ESET Tech Center

Knowledgebase > Endpoint Solutions > Resolve the intranet single sign-on authentication issues with TLS filtering activated

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

Steef | ESET Nederland - 2021-04-21 - Comments (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-authentic ation-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.

Advanced setup		Q,	× ?
DETECTION ENGINE	• PROTOCOL FILTERING		0
UPDATE	SSL/TLS		5 0
NETWORK PROTECTION	Enable SSL/TLS protocol filtering		
WEB AND EMAIL	SSL/TLS protocol filtering mode	Automatic mode	~
Email client protection Web access protection	In Automatic mode, SSL/TLS filtering is active only for autor and email clients. The behavior can be overriden per applica		ike web browsers
Anti-Phishing protection			
DEVICE CONTROL	List of SSL/TLS filtered applications	Edit	
TOOLS	List of known certificates	Edit 3	0
USER INTERFACE	Exclude communication with trusted domains		0
oser an en Ace	Block encrypted communication utilizing the obsolete protocol SSL v2	~	
	ROOT CERTIFICATE		0
	Add the root certificate to known browsers	×	
	View certificate		
Default		© ОК	Cancel

4. Click Add.

List of known certificates					?
					Q,
Name	Certificate issuer	Certificate subject		Access	Scan
2					
4					
Add Edit Delete					
			1	ОК	Cancel

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**.

Add certificate		?
Import certificate from: Certificate name Certificate issuer Certificate subject	URL File	
Access action	Advanced setup - ESET Endpoint Antivirus Load certificate from URL (?)	
Scan action	URL address: https://intranet-website	
	OK Ca	ancel

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

Add certificate		?
Import certificate from:	URL File	
	*.eset.com	
	Thawte TLS RSA CA G1	
Certificate subject	C=SK, L=Bratislava, O="ESET, spol. s r.o.", OU=IT Support, CN=*.eset.com	
Access action	Auto (allow trusted, ask for untrusted) Allow (even if untrusted) Block (even if trusted) Ask	
Scan action	Auto (depends on SSL/TLS filtering mode) Scan Ignore Ask	
	OK Car	ncel

7. Click **OK** \rightarrow **OK** to confirm the configuration change.

e Advanced setup - ESET Internet	a secondy				×
List of known certificates					?
					Q,
Name	Certificate issuer	Certificate subject	Access	Scan	
www.test.com	Network Solutions DV Se	OU=Domain Control Validated, OU=nsProte	Auto	Ignore	
Add Edit Delete					
		ſ	ОК	Car	ncel
		<u>a</u> †			
Default		(7)	ФОК		Cance

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