Seqrite Endpoint Security 7.60

Release Notes

5 January 2026

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to the user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

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	26 Aug 2019	Seqrite Endpoint Security 7.6 released
1.1.	13 July 2020	Seqrite Endpoint Security 7.6 updated build released
1.2	13 November 2020	Mac Client build released. Updated Build Information, Known Issues for Mac.
1.3	30 November 2020	Linux Client build released. Updated Build Information.
1.4	17 March 2021	Mac Client build released. Updated Build Information and Enhancements.
1.5	01 December 2021	Seqrite Endpoint Security 7.6 updated build released
1.6	03 February 2022	Mac Client build released. Updated Build Information, Enhancements and Known Issues for Mac.
1.7	16 March 2022	Mac Client build released. Updated Build Information and Known Issues for Mac.
1.8	23 March 2022	Windows Client build released. Updated Build Information and Bug Fixes.
1.9	20 October 2022	Linux Client build released. Updated Build Information, Enhancements, and Bug fixes.
1.10	30 November 2022	Mac Client build released. Updated Build Information, Enhancements and Known Issues for Mac.
1.11	8 October 2024	Mac Client build released. The build is signed with a new certificate.
1.12	5 January 2026	Seqrite Endpoint Security 7.60 updated build released

Abstract

Seqrite Endpoint Security 7.60 Release Notes contains the following information about the released build:

- Build Information
- New Features and Enhancements
- Bug Fixes
- Known Issues
- Usage Information

Build Information

Build 7.60 released on 5 January 2026

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Seqrite Endpoint Security	5 January 2026	3bd31f8f42b6fc4b87b22103bc62bfd4	7.60.7	
Windows Client - 32 Bit		a2d5fea58828d61fc98b800ee6b39f32	18.00 (11.2.1.6)	08 March 2022
Windows Client - 64 Bit		267fe9d96f956394406d065b34c57e3b		

Build 7.6 released on 8 October 2024

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	8 October 2024	1f17a572cb4aeee8c1758abd49881522	18.00	24 November 2022

Build 7.6 released on 30 November 2022

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	30 November 2022	34b698889f990e3e5f13efd0bcf5b5f5	18.00	24 November 2022

Build 7.6 released on 20 October 2022

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Linux Client - 32 Bit	20 October 2022	6e579bf7e7ab77d909a61c56520c7930	18.00 (2.2.7.58)	20 September 2022
Linux Client - 64 Bit		1e45a4446e3a0c2d9d3b05ee8f925385		

Build 7.6 released on 23 March 2022

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Windows Client - 32 Bit	23 March 2022	66C2C6B402F2D93656AE8F5AA5BAB1F2	18.00 (11.2.1.5)	8 March 2022
Windows Client - 64 Bit		F35C748582684A9725E979E6582AD8DD		

Build 7.6 released on 16 March 2022

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	16 March 2022	c3ba58ceda5c49fea8ab0a9da271afb4	18.00	10 March 2022

Build 7.6 released on 03 February 2022

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	03 February 2022	8ca49000d76fecc777d3670b6cad82ca	18.00	31 January 2022

Build 7.6 released on 01 December 2021

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Seqrite Endpoint Security	01 December 2021	5bce1f6d48b574455f5633bab9e11ea9	7.60.6	29 November 2021
Windows Client - 32 Bit		d28b63aed1c3a2ed36029f18d5e8665a	18.00 (11.2.1.4)	
Windows Client - 64 Bit		3cf0600ddaff7c72b7f21a09cc27c46d		
Linux Client - 32 Bit		87f140a08e17924bc8773d1d5cb1d5fa	2.2.7.54	
Linux Client - 64 Bit		f2004c9a305235b2a640afb678831e3e		
Mac Client		bea6c6aac02dc2592b473adf2043facc	18.00	
Patch Management Server - 32 Bit		0b1a238d09f1788f7032814276697ba6	3.1	-
Patch Management Server - 64 Bit		7432d5dac75424ba771c032e26189da9		

Build 7.6 released on 17 March 2021

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	17 March 2021	e0c7239e8e9400fbd00773adf951b9f2	18.00	9 March 2021

Build 7.6 released on 30 November 2020

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Linux Client- 32-bit	30 November 2020	4da4cc3506ed2e13055d329bb79e845e	2.2.7.48	26 November 2020

Build 7.6 released on 13 November 2020

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Mac Client	13 November 2020	728ef884373b15b32660d504922b304c	18.00	11 November 2020

Build 7.6 released on 13 July 2020

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Seqrite Endpoint Security	13 July 2020	a4d596bc5fbf1d6f34f1725ffce3d378	7.60.5	18 June 2020
Windows Client - 32 Bit		3cab7b25991ec52b876911037c5c9297	18.00 (11.2.1.3)	
Windows Client - 64 Bit		d59a8d2bc0a427d161711aabc7ac90b5		
Linux Client - 32 Bit		a259b6cc7a8d5861061b88f7c55bf781	18.00 (2.2.7.42)	
Linux Client - 64 Bit		746aab5c34f69ae69d89cc2919c23dbe		
Mac Client		686bf3c8116304c0f97d58b822c8baf2	18.00	

Build 7.6 released on 26 Aug 2019

Product Name	Release Date	MD5 Checksum	Build Version	Build VDB
Seqrite Endpoint Security	26 Aug 2019	faf434b77dc66216e69e504a12ece639	7.60.3	
Windows Client–32 Bit		a97eccead18e7d1f2e4ad6b92b874c7c	18.00 (11.2.1.2)	20 August, 2019
Windows Client–64 Bit		aeec4553a841f4f6c11e42d72acdf36a		
Linux Client - 32 Bit		42ab463cfd9a2aa8b711b76ecc5c7705	2.2.7.35	
Linux Client - 64 Bit		3c1ca9224de0e6c992e5d5022b36add0		
Mac Client		1890c794d85e106c910e5979724e1898	18.00	
Patch Management Server - 32 Bit		34be697c0d449610b28aa919e2cf0653	3.1	-
Patch Management Server - 64 Bit		691cc6932c812c7aa73a84540176b69f		-
Standalone Update Manager - 32 Bit		c0e243d75b9d50b5ec3b5424c06bb0c1	7.65	20 August, 2019
Standalone Update Manager - 64 Bit		c9c9d16fcdc832d0963b42f7a9d290b4		

New Features and Enhancements

Build 7.60 released on 5 January 2026

EPS Server:

- Registration is now secured with added Email and OTP validation. The activation will require OTP validation over email/phone number.
    - **Email Validation**:

      The already existing email IDs will get an error message. It shows the error message; **Company/Administrator Email ID already exists. Please update**. To proceed with the activation, the customer needs to provide a valid email address.
    - **OTP Validation**:

      OTPs will be sent to the provided Email ID and Mobile Number (10-digit only) provided in the activation wizard. The OTP will be valid for only 3 minutes. After email validation and OTP validation, finish the registration. *A customer has a total of 3 attempts to enter the OTP. If the customer enters an invalid OTP 3 times, the activation will be blocked for the next 30 minutes. It shows the error message, '**You have made too many attempts. Please try after 30 minutes**.'* For countries other than India, the SMS OTP will not be sent to the user. OTP will be sent only to the Email ID.
- From EPS 7.60.7 onwards, based on the licensed edition, only limited OS platform support would be available. For example, for SOHO Total, if you have only a Windows license, Mac and Linux will not be available.
- The EPS Server build version displayed on the EPS Web Console > Dashboard has been updated to 7.60.7.

