

ESAP 2.3.3 Release Notes

ESAP 2.3.3 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 7.3Rx
- SA 7.2Rx
- SA 7.1Rx
- SA 7.0Rx
- SA 6.5Rx
- 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 ESAP2.3.3

Windows OS

Antivirus Products

[Trend Micro, Inc.] Trend Micro Worry Free Business Security Agent (18.x)
[360Safe.com] Security 360 (1.x)
[SecurityCoverage, Inc.] SecureIT (2012.x)
Max Secure Anti Virus Pro (19.x)
Max Secure Anti Virus Plus (19.x)
Max Internet Security (19.x)
[F-Secure Corp.] FSecure Client Security (9.x)
ALYac Internet Security (2.x)
Advanced SystemCare with Antivirus (5.x)
[360Safe.com] 360 Antivirus (3.x)

Antispyware Products

[Trend Micro, Inc.] Trend Micro Worry Free Business Security Agent (18.x)
[360Safe.com] Security 360 (1.x)
[SecurityCoverage, Inc.] SecureIT (2012.x)
Max Secure Anti Virus Pro (19.x)
Max Secure Anti Virus Plus (19.x)
Max Internet Security (19.x)
[F-Secure Corp.] FSecure Client Security (9.x)
[Bitdefender] Bitdefender Antivirus Plus (15.x)
ALYac Internet Security (2.x)
Advanced SystemCare with Antivirus (5.x)

Firewall Products

[Trend Micro, Inc.] Trend Micro Worry Free Business Security Agent (18.x)
[SecurityCoverage, Inc.] SecureIT (2012.x)
Max Internet Security (19.x)
[F-Secure Corp.] FSecure Client Security (9.x)
ALYac Internet Security (2.x)

MAC OS

Antivirus Products

[Kaspersky Labs] Kaspersky AntiVirus (13.x)
[Avira GmbH] Avira Mac Security (1.x)

Issues Fixed in ESAP2.3.3:

OPSWAT:

1. For Mac Sphos, AV detection Apis are taking excessive time (827891)
2. Virus definition check fails for AVG Anti-Virus Free Edition 2013 (834778)
3. LastScanTime though implemented is not working for AVG Anti-Virus Free Edition 2013 (834800)
4. GetLastFullSystemScanTime for Sophos Antivirus 10.x is returnin general error after the log file SAV.txt gets renamed (845306)

Upgrade Issues in ESAP2.3.3:

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 ESAP2.3.3:

OPSWAT:

1. Auto remediation for Windows Firewall (Win8) does not work for agentless HC (845980).
2. 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.
3. 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.
4. 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)
5. The password protection option in the Sunbelt Kerio Firewall product is not

supported. (495041)

6. Remediation and detection of Windows Firewall 7 and Vista in agentless mode requires administrative privileges and UAC to be turned off.
7. 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.
8. 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)