Importance of Monitoring
SSL CERTIFICATES IN BUSINESS CRITICAL APPLICATIONS

How eG Enterprise can help avoid embarrassing outages caused by expired SSL certificates and detect security risks

An eG Innovations Technical White Paper

www.eginnovations.com

Total Performance Visibility

EXECUTIVE SUMMARY

Monitoring SSL certificates is critical to application success. Mission-critical systems can crash if SSL certificates expire.

IT organizations also need to monitor erroneous or unauthorized changes to SSL certificates to prevent security attacks and system outages. Given the business criticality of SSL certificates, manual tracking is not a viable option.

This white paper outlines the challenges involved in SSL certificate management and the solutions available as part of eG Enterprise to ensure a holistic security monitoring solution.

Many high-profile, externally facing and internally facing system outages are caused due to unplanned SSL certificate expiry.

WHY SSL CERTIFICATES?

SSL Certificates (also referred to as X.509 certificates) are very effective in protecting data in transit. The two key features include:

Encryption: SSL certificates ensure that sensitive information is encrypted when it is sent across the network. This ensures that only the intended recipient can understand it. The information you send on the Internet could be sensitive information such as credit card numbers, usernames and passwords. If this is not protected, hackers and phishers could steal that information.

Authentication: SSL certificates also provide authentication. This means that with the right SSL certificates in place, the user is assured that the information they send reaches the intended server and not to a malicious entity's server.

Figure 1 – Press reports reporting outages caused by expired SSL certificates

TYPICAL LIFE FOR AN SSL CERTIFICATE

The major certificate vendors (Symantec, Thawte, DigiCert etc.) issue certificates with a maximum validity of 2 or 3 years. If SSL certificates are not renewed, it will definitely have a negative security impact on websites and applications.

WHAT APPLICATIONS USE CERTIFICATES?

SSL certificates are used in a variety of applications across the enterprise:

- **Web Servers and Application Servers:** Servers such as IIS, Tomcat, Weblogic, Websphere and Glassfish use SSL to ensure web browsers communicate securely for safe transactions.

The major certificate vendors (Symantec, Thawte, DigiCert etc.) issue certificates with a maximum validity of 2 or 3 years.

- **Active Directory:** By default, LDAP communications are not encrypted. This could compromise security. Active Directory supports LDAP over SSL/TLS to ensure secure communication.

- **Exchange Server:** For Exchange Server, SSL is used to help secure email communications between the server and clients. Clients include mobile phones, computers both inside and outside the organization's network.

- **Databases:** For mission-critical applications that need to meet data security regulations, it is important to secure data transmitted across networks between instances of the database and applications. Databases such as Oracle, SQL Server and MySQL support SSL.

CONSEQUENCES OF EXPIRED SSL CERTIFICATES

An expired SSL Certificate in an enterprise environment could have severe impact.

- **Lost business and regulatory requirements non-compliance:** When an SSL certificate expires, customers will be presented with a warning messages as shown in Figure 2. The experience varies based on the browser. If customers visit a website and have any concerns about whether their private data is secure, they will abandon their transaction and stop visiting the website. This may also result in noncompliance with regulatory or other requirements.

  The resulting impact is that businesses start to lose many customers. The corporate brand and reputation is adversely affected putting the business at risk.

- **Increase in customer support costs:** Customers who have concerns about a website's security and choose to call customer support will increase the burden on your customer support team and divert focus from high-value customer calls.

- **Personal information at risk from man-in-the-middle attacks:** In a phishing attack, a hacker assumes the identity of your business, taking advantage of expired SSL Certificates and creates a fake website that looks similar to the actual site. Customers will then enter confidential information, such as credit card or social security numbers, on this phishing site thereby feeding data directly to the hacker, who may in turn sell it to other criminals.

- **IT departments are put under pressure:** Employees who see warnings will often contact IT department staff for help in resolving the issue. This can add a significant burden to IT departments that are already overwhelmed.

> "The ease of acquiring SSL Certificate has encouraged phishers and other malicious entities to use them in establishing their online 'credibility'"
>
> – Instant SSL by Comodo

Figure 2 – Negative user experience in various browsers due to expired SSL certificates

THE PAIN OF CERTIFICATE MONITORING

- **Reactive:** Many organizations usually notice SSL certificates expiry only after it happens. This results in disruption and lost revenue.

