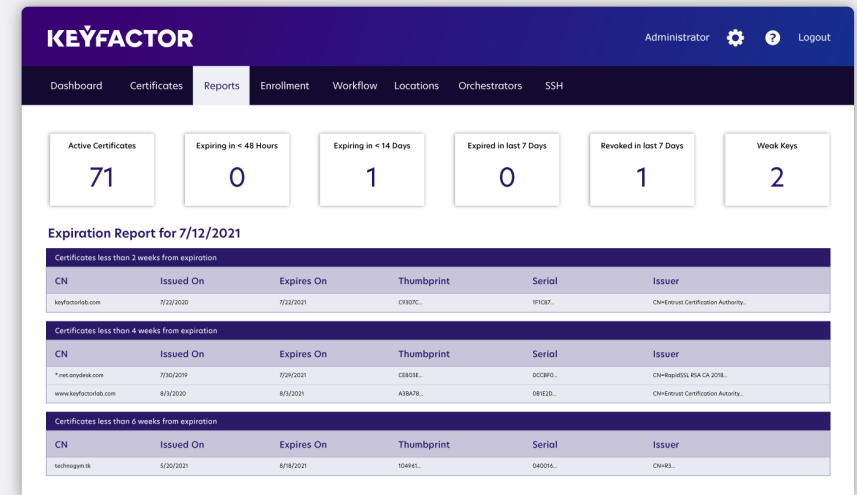
Without proper visibility over every key and certificate, you won't know when they will expire. Worse, if you don't know who to notify before it happens, the risk of network outages will keep rising as you add more identities across your business.

These outages lead to costly downtime, which ultimately comes to rest at the executive's foot when it happens.

Example Report

This report provides a view into upcoming expirations broken out by the timeframe till expiration.

This allows you to plan which certificates to renew first and see who is responsible for the renewal.



#2: Key Size and Strength

Who needs to know?

- ▶ PKI Admins
- ▶ Auditors
- ▶ Security Teams

Why should you care?

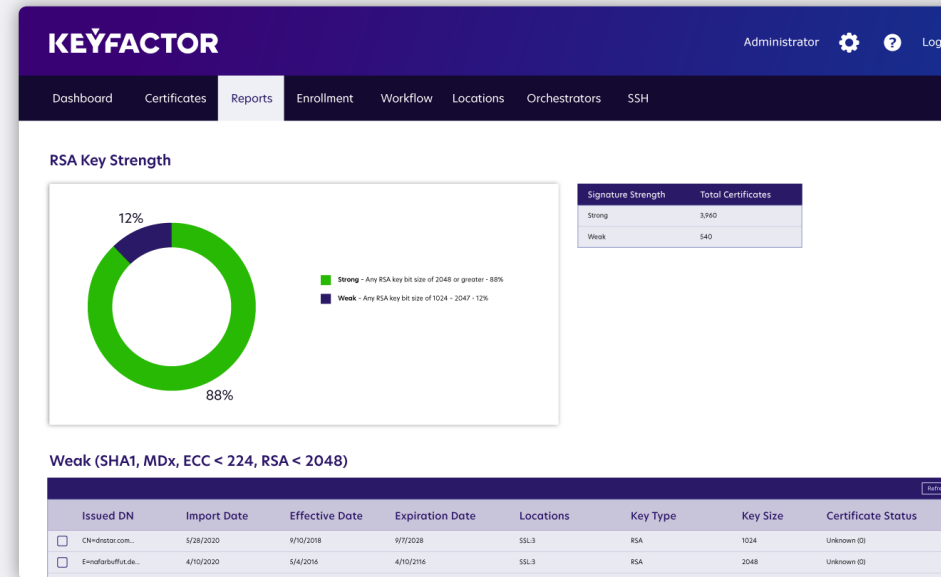
Algorithms evolve with advances in computing, and as they do, you must be able to adapt quickly and with minimal disruption to existing apps and infrastructure.

This report allows teams to see vulnerable certificates in their environment and get to work on replacing them with stronger, compliant certificates.

As a side note, bulk revocation and re-issuance of certificates through an automated platform can help significantly reduce time to remediate issues and the impact it has on your operations.

