

Steps to apply **SSL CERTIFICATE** and enable HTTPS



Purpose of the document

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.

This document shows how to secure the communication between users' web browsers and the Log360 server by applying an SSL certificate and enabling HTTPS

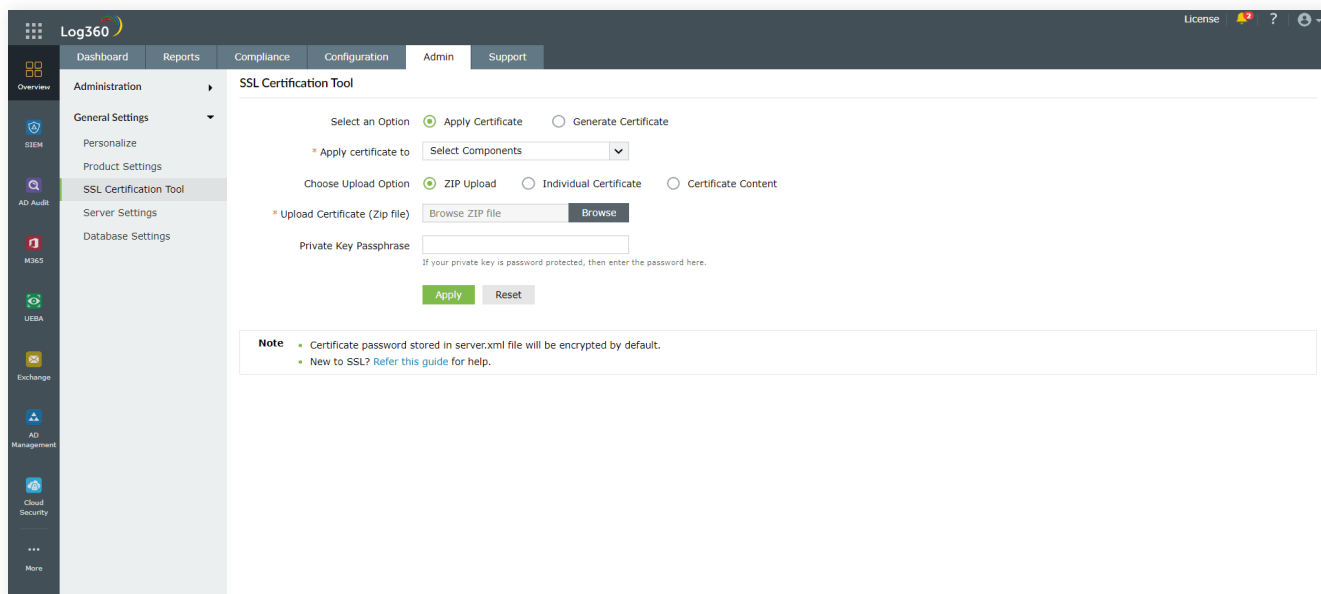
The file formats supported include:

1. .cer
2. .der
3. .crt
4. .pfx
5. .p12
6. .pem
7. .p7b
8. .jks
9. .keystore

Step 1

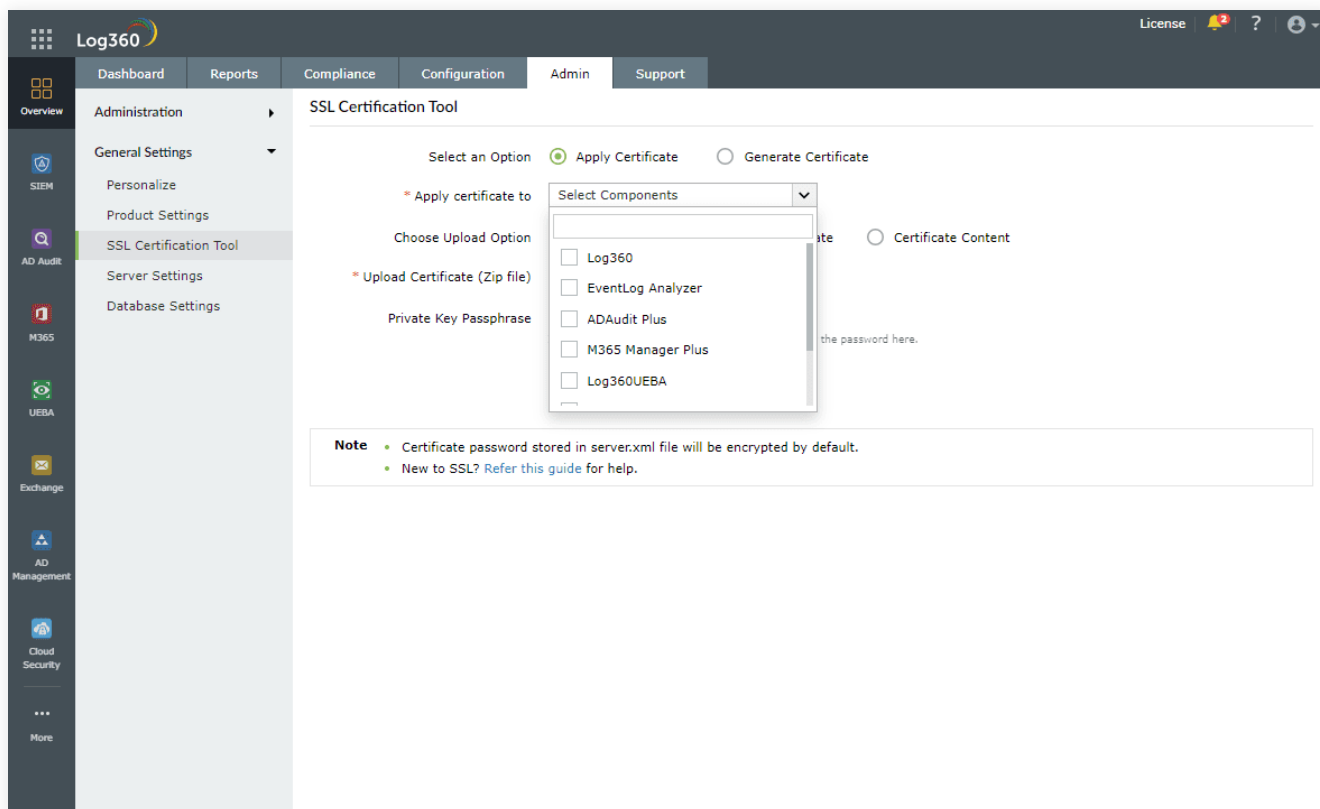
Generate and apply a SSL certificate for Log360 and its integrated components. All the components must be enabled with the HTTPs option to ensure sync.

- Navigate to **Admin** → **General Settings** → **SSL Certification Tool**.



- If you don't have a SSL certificate, select the **Generate Certificate** option and follow the steps [here](#).
- If you already have a SSL certificate, select the **Apply Certificate** option and follow the steps [here](#).

Note 1: To ensure all the components of Log360 are in sync, click the **Apply certificate** to option and select all the components. If any of the components are hosted on a different server, the respective SSL Certificate can be applied from Log360.



Note 2: SHA256 with RSA algorithm is currently supported for SSL certificates.

Apply Certificate

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

- 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:**
 1. If your CA has sent you a ZIP file, select **ZIP Upload**, and upload the file.
 2. If your CA has sent you individual certificate files—user, intermediary, and root certificates, you can put all these certificate files in a ZIP file and upload them.

- **Individual Certificates:**
 1. If your CA has sent you just one certificate file (PFX or PEM format), then select **Individual Certificates**, and upload the file.
 2. 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.
- **Certificate Content:**
 1. If your CA has sent just the certificate content, then choose **Certificate Content** option, and copy+paste the entire content in the **Paste Certificate Content** section.
- 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.

Note: Only Triple DES encrypted private keys are currently supported.

- Click **Apply**.
- Finally, restart Log360.

Generate Certificate

- In the **Common Name** field, enter the name of the server.
Example: For the URL **https://servername:8458**, the common name is **servername**.
- In the **Organizational Unit** field, enter the department's name which you want to be displayed in the certificate.
- In the **Organization** field, enter the legal name of your organization.
- In the **City** field, enter the name of the city as provided in your organization's registered address.
- In the **State/Province** field, enter the name of the state or province as provided in your organization's registered address.
- In the **Country Code** field, enter the two letter code of the country where your organization is located.
- In the **Password** field, enter a password that consists of at least 6 characters to secure the keystore.
- In the **Validity (In Days)** field, specify the number of days for which the SSL certificate will be considered valid.