- **Lack of control:** Sometimes, within organizations, teams deploy their self-signed certificates. While self-signed certificates are a quick way of proving a concept, it would be disastrous to deploy them in production.

- **Too many certificates:** Most organizations

find it difficult to keep track of how many certificates exist and on which servers they are deployed. According to a recent survey by Venafi, a leading security provider, organizations anticipate a 27% year-over-year certificate and key inventory growth rate.

- **Error-prone manual processes and personnel turnover:** System administrators often track certificates in spreadsheets and reminder notes. When this person parts ways with the organization, the SSL certificate expiry checking process is at the mercy of the knowledge transfer handoff (if it happened at all). This problem is especially acute for smaller organizations where the knowledge transfer process may not be well defined or is informal.

Figure 3 – SSL certificates are often tracked using reminder notes

> "Enterprises with hundreds of SSL Certificates from several different providers could lose track of certificates in their environment. When this happens, certificates could expire and go unnoticed for months, leaving website visitors vulnerable to hackers"
>
> **– Verisign White paper,**
> "Why SSL Certificate Management Is Critical"

According to Venafi, 85% of organizations manage encryption certificates and private keys man ally via spreadsheet and reminder notes. These choices are error-prone and often result in system outages.

Most organizations rely on spreadsheet-based tracking methods and manual processes to keep track of certificates, resulting in increased exposure to risks.

– Gartner report findings,
"X.509 Certificate Management: Avoiding Downtime and Brand Damage"

HOW eG ENTERPRISE HELPS WITH SSL CERTIFICATE MONITORING

Proactive monitoring of the validity of your SSL certificate

eG Enterprise provides proactive alerting on the SSL certificate validity based on a configurable threshold (days in advance before the SSL certificates' expiration date).

The following default alerting thresholds are available out-of-the-box for a quick setup experience (all of which are configurable):

- Minor alert: 30 days remaining validity.
- Major alert: 20 days remaining validity.
- Critical alert: 10 days remaining validity.

Multi-modal alerting is available out-of-the-box with eG Enterprise:

- Alerts on the eG Enterprise Web Console
- Email Alerts
- Text message (SMS) notifications
- Trouble tickets directly opened in your helpdesk system

Figure 4 shows the alerts in the eG Enterprise Alarm Console that allow the Administrators to keep track of and actionize SSL certificate replacement.

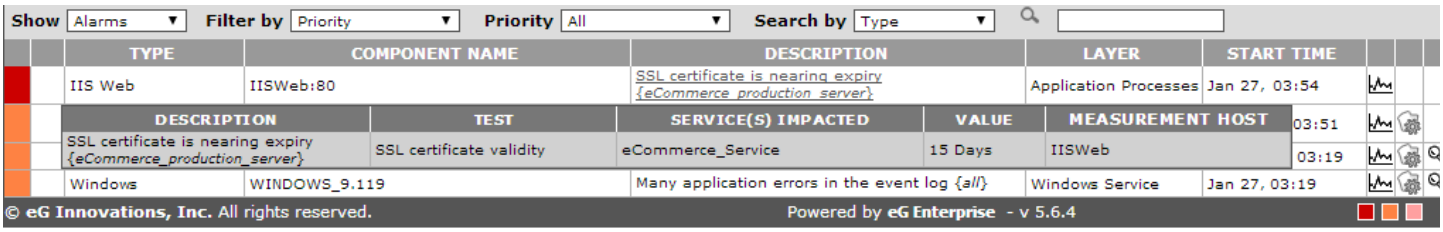


Figure 4 – Alerts on SSL Certificate Validity in the eG Enterprise Alarm Console

Figure 5 shows the email alerts generated by eG Enterprise that make it easy to keep track of SSL certificate validity.

