Pulse Secure

# Host Checker ESAP Troubleshooting Guide

Published April 2019

Document Version 1.0

Pulse Secure, LLC
2700 Zanker Road, Suite
200 San Jose, CA 95134
www.pulsesecure.net

# Contents

# Introduction

This troubleshooting guide describes how to troubleshoot Host Checker ESAP issues. This guide covers the following sections:

- ESAP version vs Opswat and Shavlik SDK versions
- Overview of Host Checker
- Details of Opswat SDK
- ESAP package
- Live Update for signature definitions
- General Opswat Policy Communication Flow
- Workarounds
- Logs needed for to open a case for ESAP issues
- Debug logs
- Error in user access logs

# SDK versions

The below SDK versions are used by ESAP 3.3.9 **https://www-prev.pulsesecure.net/download/techpubs/current/1544/pulse-connect-secure/esap/3.3.x/ps-esap-3.3.9-releasenotes.pdf**
V3 SDK is no longer supported **https://kb.pulsesecure.net/articles/Pulse_Technical_Bulletin/TSB41055**

V3 SDK Version: Mac and Windows 3.6.11667.2

V4 SDK Version: Windows 4.3.622.0, Mac 4.3.534.0

V3V4 Adapter Version: Windows 4.3.433.0, Mac 4.3.408.0

# Overview of Host Checker

Host Checker is an endpoint security assessment component and has following features:

- Supported Cross Platform (Desktops and Mobiles)
- Server and Client components
- Periodic Host Checking
- Rule Monitoring
- Remediation actions

# Details of OPSWAT SDK

Following are the key points about OPSWAT:

- Opswat SDK is a software framework for determining security product details on endpoints.
- It supports on Windows and macOS platforms.
- Data files listing supported products
- Binaries for detecting the installed products on end machines

Note: Identify whether V3 or V4 is being used. (V3 is no longer supported).

1. Go to the admin UI.
2. Go to **Authentication** > **Endpoint Security** > **Host Checker**
3. Scroll to the bottom of the page.
4. Under the ESAP packages, if **Activate Older Opswat SDK in ESAP for Host checker policy evaluation** is checked, V3 is in use. if **Activate Older Opswat SDK in ESAP for Host checker policy evaluation** is unchecked, V4 is in use.

| Opswat SDK Version | Supported Platforms | Supported PCS Versions |
|---|---|---|
| V2 | Windows | Pre 7.2 |
| V3 | Windows and Mac | Post 7.2 |
| V4 | Windows and Mac | Post 8.2 |

# ESAP Package

- It is a delivery mechanism to install the OPSWAT SDK files.
- Packages files are needed for server and clients.
- It supports 4 ESAP packages
- It gets integrated with Agentless and Pulse Clients.
- 2 ESAP packages planned to be released every month. One around Mid of every month and second one around end of month.
- For supported products list for ESAP, refer below links, for example below is link for latest ESAP 3.3.9

https://www-prev.pulsesecure.net/download/techpubs/current/1545/pulse-connect-secure/esap/3.3.x/ps-esap-3.3.9-supportedproducts-v4sdk.pdf

Also, refer to release notes for fixes and support added information etc. Here is the link:

https://www-prev.pulsesecure.net/download/techpubs/current/1544/pulse-connect-secure/esap/3.3.x/ps-esap-3.3.9-releasenotes.pdf

# Live Update for Signature Definitions

- OPSWAT publishes new signature definitions regularly
- Pulse Secure scripts hosts them on download.pulsesecure.net
- PCS/PPS can regularly update the signatures
- Signatures used for validating Antivirus signature definitions

# General OPSWAT Policy Communication Flow

Following are the steps for General OPSWAT policy communication flow:

- Client sends the installed ESAP details to server.
- Server validates ESAP and if needed asks client to download ESAP.
- Server sends instructions of what details need to be collected.
- Client collects required products and sends to server.
- Server validates the policies.
- If needed, server sends the remediation actions to client.
- Client performs remediation actions and re-evaluates policies.