Example Report

This report shows a pie chart for each selected CA showing the active certificates by key size (e.g., 1024 bit, 2048 bit). It also gives detailed row information to locate which certificates are weak.



#3: Signing Algorithms

Who needs to know?

- ▶ PKI Admins
- ▶ Auditors
- ▶ Security Teams

Why should you care?

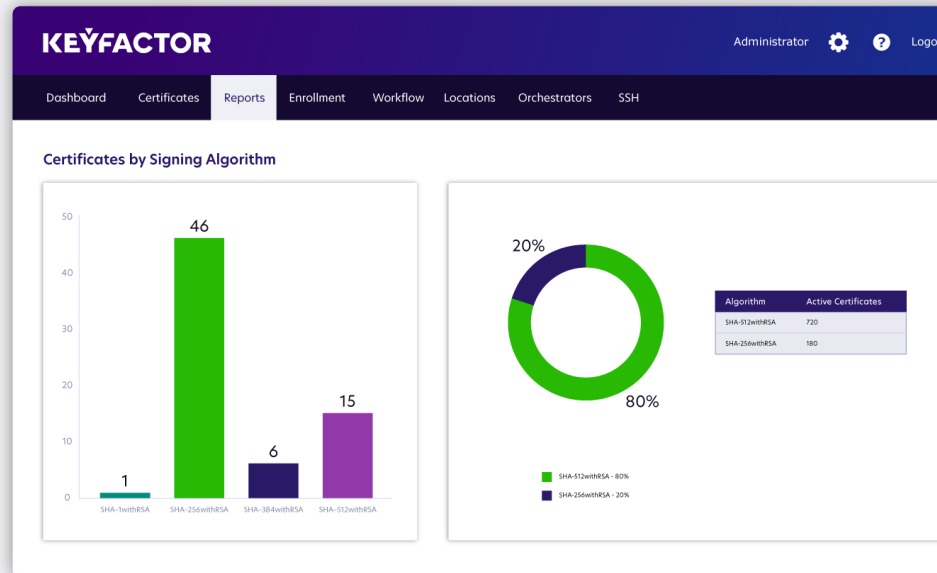
Key signing algorithms are the foundation of trust and security for your PKI. Similar to key size and strength, it's essential to track signing algorithms and prepare for migration if – or more accurately when – the algorithm is deprecated.

A well-known example of this is the migration from SHA-1 to SHA-2, a transition that was far longer and far more disruptive than it should have been for many organizations.

Larger hashes are generally more secure as they are less vulnerable to collision attacks. However, the definition of “larger” is constantly changing in the world of cryptography.

Example Report

This report will show you where you may be able to increase the robustness of your digital signatures by seeing the hashing algorithm (e.g., SHA-1, SHA-256) used to create the hash used in the signature.



#4: Certificate Authority (CA) Issuance

Who needs to know?

- ▶ PKI Admins
- ▶ Security Teams

Why should you care?

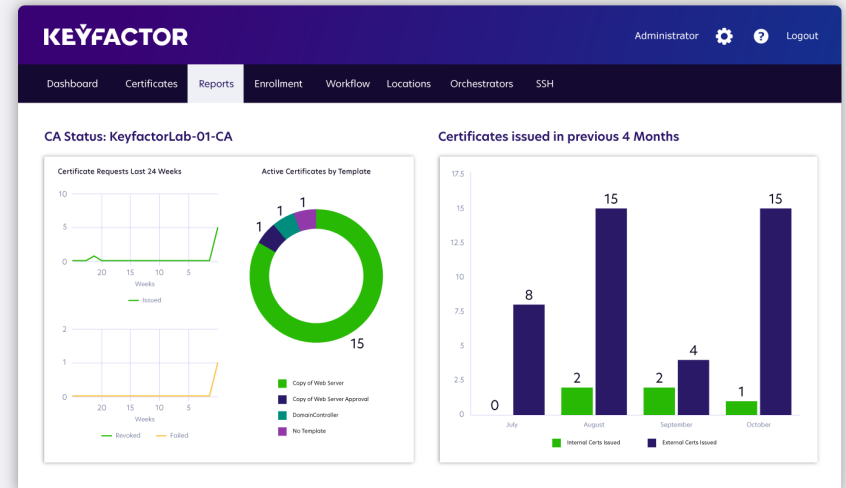
For PKI administrators working with multiple CA(s), you need an overview of the activity that is happening on the CA at any particular point in time. This can be helpful to detect anomalous activity.