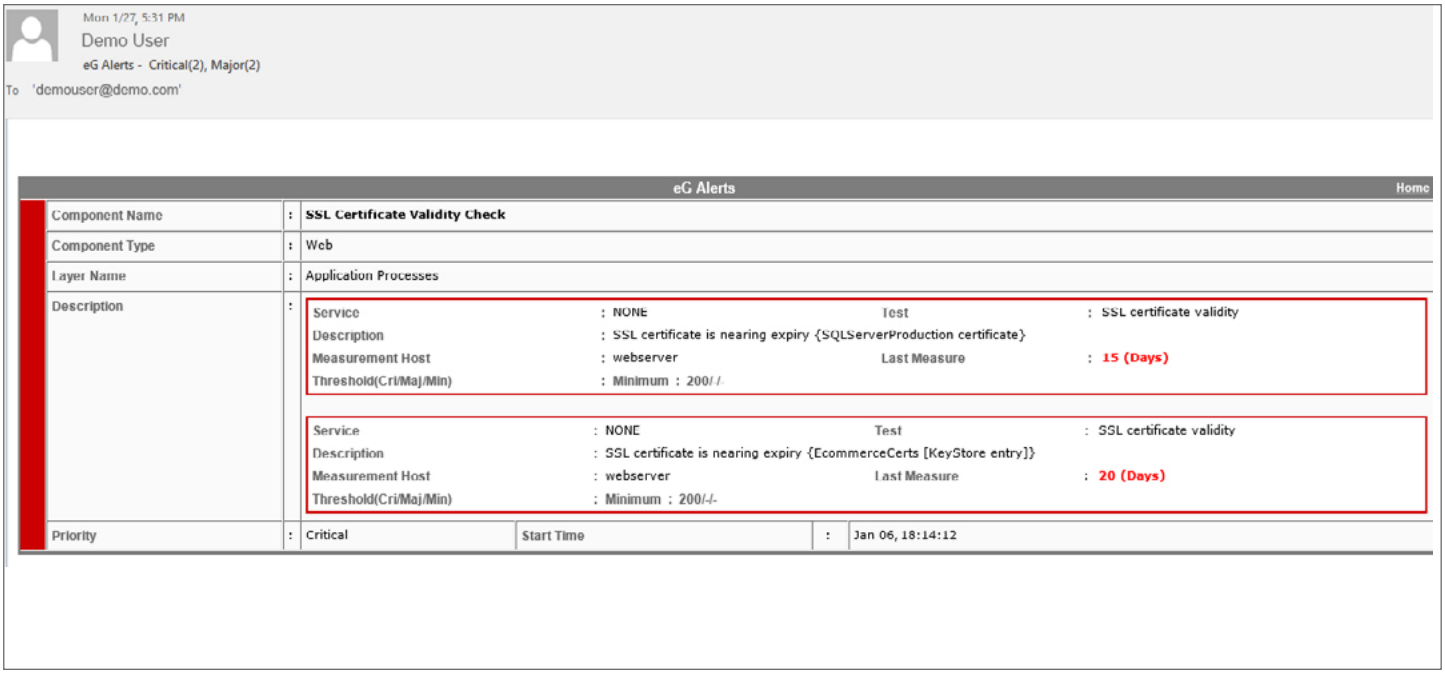


Figure 5 – Email Alerts on SSL Certificate Validity

eG Enterprise comes with pre-configured, visually intuitive and rich graphical dashboards. Flexible authentication options and configurable refresh frequencies make it ideal for NOC-style monitoring on LED monitors.

Figure 6 shows a pre-configured dashboard for SSL certificates that makes it easy to track SSL certificate validity across systems throughout the enterprise.

Track SSL certificate changes to prevent erroneous or unauthorized changes

A typical enterprise could have may have hundreds or even thousands of servers with SSL certificates installed on them. Traditionally, changes to such configuration items are tracked manually (think excel spreadsheets) making it tedious and error-prone.

