Seqrite Endpoint Security 7.60

Service Pack 2.0

Release Notes

Document Version 1.0

10 February 2020

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 Oct 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

Abstract

Seqrite Endpoint Security 7.60 Service Pack 2.0 Release Notes contains the following information:

- Purpose of Service Pack 2.0
- Application of Service Pack 2.0

Purpose of Service Pack 2.0

Service Pack 2.0 Bug Fixes and Enhancements

Seqrite Endpoint Security Service Pack 2 is released for the following bug fixes and enhancements,

Service Pack 2.0 Bug fixes

1. EPS-15070 - Client Agent 7.60 downloads v17.00 builds while redirection from EPS 7.4 to EPS 7.6 after applying SP1.
2. EPS-15082 - Explorer.exe is getting crashed due to overlayicon.dll
3. EPS-15688 - Notepad/MS Word application getting crashed due to overlayicon.dll
4. EPS-15075 - Vulnerability Scan report shows false vulnerability for Windows 10 Operating Systems.
5. EPS-15689 - File Copy/Transfer is not blocked for Anydesk application with DLP
6. EPS-15351 - Unable to connect RDP Post installing SEPS 7.60 Client on Windows Server 2003R2
7. EPS-15812 - Unable to connect RDP Post installing SEPS 7.60 Client on Windows Server 2008 R2
8. EPS-15820 - Agent Server 7.4 service crashes randomly.
9. EPS-15706: Asset Information of Hard Disk and Memory Showing changed as 0GB in EPS Reports and Notification Emails.
10. EPS-16027 - Incorrect Mac Address Showing in Asset Report.
11. EPS-13254 – Asset Management notifies change for Motherboard due to space after Motherboard name.

Service Pack 2.0 Enhancements

1. Build download URL will be written in accaconf.ini for downloading the AV builds for new installation and client redirection, post applying the service pack.

   Example: buildurl: http://10.10.2.10:8101/ALLBUILDS
2. Recovery actions for Agent Server and Update Manager service for first and second failure.

Service Pack 1.0 Bug Fixes and Enhancements

Service Pack 1.0 Bug fixes

1. EPS-11478 - MySQL table consuming gigantic space on installed location of disk.
2. EPS-11839 - Policy status for clients shows pending on EPS Server due to corruption of varconf.dat at client.
3. EPS-14042 - Policy status for clients shows pending on EPS Server due to corruption of admnlink.dat at client.
4. AVCE-1436 - Network data of SMB/SMB2 protocol (445/139 ports) taking long time to access due to IDS/IPS protection.
5. AVCE-1836 - Data saving on network location takes more time post installation of QH v18.
6. AVCE-1688 - Failed to send PDF attachment with Busy Accounting software due to Virus Protection
7. EPS-12072 - Unable to send mail from Thunderbird post applying the SQEPS 7.4 Service Pack 2.0.

Service Pack 1.0 Enhancements

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

Application of Service Pack 2.0

Service Pack 2.0 will be applied automatically when **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

Location	File Name	MD5 Checksum
C:\Program Files\Seqrite\Endpoint Security 7.60\Admin\Web\build	acsvpack.exe	4ea512cc6875890cb6c012bb6df270a9

Service Pack 2.0 Binaries

Location	File Name	File Version	MD5 Checksum
C:\Program Files\Seqrite\ Endpoint Security 7.60\Admin\Web\ build	capatch.ini	-	264e79bd898d1a4a629310f3cab31c0a
	capatch.exe	-	1d21880f5ee55c0b361dc4a9dd720dcc
	capch64.exe	-	e12de26e3707853604a5f01a9e7c250e
C:\Program Files\Seqrite\ Endpoint Security 7.60\Admin	acassrvc.exe	7.0.0.7	d32cd4f1e9a75144a26a7e1769c0ed73
C:\Program Files\Seqrite\ Endpoint Security 7.60\Admin\Config	acascore.dll	7.0.0.7	1ec959d6f5fe617f4bd06e0b7fb89c9d
C:\Program Files\Seqrite\ Endpoint Security 7.60\Admin\web\cgi	admnsett.cgi	7.0.0.7	3d4d3a72f87be644e0e2f600c84f63ae
C:\Program Files\Seqrite\ Endpoint Security 7.60\ Updmgr	umngrsvc.exe	7.0.0.7	32-bit: 1f3093cdecc53c33cd539f08a3328940 64-bit: 930a6374d7146ee61429f3736238195b
C:\Program Files\Seqrite\	accacore.dll	7.0.0.6	32-bit: 1e3a179302c1c6a230eb17d10c5b5142 64-bit: c0dcd51393be38c7b8cb3ce0ed571da1

