ManageEngine
EventLog Analyzer

EventLog Analyzer

GUIDE TO INSTALL SSL CERTIFICATE

www.eventloganalyzer.com

Table of Contents

Purpose of the document

This document guides you through the process of securing EventLog Analyzer with SSL certification. By doing this, you can ensure that the connection between users' web browser and EventLog Analyzer is secure from various threats including data theft.

Need for 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.

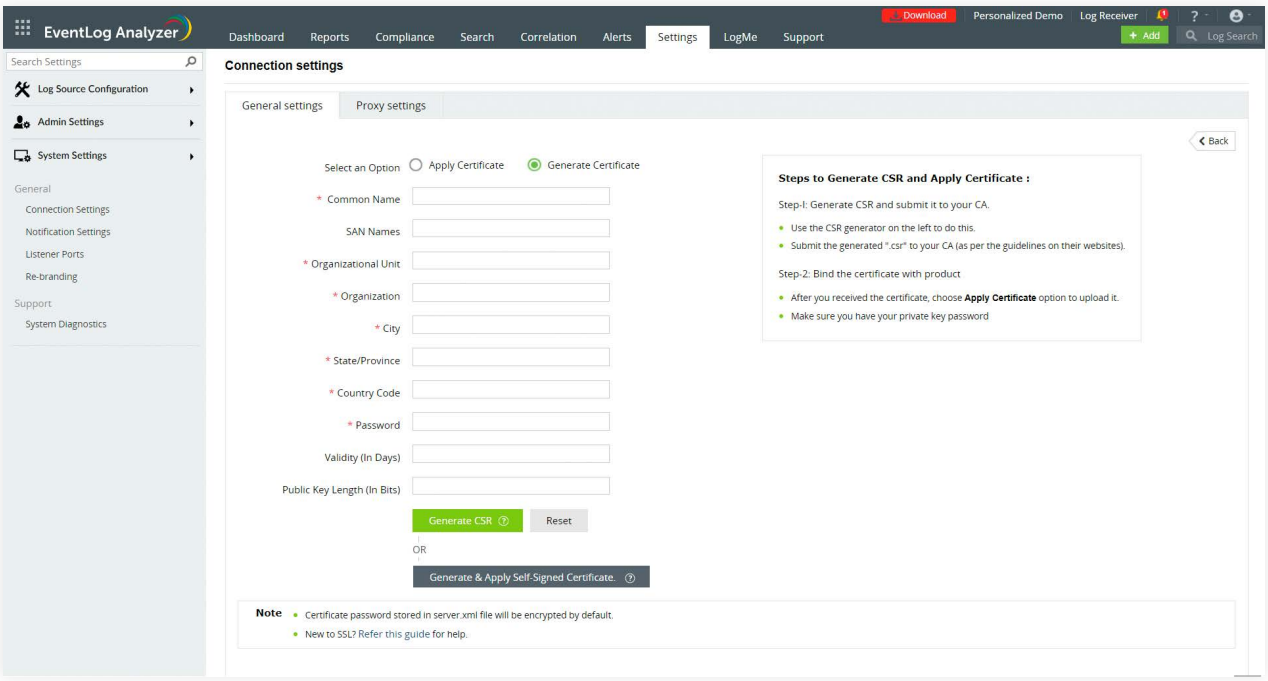
Steps for enabling SSL

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

To apply for a new SSL certificate, you will have to generate a Certificate Signing Request (CSR) and submit it to the Certifying Authority (CA). To do so, follow the given steps.

- Log in to EventLog Analyzer using admin credentials.
- Go to the **Settings Tab > System Settings > Connection Settings > General Settings.**
- Select the **Enable SSL Port [https]** checkbox and click on the SSL Certification Tool button.
- The SSL Tool and Guide page opens. Select **Generate Certificate** to bring up the form below.



- Enter the required details in the form using the table below as a guide.

Common Name	The NetBIOS or FQDN name of the server in which EventLog Analyzer is running.
SAN Names	The domain names and IP addresses which are secured by the certificate
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.

- After all values have been entered, you can select either of these two options:
- **Generate CSR:**

  This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.

  1. Click Download CSR or manually get it by going to the <Install_dir>\Certificates folder.
  2. Once you have received the certificate files from your CA, you can apply the SSL certificate.

- **Generate & Apply Self-Signed Certificate:**

  This option allows you to create a self-signed certificate and apply it instantly in the product.

Step 2: Apply Certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

- Log in to EventLog Analyzer using admin credentials.
- Go to the **Settings Tab > System Settings > Connection Settings > General Settings.**
- Select the **Enable SSL Port [https]** checkbox and click on the SSL Certification Tool button.
- The SSL Tool and Guide page opens. Select **Apply Certificate.**
- In the Apply Certificate to drop-down, select the component for which you want to apply the SSL certificate.
- Choose an Upload Option based on the certificate file type.
- **ZIP upload:**

  i. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.

  ii. If your CA has sent you individual certificate files—user, intermediary, and root certificates, then you can put all these certificate files in a ZIP file and upload it.

- **Individual Certificates:**

  i. If your CA has sent you just one certificate file (PFX or PEM format), then select the Individual Certificate, and upload the file.

  ii. If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.

  iii. If you have a CA bundle containing the root and intermediate files along with the SSL certificate of the domain, you can upload it too.

- **Certificate Content:**

  i. If your CA has sent just the certificate content, then choose Certificate Content option, and paste the entire content.

- If the certificate file requires a password, then enter it in the Certificate Password field. Or, if the certificate contains a password-protected private key, enter the password in the Private Key Passphrase field.
- Click **Apply.**
- Finally, restart EventLog Analyzer.

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 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.

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-time services 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.

Our Products

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus | DataSecurity Plus | SharePoint Manager Plus

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. blogs.manageengine.com/eventloganalyzer

$ Get Quote Download