ManageEngine
EventLog Analyzer

EventLog Analyzer:

GUIDE TO INSTALL SSL CERTIFICATE

www.eventloganalyzer.com

Contents

Document Summary

The purpose of this document is to guide you through the process of securing EventLog Analyzer with SSL certification. In doing so, you can ensure that the connection between users' web browser and EventLog Analyzer is secure from various threats including data theft. This document covers:

- An overview of EventLog Analyzer
- Need for SSL Certification
- Steps to enable SSL

EventLog Analyzer Overview

EventLog Analyzer is an IT compliance and SIEM solution for your network. Its features include:

- Collects, analyzes, and archives log data from sources across your physical, virtual, cloud environments.
- Provides a vast range of predefined reports, and the freedom to design custom reports that help meeting your specific needs.
- Generates real time alerts so you can combat potential security threats.
- Helps you meet all mandatory IT compliance requirements.
- Securely archives your logs, and has a powerful search engine that facilitates in-depth forensic analyses.

Why do you need SSL Certification?

EventLog Analyzer is a web-based solution which offers access to its various features from any host on the network. To secure the connection between the users' web browser and the EventLog Analyzer server, the connection between these two entities must be secured.

Secure Sockets Layer (SSL) is the de facto standard on the web for establishing an encrypted link between a server and a web browser. It ensures that all data transferred between the server and the browser remains secure.

