Resolve the intranet single sign-on authentication issues with TLS filtering activated

Steef | ESET Nederland - 2021-04-21 - Reacties (0) - Endpoint Solutions

Issue

- ESET Windows endpoint products with TLS filtering enabled cannot connect to an intranet or localhost site using HTTPS
- You are asked for the password repeatedly, but the credentials are rejected
- Single sign-on does not work with TLS filtering enabled in ESET endpoint products when accessing intranet sites using HTTPS
- Credentials must be entered manually using an HTML form.
- Create an exception on the affected computers to resolve the issue

Details

This situation can occur if the authentication is based on protocols such as SPNEGO (WWW-Authenticate: Negotiate), Kerberos, NTLM and if Channel Binding Tokens are utilized.

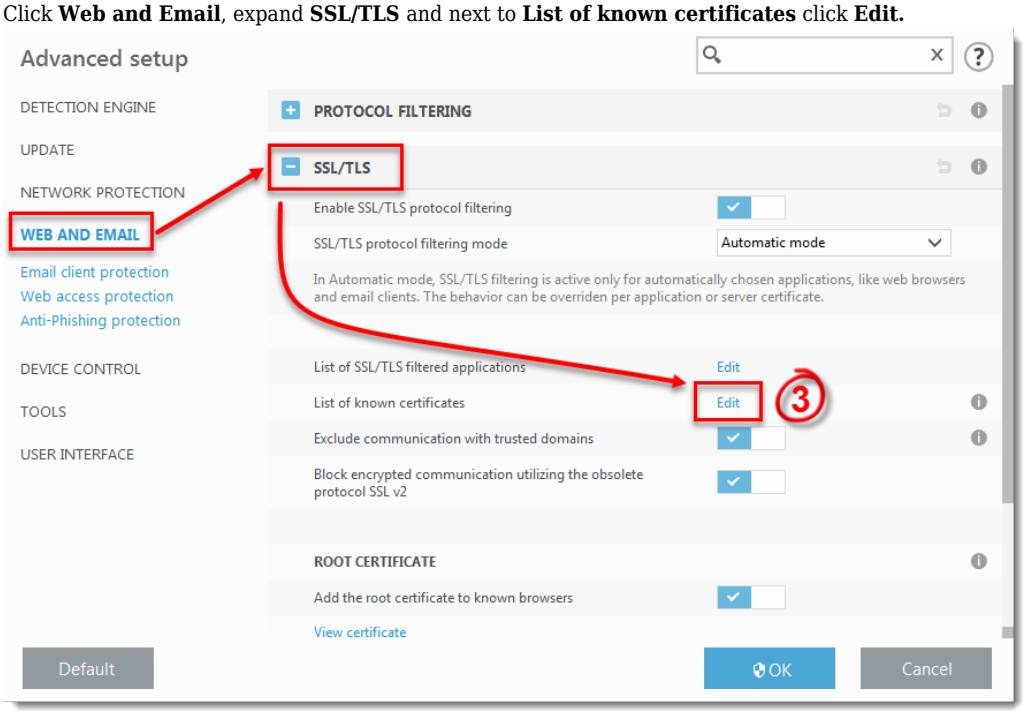
This behavior is a security feature of the underlying authentication protocol:

- https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview

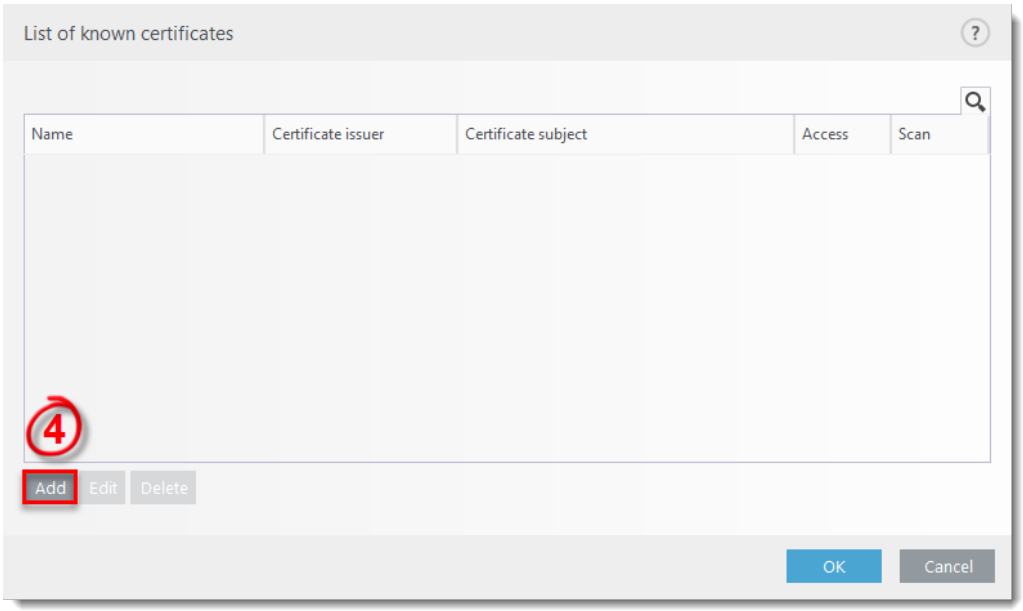
Solution

Create an exception on the affected computers-preferred solution

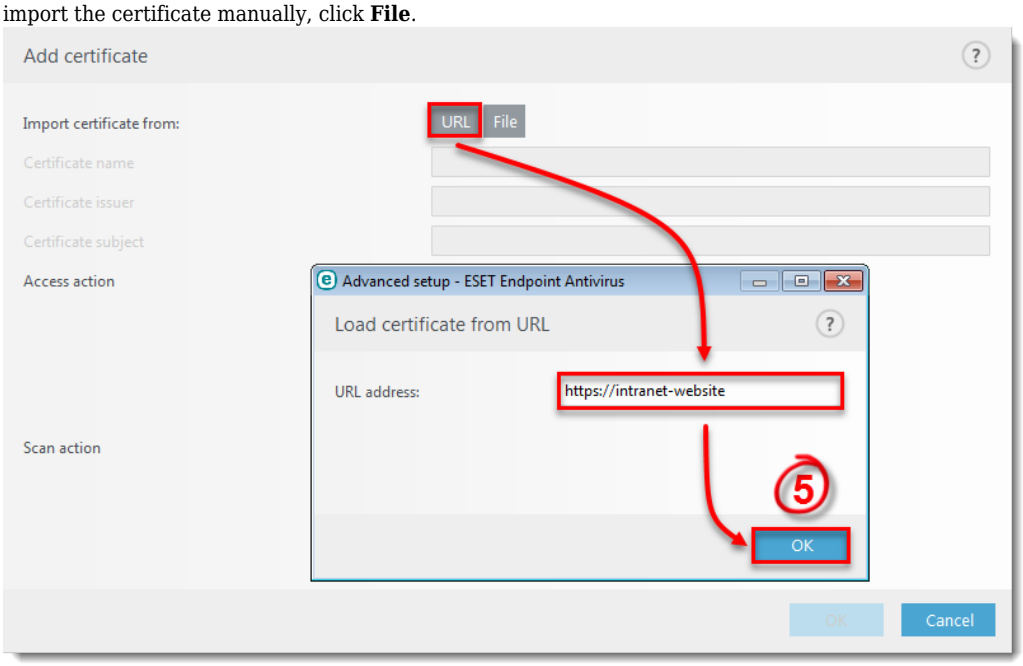
1. Open the main program window of your ESET Windows product.
2. Press the **F5** key to access Advanced Setup.
3. Click **Web and Email**, expand **SSL/TLS** and next to **List of known certificates** click **Edit.**



