madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

Comunidad de Madrid | CONSEJERÍA DE DIGITALIZACIÓN

VPN de Acceso Remoto para personal externo AREX

Guía de instalación

Dirección de Servicios y Redes de Comunicaciones

Contenido

1 Introducción

El documento describe cómo instalar en un PC **Windows 10 o Windows 11** el cliente *Paloalto GlobalProtect*, que permitirá conectarse por VPN (*Virtual Private* Network o Red Privada Virtual) a los recursos de la Consejería utilizando un doble factor de autenticación.

El servicio de Acceso Remoto para personal externo, AREX, con doble factor de Autenticación (MFA, *Multiple Factor Authentication*) requiere de un agente, que es el software que se ejecuta en el equipo remoto cliente, desde el que se inicia la conexión hacia el portal y la pasarela VPN. Este agente es instalado en el puesto de trabajo y se encarga de iniciar la conexión VPN, así como, de analizar la información mínima de seguridad requerida para el equipo remoto.

Por tanto, para poder utilizar el servicio de acceso remoto AREX es necesario instalar en los equipos remotos el Agente GlobalProtect. Para ello, es necesario ejecutar el fichero de instalación que se descarga previamente desde el Portal GlobalProtect. Para asegurar que se instala la versión adecuada del Agente GlobalProtect, se recomienda realizar la descarga del instalable directamente desde el portal ubicado en **arex.ar.madrid.org**.

2 Condiciones de uso del servicio VPN

El servicio de acceso remoto está diseñado para utilizar un único portal de acceso con múltiple factor de autenticación (MFA) e identificar el entorno al que pertenece el usuario para aplicar la configuración de túnel y la política de acceso remoto correspondiente en base a la pertenencia a grupos de DA específicos para los que está autorizado el Acceso Remoto.

Las características de Acceso Remoto para las empresas externas son las siguientes:

Entorno	Sitio	Usuario a utilizar	Requiere doble factor de autenticación	Comprobación de requisitos de puesto
AREX	**arex.ar.madrid.org**	Login corto (samaccountname)@salud.madrid.org	**SÍ**	**SÍ**

Además de la instalación del software en su equipo, el usuario final debe realizar el proceso de enrolado del teléfono en el segundo factor de autenticación de Microsoft. Si no lo ha realizado, se deberán seguir los pasos indicados en el documento *2FA – Guía de Usuario.*

Para la instalación del Agente de GlobalProtect será preciso un usuario que posea suficiente nivel de privilegios para ejecutar la instalación en la máquina local. En caso de que el usuario no los posea deberá solicitar su instalación a un técnico de su organización con permisos de administración a su puesto de trabajo.

Para poder utilizar la conexión de acceso remoto, el servicio verifica las condiciones de seguridad mínimas requeridas por Madrid digital, que inicialmente son:

Perfil Cumplimiento Postura de Seguridad	**PC_Externo_Compliant**
Requisito de Seguridad	**Criterio**
Servicio actualización software activo	**Windows Update** • Instalado • Habilitado • Nivel parcheado: Instalado algún parche de S.O.
Firewall Windows activo	**Firewall Windows** • Instalado • Habilitado
Antivirus Corporativo active	**Software Anti-Malware (cualquiera):** • Instalado • Protección real-time • Actualizado en los últimos 30 días
Servicio de actualizaciones	**Windows Update** • Instalado • Habilitado • Nivel parcheado: Instalado algún parche de S.O.
Equipo no está unido al DA Institucional	**PC no está en Dominio**: "Madrid.org"
Equipo no está unido al DA Sanidad	**PC no está en Dominio:** "Salud.madrid.org"
Sistemas operativo bajo soporte oficial del fabricante	**Host Info:** Versión de S.O con soporte por el fabricante: • **OS** = Microsoft Windows 10 • **OS** = Microsoft Windows 11 • **OS** = Otras versiones Windows No permitidas

3 Procedimiento de instalación

Este procedimiento describe las tareas necesarias para llevar a cabo la instalación de Agente GlobalProtect version 6.1.0 en un equipo remoto.

Tareas de instalación:

1. Conexión al Portal GlobalProtect
2. Descarga del software de instalación
3. Ejecución del fichero instalable
4. Configuración inicial y directorio de Instalación
5. Finalizar el proceso de instalación
6. Ejecutar el agente GlobalProtect

3.1 Conexión al Portal GlobalProtect

- La descarga del Agente GlobalProtect se realiza accediendo al Portal AREX desde un navegador web utilizando el protocolo https.
- Para ello, en el navegador se debe introducir la URL del Portal: https://arex.ar.madrid.org
- Al acceder al Portal, es necesario poseer ya unas credenciales de acceso válidas. El navegador muestra una página para introducir el usuario y la contraseña.

