

PKI Insights – Health monitoring for CA

PKI Insights actively monitors your Enterprise Microsoft CA giving insights on its health and performance

- ✓ Get an in-depth analysis of your PKI
- ✓ Performs active scanning of your CA
- ✓ Detects PKI weakness and raises alerts
- ✓ Performs 250+ critical PKI checks
- ✓ Get access to health reports any time, any device

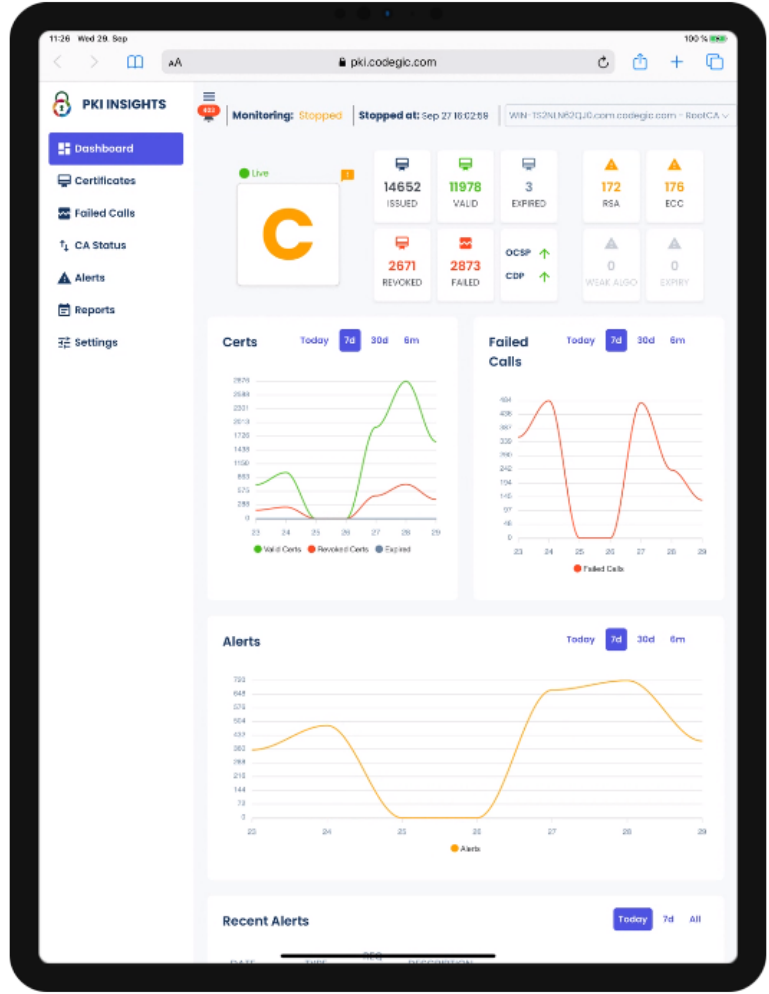


What is PKI Server Health Monitoring?

A PKI health check involves active monitoring of critical issues related to your PKI. Some of these are certificate issuance failures caused due to miss-configured Microsoft CA templates or attackers trying to issue fake certificates. Checking includes analyzing how many certificates are issued, revoked and expired at a particular point in time. Most importantly this includes gauging your PKI health. This is based on critical checks like detection of weak algorithms, weak keys, issuance of long-lived certificates, PKI related anomalies like issuance of non-standard certificate extensions, server status and lot more.

Why PKI Insights?

Analyzing a PKI against vulnerabilities without using a health monitoring tool is cumbersome, time consuming and costly calling the need for a specialist PKI monitoring product, which is what PKI Insights in essence is!



