Pulse Secure®

ESAP
Release Notes

Contents

Introduction

V2 Unified + V3 SDK Version: Mac and Windows 3.6.11667.2

V4 SDK Version: Windows 4.3.405.0, Mac 4.3.314.0

V3V4 Adapter Version: Windows 4.3.269.0, Mac 4.3.244.0

Note: The SDK embedded in this ESAP version has been tested and qualified to interoperate with an extensive list of endpoint security applications covering most products listed in the supported products list.

Interoperability and Supported Platforms

Please refer to the **ESAP Supported Platforms Guide** for supported versions of browsers and operating systems in this release.

Noteworthy Changes

- Pulse Secure introduced support for consuming the latest OPSWAT SDK Version 4 in 8.2R5 PCS and PPS 5.3 R5 PPS release.
    - OPSWAT SDK's are bundled within our Endpoint Security Assessment Plugin (ESAP). From ESAP 3.0.3 onwards, OPSWAT V4 SDK for Windows and Mac are packaged alongside existing V2 and V3 SDKs.
    - Uploading ESAP 3.0.3 or Later on PCS 8.2R4 and below or PPS 5.3R4 and below release will continue to install and leverage the older Version 2 and Version 3 OPSWAT SDKs. There will be no change in the functionality/usage on PCS 8.2R4 / PPS 5.3R4 and below release versions.
    - Uploading ESAP 3.0.3 or later on PCS 8.2R5 PCS or PPS 5.3R5 releases, we will install OPSWAT V4 SDK version along with V2 and V3 SDKs.
    - On the PCS 8.2R5 and PPS 5.3R5 Admin UI, Administrators have a choice to select whether OPSWAT V3 or V4 SDK will be consumed on the device running PCS 8.2R5 or PPS 5.3R5. Please refer to the section "Activating the OPSWAT SDK Version" in the PCS 8.2R5 and PPS 5.3R5 Administration Guide available on Techpubs website for more information.
    - Endpoint Security Assessment Plug-In (ESAP) provides support for predefined checks on Windows and MAC platforms. ESAP package contains V2, V3 and V4 OPSWAT SDK versions. Support for V2 and V3 OPSWAT SDK is ended. Hence, this ESAP release has only OPSWAT V4 version updated in ESAP package. Refer to KB article http://kb.pulsesecure.net/articles/Pulse_Technical_Bulletin/TSB41055 on Pulse Secure site for more details.

ESAP 3.3.2 and Pulse Connect Secure/Pulse Policy Secure Compatibility Chart

This ESAP package can be installed on the following Pulse Connect Secure/ Pulse Policy Secure software versions.

- PCS 8.3Rx
- PCS 8.2Rx
- PCS 8.1Rx
- PCS 8.0Rx
- PCS 7.4Rx
- PCS 7.3Rx
- PCS 7.2Rx
- PCS 7.1Rx
- PCS 7.0Rx
- PCS 6.5Rx
- PPS 5.4Rx
- PPS 5.3Rx
- PPS 5.2Rx
- PPS 5.1Rx
- PPS 5.0Rx
- PPS 4.4Rx
- PPS 4.3Rx
- PPS 4.2Rx
- PPS 4.1Rx
- PPS 4.0Rx
- PPS 3.1Rx

Note:

- The ESAP package may install and function without any errors on older releases. However, as the install has not been tested, we recommend that it be used only on the above versions of software releases.
- This ESAP package contains V2, V3 and V4 versions of OPSWAT SDK. From the above compatibility chart V4 is applicable only for release above 8.2R5 and 5.3R5.