Improper / unauthorized changes to SSL certificates

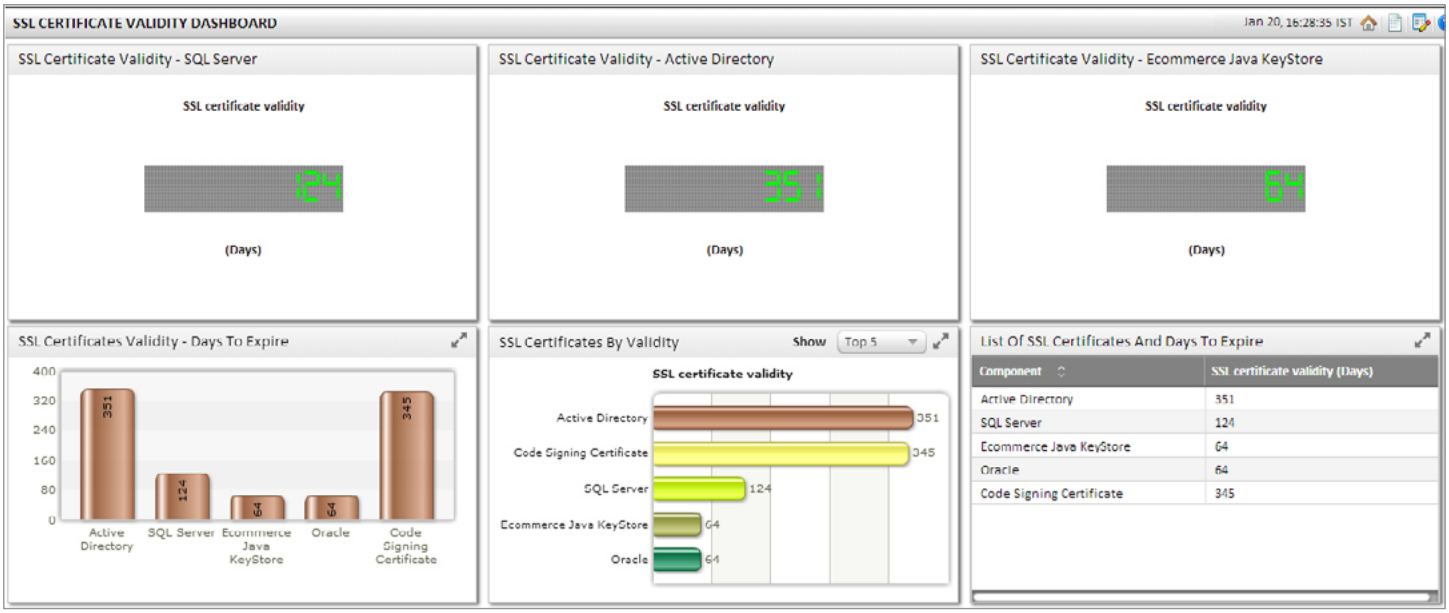


Figure 6 – SSL Certificate Validity Dashboard in eG Enterprise

may also cause system outages. It is therefore essential for administrators to track the SSL certificate changes effected in an IT environment on a regular basis so that, erroneous changes can be promptly identified and rolled back.

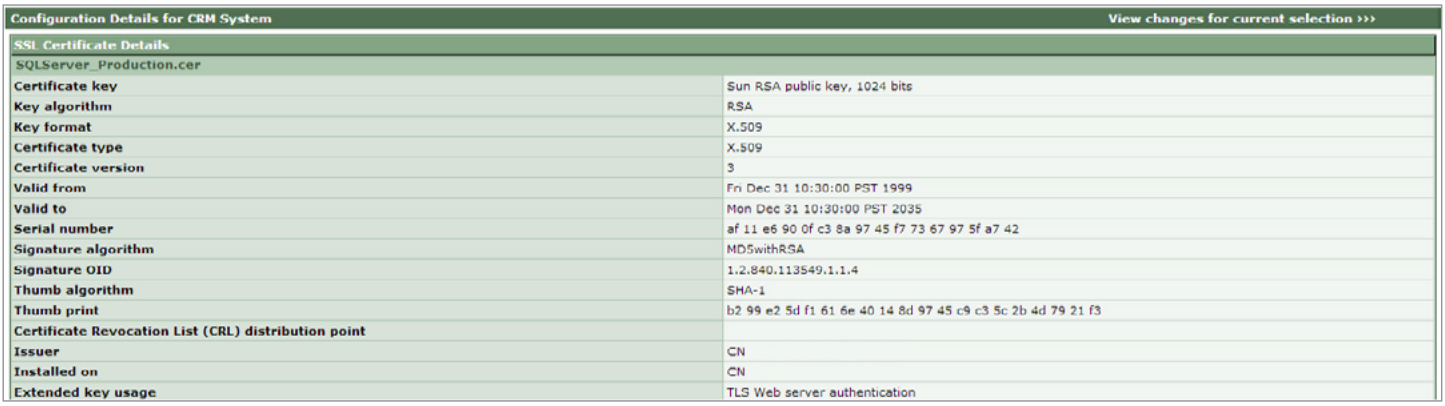
To enable administrators to efficiently monitor SSL certificate changes and easily view what was changed and when, eG Enterprise Configuration Management console provides intuitive interfaces.

eG Enterprise makes it easy to visualize and track the number of changes in SSL certificates throughout the enterprise rather than having to maintain such information in manually through tedious excel spreadsheets.

