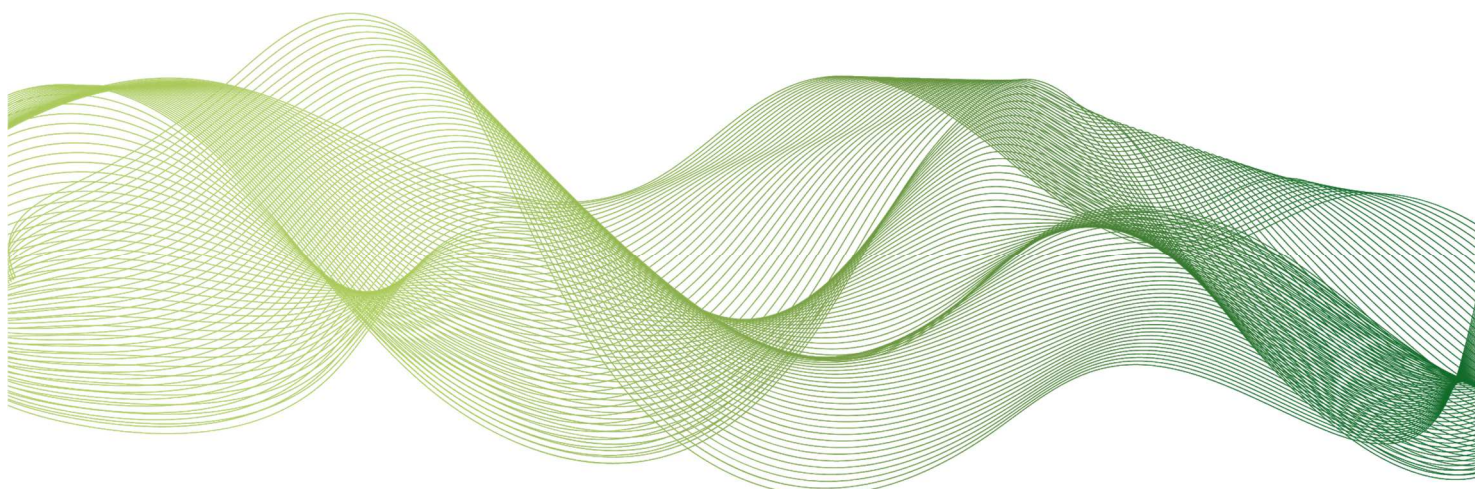




Manual Cliente VPN MAC Checkpoint RCJAv5

Ingeniería SANDETEL

ÍNDICE

- 1. Objetivo**
- 2. Versiones Soportadas**
- 3. Instalación**
- 4. Conexión**
- 5. Desinstalación**

1. Objetivo

Manual de usuario del cliente VPN Checkpoint Harmony Endpoint en Sistema Operativo MAC. El presente documento tiene como objetivo mostrar los pasos de instalación, conexión y desinstalación del cliente Harmony Endpoint para MACOS. Este cliente es el que se empleará en RCJAv5 para dar continuidad al servicio VPN.

2. Versiones Soportadas

macOS

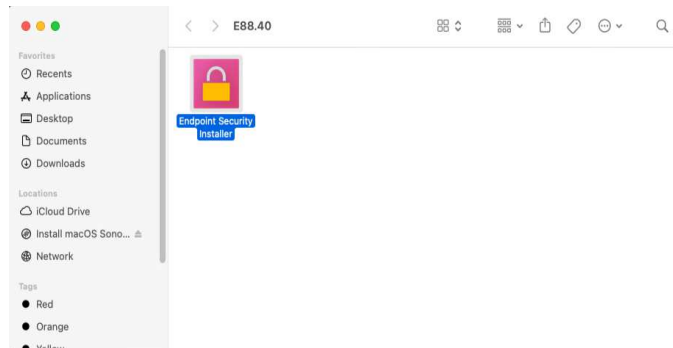
macOS Version	Supported starting from
macOS Sonoma (14)	EA support: Endpoint Security Client E87.60 GA support: Endpoint Security Client E87.70
macOS Ventura (13)	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
macOS Monterey (12)	EA support: Endpoint Security Client E85.30 GA support: Endpoint Security Client E86.20
macOS Big Sur (11)	Endpoint Security Client E84.30

Notas:

- Para despliegues existentes del Endpoint Security, antes de actualizar la versión de OS, es necesario actualizar previamente el Endpoint Security client a una versión que soporte la versión deseada del OS basándose en la tabla anterior.

3. Instalación

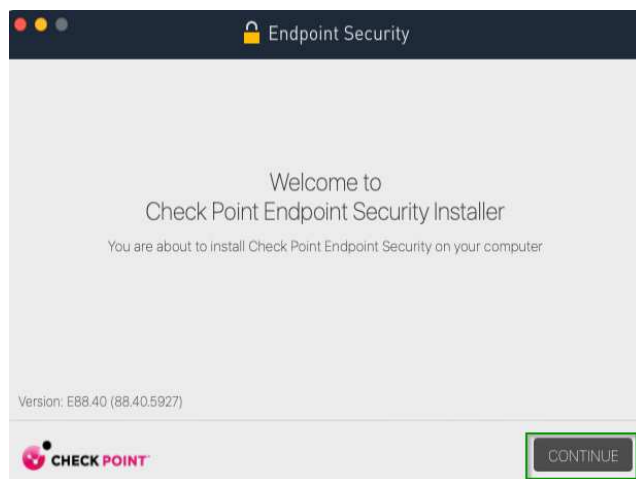
La instalación se realiza usando un paquete .app.



