Seqrite
Endpoint Protection Cloud

Note di rilascio

Cloud 6.5 | Lug 2026

www.seqrite.it

Informazioni sul copyright

Seqrite Italia – Distribuito da s-mart

Sito web: www.seqrite.it
E-mail: cs@s-mart.biz
Telefono: +39 055 43 03 52
Distributore: s-mart.biz

Marchi

Termini di licenza

L'installazione e l'utilizzo di Seqrite Endpoint Protection sono subordinati all'accettazione incondizionata, da parte dell'utente, dei termini e delle condizioni di licenza per l'utente finale Seqrite.

Per leggere i termini di licenza, visitare http://www.seqrite.com/eula e consultare il Contratto di licenza con l'utente finale (EULA) relativo al proprio prodotto.

Indice

Cronologia delle revisioni

Le informazioni contenute in questo documento sono fornite ad uso esclusivo del team Ricerca e Sviluppo e del team di Supporto di Quick Heal. È severamente vietato pubblicare o distribuire qualsiasi parte di questo documento a terzi.

Versione doc.	Data	Commento
1.0	07 lug 2026	Aggiornamento del client per Windows e Linux

Novità di EPP 6.5

Con questo rilascio, EPP Cloud 6.5 introduce i seguenti miglioramenti:

Aggiornamento del client

- L'aggiornamento del client è ora supportato per gli endpoint **Windows** e **Linux**.
- L'ultima versione del client è la **v10.14.2.0**.
- L'aggiornamento è disponibile per Virus Database (VDB) con data **7 luglio 2026** o successiva.
- La notifica di aggiornamento viene inviata dalla console web di EPP all'endpoint selezionato oppure a livello di gruppo.
- Gli endpoint Mac non supportano l'aggiornamento in-place. Disinstallare il client esistente e installare il pacchetto client più recente.

Limitazioni note per Windows

- Se il sistema operativo (OS) Windows avvia un aggiornamento o un upgrade dell'OS ed esegue un riavvio durante l'installazione dell'AV nel corso del processo di aggiornamento del client, l'installazione dell'AV potrebbe interrompersi. In questi casi è necessario ripulire e reinstallare il client.
- In alcuni scenari, il processo di disinstallazione dell'antivirus può bloccarsi quando il servizio Real-Time Behaviour Detection rimane nello stato Stopping. Ciò può impedire il completamento dell'aggiornamento del client.

In entrambi gli scenari sopra descritti, lo stato AV nella console web di EPP viene visualizzato come **Reboot Required**.

Supporto al deployment unificato per Seqrite EPP

Seqrite EPP è ora integrato nel setup di deployment SUA, che consente agli amministratori di distribuire EPP insieme a ZTNA, Data Privacy e XDR con un unico installer. Questo miglioramento semplifica il deployment consolidando i flussi di installazione in un'esperienza unificata per tutti i prodotti di sicurezza Seqrite.

Vantaggi principali

- Distribuzione di più soluzioni di sicurezza Seqrite tramite un unico pacchetto di installazione.
- Nessuna necessità di gestire installer e processi di deployment separati.
- Rischio ridotto di configurazioni non allineate tra i prodotti.
- Setup semplificato e deployment più rapido in tutti gli ambienti.
- Una base scalabile per integrare ulteriori prodotti nel framework di deployment unificato.

Modifiche alla gestione del deployment

- Nell'ambito di questo miglioramento, la gestione del deployment è stata centralizzata nella console CSM:
- I metodi di deployment non sono più disponibili nella console EPP.
- Tutte le attività relative al deployment sono ora accessibili dalla scheda **Deployment** della **console CSM**.
- Nella console EPP rimane disponibile solo la scheda **Online Installer**, in **modalità di sola lettura**.
- Gli amministratori possono continuare a creare installer dalla console EPP; tuttavia, gli installer generati devono essere scaricati dalla console CSM.

Controlli di sicurezza del browser

Introdotti i Browser Controls in Web Access Controller, per gestire centralmente le impostazioni di sicurezza del browser dalla console EPP.

- Aggiunti controlli per abilitare o disabilitare l'installazione di estensioni del browser, la modalità di navigazione in incognito/privata e gli strumenti per sviluppatori (Developer Tools).
- Garantita la retrocompatibilità: le nuove impostazioni di controllo del browser sono disabilitate per impostazione predefinita nelle policy esistenti.
- Le nuove impostazioni di controllo del browser sono abilitate per impostazione predefinita nelle policy di nuova creazione.
- Activity Logs potenziati per registrare le modifiche alle policy di sicurezza del browser, inclusi l'amministratore che ha effettuato la modifica, le impostazioni modificate e il relativo timestamp, a fini di audit e compliance.

