ESET Tech Center

Enable and apply Advanced security on your network using ESMC

Anish | ESET Nederland - 2019-02-04 - Comments (0) - ESET Security Management Center

Applies to: ESET Security Management Center | Product version: 7.x

Details

Solution

Compatibility issues with older systems

Advanced security is not compatible with older systems (for example, Windows XP and Windows Server 2003). ESET Management Agents disconnect from the ERA Server after the certificate change. To keep managed devices with an older unsupported OS connected to ERA Server, do not replace certificates for these devices and do not revoke the original CA and peer certificate.

To verify if your Linux client is compatible, use the following command:

```
openssl s_client -connect google.com:443 -tls1_2.
```

Minimum compatibility requirements for Advanced security

Advanced security does not influence the already existing CAs and certificates, only new CAs and certificates created after advanced security is enabled. To apply Advanced security in your existing ESMC infrastructure, you will need to replace the existing certificates.

Enable Advanced security in ESMC

1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
2. Click **More → Server Settings** and click the slider next to **Advanced security (require restart!)** to enable it.
3. Click **Save** to apply your changes.

Figure 1-1
Click to view larger in new window

1. Close the ESMC Web Console and restart the ESMC Server service.
2. Wait a few minutes after the service has started and then log in to the ESMC Web Console.
3. Verify that all computers are still connecting and no other problems have occurred.
4. Create a new Certification Authority (CA). The new CA is automatically sent to all client computers during next Agent-to-Server connection.
5. Create new peer certificates signed with this new CA. Create a peer certificate for Agent and one for Server (select the applicable value in the **Product** drop-down menu in step 3 of the linked process).
6. Complete the steps in our Client computer migration in ESMC article to:
    1. Create a new ESET Management Agent policy to set up your Agents to use the new Agent certificate.
    2. Assign the policy to computers where you want to use the Advanced security.

To minimize the risk of accidentally orphaning client computers, apply the changes to a test computer prior to applying them to all target computers.

1. When all devices are connecting with the new certificate, complete the steps in our Server migration in ESET Security Management Center 7.x article to update your current ESMC Server certificate with the new one. You can also delete your old CA and revoke old certificates unless if you applied Advanced security to only some (and not all) of your connected client computers.

Advanced security is now enabled on your client devices.

Advanced security on systems with installed MDM

Advanced security will affect only communication between an ESMC Server and a MDM Server. Communication between an MDM Server and Mobile Devices will not be affected. To apply Advanced security to the MDM component, create new MDM and Proxy certificates signed by the new CA and assign them using a policy to the MDM server as follows:

1. ESET Mobile Device Connector Policy → **Settings → General → HTTPS certificate**. Click **Change certificate** to import the new MDM Certificate.

Figure 2-1
Click to view larger in new window

1. ESET Mobile Device Connector Policy → **Settings → Connection → Certificate**. Click **Change certificate → Open certificate list** and select **Proxy certificate**. Click **OK**.

Figure 2-2
Click to view larger in new window

Advanced security is now enabled on the MDM component.

KB Solution ID: KB7078 |Document ID: 26507|Last Revised: December 17, 2018