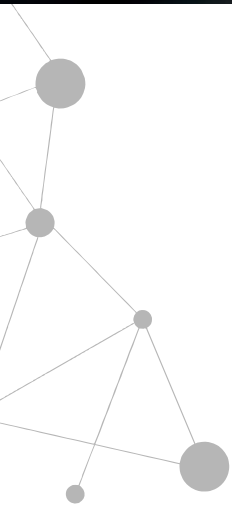
AppViewX



# Overcoming the Top 3 Bottlenecks in SSL/TLS Certificate Management



**White Paper**

by AppViewX

# Contents

# Overcoming the Top 3 Bottlenecks in SSL/TLS Certificate Management

## Introduction

Data security is one of the most discussed topics in enterprise IT today. As more and more applications become web-based and require encryption, the need to protect and secure data is more important than ever before. Users must feel confident that they are at legitimate websites before they will share valuable information. Recent security breaches and hacking attempts have forced enterprises to employ best-in-class security features to reinforce web security.

SSL/TLS certificates are the first thing that comes to mind when web security is discussed. SSL/TLS certificates are the backbone of web security because they protect data and make sure it remains intact as it traverses networks. They also enable authentication and encryption, two key pillars of web security. Enterprises spend huge amounts of money to procure and maintain SSL/TLS certificates. A typical enterprise has thousands of certificates protecting its data throughout the network.

All SSL/TLS digital certificates have a finite lifespan and are no longer deemed valid once they have expired. Certificates may have varying periods of validity and are often set to expire after anywhere between one and five years, depending on company policy and/or cost considerations. At a minimum, certificates need to be replaced at the end of their life to avoid service disruption and decreased security. However, there are a number of scenarios in which a certificate may need to be replaced earlier (e.g., Heartbleed bug, SHA-1 end-of-life migration, company mergers, change in company policy).

Maintaining an accurate accounting of SSL/TLS certificates is critical, but managing the entire lifecycle of SSL/TLS certificates, from initial procurement to eventual renewal and every step in between, is fraught with potential danger. Failure to properly manage all the moving pieces in a complex SSL/TLS environment can result in improperly configured or expired certificates. Enterprises can suffer revenue losses if an expired certificate causes an outage. Expired SSL/TLS certificates can also put an enterprise's network at risk and do lasting damage to the corporate brand.

Enterprises generally opt for a spreadsheet-based approach to managing SSL/TLS certificates. The certificate team maintains and updates the spreadsheet with certificate details on a regular basis, and monitors it for renewal, revocation, and other certificate-related activities. Because this approach is manual, it is error prone. A single miss can cause a huge revenue loss to an enterprise.

Given the finite lifespan of SSL/TLS certificates and their widespread use throughout an organization, there are numerous reasons to take a more holistic lifecycle management approach.

# Bottlenecks in the Certificate Lifecycle

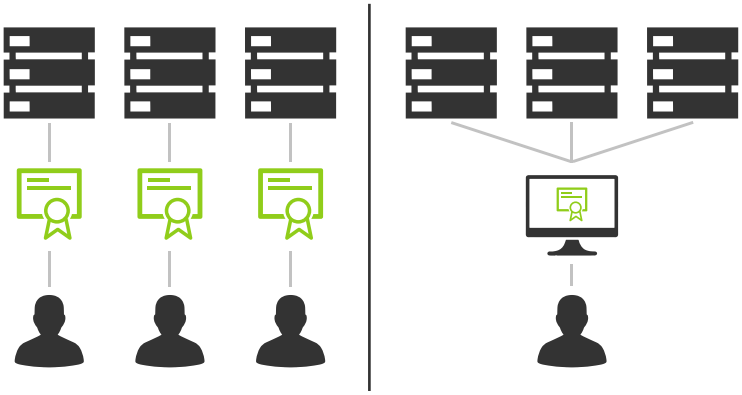
Every SSL/TLS certificate plays a crucial part in an enterprise security, so managing and monitoring SSL/TLS certificates is extremely important. Managing a couple of certificates does not require a specialized tool. However, things become tricky and quite complicated when an environment grows along with SSL/TLS certificates. When the count of SSL/TLS certificate crosses the double-digit mark, management becomes cumbersome and difficult. Enterprises typically experience the following problems when an SSL/TLS infrastructure goes beyond a few SSL/TLS certificates.