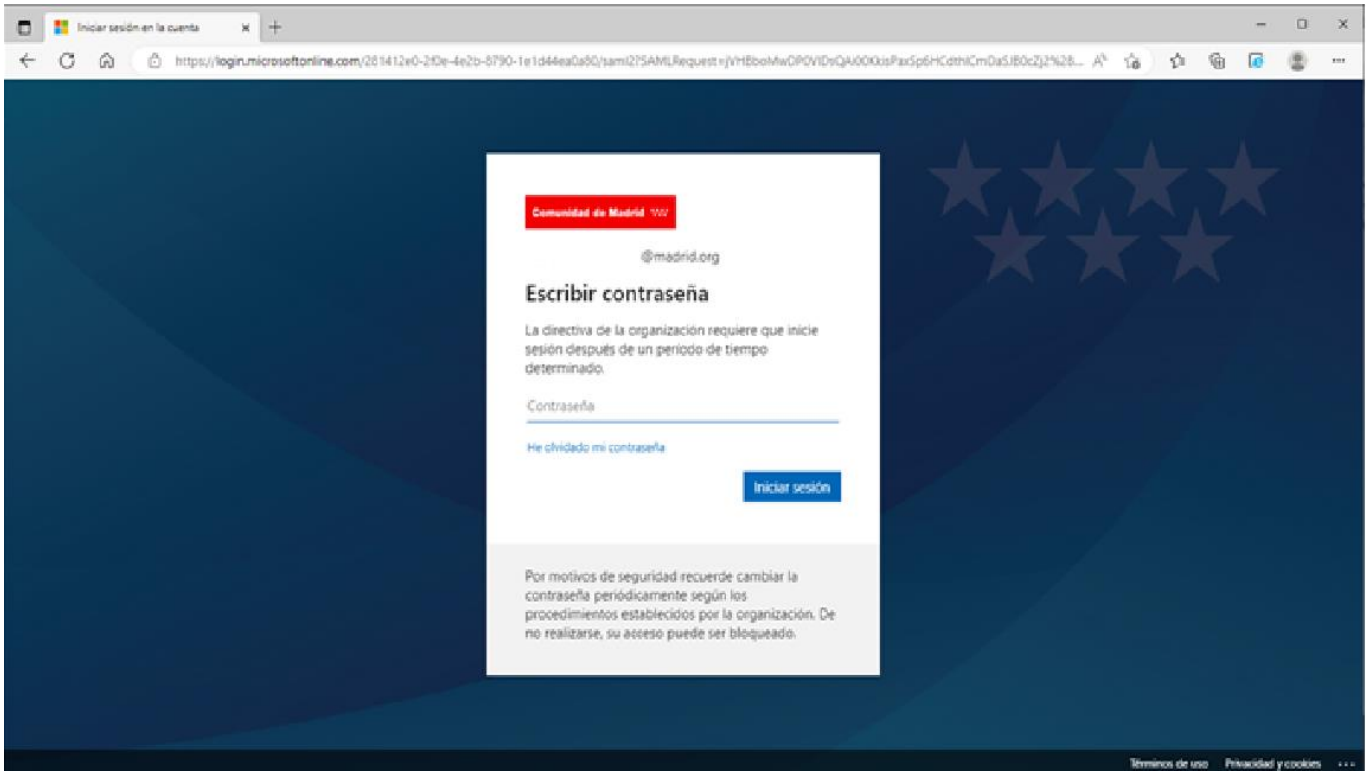


Ilustración 1 Página portal software para introducción de credenciales.

3.2 Descarga del software Paloalto GlobalProtect

- Una vez que se accede al portal de descargas, se muestran la distintas opciones de descarga disponibles.
- Para iniciar la descarga, pulsamos sobre el enlace de la opción adecuada para la version de S.O. de nuestro equipo remoto.