Windows client AV builds:

- The build is prepared for the following bug fix:
    - EPS-29342 System enters Recovery Mode with INACCESSIBLE BOOT DEVICE after migration from 7.4 to 7.60
- The product version displayed on Scanner > Help > About is updated to 18.00 (11.2.1.6)

Mac Client Build released on 8 October 2024

- Build is signed with a new certificate.

Mac Client Build released on 30 November 2022

- Spam Protection feature is now supported on Apple's M1 chip.
- Mac client compatibility with macOS Ventura 13.
- macOS upgrade issue fix when Self-protection is ON.
- Latest engine files are included in this build.

Linux Client Build released on 20 October 2022

- The build is prepared for the following bug fixes.
    - Fixed Local Privilege Escalation Vulnerability in EPS - Linux Client.
- Latest engine files are included in this build.

Windows Client Build released on 23 March 2022

- The build is prepared for the following bug fix.
    - EPS-27581: Unable to install the EPS client on Windows XP, And Getting ERROR: Seqrite Installation Data file is corrupt - 7.60
- Latest engine files are included in this build.

Mac Client Build released on 16 March 2022

- Mac client provides support to Apple's M1 chip.
- Copyright year updated to 2008-2022, integrated in this build.
- Latest engine files are included in this build.
- Latest Remote Support tool (v 15.27.3) compatible with Apple's M1 chip is included.

  Intel system will continue to use the Remote Support tool (v 14.2).
- **IMPORTANT**:
    - AV updates released on 8 March 2022 for M1-specific 0000000c_updtconf.dat and definition files should be applied on the Seqrite EPS 7.6 Server before installing this Mac build on the Mac system.

      If the latest AV updates are not applied, the Mac client will not take updates from the Endpoint Security Server, and the following error message appears: 'Definition files not found'.
    - Mac clients cannot download and apply AV updates if the EPS 7.60 Server is installed in the multiserver mode, as AV will not be present.

      To download the AV updates, use one of the following methods till the EPS Server is in the multiserver mode:
        - Create a new EPS Group Policy for the Mac clients to download updates from the internet.
        - Install the Alternate Update Manager (AUM) and create a new EPS Group Policy for the Mac clients to download updates from the AUM.

Mac Client Build released on 03 February 2022

- Mac client compatibility with macOS Monterey 12.
- Latest engine files are included in this build.

Build 7.6 released on 01 December 2021

- 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 the 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 the enumeration of a large number of objects (10,000) in Active Directory while synchronizing Active Directory.
- The Patch Management reports section now contains additional reports for Up-to-date, Patch Scan failed, and Patch Installation failed endpoints. Earlier, only the Missing and Installed patches reports options were available.
- The default applications listed in the 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 the Windows 10 operating system through Seqrite Patch Management.
    - Configure the Seqrite Patch Server to get upgrade patches for the 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 the EPS web console dashboard if the EPS server does not have a Secondary EPS server.
- On the EPS dashboard top 10 incident count will be displayed instead of the top 5. The top 10 incidents can be exported to csv report.
- Notifications are displayed on the browser if any website is blocked by the Web Security feature. Earlier, only alert messages used to appear.

This feature is applicable only for clients installed on the Windows platform.

- EPS server compatibility with Windows 10 21H2, Windows 11, and Windows Server 2022 (Now IIS will be installed automatically, Correct OS name will appear in info.qhc).

  Note:

  - If the Master EPS Server is installed on Windows Server 2022 and Windows 11, then, Secondary Server and the Patch Management server installed on Windows 7, Windows Server 2008, and lower operating systems fail to communicate with the Master EPS server.

    - Secondary Server console is not able to connect from Master Server EPS web console > Manage Secondary Servers > Status of Secondary Servers > Go to Server.
    - The Patch Management server is not able to add from the EPS web Console > Admin Settings > Server > Patch Management > Add New Patch Server. It shows an error message: 'Patch server is unreachable. Please try later.

    To resolve the above issues, follow the workaround steps below.

    Seqrite does NOT recommend this workaround.

    1. Add the following registry entries on Windows 7, Windows Server 2008, and lower operating systems to enable TLS version 1.2.

       [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

       "Enabled"=dword:ffffffff
       "DisabledByDefault"=dword:00000000

       [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

       "Enabled"=dword:ffffffff

       "DisabledByDefault"=dword:00000000

    2. Restart the system.

    Seqrite recommends installing the Secondary Server and the Patch Management server on a higher version of the OS.

- Latest engine files are included in this build.
- The following new antivirus solutions detection is added (in OAV.DAT) when Seqrite Endpoint Security is installed.
  - ESET Endpoint Security 8.1.2031.0
  - ESET Endpoint Antivirus 8.1.2031.0
  - Kaspersky Endpoint Security for Windows 11.5.0.590

- Kaspersky Endpoint Security for Windows 11.6.0.394
- Kaspersky Security Center 13.1.909
- Kaspersky Small Office Security 21.3.10.391
- K7 Business Security 4.4.0.53

Mac Client Build released on 17 March 2021

- The following known issues in the 'Mac Client Build released on 13 November 2020' are fixed.
  - Data Loss Prevention

    Data transfer through the clipboard and Application/Online Services will not be monitored and blocked on macOS Big Sur.
  - File Activity Monitor reports may not be generated in certain cases for clients installed on macOS 10.15 and above.
  - If the client is deployed remotely when no user is logged in to the system on macOS 10.15 or above, the 'webflt' prompt appears after system restart.
  - Logs
    - Earlier logs used to be generated in the Seqrite installation logs directory, Seqrite > Seqrite > logs folder, which was taking large space, making the system slower.

      Now the logs are not generated.
    - Earlier dev_control_sdk logs used to be generated in the private/var/log folder, which was taking large space, making the system slower.

      Now the logs are not generated.
- To enable Virus Protection, you need to allow 'opsext' system extension in System Preferences > Security & Privacy > Full Disk Access.

  An earlier system restart was required after allowing 'opsext' from Full Disk Access.

  Now system restart is not required to activate Virus Protection.
- Latest engine files are included in this build.

Linux Client Build released on 30 November 2020

- TLS support binaries: accaadv.ini (connectionmodetls), cspsock.so, bfafv.dat
  1. Now, with the updated binaries, the client-server socket communication will be established over TLS. Earlier client-server socket communication used to be established over SSL.
- Latest engine files are included in this build.

Mac Client Build released on 13 November 2020

- Mac client compatibility with macOS Big Sur 11.0
- Latest engine files are included in this build.

Build 7.6 released on 13 July 2020

- Windows, Mac, and Linux client AV builds are integrated with the latest engine.
- Service Pack 3 bug fixes/enhancements are included.
- Roaming Platform (RP) optimization for service pack (SP): Earlier client service pack files were uploaded to the RP server from every EPS server. This used to consume a lot of disk space.