Endpoint Security 7.60\Client Agent 7.60	accamisc.dll	7.0.0.6	32-bit: bf8c7811ff95e54e393b17c574d2b529 64-bit: 3a3d5f9ddca0d10b6b0481d56cdbb5a4
	accaresp.dll	7.0.0.6	32-bit: 3b38183f89ae81723f573c4aea328472 64-bit: 2df7ffa1e732c9e321e861171387d330
	accasrvc.exe	7.0.0.7	32-bit: 7c4fc155c43cc9466ff76777906fa278 64-bit: a41b075357ae7834de326851b81937f2
	aipinst.dll	7.0.0.7	32-bit: 3850552ba59f0b18ce7c8e6ca03ac24d 64-bit: ee2ce3dc8762c1a0a04a8dadcfffcd9e
	assetmgt.dll	7.0.0.7	32-bit: 8dec84eb1348619c0f9c860dcb2e2985 64-bit: 8ca837f29828ead6210d1fd3167ce079
C:\Program Files\Seqrite\ Endpoint Security 7.60\Seqrite	avcailib.dll	11.1.0.11	32-bit: 524fadc32cb6f7ae199fe3df430b9b7a 64-bit: 4def7f9279cca5c55251ac10082dc585
	bdssvc.exe	11.1.90.29	32-bit: f14445ad81ce23fe8356bb5b304793e5 64-bit: 29d6afc82f110bfc103e0720fbdb08a2
	catflt.inf	-	32-bit: 804e87fcd53de20e695f27cd5ac4017d 64-bit: 804e87fcd53de20e695f27cd5ac4017d
	catflt2k.sys	11.1.0.59	32-bit: 7b51196f10c49079e514e44908ae2b37 64-bit: db5ed92e29d97894c7306ee93c62da80
	catflt8.sys	11.1.0.59	32-bit: ec53015c0934fd65e35ff242a92d386e 64-bit: 33f4c2865af7ea78c9406ea17a728e7d
	catitf.dll	11.1.0.5	32-bit: 4b24692e19e4f2a173520513e2b7f296 64-bit: b087401b42c04ce11cbde6f7e6615beb
	clrptmod.dll	8.0.0.1	32-bit: cf26bd0c05df72a6b8c6916dd23e5468 64-bit: 4e3bcf03794787180dbc4f32a45660ca
	filehdlr.dll	8.3.0.3	32-bit: de018a85c2db216363a8632461fa4f60 64-bit: 9ff9b3076f110da8543f956071e9bf46
	opscore.dll	11.1.0.18	32-bit: 5e87909a3bee72109395bfb574bf3e6f 64-bit: d9ad05a6ccd343813919aef9c4447d59
	scanopt.dll	11.1.0.10	32-bit: 7eed2e47c809de538b259acc4ed2f6ec 64-bit: ffbf8f35506f8394e2ebd260793e9290
	vsitf.dll	11.1.0.2	32-bit: 27946c31b046e396e6ad4c0aa44f9f59 64-bit: 442a2bf2d9b8c6775be4a6d55a59e4c5
	vulscan.exe	11.1.0.3	32-bit: 984b45a51532188fb360da2286334a09 64-bit: afa26829a0e51cdaee4eb8903b5efe47
	wstif.sys	11.1.0.6	32-bit: 00332e35a65e69cccdecc9ab8ac1597a 64-bit: 45b3bea625d22ab15e0225ed329381a
	wsutil.dll	11.1.0.8	32-bit: 4cc0158594b50ec18c0225806b0f0bcd 64-bit: a1cd363611520524aed9d2742132e0cb

C:\Program Files\Seqrite\ Endpoint Security 7.6\Seqrite\CONFIG	DefaultVarconf.dat	-	32-bit: 84ca527547a9880ea1313ef81403bed9 64-bit: 84ca527547a9880ea1313ef81403bed9
	WSINTPT.DAT	-	32-bit: af11eae2f33e2a8d2975cfa51856dc0d 64-bit: af11eae2f33e2a8d2975cfa51856dc0d
C:\Program Files\Seqrite\ Endpoint Security 7.6\Seqrite\DCCAP	OverlayIcon.dll	7.6.1.2	32-bit: 08341bd2cb2a1375d8e16038b7f864f0 64-bit: 87b8b5377ad3af70fcab6c76ce86a9b5
C:\Windows\system 32\drivers	catflt2k.sys	11.1.0.59	32-bit: 7b51196f10c49079e514e44908ae2b37 64-bit: db5ed92e29d97894c7306ee93c62da80
	catflt8.sys	11.1.0.59	32-bit: ec53015c0934fd65e35ff242a92d386e 64-bit: 33f4c2865af7ea78c9406ea17a728e7d
	wstif.sys	11.1.0.6	32-bit: 00332e35a65e69cccdecc9ab8ac1597a 64-bit: 45b3bea625d22ab15e0225ed329381a