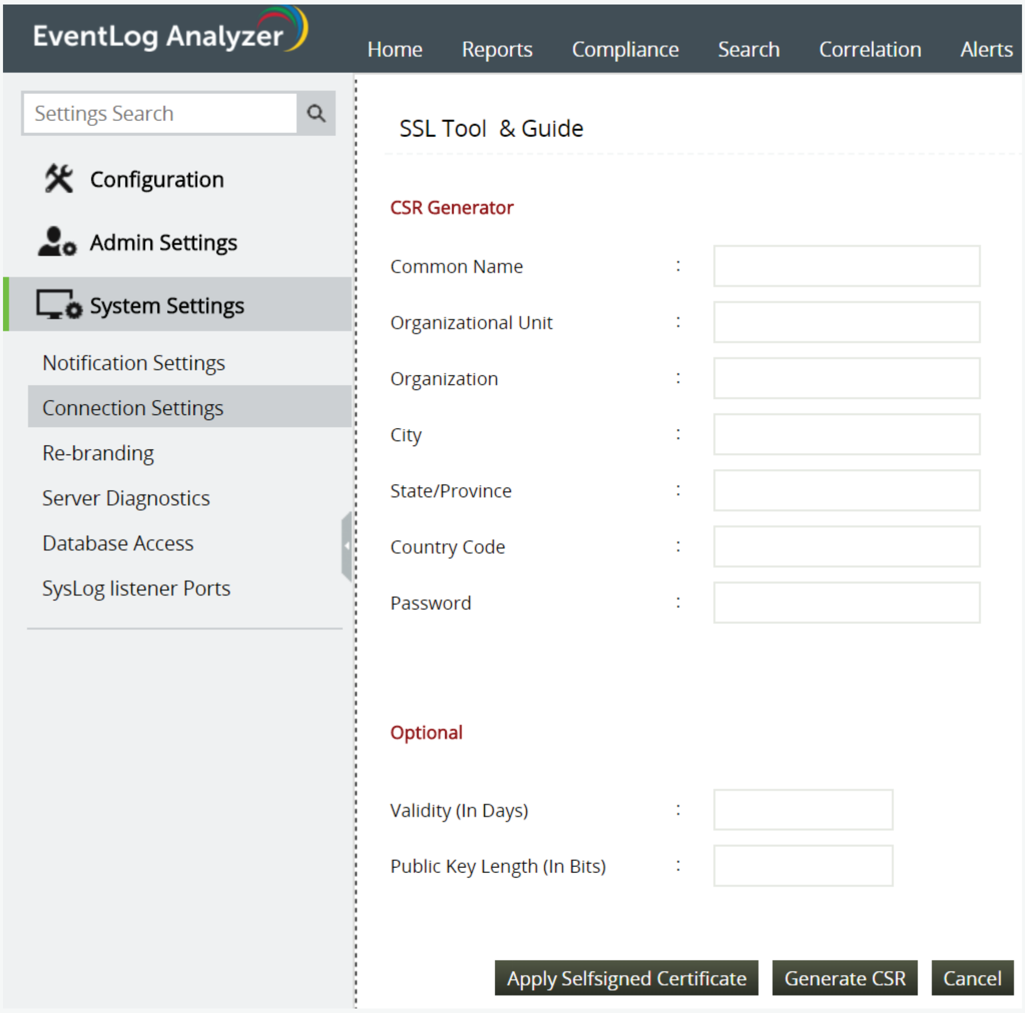
Steps for enabling SSL

The following steps will guide you through the process for enabling SSL in EventLog Analyzer:

Step 1: Generate CSR and submit it to your certifying authority

- Log in to EventLog Analyzer using admin credentials.
- Go to the **Settings Tab > System Settings > Connection Settings > Configure Connections.**
- Select the **Enable SSL Port [https]** checkbox and click on the SSL Certification Tool button.
- The SSL Tool and Guide page opens. Enter the required details in the form provided:

Common Name	The NetBIOS or FQDN name of the server in which EventLog Analyzer is running.
Organizational Unit	The department name that you want to appear in the certification.
Organization	Provide the legal name of your organization.
City	Enter the city name as provided in your organization's registered address.
State/Province	Enter the State/Province as provided in your organization's registered address.
Country Code	Provide the 2-letter code of the country your organization is located in.
Password	Enter a password of atleast 6 characters.
Validity	Specify the number of days the certificate will be valid. If no value is provided, the validity is taken as 90 days.
Public Key Length	Provide the public key length. Larger the length, stronger the key. Default size is 1024 bits. The length should be a multiple of 64.



SSL Tool & Guide

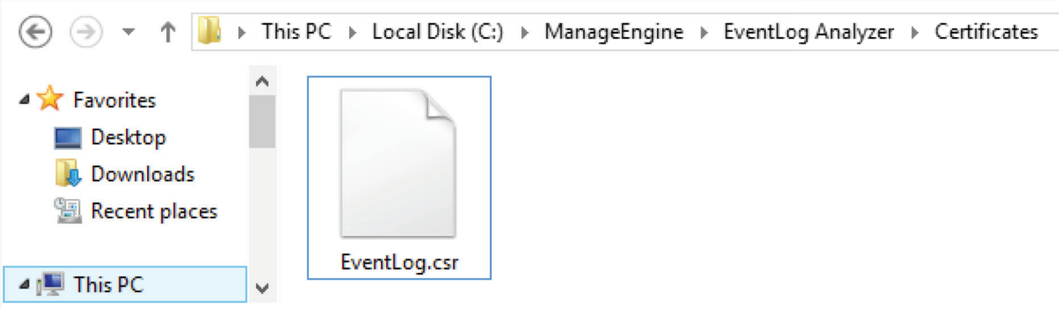
CSR Generator

Common Name	:	
Organizational Unit	:	
Organization	:	
City	:	
State/Province	:	
Country Code	:	
Password	:	

Optional

Validity (In Days)	:	
Public Key Length (In Bits)	:	

- Once you have entered the details, click on **Generate CSR.**
- Submit the CSR file to your certifying authority (CA). You can locate the CSR file at **<EventLog Analyzer installation directory>\Certificates.**



This PC ▸ Local Disk (C:) ▸ ManageEngine ▸ EventLog Analyzer ▸ Certificates
Favorites
Desktop
Downloads
Recent places
This PC
EventLog.csr

Step 2: Add the CA signed certificates to the keystore

- Unzip the certificates returned by your CA to the following path: <EventLog Analyzer installation directory>\jre\bin.
- Open the command prompt and navigate to the path <EventLog Analyzer installation directory>\jre\bin.
- Run the commands corresponding to your certifying authority:

For GoDaddy certificates:

```
keytool -import -alias root -keystore Eventlog.keystore -trustcacerts -file gd_bundle.crt
```

```
keytool -import -alias cross -keystore Eventlog.keystore -trustcacerts -file gd_cross.crt
```

```
keytool -import -alias intermed -keystore Eventlog.keystore -trustcacerts -file gd_intermed.crt
```

```
keytool -import -alias tomcat -keystore Eventlog.keystore -trustcacerts -file Eventlog.crt
```

For Verisign certificates:

```
keytool -import -alias intermediateCA -keystore Eventlog.keystore -trustcacerts -file
<your intermediate certificate>.cer
```

```
keytool -import -alias tomcat -keystore Eventlog.keystore -trustcacerts -file Eventlog.cer
```

For Comodo certificates:

```
keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore
Eventlog.keystore
```

```
keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore
Eventlog.keystore
```

```
keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore
Eventlog.keystore
```

```
keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore
Eventlog.keystore
```

For Entrust certificates:

```
keytool -import -alias Entrust_L1C -keystore Eventlog.keystore -trustcacerts -file entrust_root.cer
```

```
keytool -import -alias Entrust_2048_chain -keystore Eventlog.keystore -trustcacerts -file entrust_2048_ssl.cer
```

```
keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name>.cer
```

For Thawte certificates:

Purchased directly from Thawte

```
keytool -import -trustcacerts -alias tomcat -file <certificate-name>.p7b -keystore Eventlog.keystore
```

Purchased through the Thawte reseller channel

```
keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA>.cer -keystore Eventlog.keystore
```

```
keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA>.cer -keystore Eventlog.keystore
```

```
keytool -import -trustcacerts -alias tomcat -file <certificate-name>.cer -keystore Eventlog.keystore
```

Note: If your certifying authority is not in the list provided above, please contact them to get the commands required to add their certificates to the keystore.

Step 3: Bind the certificates with EventLog Analyzer

This configures the EventLog Analyzer server to use the keystore with your SSL certificate.

Similar to **Step 1,**

- Go to the **Settings Tab > System Settings > Connection Settings > Configure Connections.**
- Select the **Enable SSL Port [https]** checkbox and click on the **SSL Certification Tool** button.
- The SSL Tool and Guide page opens. Enter the required details in the form provided.
- Once you have entered the details, click on Apply Selfsigned Certificate.

Glossary

SSL

Acronym for Secure Socket Layer, SSL is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say submits his credit card information, the data travels to the server as plain text, which is susceptible to data theft. On the other hand if this data is encrypted, then no eavesdropper can read it. Thus, it's very important to secure a website with SSL.

SSL Certificate

This is a digital identity of a company, which ensures that a visitor is talking only to its intended website and whatever data he submits to the site is encoded and reaches only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end-users) are programmed to trust these CA presented certificates.

Certifying Authority

Regulatory organizations, with the help of standard policies, issue certificates to a domain declaring it trustworthy. Every certificate they generate is unique to the company they are certifying, which makes identification easy. CAs secure all necessary information about a company before issuing a certificate for it and also keep updating it in their records, which adds to the trustworthiness. Some of the popular CAs are Verisign, Comodo & GoDaddy.

CSR

In order for a CA to generate an SSL certificate for a company, it first collects the information about the company and other identifiers such as public key (digital signature), and then binds them all with its certificate (which could be an encrypted token or something similar). In doing so, it generates a unique identifier for the company. Thus every certificate issuance process begins with a "certificate request" from the company. Certifying Authorities refer to this process as "Certificate Signing Request". The Certifying Authorities accept the company information and digital signatures in a special form of file - the ".csr" file.

Keystore

Keystore is specifically designed to store various kinds of encryption information.

What's New in

EventLog Analyzer?

Stay up to date with our latest features, upcoming releases, events, and blogs.

Learn more

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

About EventLog Analyzer

EventLog Analyzer is a comprehensive IT compliance and log management software for SIEM. It provides detailed insights into your machine logs in the form of reports to help mitigate threats in order to achieve complete network security. https://blogs.manageengine.com/eventloganalyzer

$ Get Quote

Download

30-day trial and try this feature now.