## Lack of discovery

As multiple SSL/TLS certificates are introduced into an enterprise along with newly rolled out applications, they become more difficult to track and manage, particularly if they're issued from different certificate authorities (CAs). An average-sized organization holds thousands of certificates. In most cases, enterprises do not know where these certificates are and how are they used. With minimal visibility, managing SSL/TLS infrastructure becomes a nightmare. If an enterprise is using a spreadsheet to track and manage SSL/TLS certificates, its process is purely manual and prone to errors. Even a small error in SSL/TLS certificate management can cost a fortune to an enterprise. A discovery tool that scans the environment on regular basis to build an inventory of SSL/TLS certificates can help organizations immensely in keeping track of SSL/TLS certificates.

## Manual management

It is not easy to manage multiple (single or multi-vendor) SSL/TLS certificates across a large organization. It quickly becomes even more complicated with multiple locations and divisions and the rapidly growing use of external, cloud-based services. Organizations must keep a track of the date of issuance and date of expiration to prevent any unplanned service disruption. When using multiple vendors, renewing, requesting, and revoking certificates can become bottlenecks. The certificate team generally logs into the corresponding vendor portal manually to work on certificates. This process is cumbersome and inefficient. An automated process can enable an organization to overcome these bottlenecks and inefficiencies.



## Inadequate reporting

Reporting is one of the key pillars of certificate lifecycle management. Expired SSL/TLS certificates can cause costly, disruptive outages that inflict long-term damage to an organization's reputation and business. To prevent outages, all SSL/TLS certificates must be discovered, managed, and continuously monitored. Organizations should be able to get periodic updates and reports about the SSL/TLS infrastructure. Updates and reports pertaining to certificates helps organizations gain complete visibility of their SSL/TLS infrastructure.

# Making Certificate Lifecycle Management Easy with AppViewX CERT+

AppViewX CERT+ provides a one-stop solution for automated discovery, expiration alerting, renewal, provisioning, and revoking of SSL/TLS certificates across networks. This includes servers and managed ADCs. It arms security operations and public key infrastructure (PKI) teams with critical insights to avoid unwanted outages and other issues associated with out-of-compliance certificates.

AppViewX has technology alliances with leading CAs, such as Entrust, Comodo, GoDaddy and Microsoft CA. This means CERT+ can directly talk to these CAs using their APIs. This unique ability provides enterprises a unified screen to track and manage SSL/TLS certificates issued by multiple CAs.

As part of the AppViewX suite, CERT+ has helped countless customers in discovering, managing and automating their SSL/TLS infrastructure. Its unique architecture and exposed APIs support integration with various IT service management systems.

## A one-stop solution for discovering and managing SSL/TLS certificates

Enterprises procure multiple certificates to keep their applications and infrastructure safe, which eventually results in having multiple untracked certificates. In the absence of a central authority that can discover and manage SSL/TLS certificates, management of SSL/TLS certificates becomes difficult and complex.

CERT+ leverages multiple methods for discovering and building a certificate inventory, including:

- **IP range:** A specific IP range can be fed to CERT+, which then runs a search query and discovers all the certificates that are present in this range.
- **Subnet mask:** A complete subnet mask can be entered in CIDR notation. CERT+ scans the specified subnet and discovers the certificates.
- **Managed devices:** AppViewX is an infrastructure management and automation utility suite. It can manage a wide variety of infrastructure solutions such as web servers and managed ADCs. CERT+ can talk to these managed devices directly to discover the certificates residing on them.
- **Direct upload:** CERT+ also provides an option to upload certificates directly. If certificates are present in a specific folder or in a central location, they can be directly uploaded to the CERT+ repository.

