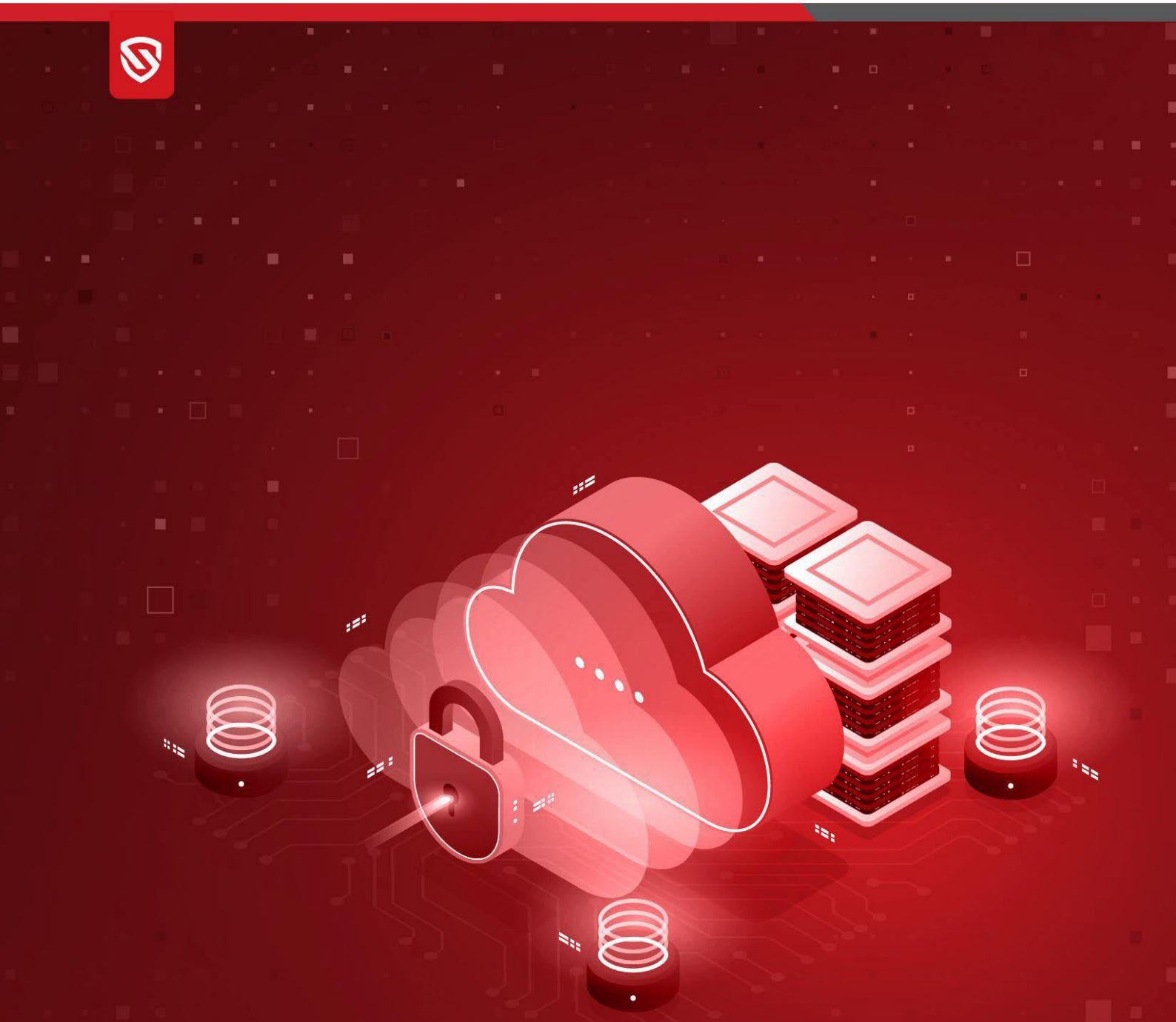
Seqrite
Endpoint Protection Cloud para Mac



www.seqrite.com

EPP Cloud v6.3

Guía del usuario
EEP Cloud v6.3

Información sobre los derechos de autor (copyright)

Fecha de publicación del documento: 20 de junio de 2025

Información sobre este documento

Esta Guía del Usuario contiene toda la información necesaria para instalar y utilizar Seqrite Endpoint Protection de la forma más sencilla posible. Nos hemos asegurado de que todos los datos proporcionados en esta guía estén actualizados con las últimas mejoras del software.

La siguiente lista describe las convenciones que hemos seguido para preparar este documento.

Convención	Significado
Fuente en negrita	Todo lo que aparece resaltado en negrita indica que se trata de una instrucción sobre cómo llevar a cabo una acción.
	Este símbolo indica información adicional o información importante sobre el tema que se está tratando.
<Paso 1> <Paso 2>	Las instrucciones mencionadas en la lista numerada indican las acciones que debe realizar.

Características destacadas de Seqrite Endpoint Protection

Seqrite Endpoint Protection garantiza la máxima protección contra cualquier amenaza o malware que pueda infectar su sistema cuando navega por Internet, trabaja en un entorno de red y accede a su correo electrónico. Puede programar análisis, establecer reglas para los archivos en cuarentena y de copia de seguridad, y bloquear correos electrónicos maliciosos y spam.

Seguridad para Mac le ayuda a personalizar los ajustes relacionados con la protección de los archivos y carpetas en su sistema. Puede configurar las preferencias de análisis, aplicar reglas para la Protección contra virus, programar análisis, excluir archivos y carpetas del análisis y establecer reglas para los archivos en cuarentena y de copia de seguridad.

Seguridad para Mac le ayuda a establecer reglas de protección para proteger su equipo contra archivos maliciosos que pueden colarse en su sistema durante actividades en línea, como operaciones bancarias, compras, navegación, etc.

Seguridad de correo electrónico le ayuda a personalizar las reglas de protección para recibir correos electrónicos de diversas fuentes. Puede establecer reglas para bloquear los correos electrónicos sospechosos de ser spam o malware.

Para obtener más información, visite http://www.seqrite.com.

Contenido

Capítulo 1. Introducción

Seqrite Endpoint Protection es fácil de instalar y utilizar. Durante la instalación, lea atentamente cada pantalla de instalación y siga las instrucciones.

Requisitos

Recuerde la siguiente información antes de instalar Seqrite Endpoint Protection en su equipo Mac:

- Un sistema que tenga varios programas antivirus instalados puede provocar un mal funcionamiento del sistema. Si hay algún otro programa antivirus instalado en su sistema, debe eliminarlo antes de continuar con la instalación de Seqrite Endpoint Protection.
- Cierre todos los programas abiertos antes de continuar con la instalación.
- Le recomendamos que haga una copia de seguridad de sus datos por si su sistema se infecta con algún virus.
- Seqrite Endpoint Protection debe instalarse con derechos administrativos.

Requisitos del sistema

Para utilizar Seqrite Endpoint Protection, su sistema debe cumplir los siguientes requisitos mínimos:

- macOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13, 14 ,15, y 26
- Dispositivos Mac con procesador Intel o chip Apple M1, M2, M3 y M4
- Mínimo 512 MB de RAM, se recomiendan 2 GB o más
- 1200 MB de espacio libre en el disco duro

  Los requisitos indicados son los requisitos mínimos del sistema. Para los mejores resultados, le recomendamos que su sistema tenga una configuración superior.

Para consultar los últimos requisitos del sistema, visite: http://www.seqrite.com.

Clientes que admiten el análisis de correo electrónico

Los clientes de correo electrónico POP3 que admiten la función de análisis de correo electrónico son los siguientes:

- Apple Mail Ver. 10.3 y posteriores
- Thunderbird
- Sparrow
- Sea Monkey
- MailSmith

Clientes que no admiten el análisis de correo electrónico

Los clientes de correo electrónico POP3 y los protocolos de red que no admiten la función de análisis de correo electrónico son los siguientes:

- IMAP
- AOL
- POP3 con Secure Sockets Layer (SSL)
- Correo electrónico basado en la web, como Hotmail y Yahoo! Mail
- Lotus Notes

Conexiones SSL no compatibles

Email Protection no admite conexiones de correo electrónico cifradas que utilicen Secure Sockets Layer (SSL). Si se utilizan conexiones SSL, los correos electrónicos no estarán protegidos por Email Protection.

Instalación de Seqrite Endpoint Protection en un sistema Mac

Antes de instalar el Cliente para Mac, cree el instalador del Cliente para Mac en el Servidor Endpoint de la siguiente manera.

Para crear un instalador del Cliente de Seqrite para Mac, siga estos pasos:

1. Inicie sesión en Seqrite Endpoint Protection Cloud.
2. Vaya a Implementación.
3. Haga clic en el botón **Crear instalador** para crear el Instalador del Cliente.

   Se abrirá el cuadro de diálogo Crear Instalador del Cliente.
4. Introduzca el **Nombre del instalador** y seleccione Grupo.
5. En la lista de **plataformas de sistema operativo**, seleccione Mac.
6. Se selecciona un período de validez predeterminado de 30 días. Puede cambiarlo a 60 o 90 días si es necesario.
7. Se muestra la ruta de la carpeta predeterminada para la instalación. Anótela.
8. Haga clic en **Crear**. Se crea el archivo <Nombre del instalador>.TAR.

Se crea el instalador sin configuración antivirus y aparece en la lista de la página Implementación > Instalador de cliente. Puede descargar este instalador.

Nota

Con el Instalador independiente (Standalone Installer), puede crear un Instalador de cliente para Mac con la configuración con antivirus.

Enlace de instalación por correo electrónico

El enlace de instalación por correo electrónico le permite enviar una notificación por correo electrónico a las terminales de la red para instalar el cliente de Seqrite Endpoint Protection.

Para notificar a los clientes que instalen el Cliente de Seqrite para Mac, siga estos pasos:

1 Inicie sesión en Seqrite Endpoint Protection Cloud.

2 Seleccione Implementación > Enlace de instalación por correo electrónico.

Aparecerá la pantalla Enlace de instalación por correo electrónico.

3 En el campo "Para", escriba la dirección de correo electrónico.

Si hay varios destinatarios, inserte un punto y coma (;) entre las direcciones de correo electrónico.

Puede modificar el asunto del mensaje si lo desea.

4 Haga clic en Enviar correo electrónico.

El administrador envía un mensaje de notificación de instalación que contiene un enlace al archivo de instalación antes de instalar Seqrite Endpoint Protection.

5 Para instalar Seqrite EPP Client en un sistema Mac, escriba el enlace del instalador en el navegador.

El enlace se le enviará a su dirección de correo electrónico.

Aparecerá una página web que mostrará los requisitos para la instalación e incluye un enlace al archivo de instalación (Descargar Cliente para Mac). Lea atentamente los requisitos.

6 Haga clic en el enlace Descargar cliente para Mac.

Se descargará un archivo tar que incluye el instalador.

7 Vaya a la ubicación donde guardó el archivo tar y extraiga todos sus componentes.

8 Haga doble clic en el archivo de instalación (MCLAGNT.DMG).

9 Ejecute el Instalador para iniciar la instalación de Seqrite Endpoint Protection.

Nota:

- El Control de dispositivos y la Prevención de pérdida de datos dependen de la Protección contra virus.
- La Protección contra phishing, la Protección de navegación y la Seguridad Web pueden crear varios informes para una sola instancia si la URL restringida se ejecuta en el navegador Opera.
- No se pueden enviar notificaciones de Análisis remoto, Actualización remota y Desinstalación remota desde la consola web de Seqrite EPP si el usuario del Cliente para Mac no inició sesión en el equipo Mac.

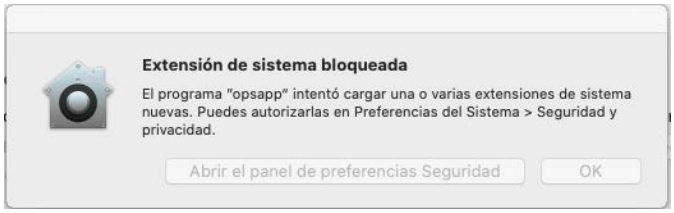
Instalación del cliente de Seqrite Endpoint Protection para Mac en macOS Catalina y versiones posteriores

macOS Catalina y sus versiones posteriores requieren la aprobación de los usuarios para ejecutar el Instalador de Endpoint Protection para Mac, cuando el archivo tar se extrae en la carpeta Escritorio/Descargas.

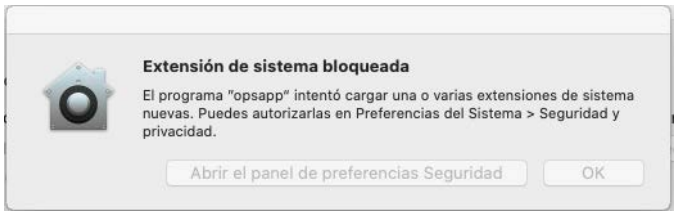
1 Durante la instalación del Cliente EPP Cloud Mac, aparece un mensaje solicitando permiso para acceder a la carpeta Escritorio/Descargas/Documentos, donde se extrae el archivo MCCLAGNT.TAR.

2 Para continuar con la instalación, haga clic en **Aceptar**.

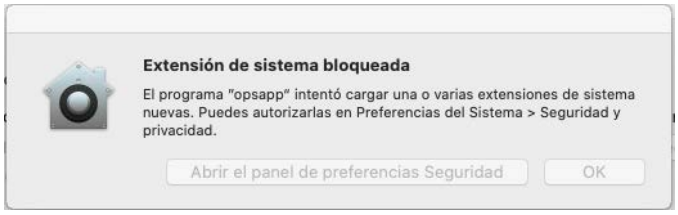
- Para los usuarios que tengan macOS Catalina, aparecerán las siguientes solicitudes de extensión del sistema una por una cuando comience la instalación. Haga clic en **Abrir preferencias de seguridad** en todas las solicitudes.



Mensaje de Autoprotección (ggcext)

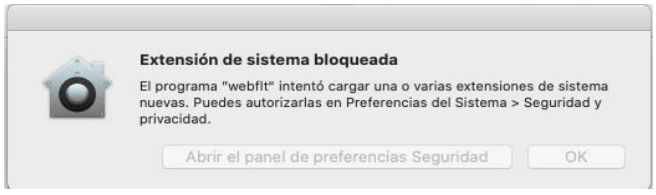


Mensaje de Protección en línea (Opsext)

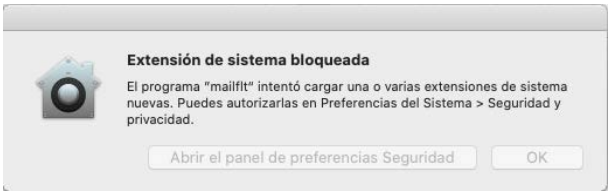


Mensaje de Prevención de pérdida de datos (dlpext)

Mensaje del Monitor de actividad de archivos (famext)



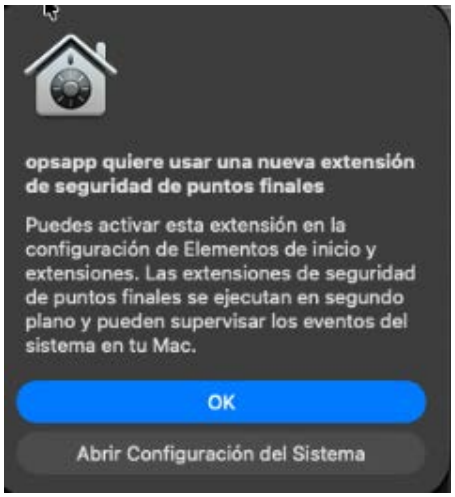
Mensaje de Seguridad Web (webflt)



Mensaje de Seguridad de correo electrónico (mailflt)

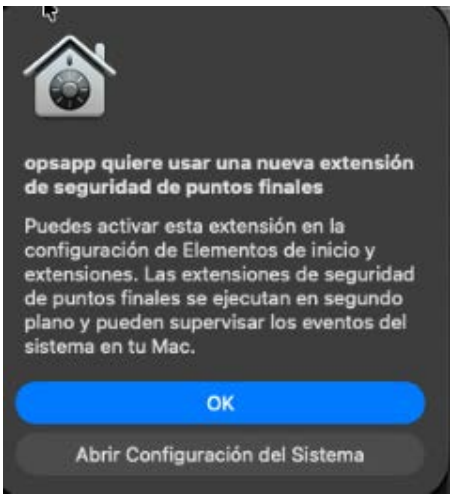
- Para los usuarios que tengan macOS Big Sur y versiones posteriores, aparecerán las siguientes indicaciones una por una cuando comience la instalación. Haga clic en **"Abrir preferencias de seguridad"** en todas las indicaciones.