For instance, a misconfigured GPO could be issuing certs that it shouldn't. This leads to deploying machine identities in your environment that you don't need. Unnecessary identities provide more doors for an attacker to try to use.

Example Report

These pie charts and line graphs show the number of certificates issued, denied, and revoked for a selected date range for the selected CA(s).

Teams can set alerts to notify them if a CA is issuing certificates at an extreme rate. This helps admins understand if abnormal certificate issuance is occurring without them knowing.



#5: Certificate Requesters and Owners

Who needs to know?

- ▶ Application Owners
- ▶ Certificate Managers

Why should you care?

When there is a certificate expiration or operational downtime, the first question that's usually asked is, "Who owns the certificate?" Without knowing who the certificate owner is, business downtime keeps extending until someone is notified to renew the certificate.

Knowing exactly who owns the certificates allows you to send out reminders and alerts to the direct owner to avoid any unplanned outages.

Example Report

Seeing who is requesting specific types of certificates can allow administrators to project certificate issuance trends over time and display requesters' contact information.

The image displays three overlapping screenshots of a 'Certificate Details' interface. The largest screenshot shows the 'Content' tab with a table of certificate metadata:

Field	Value
Subject	CN=20210712c.keyfactorlab.com
Serial Number	1A0000001BD71CE91A61C31A3400000000001B
Not Before	7/12/2021
Not After	7/12/2023
Key Usage	Digital Signature, Key Encipherment (a0)
Extended Key Usage	Server Authentication
Signing Usage	SHA-512withRSA
Template	Copy of Web Server
Thumbprint	B1F945B4D59943B157434E2E18615B23A4D
Issuer	CN=KeyfactorLab-KeyfactorLab01-CADC
Subject Alternative Names	
Total SANs	0

The middle screenshot shows the 'Status' tab with a table of certificate details:

Field	Value
Certificate ID	9488
CA Request ID	27
Certificate State	Active (1)
Requester Name	KEYFACTORLAB\KYFAdmin

The smallest screenshot shows the 'History' tab with a table of certificate operations:

Operation Start	Operation End	Username	Comment	Action
7/12/2021	7/12/2021	KEYFACTORLA...	Requested via P...	Certificate Reque...

#6: Self-Signed Certificates

Who needs to know?

- ▶ PKI Admins
- ▶ Security Teams
- ▶ Application Owners
- ▶ Certificate Managers

Why should you care?

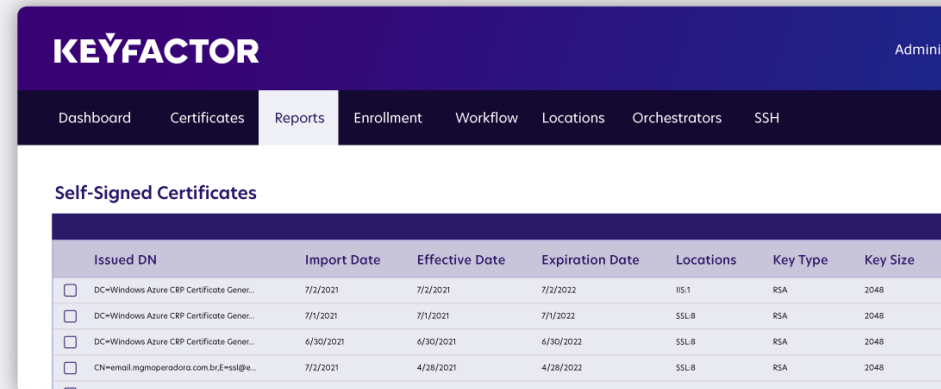
The speed of DevOps has rapidly increased the use of self-signed certificates within engineering teams. While they deploy extremely fast, a self-signed certificate is one that a CA at all does not sign – neither private nor public.