  Now, these client service pack files are maintained on a centralized location, for Example: http://download.quickheal.com/. The EPS server will send the centralized location of the service pack to the roaming clients to apply SP.
- EPS server compatibility with Windows 10 20H1 - 32 bit/64 bit.
- Mac client compatibility with macOS 10.15.4.
- Linux client compatibility with CentOS versions 7.4, 8.0, and 8.1.
- Samba version support for 4.10 and 4.11.
- The following new antivirus solutions detection is added (in OAV.DAT) when Seqrite Endpoint Security is installed.
  - Kaspersky Endpoint Security for Windows 11.3.0.773
  - Kaspersky Small Office Security 21.0.44.1537
  - eScan Endpoint Security for Windows 14.0.1400.2281
  - eScan Corporate for Windows Client 14.0.1400.2281
  - Avast Business Antivirus Pro 20.3.2588
  - Avast Endpoint Protection Client 8.0.1603
  - Bitdefender Endpoint Security Tools 6.6.18.265
  - K7 Enterprise Security 4.2.3.0
  - K7 Business Security 4.1.0.201
  - McAfee Endpoint Security 10.7.0
  - ESET Endpoint Security 7.3.2032.0
  - Trend Micro Worry-Free Business Security 6.7.1319
  - Trend Micro Apex One Security Agent 14.0.7867
  - Symantec Endpoint Protection 14.3.558.0000

- G Data Antivirus Business 14.3
- AVG Antivirus Business 20.4.3125
- Sophos Endpoint Agent 2.7.8
- Sophos Endpoint Security and Control 10.8.7
- Sophos Intercept X Endpoint 2.0.16

Build 7.6 released on 26 Aug 2019

- Master and multi-level secondary server architecture - As per your geographical locations, multiple and multi-level secondary servers are possible as per your requirement.
- EPS server compatibility with Windows 10 RS5 – 32-bit/64-bit.
- EPS server supports MySQL 5.6.42 version.
- Asset Management feature displays the following additional info,
  - OS Product key
  - Software upgrade changes in Reports and Dashboard
- Provision to exclude MD5 from Scan Settings. To do this, go to Settings > Scan Settings > Exclusion. In the Scan Settings > Advanced> Archive Scan Level, Archive Scan Levels support up to 16 levels.
- Provision to block/deny all URLs in the Web security feature with a single button.
- The License Manager page shows additional details of license usage regarding Master/Secondary server and DLP licenses as applicable.
- Hierarchy representation of Server name on EPS Dashboard

  On the Master server, the “Hierarchy” name will be represented as “Master”.

  On the Secondary Server, it displays the hierarchy of the Server you have logged on to. This shows the names of the parent servers up to Master. Example: Master / Primary001 / Secondary001. In this case, the logged-on Server name is Secondary001 and the parent Server is Primary001, which is reporting to the Master.
- Displays online/offline status of Secondary Server on the Dashboard > Manage Secondary Server. The Green dot indicates online status. The Red dot indicates offline status. If the last connected time of the Secondary server with the Master/parent server exceeds 2 hours, the status will be shown as offline.
- Centralized Policy Deployment

  On the Master server, the administrator will assign a policy for the Secondary Server. This policy is applied to the Secondary Server, its endpoints to the leaf Secondary Server. On the Secondary Server, this policy is not allowed to be modified.

- Provision to add Multiple IP addresses and DNS names (URL) in the exception of the Seqrite Firewall.
- GDPR - General Data Protection Regulation check box added on Software License Agreement.
- Displays VDB date along with Update time [hh:mm: ss] on Windows, Mac, and Linux Client Scanner and on EPS Web Console.
- Provision to lock the license with respect to the country. The EPS License should be functional only in the specified countries.
- Provision to select all Patches at once for specific endpoints.
- Provision to store data backup in a customized way. You can add custom extensions to the custom list. Provision for customized backup reports.
- Authorized USB can be accessed in different EPS networks if the administrator exports the policy with authorized USB settings and imports it into different EPS networks.
- On a 64-bit Linux operating system - Linux Client AV GUI is now supported.
- When the Master admin logs on Secondary server via auto login, then the Master admin activity logs will be generated in the Secondary server event logs. Included the latest 'Remote Support Tool - TeamViewer version (14.1.18533 QSC)' in Windows client AV builds.
- As a part of branding, added the logo for GoDeep.AI on the EPS console footer.
- The following new antivirus solutions detection is added (in OAV.DAT) when Seqrite Endpoint Security is installed.
  - Kaspersky Endpoint Security for Windows 11.1.0.15919
  - Symantec Endpoint Protection 14.2.1023.0100
  - McAfee Endpoint Security 10.6
  - eScan Endpoint Security for Windows 14.0.1400.2103
  - Trend Micro Business Security 20.0
  - Avast Business Antivirus 19.3.2554
  - Bitdefender Endpoint Security Tools 6.6.10.146

Bug Fixes

Build 7.60 released on 5 January 2026

The following bug is fixed:

Bug ID	Bug Summary
EPS-29342	System enters Recovery Mode with INACCESSIBLE BOOT DEVICE after migration from 7.4 to 7.60

Build 7.6 released on 20 October 2022

The following bugs are fixed:

Bug ID	Bug Summary
EPS-27437	[Aavas Financiers -13120 – Jaipur] EPS Linux Client AV shows the license has expired for AV, even though it's been renewed and is showing extended validity in the EPS server.
EPS-27522	[Midland Microfin Limited -13301-Jalandhar] A Few asset information on Ubuntu is not getting fetched properly in Asset Management Reports.
EPS-27617	[Zebpay- Ahmedabad] Blocked categorized websites from getting accessed on the Linux system.
EPS-26665	[Grameenkoota Financial Services Pvt Ltd - 12857 - Bangalore] Schedule scan is not happening as per their schedules on the Linux endpoint due to huge records of device blocking.
EPS-28173	[Amantya Technologies - 1621904 - Gurgaon] - Unable to get a response from license modules in the Django application on Linux.

Build 7.6 released on 23 March 2022

The following bug is fixed:

Bug ID	Bug Summary
EPS-27581	Unable to install the EPS client on Windows XP, And Getting ERROR: Seqrite Installation Data file is corrupt - 7.60

Build 7.6 released on 01 December 2021

The following bugs are fixed:

Bug ID	Bug Summary
EPS-27014	Secondary console status goes into a disconnected state and does not show green unless restarting the Agent server service.
EPS-26181	Seqrite EPS client icon loading issue in the taskbar notification area post upgrade.
EPS-26400	Policy status is showing as Pending for Roaming clients even if it's applied at the client side.
EPS-17648	Patch Management Reports are not getting generated in PDF format from Mozilla Firefox and Chrome.
EPS-23215	Seqrite renewal pop-up shows on Windows 10 even if the license is already renewed.
EPS-16269	Getting "Aw Snap error " while launching Chrome browser in Secure browser and safe Banking
EPS-17083	The EPS console is showing “Secondary servers are unregistered” under Event logs, even if the secondary server is not configured.
EPS-23300	Getting HTTP Error 404.15 while editing the custom applications list under Application Control settings
EPS-18310	Unable to block data transfer from AnyDesk through DLP
EPS-18688	The Report Viewer user account can view/modify DLP and manage device settings.

EPS-19306	Temporary device access time shows for OTP expiry timing and vice versa in an email text (Notify by Mail)
EPS-19716	DLP license count is showing zero if EPS is installed in multi-server mode
EPS-25424	The secondary server shows policy status as Pending even if it's not applied.
EPS-16618	Definition files corrupt ID-3 issue while applying the updates on the client AV.
EPS-18518	Unable to manage Non-MS product if the upstream patch server is WSUS
EPS-19314	Unable to install Patches on Endpoints due to the Endpoint Selection being grayed out
EPS-23164	Patch sync is failing, and the system is getting frozen while patch synchronization from WSUS on the 2016 Server.
EPS-17365	Local IPs & ports are getting blocked in the Seqrite firewall after adding the exceptions for blocking incoming traffic (Public IPs) for Maze ransomware.