Figure 7 shows the eG Enterprise Configuration Management console showing full details of an SSL certificate making it easy to view the information during troubleshooting scenarios.

eG Enterprise assures the legitimacy of the certificate. If there is a discrepancy, eG Enterprise will immediately send multi-modal alarms to your security team to get instantly notified and engaged in order to remediate the situation.

Figure 8 shows the eG Enterprise Configuration Management Dashboard that makes it easy to visualize the number of changes in SSL certificates. This makes it easy to track changes to SSL certificates throughout the enterprise rather than having to maintain such information in tedious excel spreadsheets.



Configuration Details for CRM System	View changes for current selection ›››
SSL Certificate Details	
SQLServer_Production.cer	
Certificate key	Sun RSA public key, 1024 bits
Key algorithm	RSA
Key format	X.509
Certificate type	X.509
Certificate version	3
Valid from	Fri Dec 31 10:30:00 PST 1999
Valid to	Mon Dec 31 10:30:00 PST 2035
Serial number	af 11 e6 90 0f c3 8a 97 45 f7 73 67 97 5f a7 42
Signature algorithm	MD5withRSA
Signature OID	1.2.840.113549.1.1.4
Thumb algorithm	SHA-1
Thumb print	b2 99 e2 5d f1 61 6e 40 14 8d 97 45 c9 c3 5c 2b 4d 79 21 f3
Certificate Revocation List (CRL) distribution point	
Issuer	CN
Installed on	CN
Extended key usage	TLS Web server authentication

Figure 7 – eG Enterprise Configuration Management console

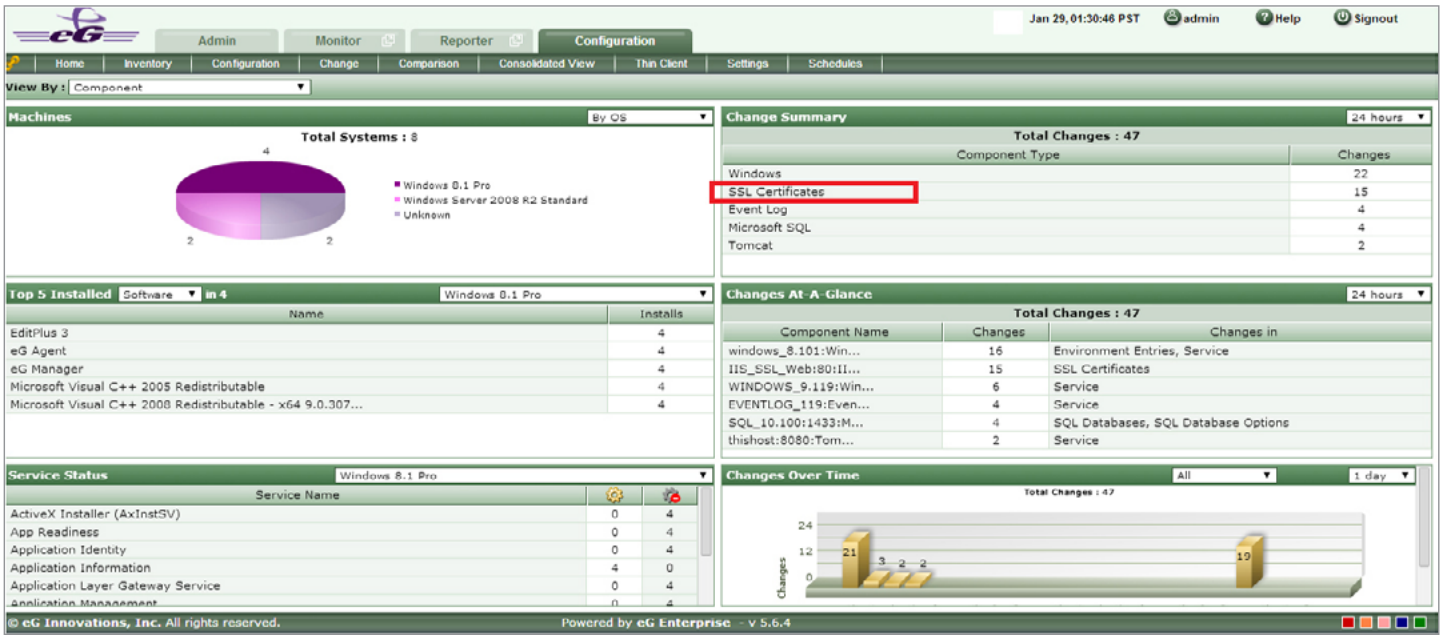
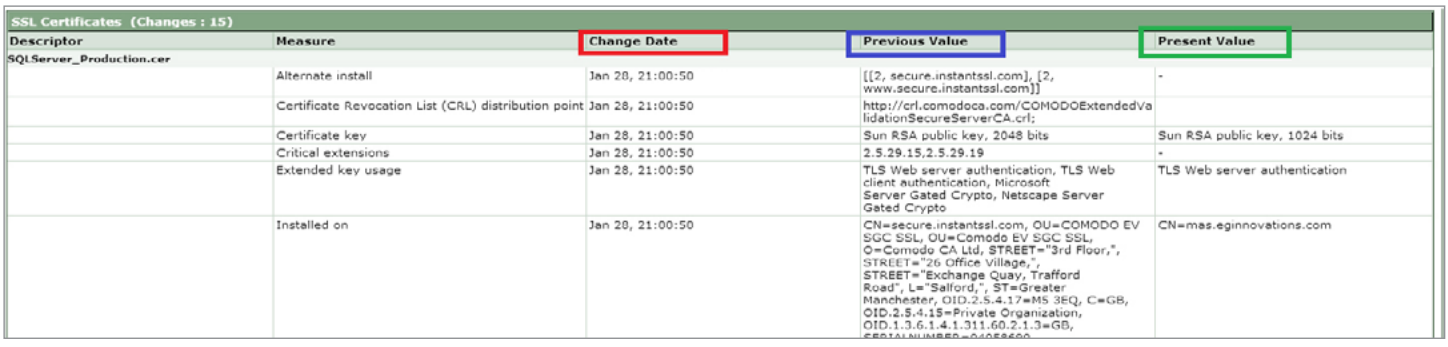