That's why it's recommended you integrate to secrets managers with policy-compliant issuers (public or private CA(s)). This way, you can set up monitoring of the high-volume certificate issuance from these secret managers. Without this integration, auditing certificate lifecycle becomes nearly impossible.

Example Report

This report will display the number of self-signed certs per environment with parameters monitoring certificate thresholds. If the certificate threshold is reached, then the PKI administrator would be aware of the high number of self-signed certificates being used.

By comparing self-signed certificate counts with CA-backed certificates, teams can understand where the risk resides in the organization.



The screenshot shows the KEYFACTOR interface with a navigation menu at the top containing Dashboard, Certificates, Reports, Enrollment, Workflow, Locations, Orchestrators, and SSH. The 'Reports' tab is active, displaying a table titled 'Self-Signed Certificates'. The table has columns for Issued DN, Import Date, Effective Date, Expiration Date, Locations, Key Type, and Key Size. There are four rows of data, each with a checkbox in the first column.

	Issued DN	Import Date	Effective Date	Expiration Date	Locations	Key Type	Key Size
<input type="checkbox"/>	DC=Windows Azure CRP Certificate Gener...	7/2/2021	7/2/2021	7/2/2022	IS-1	RSA	2048
<input type="checkbox"/>	DC=Windows Azure CRP Certificate Gener...	7/1/2021	7/1/2021	7/1/2022	SSL-8	RSA	2048
<input type="checkbox"/>	DC=Windows Azure CRP Certificate Gener...	6/30/2021	6/30/2021	6/30/2022	SSL-8	RSA	2048
<input type="checkbox"/>	CN=emal.mgoperadora.com.brE=ssl@...	7/2/2021	4/28/2021	4/28/2022	SSL-8	RSA	2048

#7: Wildcard Certificates

Who needs to know?

- ▶ PKI Admins
- ▶ Security Teams

Why should you care?

SSL wildcard certificates can be beneficial for organizations wanting to deploy and secure a large number of subdomains. In contrast, while they provide cost savings and flexibility, their reliance on the same private key increases the risk of an organization-wide compromise.

Example Report

This report would show the number of wildcard certificates in inventory and every endpoint that's used with each certificate. Searching for "*" helps the PKI administrator understand the scope of wildcard certificates usage and remediate any single point of failure.

The screenshot shows the KEYFACTOR interface with a navigation bar containing Dashboard, Certificates, Reports, Enrollment, Workflow, Locations, Orchestrators, and SSH. The 'Reports' tab is active. Below the navigation bar is the 'Certificate Search' section. It features a search form with a 'Field' dropdown set to 'CN', a 'Comparison' dropdown set to 'contains', and a 'Value' input field containing an asterisk (*). There are radio buttons for 'Include Revoked' and 'Include Expired', with 'Include Expired' selected. A 'Search' button is located to the right of the search form. Below the search form is a table with the following columns: Issued DN, Import Date, Effective Date, Expiration Date, Locations, Key Type, and Key Size. The table contains four rows of data, each with a checkbox in the first column.

Issued DN	Import Date	Effective Date	Expiration Date	Locations	Key Type	Key Size
<input type="checkbox"/> CN=*	9/1/2020	8/12/2020	8/12/2022	HS-1	RSA	2048
<input type="checkbox"/> CN=*	9/1/2020	7/30/2019	7/29/2021	SSL-8	RSA	2048
<input type="checkbox"/> CN=*	4/10/2020	10/16/2017	11/10/2020	SSL-1	RSA	2048
<input type="checkbox"/> CN=*	1/24/2020	4/12/2017	12/11/2020	SSL-1	RSA	2048

#8: Automated vs Manual Certificates

Who needs to know?