Support Has Been Added for the Following Products in ESAP 3.3.2

V4 List of Supported Products

Windows OS

Antivirus Products
- Advanced Threat Prevention (2.x)
- Bitdefender Total Security (23.x)
- ESET Endpoint Antivirus (7.x)
- GridinSoft Anti-Malware (4.x)
- McAfee Internet Security (22.x)
- PROSHIELD Antivirus (4.x)
- Trend Micro Titanium Maximum Security (15.x)
- ViRobot 7.0 (6.x)
- ViRobot 7.0 (7.x)

Antispyware Products
- Advanced Threat Prevention (2.x)
- Bitdefender Total Security (23.x)
- ESET Endpoint Antivirus (7.x)
- GridinSoft Anti-Malware (4.x)
- McAfee Internet Security (22.x)
- PROSHIELD Antivirus (4.x)
- Trend Micro Titanium Maximum Security (15.x)
- ViRobot 7.0 (6.x)
- ViRobot 7.0 (7.x)

Firewall Products
- Bitdefender Total Security (23.x)
- McAfee Internet Security (22.x)
- PS-PROFILER McAfee Total Protection (16.0.x)

HardDisk Encryption
- Bitdefender Total Security (23.x)

MAC OS

Antispyware Products
- Avast Business Antivirus (13.x)
- Mcafee Multi Access - Internet Security (4.x)
- Trend Micro Internet Security (9.x)

Antivirus Products

- Avast Business Antivirus (13.x)
- Mcafee Multi Access - Internet Security (4.x)
- Trend Micro Internet Security (9.x)

Fixed Issues in ESAP 3.3.2

The following table lists Fixed issues in ESAP3.3.2.

Problem Report Number	Summary
PRS-370147	**Summary:** Need to Add support for BitDefender Total Security Antivirus 23.x.
PRS-370016	**Summary:** Hostchecker does not detect the AV when the AV process is killed using process hacker tool for "Symantec Endpoint protection 14.0".
PRS-369894	**Summary** Add support for Trend Micro Titanium Maximum Security (15.x).
PRS-369846	**Summary** Host Checker fails to detect Kaspersky Endpoint Security 11.x.
PRS-369843	**Summary** Check RTP fails for Kaspersky Internet Security 19.x with v4 SDK.
PRS-368830	**Summary** Host checker is not detecting Trend Micro Security Agent 6.5.1279.
PRS-368497	**Summary** Host checker checking for Trend Micro Officescan client 10.6.x failing on ESAP 3.2.9 V4 SDK.
PRS-368484	**Summary** Add support for Virobot 7.0 for Windows.
PRS-368439	**Summary** Norton Internet Security 7.8 fails to GetRealTimeProtectionState on MAC.
PRS-367873	**Summary** Request to add support for GetRealTimeProtection, GetDefinitionState (last_update and version) & GetLastScanTime for ESET Endpoint Antivirus 7.0.2073.1 Antivirus.
PRS-367159	**Summary** Add Dell Advanced Threat Protection in the ESAP supported AV list.
PRS-366388	**Summary** Failed to detect scan_time under GetLastScanTime for ESET Endpoint Antivirus 6.6.2078.5.
PRS-366110	**Summary** Host checker failing for Kaspersky Endpoint security 10.x in ESAP 3.2.7 V4 SDK.
PRS-364448	**Summary** Add support for Trend Micro Security 3.0.3044 AV for MAC 10.13.2 (Japanese OS).
PRS-364155	**Summary** GetRealTimeProtectionState fails for Norton Internet Security 7.7 for MAC.
PRS-362678	**Summary** Host checker fails to detect Cisco Advanced Malware Protection 1.7.0 in MAC machine.

Upgrade Issues in ESAP3.3.2

The following table lists upgrade issues in ESAP 3.3.2.