# Workarounds

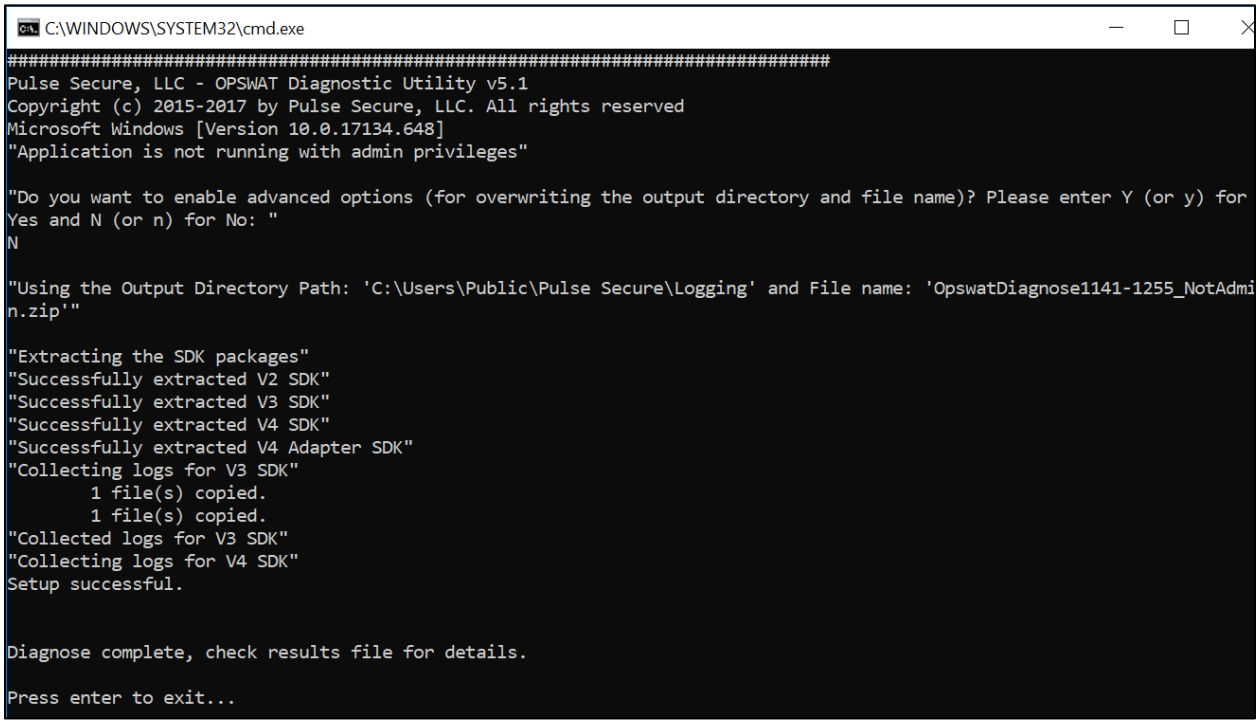
Refer **http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43790** For RTP not detected also, we can configure a process check rule as a workaround till the fix is available as shown in **http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43790**.

Same kb has information on configuring number of days as a workaround for virus definition checks if check based on number of updates fail till fix is available.

# Logs needed to open a case for ESAP issues

- OESIS diagnostic logs, download and run the ESAP-Diagnostic Tool available on our support download portal for the latest ESAP version available, download and collect logs from windows or MAC depending on the issue.


Press N and the enter to exit and collect the file under C:\Users\Public\Pulse Secure\Logging




- Pulse client logs at detail level (If user is logging in via Pulse client and reporting issue).Refer **http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB17327**
- Debug log at level 5(if issue is seen via browser login only).Refer **http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB25344**
- Screenshot of about page of AV/FIREWALL (as we need the build and version details).
- User access logs error.
- Any information on where to download Trial package will help.

With level 5 logs, we can see the information collected and sent by client to the server:

00537,09 2018/06/11 16:14:50.097 4 admin dsHostChecker.exe OpswatIMC p3664 t17D0 opsantivirusdata.cpp:41 - 'toImvMessage' IMV Message : <parameter name="AntiVirus" value="product_id=2884;product_sig=2938;product_name=Sophos Cloud Endpoint;vendor_name=Sophos Limited;product_version=2.0.3;is_authentic=UNKNOWN;gmt_offset=-570;fsrtp=YES;last_scan_time=2018/06/11 07:25:35;signature_def_time=2018/06/11 06:44:31;signature_def_version=2018.06.11;virus_def_sig=;def_update_in_progress=UNKNOWN;scan_in_progress=NO;services_running=UNKNOWN;eror=;"> :

# Debuglog

This section describes debuglog for the following:

1. Client sending the installed ESAP details
2. Server requesting for Antivirus details
3. Client sending installed Antivirus details
4. Server requesting for remediation actions
5. Client performing policy evaluation again after completing remediation action
6. Example of Server requesting client to download ESAP

### 1. Client sending the installed ESAP details

00667,09 2016/04/19 12:41:24.805 4 root dsAccessService OpswatIMC p17846 t2203 OpsIMC.cpp:268 - 'beginHandshake' Sending message to IMV: [<parameter name="policy_request" value="message_version=2;"><parameter name="esap" value="esap_version=2.9.0;fileinfo=name:libCoreUtils.dylib^md5:4fa3417a01a044c6^|name:libImplAntivirus.dylib^md5:de78b1a900ec0b5b^|name:libImplFirewall.dylib^md5:ab81434006a66378^|name:libImplHDEncryption.dylib^md5:9a6634f25ff014e1^|name:libImplSoftwareProduct.dylib^md5:116836e662c71515^|name:libOesisCore.dylib^md5:0beb5101ac9055b5^|name:scpt.dat^md5:84aa553441fccace^|name:tables.dat^md5:e27e8d4daa5d91dd^|;has_file_versions=NO;needs_exact_sdk=NO;">]

2. **Server requesting for Antivirus details**

00202,09 2016/08/10 12:25:43.773 4 admin dsHostChecker.exe OpswatIMC p3088 t1414 opsimc.cpp:91 - 'receiveMessage' Message received from IMV: [<parameter name="AntiVirus" value="needsMonitoring=0;needsData=1">]

