



## 릴리즈 노트

Cloud 4.0

2024년 4월

## 저작권 정보

---

저작권 © 2018-2024 Quick Heal Technologies Ltd. 모든 권리 보유.

이 출판물의 어떤 부분도 어떤 형태로든 복제, 복제 또는 수정될 수 없으며 정보 검색 시스템, 전자 또는 기타 매체에 통합되거나 사전 허가 없이 어떤 형태로든 전송될 수 없습니다. Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Quick Heal Technologies Ltd.가 승인한 사람을 제외한 모든 사람의 마케팅, 배포 또는 사용은 법적 기소의 책임이 있습니다.

### 상표

Seqrite 및 DNAScan 은 Quick Heal Technologies Ltd.의 등록 상표이고 Microsoft 및 Windows 는 Microsoft Corporation 의 등록 상표입니다. 기타 브랜드 및 제품명은 해당 소유자의 상표입니다.

### 라이선스 조건

Seqrite Endpoint Protection 의 설치 및 사용은 사용자가 Seqrite 최종 사용자 라이선스 이용약관을 무조건적으로 수락하는 것을 전제로 합니다.

라이선스 조건을 읽으려면 <http://www.seqrite.com/eula> 를 방문하여 제품에 대한 최종 사용자 라이선스 계약을 확인하십시오.

# 내용물

---

1. 기능 및 개선 사항.....	3
2. 시스템 요구 사항.....	6
3. 버그 수정.....	10
4. 이용정보.....	12

## 개정 내역

---

이 문서의 정보는 Quick Heal 연구 개발 및 지원 팀의 단독 사용을 위해 제공됩니다. 이 문서의 일부를 다른 사람에게 게시하거나 배포하는 것은 엄격히 금지되어 있습니다.

문서 버전	날짜	논평
1.0	2024 년 4 월 6 일	Secrite Endpoint Protection Cloud 4.0 출시된

## 기능 및 개선 사항

---

이번 릴리스에서는 다음과 같은 기능을 제공합니다. EPP Cloud 4.0 에 추가되었습니다.

- 새로운 브랜드 이름 및 로고
  - 브랜드 이름이 이제 Seqrite Endpoint Security 에서 Seqrite Endpoint Protection 으로 변경되었습니다.
  - 제품 로고는 현대적인 산업 중심 접근 방식에 맞춰 재설계되었습니다.
- 암호화 정책: Seqrite 암호화 정책을 사용하면 중요한 데이터를 암호화하고 Microsoft BitLocker 를 사용하여 무단 액세스로부터 데이터를 보호할 수 있습니다.  
이 기능을 사용하면 다음을 암호화하거나 해독할 수 있습니다.
  - Windows 운영 체제 볼륨.
  - 고정된 데이터 볼륨.
- 데이터 손실 방지
  - 사용자 지정 응용 프로그램 – 이 기능을 사용하면 DLP 에서 모니터링하거나 제외해야 하는 응용 프로그램을 추가할 수 있습니다.
- 사용자는 엔드포인트 상태 화면(상태 > 엔드포인트 이름 > 엔드포인트 상태 > 제품 버전)에서 CA 버전과 함께 Windows 클라이언트 AV 빌드 버전을 볼 수 있습니다. 예: 18.00 (13.0.0.1)  
또한 이 정보는 내보낸 csv 파일에도 포함됩니다.
- Windows Client AV 를 설치하는 동안 다음과 같은 새로운 타사 바이러스 백신 탐지 기능이 추가됩니다.
  - F-Secure Client Security Premium 15
  - Coro 2
  - TotalAV 5

- Cybereason ActiveProbe Antimalware 22 및 23
- Cybereason ActiveProbe 22 및 23
- Trellix Endpoint Security 10
- Trellix Agent 5
- VIPRE Endpoint Security Agent 13
- CylancePROTECT 3
- Sophos Endpoint Agent 2023
- Avast Business Security 23
- Mac 의 경우:
  - Mac OS ARM64 기반 시스템에서 고급 장치 제어에 대한 지원을 제공했습니다. 지원되는 장치는 다음과 같습니다:
    - 저장 장치:
      - USB 저장 장치
      - CD/DVD
    - 무선 및 유선:
      - Wi-Fi
      - Bluetooth
    - 기타:
      - 로컬 프린터
    - 장치 예외
    - 임시 장치 접속 허용
  - 시스템 무결성 보호 사용(SIP)가 Mac OS 에서 활성화되면 전체 시스템 검사 및 예약 검사는 SIP 로 보호되지 않는 폴더를 포함합니다. 반대로, Mac OS 에서 SIP 가 비활성화되면 스캔에는 모든 폴더가 포함됩니다.
  - 자산 관리를 위해 Mac 에 대한 로깅 지원 제공