Service Pack 1.0 Binaries

Location	File Name	MD5 Checksum
C:\Program Files\Seqrite\Endpoint Security 7.60\Admin	acascore.dll	c1702ed74e64c5455bba91d79f3c7e04
C:\Program Files\Seqrite\Endpoint Security 7.60\Cagent	accacore.dll	32-bit: 1e3a179302c1c6a230eb17d10c5b5142 64-bit: c0dcd51393be38c7b8cb3ce0ed571da1
	accamisc.dll	32-bit: bf8c7811ff95e54e393b17c574d2b529 64-bit: a3d5f9ddca0d10b6b0481d56cdbb5a4
	accaresp.dll	32-bit: 3b38183f89ae81723f573c4aea328472 64-bit: 2df7ffa1e732c9e321e861171387d330
	accasrvc.exe	32-bit: 3dcccf5a1544c7d1d531376f5d754a36 64-bit: fb57d67b9879d4431c1fb107c2bdb1a9
C:\Program Files\Seqrite\Endpoint Security 7.6\Seqrite	avcailib.dll	32-bit: 524fadc32cb6f7ae199fe3df430b9b7a 64-bit: 4def7f9279cca5c55251ac10082dc585
	bdssvc.exe	32-bit: f14445ad81ce23fe8356bb5b304793e5 64-bit: 29d6afc82f110bfc103e0720fbdb08a2
	catflt2k.sys	32-bit: 7b51196f10c49079e514e44908ae2b37 64-bit: db5ed92e29d97894c7306ee93c62da80
	catflt8.sys	32-bit: ec53015c0934fd65e35ff242a92d386e 64-bit: 33f4c2865af7ea78c9406ea17a728e7d
	catflt.inf	804e87fcd53de20e695f27cd5ac4017d
	catitf.dll	32-bit: 4b24692e19e4f2a173520513e2b7f296

		64-bit: b087401b42c04ce11cbde6f7e6615beb
	clrptmod.dll	32-bit: cf26bd0c05df72a6b8c6916dd23e5468 64-bit: 4e3bcf03794787180dbc4f32a45660ca
	opscore.dll	32-bit: 5e87909a3bee72109395bfb574bf3e6f 64-bit: d9ad05a6ccd343813919aef9c4447d59
	scanopt.dll	32-bit: 7eed2e47c809de538b259acc4ed2f6ec 64-bit: ffbf8f35506f8394e2ebd260793e9290
C:\Program Files\Seqrite\Endpoint Security 7.6\Seqrite\CONFIG	WSINTPT.DAT	af11eae2f33e2a8d2975cfa51856dc0d
C:\Windows\system32\drivers	catflt2k.sys	32-bit: 7b51196f10c49079e514e44908ae2b37 64-bit: db5ed92e29d97894c7306ee93c62da80
	catflt8.sys	32-bit: ec53015c0934fd65e35ff242a92d386e 64-bit: 33f4c2865af7ea78c9406ea17a728e7d

Notes:

Service Pack 2.0:

- Global Service Pack 2.0 is cumulative of Global Service Pack 1.0
- On EPS Client Service pack will be applied only if VDB is 19-Dec-2019 [18:23:53] and Build Version is 18.00 (11.2.1.2).
- The following SP1 and SP2 binaries will be copied with. av extension.
  - opscore.dll
  - catitf.dll
  - OverlayIcon.dll
  - Catflt.sys
  - wstif.sys
- SP1.0 and SP2.0 binaries other than mentioned above will be copied as original and existing binaries will be renamed with. BKP extension. Reamed. BKP binaries will be deleted on system restart.
- Updated binaries will be applied post system restart.
- Post applying Service Pack 2.0, client system restart is mandatory in order to load the updated binaries.
- If Service Pack 2.0 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.txt' file from C:\Logs folder.

    If the Service pack is applied successfully, then 'genpch.txt' log file is removed from the location.

- If Service Pack 2.0 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.txt’ file from C:\Logs folder.
    - If the Service Pack 2.0 is applied successfully then ‘genpch.txt’ log file is removed from the location.