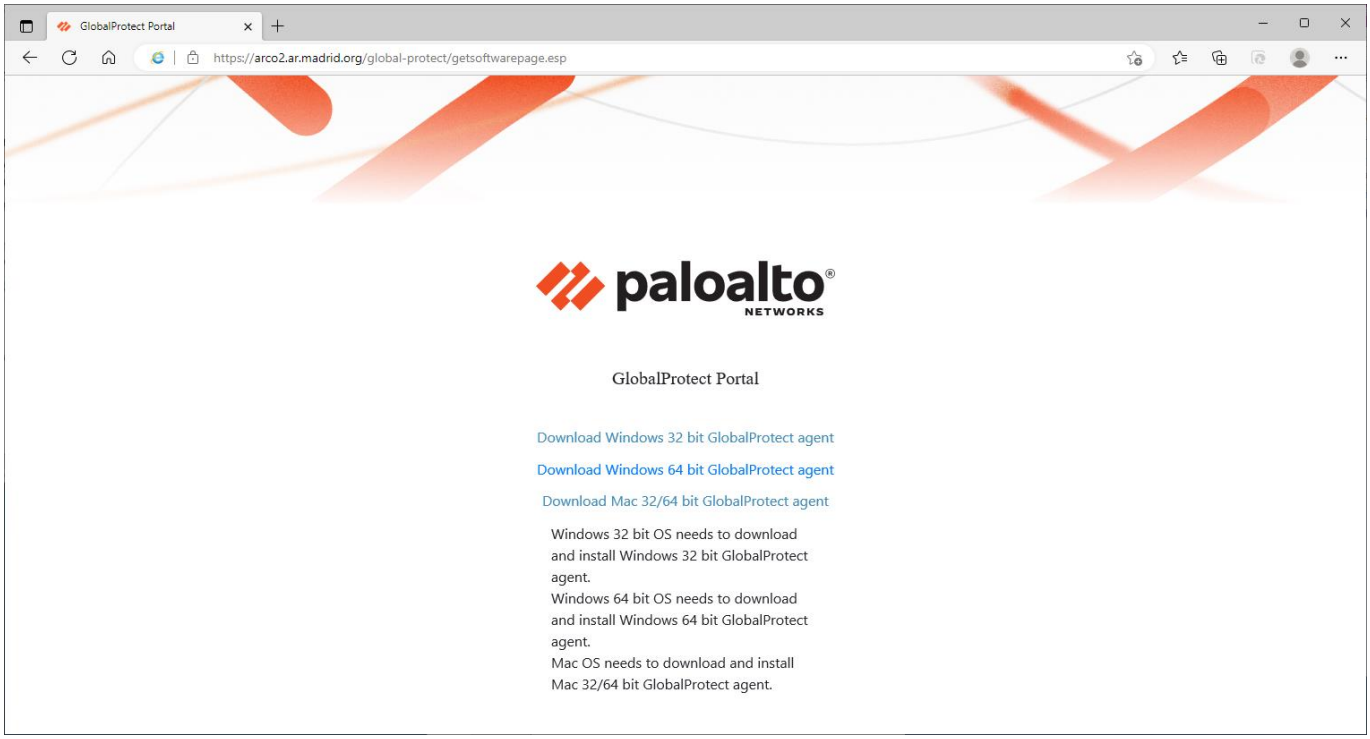


Ilustración 2 Página portal de descarga Agente GlobalProtect

Ilustración 3 Versiones de Software Agente GloalProtect

- A continuación, se inicia la descarga del archivo de instalación.

3.3 Ejecución de fichero instalable

- Una vez finalizada la descarga del archivo de configuración procedemos a ejecutar el archivo de instalación.
- Seleccionamos Ejecutar para iniciar el Wizard de instalación GlobalProtect.