EPS-18211	The NAS drive is getting displayed under the Unprotected Clients list.
EPS-24842	The application control custom category is not getting fetched properly in the EPS console web page.
EPS-16755	The client agent service gets terminated due to garbage memory access.
EPS-16741	Schedule Scan is not getting performed on the endpoint due to ClScanSet.dat file corruption.
EPS-20178	Installed Clients are reflecting under Unprotected Clients
EPS-16962	Policy with given name already exists error while creating a new policy.
EPS-17290	Vulnerability Scan Reports are not reflecting on the Console.
EPS-13922	Incorrect endpoint count for Top Vulnerabilities displayed on the EPS web console dashboard > Security > Vulnerabilities in specific cases.
EPS-14016	Incorrect endpoint count for Top incidents displayed on EPS web console dashboard > Top Incidents in some cases
EPS-13575	Endpoints protected with EPS clients are listed under the unprotected endpoint list on the EPS web console dashboard if the endpoints with the same NetBIOS names but different DNS domain names are present in the network.

EPS-13859	Unable to enumerate to get the updated list of unprotected endpoints on the EPS Dashboard
EPS-14353	Virus Incident data of the leaf EPS server is not displayed on the Secondary EPS Server's Consolidated dashboard.
EPS-15818	Patch Scan results for Missing patches are not reflected on EPS Console > Reports > Patch Management > Patch Status in a specific scenario.
EPS-14275	The status of the Roaming client shows offline on the EPS dashboard, even though Roaming Clients are connected to the Internet.
EPS-15821	Roaming Clients are not getting installed/activated even though the EPS Server has the required remaining license to accommodate new Client installation/activation.
EPS-16572	Error "Policy with given name already exists" while creating a new policy due to insufficient privileges for the environment variable path
EPS-13960	Tune-up reports are not deleted as per the set schedule from EPS Console > Reports > Manage > Delete Reports.

EPS-12928	'SYSTEM' user name is displayed instead of the actual user name in DLP reports for some violations.
EPS-11814	Unable to add the Google Drive application for exclusion from DLP in some cases
EPS-13569	Error 'Unable to load data' while accessing the Clients Status tab from EPS Console
EPS-13961	Virus Protection status on the EPS Dashboard shows off when Clients are offline.
EPS-13964	'Remove Client' button is not displayed on the EPS web console > Clients > Client Status page due to the space in the EPS Server installation long path.
EPS-14349	Sorting of offline clients in ascending/descending order from the EPS web console dashboard does not work due to a mismatch in the sequence of columns.
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 is getting revoked.

EPS-16715	The EPS edition and some features are not displayed in the EPS web console if a higher version of the EPS Server is installed in multi-server mode on the Secondary EPS Server EPS edition is displayed as SME on the EPS web console dashboard.
EPS-15692	The agent server service goes into a not responding state and does not respond to client requests.
EPS-18598	Incorrect reports are displayed for DLP if multiple endpoints have the same user name.
EPS-15352	Delay in the operation of the Tally application if IDS/IPS Protection is enabled on the Tally Server
EPS-13914	Unable to Approve Sales Order/ Purchase Order in MS Dynamics ERP using Digital Signature if 'Report Source of Infection' is enabled on EPS Console under Scan Settings>Virus Protection settings
EPS-14414	Sender's display name in the Outlook Mail client shows as Junk characters due to Email Protection Add-ins.
AVCE-1752	Status of Browsing Protection shows Off, and Scanner dashboard displays 'System at risk' message.
AVCE-1801	Scanner dashboard shows status as 'Automatic Update is turned off.'

EPS-27053 (Mac)	com.quickheal.sysextcontainer.ggc memory utilization increases gradually over the period.

Build 7.6 released on 17 March 2021

The following bug is fixed:

Bug ID	Bug Summary
AVCE-3966	[Lodestone Software Services Pvt. Ltd. 11855] Virus protection disabled in MAC on Big Sur

Build 7.6 released on 13 July 2020

All the bugs fixed in Service Pack 3.0 are integrated in this build.

The following bugs are also fixed:

Bug ID	Bug Summary
EPS-16715	[1Point1-10577-Mumbai] Product Flavor and Features got removed after multi-server installation of Secondary Console| EPS 7.6
EPS-16727	Mumbai | Mantralaya | EPS 7.6 | Seqrite Endpoint Security Build gets downloaded twice
EPS-14275	[CopMed - 9347 - Mumbai] Roaming client showing offline on the EPS console
EPS-14353	[Escalation-DIT Navy-Delhi-9484] Virus Incident data for Leaf server not able to fetch under Secondary Consolidated dashboard - 7.6 Navy
EPS-17083	(Chripal Group - Ahmedabad- 10870] EPS console showing “Secondary servers are unregistered. “ under Event logs reports of the server, while the secondary server is not configured
EPS-15821	[AyeFinance - 9757 - Delhi] Seqrite license exceeded due to roaming clients' entries in the rpclient table, which are not yet confirmed to move to the client_master table

EPS-16561	[1 Point 1 - 10450 - Mumbai] Redirection setting is getting revoked for selected clients | EPS 7.4
EPS-16289	[Philip Edlund - 10338 - USA] Explorer.exe is crashing due to partial uninstallation of AV
EPS-13979	[Agam Mehta - 9233 - Surat] ARWSRVC.EXE taking 99% CPU utilization, causing system hard hang | EPS 7.4
EPS-15936	[Brainware - 9875 - Kolkata]Google Drive getting blocked on Linux client due to browsing protection - EPS 7.60

EPS-15352	[Bombay Hospital - 9822 - Indore] Tally working slowly in network due to IDS/IPS even after SP1 applied [wsfilter.sys included in build]
EPS-16270	[Summit Technodyne - 10312 - Mumbai] Unable to activate the EPS 7.6 console with error ID 119 on Windows Server 2019
EPS-17636	[GESCO - 11017 - Mumbai] | Agent Server gets stopped randomly | EPS 7.4

Build 7.6 released on 26 Aug 2019

The following bugs are fixed:

Bug ID	Bug Summary
EPS-11636	[RNSB - 8281 - Rajkot] Reports viewer user able to log in Secondary Server from Consolidate Dashboard - EPS 7.4
EPS-11454	POC - Gandhi Automation-Incorrect File Activity Monitor Reports-EPS-7.4
EPS-10150	[Atul LTD-Surat-6367] Incorrect information showing on console for Linux clients- 7.4.1
EPS-11476	[Steven - Pulaski] AD Synchronization is failing due to an authentication problem with the AD server
EPS-11442	[Steven: United States]: Client deployment failed through Active Directory 7.4.2
EPS-11356	[Gandhi Automation]- Mail remains in the outbox while sending to the recipient
EPS-10152	[MHEAI Ltd-Chennai-6507] Chinese / Korean fonts in Mail Subject receiving as Junk characters due Email Add-ins - 7.4.1

EPS-11422	[Aavas: Jaipur: 8027] Incorrect update status count is showing on SEPS console dashboard 7.4.1
	Fixed the issue post receiving Windows updates on 9th April 2019.
EPS-12929	[Cera: Ahmedabad :] Outlook takes a long time to load due to Seqrite plugins:7.4.1
EPS-11528	[Gulf Oil- Mumbai-8311] Random Mails are getting stuck in Outbox due to Email Protection-7.4.1

