GlobalSign
GMO INTERNET GROUP

Certificate Inventory Tool (CIT)

Locate all SSL Certificates on your internal and public networks regardless of issuing CA

The Need for Better SSL Tracking

Do you know where you have SSL certificates installed? How about when each certificate is going to expire and which CA you ordered from? What about the hashing algorithm or key lengths used? The answers are likely no, or at the very least yes, but it's difficult to compile all the information.

Organizations often order certificates from multiple vendors and install throughout their networks, both internally and externally. While there are many advantages to this flexible, custom approach, it can make things difficult for whoever's in charge of managing the certificates and renewals.

Our new Certificate Inventory Tool finds all SSL certificates on your networks, both internal and public-facing, regardless of the issuing CA. The resulting inventory is available in an easy-to-use portal, allowing you to run reports on usage, upcoming renewals, configurations, and CA issuance.

How It Helps

- Find and monitor all internal and public SSL Certificates from one location, regardless of issuing CA, including self-signed
- Avoid unexpected expiration with email reminders to renew
- Easily track the source/issuing CA for all of your certificates
- Locate any certificates that may have been purchased ad hoc by other individuals or departments
- Save valuable time and resources over manual monitoring
- Keep up with baseline requirements and best practices with the ability to run reports on key length, hashing algorithm, and other configuration options

Avoid Expirations

Expired public SSL certificates can trigger alarming warnings in browsers, damaging your company's reputation and decreasing traffic to your site. Internally, expirations can disrupt the processes dependent on the encrypted communication. Fortunately, the Certificate Inventory Tool makes it very easy to avoid costly certificate expirations.

After your certificates have been inventoried, you will receive email alerts when they are nearing expiration. Once you renew the certificate and run the scan again, the status will be updated and you will stop receiving expiration notices.

Keep Up with SSL Best Practices

Best practices for key lengths, validity period, hashing algorithm, and other certificate options are constantly being revised. The Certificate Inventory Tool makes it easy to scan your entire repository of certificates to ensure they are all up to date and compliant with the latest recommendations.

You can configure your account to match your corporate policies on minimum settings for key length, signing algorithm, Issuing CA, validity period minimum/maximum, etc. All of your certificates will be measured and reported against these custom policies. You can have different policies for internal and external certificates, or for different network segments.

How It Works

Running Scans

The process for scanning your networks to locate certificates is slightly different for public-facing versus internal use cases. To scan internal networks, you must first download and install an agent locally. After that, everything is handled through the Inventory Tool portal.

1. Create a job in the portal (ie., a range of IP addresses, a domain, or a host name) and then select if you want this run from the Inventory Tool server, or sent to a local agent.

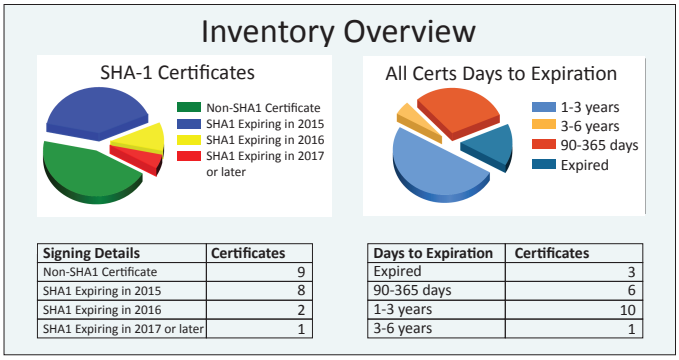
2. Run the job or schedule it to be run later.

3. The Inventory Tool will scan the sites for SSL Certificates either from the service, or via the specified local agent.

4. Results will be automatically uploaded to your portal for reporting and further investigation.

Viewing Results

Results from the scans are automatically uploaded to your portal where you can easily run reports and view the status of certificates, including issue date, issuing CA, expiration date, and validity period.



Signing Details	Certificates
Non-SHA1 Certificate	9
SHA1 Expiring in 2015	8
SHA1 Expiring in 2016	2
SHA1 Expiring in 2017 or later	1

Days to Expiration	Certificates
Expired	3
90-365 days	6
1-3 years	10
3-6 years	1

Contact us for more information about the Certificate Inventory Tool.

www.globalsign.com | sales@globalsign.com