SEQRITE

Seqrite Endpoint Security 7.60

Service Pack 5.0

Release Notes

Document Version 1.0

Copyright Information

Trademarks

Contents

Revision History

The information in this document is provided for the sole use of Quick Heal Research and Development, and Support Team. It is strictly forbidden to publish or distribute any part of this document to any other party.

Version	Date	Comment
1.0	23 October 2019	Seqrite Endpoint Security 7.60 Service Pack 1.0 released
1.1	10 February 2020	Seqrite Endpoint Security 7.60 Service Pack 2.0 released
1.2	16 June 2020	Seqrite Endpoint Security 7.60 Service Pack 3.0 released
1.3	21 June 2021	Seqrite Endpoint Security 7.60 Service Pack 5.0 released

Abstract

Seqrite Endpoint Security 7.60 Service Pack 5.0 Release Notes contains the following information:

- Purpose of Service Pack 5.0
- Application of Service Pack 5.0

Purpose of Service Pack 5.0

Service Pack 5.0 Enhancements and Bug Fixes

Seqrite Endpoint Security Service Pack 5.0 is released for the following enhancements and bug fixes.

Service Pack 5.0 Enhancements

- Endpoint IP Address details included in IDS/IPS, Port Scan and DDoS Report.
- Local and Remote Port details included in the Firewall Report.
- Complete Asset details of all endpoints can be exported in a single report from EPS web console > Clients > Assets > Download Complete Asset Details button.
- Endpoint Name and IP Address details included in SMS Notification for Virus and Ransomware attack.
- Option to configure OCR and File Fingerprinting settings added in EPS web console > Settings > Data Loss Prevention (DLP).
- Enhancement in client deployment method through Active Directory to support enumeration of large number of objects (10,000) in Active Directory while synchronizing Active Directory.
- Patch Management reports section now contains additional reports for Up-to-date, Patch Scan failed, and Patch Installation failed endpoints. Earlier only Missing and Installed patches reports options were available.
- The default applications listed in Application Control feature will be updated automatically to the latest version. The latest application version signatures will be released periodically through AV updates.
- Upgrade support is added for Windows 10 operating system through Seqrite Patch Management.

  Configure Seqrite Patch Server to get upgrade patches for Windows 10 operating system from “Seqrite EPS Web console > Admin Settings > Server > Patch Management > Configure Patch Server > Filters” page.

  In the Products tab, under Microsoft > Windows, select “Windows 10” and “Windows 10, version 1903 and later” and In the Categories tab, select the “Upgrades”.
- Consolidated Dashboard and Manage Secondary Server tabs will not be visible on EPS web console dashboard if EPS server does not have Secondary EPS server.
- On EPS dashboard top 10 incident count will be displayed instead of top 5. The top 10 incident can be exported to csv report.

- Notifications are displayed on browser if any website is blocked by Web Security feature. Earlier only alert messages used to appear. This feature is applicable only for clients installed on Windows platform.
- Manual and web-based help with details about changes released through Service Pack 5.0 included.

Service Pack 5.0 Bug Fixes

- EPS-16269 - Getting "Aw Snap error" while launching chrome browser in Secure browser and Safe Banking
- EPS-18310 - Unable to block data transfer from Any Desk through DLP
- EPS-11814 - Unable to add google drive application for exclusion from DLP in some cases
- EPS-19716 - DLP license count is showing zero if EPS is installed in multi-server mode
- EPS-18598 - Incorrect reports are displayed for DLP if multiple endpoints have same user name
- EPS-17083 - EPS console showing “Secondary servers are unregistered.” under Event logs even if secondary server is not configured
- EPS-16618 - Definition files corrupt ID-3 issue while applying the updates on client AV
- EPS-18518 - Unable to manage Non-MS product if upstream patch server is WSUS
- EPS-19314 - Unable to install Patches on Endpoints due to Endpoint Selection grayed out
- EPS-23164 - Patch sync is getting failed and system getting freeze while patch synchronization from WSUS on Windows Server 2016
- EPS-15818 - Patch Scan results for Missing patches are not reflected on EPS Console > Reports > Patch Management > Patch Status in specific scenario
- EPS-17648 - Patch Management Reports not getting generated in PDF Format from Mozilla Firefox and Google Chrome
- EPS-16741 - Schedule Scan is not getting performed on endpoints due to ClScanSet.dat file corruption
- EPS-16962 - Policy with given name already exists error while creating new policy
- EPS-13922 - Incorrect endpoint count for Top Vulnerabilities and Top incidents are displayed on EPS web console dashboard in specific cases
- EPS-14349 - Sorting of offline clients in ascending/descending order from EPS web console dashboard does not works due to mismatch in sequence of columns
- EPS-16715 - EPS edition and some features are not displayed in EPS web console if higher version of EPS Server is installed in multi-server mode on Secondary EPS Server EPS edition is displayed as SME on EPS web console dashboard

- EPS-14275 - Status of Roaming client shows offline on EPS dashboard even the though Roaming Clients are connected to Internet
- EPS-15821 - Roaming Clients not getting installed/activated even though EPS Server has required remaining license to accommodate new Client installation/activation
- EPS-16557 - Unable to add application under trusted email client protection on EPS web console > Settings > Email Settings > Enable Trusted Email Client Protection if the file name consists of multiple extensions
- EPS-16561 - Redirection setting for selected clients getting revoked in some cases
- EPS-15692 - Agent server service goes in not responding state and does not responds to client requests
- EPS-15352 - Delay in operation of Tally application if IDS/IPS Protection is enabled on Tally Server
- EPS-13914 - Unable to Approve Sales Order/ Purchase Order in MS Dynamic ERP using Digital Signature if 'Report Source of Infection' is enabled on EPS Console under Scan Settings>Virus Protection settings

Service Pack 3.0 Bug Fixes

Seqrite Endpoint Security Service Pack 3.0 is released for the following bug fixes.