EPS-13000	[Zeb - 8773 - Ahmedabad] Linux clients update issue "Error retrieving updates" - Rollback/backup Failed]
EPS-11845	[Escalation-Unicode-Lucknow-8490] Browsing is failing post installation of Seqrite Linux client- 7.4.1
EPS-11427	[Suyati Tech- Cochin-7537] Firewall LDAP Authentication getting failed post installation of Seqrite Linux client- 7.4.1
EPS-9455	[Cybage-Pune] Linux clients showing Offline due to random crashing of 'qhavclgnt' - 7.3
EPS-8398	[Webguru - Kolkata - 5641] Randomly unable to browse websites if Qhwebsec is in running state - EPS 7.3 Linux
EPS-11425	[Aavas : Jaipur : 8064] : Incorrect Product Version Showing 18.00 instead of 17.00 7.4.1 caused by multiple parallel update processing
EPS-10155	[AFour Technologies Pvt. Ltd.- 6921 - PUNE] website getting blocked if added in Web security exclusion of B/P and specific URL block - EPS 7.2
EPS-10713	[POC -WESEE Navy-7711] Linux System Shutdown getting stuck due post installation of Seqrite - 7.4.1
EPS-10190	Aavas Fin. Ltd.: Jaipur: Randomly unable to browse websites on Ubuntu 16.04 System, whereas qhwebsec service status is running - EPS 7.4

Known Issues

Mac Client Build released on 30 November 2022

Mac Client

Virus Protection status goes into the OFF state on macOS Monterey 12.6.1 and macOS Ventura. 13.0.1 Intermediately, when the machine is kept in the ideal state for 15 min or above. However, the Virus protection functionality works as expected. Virus protection status is turned ON automatically.

Mac Client Build released on 16 March 2022

Mac Client

- The following features are not supported on Apple's M1 chip.
  - Advance Device Control
  - Spam Protection
  - On macOS 11.5.x system, the following issues may occur.
    - Data Loss Prevention (DLP) extensions may get unloaded.
  - Apple Mail application may not be launched if Data Loss Prevention (DLP) is enabled and in the Confidential Data tab, the 'Personal' check box is selected.

  Upgrade to macOS 11.6 to resolve these issues.
- Email Protection will not work if the SSL/TLS setting is ON at the Mail application. This issue occurs in macOS M1 chip and macOS Monterey 12 and above. How to verify SSL/TLS settings

  SSL/TLS Settings are available at different locations for different Mail clients.

  Examples:

  - Apple Mail Application:
    a. Open Mail application.
    b. Select your Email account.
    c. In the Server Settings tab, clear the 'Automatically manage connection settings' check box and verify TLS/SSL settings.
  - Thunderbird:

a. Open Thunderbird application.

b. Select your Email account.

c. Go to Account settings > Select Server Settings. Verify SSL/TLS settings under Security Settings.

- Bluetooth blocking functionality does not work on macOS Monterey 12, though the Device Control Blocked prompt appears.

- If the Mac system is kept unlocked and in idle state for 2-3 days, the Client Dashboard does not launch. The policy status is also shown as Pending on the EPS Server Web Console, Client > Manage Policies page. Restart the system to resolve this issue.
- On the console utility of Mac System, 'com.quickheal.sysextcontainer.onlineext' process name appears in the Crash reports on macOS Monterey 12. But this issue does not affect product functionality as macOS reloads 'com.quickheal.sysextcontainer.onlineext' automatically.
- While scanning, if the scan is initiated on One OneDrive folder as per scan sequence, scanning does not progress/continue. The Client Dashboard also does not respond.
- Asset Management
    - On the Asset Management Reports page, in the Current Assets tab, in the 'Operating System' drop-down list, the 'macOS Monterey' name is displayed as blank space. If you select the blank space, the respective data appears with the Mac OS name.
    - On the EPS Dashboard, if you select Asset > Platforms > Mac, macOS Monterey details are displayed under the 'Big Sur' bar chart.

Mac Client Build released on 03 February 2022

Mac Client

- The Apple M1 chip is not supported.
- On the macOS 12.x system, the following issues may occur.
    1. Bluetooth blocking functionality does not work on macOS Monterey 12, though the Device Control Blocked prompt appears.
    2. Email Protection will not work if the SSL/TLS setting is ON in the Mail application.

       How to verify SSL/TLS settings

SSL/TLS Settings are available at different location for different Mail clients. Examples:

- Apple Mail Application:
  a. Open Mail application.
  b. Select your Email account.
  c. In the Server Settings tab, clear the 'Automatically manage connection settings' check box and verify TLS/SSL settings.
- Thunderbird:
  a. Open Thunderbird application.
  b. Select your Email account.
  c. Go to Account settings > Select Server Settings. Verify SSL/TLS settings under Security Settings.

3. On the console utility of Mac System, 'com.quickheal.sysextcontainer.onlineext' process name appears in the Crash reports on macOS Monterey 12. But this issue does not affect product functionality as macOS reloads 'com.quickheal.sysextcontainer.onlineext' automatically.
4. Asset Management
   - On the Asset Management Reports page, in the Current Assets tab, in the 'Operating System' drop down list, 'macOS Monterey' name is displayed as blank space. If you select the blank space, the respective data appears with Mac OS name.
   - On the EPS Dashboard, if you select Asset > Platforms > Mac, macOS Monterey details are displayed under the 'Big Sur' bar chart.

Build 7.6 released on 01 December 2021

Mac Client

- The macOS Monterey and Apple M1 chip is not supported.
- On the macOS 11.5.x system, the following issues may occur.
  - Data Loss Preventions (DLP) extensions may get unloaded.
  - Apple Mail application may not be launched if Data Loss Prevention (DLP) is enabled and in the Confidential Data tab, the 'Personal' check box is selected.

  Upgrade to macOS 11.6 to resolve these issues.

- While scanning, if the scan is initiated on One OneDrive folder as per scan sequence, scanning does not progress/continue. The Client Dashboard also does not respond.

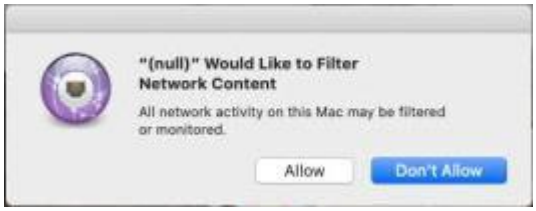
Mac Client Build released on 13 November 2020

Mac Client

- Data Loss Prevention

  Data transfer through the clipboard and Application/Online Services will not be monitored and blocked on macOS Big Sur.

- If the client is deployed remotely when no user is logged in to the system on macOS 10.15 or above, the following prompt appears after system restart. Click **Allow** to allow the 'webflt' system extension.



  If you click **Don't Allow**, you need to generate the above prompt manually by executing the following command:

  ```
  /Applications/webflt.app/Contents/MacOS/webflt -start
  ```

  After executing the command, the prompt appears. Click **Allow**.

- File Activity Monitor reports may not be generated in certain cases for clients installed on macOS 10.15 and above.

Build 7.6 released on 13 July 2020

1. Server

- EPS server installation on the AWS or Azure cloud machine

  During EPS server installation on the AWS or Azure cloud machine, the remote connection to the AWS/Azure system is disconnected. To reconnect, restart the instance of the cloud machine from the AWS/Azure web portal.

  This is applicable only for Windows 7 and earlier versions.