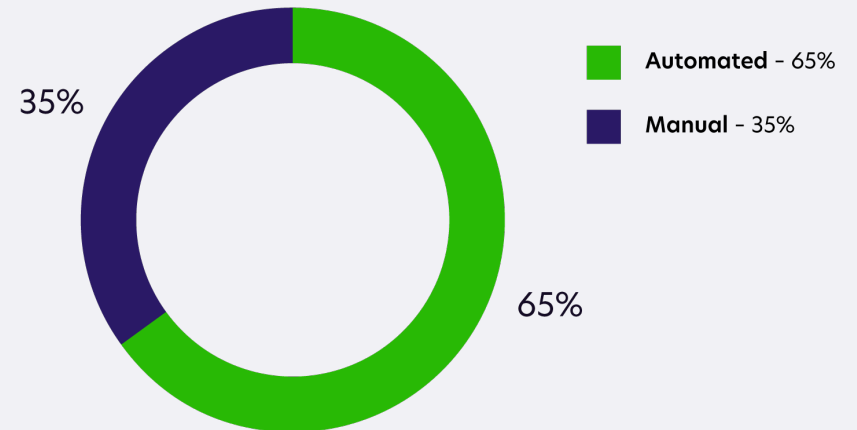
- ▶ PKI Admins
- ▶ Security Teams
- ▶ Executives

Why should you care?

Your goal should be to achieve as much certificate lifecycle automation as possible for the certificates within your control. However, without understanding the amount of ad hoc and manual certificate management processes you have in place, it's hard to set automation goals.

Example Report

This comparative report would show the number of automated certificates vs. managed certificates. This report will actively monitor which certificates have enabled automated renewals and deployments to workloads and endpoints.



#9: CRL Health

Who needs to know?

- ▶ PKI Admins
- ▶ Security Teams

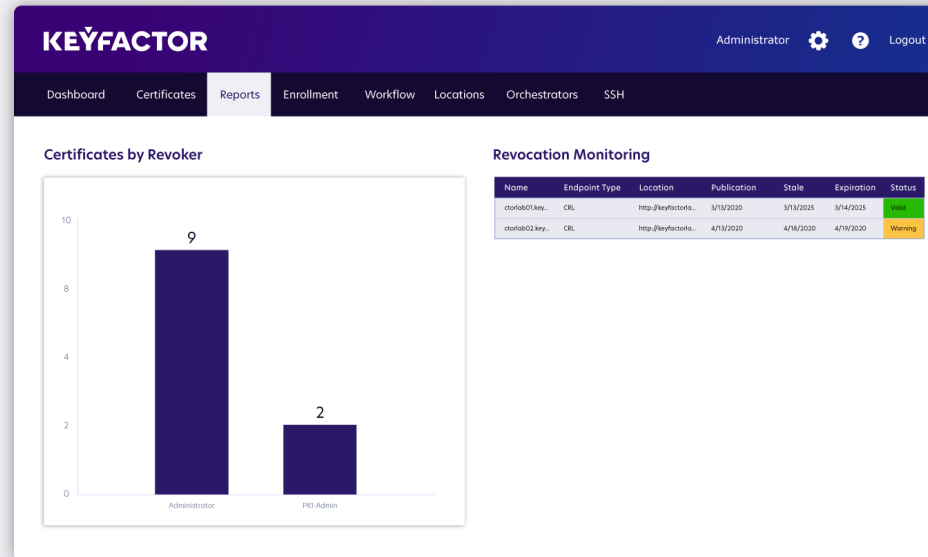
Why should you care?

Certificates are revoked for various reasons: key or CA compromise, certificate no longer needed, or certificate superseded. Seeing who is revoking the certificates allows a PKI administrator to follow up to see if related applications or endpoints might need to be similarly remediated.

For instance, if a key is compromised, the security administrator may want to follow up with the revoker to understand what caused the key to be compromised. Now they can figure out processes to avoid a future compromise that could allow an attacker access into the system.

Example Report

This report shows a bar graph of the number of certificates revoked from a selected date range for specific CA(s). This report can further break down which user is doing the revocation.



#10: Unknown Certificates

Who needs to know?

- ▶ PKI Admins
- ▶ Security Teams

Why should you care?

What's worse than not managing a known certificate? It's not managing an unknown one. These anonymous certificates are the ones that come from CA(s) you don't know about. They are certificates that are on unknown endpoints.

Without knowing where every certificate lives, you're vulnerable to unplanned outages, costly downtime, and increased risk exposure.