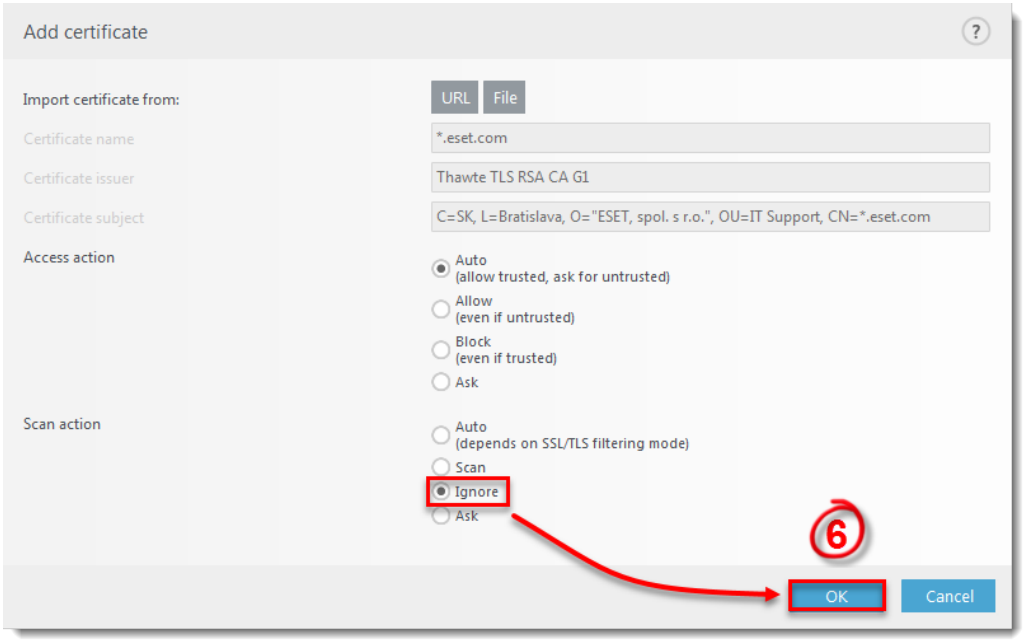
4. Click **Add**.



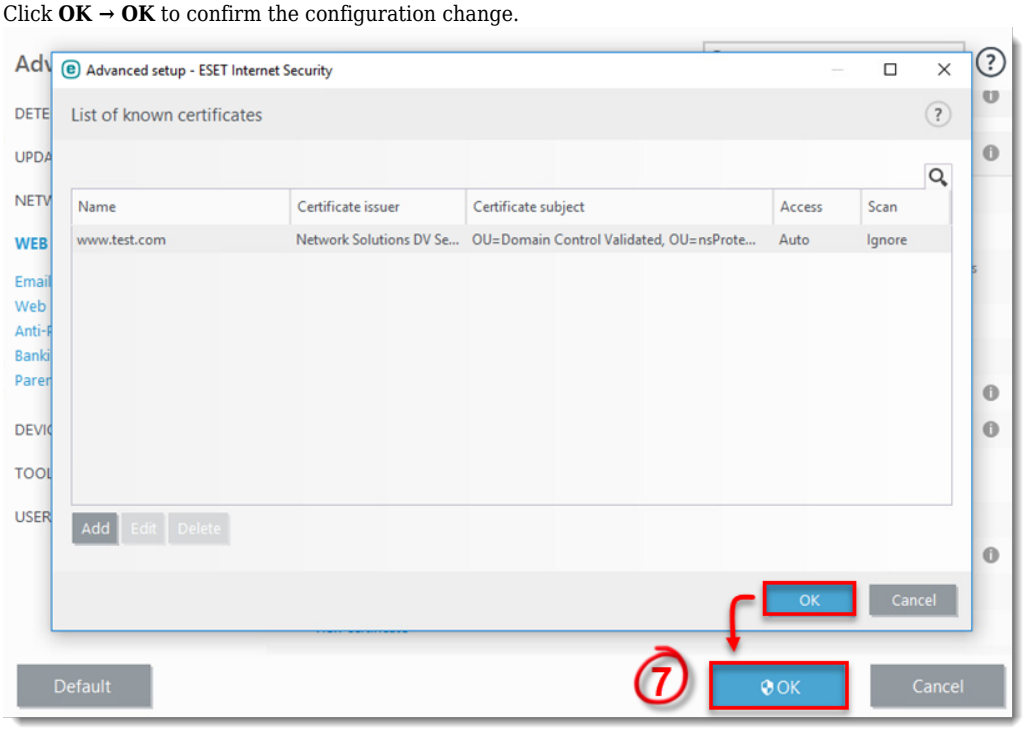
5. Click **URL** and in the **URL address** field, type the domain name of the server and then click **OK**. To import the certificate manually, click **File**.



6. Next to **Scan action**, select **Ignore** and click **OK**.



7. Click **OK → OK** to confirm the configuration change.



If you are managing ESET endpoint products remotely using ESET PROTECT (Cloud) , apply these settings as a policy.

Disable the "Extended Protection for Authentication" feature on the server

Disabling this feature will leave your server vulnerable to Man in the Middle attacks and is not recommended. We recommend that you attempt the solution above.

For more information see:

- https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-practices-for-secure-planning-and-deployment-of-ad-fs (part "Utilize extended protection for authentication")
- https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-iwa#channel-binding-token