  Note: Restart the instance after a few minutes of disconnection to avoid interruption during EPS server or client installation.

- The following operating systems support only the Master Server without any secondary server
    - Microsoft Windows XP SP1 and SP2 / Professional Edition (all 64 Bit)
    - Microsoft Windows Server 2003 Web/ Standard / Enterprise (all 64-bit)
- While deploying Client using the Notify Install method, Windows Defender SmartScreen prompt may appear while executing the cainstlr.exe file. If so, click the 'Run Anyway' button on the Windows Defender SmartScreen prompt to continue the installation.

2. Windows Client

   a. Advanced Device Control

   - Customized access to devices is not supported on Windows XP Service Pack 1 and earlier versions, and Windows 2003 (Without SP) operating systems.
   - Devices encrypted with the Device Encryption feature will not be accessible on Windows XP Service Pack 1 and earlier versions, and Windows 2003 (Without SP) operating systems.
   - The user name is displayed as ‘System’ for blocked USB Storage Devices in Devices Control.
   - The blocking of mobile phone charging through the USB cable feature is not provided.

   b. Data Loss Prevention

   - Confidential and User Dictionary Data will not be blocked in the subject line, message body of messenger communication.
   - File transfer from system folder (for example, C:\Windows or C:\Program Files) will not be monitored.
   - On the Windows 10 operating system, the DLP functionality is not supported for the Microsoft Edge web browser and Mail Client.
   - On Windows XP and Windows Server 2003, DLP or DC may not work due to some operating system limitations w.r.t max limit of process callback.
   - 'Device Control' alerts are displayed after applying the DLP policy to the client for the first time, though 'Advanced Device Control' is disabled. The reports of device control are also generated.
   - When you select the ‘Block and Report’ option and incur a DLP violation in Outlook Express, the mail remains in the outbox queue. Due to this, the clean mails are not triggered.

     Workaround - Delete the blocked DLP-violated mail from the outbox manually to trigger other emails successfully.

In Outlook 2003, the DLP violates mail remains in the outbox queue, but the send, receive operations are performed successfully.

- When the mails are sent from the Outlook mail client, having an MAPI account configured to the other MAPI account, the mails are not blocked. In Reports, skipped action is displayed.

  But if the mails are sent from the Outlook mail client, having an MAPI account configured to the POP3/IMAP account, the mails are blocked.
- Optical Character Recognition (OCR) feature- Add-on feature of DLP
  - OCR does not support embedded image scanning.
  - There may be a performance hit while copying bulk images.
  - Only Roman (English) alphanumeric script is detected from the images.
  - Only clear and high-quality images are detected by OCR. The blurred, distorted, too small, or too large images may not be detected.

c. The user may get the Application Control block prompt while copying or renaming unauthorized applications.

d. While deploying the client using the Notify Install method, the Windows Defender SmartScreen prompt may appear. Click **Run Anyway** to continue the installation.

e. Advanced Device Control, Data Loss Prevention, File Activity Monitor, and Application Control features will not work if Virus Protection is turned off.

f. 'Pick from specified path' feature of Update Manager will not be able to pick the updates from shared networks.

g. FoxPro/DOS applications running in full-screen mode may get minimized when the EPS client is updating.

h. Firewall
   - Monitor Wi-Fi network feature is not supported on the following OS:
     - Windows XP 64-bit
     - Windows 2003 64-bit
     - Windows 2003 32-bit
   - On Windows XP 32 SP2 feature will work only if the hot fix (Redistributable for Wireless LAN API) is installed.
   - Proxy is not supported for a firewall exception rule.
   - IPv6 is not supported for firewall exception rules.

i. Device encryption

- Only the NTFS file system is supported for Partial encryption.
- While changing the encryption method device has to be cleaned using the 'diskpart' command.

j. USB By Model

Java Applet is not supported for the Chrome browser, so the USB by model feature will not work for the Chrome browser.

k. SMTP Settings

EPS cannot send emails if the SMTP settings are configured for a public mail server (Example, Gmail) if Allow less secure apps setting is disabled on the public mail servers.

l. Patch Management

- The limitation with IIS version 5.1 is EPS Server and PM Server cannot be installed on Windows XP.
- On Non-Activated OS/License expired Applications, Seqrite recommends not to install the patches using the Patch Management server.
- On XP and 2003 Server systems, the Patch Management server uses default IIS ports (HTTP 80 and HTTPS 443) and does not support custom ports.
- After the EPS License has expired, the user is unable to use the full functionality of the PM server. After reactivation, the PM server functionality will resume.
- Installation of Windows 10 Anniversary update on the Windows 10 client machine is not supported for Patch Management.
- Windows 8.1 optional updates are stored in the Control Panel and may not be installed on the system during the first reboot. Multiple reboots may be required to install Windows 8.1 optional updates.
- The Upgrades category of patches is removed from Windows Patch Synchronization filter settings.
- While installing PM Server, if UAC is enabled on the system, then it would prompt while binding the SSL certificate; the installer would not proceed till the prompt is acknowledged.
- PM hosted on Windows Server 2003 and XP 64 server will not download patches for Notepad++.
- For every new Non-MS patch download, EPS event viewer logs would display a message as EPS and PM patch sync is completed, patch scan can now be initiated, which will be for the very first time for downloading non-MS patch binaries.
- On 2003 Server and XP, after uninstalling PM Site remains in IIS; the user has to manually delete the site from IIS Manager and install the PM server again.

- Offline patch repository creation may fail if the user is downloading the patch binaries in GB.
- ‘System’ user-generated in the report whenever any process runs in ‘System’ context for any scan or on access actions.
- Patch Database importing does not support importing from the older version to Patch Management 3.0.
- Windows XP 64 and Windows Server 2003 do not support SSL communication between the client with the Patch Server.

m. On Windows Vista, the Screen Locker Protection feature will work if either service pack SP1 or SP2 is applied.

n. KB2685811 Windows update is a prerequisite on Windows Vista SP0 OS for the Screen Locker Protection feature.

o. The Wsnf driver is not logo signed on Windows 2003 and Windows 2008 operating systems.

p. For the 'Vulnerability Scanning' module, a 'System' user is generated for all types of scans.

q. The FoxPro application is unable to communicate with the server due to Email Protection settings. The bug fix for 44958 will be provided in the future release.

r. Emails may not be scanned for malicious attachments and SPAM if they are received over IMAP protocol using Thunderbird on a Windows 10 64-bit operating system.

s. The email client application may not work if it is configured to download Emails over the IMAP protocol and if Seqrite Email Protection is enabled.

t. Randomly mail sending failed using Thunderbird Email Client due to ‘nsmail.tmp’ file being scanned by Virus Protection.

3. Mac Client

a. Phishing Protection, Browser Protection, and Web Security may create multiple reports for a single instance if a restricted URL is run on the Opera browser.

b. Notification for Remote Scan, Remote Update, and Remote Uninstall from the Seqrite EPS web console cannot be sent if the Mac client user is not logged on to the Mac machine.

c. Advanced Device Control

- The attached CD\DVD will get both read and write permissions even though the read-only setting is applied in Seqrite EPS Device Control.
- If i-Devices, Webcam, CD-DVD, Internal Card Reader, Mobile Phones, and HFS Encrypted devices are already attached to the endpoint while Device Control settings are changed, then the attached devices may need to be re-attached for new device access rights to be applied.