Example Report

This report shows the result of a scheduled or on-demand scanning for TLS/SSL endpoints. By scanning your endpoints, your team can continuously monitor all unknown certificates so you can bring them under lifecycle management.

The screenshot shows the KEYFACTOR dashboard with a navigation menu including Dashboard, Certificates, Reports, Enrollment, Workflow, Locations, Orchestrators, and SSH. The 'Reports' section is active, displaying a report titled 'Certificates Found at TLS/SSL Endpoints'. An 'Export' button is visible above a table of certificate data.

Ip Address	Port	Issued DN
192.155.109.28	443	E=root@wordpress.CN=wordpress...
192.155.110.100	443	DC=Windows Azure CRP Certificate Gener...
192.155.110.100	443	CN=PanelL, Inc. Certification Authority...
192.155.110.100	443	CN=winnersmails.com...
192.155.110.115	443	CN=ISRG Root X1...
192.155.110.115	443	CN=R3, O=Let's Encrypt, C=US



Bringing it All Together with Keyfactor Dashboards

Looking at these metrics can help analyze the health of your PKI. However, it's tough to pinpoint precisely where you should focus without seeing them together in one holistic and consumable view.

That's where Keyfactor can help.

By combining these metrics into executive and team dashboards, Keyfactor gives you better visualizations of where you need to focus on improving your certificate management and automation practices.

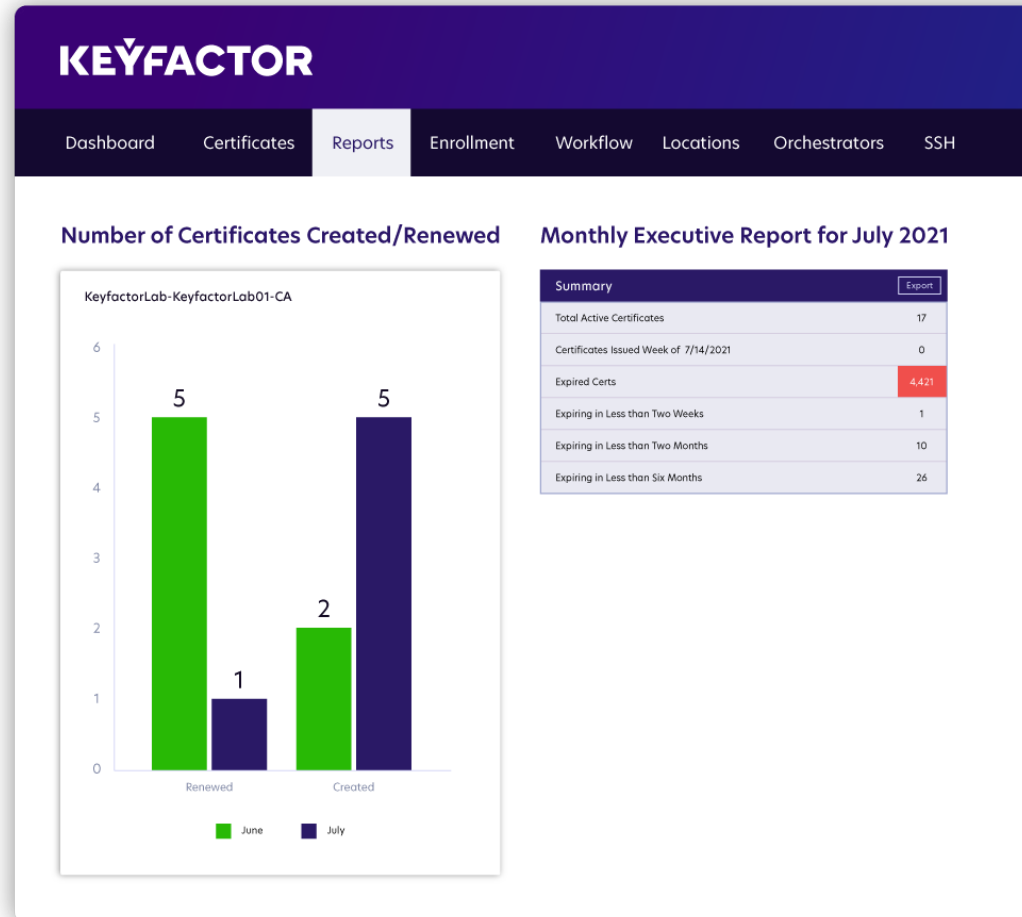


Monthly Executive Report

This dashboard provides executives a glance view of the issuance activity over the past month, compared with the previous month. It also allows them to see the number of certificates about to expire in the next 30 days, and how many certificates are on the CA.