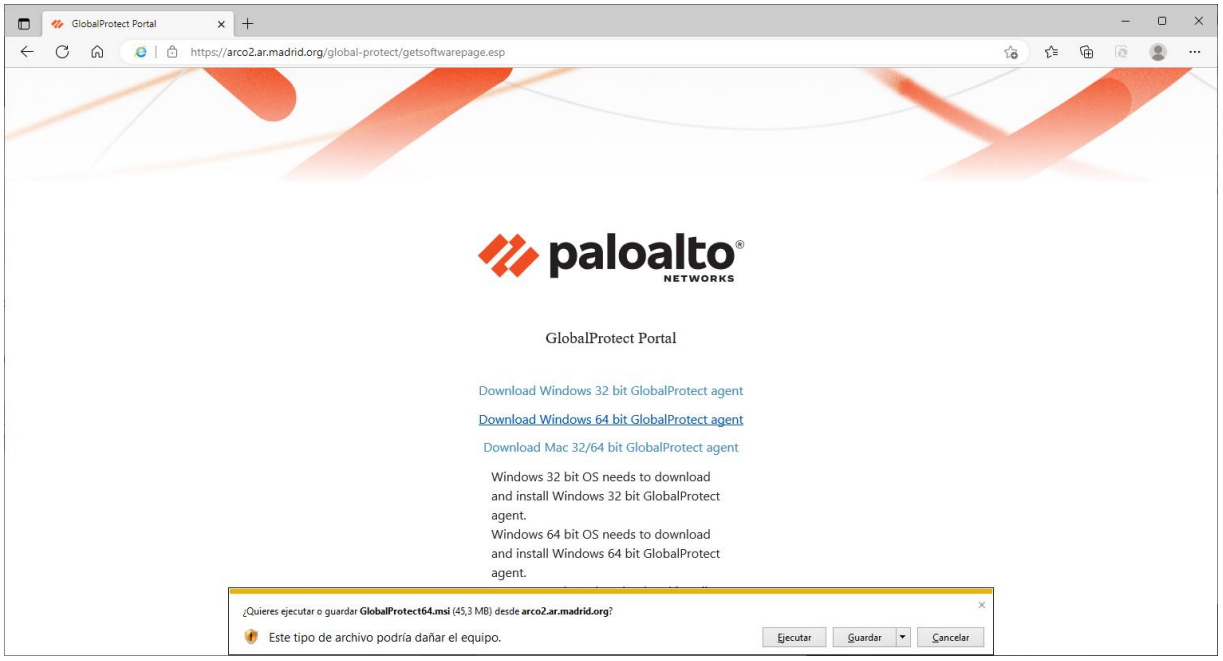


Ilustración 4 Prompt para ejecución de instalador del Agente GlobalProtect

NOTA: En este punto es posible que sea necesario aprobar la ejecución del instalador. Esto depende del nivel de privilegios del usuario en el equipo local.

- A continuación, aparece la pantalla de inicio del instalador del Agente de GlobalProtect. Seleccionamos “Next” para iniciar la instalación.

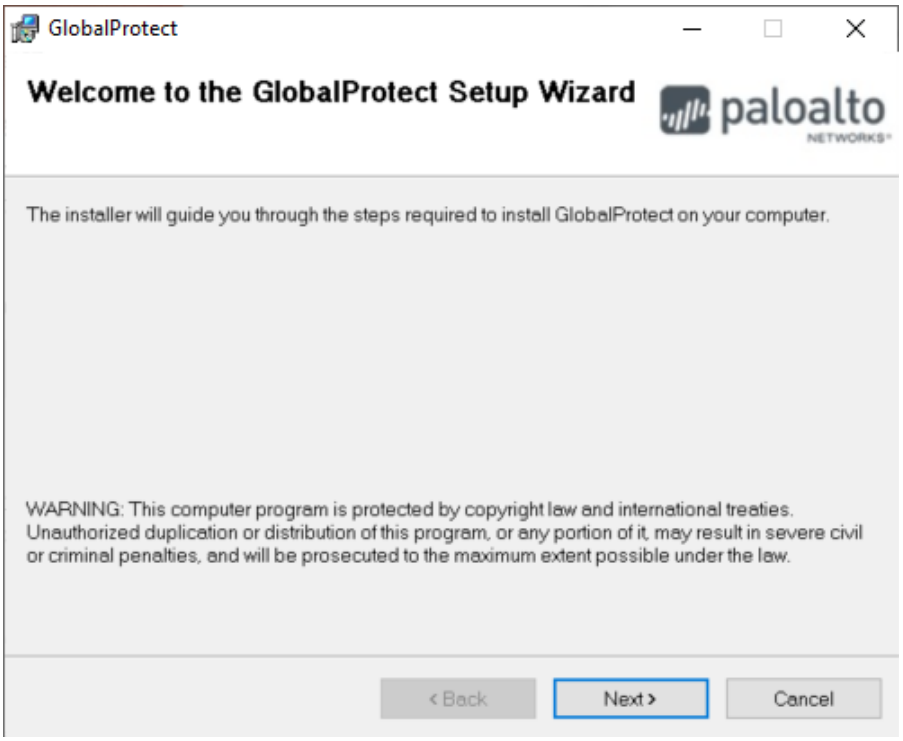


Ilustración 5. Inicio de instalador Agente GlobalProtect

- El instalador solicita información sobre el directorio en el que se desea instalar el software. Se mantiene la ruta que aparece por defecto para la instalación del software (C:\Program Files\Palo Alto Networks\ ) y pulsamos sobre “Next”.

