

Enable HTTP Strict Transport Security on the Web Console in ESMC (7.x)

Anish | ESET Nederland - 2018-08-20 - [Reacties \(0\)](#) - [7.x](#)

Issue

- To enable a higher security standard on your ESMC Web Console, it is recommended to use a signed certificate and enable HTTP Strict Transport Security
- [Enable HSTS](#)
- [Disable HSTS](#)

Details

Solution

Prerequisites

- A supported web browser
- [Use a valid and trusted certificate in Tomcat](#)
- You cannot use a self-signed certificate; only a certificate that is signed by a trusted CA can be used
- Hostname of your Web Console machine has to be the same as the Common name of the certificate

Enable HSTS

1. On the machine where the Web Console is installed, edit the configuration file (the exact location of the file may differ depending on the OS and Tomcat versions).

Windows

```
C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

Linux

```
/var/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties
```

2. In the file, change the line from:
HSTS_enable=true
to
HSTS_enable=true
3. Save the file and restart the Tomcat service.

Verify the Web Console is requesting the HSTS

Google Chrome and Mozilla Firefox

The procedure to verify the Web Console is requesting HSTS as shown below is valid for Google Chrome and Mozilla Firefox.

1. Open the Web Console in the web browser; you do not need to log in.
2. Check that the HTTPS connection is established. If it is, your browser will display the icon as shown in

the address bar: 

3. Press the **F12** key to access Developers mode.

4. Click the **Network** tab → `webconsole.nocache.js` → **Headers** tab.
5. If you have an HTTPS connection and HSTS is enabled in the Web Console, you will see the **Strict-Transport-Security** line in the **Response Headers** section.

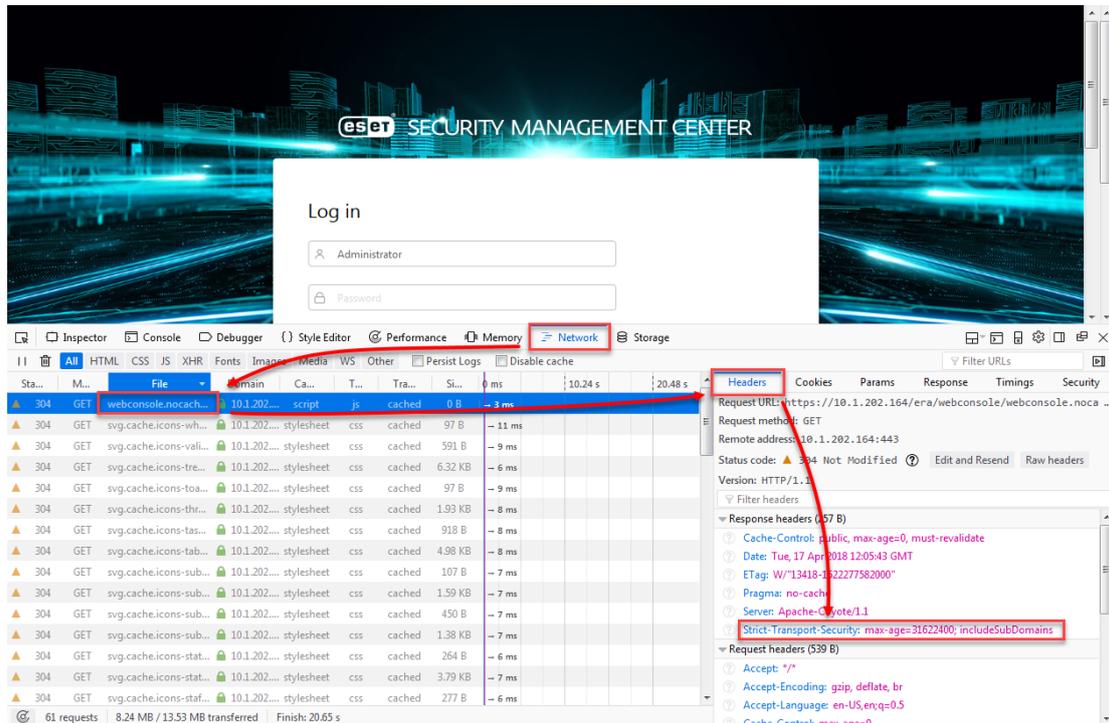


Figure 1-1
Click the image to view larger in a new window

Internet Explorer

The procedure to verify the Web Console is requesting HSTS as shown below is valid for Internet Explorer.

1. Open the Web Console in the web browser; you do not need to log in.
2. Check that the HTTPS connection is established.
3. Press the **F12** key to access Developers mode.
4. Click the **Network** tab → click play icon to record the network flow → double click `webconsole.nocache.js` → click **Response Headers** tab.
5. If you have an HTTPS connection and HSTS is enabled in the Web Console, you will see the **Strict-Transport-Security** line in the **Response Headers** section.

If the HSTS has not taken effect, you have not fulfilled all pre-requisites. The appearance of the HSTS in the **Headers** only indicates the Web Console is requesting it.

- If you are using an untrusted certificate, HSTS will not be applied.
- When the HSTS is applied and the web browser is using it, it is not possible to access the Web Console via HTTP connection.

Disable HSTS

You may want to disable HSTS if:

- Your trusted certificate is about to expire and you are replacing it with a self-signed certificate
- HSTS is causing issues

- You are changing your certificate

Connect each browser to the Web Console during the switch-off period!

Each browser that you use to connect to the Web Console needs to connect at least once, while the certificate is still valid during the switch-off period.

1. On the machine where is the Web Console installed, edit the configuration file (the exact location of the file may differ depending on the OS and Tomcat versions).

Windows

C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Linux

/ver/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties

2. In the file, change the line from:
HSTS_enable=true
to
HSTS_enable=false
3. Save the file and restart the Tomcat service.
4. Once the new settings are applied, connect each browser you use to ESMC Web Console to save the new HSTS setting to the browser.