Mensaje de Autoprotección (ggcext)



Mensaje de Protección en línea (Opsext)

Mensaje de Prevención de pérdida de datos (dlpext)



Mensaje del Monitor de actividad de archivos (famext)

Mensaje de Seguridad Web (webfIt)

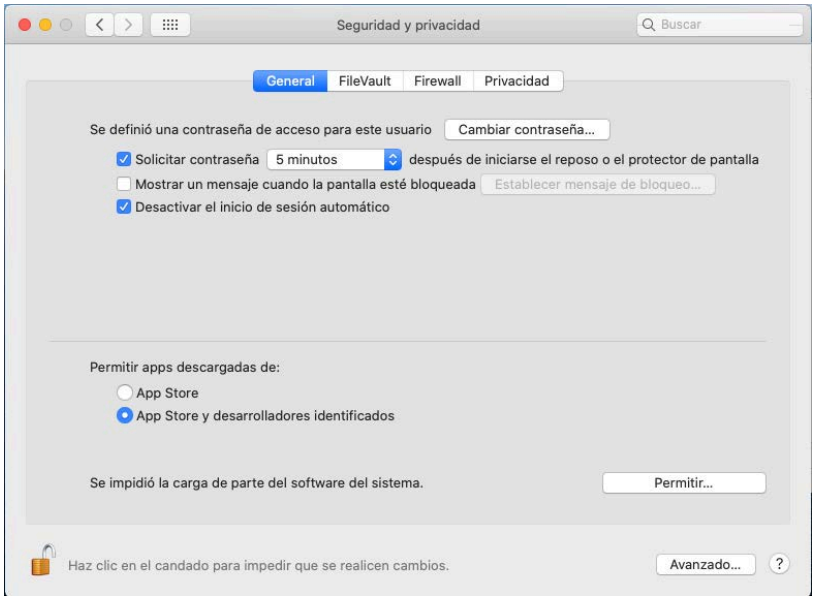
Mensaje de Seguridad de Correo electrónico (mailfIt)

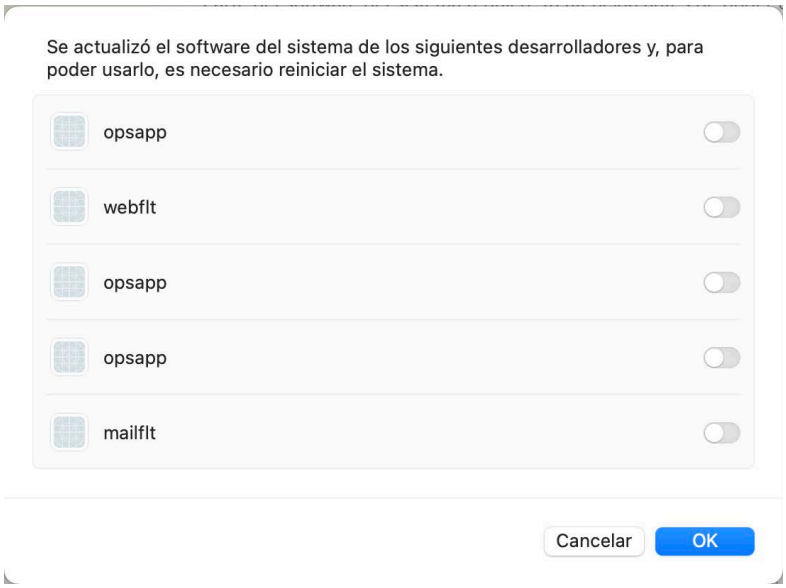
3 El usuario debe PERMITIR todas las solicitudes de extensión del sistema que se muestran arriba para garantizar la siguiente configuración en macOS Catalina y macOS Sonoma.

i. Vaya a **Preferencias del sistema > Seguridad y privacidad**.

ii. Haga clic en el icono del candado y proporcione la contraseña si está bloqueado.

iii. Haga clic en el botón **Permitir,** como se muestra en la siguiente captura de pantalla.





Nota: En macOS Catalina, aparece "Placeholder Developer [Marcador de posición Desarrollador]" en lugar del nombre de la aplicación correspondiente. Apple ha reconocido este problema y, según la empresa, se solucionará en Big Sur. *https://developer.apple.com/forums/thread/130056*

iv. Aparecerá la lista de software del sistema actualizado. Haga clic en **Aceptar**.

v. Reinicie el equipo.

4 Permitir las solicitudes de extensión del sistema en macOS Sequoia

Para configurar las extensiones del sistema en macOS Sequoia, siga estos pasos para habilitar tanto las extensiones de seguridad de las terminales como las extensiones de red:

- **Extensiones de Endpoint Security**
  a) Vaya a **Configuración del sistema** > **General** > **Elementos de inicio de sesión y extensiones**. Haga clic en el **icono de información** situado junto a **Extensiones de Endpoint Security**.
  Para usuarios de **Tahoe**: **Seleccione Por categoría** y, a continuación, vaya a **«Extensiones de Endpoint Security».**

  b) En la sección Extensiones de Endpoint Security, habilite individualmente las siguientes extensiones:
  `opsext`
  `dlpext`
  `famext`
  `ggcext`

  c) Después de habilitar cada extensión, haga clic en **Hecho**.

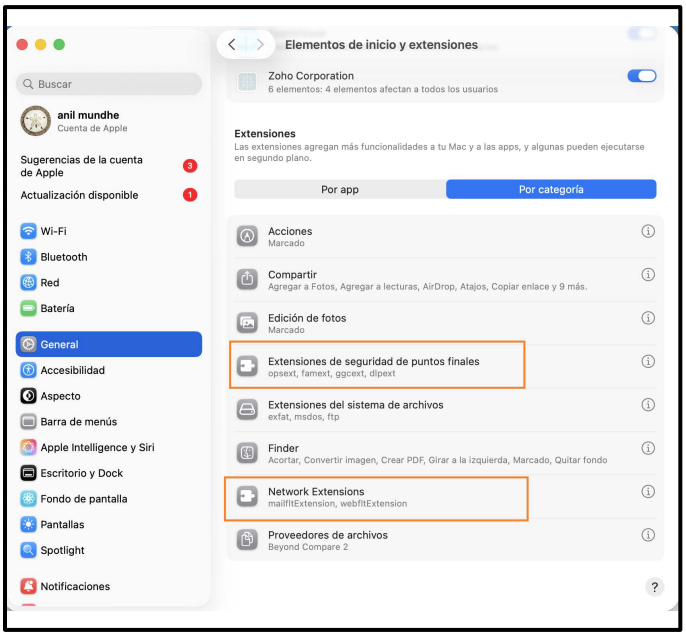
- **Extensiones de red**

a) Vaya a **Configuración del sistema** > **General** > **Elementos de inicio de sesión y extensiones**. Haga clic en el **icono de información** situado junto a **Extensiones de red**.
Para usuarios de **Tahoe**: Seleccione **Por categoría** y, a continuación, vaya a «**Extensiones de red**».

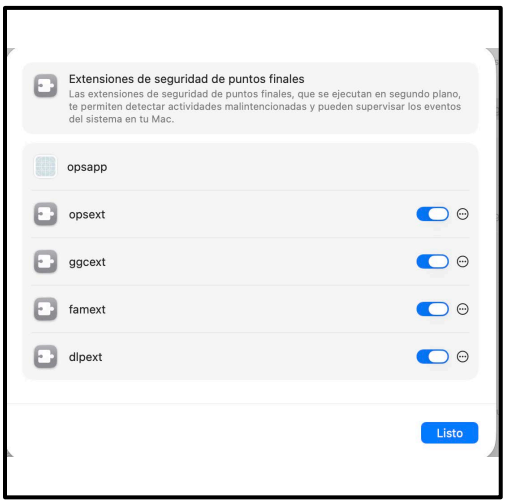
b) En la sección Extensiones de red, habilite individualmente las siguientes extensiones:

```
Webflt
mailflt
```

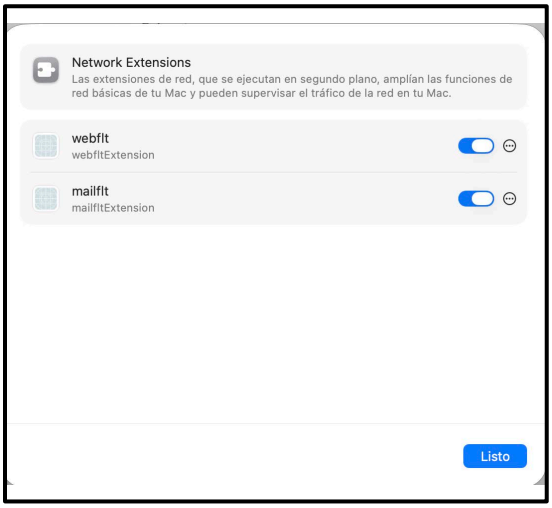
c) Después de habilitar cada extensión, haga clic en **Hecho**.



Extensiones de Endpoint Security:



Extensiones de red:



Se requiere permiso para admitir macOS Catalina y versiones posteriores

El producto [Seqrite] y los servicios requieren permiso para acceder a los archivos del sistema en macOS Catalina y versiones posteriores. Después de habilitar todas las aplicaciones y servicios, es necesario reiniciar el sistema.

1. Tras la instalación correcta de Seqrite Endpoint Protection, aparecerán las siguientes indicaciones.
   - Para los usuarios que tengan macOS Catalina, aparecerán las siguientes indicaciones. Haga clic en **Permitir** en todas las indicaciones.

Configuraciones de VPN de seguridad de correo electrónico

Contenido de red de Seguridad Web

- Para los usuarios que tengan macOS Big Sur y versiones posteriores, aparecerán los siguientes mensajes. Haga clic en **Permitir** en todos los mensajes.

Configuraciones de VPN de seguridad del correo electrónico **Contenido de red de Seguridad Web**

2 Aparecerá el mensaje de aviso de Avprompt como se muestra a continuación.

AVprompt

3 Realice los siguientes ajustes en macOS.

i. Abra **Preferencias del sistema**.

ii. Vaya a **Seguridad y privacidad >** pestaña **Privacidad**.

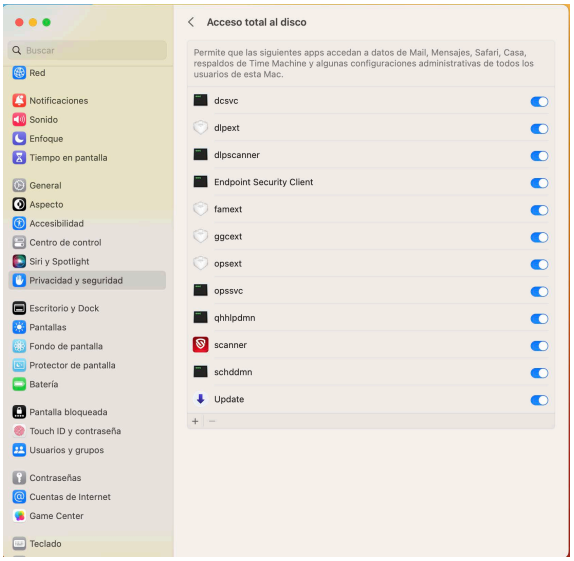
iii. Haga clic en el icono del candado e introduzca la contraseña si está bloqueado.

iv. Seleccione **Acceso completo al disco** en el panel izquierdo.

Añada los siguientes procesos en la ruta indicada y, a continuación, seleccione los procesos en la ventana Seguridad y privacidad > Acceso completo al disco:

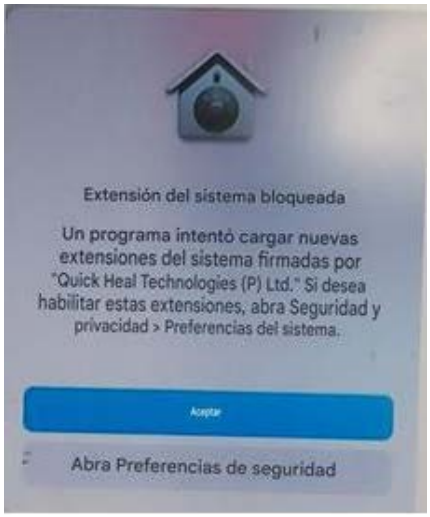
- /Library/Application Support/Seqrite/ Seqrite/opssvc
- /Library/Application Support/Seqrite/ Seqrite/qhhlpdmn
- /Library/Application Support/Seqrite/ Seqrite/dlpscanner
- /Library/Application Support/Seqrite/ Seqrite/scanner.app
- /Library/Application Support/Seqrite/ Seqrite/update.app
- /Library/ Application Support/Seqrite/ Client Agent 10.13/Endpoint Protection Client
- /Library/ Application Support/Seqrite/Seqrite/schddmn
- opsext (ya presente en la sección de privacidad)
- ggcext (ya presente en la sección de privacidad)
- Dlpext (ya presente en la sección de privacidad)
- famext (ya presente en la sección de privacidad)
- /Library/Application Support/Seqrite/Seqrite/dcsvc (aplicable solo a macOS Big Sur y versiones posteriores)

4 Aparecerá la siguiente captura de pantalla que mostrará **la configuración de Acceso completo al disco** en Preferencias del sistema.



Acceso completo al disco

Si instala el Cliente de Seqrite Endpoint Protection para Mac en macOS Catalina por primera vez, aparecerá el siguiente mensaje de alerta:

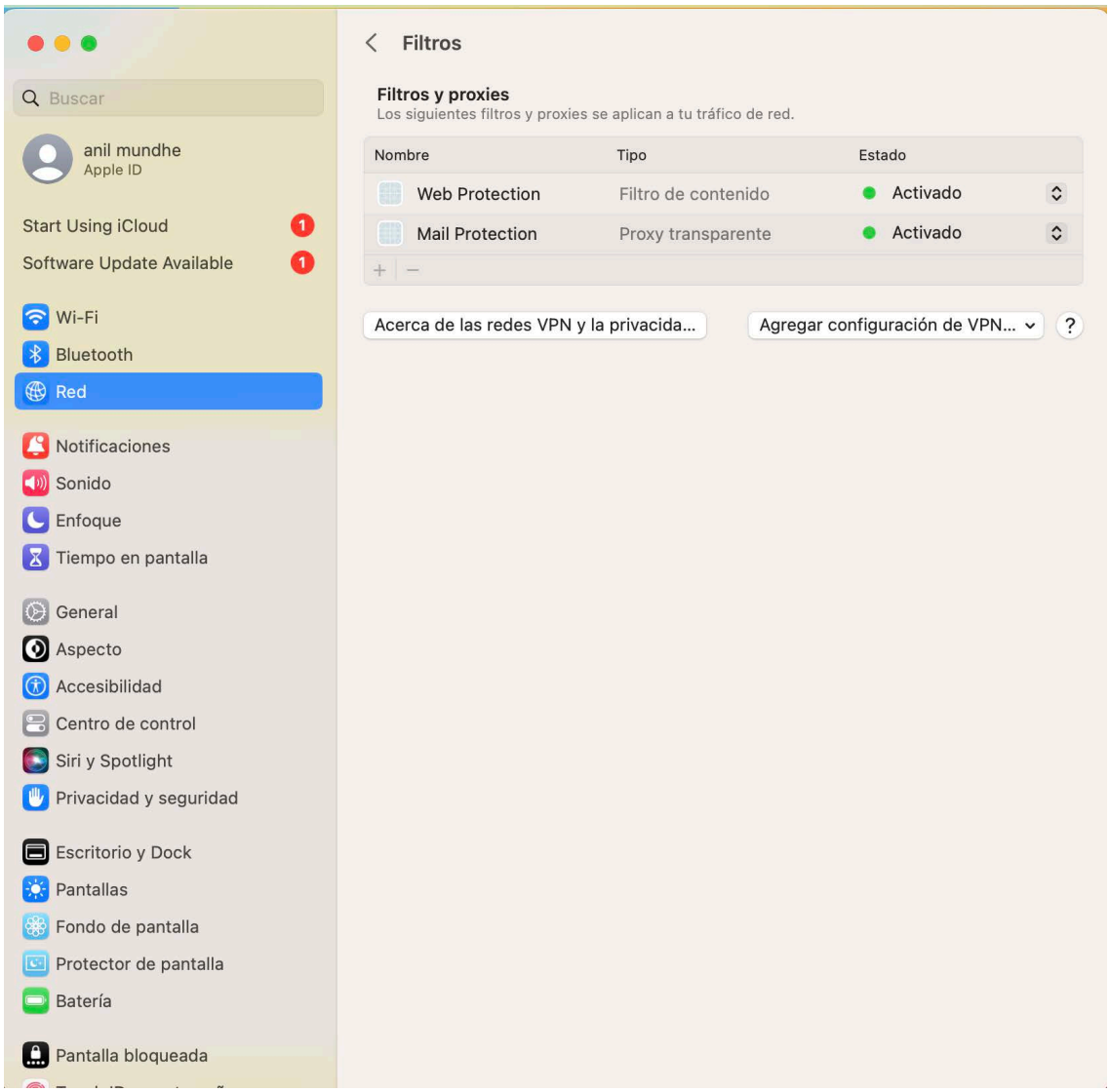


Nota: El mensaje anterior no aparece en macOS Big Sur y versiones posteriores (sistema Intel y ARM64 de Apple).