Notifiche basate sui gruppi

Introdotte le notifiche degli eventi endpoint basate sui gruppi per Group Administrator e HOD.

- Le notifiche possono essere inviate solo per gli eventi associati agli utenti dei gruppi assegnati all'amministratore.
- Aggiunto il supporto alla notifica di più amministratori assegnati allo stesso gruppo.
- Visibilità operativa e monitoraggio della compliance migliorati grazie a notifiche mirate sugli eventi.

Supporto client per Linux 32 bit deprecato

A partire da Endpoint Protection versione 8.5.1, la build del client Linux a 32 bit è deprecata e non è più disponibile.

Notifiche basate sui gruppi per gli eventi endpoint

Aggiunto il supporto alle notifiche basate sui gruppi, che consentono a Group Admin e HOD di ricevere avvisi per gli eventi endpoint che si verificano nei gruppi loro assegnati. Le notifiche vengono inviate a tutti i Group Admin associati, anche quando un gruppo ha più amministratori.

Microsoft Access Controller per Web Security

Introdotto Microsoft Access Controller (MAC) per gli endpoint Windows in Web Security. Questa funzionalità consente agli amministratori di controllare l'accesso ai servizi Microsoft configurando gli URL di login dell'organizzazione e i domini consentiti. Gli amministratori possono abilitare o disabilitare la funzionalità tramite le impostazioni delle policy e definire gli endpoint di login e i domini Microsoft approvati, così da garantire che gli utenti accedano alle risorse dell'organizzazione solo tramite account autorizzati. La funzionalità fornisce inoltre un report degli eventi per il monitoraggio e l'audit delle attività di accesso.

Modifica dei requisiti di sistema

Il client EPP può essere installato su endpoint con 4 GB di RAM quando si utilizza un tenant non SUA (Seqrite Universal Agent). Tuttavia, se il pacchetto di installazione viene scaricato da un tenant con SUA abilitato, l'installazione non andrà a buon fine su sistemi con 4 GB di RAM, poiché Seqrite Universal Agent richiede più di 4 GB di RAM per essere installato.

Requisiti di sistema

Requisiti di sistema per i client EPP

Per installare il client Seqrite Endpoint Protection tramite la client install utility, i requisiti di sistema sono i seguenti:

Uno dei seguenti sistemi operativi:

Windows OS

- Microsoft Windows 7 Home Basic / Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Pro / Enterprise (32-bit/64-bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-bit / 64-bit)
- Microsoft Windows 11
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacentre (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 R2 Standard / Datacentre (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacentre (64-bit)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2022 Standard / Datacentre / Essentials
- Microsoft Windows Server 2025 Standard / Datacentre / Essential

MAC

Processore

- Intel Core o chip Apple M1, M2, M3, M4 compatibili

macOS

- macOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13, 14, 15 e 26

Linux

Linux 32-bit

- GNU C Library 2.5 e successive
- SAMBA versione 4.16 e precedenti

Distribuzioni supportate per il client EPP

- Debian 9, 10
- Ubuntu 14.04, 16.04

- Boss 6.0
- Linux Mint 19.3

Nota: supportate solo fino alla versione 10.9 dell'agent Linux.

Linux 64-bit

- GNU C Library 2.5 e successive
- SAMBA versione 4.22 e precedenti

Distribuzioni supportate per il client EPP:

- Fedora 30, 32, 35, 37, 38, 39, 40, 41, 42
- Linux Mint 19.3, 20, 21.3
- Ubuntu 16.04, 18.04, 20.4, 22.04, 24.04 LTS
- Debian 9, 10
- CentOS 7.8, 8.2
- RHEL 7.5, 7.8, 8.2, 8.6, 8.8 Enterprise, 9.0, 9.1, 9.2, 9.3, 9.4 e 9.5
- SUSE Linux 12 SP4 / Enterprise Desktop 15
- Rocky Linux 8.4, 9.3, 9.4, 9.5
- Boss 6.0, 8.0, 9.0 (Desktop), 8.0 (Server)
- Oracle Linux 7.1, 7.9 e 8.1

Nota: dalla versione 10.11 dell'agent Linux in poi, sono supportati solo i sistemi Linux a 64 bit.