Note: When no value is entered, the certificate is considered valid for 90 days.

- In the **Public Key Length (In Bits)** field, specify the size of the public key.

Note: The default value is 2048 bits, and its value can only be incremented in multiples of 64.

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

- **Generate CSR**

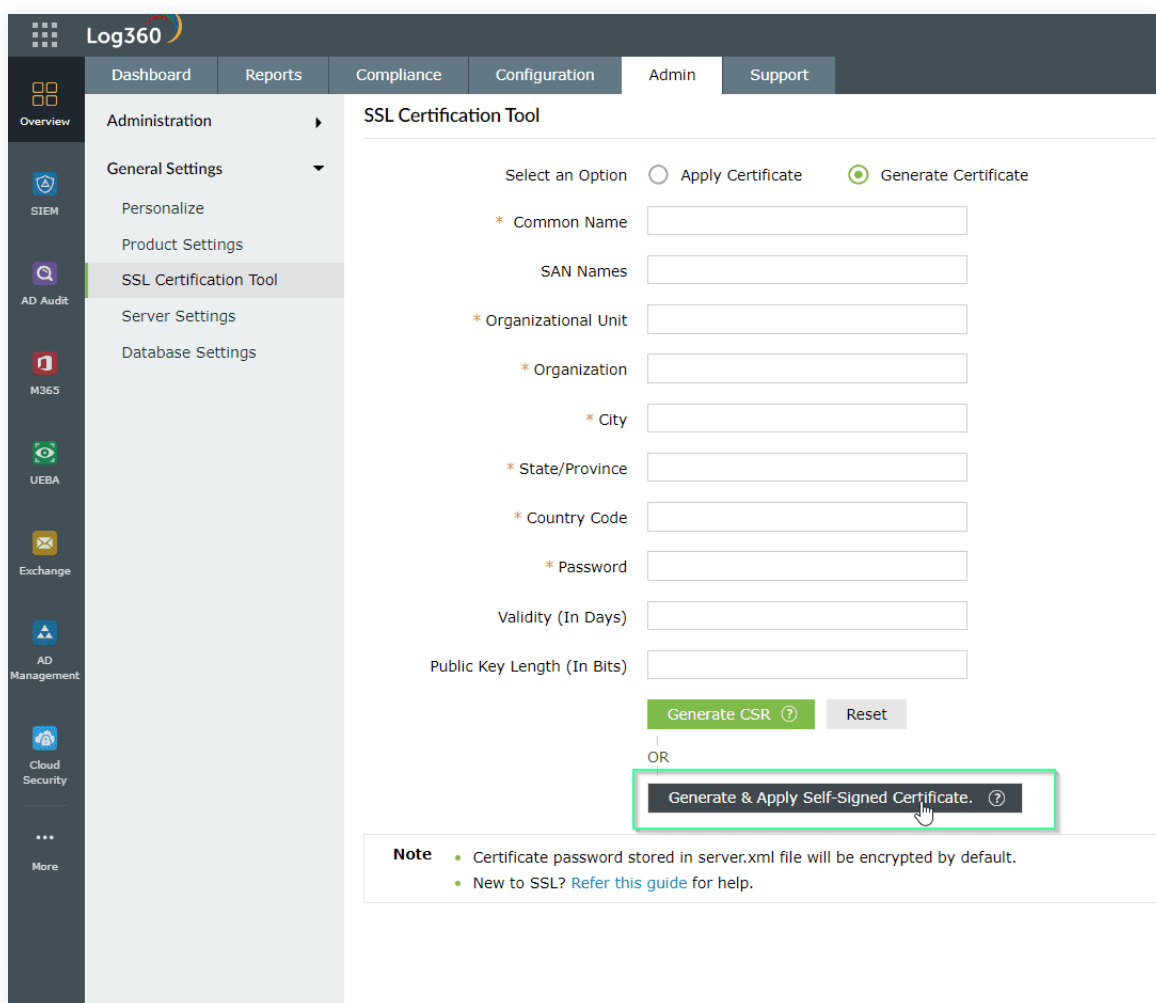
This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.