#	Description
OPSWAT	
1	"Spyware Terminator 3.x" is replaced with the correct name, "Spyware Terminator (AntiSpyWare) 3.x" under list of available AntiSpyWare products. Upgrade from ESAP 2.1.7 or lower fails if an AntiSpyWare policy is configured and "Spyware Terminator 3.x" is selected. To successfully upgrade to ESAP2.2.6 or greater, unselect the product. After the upgrade, you can select "Spyware Terminator (AntiSpyWare) 3.x". This doesn't result in any loss of functionality.
2	G Data Notebook 20.x is not supported in ESAP1.8.0 or greater. Upgrade from ESAP1.7.5 or lower fails if an Antivirus or an Antispyware policy is configured and GData Notebook 20.x is selected. To successfully upgrade to ESAP1.8.0 or greater, unselect the product.
3	G Data Internet Security 22.x of Firewall is renamed to G Data Firewall 22.x. Upgrade from ESAP 1.7.5 or lower fails if a Firewall policy configured and G Data Internet Security 22.x is selected. To successfully upgrade to ESAP1.7.6 or greater, unselect the product and select 'G Data Firewall 22.x'. There is no loss of functionality.
4	AntiSpyWare of Kaspersky Anti-virus for Windows Workstations 6.x is renamed to Kaspersky Anti-virus for Windows Workstations 6.x [AntiSpyWare]. Upgrade from ESAP1.6.4 or lower fails if an Antispyware policy is configured where "Require Specific Products" is checked and Kaspersky Anti-virus for Windows Workstations 6.x is selected. To successfully upgrade to ESAP1.6.5 or greater, unselect the product and select Kaspersky Anti-virus for Windows Workstations 6.x [AntiSpyWare]. There is no loss of functionality.
5	Upgrade from ESAP1.5.2 or older fails if a firewall policy is configured where "Require Specific Products" is checked and McAfee Desktop Firewall (8.0) is selected. The upgrade doesn't fail if McAfee Desktop Firewall (8.0.x) is selected. To successfully upgrade to ESAP 1.5.3 or greater, unselect McAfee Desktop Firewall (8.0) and select McAfee Desktop Firewall (8.0.x). This doesn't result in any loss of functionality.
Shavlik	
1	The following note applies only to the patch assessment functionality. When upgrading ESAP from a 1.5.1 or older release to the current release, the services on the SA or IC device needs to be restarted for the binaries on the endpoint to be automatically upgraded. (470003, 491073)

Known Issues/Limitations in ESAP3.3.2

The following table lists known issues/limitations in ESAP3.3.2.

Problem Report Number	Release Note
OPSWAT	
958840, 845980	Remediation of Windows Firewall 8 in agentless mode requires administrative privileges and UAC should be turned off.
502783	Endpoint Protection 11.x/12.x is not performed when UAC is enabled or if the scan logs have been deleted or if system scans has never been performed.
495041	The password protection option in the Sunbelt Kerio Firewall product is not supported.
	Remediation and detection of Windows Firewall 7 and Vista in agentless mode requires administrative privileges and UAC to be turned off.
	For Symantec, Hosted Endpoint Protection 2.x installed on server operating systems, GetLastFullSystemScanTime function will return either the last full system scan time or last quick system scan time. Server operating systems include, Server 2008, Server 2008 R2, Server 2003 and XP x64.
785223	FSRTP status for avast! Free Antivirus 7.x will not be detected until user manually configures FSRTP status at least once. That is, user should turn off "File System Shield" and turn it on.
950123	Signatures cannot be downloaded with Trend Micro Office scan Client 10.5 and 10.6. Therefore, the remediation functionality for failing the virus definition check is not supported for Trend Micro Office scan Client 10.5 and 10.6. This is because the executable required to support this functionality is not bundled as part of the TrendMicro product.
PRS-318680	Microsoft's API, will only report the drives which the system has access to. Therefore, BitLocker Drive Encryption to detect the drive, the drive should be in "unlock" state.
PRS-357241	Host checker is failing to detect Bitlocker HD encryption 10.x in Windows RS3 via browser, but detects with Pulse.

Documentation

Pulse documentation is available at **https://www.pulsesecure.net/techpubs/**

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@pulsesecure.net.**

Technical Support

When you need additional information or assistance, you can contact "Pulse Secure Global Support Center (PSGSC):

· **https://www.pulsesecure.net/support**

· **support@pulsesecure.net**

· Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support website **https://www.pulsesecure.net/support.**

Revision History

The following table lists the revision history for this document.

Revision	Date	Description
1.0	November 2018	Initial Publication – 9.0R1 Beta