- 이 기능을 사용하면 제품 설치 아래에서 자산 관리 로그를 활성화할 수 있습니다.
- Mac 클라이언트에서 자산 관리와 관련된 문제가 발생하는 경우 디버그 로그를 활성화할 수 있습니다.
- 이 기능은 Mac 클라이언트에만 적용됩니다.

*특징 및 기능에 대한 자세한 내용은 도움말/설명서를 참조하세요.*

# 시스템 요구 사항

---

## EPP 클라이언트 EPP 에 대한 시스템 요구 사항

클라이언트 설치 유틸리티를 통해 Seqrite Endpoint Protection 클라이언트를 설치하는 경우 시스템 요구 사항은 다음과 같습니다.

다음 운영 체제 중 하나:

### Windows 운영 체제

- Microsoft Windows 2008 Server R2 Web/Standard/Enterprise/Datacenter (64 비트)
- Microsoft Windows 7 Home Basic/Premium/Professional/Enterprise/Ultimate (32 비트/64 비트)
- Microsoft Windows SBS 2011 Standard/ Essentials
- Microsoft Windows Server 2012 R2 Standard/Datacenter(64 비트)
- Microsoft Windows Server 2012 Standard/Essentials/Foundation/Storage Server/Datacenter (64 비트)
- Microsoft Windows 8.1 Professional/Enterprise (32 비트/64 비트 ) )
- Microsoft Windows 10 Home/Pro/Enterprise/Education (32 비트/64 비트)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019(64 비트)
- Windows 10 2019 년 11 월 업데이트
- Microsoft Windows Server 2022 표준/데이터 시작/필수 요소

### Mac

프로세서



- Intel core or Apple's M1, M2, M3 chip compatible

### **Mac 운영 체제**

- MacOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13 and 14

### **Linux 32 비트**

- GNU C Library 2.5 이상
- SAMBA 버전 4.16 이하

### **EPP 클라이언트 지원 배포판**

- Debian 9, 10
- Ubuntu 14.04, 16.04
- Boss 6.0
- Linux Mint 19.3

### **Linux 64 비트**

- GNU C Library 2.5 이상
- SAMBA 버전 4.16 이전

### **EPP 클라이언트 지원 배포판:**

- Fedora 30, 32, 35
- Linux Mint 19.3, 20
- Ubuntu 16.04, 18.04, 20.4, 22.04
- Debian 9, 10
- CentOS 7.8, 8.2
- RHEL 7.5, 7.8, 8.2, 8.6, 8.8 Enterprise
- SUSE Linux 12. SP4/Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0(데스크탑), 8.0(서버)
- Oracle Linux 7.1, 7.9 및 8.1

**참고:** EPP Cloud 4.0 은 Linux 64 비트 OS 에서만 EPP 에이전트(v10.11) 배포를 지원합니다.  
Linux 32 비트(v10.9)에 기존에 배포된 에이전트는 예상대로 계속 작동합니다.

## 암호화 정책 구성을 위한 시스템 요구 사항

클라이언트 전제 조건:

- 클라이언트 버전: 10.11
- 라이선스 버전: 프리미엄

하드웨어:

- TPM 2.0
- UEFI 모드

OS 가 포함된 BIOS:

- Windows 10 64 비트
- Windows 11

## 일반적인 요구 사항

### Windows

프로세서

- 최소: 1 GHz 32 비트(x86) 또는 64 비트(x64) 프로세서
- 추천: 2 GHz 32 비트(x86) 또는 64 비트(x64) 프로세서

