ESET Tech Center

Set up a HTTPS/SSL connection for ESET Security Management Center Web Console (7.x)

Anish | ESET Nederland - 2019-08-16 - Comments (0) - ESET Security Management Center

Issue

- You receive the warning message **Using unencrypted connection! Please configure the webserver to use HTTPS** when accessing the ESET Security Management Center Web Console (ESMC Web Console) via HTTP.
  For security reasons, we recommend that you set up ESMC Web Console to use HTTPS.

Solution

Before you start

- The steps below refer to certificates for Apache Tomcat, which are used to ensure secure HTTPS connections. For information about ESET Security Management Center certifications, see our Online Help topic.
- The steps as described below are performed on a 64-bit Microsoft Windows Server operating system (with 64-bit Java and 64-bit Apache Tomcat installed). Some paths may vary depending on the operating system you are using.

Use an existing certificate

1. Move the certificate .pfx file to your Tomcat install directory (the folder name may vary - substitute "Tomcat_folder" with the actual folder name).

   ```
   C:\Program Files\Apache Software Foundation\Tomcat_folder\
   ```

2. Open the **conf** folder in the Tomcat install directory and locate the **Server.xml** file. Edit this file using a text editor (such as Notepad ++).

   1. If there is no <Connector after </Engine> in Server.xml (for example when you perform a new instalation of Apache Tomcat), copy the following string into the Server.xml after </Engine> (use you values for keystoreFile, keystorePass, and keystoreType):

      ```
      <Connector server="OtherWebServer" port="443"
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      SSLEnabled="true" maxThreads="150" scheme="https"
      ```

```
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\Program Files\Apache Software
Foundation\Tomcat_folder\certificate_file.pfx"
keystorePass="Secret_Password_123"keystoreType="PKCS12" ssl
EnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA"/>
```

2. If `<Connector` is present after `</Engine>` in Server.xml (for example when you restore Server.xml after Apache Tomcat upgrade), replace the values of parameters listed below with your values:
   `keystoreFile` - Provide full path to the certificate file (`.pfx, .keystore`, or other).
   `keystorePass` - Provide certificate passphrase.
   `keystoreType` - Specify the certificate type.

Apache Tomcat documentation:

Read Apache Tomcat documentation for more information about the HTTP Connector.

3. Restart the **Tomcat** service.

Always use .pfx with password!

The `.pfx` certificate must **not** use blank password.

Create a new certificate and get it signed
To use a secure HTTPS/SSL connection