5 Para que el cliente de Seqrite EPP Mac funcione en macOS Catalina y versiones posteriores, proceda como se indica a continuación:

i. Haga clic en Abrir preferencias de seguridad.
ii. Habilite "Quick Heal Technologies (P) Ltd." en "Preferencias del sistema >> Seguridad y Privacidad".

6 La siguiente captura de pantalla muestra el estado de conexión de las extensiones de red mailflt y webflt en Preferencias del sistema > Red.



Nota: Una vez que se hayan permitido todas las extensiones del sistema y se hayan concedido los permisos necesarios, reinicie el equipo.

Tenga en cuenta que:

- El Control de dispositivos, la Prevención de pérdida de datos y el Monitor de actividad de archivos dependen de la Protección contra virus.

- La Protección contra phishing, la Protección de navegación y la Seguridad Web pueden crear varios informes para una sola instancia si se ejecuta una URL restringida en el navegador Opera.
- No se pueden enviar notificaciones para el Análisis remoto, la Actualización remota y la Desinstalación remota desde la consola web de Seqrite EPP si el usuario del Cliente para Mac no ha iniciado sesión en el equipo Mac.

Instalación remota de Seqrite Endpoint Protection en un sistema Mac

Puede instalar Cliente de Seqrite para Mac utilizando cualquiera de las siguientes opciones.

- Instalación mediante Apple Remote Desktop o Casper
- Conexión remota mediante Secure Shell
    - Uso de Terminal (para sistemas operativos Mac y Linux)
    - Uso de PuTTY (para sistemas operativos Windows)
- Implementación a través de ManageEngine

Creación del Instalador del Cliente para Mac

Para crear el instalador del Cliente para Mac, siga estos pasos:

1. Inicie sesión en Seqrite Endpoint Protection Cloud.
2. Vaya a Implementación y haga clic en el botón **Crear instalador**.

Se abrirá el cuadro de diálogo Crear Instalador de cliente.

3. Introduzca el nombre del paquete y seleccione **Grupo**.
4. En la lista de plataformas de sistema operativo, seleccione **Mac**.
5. Seleccione el período de validez en el cuadro de lista. El período de validez puede ser de 30, 60 o 90 días.
6. Haga clic en **Crear**.

Se crea el archivo <Nombre del paquete>.TAR.

Se crea el instalador sin la configuración antivirus y aparece en la lista de la página Implementación > Instalador de cliente. Puede descargar este instalador.

Nota

Con el Instalador independiente (Standalone Installer), puede crear un Instalador de Cliente para Mac con la configuración antivirus.

Instalación mediante Apple Remote Desktop o Casper

Apple Remote Desktop (ARD) le ayuda a conectarse de forma remota a los equipos Cliente para Mac de la red, enviarles software, instalar software en ellos, ayudar a otros usuarios finales en tiempo real y realizar diversas tareas.

Requisitos

Antes de instalar el Cliente de Seqrite para Mac, asegúrese de que se cumplan los siguientes requisitos.

- El equipo administrador con ARD o Casper instalado debe tener Mac OS 10.12 o posterior.
- El instalador del Cliente de Seqrite para Mac debe crearse en Seqrite Endpoint Protection Cloud. Para saber cómo crear el instalador del cliente, consulte Creación del Instalador del Cliente para Mac.
- El administrador debe tener una cuenta en los equipos Cliente para Mac con privilegios de administrador.
- Se debe habilitar la Administración remota en los equipos Cliente para Mac.
- Su equipo administrador debe tener instalado Packages. Packages es una aplicación del sistema operativo Mac que le ayuda a crear paquetes para su carga útil e instalación. Para descargar Packages, visite http://s.sudre.free.fr/Software/Packages/about.html.
- Solo para macOS Catalina y versiones posteriores, haga lo siguiente en su sistema Mac:

1. Abra Preferencias del sistema.
2. Vaya a **Seguridad y privacidad >** pestaña **Privacidad**.
3. Haga clic en el icono del **candado** y proporcione la contraseña si está bloqueado.
4. Seleccione **Acceso completo al disco** en el panel izquierdo.
5. Añada el siguiente proceso en la ruta indicada y, a continuación, seleccione los procesos en la ventana **Seguridad y privacidad** > **Acceso completo al disco,**

   /Library/PrivilegedHelperTools/fr.whitebox.packages/packages_dispatcher

Instalación del Cliente para Mac mediante Apple Remote Desktop o Casper

Este procedimiento le ayudará a instalar el Cliente para Mac en los equipos Cliente para Mac remotos utilizando ARD o Casper. Para obtener más detalles, puede consultar la documentación de las respectivas aplicaciones de software.

Creación del paquete del Cliente para Mac

1. En Seqrite Endpoint Protection Cloud, descargue UEMREMOTEINST.TAR desde la URL

   http://dlupdate.quickheal.com/builds/seqrite/uemcp/en/UEMREMOTEINST.tar
   Descargue las compilaciones del Cliente para Mac desde el servidor EPP Cloud. Estas compilaciones estarán en formato TAR.
2. Cambie el nombre del instalador del Cliente para Mac de la siguiente manera:
   - Instalador del cliente para Mac: MCCLAGNT.TAR
3. Extraiga UEMREMOTEINST.TAR.
4. Copie MCCLAGNT.TAR en "<Directorio de descarga>/UEMREMOTEINST".
5. Abra Terminal.app en el equipo Mac del administrador y vaya a la carpeta UEMREMOTEINST.
6. Introduzca los siguientes comandos:

```
cd ./Remote_Installation/PKG
sudo sh ./ClientAgentInstaller/CreatePackage.sh
```

Se requieren derechos de administrador para ejecutar este comando.

Cuando la creación del paquete se completa correctamente, se crea el archivo ClientAgentInstaller.pkg en la carpeta ./Remote_Installation/PKG/ClientAgentInstaller/.

Si no se puede crear el Empaquetador del cliente en macOS Catalina y versiones posteriores, haga lo siguiente:

1. Abra Preferencias del sistema.
2. Vaya a **Seguridad y privacidad >** pestaña **Privacidad**.
3. Haga clic en el icono del **candado** y proporcione la contraseña si está bloqueado.
4. Seleccione **Acceso completo al disco** en el panel izquierdo.
5. Seleccione la casilla **packages_dispatcher**.
6. Ahora vuelva a intentar crear el Empaquetador del cliente y se creará correctamente.

Implementación del Cliente de Seqrite para Mac mediante Apple Remote Desktop

Además de los requisitos descritos en la sección anterior, siga este requisito previo.

Requisito previo

Antes de implementar el Cliente de Seqrite para Mac, asegúrese de tener instalada la herramienta Apple Remote Desktop (ARD) en su equipo administrador. Para descargar ARD, visite https://www.apple.com/in/remotedesktop.

Para implementar el Cliente de Seqrite para Mac utilizando Apple Remote Desktop, siga estos pasos:

1. Abre Apple Remote Desktop.
2. Seleccione los equipos Cliente para Mac de la lista de todos los equipos disponibles y, a continuación, haga clic en *Instalar* para agregar el paquete.
3. Haga clic en el signo más (+) para localizar y agregar ClientAgentInstaller.pkg y, a continuación, haga clic en *Instalar* para iniciar la implementación.

Implementación del Cliente de Seqrite para Mac con Casper

Además de los requisitos descritos en la sección anterior, siga este requisito previo.

Requisito previo

Antes de implementar el cliente de Seqrite para Mac, asegúrese de tener la herramienta Casper instalada en su equipo administrador. Casper ayuda a instalar software y ejecutar scripts de forma remota en los equipos cliente. Para descargar Casper, visite http://www.jamfsoftware.com/products/casper-suite/.

Para implementar el Cliente de Seqrite para Mac con Casper, siga estos pasos:

1. Inicie sesión en **Casper Admin**.
2. Arrastre ClientAgentInstaller.pkg a la ventana y, a continuación, seleccione **Archivo > Guardar**.
3. Inicie sesión en **Casper Remote**.
4. En la pestaña Equipos, seleccione los equipos cliente para Mac de la lista de equipos disponibles.

5 En la pestaña Paquetes, seleccione ClientAgentInstaller.pkg.

6 Haga clic en **Ir.**

Conexión remota mediante Secure Shell

Secure Shell (SSH) es un protocolo de red que se utiliza para conectarse a los equipos Cliente para Mac remotos a través de una comunicación de datos segura mediante la línea de comandos para administrar los equipos cliente.

Uso de Terminal (para sistemas operativos Mac o Linux)

El equipo administrador con el sistema operativo Mac o Linux puede instalar el cliente utilizando este método.

Requisitos

Antes de instalar el cliente de Seqrite para Mac, asegúrese de que se cumplan los siguientes requisitos.

- El administrador debe tener una cuenta en los equipos Cliente para Mac con privilegios de administrador.
- Habilite el inicio de sesión remoto y permita el acceso a todos los usuarios o solo a usuarios específicos, como los administradores. Puede encontrar esta configuración en el equipo Mac en Preferencias del sistema > Compartir > Inicio de sesión remoto.
- Asegúrese de que el firewall no bloquee el puerto que utiliza Secure Shell (SSH), que por defecto es el puerto TCP 22. Este puerto permite la comunicación necesaria para el inicio de sesión remoto.
- Si utiliza el firewall de Mac, desactive el modo oculto. Con el modo oculto activado, la instalación remota push no puede detectar el cliente a través de Buscar red.
- Para desactivar el modo oculto en los equipos Mac, haga lo siguiente:

1 En Preferencias del sistema, vaya a **Seguridad y privacidad**.

2 Haga clic en el icono del **candado** e introduzca la contraseña si está bloqueado.

3 Seleccione **Firewall > Opciones de firewall**.

4 Desactive la casilla de verificación **Habilitar modo oculto** si está seleccionada.

5 Haga clic en **Aceptar**.

- El instalador del cliente de Seqrite para Mac debe crearse en EPP Cloud. Para saber cómo crear el instalador del cliente, consulte Creación del instalador del cliente para Mac.

Instalación del Cliente de Seqrite para Mac

Para instalar el Cliente de Seqrite para Mac mediante Terminal, siga estos pasos en el equipo Mac del administrador:

En Seqrite Endpoint Protection Cloud, descargue UEMREMOTEINST.TAR desde la URL http://dlupdate.quickheal.com/builds/seqrite/uemcp/en/UEMREMOTEINST.tar

1 Descargue las compilaciones del Cliente para Mac desde el servidor EPP Cloud. Estas compilaciones estarán en formato TAR.

2 Cambie el nombre del instalador del Cliente para Mac de la siguiente manera:

Instalador del Cliente para Mac: MCCLAGNT.TAR

3 Extraiga UEMREMOTEINST.TAR.

4 Copie MCCLAGNT.TAR en "<Directorio de descargas>/UEMREMOTEINST". El directorio de descargas es el directorio en el que se descargó y extrajo UEMREMOTEINST.TAR.

5 Abra Terminal.app y vaya a la carpeta Instalación remota.

6 Introduzca el siguiente comando

```
sh ./Scripts/copy.sh <username> <ip_address>
```

Descripción de los parámetros

sh ./Scripts/copy.sh es estático.

<username> especifica el nombre de usuario del equipo Mac remoto, por ejemplo, 'test'.

<ip_address> especifica la dirección IP del equipo Mac remoto, por ejemplo, '10.10.0.0'.

Ejemplo: sh ./Scripts/copy.sh "test" "10.10.0.0"

7 Introduzca la contraseña del equipo remoto para conectarse a él.

8 Introduzca el comando `sudo sh /tmp/install.sh`.

9 Introduzca la contraseña del equipo remoto cuando se le solicite.

10 Aparecerá un mensaje de confirmación: "Si se encuentra una versión anterior del cliente de Seqrite Endpoint Protection en el sistema, se desinstalará automáticamente. ¿Desea continuar? [Sí/No]:".

11 Introduzca **Sí** o **No**.

- Si introduce **Sí,** la instalación continuará.
- Si introduce **No,** la instalación se cancelará con el mensaje "Se ha seleccionado la opción No. Instalación cancelada".

12 Introduzca el comando `exit` para cerrar la sesión SSH remota.

13 Repita los pasos del 6 al 10 para instalar el Cliente de Seqrite para Mac en otro equipo remoto.

Uso de PuTTY (para el sistema operativo Windows)

El equipo administrador con el sistema operativo Windows puede instalar el Agente del cliente utilizando este método.

Requisitos

Antes de instalar el Cliente de Seqrite para Mac, asegúrese de que se cumplan los siguientes requisitos.

- El administrador debe tener una cuenta en los equipos Cliente para Mac con privilegios de administrador.

- Habilite el Inicio de sesión remoto y permita el acceso a todos los usuarios o solo a usuarios específicos, como los Administradores. Puede encontrar esta configuración en el equipo Cliente para Mac en Preferencias del sistema > Compartir > Inicio de sesión remoto.
- Asegúrese de que el firewall no bloquee el puerto que utiliza Secure Shell (SSH), que por defecto es el puerto TCP 22. Este puerto permite la comunicación necesaria para el inicio de sesión remoto.
- Si utiliza el firewall de Mac, desactive el modo oculto. Con el modo oculto activado, la instalación remota no puede detectar el cliente a través de Buscar red.
- Para desactivar el modo oculto en los equipos Mac, haga lo siguiente:

1. En Preferencias del Sistema, vaya a **Seguridad y Privacidad**.
2. Haga clic en el icono del **candado** e introduzca la contraseña si está bloqueado.
3. Seleccione **Firewall > Opciones de firewall**.
4. Desactive la casilla de verificación **Activar modo oculto** si está seleccionada.
5. Haga clic en **Aceptar**.

- El instalador del Cliente de Seqrite para Mac debe crearse en Seqrite Endpoint Protection Cloud. Para saber cómo crear el instalador del cliente, consulte Creación del instalador del Cliente para Mac.
- Si utiliza macOS Catalina (10.15) e instala Endpoint Protection Cloud para Mac, haga lo siguiente:

  Para continuar con la instalación, macOS Catalina requiere su aprobación para acceder al directorio donde se extrae el archivo MCCLAGNT.TAR (por ejemplo, el escritorio, la carpeta Descargas o la carpeta Documentos). En la ventana Preferencias del sistema > Seguridad y privacidad > Privacidad > Archivos y carpetas, seleccione todas las opciones junto a "Acceder al directorio".

Instalación del Cliente de Seqrite para Mac

Para instalar el Cliente de Seqrite para Mac con PuTTY, siga estos pasos:

En Seqrite Endpoint Protection CloudDE, descargue UEMREMOTEINST.TAR desde la URL http://dlupdate.quickheal.com/builds/seqrite/uemcp/en/UEMREMOTEINST.tar

1. Descargue las compilaciones del Cliente para Mac desde el servidor EPP Cloud. Estas compilaciones estarán en formato TAR.
2. Cambie el nombre del instalador del Cliente para Mac de la siguiente manera:

   Instalador del Cliente para Mac - MCCLAGNT.TAR
3. Extraiga UEMREMOTEINST.TAR.
4. Copie MCCLAGNT.TAR en "<Directorio de descarga>/UEMREMOTEINST". El directorio de descarga es el directorio en el que se descargó y extrajo UEMREMOTEINST.TAR.
5. Abra cmd.exe y vaya a la carpeta "<Directorio de descarga>/UEMREMOTEINST".
6. Haga lo siguiente:

- Introduzca el siguiente comando si el antivirus no está incluido en el empaquetador del cliente
  .\Remote_Installation\Softwares\pscp.exe .\MCCLAGNT.TAR .\Remote_Installation\Scripts\install.sh <username>@<ip_address>:/tmp/

Descripción de los parámetros

<username> especifica el nombre de usuario del equipo Cliente para Mac remoto, por ejemplo, 'test'

<ip_address> especifica la dirección IP del equipo Cliente para Mac remoto, por ejemplo, '10.10.0.0'.

Ejemplo: .\Remote_Installation\Softwares\pscp.exe .\MCCLAGNT.TAR .\Remote_Installation\Scripts\install.sh test@10.10.0.0:/tmp/.

7 Abra .\Remote_Installation\Softwares\putty.exe.

8 Introduzca la dirección IP del equipo Cliente para Mac remoto y haga clic en *Abrir*.

9 En la ventana del terminal PuTTY, introduzca el nombre de usuario y la contraseña de un usuario administrador del equipo remoto.

10 Una vez conectado al equipo remoto, escriba el siguiente comando `sudo sh /tmp/install.sh`.

11 Aparecerá un mensaje de confirmación: "Si se encuentra una versión anterior del cliente de Seqrite Endpoint Protection en el sistema, se desinstalará automáticamente. ¿Desea continuar? [Sí/No]:".