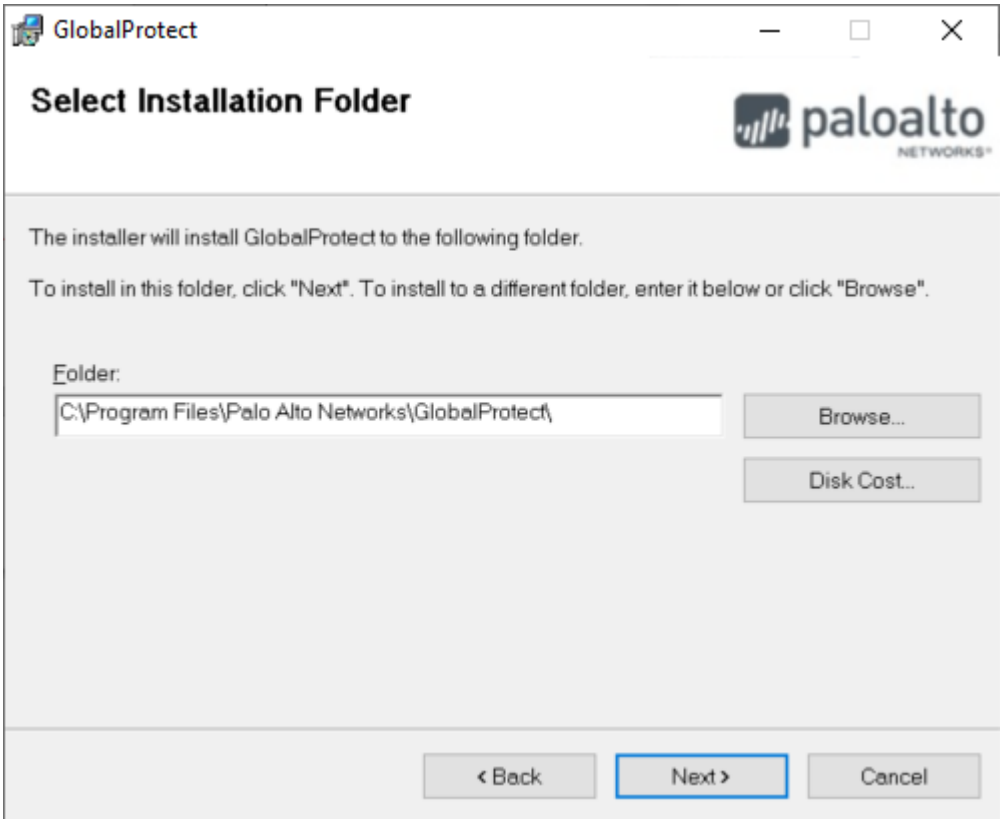


Ilustración 6. Información de directorio de instalación Agente GlobalProtect

- El instalador solicita confirmación para iniciar el proceso de instalación. Pulsamos sobre “Next” para iniciar la instalación.

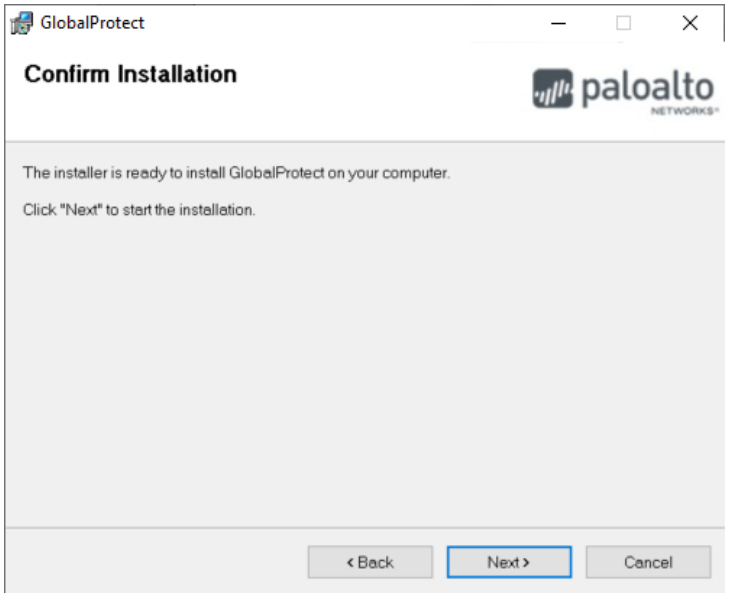


Ilustración 7 Mensaje de aprobación para inicar la instalación del Agente GlobalProtect.

- Se inicia el proceso de instalación se inicia, mostrándose el progreso de la instalación.