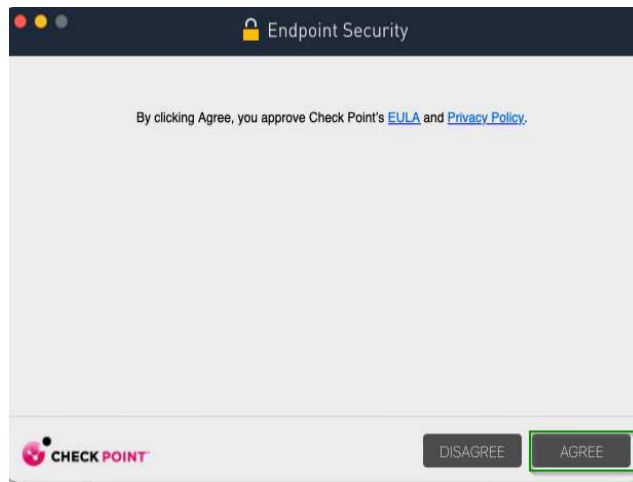
Haciendo doble clic en el paquete, aparecerá primero un aviso indicando que la app se ha descargado desde internet:



Pinchando en Open, continuamos con la instalación.

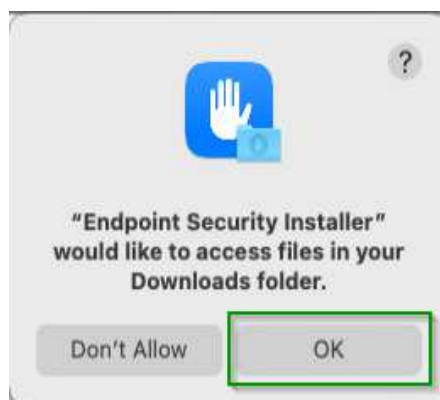


Pulsamos en "Continue" y aparecerá la ventana con el acuerdo de usuario y la política de privacidad:



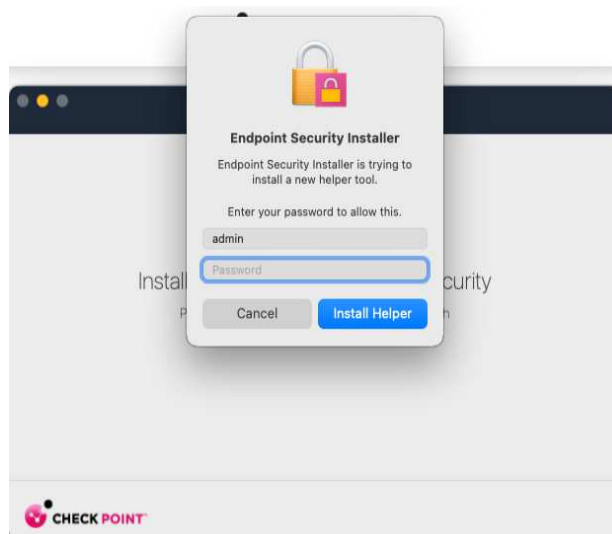
En caso de conformidad con los términos incluidos (pueden verse haciendo clic en Eula y Privacy Policy), haremos clic en “Agree”.

Tras esto aparecerá un mensaje indicando que el instalador quiere acceder a la carpeta donde está en paquete .app:

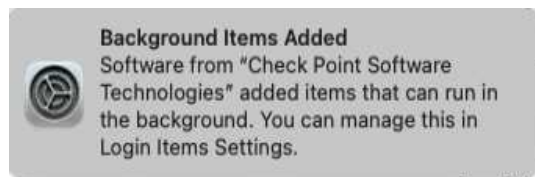


Pulsamos en OK.

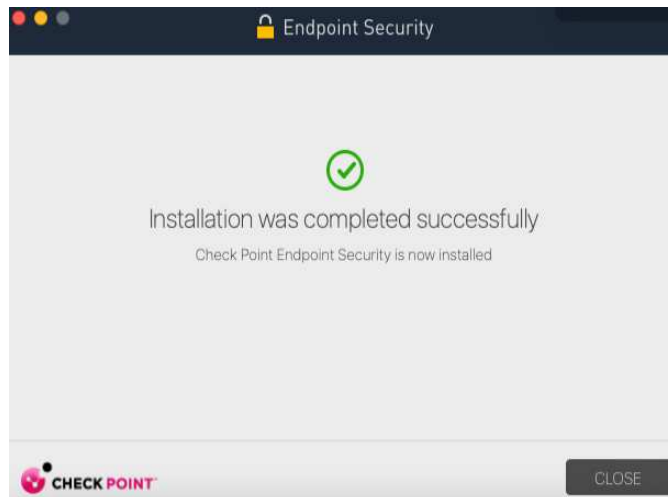
A continuación, comenzará con la instalación y pedirá credenciales de administrador:



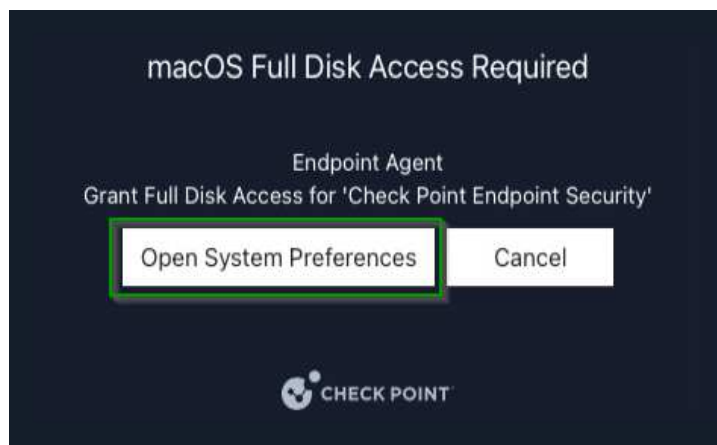
Aparece un mensaje en la barra superior que indica que se añaden objetos que pueden ser ejecutados en background, mientras continúa la instalación:



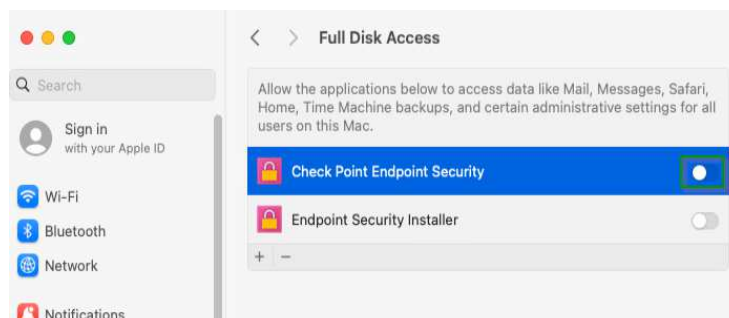
Al finalizar la instalación podemos ver un mensaje indicándolo:



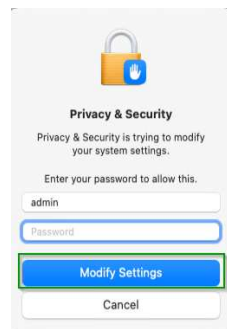
Tras instalar solicitará acceso al disco para el cliente Endpoint:



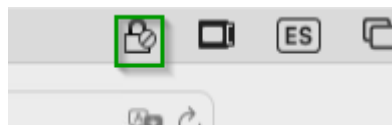
Haciendo clic en "Open System Preferences" garantizamos el acceso:



Nos pedirá de nuevo que introduzcamos las credenciales de administrador:



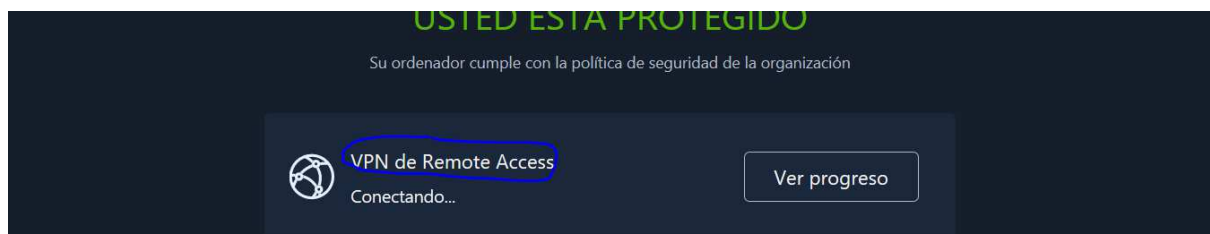
Tras esto estará completamente instalado. En la barra de tareas, aparecerá el icono del cliente:



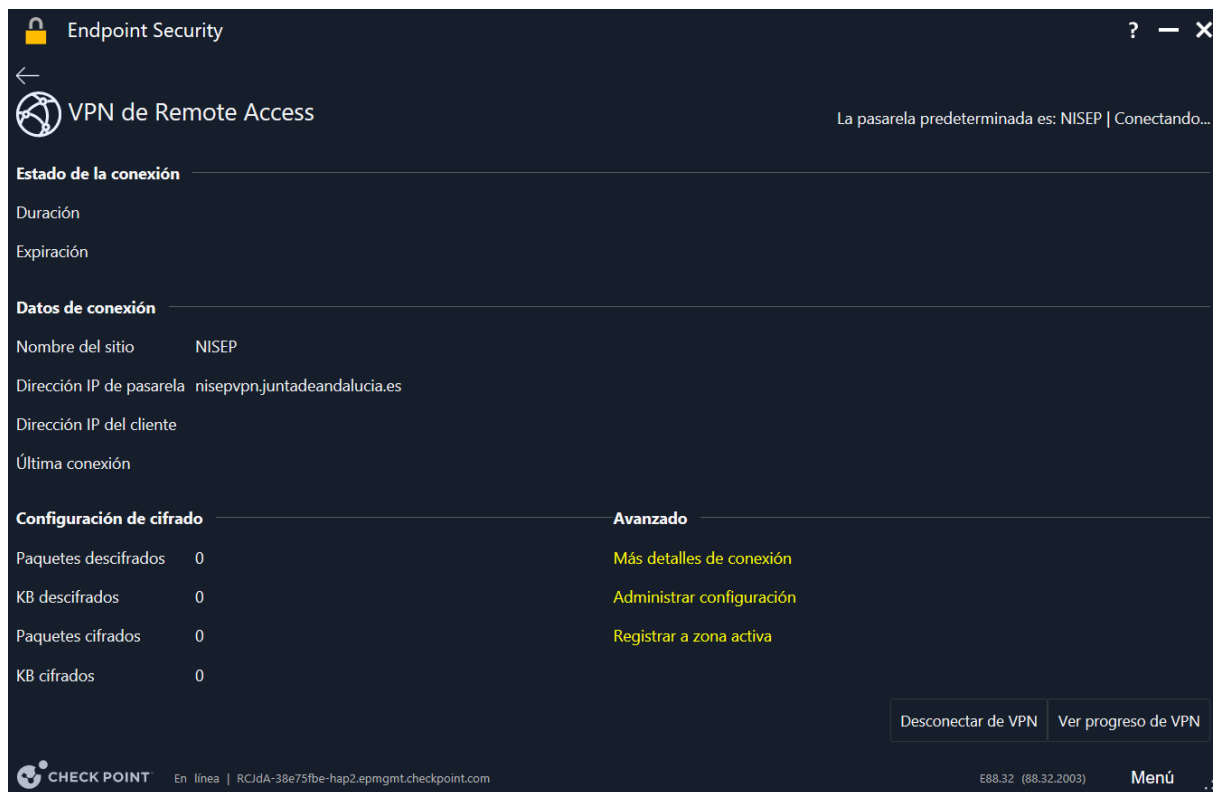
OPCIONAL (en verde):

En caso de querer acceder al detalle de la configuración del cliente, se puede proceder de la forma que se detalla a continuación (aunque no es necesario realizar estos pasos, ya que la información necesaria por parte del usuario final se solicitará automáticamente la primera vez que se intente la conexión).

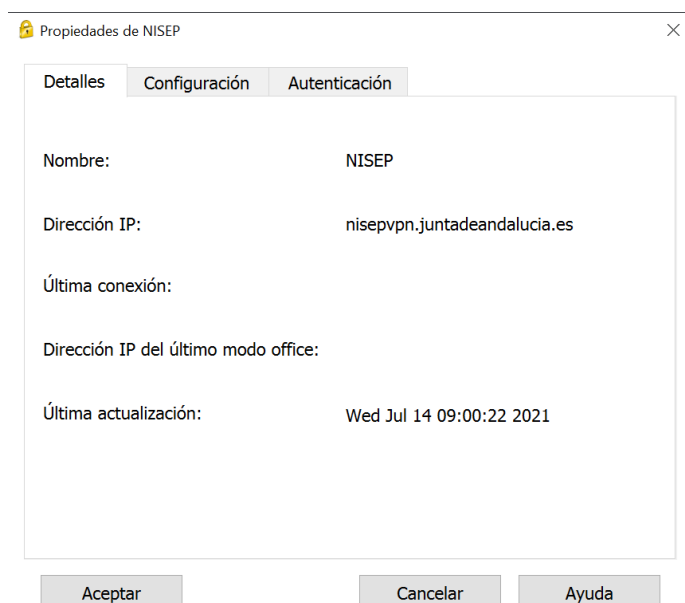
Si pulsamos sobre el texto "VPN de Remote Access"



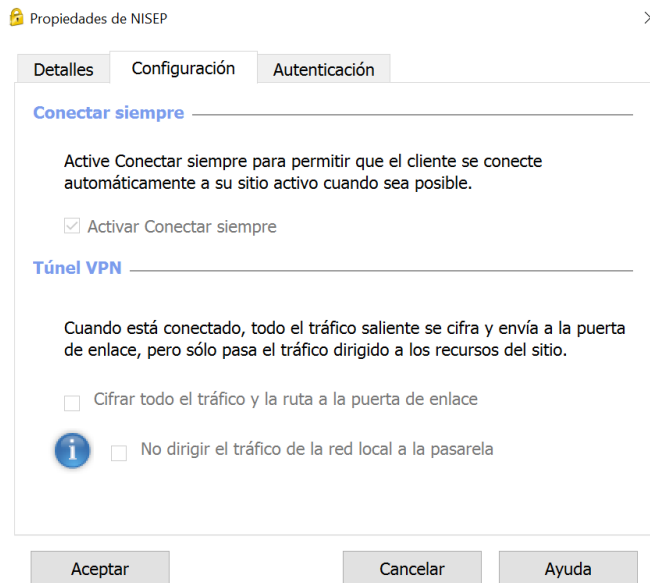
Accederemos a la configuración del cliente VPN:



Pulsando sobre “Más detalles de conexión” veremos las propiedades de la conexión **NISEP**, que es la que viene preconfigurada en el paquete de instalación y que apunta a la URL **nisevpn.juntadeandalucia.es** que es la URL del servicio VPN en RCJAv5:

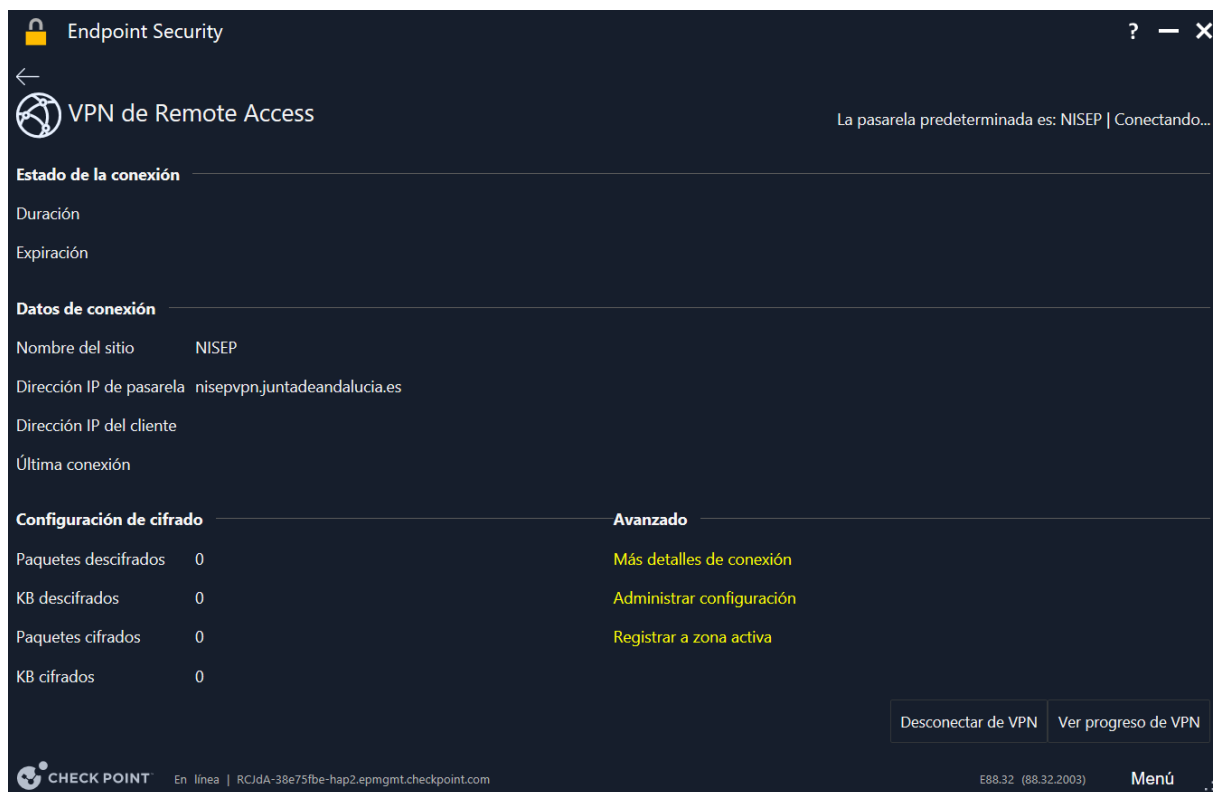


Podremos consultar estos detalles de configuración. En la pestaña “Configuración” veremos que viene activada por defecto la opción de siempre activa. Esta configuración no es modificable por el usuario final, por lo que si en algún caso fuera necesario modificarla, el responsable de datos del Organismo deberá solicitar, mediante solicitud debidamente justificada, y por los cauces habituales su modificación.



No vamos a ver en este punto la pestaña “Autenticación”, ya que la información que contiene es la misma que tiene que introducir el usuario al realizar la primera conexión.

Por otro lado, si en la pantalla principal de configuración del cliente VPN:



Pulsamos sobre “Administrar configuración” veremos la siguiente pantalla:



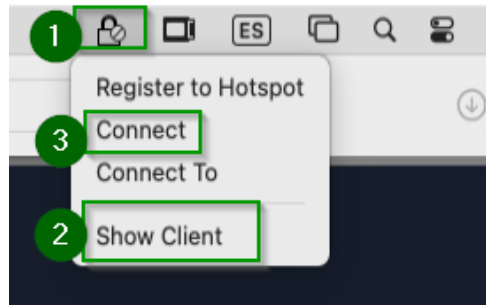
NISEP es el sitio preconfigurado por defecto. Los usuarios que tengan la posibilidad de conectarse a otros sitios con el cliente VPN Checkpoint, podrán configurarse nuevos sitios, sin embargo, esa opción no es objeto de este manual, que se centra únicamente en el sitio **NISEP** ya preconfigurado, por lo que la opción “Nuevo” no se describe.