12 Introduzca **Sí** o **No**.

- Si introduce **Sí**, la instalación continuará.
- Si introduce **No**, la instalación se cancelará con el mensaje "Se ha seleccionado la opción No. Instalación cancelada."

13 Escriba el comando `exit` para cerrar la conexión SSH.

14 Repita los pasos del 6 al 11 para instalar en otro equipo Cliente para Mac.

Nota

Al instalar el Cliente para Mac por primera vez en Mac OS 10.13, el usuario debe dar permiso para cargar los controladores manualmente cuando se le solicite.

Implementación a través de ManageEngine

A continuación, se indican los pasos para implementar clientes de Endpoint Protection mediante ManageEngine.

Requisitos

- El administrador debe tener una cuenta en los equipos Cliente para Mac con privilegios de administrador.
- Habilite la Administración remota en los equipos Cliente para Mac.
- El equipo administrador debe tener instalado Packages. Packages es una aplicación del sistema operativo Mac que le ayuda a crear paquetes para su carga útil e instalación. Para descargar Packages, visite http://s.sudre.free.fr/Software/Packages/about.html.
- ManageEngine Agent debe estar instalado en el dispositivo Mac.
- El dispositivo Mac debe estar registrado en ManageEngine.
- Solo para macOS Catalina y versiones posteriores, haga lo siguiente en su sistema Mac:
  1. Abra **Preferencias del sistema**.
  2. Vaya a **Seguridad y privacidad >** pestaña **Privacidad**.
  3. Haga clic en el icono del candado e introduzca la contraseña si está bloqueado.
  4. Seleccione **Acceso completo al disco** en el panel izquierdo.

     Añada el siguiente proceso en la ruta indicada y, a continuación, seleccione los procesos en la ventana **Seguridad y Privacidad Acceso completo al disco,**

     /Library/PrivilegedHelperTools/fr.whitebox.packages/packages_dispatcher

Pasos

Siga estos pasos para crear el paquete del Cliente para Mac:

1. En Seqrite Endpoint Protection, descargue UEMREMOTEINST.TAR desde la URL.

   Nota: Este archivo tar es común para los clientes EPP Cloud y NG Mac. Contiene los archivos necesarios para crear el empaquetador del Cliente para Mac. http://dlupdate.quickheal.com/builds/seqrite/uemcp/en/UEMREMOTEINST.tar
2. Descargue el instalador del Cliente para Mac desde el servidor EPP. Estas compilaciones estarán en formato TAR.
3. Cambie el nombre del instalador del Cliente para Mac de la siguiente manera:
   - Instalador del Cliente para Mac: MCCLAGNT.TAR
4. Extraiga UEMREMOTEINST.TAR.
5. Copie MCCLAGNT.TAR en /UEMREMOTEINST.

6. Abra Terminal.app con un usuario que tenga privilegios administrativos en el equipo Mac y vaya a la carpeta UEMREMOTEINST.

   Introduzca los siguientes comandos:

   - cd ./Remote_Installation/PKG
   - sudo sh ./ClientAgentInstaller/CreatePackage.sh

   Cuando la creación del paquete se haya completado correctamente, se creará el archivo ClientAgentInstaller.pkg en la carpeta **./Remote_Installation/PKG/ClientAgentInstaller/.**

Nota: Utilice este archivo **ClientAgentInstaller.pkg** para la implementación del Cliente para Mac con ManageEngine Endpoint Central.

Implementación del perfil

Siga estos pasos para implementar el perfil con ManageEngine con el fin de cargar las extensiones del producto de forma silenciosa y proporcionar acceso completo al disco:

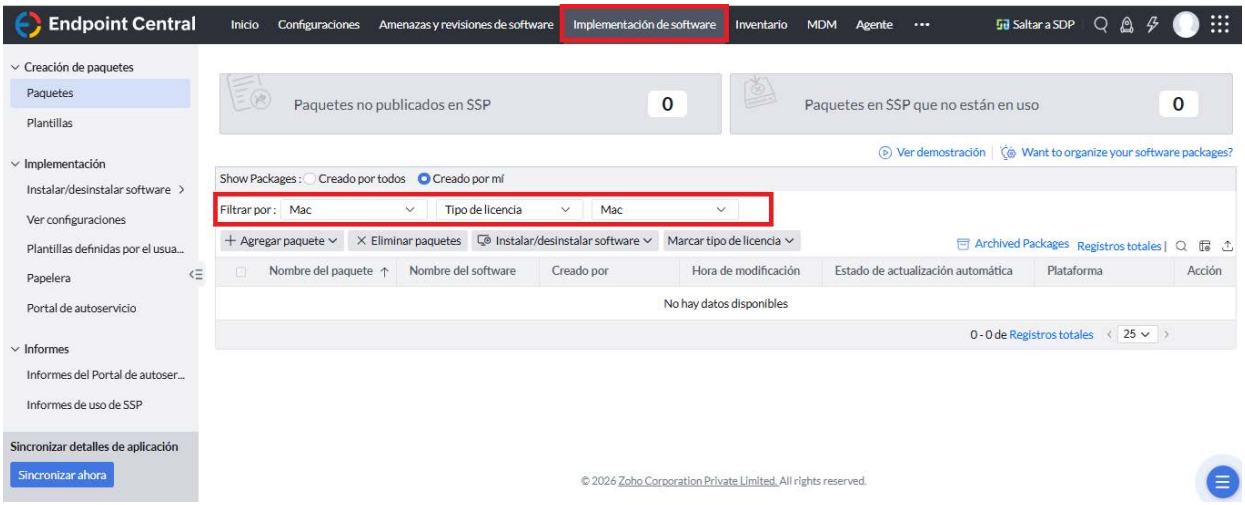
1. Inicie sesión en la Consola Central de Administración de Terminales.
2. Vaya a **Configuración** y seleccione **Mac**.
3. Seleccione **Configuración personalizada**.
4. Introduzca el nombre de la configuración personalizada.
5. Descargue el perfil desde **http://download.quickheal.com/builds/seqrite/63/en/build/SeqriteMacProfile.zip**

   Extraiga el archivo SeqriteMacProfile.zip descargado, que contendrá **SeqriteMacProfile10.13.mobileconfig**
6. Haga clic en **Examinar**. El archivo **SeqriteMacProfile10.13.mobileconfig** descargado se agregará al **Perfil de configuración personalizada**.

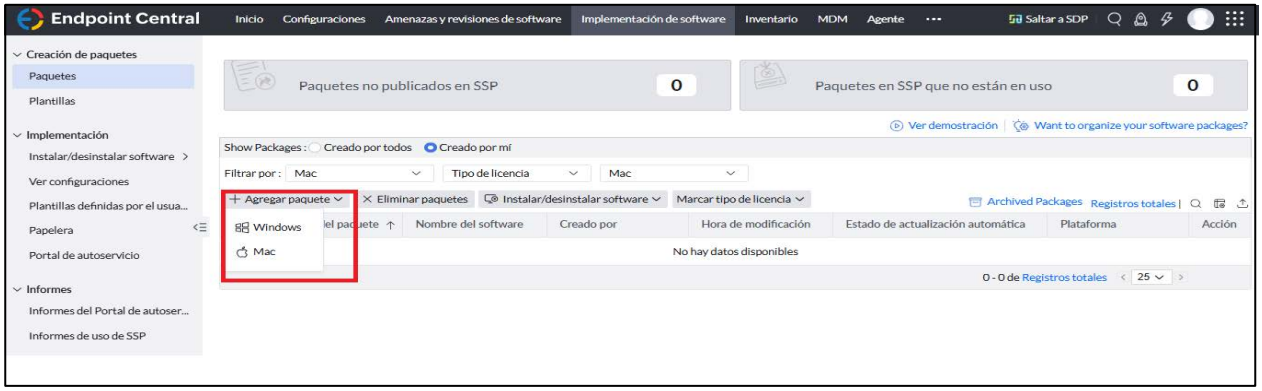
   Nota: Este perfil funcionará en macOS Big Sur y sistemas posteriores.
7. Defina el destino:
   a. Oficina remota/dominio: seleccione el nombre de dominio.
   b. Filtrar equipo según: Computadora: Seleccione el nombre del equipo Mac. (Puede encontrar el nombre del equipo Mac en > haga clic en los puntos suspensivos > haga clic en "Agente" > haga clic en el gráfico "Mac" de la plataforma del sistema operativo).
8. Haga clic en **Implementar** inmediatamente.

Implementación del Cliente para Mac con ManageEngine

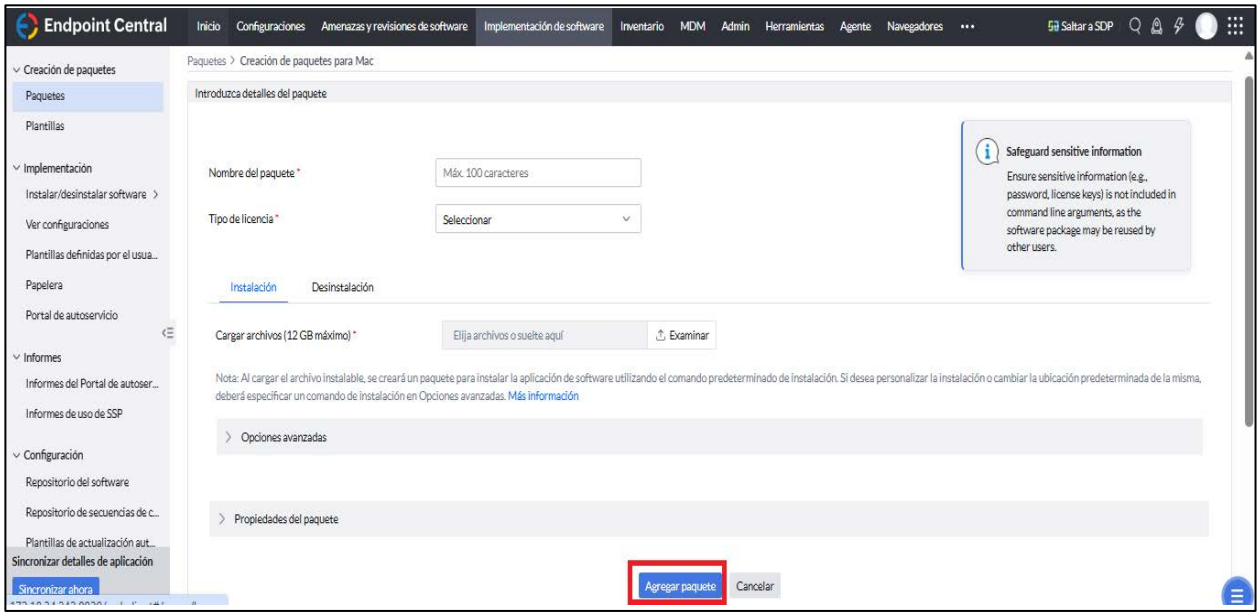
1. Inicie sesión en la Consola Central de Administración de Terminales.
2. Vaya a Implementación de software.



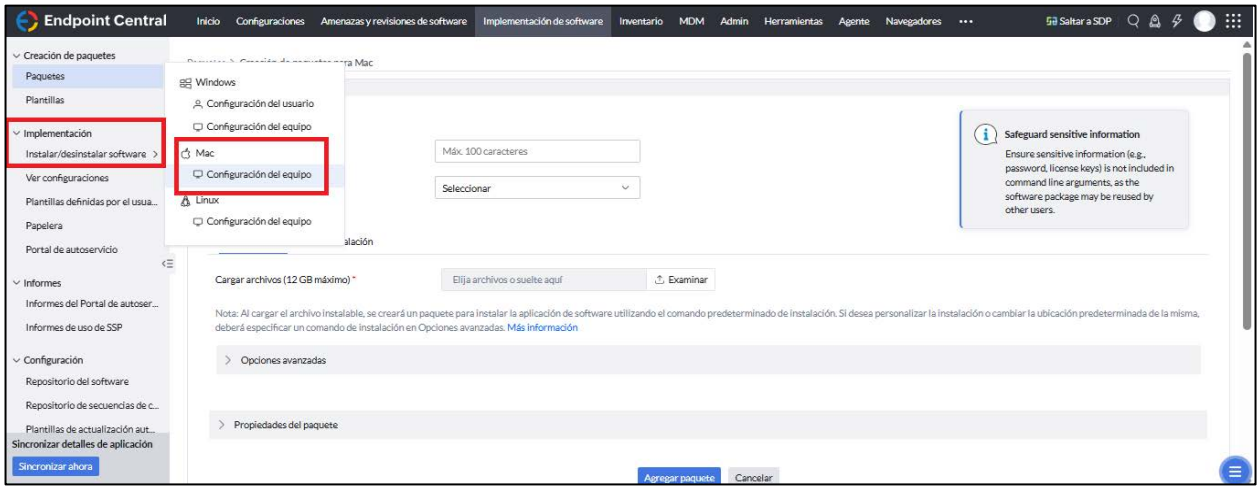
3. Haga clic en **Agregar paquete**. Seleccione Mac en los valores desplegables.



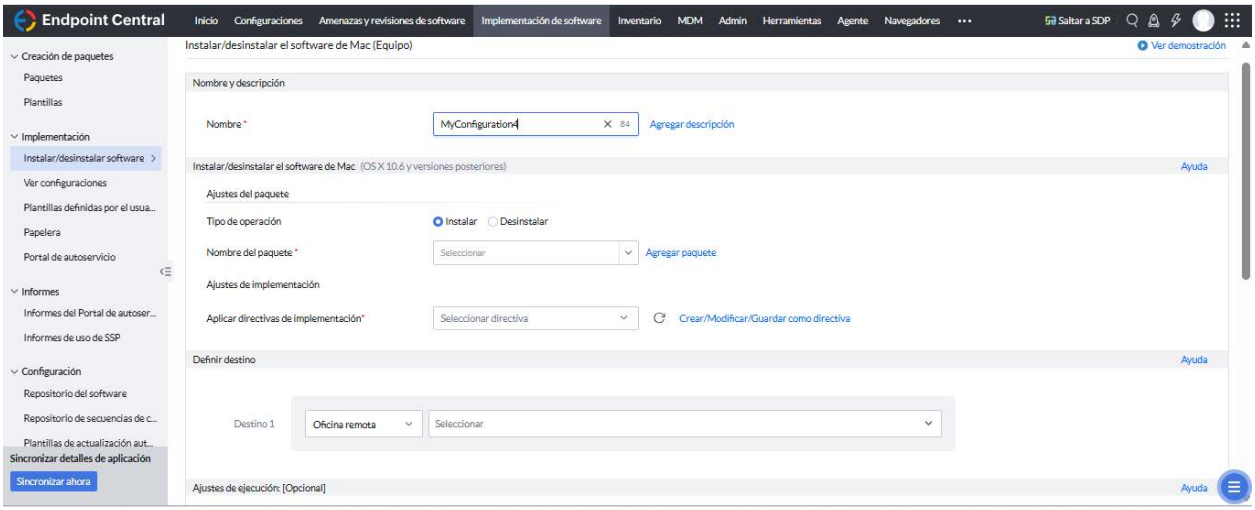
4. Introduzca el **Nombre del paquete**.



5. Seleccione **Comercial** en el menú desplegable **Tipo de licencia**.
6. Haga clic en **Examinar** para cargar el empaquetador de Mac, es decir, **ClientAgentInstaller.pkg**.
7. Haga clic en **Agregar paquete**. Se añade el empaquetador.
8. Ahora, en el panel izquierdo, vaya a Implementación > Instalar/Desinstalar software > Mac > Configuración del equipo.



9. Asigne un nombre adecuado a la configuración.



10. Seleccione Tipo de operación: **Instalar**.
11. Seleccione el nombre del paquete que introdujo anteriormente en la lista desplegable Valores del nombre del paquete.
12. Seleccione **Implementar en el momento más temprano posible** en los valores de la lista desplegable Aplicar política de implementación.
13. Defina el destino:
    a. Oficina remota/dominio: Seleccione el nombre de dominio.
    b. Filtre el equipo según: Equipo: Seleccione el nombre del equipo Mac. (Puede encontrar el nombre del equipo Mac en > haga clic en los puntos suspensivos > haga clic en "Agente" > haga clic en el gráfico "Mac" de la plataforma del sistema operativo).
14. Haga clic en **Implementar** inmediatamente.

Capítulo 2. Información sobre el Panel de control de Seqrite Endpoint Protection

Puede acceder a Seqrite Endpoint Protection desde el escritorio de cualquiera de las siguientes maneras:

- Haga clic en el icono de Seqrite en la barra de menú y seleccione Abrir Seqrite Endpoint Protection.
- Haga clic en el icono de Seqrite Endpoint Protection en el Dock, si ha agregado Seqrite Endpoint Protection a la bandeja del Dock.
- En la bandeja Doc, haga clic en Buscador y, a continuación, seleccione Aplicaciones en FAVORITOS. Haga clic en Seqrite Endpoint Protection en el panel Aplicaciones para abrir la aplicación.

