ESET Tech Center

ESET Remote Administrator HTTP Server will not start – error with signed certificate (5.x)

Ondersteuning | ESET Nederland - 2024-08-28 - Reacties (0) - 5.x

https://support.eset.com/kb6005

Issue

You are trying to set up SSL/HTTPS on ESET Remote Administrator version 5 dashboard
ESET RA HTTP Server will not start
In the ESET Remote Administrator 5 dashboard, you receive a warning message that you do not have a signed certificate
Convert pfx certificate to pem and key

Solution

You can repair the ESET Remote Administrator HTTP Server service by converting the pfx certificate to pem and key. Follow the instructions below to convert the file and the service should start as expected.

1. Download the Win32OpenSSL application:

   DOWNLOAD WIN32 OPEN SSL LIGHT

2. Create a new folder in your C: folder and name it "certs" (without the quotes).

3. Move the cert.pfx file to the new folder you created in step 2.

4. Open a command prompt as admin and from the directory path `c:\OpenSSL-Win32\bin` (path name may vary) run the following command:

   ```
   openssl pkcs12 -in c:\certs\cert.pfx -out
   ```

```
c:\certs\cert.key -nocerts -nodes
```

You will be asked to type in your certificate password. Next, type in the following two commands:

```
openssl rsa -in c:\certs\cert.key -out
c:\certs\cert.key

openssl pkcs12 -in c:\certs\cert.pfx -out
c:\certs\cert.pem -nokeys -clcerts
```

5. Verify that the output md5 hashes match when you run the following commands:

   ```
   openssl x509 -noout -modulus -in
   c:\certs\cert.pem | openssl md5

   openssl rsa -noout -modulus -in
   c:\certs\cert.key  | openssl md5
   ```

6. Move the certificates to the following location:

   ```
   C:\ProgramData\ESET\ESET Remote
   Administrator\Server\configuration
   ```

7. To configure the certificates to use the new certificate keys you created above, in ESET Remote Administrator Console navigate to **Tools → Server Options → Advanced** and then click **Edit Advanced Settings**.

   Expand **Remote Administrator → Era Server → Settings → Dashboards**.

Figure 1-1

8. Click to select each setting and type in the following values:

   a. **Local certificate**: configuration\cert.pem

Figure 1-2

b. **Local certificate key**: configuration\cert.key

Figure 1-3

9. Click **Console** → **Yes** to save the changes and exit the **Advanced settings** window.

10. Restart ESET RA HTTP Server services. Click **Start** → **Run**, type **services.msc** and then click **OK**.

11. Locate the **ESET RA HTTP Server** service in the **Services** window, right-click it and select **Restart** from the context menu.

Figure 1-4

12. Test the public web address that the certificate is signed for.

Tags

ERA 5.x