No pulsar sobre la opción “Eliminar”, si bien el paquete de instalación distribuido no debe permitir la eliminación del sitio **NISEP**.

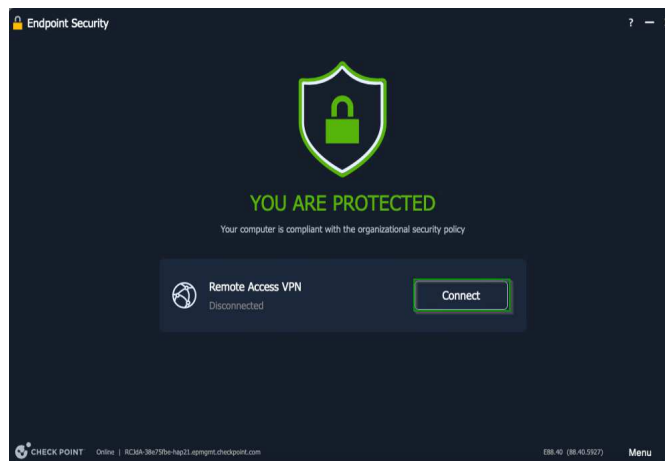
Si pulsamos sobre la opción “Propiedades” veremos las mismas ventanas ya descritas anteriormente cuando se describió la opción “Más detalles de conexión”.

4. Conexión

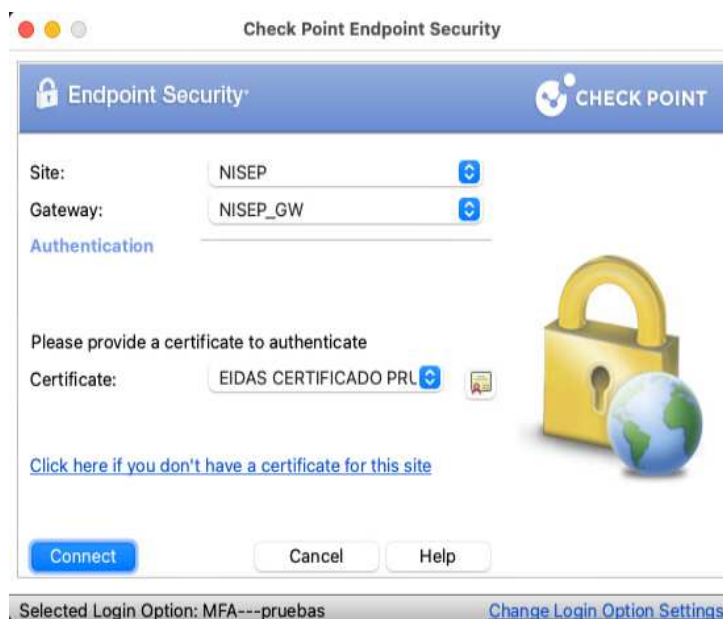
Tal y como se comentó en el apartado anterior, en la barra de tareas, aparecerá el icono del cliente(1):



Pulsando en (2), aparecerá la interfaz del cliente:

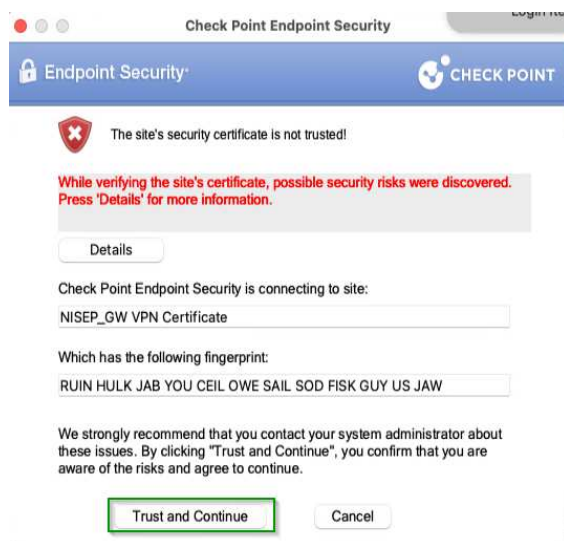


Dándole a Connect en la barra de tareas (3) o en el botón Connect de la ventana mostrada arriba, iniciará la conexión automáticamente hacia el sitio NISEP configurado.