RAM

- 최소: 1 GB
  - 추천: 2 GB 자유 RAM

하드 디스크 공간

- 3200 MB 자유 공간

## 웹 브라우저

- Internet Explorer 7 또는 나중에

## 네트워크 프로토콜:

- TLS 1.2

## Mac

### 프로세서

- Intel core 또는 Apple's M1, M2, M3 chip 호환 가능

### RAM

- 최소: 512 MB
- 추천: 2 GB 무료 RAM

### 하드 디스크 공간

- 1200 MB 자유 공간

## Linux

### 프로세서

- Intel 또는 호환 가능

### RAM

- 최소: 512 MB
- 추천: 1 GB 무료 RAM

### 하드 디스크 공간

- 1200 MB 자유 공간

## 버그 수정

---

다음은 EPP Cloud 4.0 릴리스에서 수정된 버그 목록입니다.

아니야.	요약
<b>Windows</b>	
1	오버레이로 인해 클라우드 드라이브 내부 폴더에 접근할 수 없습니다. Icon.dll
2	scanexl.dll 로 인해 온라인 보호 시스템 서비스가 중단됩니다.
3	Chrome 에서는 웹사이트에 액세스할 수 없습니다. browse 와 함께 Browser 샌드박스 기능.
4	튠업 reports 는 콘솔 아래에 나타나지 않습니다. Reports section.
5	스케줄 스캔 시간이 EPP 에 반영되지 않습니다. dashboard.
6	instalEPP 클라우드 클라이언트의 운영 Anti-Virus (AV)는 Windows 클라이언트 패키지 생성 중에 프록시 설정을 구성할 때 문제가 발생합니다.
7	DLP, OCR, 클립보드 기능의 조합으로 인해 Seqrite 폴더 내에 과도한 임시 파일이 생성되어 디스크 공간이 부족해집니다.

아니야.	요약
8	다음으로 분류된 파일 기밀 DLP 응용 프로그램 채널 내에서 효과적으로 차단되지 않습니다.
9	자체 모듈 내의 Openssl 취약점을 탐지하는 Seqrite 취약점 스캔입니다.
<b>Mac</b>	
10	클라이언트를 닫는 동안 Mac 시스템이 중단 상태가 됩니다. dashboard.
11	과정 com.quickheal.sysextcontainer.ggc Mac OS 에서 과도한 메모리 사용량을 소비하고 있습니다.
12	Emlprod 포트 5432 가 Postgresql 데이터베이스와 충돌합니다.
13	자산 세부 정보가 콘솔 끝점에 채워지지 않습니다. status Mac 엔드포인트용 페이지입니다.

## 이용정보

---

1. Windows 2016, Windows 2019 Server 및 Windows 2022 Server 의 경우 EPP 4.0 클라이언트를 설치하기 전에 Windows Defender 를 제거하십시오.
2. Windows 7 및 Windows 2008 R2 에 EPP 4.0 클라이언트를 설치하려면 SHA2 호환성을 위해 다음 Windows 패치를 설치해야 합니다.
  - Windows 7 의 경우: [KB4474419](#) 및 [KB4490628](#).
  - Windows 2008 R2 의 경우: KB-[KB4474419](#) 및 [KB4490628](#)
3. Windows 7 32 비트 클라이언트에 패치를 설치하려면 Internet Explorer 버전 11 로 업그레이드해야 합니다.
4. 관리자가 끝점에 대한 조정 알림을 시작하고 끝점이 로그인되어 있지 않으면 조정 알림이 실패합니다.
5. 고급 장치 제어: 인증되고 암호화된 장치를 포맷하면 해당 장치는 승인되지 않은 장치로 처리됩니다. 이 경우 관리자는 다음을 추가해야 합니다.  
장치 제어에서 장치를 다시 설정하고 이에 따라 정책을 구성하십시오.
6. 브라우저 샌드박스를 사용하려면 BIOS 구성에서 시스템의 보안 부팅 기능을 끄십시오.
7. 기본적으로 스팸 방지는 비활성화되어 있습니다. 따라서 클라이언트 대시보드에 빨간색 느낌표가 나타납니다.
8. 맬웨어 방지 검사 보고서에는 이전 브랜드 이름 'Endpoint Security'가 포함되어 있습니다.