Panel de control de Seqrite Endpoint Protection

Al abrir Seqrite Endpoint Protection, aparece el Panel de control. El Panel de control de Seqrite Endpoint Protection es el área principal desde la que se puede acceder a todas las funciones. El Panel de control se divide en varias secciones: menú de Seqrite Endpoint Protection, área de notificaciones de seguridad del sistema, funciones de Seqrite Endpoint Protection, noticias y la opción para analizar el equipo.

El área de notificaciones de seguridad del sistema indica si su sistema está protegido y si necesita realizar alguna acción mediante un mensaje y un icono de protección, mientras que el área de noticias muestra noticias sobre nuevos eventos, como alertas de seguridad, lanzamientos especiales de Seqrite, etc.

El área de notificaciones de seguridad del sistema proporciona información sobre el estado de seguridad de Seqrite Endpoint Protection mediante iconos de colores. A continuación, se describen los iconos de colores y su significado específico:

Iconos	Descripción
	Indica que Seqrite Endpoint Protection está configurado con los ajustes óptimos y que su sistema está protegido.
	Indica que una función de Seqrite Endpoint Protection requiere su atención, si no de forma inmediata, al menos lo antes posible.
	Indica que Seqrite Endpoint Protection no está configurado con los ajustes óptimos y su atención inmediata es necesaria. La acción correspondiente al mensaje debe ejecutarse inmediatamente con el fin de mantener su sistema protegido.

El área de notificaciones de seguridad del sistema es su interfaz instantánea para acceder a ajustes de protección vitales que pueden afectar a archivos, carpetas, correos electrónicos, etc. También permite a los usuarios configurar la protección contra virus que intentan entrar a través de Internet, unidades externas y correos electrónicos. Seqrite Protection Center se divide en dos secciones.

Funciones de Seqrite Endpoint Protection

Seqrite Endpoint Protection garantiza una protección completa contra cualquier posible amenaza o malware que pueda infectar su sistema a través de diversos medios. Seqrite Endpoint Protection protege su sistema de las siguientes maneras:

Funciones	Descripción
Seguridad para Mac	Le ayuda a configurar las preferencias de análisis, la Protección contra virus, programar análisis, excluir archivos y carpetas del análisis y establecer reglas para la cuarentena y la copia de seguridad de archivos.
Seguridad Web	Le ayuda a proteger su sistema contra amenazas maliciosas cuando navega por Internet o cuando transfiere datos a través de la red.
Seguridad de Correo	Le ayuda a proteger su sistema contra amenazas maliciosas y spam que intentan colarse en su sistema a través de correos electrónicos.

Las siguientes son funciones de uso frecuente:

Funciones	Descripción
Análisis	Inicia el escáner que analiza el equipo según las preferencias de análisis.

Menús de Seqrite Endpoint Protection

Con los menús de Seqrite Endpoint Protection, puede configurar los ajustes generales para realizar actualizaciones automáticamente, proteger con contraseña su Seqrite Endpoint Protection para que ninguna persona no autorizada pueda acceder a la aplicación Seqrite Endpoint Protection, proporcionar ajustes para la compatibilidad con proxy y eliminar informes de la lista automáticamente.

El menú de Seqrite Endpoint Protection incluye lo siguiente:

Menú	Descripción
Configuración	Le ayuda a personalizar y configurar los ajustes del Antivirus de Seqrite, tales como la Actualización automática, la Configuración de Internet, la Protección con contraseña, la Autoprotección, el Control de dispositivos y la Configuración de informes.
Informes	Le ayuda a ver los informes de actividad del Escáner, la Protección contra virus, la Protección del correo electrónico, la Actualización rápida, la Protección contra phishing, la Protección de la navegación y la Seguridad Web.

Opciones de acceso rápido

Las opciones de acceso rápido son las opciones que se utilizan para acceder a Seqrite Endpoint Protection, activar o desactivar la Protección contra virus, actualizar el producto y analizar el equipo cuando sea necesario.

Las siguientes opciones de acceso rápido estarán disponibles en el icono de la bandeja del sistema de Seqrite Endpoint Protection cuando solo Seqrite EPP esté instalado en la terminal:

Opciones	Descripción
Abrir Seqrite Endpoint Protection	Inicia Seqrite Endpoint Protection.
Habilitar / Deshabilitar Protección contra virus	Le ayuda a activar o desactivar la Protección contra virus.
Actualizar ahora	Le ayuda a actualizar Seqrite Endpoint Protection.
Analizar mi Mac	Le ayuda a analizar su equipo en busca de virus.
Sincronizar ahora	Ayuda a sincronizar la terminal de acuerdo con las directivas aplicadas.

El producto EPP, junto con las siguientes opciones de acceso rápido, está disponible en el icono de la bandeja del sistema SUA cuando Seqrite Endpoint Protection y Seqrite Universal Agent (SUA) versión 1.3.9 o superior están instalados en la terminal.

Opciones	Descripción
Abrir Seqrite Endpoint Protection	Inicia Seqrite Endpoint Protection.
Actualizar firmas	Le ayuda a actualizar Seqrite Endpoint Protection.
Solicitar Acceso temporal al dispositivo	Le ayuda a disponer de acceso temporal al dispositivo. *Tenga en cuenta que esta opción solo está visible si **Control avanzado del dispositivo** está habilitado en las directivas.*
Sincronizar directivas	*Ayuda a sincronizar el dispositivo con las directivas aplicadas.*
Actualizar firmas	Le ayuda a actualizar Seqrite Endpoint Protection.

Temas de ayuda

Los temas de ayuda le ayudan a comprender las funciones de Seqrite Endpoint Protection, cómo utilizarlas y cómo solicitar soporte técnico cuando sea necesario.

Para acceder a los temas de ayuda integrados en el escritorio, siga estos pasos:

1 Vaya a Seqrite Endpoint Protection > Menú > Ayuda > Ayuda de Seqrite Endpoint Protection.

Aparecerán los temas de ayuda.

2 Busque la información que desee.

Información sobre Seqrite Endpoint Protection

La pantalla "Información sobre Seqrite Endpoint Protection" incluye la información de la empresa con la que está registrado Seqrite Endpoint Protection.

Para acceder a la pantalla "Información sobre Seqrite Endpoint Protection", siga estos pasos:

- Vaya a Seqrite Endpoint Protection > Menú > Seqrite Endpoint Protection > Información sobre Seqrite Endpoint Protection.

  Aparecerá la pantalla "Información".

La pantalla "Información" incluye la siguiente información sobre la licencia:

- *Información sobre la licencia de Seqrite Endpoint Protection*: Nombre de la organización y Fecha de la base de datos de virus.
- *Datos del servidor:* Después de hacer clic en el botón "Datos del servidor", verá la siguiente información sobre el Servidor de Seqrite Endpoint Protection, incluido el grupo y la directiva asociados con el cliente y el estado de la conexión de red entre el cliente y el servidor.
    - Servidor: La dirección IP o el nombre de dominio del Servidor de Seqrite Endpoint Protection.
    - Grupo: El grupo de Seqrite Endpoint Protection asociado al cliente.
    - Directiva: La directiva de Seqrite Endpoint Protection aplicada al cliente.
    - Estado de la conexión: Indica si la conexión está activa o inactiva.
    - Última conexión: La última vez que se estableció correctamente la conexión.
    - Mensaje de error: Proporciona detalles sobre cualquier problema encontrado durante la conexión. Si no hay ningún problema, aparecerá "Sin errores".

- *Actualizar ahora:* Este botón le ayuda a actualizar Seqrite Endpoint Protection.

Actualización con archivos de definición

Si ya dispone del archivo de definición de actualización, puede actualizar Seqrite Endpoint Protection sin conectarse a Internet. Esto resulta especialmente útil para entornos de red con más de un equipo. No es necesario descargar el archivo de actualización de Internet en todos los equipos de la red que utilizan Seqrite.

1 Vaya a **Seqrite Endpoint Protection > Menú > Seqrite Endpoint Protection > Buscar actualizaciones**.

2 En la pantalla Bienvenido a la actualización de Endpoint Protection, haga clic en **Continuar**.

Aparecerá la pantalla *Seleccione el modo que prefiera para actualizar Endpoint Protection.*

3 Seleccione ***Elegir desde una ubicación específica***.

4 Escriba la ruta o haga clic en el botón **Archivo** para seleccionar la ubicación del archivo y, a continuación, haga clic en **Continuar**.

Nota

La actualización rápida toma el archivo de definición de la ruta designada, verifica su aplicabilidad en la versión instalada y actualiza su copia de Seqrite Endpoint Protection en consecuencia.

Capítulo 3. Funciones de Seqrite Endpoint Protection

Las funciones de Seqrite Endpoint Protection incluyen las características más importantes que le ayudan a configurar las preferencias de análisis, las reglas de protección para su equipo, la programación del análisis, las reglas de Cuarentena y Copia de seguridad de archivos, la aplicación de protecciones para la navegación en línea, la Seguridad Web y el bloqueo de correos electrónicos maliciosos y spam.

Estas funciones proporcionan una protección óptima a su sistema. Además, deben mantenerse activadas en todo momento. Si las desactiva por cualquier motivo, los iconos correspondientes se volverán rojos.

Seguridad para Mac

La opción Seguridad para Mac del Panel de control le permite personalizar los ajustes relacionados con la protección de archivos y carpetas en su sistema. Con Seguridad para Mac, puede configurar las preferencias de análisis, aplicar reglas para la protección contra virus, programar análisis, excluir archivos y carpetas del análisis y establecer reglas para la cuarentena y el respaldo de archivos.

Seguridad para Mac incluye lo siguiente:

Configuración del análisis

Con la Configuración del análisis, puede personalizar la forma en que se realiza un análisis y la acción que se debe tomar cuando se detecta un virus. Sin embargo, la configuración predeterminada es óptima y puede proporcionar la protección necesaria a su equipo.

Para configurar el análisis, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

Aparecerá la pantalla de datos de la configuración de Seguridad para Mac.

2 Haga clic en **Configuración del análisis**.

3 Establezca la opción adecuada para el tipo de análisis, la acción que se debe realizar si se encuentra un virus en los archivos y si desea realizar una copia de seguridad de la configuración anterior.

4 Haga clic en **Guardar** para guardar la configuración.

Seleccionar tipo de análisis

- *Automático (recomendado)*: El tipo de análisis automático es el modo de análisis predeterminado, que se recomienda ya que garantiza la protección óptima que requiere su equipo. Esta configuración también es una opción ideal para usuarios novatos.
- *Avanzado*: Seleccione el modo Avanzado si desea personalizar el comportamiento del análisis. Esto es ideal solo para usuarios experimentados. Cuando selecciona la opción Avanzado, se habilita el botón **Configurar** y puede configurar los ajustes avanzados para el análisis.

Acción que se debe tomar cuando se encuentra un virus

La acción que seleccione aquí se llevará a cabo automáticamente si se encuentra un virus, por lo que debe seleccionarla con cuidado. Las acciones y sus descripciones son las siguientes:

Acciones	Descripción
Reparar	Si durante el análisis se detecta un virus, repara el archivo o lo pone automáticamente cuarentena si no se puede reparar. Cuando finaliza el análisis, aparece una ventana de resumen con los datos de todas las acciones realizadas y otros detalles del análisis. Si el archivo infectado es una backdoor (puerta trasera), un gusano, un troyano o un malware, Seqrite Endpoint Protection lo elimina automáticamente.
Eliminar	Elimina un archivo infectado por virus sin avisarle. Cuando finaliza el análisis, aparece una ventana de resumen con los datos de todas las acciones realizadas y otros detalles del análisis. Una vez eliminados los archivos, no se pueden recuperar.
Omitir	Si se selecciona esta opción, los archivos se analizan, pero no se realiza ninguna acción sobre los archivos infectados y se omiten. Seleccione esta opción si no desea realizar ninguna acción aunque se encuentre un virus. Cuando finaliza el análisis, aparece un informe resumido con todos los datos del análisis.
Realizar copia de seguridad antes de tomar medidas	El escáner guarda una copia de seguridad de los archivos infectados antes de desinfectarlos. Los archivos almacenados en la copia de seguridad se pueden restaurar desde el menú Cuarentena.

Configuración del tipo de análisis avanzado

Para configurar el tipo de análisis avanzado, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

Aparecerá la pantalla de datos de la configuración de Seguridad para Mac.

2 Haga clic en **Configuración de análisis**.

3 En Tipo de análisis, seleccione **Avanzado**.

El botón "Configurar" estará habilitado.

4 Haga clic en **Configurar**.

Aparecerá la pantalla de datos de configuración del Análisis avanzado.

5 Marque *los elementos que desea analizar* en busca de malware basado en Windows.

Esta opción está seleccionada de forma predeterminada.

6 Seleccione uno de los siguientes elementos para el análisis:

- *Analizar archivos ejecutables*: Seleccione esta opción si desea analizar solo los archivos ejecutables.
- *Analizar todos los archivos*: Seleccione esta opción si desea analizar todos los tipos de archivos. Sin embargo, la ejecución de esta opción lleva tiempo y el proceso de análisis se ralentiza considerablemente.

7 Active la opción *Analizar archivos archivados* y, a continuación, configure las preferencias de análisis para los archivos comprimidos, como archivos zip, etc.

8 Para cerrar la pantalla Archivos comprimidos, haga clic en "Aceptar". Para cerrar la configuración del Análisis avanzado, haga clic en "Aceptar" y, a continuación, haga clic en "Guardar" para guardar la configuración.

Analizar archivos comprimidos

Si selecciona *Analizar archivos comprimidos*, el escáner también analizará archivos comprimidos, como archivos zip, archivos de archivo, etc. Si selecciona *Analizar archivos comprimidos*, el botón Configurar se habilita y le ayuda a configurar la forma en que el escáner debe tratar los archivos comprimidos maliciosos. Puede analizar archivos de varios tipos de archivos comprimidos hasta cinco niveles de profundidad para asegurarse de que no quede ningún archivo sin analizar.

A continuación, se indican las acciones que puede seleccionar para que se lleven a cabo cuando se detecte un virus en cualquiera de los archivos comprimidos:

Acciones	Descripción
Poner en cuarentena	Seleccione esta opción si desea poner en cuarentena un archivo comprimido que contiene un virus.
Eliminar	Seleccione esta opción si desea eliminar un archivo comprimido que contenga archivos infectados con virus. Sin embargo, no se le notificará si se elimina un archivo, aunque se generará un informe que podrá ver en la lista Informes.
Omitir	Seleccione esta opción si no desea realizar ninguna acción aunque se encuentre un virus en alguno de los archivos comprimidos. Sin embargo, esta opción está seleccionada de forma predeterminada.

Nivel de análisis del archivo

Establezca el nivel de análisis hasta el que desea explorar los archivos comprimidos. Puede establecer hasta cinco niveles dentro de los archivos comprimidos. De forma predeterminada, el análisis está establecida en el nivel 2. Sin embargo, puede aumentar el nivel de exploración de los archivos comprimidos, lo que puede afectar a la velocidad de exploración.

Seleccione el tipo de archivo que desea analizar

Puede seleccionar los tipos de archivos comprimidos que desea analizar en la lista de archivos comprimidos. Algunos de los tipos de archivos comprimidos más comunes están seleccionados de forma predeterminada. Sin embargo, puede cambiar la configuración de acuerdo con sus preferencias.

Tipos	Descripción
Seleccionar todo	Seleccione esta opción para seleccionar todos los tipos de archivos disponibles en la lista.
Deseleccionar todo	Seleccione esta opción para desmarcar todos los tipos de archivo disponibles en la lista.

- Cuando finaliza el análisis, aparece un informe resumido con los datos de todas las acciones realizadas y otros detalles del análisis, independientemente de la opción que haya configurado.
- Las notificaciones de funciones como Análisis, Actualización y Desinstalación remota desde la consola web de Seqrite EPP no se enviarán a los usuarios si no han iniciado sesión en Mac.
- En el caso del análisis programado, si el sistema está apagado en el momento del análisis programado, este no se ejecutará cuando se inicie el sistema.

- En cuanto a la directiva del programador, si se habilita el análisis repetido, el primer análisis se ejecutará a la hora de inicio programada + horas de repetición.

Nota: Cuando la Protección de integridad del sistema (SIP, System Integrity Protection) está habilitada en macOS, el Análisis completo del sistema y el Análisis programado solo abarcarán las carpetas que no estén protegidas por SIP. Por el contrario, si SIP está deshabilitado en macOS, el análisis abarcará todas las carpetas.

Protección contra virus

Con la Protección contra virus, puede supervisar continuamente su equipo para detectar virus, malware y otras amenazas maliciosas. Estas amenazas intentan colarse en su equipo desde diversas fuentes, como archivos adjuntos de correo electrónico, descargas de Internet, transferencias de archivos, ejecución de archivos, etc.