- Exception functionality is not applicable for Bluetooth, Wi-Fi, Webcam, and External CD-DVD.
- Multiple notifications may be generated for CD-DVD.
- Mobile phones except i-devices that are connected in 'USB Mass Storage' mode will be detected under the 'USB Storage device' category.
- Mobile Phones connected in MTP mode will be detected under 'Windows Portable Category'.
- If you are installing the Mac client with USB devices attached to the system, such devices get unmounted for a few seconds after installation.
- If a USB device with an NTFS file system is attached during Mac client installation, two copies of the attached USB may be visible for a few seconds.
- If USB devices are mounted or unmounted by terminal commands, the Device Control policy will not apply to that device.
- If you are installing a Mac client on Mac OSX 10.9 with FAT USB devices attached to the system, such devices get unmounted until they are disconnected and reconnected, and also for some Android mobiles if the mobile is connected to the Mac system in "MTP" mode.
- USB storage device won't be formatted with Mac OS Extended (Journaled, Encrypted) file format.
- Allow USB devices based on their model nameDevice information will not be fetched automatically if the admin accesses the EPS console using a web browser on Mac OS.
- When a device with partial or full encryption is connected, "Mac OS X can't repair disk" or "Disk you inserted was not readable by this computer" prompts will be displayed.
- Complete USB Interface blocking:

  USB dongles are identified under the Wi-Fi category, so currently, dongles will not get blocked. Access Permissions for the device will get reflected after reconnecting the device if access permission is changed while the device is connected to the system. If the USB interface is blocked, USB devices added to the exception will not work.

d. Data Loss Prevention

- Confidential and User Dictionary Data is not blocked in the subject line, message body of email, or messenger communication.
- Prompts and reports will be generated if a monitored file type is being downloaded.

- Certain file types (POT, PPT, PPTX, DOC, DOCX, XLS, XLSX, RTF) containing Unicode data will not be blocked.

e. Asset Management
   - Domain/Workbook information is not displayed for the Mac client.
   - I-Phone/Android devices' storage information is not getting listed under H/W information.
   - EPS Console is not sending "Hardware change Email Notification" for Asset management.
   - Default Gateway information appears blank for all configured Network Adapters.
   - A few of the network adapter examples: VPN, Bluetooth PAN, Wi, etc. appear blank.

f. While installing the Mac client for the first time on Mac OS 10.13, the user should allow permission for loading the drivers manually when prompted.

g. In the **Support** section, **Remote Support** does not work on Mac OS X 10.9 and 10.10 due to limitations of the TeamViewer application.

4. Linux Client

   a. On some operating systems (OS), users need to disable SELinux or AppArmor to allow Seqrite features such as Online Protection, Samba Protection, Schedule Scan, and Device Control to work properly.

   b. If infected files are moved within the SAMBA share, the files will not be detected.

   c. If IncludePath= "/" is provided in Seqrite Online Protection, Daemon gets unloaded immediately after starting. The infected file is created/copied in the IncludePath of Seqrite Online Protection.

   d. SEPS scan notification, supports only the 'ext' file system in the Linux operating system.

   e. Advance Device Control:
      - Bluetooth USB dongle may not be supported on a few operating systems (OS).
      - MTP/PTP-based phones are not supported except for UMS support.
      - Device encryption is not supported.
      - USB Hub is not supported.
      - If any process is working on a device mount point, the process will not be cleared or deleted from the mounted directory when the storage device is ejected.
      - If the Read-only option is set for internal CD/DVD, USB storage device on the EPS server, it is treated as ‘Block’ on the Linux client.
      - Though the permission set for the USB device is 'blocked' and the USB device is plugged in, on system reboot, the USB device is accessible.

      External Drive and Devices:

- Scanning is not supported for External CD/DVD drives and mobile device phones.

f. Web Security:
   - Websites, if accessed by their IP addresses, may not be accessible in the following cases:
     - DNS is not configured when setting the domain-based policy.
     - Websites that change IP addresses periodically will not work for the changed IP addresses.
   - Web security will not work if the iptables/firewall service is turned off.
   - SSL versions earlier than 3.1 are not supported for the HTTPS protocol.

g. On some operating systems (OS), Seqrite shortcuts will be displayed in the Launcher menu after the next login.

h. The Online Protection feature may not work on some operating systems mentioned under the Supported Distributions list.

i. Samba protection is not supported for versions 4.6 to 4.9 and 4.12.

j. Samba Protection will not be supported when a Samba share is accessed from Macintosh to Linux and Linux to Linux.

k. Linux Mint 18, Fedora 25, Ubuntu 17.04 (32/64 bit): System hangs on the plugin of the USB External CD/DVD drive.

l. .File /Directory path longer than 1024 characters might be skipped from scanning.

m. Redirection:
   - Redirection is not applicable for the client installed on a Linux operating system.

n. On SUSE 11, the external drives are not scanned.

o. On SUSE 12, after Linux client installation, some Linux client services may be unused. After reboot, the client services will start.

p. Remote support tool is not supported on CentOS 8.0 and 8.1.

5. Roaming Service
   - Proxy is not supported for downloading builds of roaming clients.
   - In the Advanced Device Control section, for the Temporary Access feature, the Notify button will be disabled.
   - If the Complete USB Block setting has been configured in the policy, then the clients on which the policy is applied will not be able to use 3G/4G dongles. The dongle will be blocked because of the Complete USB Block setting.
   - Disk Part/Cleanup is a mandatory activity that needs to be done manually before any change in any of the partitioning rules.

6. While installing the EPS server on a Windows Server 2003 – 32 Bit operating system without any Service Pack applied, the Microsoft .NET Framework 4 installation window gets closed after extraction without showing any error message. This is because Microsoft .NET Framework 4 installation requires Service Pack 2 to be installed on Windows Server 2003 – 32 Bit operating system.

Usage Information

1. While configuring the Secondary Server with the Master server, enter the Master Server Port number as 443 in case of the Windows XP operating system.
2. Configuring ports on the Azure or AWS Cloud machine:
   You should configure the ports to establish communication between the EPS server and the clients. Allow the ports of the EPS server, Database, Patch Server, and Update Manager in the cloud machine where EPS will be deployed.
   Allow the following ports from the Azure or AWS machines:
   - EPS Console - 9111
   - CGI - 6805
   - Download - 8101
   - Communication - 5057
   - MySQL - 62228
   - Patch Server HTTPS - 6201
   - Patch Server HTTP - 3698
3. If the administrator initiates a tuneup notification to the endpoint and if the endpoint is not logged in, then the tuneup notification will fail.
4. While installing EPS using a domain name, the computer name must not be longer than 15 characters.
5. While installing the EPS Client, if a third-party antivirus is detected, then the EPS antivirus installation will uninstall the third-party antivirus. The EPS antivirus installation will not proceed further until the third-party antivirus is removed.
6. For Windows 2016 Server, uninstall Windows Defender before installing the Seqrite EPS client. If you are upgrading the EPS client to Windows 2016 Server, uninstall Windows Defender after the upgrade.
7. Active Directory (AD) synchronization:
   a. Windows Firewall should be turned off on the client computers while deploying the EPS client.
   b. It is not recommended to synchronize the entire domain controller while setting up AD Synchronization. Instead, you can synchronize only those groups that contain computers.
8. Advanced Device control:
   If an authorized and encrypted device is formatted, the device will be treated as an unauthorized device. In this case, the administrator will need to add the device again in Advanced Device Control and configure the policies accordingly.
9. To install clients on Mac and Linux endpoints, the client builds should be downloaded from the build server separately. Refer to the Administrator Guide for more details.
10. Due to high security settings of Internet Explorer (IE) on server operating systems, some EPS web console pages may not be displayed properly.
11. It is recommended to perform the following steps on the Windows Server operating system to view the EPS web console properly.
    a. Open IE.
    b. Go to Tools/Settings > Internet Options > Advanced.

c. Clear the following check boxes under Security Settings:
   - Do not save encrypted pages to disk.
   - Empty the Temporary Internet Files folder when the browser is closed.
d. Select the 'Play animations in web pages*' check box under Multimedia Settings.
e. Click Apply.