3. **Client sending installed Antivirus details**

01212,09 2016/08/10 12:25:45.367 4 admin dsHostChecker.exe OpswatIMC p3088 t1414 opsimc.cpp:303 - 'receiveMessage' Sending message to IMV: [<parameter name="AntiVirus" value="product_id=5001;product_sig=0;product_name=McAfee VirusScan;vendor_name=McAfee, Inc.;product_version=18.0.4054;is_authentic=UNKNOWN;gmt_offset=-330;fsrtp=NO;last_scan_time=;signature_def_time=2016/8/9 18:30:0;signature_def_version=2363.0;virus_def_sig=;def_update_in_progress=UNKNOWN;scan_in_progress=UNKNOWN;services_running=UNKNOWN;error=GetLastFullScanTime:Object not foundGetDataFileSignatures:Not implementedIsUpdateInProgress:Not implementedIsFullScanInProgress:Not implemented<parameter name="system_info" value="os_version=2.6.2;sp_version=0;">]

4. **Server requesting for remediation actions**

00303,09 2016/08/10 12:25:45.414 4 admin dsHostChecker.exe OpswatIMC p3088 t1414 opsimc.cpp:91 - 'receiveMessage' Message received from IMV: [<parameter name="remediate" value="product_type=AntiVirus;product_id=5001;product_name=McAfee VirusScan;product_version=18.0.4054;product_sig=0;actions=enable_fsrtp;">]

5. **Client performing policy evaluation again after completing remediation action**

00220,09 2016/08/10 12:25:45.664 4 admin dsHostChecker.exe OpswatIMC p3088 t10A8 opsremedaction.cpp:223 - 'OpswatImcRemed' Successfully finished the remediation action... hence triggering handshake for cid : 1 : and imcid : 1 :

6. **Example of Server requesting client to download ESAP**

01595,09 2017/01/17 10:51:46.461 4 SYSTEM PulseSecureService.exe OpswatIMC p7504 t1EB4 opsimc.cpp:91 - 'receiveMessage' Message received from IMV: [<parameter name="server_details" value="cert_md5=8df1ee431dd2edb0e0a259c0ebff81f2"><parameter name="esap" value="esap_version=3.0.5;opswat_sdk_version=3;fileinfo=name:vmap.dat^md5:53C386420AFE756A79A6AB1B86CA34AC^version:^|name:tables.dat^md5:5E79E5289EEB2C8F579E7FF3A86BC912^version:^|name:scpt.dat^md5:966EC982A8A3D864919FE5A63530DC5A^version:^|name:pinfo.dat^md5:E56FA35B5807321B846A07A92C296421^version:^|name:OESISCore.dll^md5:A2DA096D2427ACEB3135B720077BCBCC^version:3.6.10970.2^|name:Impl_SoftwareProductLib.dll^md5:7E931C95CB2452CA1988FA8ED4D1FF2F^version:3.6.10970.2^|name:Impl_PatchManagementLib.dll^md5:140436101277C79BB91B67AC978DBE95^version:3.6.10970.2^|name:Impl_HdEncLib.dll^md5:F955CDCDB7C74CD13BE74A20B7C62D1F^version:3.6.10970.2^|name:Impl_FirewallLib.dll^md5:C3CA51AB9BB444ADA33DB38032C666D9^version:3.6.10970.2^|name:Impl_AntivirusLib.dll^md5:FFF1B0140A7F98CB0ED936E67AA2F29D^version:3.6.10970.2^|name:FWManager.dll^md5:B828053F7C1220E3E98E2F60F9935D67^version:3.6.10970.2^|name:efc.dat^md5:7A551615F8D47CB5C76C053CD92121BF^version:^|name:CoreUtils.dll^md5:7847A6A5F74FF55C01131EC61BD8EECC^version:3.6.10970.2^|name:AVManagerUnified.dll^md5:E84446DDA4BEAA357E016E29A29BB369^version:3.6.10970.2^|name:64bitProxy.exe^md5:0878846DFD1B9FFCF15AA0585201D985^version:3.6.10970.2^|;downloadFiles=name:UnifiedSDK.zip^type:zip^path:OPSWAT/UnifiedV3/Windows/dlls/UnifiedSDK;"><parameter name="AntiVirus" value="needsMonitoring=0;needsData=1">]

# Errors in user access logs:

## Detection issue

"Anti-Virus software listed in security requirements is not installed".

## RTP issue

Host Checker policy failed on host for user ' reason Rule Endpoint Security 10.5.4 does not comply with policy. Compliance requires real time protection enabled. Windows Defender 4.13.17134.1 does not comply with policy. Compliance requires real time protection enabled.'.

In above, we can ignore windows defender as it is the default AV in Windows.

## Virus definition issue

Host Checker policy failed on host for user Reason McAfee Endpoint Security Threat Prevention 10.5.2.2108 does not comply with policy. Compliance requires latest virus definitions.