ESET Tech Center

How do I set up an HTTPS/SSL connection for ESET Remote Administrator Web Console? (6.x)

Ondersteuning | ESET Nederland - 2017-11-24 - Reacties (0) - 6.x

https://support.eset.com/kb3724

Issue

You receive the warning message **Using unencrypted connection! Please configure the webserver to use HTTPS** when accessing the ESET Remote Administrator Web Console (ERA Web Console) via HTTP.

For security reasons, we recommend that you set up ERA Web Console to use HTTPS.

Solution

ERA certificates vs. Apache Tomcat certificates

The steps below refer to certificates for Apache Tomcat, which are used to ensure secure HTTPS connections. For information about ESET Remote Administrator certifications, see our Online Help topic.

Steps may vary depending on operating system

The steps as described below are performed on a 64-bit Microsoft Windows Server operating system. Some paths may vary depending on the operating system you are using.

To use an existing certificate

1. Move the certificate .pfx file to your Tomcat install directory.

   By default, this is `C:\program files(x86)\Apache Software Foundation\Tomcat X.X` on 64-bit Windows Server systems or `C:\program files\Apache Software Foundation\Tomcat X.X` on 32-bit systems.

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 ++. Copy the following string into the Server.xml:

   ```
   <Connector port="443" maxHttpHeaderSize="8192"
   maxThreads="150" minSpareThreads="25"
   maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100"
   scheme="https" secure="true" SSLEnabled="true"
   clientAuth="false" sslProtocol="TLS"
   keystoreFile="enter_pfx_filename_here"
   keystorePass="enter_password_here"
   keystoreType="PKCS12"/>
   ```

3. Restart the Tomcat service.

To use a secure HTTPS/SSL connection for ERA Web Console, follow the steps below:

1. Create a **keystore** with an **SSL certificate**. You must have **Java JRE** installed, we recommend that you use the latest version.

   Java JRA includes the **Java Keytool** (keytool.exe), which allows you to create a certificate via command line. You must generate a new certificate for each tomcat instance (if you have multiple tomcat instances) to ensure that if one certificate is

compromised, other tomcat instances will remain secure.

Below is a sample command to create a keystore with an SSL certificate.

Navigate to the exact location of the **keytool.exe** file, for example `C:\Program Files (x86)\Java\jre1.8.0_40\bin` and then run the command):

```
keytool.exe -genkeypair -alias "tomcat" -keyalg RSA -keysize 4096 -validity 3650 -keystore "C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\tomcat.keystore" -storepass "yourpassword" -keypass "yourpassword" -dname "CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown"
```


-storepass and -keypass parameters

Values for `-storepass` and `-keypass` must be the same.

2. Export the certificate from the keystore. Below is a sample command to export the certificate sign request from the keystore:

```
keytool.exe -certreq -alias tomcat -file "C:\Install\tomcat\tomcat.csr" -keystore "C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\tomcat.keystore" -ext san=dns:ERA6-2008R2
```

Are you a Linux user?

Replace values appropriately

Replace the value `"C:\Install\tomcat\tomcat.csr"` for the `-file` parameter with the actual path and file name where you want the certificate to be exported.

Replace the value `ERA6-2008R2` for the `-ext` parameter with the actual hostname of the server on which your Apache Tomcat with ERA Web Console is running.

3. Get the SSL certificate signed with the Root Certificate Authority (CA) of your choice.

   You can proceed to step 5 if you plan to import a Root CA later. If you choose to proceed this way your web browser may display warnings about a self-signed certificate and you will need to add an exception to connect to ERA Web Console via HTTPS.

3. Once you have received the signed certificate with the Root CA, import the public key of CA and then certificate (`tomcat.cer`) into your keystore. Below is a sample command that imports a signed certificate into the keystore:

```
keytool.exe -import -alias tomcat -file
"C:\Install\tomcat\tomcat.cer" -keystore
"C:\Program Files (x86)\Apache Software
```

```
Foundation\Tomcat 7.0\tomcat.keystore"
```

Are you a Linux user?

> ### Replace values appropriately
>
> Replace the value "`C:\Install\tomcat\tomcat.cer `" for the `-file` parameter with the actual path and file name where the signed certificate is located.

If you want to use an already existing certificate (for example company certificate), follow these instructions.

5. Edit the `server.xml` configuration file so that tag is written similar to the example below:

   ```
   <Connector server="OtherWebServer" port="443"
   protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS"
   keystoreFile="C:\Program Files (x86)\Apache
   Software Foundation\Tomcat 7.0\tomcat.keystore"
   keystorePass="yourpassword" keyAlias="tomcat"/>
   ```

   This modification also disables non-secure tomcat features, leaving only HTTPS enabled (`scheme=` parameter). For security reasons, you may also need to edit `tomcat-users.xml` to delete all tomcat users and change ServerInfo.properties to hide the identity of the tomcat.

Are

you a Linux user?

6. Restart the Apache tomcat service.

Are you a Linux user?

What if secure connection is still failing on Linux?

Error message in the `/var/...../tomcat` directory: `failed to initialize end point associated with ProtocolHandler ["http-bio-443"]`

If the problem persists, change the `port` in the `server.xml` file to a value higher than *1024*, because ports below *1024* may not be accessible to non-root users. If for some reason you have to use port *443*, you can still change the value and then forward the port.

Related articles:

Set an ESET Remote Administrator Web Console running on Linux to

utilize HTTPS (6.x)

Tags

ERA 6.x