250
PKI Checks



21
Data Elements



5
Real-time graphs

3 Core Reasons to choose PKI Insights

Comprehensive PKI Monitoring

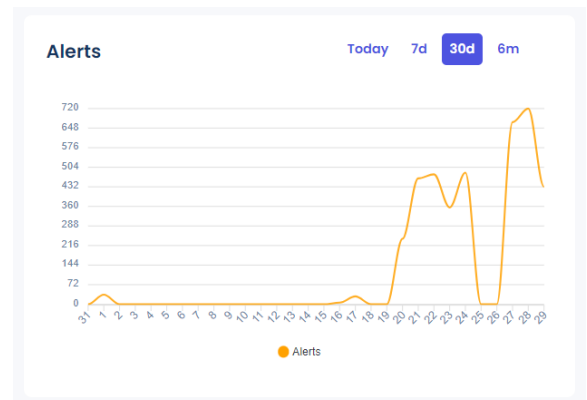
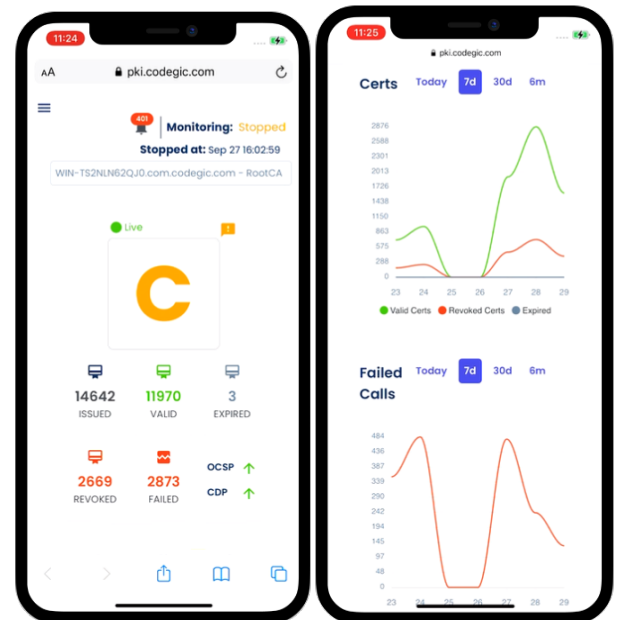
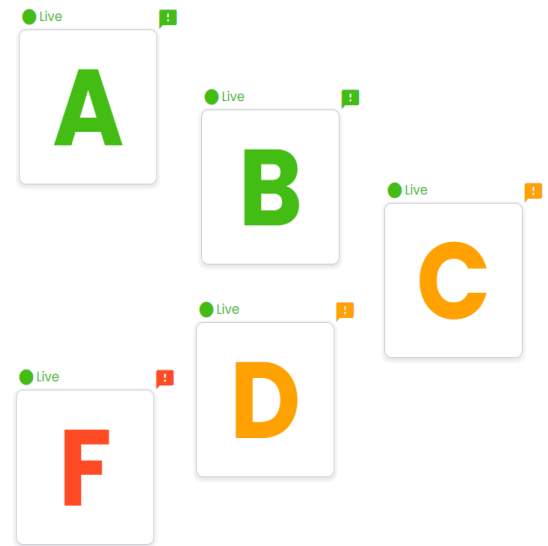
Your CA might be creating digital certificates using weak algorithms like SHA-1, RSA 1024 or ECC-160 bit. The worry quadruples with the issuance of thousands of digital certificates specially when it comes to issuing thousands of digital certificates to IOT or end-users. PKI Insights give your PKI admin a true picture of whether to worry or relax. With its advanced monitoring engine, PKI Insights checks issued certificate against 250+ PKI tests. You can manage multiple CAs, see trends of certificate issuance, revocation and expiry. Lastly PKI administrator can easily search and find details about certificates, failures, CA up/down time and get daily summary reports giving details of the current performance of your CA.

Dashboard for PKI Analytics

PKI Insights summarizes all the key aspects of your Microsoft CA in a concise dashboard allowing decision making fast. Administrators can see the peak hours where digital certificates were issued the most, time during which failures occur in certificate issuance and the PKI issues identified against them. There is no limit on the number of CAs to work with. All of this is then summarized in a CA Health rating giving PKI administrators a sense of achievement or to improve further. You can monitor multiple CAs in your entire PKI from just one secure user interface. There is no need to login to the CA server to get just boring transactional data or information which doesn't make PKI sense. Monitor your PKI any time and any where using your PC, tablet or mobile.

Prompt Alarms for Troubleshooting

PKI servers issues can be very hard to troubleshoot. It is quite difficult to know that your CA was down at the middle of off-peak hours and then went up. Similarly your OCSP server might be down for few minutes or access to CRL was interrupted. You might be on a vacation while your CA server is issuing weak keys, getting requests from rogue devices for certificate issuance or issuing long lived digital certificates. PKI Insight raises alarms by sending alerts to your PKI administrator. All of this is detected and notified to you right away before PKI auditors raise it.



Key Features

Get 360° View

Get an overall health of your PKI by:

- Detecting anomalies in your PKI
- Filtering data via searchable portal
- Accessing data for all CAs from one dashboard
- Get stats on certificates, failures, templates, up time
- Stats based on RFC 5280, 6560 standards
- Follows CA/B Forum guidelines for SSL certs

Performs 250+ PKI Checks

Running CA is simple, detecting if it is issuing weak certificate or keys is hard. PKI Insight detects a range of PKI issues covering:

- Signing, Public Key Algorithm & Lengths
- Certs expiry beyond acceptable limits
- Failures coming while issuing certificate
- Detects deviance from RFC 5280

Reports

Get daily summary reports covering:

- Get all time stats
- See detailed list of issues found in the PKI
- Daily stats on certs issued, failures, alerts

Analyze Trends

Get graphs on 10+ key PKI areas:

- Alerts, Failed calls
- Certificate Expiry, CA Up/Down time
- Certificates issuance (valid, expired)
- Certificate Templates, Revocation
- About to Expire Certificates
- Key Length, Signing Algorithm

Secure Access

PKI Insight portal is only accessible to trusted resources of your organization. Authentication is done over SSL/TLS Client authentication giving the most powerful, password less authentication. Supports all major browsers over PC, MAC and Devices.

Alerts

Get instant email/SMS based alerts when CA goes down or CA is not working as it should. Detects any major changes as they occur e.g. CRL/OCSP Server not accessible or changes in your PKI Rating.

Algorithms / Supported CA / H/W / Database

- RFC 5280, 6560
- Windows CA Server (2008, 2012, 2016, 2019, 2022)
- 2 GB RAM, Core i5 2.4 GHz CPU, 500 MB Hard disk
- PostgreSQL, MySQL, SQL Server
- Any browser on PC, Tablet or Mobile

Codegic

www.codegic.com

info@codegic.com

© Codegic. All Rights Reserved



Codegic works in the domain of PKI & Security. We specialize in Timestamping, Document Signing, Digital Signature Verification, Digital Certificates, PKI Monitoring, HSMs which help in your secure digital transformation. We utilise all the latest technologies at hand to help companies and enterprises solve complex issues that always emerge during their digital evolution journey.

Learn more at www.codegic.com