

ESET Tech Center

Knowledgebase > Legacy > Legacy ESET Remote Administrator (6.x / 5.x / 4.x) > 6.x > Set an ESET Remote Administrator Web Console running on Linux to utilize HTTPS (6.x)

Set an ESET Remote Administrator Web Console running on Linux to utilize HTTPS (6.x)

Ondersteuning | ESET Nederland - 2017-11-08 - Comments (0) - 6.x

<https://support.eset.com/kb5695>

Be careful to change the service name

This solution is for apt based distributions like Ubuntu. For the other distributions like Fedora you have to change the service name tomcat7 to tomcat .

[Click here for instructions on using an already signed key.](#)

1. Run the following command:

```
sudo keytool -genkey -alias tomcat -keyalg RSA -  
keystore/etc/ssl/certs/java/era_web_console.keyst  
ore -storepass password -validity 3650 -keysize  
4096
```

2. Open the file `sudo nano /var/lib/tomcat7/conf/server.xml`.
3. Search or scroll until you find `<Connector port="8443">` and edit the area for connector port as follows:

```
<Connector port="8443" protocol="HTTP/1.1"  
SSLEnabled="true"  
maxThreads="150"  
scheme="https"  
secure="true"  
keystoreFile="/etc/ssl/certs/java/era_web_console  
.keystore"keystorePass="password"  
keyAlias="tomcat"  
clientAuth="false"  
sslProtocol="TLS"
```

/>

Use an already signed key

1. Purchase a key file from one of the certifying authorities for your ESET Remote Administrator (ERA) address.
2. Copy this key to your Ubuntu server, preferably as a .pfx file.
3. Determine the alias of the key file by running the following command:

```
keytool -list -storetype pkcs12 -keystore  
keyfilename.pfx -v | grep Alias
```

Password required

This command will prompt you for the password you used to create the key from the certifying authority.

4. Convert the .pfx file to .jks using the following command:
keytool -importkeystore -srckeystore
keyfilename.pfx -srcstoretype pkcs12
-destkeystore keyfilename.jks -deststoretype jks

Password required

This command will prompt you for the password you used to create the key from the certifying authority. It will also prompt you to create a password for the newly converted key file.

5. Edit the configuration file to use the new .jks file, using the following command:
sudo nano /var/lib/tomcat7/conf/server.xml

Find the section that says <Connector port="8443"> and edit the section to look like this:

```
<Connector port="8443"  
protocol="HTTP/1.1"  
SSLEnabled="true"  
maxThreads="150"  
scheme="https"  
secure="true"  
keystoreFile="location of the newly created .jks  
file, for example /home/user/keyfilename.pfx"  
keystorePass="password"  
keyAlias="use the alias you determined in the  
previous step"  
clientAuth="false"  
sslProtocol="TLS"  
>
```

6. Restart Tomcat using the following command:

```
sudo service tomcat7 restart
```

Tags

ERA 6.x

Linux