- Windows Firewall gets Turned ON post applying Service Pack 2 as Seqrite was unable to convey its firewall status to WSC due to mismatch signing hash in wsutil.dll
- EPS-16722 - Failed to apply service pack on EPS Server due to missing registry entry of UpdMngr.exe at 'Wow6432Node > App Paths' on Windows 2008 and below 64-bit operating system

Service Pack 2.0 Enhancements and Bug Fixes

Seqrite Endpoint Security Service Pack 2.0 is released for the following Enhancements and Bug Fixes.

Service Pack 2.0 Enhancements

- Recovery actions for Agent Server and Update Manager service for first and second failure

Service Pack 2.0 Bug fixes

- EPS-15070 - Client Agent 7.60 downloads v17.00 builds while redirection from EPS 7.4 to EPS 7.60 after applying Service Pack 1.0
- EPS-15082 - Explorer.exe is getting crashed due to overlayicon.dll

- EPS-15688 - Notepad/MS Word application getting crashed due to overlayicon.dll
- EPS-15075 - Vulnerability Scan report shows false vulnerability for Windows 10 operating systems
- EPS-15351 - Unable to connect RDP post installing EPS 7.60 client on Windows Server 2003 R2 and 2008 R2
- EPS-15820 - Agent Server 7.60 service crashes randomly
- EPS-15692 - Agent server service resetting (/not responding) client communication on port 5057
- EPS-15706 - Asset information of Hard Disk and Memory showing changed as 0 GB in EPS Reports and Notification Emails
- EPS-16027 - Incorrect Mac Address showing in Asset Report
- EPS-13254 - Asset Management notifies change for Motherboard due to space after Motherboard name

Service Pack 1.0 Enhancements and Bug Fixes

Service Pack 1.0 Enhancements

- Policy Status Enhancement:
  - On policy change, server will maintain one more queue to check policy status.
  - If policy is applied at AV and status is still pending in database, we will mark it as applied.
  - A log file ‘policy.log’ will be maintained on EPS Server Event log folder.
- Recovery action for Client Agent service for first and second failure.
- Randomization during EPS client start-up
  - On start-up, if client is not able to connect to server, it will try after random time interval between 1 to 5 minutes.
  - Previously client used to connect after 30 seconds.
  - This randomization to reduce concurrent request to server from clients.
- Using ICMP for checking server availability for Roaming Platform
  - Client will now use ICMP protocol to check if there is connectivity to server.
  - If that fails, it will try to connect with normal TCP port.
  - If that too fails, it will connect to roaming server.

Service Pack 1.0 Bug fixes

- EPS-11478 - MySQL table consuming gigantic space on installed location of disk
- EPS-11839 - Policy status for clients shows pending on EPS Server due to corruption of varconf.dat at client
- EPS-14042 - Policy status for clients shows pending on EPS Server due to corruption of admnlink.dat at client
- AVCE-1436 - Network data of SMB/SMB2 protocol (445/139 ports) taking long time to access due to IDS/IPS protection
- AVCE-1836 - Data saving on network location takes more time post installation of client
- AVCE-1688 - Failed to send PDF attachment with Busy Accounting software due to Virus Protection
- EPS-12072 - Unable to send mail from Thunderbird

Application of Service Pack 5.0

Service Pack 5.0 will be applied automatically if **Automatic installation of the Service Pack** check box is selected under **Admin Settings > Server > General** from EPS Web Console. If the above check box is not selected, manually execute acsvpack.exe from the following path:

C:\Program Files\Seqrite\Endpoint Security 7.60\Admin\web\build\

Notes:

1. On EPS Client, Service pack 5.0 will be applied only if Virus database date is 03-June-2021 or later and AV Build version is 18.00 (11.2.1.2) or 18.00 (11.2.1.3).
2. Service Pack 4.0 was not released globally. It was a controlled release.
3. Post applying Service Pack 5.0, system restart is mandatory to load the updated binaries.
4. If Service Pack 5.0 is failed to apply on the EPS server, provide us the following Information for analysis:
   - Installed Seqrite Endpoint Security build details and system information.
   - 'genpch.log' file from C:\Logs folder.

   If the Service pack is applied successfully, then 'genpch.log' will be deleted.
5. If Service Pack 5.0 is failed to apply on the Client, provide us the following Information for analysis:
   - System information.
   - 'accabldn.log' and 'accasrvc.log' files located in 'Client Agent 7.60\eventlog' folder.
   - genpch.log' file from C:\Logs folder.
   - If the Service Pack 5.0 is applied successfully, then 'genpch.log' will be deleted.