

ESAP 2.6.6 Release Notes

SDK Version: Mac and Windows 3.6.9366.2 (V2 Unified + V3)

Note: The SDK embedded in this ESAP version has been tested and qualified to interoperate with a limited list of end endpoint security applications covering most of the widely used products listed in the supported products list, all new products added to the supported list and all products for which a bug fix was added 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 SA and IC.

ESAP 2.6.6 and Junos Pulse Secure Access/Access Control Service Compatibility Chart:

This ESAP package can be installed on the following Junos Pulse Secure Access/Access Control Service software versions.

- SA 8.0Rx
- SA 7.4Rx
- SA 7.3Rx
- SA 7.2Rx
- SA 7.1Rx
- SA 7.0Rx
- SA 6.5Rx
- 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 ESAP2.6.6

Windows OS

Antivirus Products

[360Safe.com] 360 Total Security (4.x)
[ArcaBit] Arcabit Endpoint AntiVirus (2014.x)
[ArcaBit] Arcabit Endpoint Security (2014.x)
[ArcaBit] ArcaVir Antivirus (2014.x)
[ArcaBit] ArcaVir Internet Security (2014.x)
[Avira GmbH] Avira Antivirus Pro (14.x)
[MSecure Data Labs] MSecure Antivirus (9.x)
[Agnitum Ltd.] Outpost Security Suite Pro (9.x)
[TrustPort, a.s.] TrustPort Internet Security (14.x)

Antispyware Products

[ArcaBit] Arcabit Endpoint AntiVirus (2014.x)
[ArcaBit] Arcabit Endpoint Security (2014.x)
[ArcaBit] ArcaVir Antivirus (2014.x)
[ArcaBit] ArcaVir Internet Security (2014.x)
[Avira GmbH] Avira Antivirus Pro (14.x)
[MSecure Data Labs] MSecure Antivirus (9.x)
[Agnitum Ltd.] Outpost Security Suite Pro (9.x)
[TrustPort, a.s.] TrustPort Internet Security (14.x)

Firewall Products

[ArcaBit] Arcabit Endpoint Security (2014.x)
[ArcaBit] ArcaVir Internet Security (2014.x)
[Agnitum Ltd.] Outpost Security Suite Pro (9.x)
[TrustPort, a.s.] TrustPort Internet Security (14.x)

Mac OS

Antivirus Products

[AVG Technologies] AVG AntiVirus (14.x)
[Bitdefender] Bitdefender Antivirus for Mac (3.x)

Antispyware Products

[AVG Technologies] AVG AntiVirus (14.x)

Issues Fixed in ESAP2.6.6

OPSWAT issues fixed:

1. Signature update remediation not seems to be working for avast! Internet Security 8.x and Windows Defender 4.x (921028)
2. Opswat SDK is not detecting the AV product. It is detected as "Other AVG Technologies Antivirus" (986432)
3. Virus definition check for Avira Free Antivirus 14.0.4.672 fails for both number of days and number of updates (1004607)

New OPSWAT products supported/ Enhancement to existing OPSWAT products:

1. CheckRTP() APIs for Trend Micro Security 2.0.1036 in Mac require Root permissions(973690)

Upgrade Issues in ESAP2.6.6:

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 InternetSecurity 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 InternetSecurity 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 ESAP2.6.6:

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. FS RTP status for avast! Free Antivirus 7.x will not be detected until user manually configures FS RTP 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)