Pulse Secure

ESAP

Release Notes

Contents

Introduction

SDK Version: Mac and Windows 3.6.10547.2 (V2 Unified + V3).

ⓘ **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

This ESAP version contains additional files in preparation of new features that will be enabled in the next major release of PCS and PPS.

ESAP 2.9.3 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.

- **SA 8.2Rx**
- **SA 8.1Rx**
- **SA 8.0Rx**
- **SA 7.4Rx**
- **SA 7.3Rx**
- **SA 7.2Rx**
- **SA 7.1Rx**
- **SA 7.0Rx**
- **SA 6.5Rx**
- **UAC 5.3Rx**
- **UAC 5.2Rx**
- **UAC 5.1Rx**
- **UAC 5.0Rx**
- **UAC 4.4Rx**
- **UAC 4.3Rx**
- **UAC 4.2Rx**
- **UAC 4.1Rx**
- **UAC 4.0Rx**
- **UAC 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.

Support has been added for the following products in ESAP2.9.3

Operating System Detection

Chrome OS detection is now supported as an Operating System check.

Windows OS

Antivirus Products

360 Total Security (8.x)
avast! Premier (11.x)

Antispyware Products

avast! Premier (11.x)

Firewall Products

Trend Micro Deep Security (Firewall) (9.x)

MAC OS

Antivirus Products

Norton Security (7.x)

Issues Fixed in ESAP2.9.3

OPSWAT issues fixed:

1. Avira Free Antivirus 15.x failing for RTP check - GERMAN VERSION (PRS-339449)
2. ESET Endpoint 6.3.2016.0 fails CheckRTP (PRS-339372)
3. Host Checker fails to detect CheckRTP for ESET NOD32 Antivirus 9.x (9.0.349.0) (PRS-338774)
4. RTP check fails for F-Secure PSB Workstation Security 9.34.12117.0. (PRS-338418)
5. Trend Micro Office Scan return incorrect GetDataFileTime (PRS-338364)
6. Host Checker fails to detect CheckRTP for Trend Micro Deep Security 9.6.1308 (PRS-338357)
7. Kaspersky Endpoint Security 10 for Windows - Encryption not detected (PRS-337592)
8. Detection fails for McAfee Endpoint Security 10.X (PRS-337471)
9. Trend Micro OfficeScan Client fails to detect latest Virus definition files (PRS-336860)
10. Detection failing for Norton Security Deluxe and Norton Security Premium (PRS-336328)

New OPSWAT products supported/ Enhancement to existing OPSWAT products

1. Support needed for avast! Premier (11.x) (PRS-339171)
2. Add support for Add Support for 360 Total Security Essentials 8.x (PRS-339286)
3.

Upgrade Issues in ESAP2.9.3

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 ESAP2.9.3

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 Officescan Client 10.5 and 10.6. Therefore the remediation functionality for failing the virus definition check is not supported for Trend Micro Officescan 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)

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 - Apr 2016	Initial publication.