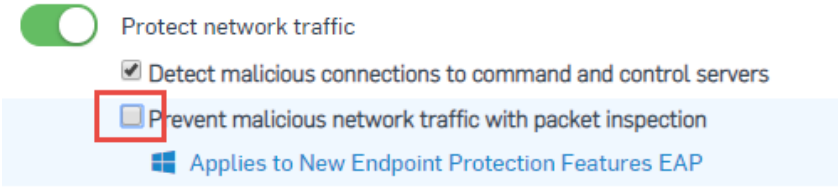


Known Issues List for AMSI and IPS EAP

Date: 3 December 2019

Enhanced Protection EAP with AMSI and IPS.

Issue	Details	Notes
[AMSI] No detections for .NET assemblies	In order to mitigate an issue where AMSI incorrectly identifies certain applications as threats, detections for .NET assemblies have temporarily been disabled.	The EAP refresh of the week commencing 2 December 2019 will contain a fix for this issue. Detections for .NET will stay disabled for a few more weeks to make sure all clients are updated.
[IPS] On some devices the Wi-Fi adapter has issues connecting	<p>Certain devices with IPS have issues with the Wi-Fi network adapter. Connections can be made, but are interrupted after a few minutes. Network connections with ethernet cables are not affected.</p> <p>To mitigate the issue disable the IPS setting for those machines:</p>  <p>Protect network traffic</p> <p><input checked="" type="checkbox"/> Detect malicious connections to command and control servers</p> <p><input type="checkbox"/> Prevent malicious network traffic with packet inspection</p> <p>Applies to New Endpoint Protection Features EAP</p>	<p>If you should encounter the issue, please send us the SDU log (see https://community.sophos.com/kb/en-us/33533 on how to create the logs).</p> <p>You can send a private message on the forum to Vincent Vanbiervliet, with the file attached.</p>
[IPS] Device shows "Bad Health State" after client installation	After joining the Early Access Program (EAP) for Enhanced Protection/IPS and AMSI, the endpoint may report a Bad health state due to Sophos Snort service not starting until after a reboot.	See also this post .

	A reboot is required to complete the install of the new IPS and AMSI components. This will be fixed in the next release of the Core Agent in November 2019.	
[IPS] IPS fails to attribute traffic to correct application due to packet modification	<p>When certain applications such as NetBalancer are installed on the endpoint, IPS fails to correctly identify the source application of the malicious traffic.</p> <p>IPS still detects and blocks the malicious traffic, but fails to report the name of the application, nor can it block the application.</p>	
[EAP] Device shows "Bad Health State" after client upgrade to v2.5.4 BETA	After upgrading to the latest release the endpoint may report a Bad health state; this will be fixed by the following update an hour later. A reboot or manual update of the endpoint will clear the health state issue.	