Se recomienda mantener siempre activada la Protección contra virus para mantener su equipo limpio y protegido frente a posibles amenazas. Sin embargo, la Protección contra virus está activada de forma predeterminada, pero puede desactivarla si lo desea.

Para configurar la Protección contra virus, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

Aparecerá la pantalla de detalles de la configuración de Seguridad para Mac.

2 Para proteger su equipo de amenazas maliciosas, active la Protección contra virus.

3 Paraconfigurar la Protección contra virus, haga clic en **Protección contra virus**.

4 En la pantalla Protección contra virus, haga lo siguiente:

- *Elementos que se van a analizar*: Seleccione esta casilla si desea analizar el malware basado en Windows. Sin embargo, esta casilla está seleccionada de forma predeterminada.
- *Analizar volumen de red*: Seleccione esta opción si desea analizar los volúmenes de red que están montados en su equipo. Sin embargo, esta opción está activada de forma predeterminada.
- *Mostrar notificaciones*: Seleccione SÍ si está seleccionada la opción Mostrar notificaciones, que muestra un mensaje de alerta cada vez que se detecta un malware. Esta función está seleccionada de forma predeterminada.
    - Si se encuentra un virus: Seleccione una acción que se llevará a cabo cuando se encuentre un virus en un archivo, como Reparar, Eliminar y Denegar acceso.
    - Hacer una copia de seguridad antes de realizar una acción: Seleccione esta opción si desea hacer una copia de seguridad de un archivo antes de realizar una acción sobre el archivo. Los archivos almacenados en la copia de seguridad se pueden restaurar desde el menú Cuarentena.

5 Para guardar la configuración, haga clic en **Guardar**.

Acción que se debe realizar cuando se detecta un virus

Acciones	Descripción
Reparar	Durante el análisis, si se encuentra un virus, repara el archivo o lo pone automáticamente en cuarentena, si no se puede reparar.
Eliminar	Elimina un archivo infectado por un virus sin avisarle.
Denegar acceso	Restringe el acceso a un archivo infectado por un virus para impedir su uso.

Desactivar la Protección contra virus

Desactiva la Protección contra virus. Sin embargo, cuando intentas desactivar la Protección contra virus, se muestra un mensaje de alerta. Se recomienda desactivar la Protección contra virus solo cuando sea realmente necesario.
Además, puede desactivarla durante un periodo de tiempo determinado para que se active automáticamente después.

A continuación, se indican las opciones para desactivar la Protección contra virus durante un periodo determinado:

- Activar después de 15 minutos
- Activar después de 30 minutos
- Activar después de 1 hora
- Activar después del próximo reinicio
- Desactivar permanentemente

Seleccione una opción y haga clic en **Aceptar**.

Una vez que desactiva la Protección contra virus, el color del icono cambia de verde a rojo en la bandeja de la barra de menú, lo que significa que la Protección contra virus se desactivó de forma temporal o permanente, según su selección. Si seleccionó alguna de las opciones para desactivarla temporalmente o después del siguiente arranque, el color del icono volverá a cambiar de rojo a verde una vez transcurrido un determinado tiempo o en el siguiente arranque. Si seleccionó desactivarla de forma permanente, el color del icono permanecerá rojo hasta que active la Protección contra virus manualmente.

Análisis programados

Con la función Programar análisis, puede definir la hora a la que desea que se inicie automáticamente el análisis de su equipo. Puede programar varios análisis para poder iniciar el análisis de su equipo cuando le resulte más conveniente. La frecuencia se puede configurar para análisis diarios y semanales, lo que le permite refinar aún más su solicitud para programarlo de forma que se ejecute al iniciar el equipo a una hora determinada.

Configuración de los Análisis programados

Para configurar los Análisis programados, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

2 En la pantalla de configuración de Seguridad para Mac, haga clic en **Programar análisis**.

Aparecerá la pantalla de datos de los Análisis programados. Aquí verá una lista de todas las programaciones de análisis, si ha definido alguna anteriormente.

3 Para crear una nueva programación de análisis, haga clic en **Agregar**.

Aparecerá la pantalla Agregar análisis programado, donde podrá crear un nuevo nombre para la programación de los análisis, su frecuencia y otros datos.

4 En el cuadro de texto Nombre del análisis, escriba un nombre para la programación del análisis.

5 Establezca la Frecuencia del análisis:

- *Diario*: Seleccione la opción Diario si desea iniciar el análisis de su equipo a diario. Sin embargo, esta opción está seleccionada de forma predeterminada.
- *Semanal*: Seleccione la opción Semanal si desea iniciar el análisis de su equipo en un día concreto de la semana. Al seleccionar la opción Semanal, se habilita la lista Semanal, donde puede seleccionar un día de la semana.

6 Establezca la Hora de análisis:

- *Iniciar análisis al primer arranque*: Seleccione la opción *Iniciar análisis al primer arranque* para programar el análisis al primer arranque del sistema ese día. Al seleccionar Iniciar al primer arranque, no es necesario especificar la hora del día en que se iniciará el análisis. El análisis solo se realizará durante el primer arranque, independientemente de la hora a la que se inicie el sistema.
- *Iniciar análisis a una hora fija*: Seleccione la opción *Iniciar análisis a una hora fija* si desea iniciar el análisis de su máquina a una hora determinada. Cuando selecciona Hora fija, se habilita la lista Hora de inicio, donde puede fijar la hora para el análisis. Sin embargo, esta opción está seleccionada de forma predeterminada.

7 Establecer prioridad de análisis.

- *Alta*: seleccione la opción Alta si desea que la prioridad del análisis sea alta.
- *Baja*: Seleccione la opción Baja si desea que la prioridad de análisis sea baja. Sin embargo, esta opción está seleccionada de forma predeterminada.

8 Ubicación del análisis:

- Haga clic en Configurar para abrir la pantalla Ubicación de análisis, donde puede seleccionar los archivos y carpetas que desea analizar. Puede establecer varias ubicaciones. Seleccione las unidades, carpetas o varias carpetas que desea analizar y pulse Aceptar. Puede configurar Excluir subcarpeta al analizar una carpeta específica. Esto omitirá el análisis dentro de las subcarpetas durante el análisis.

9 Configuración del análisis:

- Haga clic en Configurar para abrir la pantalla Configuración de análisis. En Configuración de análisis, puede especificar los elementos concretos que se van a analizar, las medidas que se deben tomar si se encuentra un virus y el uso de las opciones avanzadas durante el análisis. La configuración predeterminada establece las opciones adecuadas para el análisis.
    - En Tipo de análisis, seleccione una de las opciones: Automático y Avanzado. Para obtener información sobre cómo configurar el análisis, consulte Configuración del análisis, pág. 37.
    - Seleccione SÍ si desea realizar una copia de seguridad de los archivos antes de realizar cualquier acción sobre ellos. De lo contrario, seleccione NO si no desea realizar ninguna copia de seguridad de los archivos. Esta opción está seleccionada de forma predeterminada.

10 Para guardar la configuración, haga clic en **Guardar**.

Edición de Análisis programados

Puede modificar cualquiera de los análisis programados cuando lo necesite. Para editar un análisis programado, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

2 En la pantalla de configuración de Seguridad para Mac, haga clic en **Programar análisis**.
Aparecerá una lista con todas las programaciones de análisis.

3 Seleccione una programación de análisis y haga clic en **Editar**.

4 En la pantalla Agregar Análisis programado, cambie la programación del análisis según sea necesario.

5 Para guardar la configuración, haga clic en **Guardar** y, a continuación, en **Cerrar**.

Eliminación de Análisis programados

Si no necesita la programación de un análisis, puede eliminarla cuando lo desee. Para eliminar la programación de un análisis, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

2 En la pantalla de configuración de Seguridad para Mac, haga clic en **Programar análisis**.

Aparecerá una lista con todas las programaciones de análisis.

3 Seleccione una programación de análisis y haga clic en **Eliminar**.

4 Haga clic en **SÍ** para confirmar que desea eliminar la programación de análisis y, a continuación, haga clic en **Cerrar**.

Excluir archivos y carpetas

Con Excluir archivos y carpetas, puede decidir qué archivos y carpetas no deben incluirse durante el análisis en busca de virus o problemas conocidos. Esto le ayuda a evitar la repetición innecesaria del análisis de los archivos que ya se analizaron o que está seguro de que no deben analizarse. Puede excluir archivos del análisis desde los dos módulos de análisis: Escáner de Seguridad para Mac y Protección contra virus.

El Escáner de Endpoint Protection analiza los archivos y carpetas cuando se realiza un análisis manual, mientras que la Protección contra virus analiza cada archivo y carpeta automáticamente cuando se accede a ellos.

Configuración de Excluir archivos y carpetas

Para configurar la exclusión de archivos y carpetas, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

2 En la pantalla de configuración de Seguridad para Mac, haga clic en **Excluir archivos y carpetas**.

Aparecerá la pantalla de datos para Excluir archivos y carpetas. Aquí verá una lista de los archivos y carpetas que se excluirán del análisis, si ha añadido alguno.

3 Haga clic en **Agregar**.

4 En la pantalla Nuevo elemento excluido, haga clic en el botón **Archivo o Carpeta** para agregar el archivo o la carpeta correspondiente a la lista.

Cuando añada una carpeta, puede marcar Excluir subcarpetas para que las subcarpetas también se excluyan del análisis.

5 Seleccione un archivo o carpeta y, a continuación, haga clic en **Abrir** para agregar el archivo o carpeta seleccionado y, a continuación, haga clic en **Guardar** para guardar la configuración.

6 Para cerrar la pantalla Excluir archivos y carpetas, haga clic en **Cerrar**.

Edición de Excluir archivos y carpetas

Si lo necesita, puede cambiar la configuración de Excluir archivos y carpetas de las siguientes maneras:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.
2. En la pantalla de configuración de Seguridad para Mac, haga clic en **Excluir archivos y carpetas**.

Aparecerá la pantalla de datos Excluir archivos y carpetas. Aquí verá una lista de los archivos y carpetas que agregó para excluir del análisis.

3. En Ubicación, seleccione un archivo o carpeta y, a continuación, haga clic en **Editar**.
4. En la pantalla Nuevo elemento excluido, haga clic en el botón **Archivo o Carpeta** para agregar otro archivo o carpeta a la lista.

Cuando agregue una carpeta, puedes marcar la casilla Excluir subcarpetas para que las subcarpetas también queden excluidas del análisis.

5. Seleccione un archivo o carpeta y, a continuación, haga clic en **Abrir** para agregar el archivo o carpeta seleccionado y, a continuación, haga clic en **Guardar** para guardar la configuración.
6. Para cerrar la pantalla **Excluir archivos y carpetas**, haga clic en **Cerrar**.

Eliminar archivos y carpetas excluidos

Si lo necesita, puede eliminar cualquier archivo o carpeta que haya incluido en la lista Excluir archivos y carpetas de las siguientes maneras:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.
2. En la pantalla de configuración de Seguridad para Mac, haga clic en **Excluir archivos y carpetas**.

Aparecerá la pantalla de datos de Excluir archivos y carpetas. Aquí verá una lista de los archivos y carpetas que agregó para excluir del análisis.

3. En Ubicación, seleccione un archivo o carpeta y, a continuación, haga clic en **Eliminar**. Puede eliminar todos los archivos y carpetas de la lista haciendo clic en **Eliminar todo**.

Los archivos o carpetas seleccionados se eliminarán de la lista de exclusión.

4. Para cerrar la pantalla Excluir archivos y carpetas, haga clic en **Cerrar**.

Cuarentena y Copia de seguridad

La Cuarentena y la Copia de seguridad ayudan a aislar de forma segura los archivos infectados o sospechosos. Cuando se agrega un archivo a la Cuarentena, Seqrite Endpoint Protection lo cifra y lo mantiene dentro de la carpeta de Cuarentena. Al estar cifrados, estos archivos no se pueden ejecutar y, por lo tanto, son seguros. La Cuarentena también guarda una copia del archivo infectado antes de repararlo si se selecciona la opción Copia de seguridad antes de reparar en la Configuración del escáner.

Con Cuarentena y Copia de seguridad, también puede establecer una regla para eliminar los archivos después de un período de tiempo determinado y tener una copia de seguridad de los mismos.

Configuración de Cuarentena y Copia de seguridad

Para configurar la Cuarentena y la Copia de seguridad, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad para Mac**.

2 En la pantalla de configuración de Seguridad para Mac, haga clic en **Cuarentena y Copia de seguridad**.

3 En "Eliminar archivos automáticamente después de", arrastre el control deslizante para seleccionar los días tras los cuales los archivos se eliminarán automáticamente de la carpeta Cuarentena.

> Configurar esta función ayuda a eliminar los archivos en Cuarentena/Copias de seguridad tras el periodo de tiempo configurado. La eliminación de archivos está configurada de forma predeterminada en 30 días.

4 Haga clic en **Ver archivos** para ver los archivos en Cuarentena. Puede realizar cualquiera de las siguientes acciones con los archivos en cuarentena:

- *Agregar archivo*: Puede agregar archivos de carpetas y unidades para ponerlos en cuarentena manualmente.
- *Restaurar seleccionados*: Puede restaurar los archivos seleccionados manualmente si es necesario.
- *Enviar seleccionados*: Puede enviar los archivos sospechosos al laboratorio de investigación de Seqrite para su análisis posterior desde la lista de cuarentena. Seleccione el archivo que desea enviar y haga clic en **Enviar**.
- *Eliminar seleccionados*: Puede eliminar los archivos seleccionados de la lista de Cuarentena.
- *Eliminar todo*: Puede eliminar todos los archivos en cuarentena de la lista de Cuarentena.
- Funcionalidad de Enviar archivo en cuarentena.

  En Cuarentena, cuando selecciona un archivo y hace clic en el botón **Enviar**, aparece un mensaje solicitando permiso para proporcionar su dirección de correo electrónico. También debe proporcionar un motivo para enviar los archivos. Seleccione uno de los siguientes motivos:

  - *Archivo sospechoso*: Seleccione este motivo si cree que un archivo concreto de su sistema ha sido el causante de una actividad sospechosa en el sistema.
  - *Archivo irreparable*: Seleccione este motivo si Seqrite pudo detectar el archivo malicioso en su sistema durante sus análisis, pero no pudo reparar la infección del archivo.
  - *Falso positivo*: Seleccione este motivo si Seqrite detectó como archivo malicioso un archivo de datos no malicioso que usted ha estado utilizando y cuya función conoce.

Seguridad Web

Con Seguridad Web, puede establecer reglas de protección para proteger su equipo de archivos maliciosos que pueden colarse en su sistema durante actividades en línea, como operaciones bancarias, compras, navegación, etc.

Seguridad Web incluye lo siguiente:

Protección de navegación

Con la Protección de navegación, puede bloquear sitios web maliciosos mientras navega para no entrar en contacto con ellos y estar seguro. Sin embargo, la Protección de navegación está habilitada de forma predeterminada.

Configuración de la Protección de navegación

Para configurar la Protección de navegación, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad Web**.
2. Habilite la Protección de navegación.

Puede deshabilitar la Protección de navegación cuando lo desee.

Protección contra phishing

Con la Protección contra phishing, también conocida como Protección contra suplantación de identidad, puede impedir el acceso a sitios web fraudulentos y de phishing. El phishing es un intento fraudulento, normalmente realizado a través del correo electrónico, que busca robar su información personal. Por lo general, parece provenir de organizaciones y sitios conocidos, como bancos, empresas y servicios con los que ni siquiera tiene una cuenta, y le pide que visite sus sitios web para que proporcione su información personal, como el número de la tarjeta de crédito, el número de la seguridad social, el número de cuenta o la contraseña.

La Protección contra phishing analiza automáticamente todas las páginas web a las que se accede en busca de actividades fraudulentas, protegiéndole contra cualquier ataque de phishing mientras navega por Internet. También evita el robo de identidad bloqueando los sitios web de phishing, para que pueda realizar compras en línea, operaciones bancarias y navegar por Internet de forma segura.

Configuración de la Protección contra phishing

Para configurar la Protección contra phishing, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad Web**.
2. Habilite la Protección contra phishing.

Puede deshabilitar la Protección contra phishing cuando lo desee. Sin embargo, se recomienda mantener siempre activada la Protección contra phishing.

Seguridad de correo electrónico

Con Seguridad de correo electrónico, puede personalizar las reglas de protección para recibir correos electrónicos de diversas fuentes. Puede establecer reglas para bloquear los correos electrónicos sospechosos de ser spam o malware.

Seguridad de correo electrónico incluye lo siguiente.

Protección de correo electrónico

Con la Protección de correo electrónico, puede habilitar reglas de protección para todos los correos electrónicos entrantes. Puede bloquear los archivos adjuntos infectados en los correos electrónicos que puedan ser sospechosos de contener malware, spam y virus. También puede personalizar la acción que se debe realizar cuando se detecta malware en los correos electrónicos.