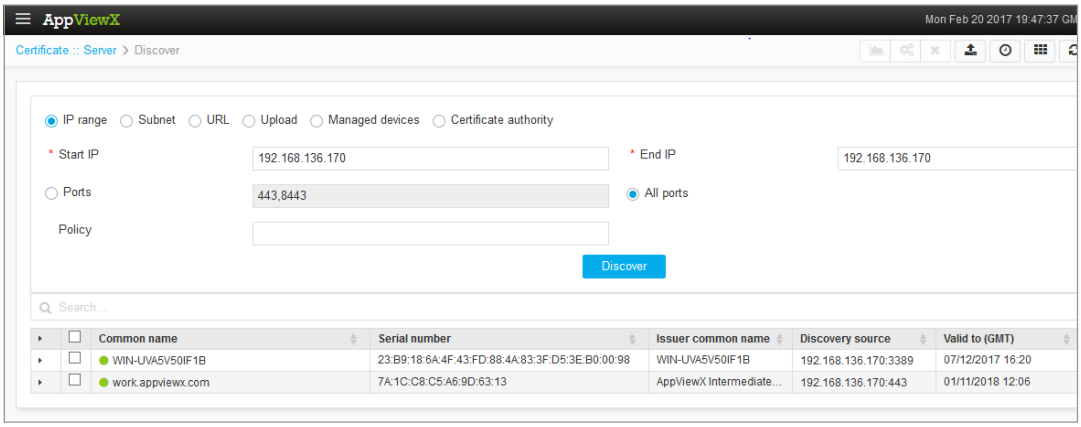



Figure-1

Once CERT+ discovers all the certificates, it builds a comprehensive inventory. It displays multiple attributes, such as CA name, date of issuance, date of expiration, algorithm, etc. This inventory is also interactive. It can be customized to add fields, including SAN, key usage, version, and others, to make it more informative as needed. The CERT+ inventory acts as a single point of contact to gather information about the SSL/TLS certificates present in an environment.

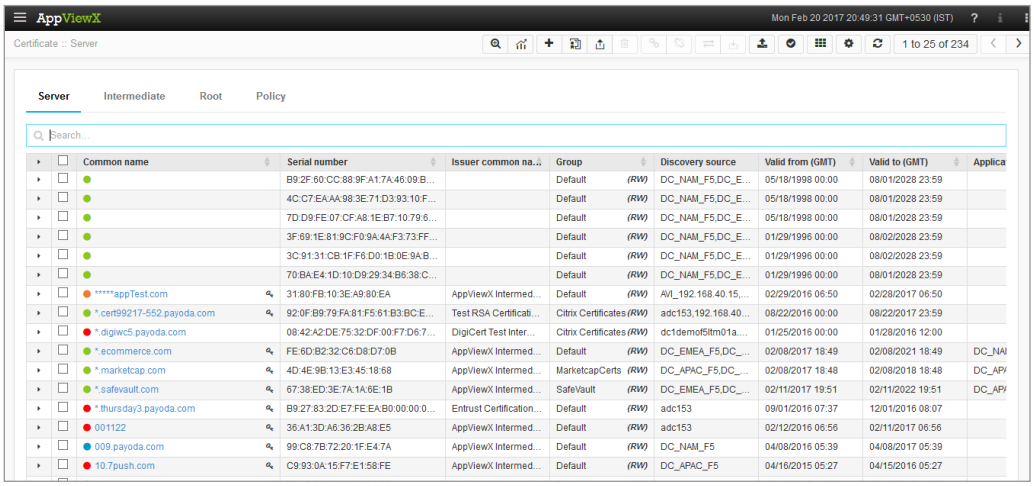



Figure-2

CERT+ also provides a scheduler-based discovery option. It can be configured to run SSL/TLS certificate discovery periodically. This feature is quite handy when enterprises procure SSL/TLS certificates often. CERT+ scans the network to detect newly added certificates and automatically adds them to the inventory.

## Certificate management automation

CERT+ automates the process of managing certificates and keys, greatly enhancing the efficiency of the process while dramatically reducing errors. It leverages a unique self-service and form-based approach to make SSL/TLS certificate lifecycle management effortless. It facilitates collaboration among cross-functional teams with a multi-stage workflow configuration system.

Simple self-service forms can be easily created in minutes and can be delegated to different teams for activities such as certificate issuance, renewal, and revocation. It can also integrate with various ITSM systems such as ServiceNow, BMC Remedy, and HP Service Manager. Integration with ITSM systems ensures that different teams follow standardized protocols for SSL/TLS certificate management.

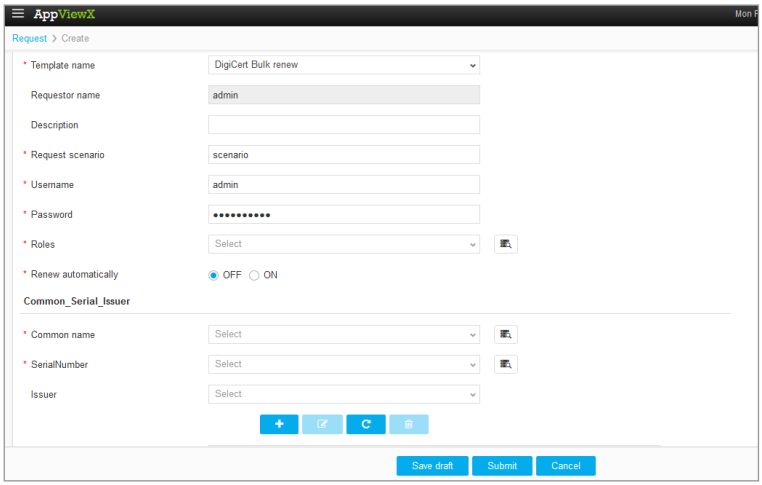



Figure-3

## Complete visibility with comprehensive reports and alerts

CERT+ provides comprehensive monitoring, reporting, and alerting capabilities that give organizations complete visibility into the SSL/TLS infrastructure. It empowers security teams with multiple reports based on various factors and parameters to achieve a granular level of visibility. Security teams can use these reports to understand how many certificates are about to expire or are already expired. It can also generate reports based on the specific CA. In an environment where multiple CAs are employed for issuing certificates, this provides valuable information on certificate counts. These reports can be exported as a PDF document and can be shared with different stakeholders at regular intervals.