Problemi noti

- Quando gli utenti fanno clic con il tasto destro su un file PDF in un endpoint, viene visualizzato l'avviso **"File is being watermarked"**, anche se il tipo di file PDF non è selezionato per il watermarking nella policy DLP.
- I file continuano a essere tracciati dalla DLP quando vengono copiati in percorsi di rete condivisi configurati come eccezioni.
- La funzionalità **DLP Match Count** non rileva i dati riservati presenti nelle intestazioni o nei piè di pagina dei documenti.
- Le funzionalità di watermarking non sono supportate su Microsoft Publisher o MS Access.
- Quando un utente apre e stampa da Microsoft Publisher con l'opzione 'Save as PDF', il PDF salvato non mostra il watermark.
- Il watermark non viene applicato con alcune opzioni specifiche di layout della stampante, come Mirrored, 2Pages o 16PerPage.
- Il menu a tendina di classificazione dei file non compare nel menu contestuale (tasto destro) quando la DLP viene abilitata per la prima volta tramite policy. Salvando e riapplicando la stessa policy DLP, l'opzione di classificazione dei file compare nel menu contestuale.
- Il watermark non viene applicato quando un file riservato viene incorporato in un documento Office padre non riservato (es. Word) tramite Insert → Object → Create from File, anche se la policy DLP è impostata su "Report only" per i file riservati e il watermarking è abilitato.
- I watermark non vengono applicati quando i documenti vengono stampati tramite Command Prompt o PowerShell.
- I documenti stampati mostrano i watermark con orientamento diagonale, anche quando è impostato Horizontal in DLP > Watermark > Orientation.
- Durante le scansioni pianificate Asset su Windows, la dimensione delle applicazioni installate non viene rilevata.
- La funzionalità di blocco Bluetooth non funziona su macOS Tahoe 26, anche se viene visualizzato il prompt "Device Control Blocked".
- Il dispositivo USB aggiunto all'elenco delle eccezioni tramite numero di serie con 'USB Devices' del tool dcconfig non funziona su macOS. In alternativa, è possibile aggiungere il dispositivo USB con 'USB by Serial Number' nelle impostazioni di Device Control Configuration per rendere effettiva l'eccezione su macOS.

Informazioni d’uso

1. Per Windows 2016, Windows 2019 Server, Windows 2022 Server e Windows 2025 Server, disinstallare Windows Defender prima di installare il client EPP.
2. Per installare il client EPP su Windows 7 e Windows 2008 R2, è necessario installare le seguenti patch Windows per la compatibilità SHA2:
   - Per Windows 7: KB4474419 e KB4490628.
   - Per Windows 2008 R2: KB4474419 e KB4490628.
3. Per installare le patch su un client Windows 7 a 32 bit, è necessario aggiornare Internet Explorer alla versione 11.
4. Se l’amministratore avvia una notifica di tune-up per l’endpoint e sull’endpoint non è stato effettuato l’accesso, la notifica di tune-up non andrà a buon fine.
5. Advanced Device Control: se un dispositivo autorizzato e crittografato viene formattato, il dispositivo verrà considerato non autorizzato. In questo caso, l’amministratore dovrà aggiungere nuovamente il dispositivo in Device Control e configurare le policy di conseguenza.
6. Per utilizzare Browser Sandbox, disattivare la funzionalità Secure Boot del sistema dalla configurazione del BIOS.

   Nota: la funzionalità Browser Sandbox non è supportata su Microsoft Edge.
7. Per impostazione predefinita, Spam Protection è disabilitato. Per questo motivo, nella Dashboard del client compare un punto esclamativo rosso.
8. Il report di scansione Antimalware riporta un vecchio nome del brand, ‘Endpoint Security’.
9. La funzionalità Watermark è compatibile solo con Microsoft Office 2016, 2019 e 2022 e non è supportata da WPS Office, LibreOffice, Office 365 o OpenOffice.
10. Linux
    - Il Remote Support tool non può essere eseguito con il comando ‘sudo’. Il tool può essere eseguito con il comando superuser (su).
    - Selezionando l’opzione di migrazione per un gruppo con una macchina client Linux e un’altra Windows, viene visualizzato il messaggio di avviso **Linux client migration is not supported**.

SEQRITE

Quick Heal Technologies Limited

Seqrite Italia www.seqrite.it | cs@s-mart.biz | +39 055 43 03 52 | Distribuito da s-mart.biz