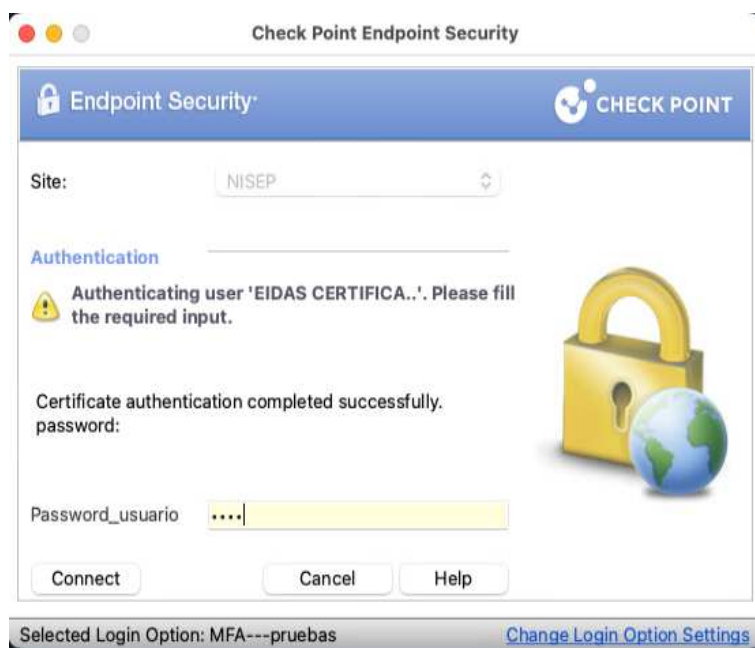


El certificado o certificados se cargarán de forma automática del almacén de keychain de macOS.

La primera que conecte con el Servidor, necesitará aceptar el fingerprint del servidor:



Tras esto, pedirá la contraseña del usuario asociado al certificado:

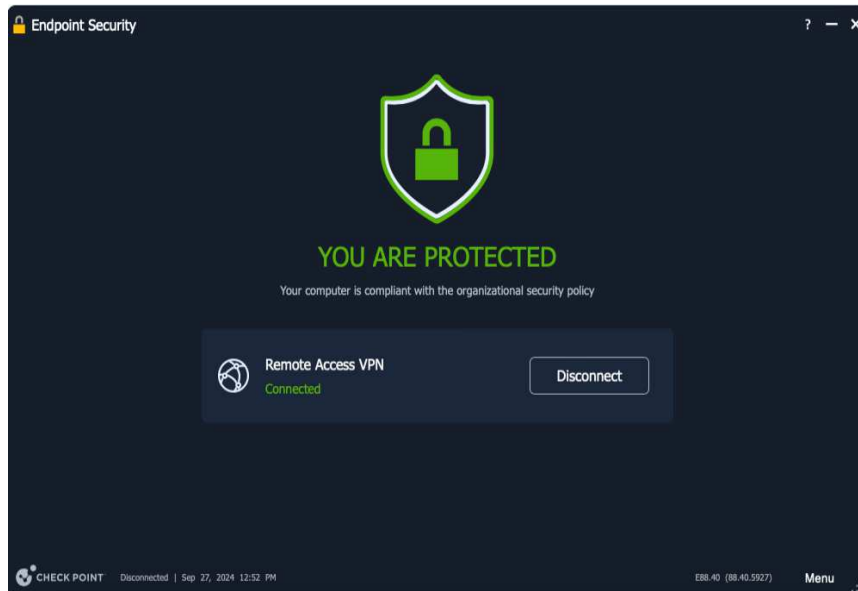


*** NOTA 1: Importante** lo que hay que introducir es la **contraseña LDAP**, no la contraseña del certificado. La solución utiliza el certificado digital introducido para obtener el DNI del usuario, con el DNI se identifica el usuario LDAP en el LDAP de la Junta de Andalucía, y se utiliza la contraseña del usuario LDAP como doble factor de autenticación (2FA).

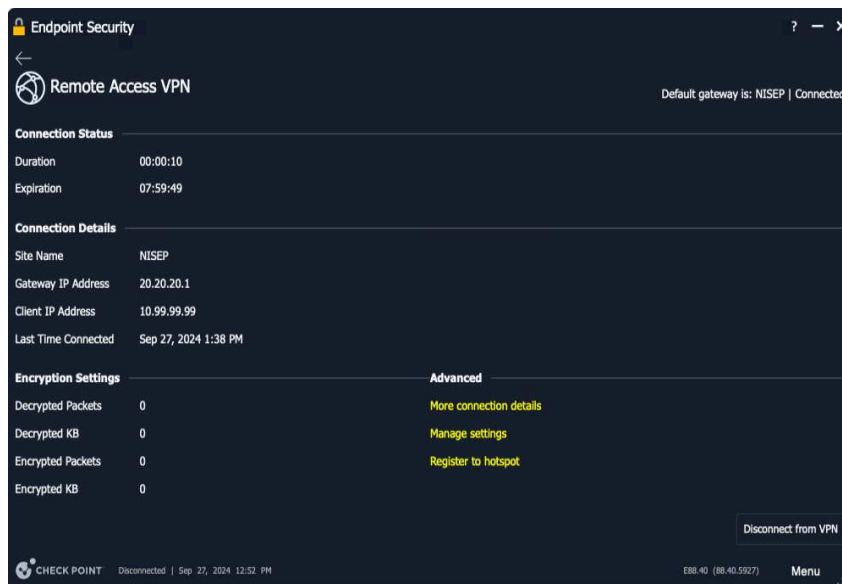
*** NOTA 2:** En caso de que el usuario disponga de más de un UID LDAP asociado al mismo DNI del certificado, podrá indicar al cliente VPN con qué UID se quiere logar, introduciendo en el campo *Password* el UID deseado, concatenado con una @ y la contraseña asociada a ese UID, es decir **usuario@contraseña**. No debe preocuparnos que nuestra contraseña contenga una @, ya que el cliente VPN utilizará la primera @ que encuentre para separar el UID de la contraseña. En función del UID recibiremos una dirección IP u otra, dependiendo del

Organismo y la rama a la que pertenezca, y se aplicarán las visibilidades que correspondan a ese usuario.