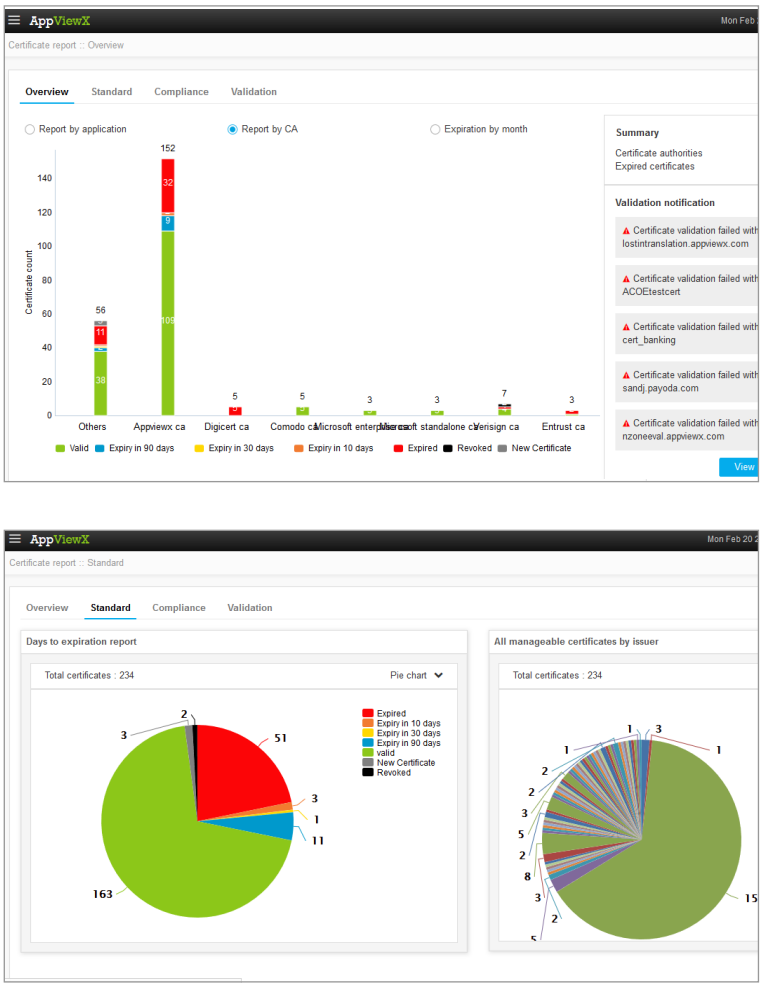



Figure-4

AppViewX CERT+ has a strong alerting mechanism as well. It can be configured to send out email alerts or SNMP traps for certificates based on their expiration. Security and compliance teams can leverage these alerts to be proactive and replace or renew revoked or expired certificates. This can save an organization thousands of dollars by preventing a sudden outage due to an expired or revoked certificate.

## Conclusion

Managing SSL/TLS certificates across complex infrastructures can be a manual, time-consuming, and error-prone process. Most CAs offer management tools for their certificates; however, they lack discovery tools for all certificates and require IT administrators to manage multiple platforms and logins for different certificates.

AppViewX CERT+ is a vendor-agnostic SSL/TLS management and automation solution. CERT+ provides a simple yet powerful platform to discover, manage, and automate SSL/TLS certificates. The solution enables security and compliance teams to automate critical tasks and reduce costs and minimize risks in managing SSL/TLS certificates across the enterprise.

### Learn more

An automation tool can help you achieve unlimited possibilities with limited resources. To learn more about our solutions, please visit **https://www.appviewx.com/products/cert.**

**About AppViewX**

AppViewX is a global leader in the management, automation and orchestration of network services in brownfield and greenfield data centers. The AppViewX Platform helps network operations (NetOps) adapt to technology and process demands, such as agile, DevOps, IoT, cloud, and software-defined infrastructure. AppViewX delivers greater business agility and efficiency at a lower cost.
For more information, visit www.appviewx.com.

**AppViewX Inc.,**
500 Yale Avenue North, Suite 100, Seattle, WA 98109

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226