ESAP 2.6.3 Release Notes

SDK Version: Mac and Windows 3.6.9108.2 (V2 Unified + V3)

Noteworthy changes:

- Starting ESAP 2.6.1, each release contains additional files in preparation of new features that will be enabled in the next major release of SA and IC.

ESAP 2.6.3 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 ESAP2.6.3

Windows OS

Antivirus Products
[AVG Technologies] AVG CloudCare Antivirus (2014.x)
[Tech Guard Technologies] Tech Guard Internet Security (1.x)

Antispyware Products
[AVG Technologies] AVG CloudCare Antivirus (2014.x)
[Tech Guard Technologies] Tech Guard Internet Security (1.x)

Mac OS

Antivirus Products
[Eset Software] ESET Cybersecurity (6.x)
[Eset Software] ESET Cybersecurity Pro (6.x)

Issues Fixed in ESAP2.6.3

OPSWAT issues fixed:

1. Symantec Endpoint Protection 12.1.x failing for Last Full System scan checks(978752)

2. Checkfsrtp returns invalid state for F-Secure PSB Workstation Security 10.x(987908)

3. GetLastScanTime API is taking a lot of time to respond causing failures (988779)

4. GetDataFileTime API is returning incorrect value for Trend Micro OfficeScan Client 11.0.1028 (990825)

New OPSWAT products supported/ Enhancement to existing OPSWAT products:

1. API support for detecting Signature status, triggering signature download, detecting scan time, triggering scan and checking scan is in progress for AVG Internet security 2014 (927635)

2. Support need to be added for AVG Cloudcare 2014

Upgrade Issues in ESAP2.6.3:

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 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 ESAP2.6.3:

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)