Figure 8 – eG Enterprise Configuration Management Dashboard

Figure 9 shows the specific change tracking for a given SSL certificate. In the following example, an administrator replaced a SQL Server production certificate. eG Enterprise Configuration Management change tracking makes it easy to visualize the specific change and ensure that it was made as intended.



SSL Certificates (Changes : 15)				
Descriptor	**Measure**	**Change Date**	**Previous Value**	**Present Value**
SQLServer_Production.cer				
	Alternate install	Jan 28, 21:00:50	[[2, secure.instantssl.com], [2, www.secure.instantssl.com]]	-
	Certificate Revocation List (CRL) distribution point	Jan 28, 21:00:50	http://crl.comodoca.com/COMODOExtendedValidationSecureServerCA.crl;	
	Certificate key	Jan 28, 21:00:50	Sun RSA public key, 2048 bits	Sun RSA public key, 1024 bits
	Critical extensions	Jan 28, 21:00:50	2.5.29.15,2.5.29.19	-
	Extended key usage	Jan 28, 21:00:50	TLS Web server authentication, TLS Web client authentication, Microsoft Server Gated Crypto, Netscape Server Gated Crypto	TLS Web server authentication
	Installed on	Jan 28, 21:00:50	CN=secure.instantssl.com, OU=COMODO EV SGC SSL, OU=Comodo EV SGC SSL, O=Comodo CA Ltd, STREET="3rd Floor,", STREET="26 Office Village,", STREET="Exchange Quay, Trafford Road", L="Salford,", ST=Greater Manchester, OID.2.5.4.17=M5 3EQ, C=GB, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=GB,	CN=mas.eginnovations.com

Figure 9 – eG Enterprise Configuration Management changes

Detect SSL man-in-the-middle attacks

A man-in-the-middle exploit is one in which a hacker impersonates the server and then exchanges his fake SSL certificate with the customer. This allows the hacker to intercept confidential information such as account numbers and passwords.

eG Enterprise uses SSL certificate fingerprint to assure the legitimacy of the certificate. The fingerprint is a hash value computed over the complete certificate, which includes all its fields, including the signature.
As part of the SSL configuration process (see Figure 10), eG Enterprise dynamically fetches the fingerprint and will seek confirmation on whether the fingerprint is accurate. Once confirmed by the administrator, eG Enterprise will continually compare the correct SSL certificate fingerprint that you specify, to the live one being used on your servers every few mins.