This quick peek into the health of the CA allows an executive to see in a few seconds if there are any high-level flags that something further needs to be investigated.

For instance, a large number (or even any!) certificates set to expire in the next 16-30 days could indicate that there's a risk of an outage and prompt investigation to get the certificate replaced before that happens.



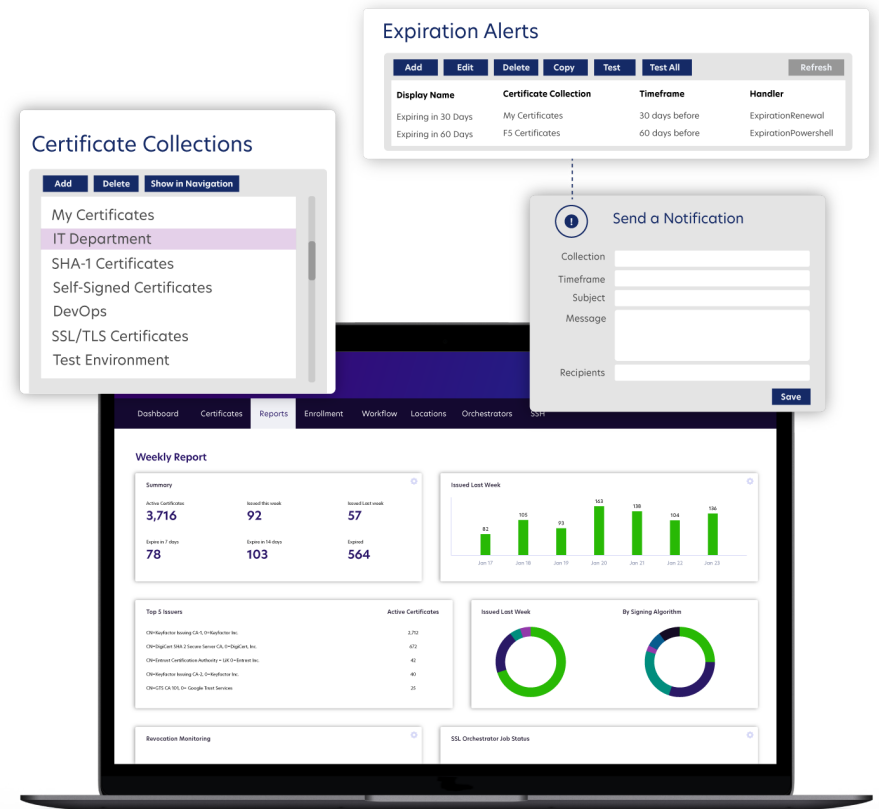


PKI Status Health Status

For the more technically minded executives, as well as for PKI admins and application owners, this report provides a dashboard view of all sorts of metrics for PKI health for the certificates being reported on.

At a glance, the report shows issuance, expirations, key strength, issuers, and CA activity, amongst other things.

Having a high-level view of the health of the PKI can be a good starting point to determine what, if any, areas of the environment need attention to remediate outages, misconfigured GPOs, etc.





It's time for better reporting.

Take back control of your cryptography with Keyfactor.

Keyfactor provides a single pane of glass across multiple machine identities, such as keys and certificates used within organizations' hybrid and multi-cloud environments.

Request a demo on how you can get better visibility, control, and automation for every machine identity.

[REQUEST A DEMO](#)

KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains. With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe.

For more information, [visit www.keyfactor.com](http://www.keyfactor.com) or follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#). Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

Contact Us

- ▶ www.keyfactor.com
- ▶ +1.216.785.2990