Una vez introducida correctamente, se completará la conexión al sitio:



En los detalles de conexión puede verse que ha conectado correctamente:



5. Desinstalación

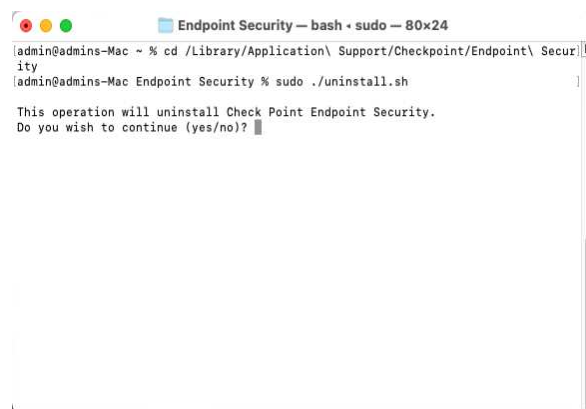
Para desinstalar, abrimos una terminal y escribimos los siguientes comandos:

```
cd "/Library/Application Support/Checkpoint/Endpoint Security/"  
sudo ./uninstall.sh
```

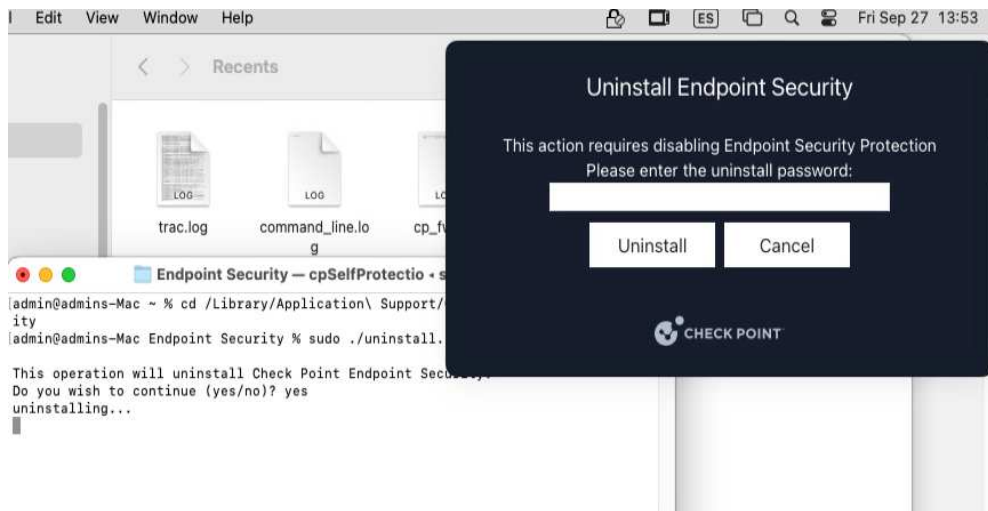


Al necesitar permisos de admin, pedirá la contraseña de administrador.

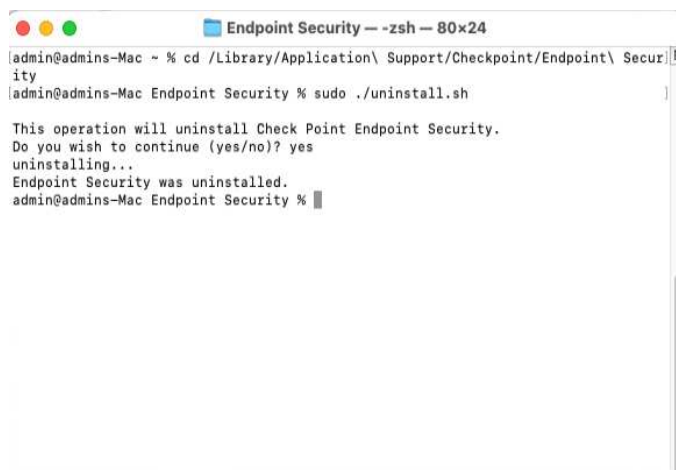
Una vez introducida esa password, solicitará confirmación:



Una vez confirmado, aparecerá una ventana emergente solicitando la contraseña de desinstalación propia del agente. Esta contraseña será distribuida a los administradores de la herramienta que la necesiten.



Una vez introducida, el software se desinstalará correctamente.





Junta de Andalucía

Consejería de la Presidencia,
Administración Pública e Interior