Sin embargo, la Protección del correo electrónico está habilitada de forma predeterminada y la configuración predeterminada proporciona la protección necesaria al buzón contra correos electrónicos maliciosos. Le recomendamos que mantenga siempre habilitada la Protección del correo electrónico para garantizar la protección del correo electrónico.

Configuración de la Protección del correo electrónico

Para configurar la Protección del correo electrónico, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad de correo electrónico**.
2. En la pantalla de configuración de Seguridad de correo electrónico, habilite la Protección del correo electrónico.

La Protección contra el malware que llega a través del correo electrónico está habilitada.

3. Para configurar más reglas de protección para los correos electrónicos, haga clic en Protección de correo electrónico.
4. Active la opción *Notificar en el correo electrónico* si desea recibir un mensaje de alerta cuando se detecte un virus en un correo electrónico o en un archivo adjunto.

> El mensaje de alerta sobre el virus incluye la siguiente información: Nombre del virus, Dirección de correo electrónico del remitente, Asunto del correo electrónico, Nombre del archivo adjunto y Acción realizada.

5. Seleccione una de las siguientes acciones que se tomarán si se encuentra un virus.
   - *Reparar*: Seleccione Reparar para reparar sus correos electrónicos o archivos adjuntos cuando se detecte un virus.
   - *Eliminar*: Seleccione Eliminar para eliminar los correos electrónicos y archivos adjuntos infectados.

> Si el archivo adjunto no se puede reparar, se eliminará.

6. Cambie la opción *Copia de seguridad antes de actuar* a SÍ si desea una copia de seguridad de los correos electrónicos antes de realizar cualquier acción sobre ellos.

Puede volver a la configuración predeterminada en cualquier momento haciendo clic en Establecer valores predeterminados.

7. Para guardar la configuración, haga clic en **Guardar**.

Protección contra spam

Con la Protección contra spam*, puede bloquear todos los correos electrónicos no deseados, como spam, phishing y pornografía, para que no lleguen a su buzón. La Protección contra spam está habilitada de forma predeterminada y le recomendamos que mantenga siempre esta función habilitada.

Configuración de la Protección contra spam

Para configurar la Protección contra spam, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Seguridad de correo electrónico**.
2. En la pantalla de configuración de Seguridad de correo electrónico, active la Protección contra spam.
3. Para configurar más reglas de protección contra el spam, haga clic en Protección contra spam.
4. Active la opción *Etiquetar asunto con texto* para incluir la etiqueta "spam" en los correos electrónicos sospechosos.
5. Seleccione una de las siguientes opciones:
   - Active Lista blanca si desea permitir que los correos electrónicos de las direcciones incluidas en la lista blanca omitan el filtro de protección contra el spam y, a continuación, haga clic en **Configurar** para introducir las direcciones de correo electrónico.

- Active la Lista negra si desea filtrar los correos electrónicos de las direcciones de correo electrónico incluidas en la lista negra y, a continuación, haga clic en **Configurar** para introducir las direcciones de correo electrónico.

6 Haga clic en **Aceptar**.

7 Para guardar la configuración, haga clic en **Guardar**.

Configuración de la regla de protección contra el spam para la Lista blanca

La Lista blanca es la lista de direcciones de correo electrónico desde las que se permite que todos los correos electrónicos pasen por alto el filtro de protección contra el spam, independientemente de su contenido. Ningún correo electrónico procedente de las direcciones que figuran en esta lista pasa por el filtro de SPAM. Se recomienda que configure únicamente aquellas direcciones de correo electrónico en las que confíe plenamente.

Para agregar direcciones de correo electrónico a la lista blanca, siga estos pasos:

1 Active la Lista blanca.

El botón Configurar estará habilitado.

2 Haga clic en **Configurar**.

3 Introduzca las direcciones de correo electrónico en la lista y haga clic en **Agregar**.

Editar o eliminar correo electrónico: para editar una dirección de correo electrónico, seleccione la dirección de correo electrónico en la lista y haga clic en Editar. Para eliminar una dirección de correo electrónico, seleccione una dirección de correo electrónico y haga clic en Eliminar.

Importar Lista blanca: puede importar la lista blanca haciendo clic en Importar. Esto resulta muy útil si tiene una lista larga de direcciones de correo electrónico que agregar.

Exportar Lista blanca: puede exportar la lista blanca haciendo clic en Exportar. Esto exporta todas las direcciones de correo electrónico existentes en la lista. Esto resulta útil si desea importar las mismas direcciones de correo electrónico más adelante. Simplemente puede importar la lista de direcciones de correo electrónico.

4 Para guardar la configuración, haga clic en **Aceptar**.

Configuración de la regla de protección contra el spam para la Lista negra

La Lista negra es la lista de direcciones de correo electrónico desde las que se filtran todos los correos electrónicos, independientemente de su contenido. Todos los correos electrónicos procedentes de las direcciones que figuran en esta lista se etiquetan como "[SPAM] –". Esta función debe activarse específicamente en caso de que algún servidor tenga un Relay abierto que esté siendo utilizado indebidamente por Programas de Envío Masivo de Correos Electrónicos y Virus.

Para agregar direcciones de correo electrónico a la Lista negra, siga estos pasos:

1 Active la Lista negra.

El botón Configurar estará habilitado.

2 Haga clic en **Configurar**.

3 Introduzca las direcciones de correo electrónico en la lista y haga clic en **Agregar**.

Importante: Al introducir una dirección de correo electrónico, tenga cuidado de no introducir en la lista negra la misma dirección que introdujo en la lista blanca, ya que de lo contrario aparecerá un mensaje.

Editar o eliminar correo electrónico: Para editar una dirección de correo electrónico, seleccione la dirección de correo electrónico en la lista y haga clic en Editar. Para eliminar una dirección de correo electrónico, seleccione una dirección de correo electrónico y haga clic en Eliminar.

Importar Lista negra: Puede importar la Lista negra haciendo clic en Importar. Esto resulta muy útil si tiene una lista larga de direcciones de correo electrónico que agregar.

Exportar Lista negra: Puede exportar la Lista negra haciendo clic en Exportar. Esto exporta todas las direcciones de correo electrónico existentes en la lista. Esto es útil si desea importar las mismas direcciones de correo electrónico más adelante. Simplemente puede importar la lista de direcciones de correo electrónico.

4 Para guardar la configuración, haga clic en **Aceptar**.

Agregar dominios a la Lista blanca o a la Lista negra

Para agregar un dominio específico a la Lista blanca o a la Lista negra, siga estos pasos:

1 Active la Lista blanca o la Lista negra y haga clic en **Personalizar**.
2 Escriba el dominio y haga clic en **Agregar**. Para editar una entrada existente, haga clic en **Editar**.

Nota

El dominio debe tener el formato: *@mytest.com.

3 Para guardar los cambios, haga clic en **Aceptar**.

4 Nota

*La Protección contra el spam solo está disponible con las versiones Advanced y Premium de Seqrite Endpoint Protection.

Capítulo 4. Opciones de análisis

La opción Analizar mi Mac del Panel de control le ofrece diversas opciones para analizar su sistema, de modo que pueda hacerlo según sus necesidades. Puede iniciar el análisis de todo el sistema, unidades, unidades de red, unidades USB, carpetas o archivos, y ubicaciones específicas (Análisis personalizado). Aunque la configuración predeterminada para el análisis manual suele ser adecuada, puede ajustar las opciones para el análisis manual.

Scan My Mac

Scan My Mac es un análisis completo de su sistema. Con Scan My Mac, puede analizar todo el equipo, los archivos y las carpetas, excepto las unidades de red asignadas, las carpetas y los archivos, siempre que considere que su sistema necesita un análisis. Sin embargo, si mantiene activada la Protección contra virus, no es necesario que realice un análisis manual. Además, la configuración predeterminada para el análisis manual suele ser adecuada, pero puede ajustar las opciones para el análisis manual si es necesario.

Para iniciar Scan My Mac, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en la lista **Scan My Mac** que aparece en la parte inferior derecha.
2. En la opción de análisis, haga clic en **Scan My Mac** para iniciar el análisis completo de su equipo.

Una vez completado el análisis, puede ver el informe de análisis en Informes > Informes del escáner.

Análisis personalizado

Con el Análisis personalizado, puede analizar registros, unidades, carpetas y archivos específicos de su equipo que necesite. Esto resulta útil cuando desea analizar solo determinados elementos y no todo el sistema.

Para iniciar el Análisis personalizado, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en la lista **Scan My Mac** que aparece en la parte inferior derecha.
2. En la opción de análisis, haga clic en **Análisis personalizado**.
3. Haga clic en **Agregar** para localizar la ruta de la carpeta o las unidades que desea analizar.

Puede seleccionar varias carpetas para analizar. Si desea eliminar un archivo del análisis, selecciónelo y haga clic en Eliminar. Para eliminar todos los archivos del análisis, haga clic en “Eliminar todo”.

4. Para iniciar el análisis, haga clic en **Iniciar análisis**.

Una vez completado el análisis, puede ver el informe de análisis en Informes > Informes del escáner.

Capítulo 5. Menús de Seqrite Endpoint Protection

Los menús de Seqrite Endpoint Protection, disponibles en la esquina superior izquierda del Panel de control de Seqrite Endpoint Protection, le permiten acceder al instante a las opciones de configuración y de informes, independientemente de la función a la que se acceda.

Con los menús de Seqrite Endpoint Protection, puede configurar los ajustes generales para que las actualizaciones se realicen automáticamente, proteger con contraseña la configuración de Seqrite Endpoint Protection para que los usuarios no autorizados no puedan acceder a ellos, configurar la compatibilidad con proxy y programar la eliminación de informes de la lista de informes.

Informes

Seqrite Endpoint Protection crea y mantiene un informe detallado de todas las actividades importantes, como el análisis de virus, los datos de las actualizaciones, los cambios en la configuración de las funciones, etc.

Se pueden consultar los informes de las siguientes funciones de Seqrite Endpoint Protection:

- Escáner
- Protección contra virus
- Protección de correo electrónico
- Actualización automática
- Protección de navegación
- Protección contra phishing
- Seguridad web

Visualización de informes

Para ver los informes y estadísticas de las diferentes funciones, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Informes**.

Aparecerá una lista de informes.

2 Para ver el informe de una función, haga clic en el nombre del informe. Por ejemplo, si desea ver el informe sobre Protección contra virus, haga clic en **Informes de Protección contra virus**.

Aparecerá la lista de datos del informe. Las estadísticas del informe sobre cada función incluyen la fecha y la hora en que se creó el informe y el motivo por el que se creó.

Botones	Acciones
Datos	Le ayuda a ver un informe detallado del registro seleccionado.
Eliminar	Le ayuda a eliminar el informe resaltado en la lista.
Eliminar todo	Le ayuda a eliminar todos los informes.
Cerrar	Le ayuda a salir de la ventana.

Configuración

En Configuración puede configurar algunos de los ajustes comunes de Seqrite Endpoint Protection, como decidir si desea recibir las actualizaciones automáticamente, proteger con contraseña

la configuración de Seqrite Endpoint Protection para que los usuarios no autorizados no puedan acceder a ella, configurar la compatibilidad con proxy y programar la eliminación de informes de la lista de informes. Sin embargo, la configuración predeterminada es óptima y garantiza la seguridad total de su sistema.

La configuración incluye lo siguiente:

Actualización automática

Con la actualización automática, Seqrite Endpoint Protection puede descargar las actualizaciones automáticamente para mantener su software actualizado con las últimas firmas de virus y proteger su sistema contra nuevos programas maliciosos. Se recomienda mantener siempre habilitada la actualización automática, que está habilitada de forma predeterminada.

Configuración de la Actualización automática

Para configurar la Actualización automática, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
2. En la pantalla Configuración, active la opción Actualización automática y, a continuación, haga clic en **Actualización automática**.
3. En la pantalla Actualización automática, cambie Mostrar notificación a **SÍ**.

De forma predeterminada, esta función está habilitada. Si la opción "Mostrar notificación" está activada, recibirá una notificación cada vez que se reciban nuevas actualizaciones y aparecerá una ventana emergente con la notificación en el Panel de control.

4. Seleccione una de las siguientes opciones:

- *Descargar desde Internet*: Esta opción le permite descargar las actualizaciones directamente desde Internet a su equipo. Puede seleccionar esta opción si su equipo no está conectado al Servidor de Endpoint Protection a través de una red LAN. Esta opción está seleccionada de forma predeterminada.
- *Descargar desde el agente de actualización:* Seleccione esta opción si desea obtener las actualizaciones desde el Agente de actualización.

  Para el Cliente para Mac, a fin de recibir las actualizaciones del Agente de actualización, se deben agregar el nombre de host y la IP del agente de actualización en el archivo hosts del sistema Mac.

  Para agregar el nombre de host en el archivo hosts, haga lo siguiente:

  v. Abra el Terminal en el sistema operativo Mac.
  vi. Introduzca el comando cd /etc.
  vii. Introduzca el comando sudo vi hosts
  viii. Introduzca el nombre de host y la IP de los Agentes de actualización disponibles en el archivo hosts.
  ix. Guarde el archivo hosts.

- *Seleccionar desde ruta especificada*: Seleccione esta opción si desea seleccionar las actualizaciones desde una carpeta local o una carpeta de red. Esto resulta útil cuando el equipo no está conectado a Internet ni está disponible en la LAN. Después de seleccionar esta opción, explore la ruta para seleccionar las actualizaciones desde la ubicación compartida.

5. Cambie Guardar archivos de actualización a **SÍ**.

Seleccione esta opción si desea guardar una copia de las actualizaciones descargadas en su carpeta local o carpeta de red. El botón Examinar estará habilitado. La opción Guardar archivos de actualización estará habilitada cuando seleccione Descargar desde Internet.

6 Haga clic en **Examinar** para especificar una carpeta o carpeta de red en la que guardar una copia de las actualizaciones descargadas de Internet.

7 Para guardar la configuración, haga clic en **Guardar**.

Autoprotección

Con la función de Autoprotección, puede impedir que usuarios no autorizados modifiquen o manipulen los archivos, carpetas, configuraciones y entradas Plist de Seqrite Endpoint Protection configuradas contra el malware. Se recomienda mantener siempre activada la función de Autoprotección.

Configuración de la Autoprotección

Para configurar la Autoprotección, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.

2 En la pantalla Configuración, active la Autoprotección.

Sin embargo, la Autoprotección está activada de forma predeterminada.

Protección con contraseña

Con la Protección con contraseña, puede restringir el acceso de todos los demás usuarios a Seqrite Endpoint Protection para que ningún usuario no autorizado pueda realizar cambios en la configuración. Se recomienda mantener siempre activada la Protección con contraseña.

Configuración de la Protección con contraseña

Para configurar la Protección con contraseña, siga estos pasos:

1 En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.

La Protección con contraseña está desactivada de forma predeterminada, pero puede activarla si es necesario.

2 En la pantalla Configuración, active la Protección con contraseña.

Aparecerá la pantalla de Protección con contraseña.

3 Introduzca la contraseña en el cuadro de texto "Nueva contraseña" y, a continuación, confírmela introduciéndola en "Volver a escribir nueva contraseña".

Si está configurando la contraseña por primera vez, la opción Contraseña existente estará desactivada.

4 Para restablecer su contraseña, haga clic en **Protección con contraseña**.

5 Para guardar la configuración, haga clic en **Guardar**.

Control del dispositivo

Con esta función, los administradores pueden crear directivas con diferentes derechos. Por ejemplo, los administradores pueden bloquear completamente el acceso a dispositivos extraíbles, conceder acceso de solo lectura y sin escritura para que no se pueda escribir nada en los dispositivos externos. También pueden personalizar el acceso a los dispositivos configurados por los administradores. Una vez que se aplica la directiva a un grupo, también se aplican los derechos de acceso.

A continuación, se muestra una comparación de los tipos de dispositivos en diferentes sistemas Mac:

Dispositivos	Tipos de dispositivos	macOS Catalina y versiones anteriores	macOS Big Sur y versiones posteriores
Dispositivos de almacenamiento	Dispositivo de almacenamiento USB	√	√
	CD/DVD interno	√	√
	Lector de tarjetas interno	√	√
	Unidad de disquete interna	X	X
	Unidad ZIP	X	X
Inalámbrico	Wi-Fi	√	√
	Bluetooth	√	√
Interfaz	Bus FireWire	√	X
	Puerto de serie	X	X
	Controlador SATA	X	X
	Thunderbolt	√	√
	Dispositivo PCMCIA	X	X
	USB	√	√
Otros	Impresoras locales	√	√
	Placa Teensy	X	X
	Recurso compartido de red	X	X
	Dispositivo desconocido	X	X
Lectores de tarjetas	Dispositivo lector de tarjetas (MTD)	X	X

	Dispositivo lector de tarjetas (SCSI)	X	X
Dispositivos móviles y portátiles	Dispositivo portátil Windows	√	√
	iPhone	√	√
	iPad	√	√
	iPod	√	√
	BlackBerry	X	X
	Teléfonos móviles (Symbian)	X	X
	Escáneres y dispositivos de imagen	X	X
Cámara	Cámara web	√	X
Acceso temporal al dispositivo		√	√
Excepciones de dispositivos		√	√

Las directivas de control de dispositivos se pueden configurar de forma remota a través de la consola de Seqrite Endpoint Protection Cloud.