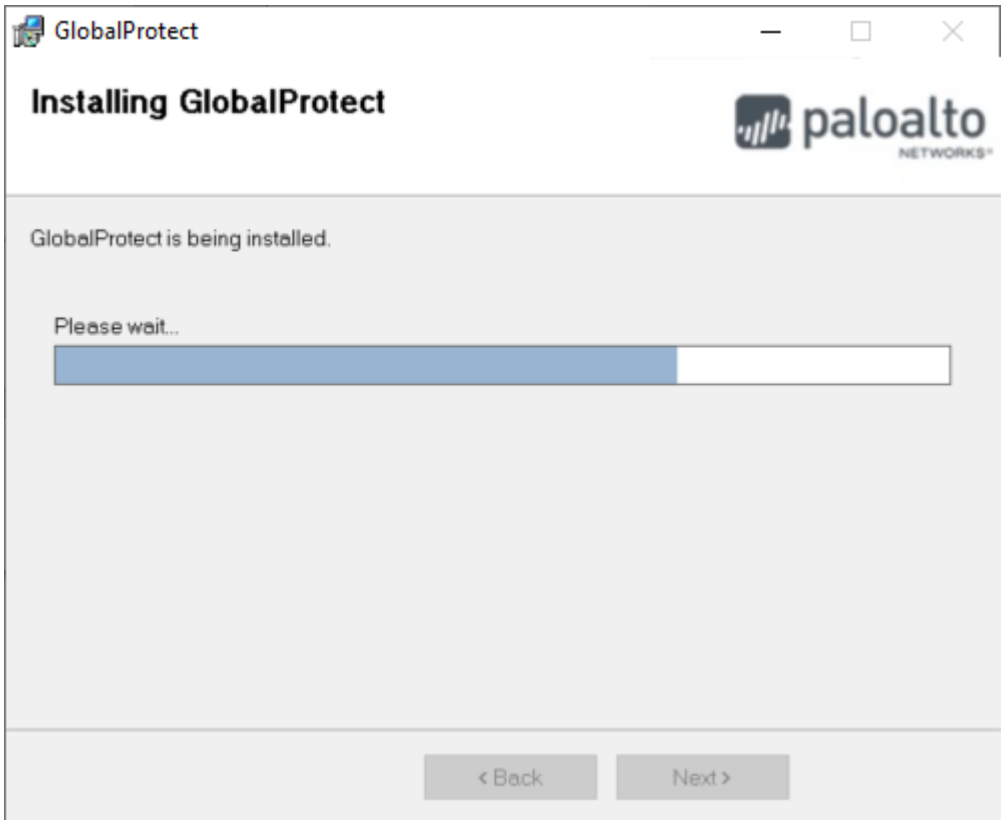


Ilustración 8. Imagen de progreso de instalación del Agente GlobalProtect

- Una vez finalizado el proceso, el instalador informa que el proceso ha finalizado. Pulsamos en botón “Close” para finalizar el instalador.

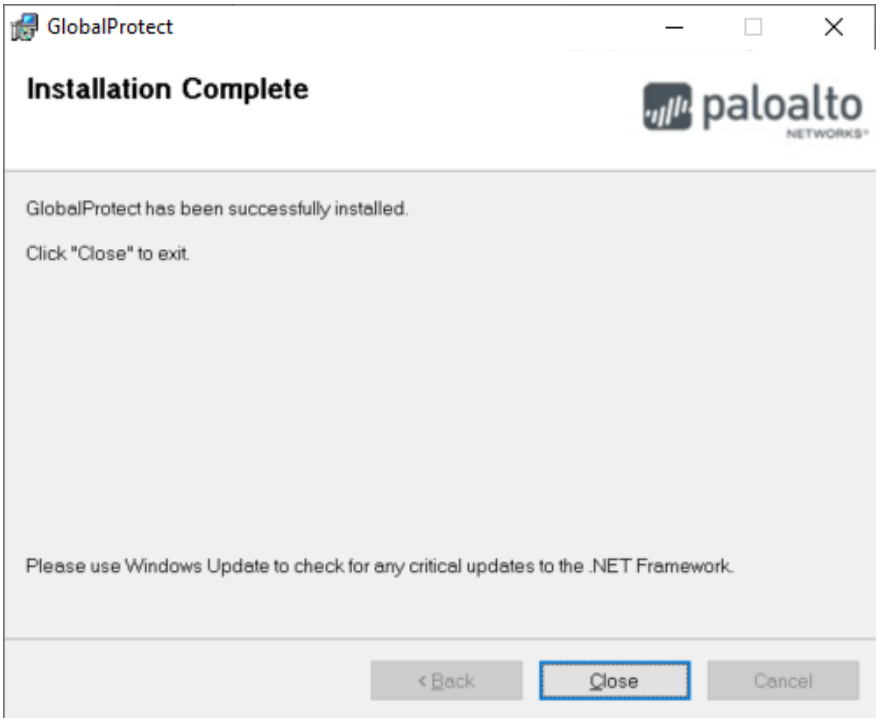


Ilustración 9. Proceso de instalación Agente GlobalProtect finalizado

- Una vez finalizada la instalación, se ejecuta automáticamente el Agente GlobalProtect, mostrándose el mensaje de bienvenida.

