ESAP 2.1.5 Release Notes

ESAP 2.1.5 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.

- o SA 7.2Rx
- o SA 7.1Rx
- o SA 7.0Rx
- o SA 6.5Rx
- o UAC 4.2Rx
- o UAC 4.1Rx
- o UAC 4.0Rx
- o 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 ESAP2.1.5

Windows OS

Antivirus Products

[Microsoft Corp.] Microsoft Security Essentials 4.x
[Beijing Rising Technology Corp. Ltd.] Rising Antivirus Network Edition 23.x
[GData Software AG] G Data TotalSecurity 21.x
[K7 Computing Pvt. Ltd.] K7UltimateSecurity 12.x
[Symantec Corp.] Norton Security Scan 3.x

Antispyware Products

[Microsoft Corp.] Microsoft Security Essentials 4.x
[GData Software AG] G Data TotalSecurity 21.x
[K7 Computing Pvt. Ltd.] K7UltimateSecurity 12.x

Firewall Products

[K7 Computing Pvt. Ltd.] K7UltimateSecurity 12.x
[GData Software AG] G Data Firewall 23.x

Macintosh

Antivirus Products

[ALWIL Software] avast! Antivirus 3.x
[SOFTWIN] BitDefender 2.x
[Sophos Plc.] Sophos Anti-Virus 8.x
[Symantec Corp.] Symantec AntiVirus 10.x

Issues Fixed in ESAP2.1.5:

OPSWAT:

1. The remediation feature, " Turn On Real Time Protection" is not supported for F-Secure AV 9.x. (754072)
2. The remediation feature, "Download latest virus definition files" is not supported for F-Secure Anti-Virus (9.x). (731753)
3. Symantec Endpoint Protection 12.x for MAC is not getting detected. (774676)

Upgrade Issues in ESAP2.1.5:

OPSWAT:

1. 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.

2. 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.

3. 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.

4. 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 ESAP2.1.5:

OPSWAT:

1. When Host Checker checks for on/off status of McAfee Personal Firewall 9.x, 10.x, it opens and closes the McAfee UI. Workaround is to disable rule-monitoring if it is enabled so that the UI pops up only during HC updates.

2. The Anti-Virus Check for Norton Internet Security 2009 (v16) and Norton AntiVirus 2009 on a non-XP-32bit machine with security centre disabled gives incorrect results. To workaround this issue, enable the Auto-Protect feature found at the Real-Time Protection tab in Anti-Virus or Internet Security Options.

3. On Vista and Windows 7 remediation action for last scan time of Symantec

Endpoint Protection 11.x/12.x is not performed when UAC is enabled or if the scan logs have been deleted or if system scan has never been performed. (502783)

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

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

6. The detection of Last successful full system scan time for Microsoft Forefront Endpoint Protection 2010 requires administrative privileges. (698839)

7. Kaspersky Anti-Virus for Windows Workstations 6.x - Firewall will not be detected for a restricted user.