Configuración del control de dispositivos en el Cliente para Mac

Para configurar el control de dispositivos, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
2. En la pantalla Configuración, active el Control de dispositivos.

Sin embargo, el Control de dispositivos está desactivado de forma predeterminada.

Las siguientes son las condiciones excepcionales

- Si se selecciona la opción "Solo lectura" en el control de dispositivos de Seqrite EPP y se conecta un dispositivo USB, es posible que no se pueda acceder a dicho dispositivo desde el panel izquierdo del Buscador durante un tiempo.
- Si se muestra un dispositivo USB como montado o desmontado mediante comandos de terminal, la directiva de Control de dispositivos no se aplicará a ese dispositivo.
- Los CD/DVD conectados obtendrán permisos de lectura y escritura, aunque se aplique la configuración de solo lectura en Control de dispositivos de Seqrite EPP.

  Si alguno de los dispositivos iDevices, Webcam, CD/DVD, lector de tarjetas interno, teléfonos móviles y dispositivos cifrados HFS ya está conectado a la terminal y se modifican los ajustes de Control de dispositivos, será necesario volver a conectar los dispositivos conectados para que los derechos de acceso se apliquen a los nuevos dispositivos.

- La función de excepción no es aplicable a Bluetooth, Wi-Fi, cámaras web y CD/DVD externos.
- Es posible que se generen varias notificaciones para CD/DVD.
- Los teléfonos móviles, excepto los dispositivos iDevices que estén conectados en modo MTP, se detectarán en la categoría de *Dispositivos de almacenamiento USB*.
    - Los teléfonos móviles conectados en modo MTP se detectarán en la categoría *Dispositivos portátiles de Windows*.
- Si está instalando el Cliente para Mac con dispositivos USB conectados al sistema, dichos dispositivos se desmontarán durante unos segundos después de la instalación.
- Si se conecta un dispositivo USB con sistema de archivos NTFS durante la instalación del Cliente para Mac, es posible que se vean dos copias de un dispositivo USB conectado durante unos segundos.
- El dispositivo de almacenamiento USB no se formateará con el formato de archivo extendido de Mac OS (con registro, cifrado).
- La función "Conexiones Wi-Fi autorizadas" no es compatible con el sistema operativo Mac.
- Si el administrador bloquea inadvertidamente la conexión Wi-Fi utilizando una directiva, la conexión Wi-Fi de la terminal Mac correspondiente se desconectará. Para volver a habilitarla desde la terminal, siga los pasos que se indican a continuación:
    - Inicie sesión en la Consola de Endpoint Protection Cloud > Haga clic en **Endpoint Protection** > Haga clic en la pestaña **Estado** > Seleccione la terminal Mac desde el que se desactiva el Wi-Fi > Haga clic en **Acciones del cliente** > Seleccione **Acceso temporal al dispositivo** en la lista desplegable > Haga clic en **Enviar** > establezca la duración según sea necesario en "Permitir acceso temporal durante" y "Usar OTP dentro de" > Haga clic en **Generar OTP** > Anote la contraseña de un solo uso (OTP) generada.
    - Ahora vaya al sistema terminal Mac > haga clic en el icono de la bandeja del sistema Seqrite Endpoint Protection > seleccione "Permitir acceso temporal al dispositivo" en la lista desplegable > Introduzca la contraseña de un solo uso (OTP) generada en la consola EPP. Ahora podrá accederse a los dispositivos durante el intervalo de tiempo definido en la consola EPP.
    - Vuelva a la consola EPP Cloud > haga clic en **Directivas** > haga clic en **Editar** en la directiva correspondiente al terminal Mac > haga clic en la pestaña **Control avanzado de dispositivos** > haga clic en **Inalámbrico y cableado** > permita el "Wi-Fi" y guarde la directiva.
    - Habilite el Wi-Fi en la terminal Mac.
    - El administrador puede solicitar al usuario que haga clic en **Sincronizar ahora** en la lista desplegable del icono de la bandeja del sistema de Seqrite Endpoint Protection desde la terminal Mac correspondiente o esperar al latido y, una vez que se haya completado con éxito, el administrador puede pedir al usuario que haga clic en "Acceso temporal al dispositivo" en la lista desplegable del icono de la bandeja del sistema de Seqrite Endpoint Protection o caducará automáticamente después del tiempo establecido en la consola EPP Cloud en "Permitir acceso temporal al dispositivo".
- En macOS Tahoe 26, la función de bloqueo de Bluetooth no funciona, aunque aparece el mensaje «Control de dispositivos bloqueado».
- Gestión de activos: En el sistema de archivos Apple_APFS, la unidad del sistema

operativo no aparecerá en la sección Almacenamiento en disco de Datos del hardware.

Prevención de pérdida de datos (DLP)

Las siguientes son las condiciones excepcionales

- Si las Aplicaciones Mac se instalan y se inician desde cualquier ubicación que no sea la carpeta "Aplicaciones" cuando DLP está habilitado y se supervisan todos los tipos de archivos para bloquearlos en esas aplicaciones, las aplicaciones no se iniciarán.
- La función de bloqueo DLP no funcionará en macOS Catalina 10.15 y versiones posteriores si el archivo adjunto se envía a través de cualquier aplicación de correo electrónico mediante el navegador Safari.
- La descarga de archivos se bloquea a través del navegador si DLP está habilitado.

Compatibilidad con proxy

Con la opción "Compatibilidad con proxy", puede habilitar la compatibilidad con proxy, establecer el tipo de proxy, configurar la dirección IP y el puerto del proxy para utilizar la conexión a Internet. Si utiliza un servidor proxy en su red o una red Socks versión 4 y 5, deberá introducir la dirección IP (o el nombre de dominio) y el puerto del proxy, el servidor SOCKS V4 y SOCKS V5 en la configuración de Internet.

Sin embargo, si configura la compatibilidad con proxy, deberá introducir su nombre de usuario y contraseña. Los siguientes módulos de Seqrite requieren estos cambios:

- Asistente de registro
- Actualización de seguridad para Mac
- Mensajería
- Seguridad Web (Protección del navegador, Protección contra phishing y Protección contra spam)

Configuración de la compatibilidad con proxy

Para configurar la compatibilidad con proxy, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
2. En la pantalla Configuración, haga clic en **Soporte de proxy**.
3. En la pantalla Soporte de proxy, active el Soporte de proxy para habilitarlo.

Se habilitarán los cuadros de texto Seleccionar tipo de proxy, Introducir servidor, Introducir puerto y Credenciales de usuario.

4. Seleccione el tipo de proxy entre HTTP, SOCKS V4 y SOCKS V5 según sus preferencias.
5. En el cuadro de texto Introducir Servidor, introduzca la Dirección IP del servidor proxy o el nombre de dominio.
6. En el cuadro de texto Introducir puerto, introduzca el número de puerto del servidor proxy.

De forma predeterminada, el número de puerto está configurado como 80 para HTTP y 1080 para SOCKS V4 y SOCKS V5.

7. Introduzca el nombre de usuario y la contraseña.
8. Para guardar la configuración, haga clic en **Guardar**.

Configuración de informes

Con la Configuración de informes, puede establecer reglas para eliminar automáticamente los informes generados sobre todas las actividades. Puede especificar el número de días tras los cuales se deben eliminar los informes de la lista.

También puede conservar todos los informes generados si los necesita. Sin embargo, la configuración predeterminada para eliminar informes es de 30 días.

Configuración de los ajustes de los informes

Para configurar los informes, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
2. En la pantalla Configuración, haga clic en **Configuración de informes**.
3. En la pantalla Configuración de informes, active la opción "*Eliminar informes automáticamente"* para eliminar los informes después del número de días especificado. Si desea conservar todos los informes generados, desactive la opción "*Eliminar informes automáticamente"*.
4. Seleccione el período en la lista "Eliminar después de" tras el cual desea que se eliminen los informes.
5. Para guardar la configuración, haga clic en **Guardar**.

Capítulo 6. Actualización de software y eliminación de virus

Las actualizaciones de Seqrite Endpoint Protection se publican periódicamente en el sitio web de Seqrite y contienen la detección y eliminación de virus recién descubiertos. Para proteger su equipo contra nuevos virus, debe disponer de la copia actualizada de Seqrite Endpoint Protection. De forma predeterminada, Seqrite Endpoint Protection está configurado para actualizarse automáticamente desde Internet. Esto se realiza sin la intervención del usuario. Sin embargo, su equipo debe estar conectado a Internet para recibir las actualizaciones periódicamente. Las actualizaciones automáticas también se pueden aplicar desde una ruta local o de red, pero dicha ruta debe tener el último conjunto de definiciones.

Algunos datos importantes sobre las actualizaciones de Seqrite Endpoint Protection son:

- Todas las actualizaciones de Seqrite Endpoint Protection son actualizaciones completas que incluyen la actualización del archivo de definiciones y las actualizaciones del motor.
- Todas las actualizaciones de Seqrite Endpoint Protection también actualizan su versión siempre que sea necesario, lo que le permite disponer de las nuevas funciones y tecnologías para su protección.
- La actualización de Seqrite Endpoint Protection es un proceso de actualización de un solo paso.

Actualización de Seqrite Endpoint Protection desde Internet

La función Actualizar ahora mantiene su copia de Seqrite Endpoint Protection actualizada automáticamente a través de Internet. Sin embargo, su equipo debe estar conectado a Internet para recibir las actualizaciones con regularidad. Esta función funciona con todo tipo de conexiones a Internet (acceso telefónico, RDSI, cable, etc.).

También puede actualizar Seqrite Endpoint Protection manualmente siempre que lo necesite, de cualquiera de las siguientes maneras:

- Haga clic en el icono de Seqrite Endpoint Protection en la barra de menú y, a continuación, seleccione Actualizar ahora.
- Si el Panel de control de Seqrite Endpoint Protection está abierto, haga clic en Actualizar ahora, que aparece si la protección está desactualizada.
- Abra Seqrite Endpoint Protection y, a continuación, en la barra de menú, vaya a Seqrite Endpoint Protection > Acerca de Seqrite Endpoint Protection. En la página Acerca de Seqrite Endpoint Protection, seleccione “Actualizar ahora”.

  Se inicia la actualización de Seqrite Endpoint Protection.

  Asegúrese de que su equipo esté conectado a Internet. Endpoint Protection Update se conecta al sitio web de Seqrite Endpoint Protection Cloud, descarga los archivos de actualización adecuados para su software y los aplica a su copia, actualizándola así con el último archivo de actualización disponible.

Actualización de Seqrite Endpoint Protection con archivos de definición

Si dispone del archivo de definición de actualización, puede actualizar Seqrite Endpoint Protection sin conectarse a Internet. Esto resulta útil para entornos de red con más de un

equipo. No es necesario descargar el archivo de actualización en todas las máquinas de la red. Puede descargar los archivos de definición más recientes del sitio web de Seqrite en un equipo y, a continuación, actualizar todos los demás equipos con los archivos de definición.

Para actualizar Seqrite Endpoint Protection mediante el archivo de definiciones, siga estos pasos:

1. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
2. Active la actualización automática y, a continuación, haga clic en **Actualización automática**.
3. Active "Mostrar notificación" para recibir una notificación cuando sea necesario actualizar.
4. Marque "*Seleccionar de la ruta especificada*" y, a continuación, especifique la ubicación desde la que se deben recoger las actualizaciones.
5. Para guardar la configuración, haga clic en **Guardar**.

Su copia de Seqrite Endpoint Protection se actualizará desde la ubicación especificada.

Directrices de actualización para entornos de red

Seqrite Endpoint Protection se puede configurar para proporcionar actualizaciones sin complicaciones en toda la red. Se recomiendan las siguientes directrices para obtener los mejores resultados:

1. Configure un equipo (puede ser un servidor) como equipo maestro de actualización. Supongamos que el nombre del servidor es SERVER.
2. Cree la carpeta SEQRITEUPD en cualquier ubicación. Por ejemplo: SEQRITEUPD.
3. Asigna el derecho de uso compartido de solo lectura a esta carpeta.
4. En el Panel de control de Seqrite Endpoint Protection, haga clic en **Configuración**.
5. En la pantalla Configuración, haga clic en **Actualización automática**.
6. Cambie "*Guardar archivos de actualización*" a Sí.
7. Haga clic en "Examinar" y localice la carpeta SEQRITEUPD. Haga clic en **Abrir**.
8. Para guardar la configuración, haga clic en **Guardar**.
9. En todos los demás equipos de la red, inicie Seqrite Endpoint Protection.
10. Vaya a la pantalla de datos de Configuración y seleccione "Actualización automática".
11. Seleccione "*Seleccionar archivos de actualización de la ruta especificada*".
12. Haga clic en **Examinar**.
13. Busque la carpeta SERVER\SEQRITEUPD en Entorno de red. También puede escribir la ruta como \\SERVER\SEQRITEUPD.
14. Para guardar la configuración, haga clic en **Guardar**.

Eliminación de virus

Seqrite le avisa de una infección por virus cuando:

- Se encuentra un virus durante un análisis manual.
- La Protección contra virus/Protección de correo electrónico de Seqrite Endpoint Protection detecta un virus.

Eliminación de virus detectados durante el análisis

Seqrite Endpoint Protection está correctamente configurado con todos los ajustes necesarios con la instalación predeterminada para proteger su equipo. Si se detecta un virus durante el análisis, Seqrite Endpoint Protection intenta repararlo. Sin embargo, si no consigue reparar los archivos infectados por el virus, dichos archivos se ponen en cuarentena. En caso de que haya personalizado la configuración predeterminada del escáner, tome las medidas adecuadas cuando se detecte un virus.

Opciones de análisis

Durante el análisis, se le ofrecen las siguientes opciones para facilitarle la operación:

Opciones	Descripción
Pestaña Estado	Muestra el estado del análisis.
Pestaña Acción	Muestra la acción realizada en los archivos.
Omitir carpeta	Le ayuda a evitar el análisis de la carpeta actual. El análisis se traslada a otra ubicación. Esta opción es útil al analizar una carpeta que sabe que contiene elementos no sospechosos.
Omitir archivo	Le ayuda a evitar el análisis del archivo actual. Esta opción es útil al analizar un archivo grande de archivos.
Pausar	Le ayuda a pausar el análisis mientras se está procesando. Se trata de una pausa temporal y puede reanudar el análisis después de un tiempo.
Detener	Le ayuda a detener el proceso de análisis. Se trata de una interrupción permanente y no podrá reiniciar el análisis desde la misma instancia.
Cerrar	Le permite salir del proceso de análisis.
Estado del análisis	Muestra el estado del proceso de análisis en porcentaje.

Capítulo 7. Soporte técnico

Seqrite ofrece un amplio soporte técnico a sus usuarios registrados. Se recomienda que tenga a mano toda la información necesaria durante la llamada para recibir un soporte eficaz por parte de los ejecutivos de soporte de Seqrite.

La opción de Soporte incluye una sección de preguntas frecuentes (FAQ) donde puede encontrar respuestas a las preguntas más habituales, enviar correos electrónicos con sus consultas o llamarnos directamente.

Para ver las opciones de soporte, siga estos pasos:

1. Abra Seqrite Endpoint Protection.
2. En la barra de menú de Seqrite Endpoint Protection, vaya a Ayuda > Soporte.

El Soporte incluye las siguientes opciones.

Soporte por teléfono: Le ayuda a llamar a nuestro equipo de soporte para resolver sus problemas.

Número de contacto para el Soporte por teléfono: 1800 212 7377

Enviar una consulta (Soporte por correo electrónico): Le ayuda a enviarnos su consulta. Le responderemos con una respuesta adecuada en breve.

Chatee con nosotros (Soporte por chat en vivo): Le ayuda a chatear con nuestros ejecutivos de soporte para resolver sus problemas al instante.

Localizar distribuidor: Le ayuda a localizar el distribuidor más cercano a su ubicación.

Otras formas de obtener Soporte

Para otras formas de Soporte, visite: http://www.seqrite.com/contact_support.

Para obtener Soporte en un país específico, visite: http://www.seqrite.com/int_techsupp.

Datos de contacto de la Oficina central

Quick Heal Technologies Limited

(Anteriormente conocida como Quick Heal Technologies Pvt. Ltd.)

Oficina registrada: Marvel Edge, Oficina n.º 7010 C & D, 7.ª piso,

Viman Nagar, Pune 411014.

Sitio web oficial: http://www.seqrite.com

Correo electrónico: support@seqrite.com