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, follow the steps listed under [Apply Certificate](#) to apply the SSL certificate.

- **Apply Self-signed Certificate**

This option allows you to create a self-signed certificate and apply it instantly in the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning telling them that the website is not trusted, which may cause concern.

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.



Step 2:

Issue the SSL certificate

In this step, you will connect to a certificate authority (CA), submit the CSR to the specific CA, and get the SSL certificate issued to you.

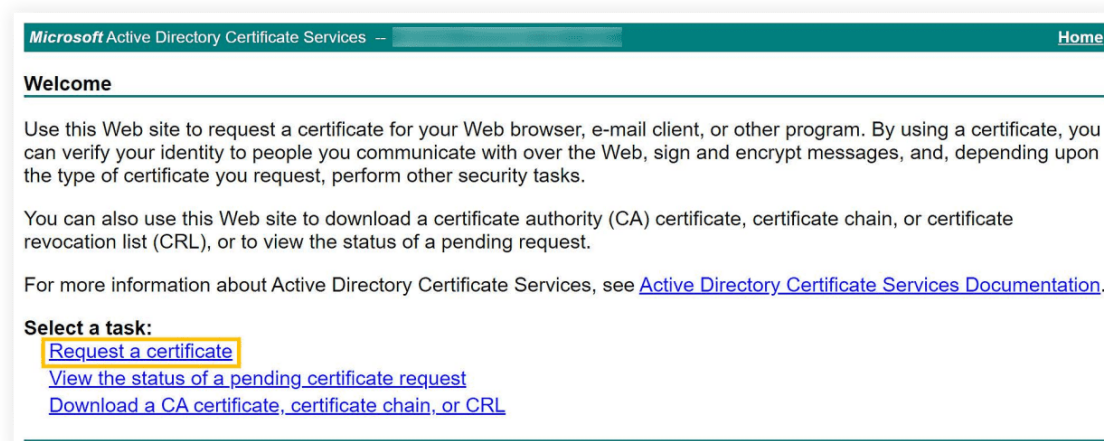
A. Issue the SSL certificate using an external CA

- To request a certificate from an external CA, submit the CSR to that CA.
- You can locate the CSR file in the \jre\bin folder. Unzip the certificates returned by your CA and put them in the \jre\bin folder.

B. Issue the SSL certificate using an internal CA

An internal CA is a member server or domain controller in a specific domain that has been assigned the CA role.

- Connect to the **Microsoft Active Directory Certificate Services** of your internal CA and click the **Request a certificate** link.



- On the Request a Certificate page, click the advanced certificate request link.



- On the Submit a Certificate Request or Renewal Request page, copy the content from your CSR file and paste it in the Saved Request field.
- Select **Web Server** or the appropriate template for Tomcat under **Certificate Template** and click **Submit**.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
 8gNVH04EFgQUT-fNK/8w5WwNdtJ8IdE1zdZm2f2Qw
 CIuKRY2CexoJxwJTnzJqNIxHVSeqZ880b7u8QwbN
 xTZn/U/g+yn3tz890wvmfODHLrV6GuHFYd557n58
 VLQzF0k0HPun6X18X4bNQG3qj6+PoHQz1asFjp3H
 crRBFwUqzDCzOxinY+yLj9s3uHX+4FeCrLV4dVBN
 7Xy8K+716tQKVLTTGICdnMLGvgk=

Certificate Template:
 Web Server

Additional Attributes:
 Attributes:


Submit >

- The certificate will be issued when you click the **Download certificate chain** link. The downloaded certificate will be in the P7B file format.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