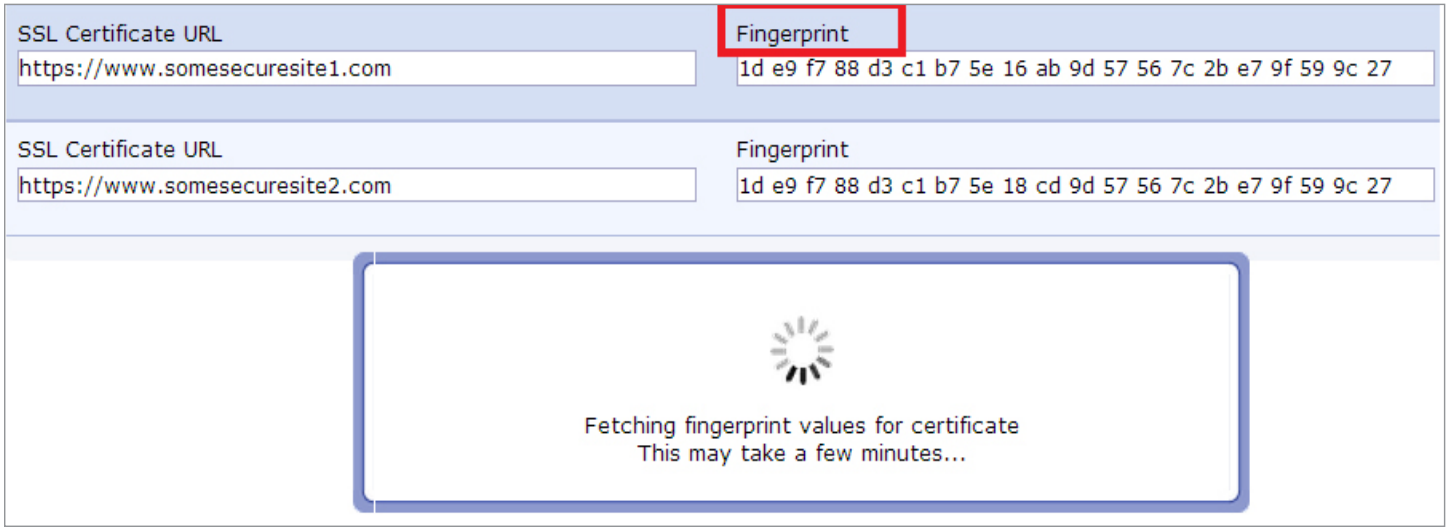


Figure 10 – Specifying the fingerprint value for an SSL certificate

If there is a discrepancy in the fingerprint, eG Enterprise will immediately send multi-modal alarms thus enabling your security team to get instantly notified and engaged in order to remediate the situation.

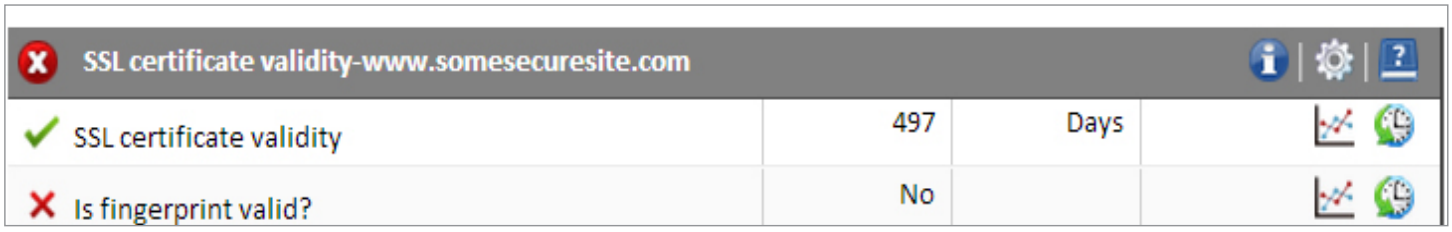


Figure 11 – eG Enterprise Console showing fingerprint validity for an SSL certificate

TYPES OF SSL CERTIFICATES AND APPLICATIONS SUPPORTED BY EG ENTERPRISE

eG Enterprise can monitor SSL certificates across a breadth of applications across the enterprise as well as depth in various types of certificates. eG Enterprise also supports a variety of SSL certificate file formats.

