ESAP

Release Notes

Contents

Introduction

V2 Unified + V3 SDK Version: Mac and Windows 3.6.11644.2

V4 SDK Version: Windows 4.2.1428.0, Mac 4.2.1245.0

V3V4 Adapter Version: Windows 4.2.1314.0, Mac 4.2.456.0

ⓘ   **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 Tec pubs website for more information.

ESAP 3.1.8 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**

> **ⓘ** **Note1:** 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.
> **Note2:** 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 ESAP3.1.8

V4 list of supported products:

Windows OS

Antivirus Products

BullGuard Internet Security (18.x)
Symantec Endpoint Protection (14.0.3.x)
Symantec Endpoint Protection Cloud (22.11..x)
ウイルスバスター クラウド (12.x)

Firewall Products

BullGuard Internet Security (18.x)
Symantec Endpoint Protection (14.0.3.x)
Symantec Endpoint Protection Cloud (22.11..x)

Antispyware Products

BullGuard Internet Security (18.x)
Symantec Endpoint Protection (14.0.3.x)
Symantec Endpoint Protection Cloud (22.11..x)
ウイルスバスター クラウド (12.x)

MAC OS

Antivirus Products

CrowdStrike Falcon (3.x)
Kaspersky Anti-Virus (10.x)
Sentinel Agent (2.x)
Symantec Endpoint Protection (14.0.2.x)

Antispyware Products

CrowdStrike Falcon (3.x)
Kaspersky Anti-Virus (10.x)
Sentinel Agent (2.x)
Symantec Endpoint Protection (14.0.2.x)

V3 list of supported products:

Windows OS

Antivirus Products

AVG Internet Security (17.x)
Bitdefender Internet Security (22.x)
Bitdefender Total Security (22.x)
BullGuard Internet Security (18.x)
ESET Internet Security (11.x)
F-Secure Client Security (13.x)
Panda Free Antivirus (17.x)
Panda Free Antivirus (18.x)
Sophos Cloud Endpoint (11.x)

Antispyware Products

AVG Internet Security (17.x)

Bitdefender Internet Security (22.x)
Bitdefender Total Security (22.x)
BullGuard Internet Security (18.x)
ESET Internet Security (11.x)
F-Secure Client Security (13.x)
Panda Free Antivirus (17.x)
Panda Free Antivirus (18.x)
Sophos Cloud Endpoint (11.x)

Firewall Products

AVG Internet Security (17.x)
Bitdefender Internet Security (22.x)
Bitdefender Total Security (22.x)
BullGuard Internet Security (18.x)
ESET Internet Security (11.x)
F-Secure Client Security (13.x)

MAC OS

Antivirus Products

Avast Mac Security (13.x)
CrowdStrike Falcon (3.x)

Antispyware Products

Avast Mac Security (13.x)
CrowdStrike Falcon (3.x)

Issues Fixed in ESAP3.1.8

V4 List of OPSWAT issues fixed:

1. Sophos Endpoint Security and Control 10.7.X Virus definition complaince check for number of updates fails on sdk v4(PRS-358165)

2. Add support for Cybereason ActiveProbe 17.x in V4 SDK(PRS-358854)

3. Host Checker: Need to Add Support for Symantec Endpoint Protection 14.0.3.x in V3 and V4 SDK(PRS-358234)

4. Host Checker detection is failing for Kaspersky Endpoint Security 10.2.6.3733 (Enterprise edition)(PRS-357696)

5. Add support for Cybereason ActiveProbe 17.x in V4 SDK(PRS-358854)

V3 List of OPSWAT issues fixed:

1. Need support for Norton Internet Security 22.x system scan remediation in V3 SDK and V4 SDK (PRS-357402)

2. Host Checker stucks in "Loading Components" after upgrading to ESAP 3.1.0(PRS-354549)

3. Host Checker: Need to Add Support for ESET Internet Security 11.x in V3 and V4 SDK(PRS-358452)
4. Bitdefender Internet Security 2018 fails last full scan check(PRS-358121)
5. Need to add support for Trend Micro maximum Security 12.x(PRS-357740)
6. Host Checker: Need to add support for F-Secure Client Security 13.x(PRS-357813)
7. Host Checker: Need to Add Support for AVG Internet Security 2017 in V3 SDK.(PRS-358060)
8. Host check failing when configuring Patch management rule on MAC OS with agentless connection for SDKV3(PRS-358219)
9. ESAP: Add support for BullGuard Internet Security 18.x(PRS-358237)
10. ESAP: Support for CrowdStrike Falcon Sensor 3.X for MAC OSx(PRS-357503)

Upgrade Issues in ESAP3.1.8

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 ESAP3.1.8

OPSWAT:

1. Remediation of Windows Firewall 8 in agentless mode requires administrative privileges and UAC should be turned off. (958840, 845980)

2. 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. (502783)

3. The password protection option in the Sunbelt Kerio Firewall product is not supported. (495041)

4. Remediation and detection of Windows Firewall 7 and Vista in agentless mode requires administrative privileges and UAC to be turned off.

5. 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.

6. 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. (785223)

7. 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. (950123)

8. 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-318680)

9. Hostchecker is failing to detect Bitlocker HD encryption 10.x in Windows RS3 via browser, but detects with Pulse(PRS-357241)

Documentation

Pulse Secure 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 the Pulse Secure Global Support Center (PSGSC):

- Pulse Secure Global Support Center (PSGSC): 1-844 751 7629 (Toll Free, US)
- All other Countries - **https://www.pulsesecure.net/support/support-contacts** call us at (408) 372-9600
- For more technical support resources, browse the support website (http://www.pulsesecure.net/support).

Revision History

Table **1** lists the revision history for this document.

Table 1 Revision History

Revision	Description
1.0 – December 2017	Initial publication.