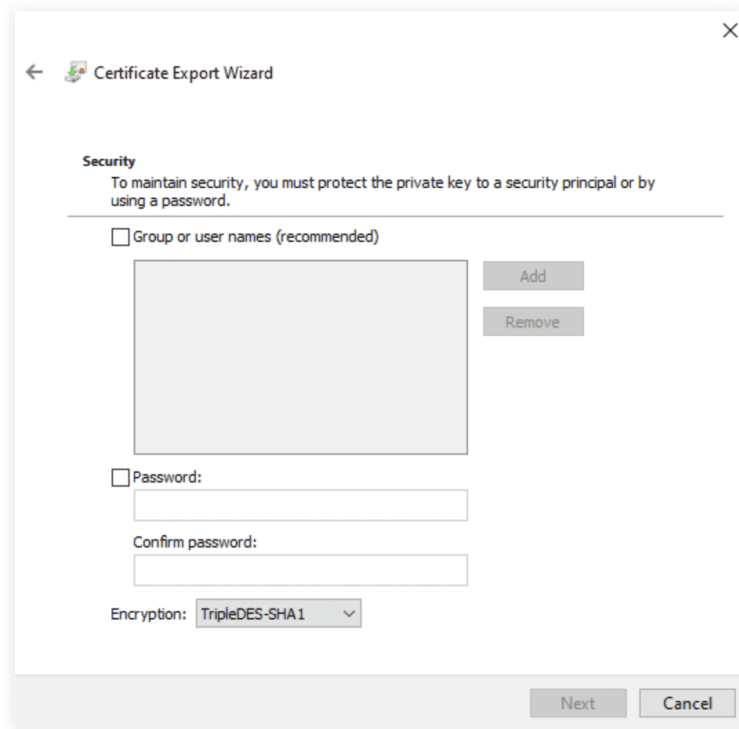
 [Download certificate](#)
[Download certificate chain](#)

Downloads window showing 'certnew.p7b' file.

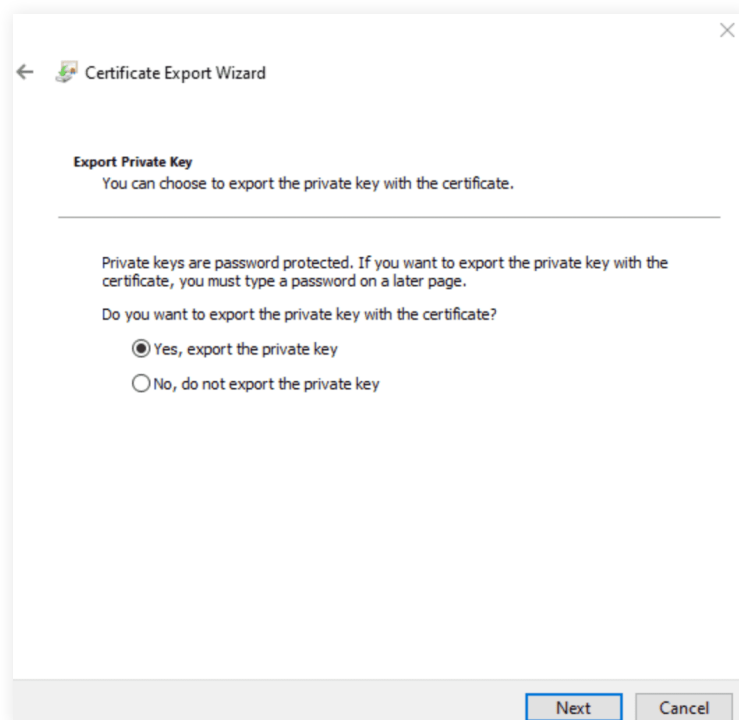
If the private key for the uploaded certificate is not found,

- Open the **Microsoft Management Console (MMC)**.
- Click **File > Add/Remove Snap-in**.
- In the Add/Remove Snap-in dialog box, select **Certificates** and click **Add**.
- In the Certificates snap-in dialog box, select **Computer account** or **My user account**, depending on the location of the certificate you want to export.
- Click **Finish** and then click **OK**.
- In the MMC console, expand the Certificates node and locate the certificate that contains the private key you want to export.
- Right-click the certificate and select **All Tasks > Export**.
- In the **Certificate Export Wizard** dialog box, select **Yes**, and export the private key.
- Choose the desired export format (usually Personal Information Exchange – PKCS #12 (.PFX)) and set a password to protect the exported file.

Note: Ensure the encryption selected is TripleDES-SHA1.



- Specify a file name and location for the exported private key file, and click **Finish**.



Note:

If the "Yes, export the private key" option is greyed out, it means the private key cannot be exported.



Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

About ManageEngine Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the [LinkedIn page](#) for regular updates.

\$ Get Quote

↓ Download