Applications (for which SSL certificate monitoring is supported):

- Web Servers and Application Servers: Servers

such as IIS, Tomcat, Weblogic, Websphere and Glassfish

- LDAP systems such as Active Directory
- Exchange Server
- Databases such as Oracle, SQL Server and MySQL

eG Enterprise monitors various types of certificates. These are outlined in Figure 12.

> "Since the man-in-the-middle can forward all communications back and forth, the web site appears authentic to the Internet user…If the user is to be protected against this attack, then it's crucial to ensure that there is a meaningful way to verify whether the key is correct or not"
>
> **– Seth Schoen**,
> Technologist for the Electronic - Frontier Foundation

Type of Certificate	Description
Public Certificates	Public Certificates hosted on Webservers or AppServers.
Code signing /Digital signing certificates	Code signing certificates are digital certificates that will help protect users from downloading compromised files or applications.
Adobe CDS signing certificates	Adobe® Certified Document Services (CDS) provides recipients with assurances that certified PDF documents are authentic.
SAN certificates (Subject Alternative Names)	Subject Alternative Names let you protect multiple host names with a single SSL certificate.
Email certificates	Email certificates provide the strongest levels of confidentiality and security for your electronic communications by allowing you to digitally sign and encrypt your mail and attachments.
Extended Validation (EV SSL) certificates	EV certificates are provided by Certificate Authorities by putting applicants through rigorous evaluation procedures to ensure their legitimacy.
Root signing certificates	Suitably qualified organizations can use root signing certificates to issue digital certificates which chain up to a publically trusted Root Certificate.
Company internal self-signed certificates	Used in test and development servers where security is not a big concern. It is considered bad practice to use self-signed certificates especially for public facing sites.

Figure 12 – Types of SSL Certificates supported by eG Enterprise

SSL Certificate file formats (and extensions) supported by eG Enterprise:

- DER encoded binary X.509 (.CER or .CRT)
- Base-64 encoded X.509 (.CER or .CRT)
- Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)
- Personal Information Exchange – PKCS #12 (.PFX or .p12)

IMPLEMENTING SSL CERTIFICATE MONITORING WITH EG ENTERPRISE

eG Enterprise provides both Agentless and Agent-based monitoring for SSL certificates.

- **Agentless:** For public certificates hosted on Web Servers/ Application Servers, agentless monitoring is a good fit. With this approach, remote SSL certificate monitoring is possible where a central data collector will remotely connect to a server and monitor the properties of the SSL certificate.

- **Agent-based:** For other types of certificates including private certificates, "file based monitoring" requires an agent to perform internal monitoring of SSL certificates installed on the server. In addition, all of the capabilities that apply for agentless monitoring also apply for agent-based monitoring.

SUMMARY

Monitoring SSL certificates is extremely critical for business continuity. Encryption has become ubiquitous and enterprises are experiencing surging encryption volumes. Given this context, manual tracking of SSL certificates is not a viable option. It is tedious, error-prone and exposes the enterprise to unnecessary risk and outages. In addition, enterprises are ill-prepared for security risks such as man-in-the-middle attacks.

eG Enterprise provides a holistic and cost-effective security monitoring solution for tracking SSL certificates and detecting security risks. With intuitive management capabilities and deep visibility into certificates across the enterprise, eG Enterprise makes it easy to manage SSL Certificates.

ABOUT eG INNOVATIONS

eG Innovations provides intelligent performance management solutions that dramatically accelerate the discovery, diagnosis, and resolution of service performance issues in virtual, cloud, and physical service infrastructures. Only eG Innovations offers 360-degree service visibility with automated, virtualization-aware performance correlation across every layer and every tier - from desktops to applications and from network to storage. This unique approach delivers deep, actionable insights into the true causes of cross-domain service performance issues and enables administrators to pre-emptively detect, diagnose and fix root-cause issues - before end users notice.

eG Innovations' award-winning performance management and monitoring solutions are trusted by the world's most demanding companies to enable delightful user experiences, keep mission-critical business services at peak performance and deliver on the ROI promise of transformational IT investments. Customers include: JP Morgan Chase, Citigroup, Depository Trust and Clearing Corporation, Cathay Bank, Allscripts, Honeywell, Samsung, Xerox, Marathon Oil and many more.

To learn more visit www.eginnovations.com