12. In Windows 8 and Windows 8.1, if the EPS web URL is not accessible in IE 10/11, perform the following steps:
    a. Open IE.
    b. Go to Tools/Settings > Internet Options > Advanced.
    c. Under Security Settings, clear the 'Enhanced Protection Mode' check box.
13. If you are unable to perform Auto-Login from the Manage Secondary Servers tab, perform the following steps. This issue is observed on Microsoft Internet Explorer 11 on Microsoft Windows 10 Creators Update and Microsoft Windows 10 Fall Creators Update (32-bit and 64-bit) if secondary servers are installed using a Domain name.
    a. Go to Internet Explorer > Internet Options.
    b. In the Security tab, clear the Enable Protect Mode check box.
    c. Click **Apply**.
    d. Click **Ok**.
    e. Restart Internet Explorer.
14. If you see the 'page not supported' error message while accessing the EPS console by host name from the Default IE browser, perform the following steps.
    a. Go to Internet Explorer > Settings > Compatibility View Settings.
    b. In the Compatibility View Settings dialog, clear the following two checkboxes,
       - **Display intranet sites in Compatibility View**
       - **Use Microsoft compatibility lists**
    c. Click **Close**.
15. On the Windows Small Business Server operating system, some pop-up windows of the EPS Web Console may not open due to Enhanced Security Configuration (ESC) in IE. To allow these pop-up windows, change the following settings:
    a. Open the Server Manager Tool.
    b. Click Configure IE ESC located on the right-hand side of the Server Manager Tool in the Security Information section.
    c. Turn off IE ESC.
    d. Click Apply.
16. Turn off the Secure Boot feature of the system to use Browser Sandbox. The Secure Boot feature can be disabled from BIOS Configuration.
17. Windows Defender should be uninstalled before EPS client installation on Windows Server 2016. For the OS upgrade, Defender should be uninstalled manually after the upgrade is complete.
18. Redirection:
    a. Clients cannot be redirected until its installation is completed.
    b. The Roaming Clients cannot be redirected to the EPS server, which is activated with the Business Key of EPS 6.4 or an older version (not having the Roaming feature). In this case, for the redirection process, the Roaming Clients need to be connected within the organization's network.

c. A higher version of the Mac client packager needs to be created on a higher version of the EPS server before Mac client redirection.

19. To create a Mac/Linux Seqrite Client packager, follow these steps:
    a. On the Seqrite Endpoint Security server, go to Start > Programs > Seqrite EPS Console > Client Packager.
    b. In the Client Agent Package list, select Custom. In the OS platform list, select Mac/Linux.
    c. Select Setup type as per the selected operating system.
    d. Download the client build from any of the mentioned links.
    e. Click **Browse** and select the downloaded folder.
    f. Click **Create** to create the client packager.
20. User needs to add the Agent Server 7.6 executable in the trusted Mail client list of installed AVs before enabling Email notification from EPS.
21. Roaming Client:
    a. Roaming service should be enabled, and automatic mode should be selected on the EPS server to deploy endpoints out of the organizational network.
    b. Roaming service should be enabled, and automatic mode should be selected on both EPS servers on which roaming clients are being redirected out of the organizational network.
22. Patch Management:
    a. Seqrite recommends installing the Patch Management server on a Windows server operating system if you have more than 25 endpoints in your network.
    b. Installation of the Patch Management server is not supported on a Windows XP 32-bit system.
    c. Installing and searching for updates is slow, and high CPU usage occurs in Windows 7 and Windows Server 2008 R2. Microsoft recommends installing KB 3102810 on these systems. This update can be obtained from the URL; https://support.microsoft.com/en-us/kb/3102810.
    d. Best practices:
        a. Install the Patch Management Server.
        b. Go to Admin Settings > Patch Management > Add Server to add the Patch Management Server to the EPS console
        c. Enter the name of the server.
        d. If the Patch server is deployed in the network of a local client, follow these steps:
            I. In the Server IP/Hostname text box, type the private IP address or hostname of the Patch Server.
            II. In Port, type the port number. Default Port HTTP is 3698, SSL:6201.
            III. Ensure that the Use SSL (Ensure Patch server supports SSL, if SSL is checked) check box is selected. This check box is selected by default.
            IV. In the EPS Details section, in the EPS IP/Hostname text box, provide the private or public IP/Hostname of the EPS server. Seqrite recommends providing the Private IP/Hostname.

        If the Patch server is deployed in the network of a remote client, follow these steps:
            I. In the Server IP/Hostname text box, type the public IP address or hostname of the Patch Server.
            II. In Port, type the port number. Default Port HTTP is 3698, SSL:6201.

III. Ensure that the Use SSL (Ensure Patch server supports SSL, if SSL is checked) check box is selected. This check box is selected by default.
IV. In the EPS Details section, in the EPS IP/Hostname text box, provide the public IP/Hostname of the EPS server.
V. Click Add.
VI. After successfully adding the Patch Server, to configure the Patch Server, select the server from the dropdown list > Patch Synchronization > Filters.
VII. Select the products, categories, and languages as per your requirement. This step is vital as this information will be used to scan missing patches in your network. Seqrite recommends selecting only those products/categories/languages installed in your network.
VIII. Click Start to initiate patch synchronization. For the first time, this process may take some time to complete the patch synchronization, depending on the products selected in the filter settings.
IX. After successful patch synchronization, configure the patch server in policy. To configure, go to the Settings tab and select the installed patch server. Once the patch server is configured, the user can initiate a patch scan for missing patches. To initiate a patch scan, go to Clients > Client Action > Patch Scan.
X. After the Scan results are displayed, the user can initiate patch install from Clients > Client Action > Patch Install Page.
XI. The User can monitor client-wise and patch-wise installation status in Reports > Patch Management.

23. Data Loss Prevention
    - File Classification feature

    While classifying a new file, the Seqrite File Classification dialog appears only for MS Office files.
    - Add-on feature - Optical Character Recognition (OCR)
        - OCR supports the following image formats,
            - JPEG (or JPG) - Joint Photographic Experts Group
            - PNG - Portable Network Graphics
            - GIF - Graphics Interchange Format
            - TIFF - Tagged Image File
            - BMP - Bitmap image files
    - OCR feature in DLP is available in Microsoft Windows Vista SP2, Windows 7 SP1 Personal computer versions and Windows Server 2008 SP2, Windows Server 2008 R2 SP1, and above of Server versions.

24. Mac Client

    AV updates released on 8 March 2022 for M1-specific 0000000c_updtconf.dat and definition files should be applied on the Seqrite EPS 7.6 Server before installing the Mac build released on 16 March 2022 on the Mac system.

    If the latest AV updates are not applied, the Mac client will not take updates from the Endpoint Security Server, and the following error message appears,

    'Definition files not found'.