Ilustración 10. Mensaje de bienvenida del Agente GlobalProtect

- Pulsamos sobre “comenzar” para iniciar la conexión remota,

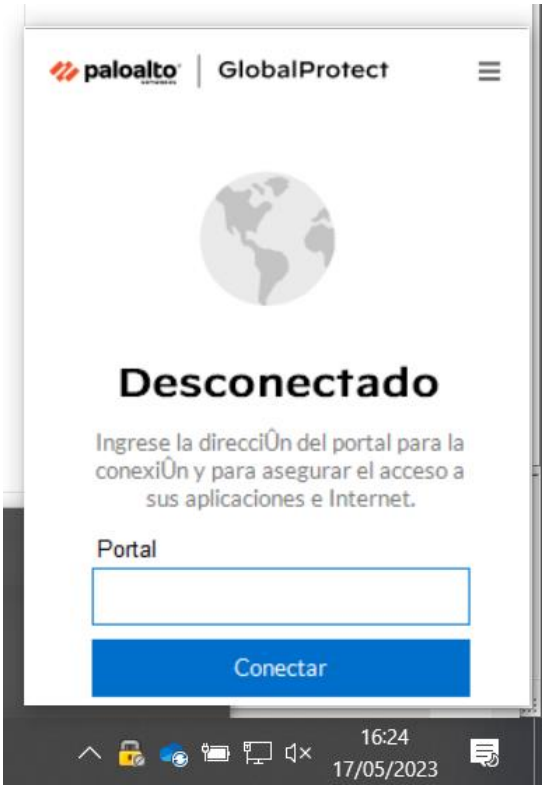


Ilustración 11 Pantalla de conexión inicial del Agente GlobalProtect

4 Conexión a la VPN

El acceso a la VPN con MFA se realiza con el cliente *Paloalto Global Protect,* que deberá estar instalado previamente en nuestro equipo.

El procedimiento para la conexión a la VPN con MFA es el siguiente:

1. Que el Agente de acceso remoto PaloAlto GlobalProtect se esté ejecutando en el equipo, **sin ninguna otra VPN levantada.**
2. Introducir la URL del Portal de Acceso Remoto.
3. Introducir el primer factor de autenticación (Usuario/Contraseña de Dominio)
4. Introducir segundo factor de autenticación
5. Comprobación de conexión VPN establecida

A continuación, se detallan los pasos a seguir para la conexión a la VPN con MFA:

4.1 Ejecutar Agente de acceso remoto GlobalProtect

- Abriremos la aplicación cliente de GlobalProtect e introduciremos la URL del portal de acceso remoto **arex.ar.madrid.org**, que es el sitio donde se requerirá MFA para acceder.
- Para ello tenemos dos posibilidades:

1. Desde el Menú Inicio, buscamos la carpeta Palo Alto Networks y abrimos la aplicación GlobalProtect.

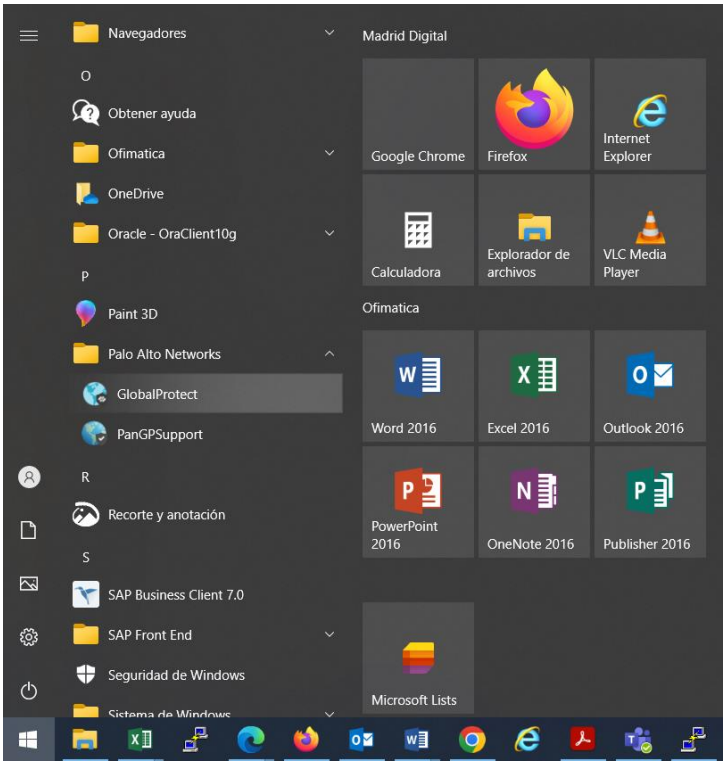


Ilustración 1 Ejecutar Agente GlobalProtect desde menú Inicio de Windows

2. Desde la barra de tareas, desplegamos para ver todas las tareas en ejecución y seleccionamos el icono de Globo gris.

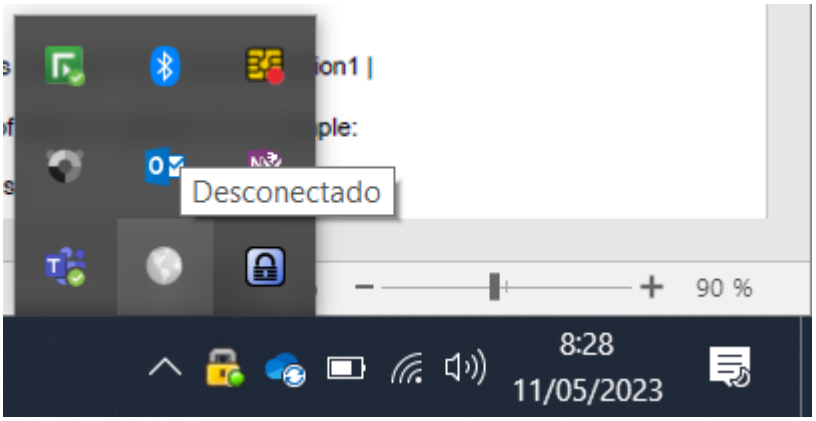


Ilustración 2 Icono de GlobalProtect en barra de tareas

- En ambos casos, se despliega una ventana con el menú básico de conexión, con el Campo “Portal” vacío.

Ilustración 3 Menú inicio conexión VPN Agente GlobalProtect

- En el campo vacío introducimos la URL (Dirección de Internet) para la conexión con el Servicio de Acceso Remoto MFA y pulsamos “Conectar”

  URL de Acceso: arex.ar.madrid.org

- Una vez pulsado sobre “Conectar” se lanza la conexión al Portal de Acceso Remoto para iniciarse el proceso de autenticación MFA.

Ilustración 4 Proceso de conexión e inicio de autenticación VPN

- A continuación, aparece una pantalla en la que se solicita el primer factor de autenticación, que corresponde con las credenciales de credenciales de acceso al dominio. Aquí debemos introducir:

  Usuario: Usuario de Inicio de Sesión en el dominio de MADRID o SALUD (DNI@[salud].madrid.org)

  Contraseña: Contraseña asociada

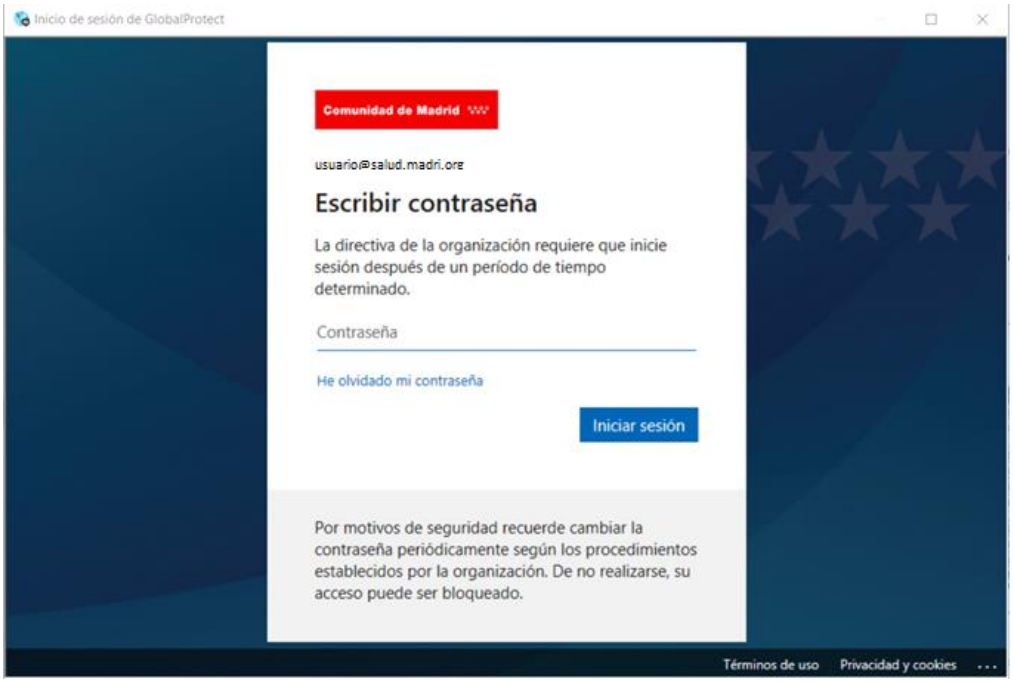


Ilustración 5 Pantalla para inicio de sesión con credenciales mediante MFA

- Si las credenciales de acceso introducidas como primer factor de autenticación son correctas, el cliente solicitará a continuación el segundo factor de autenticación.

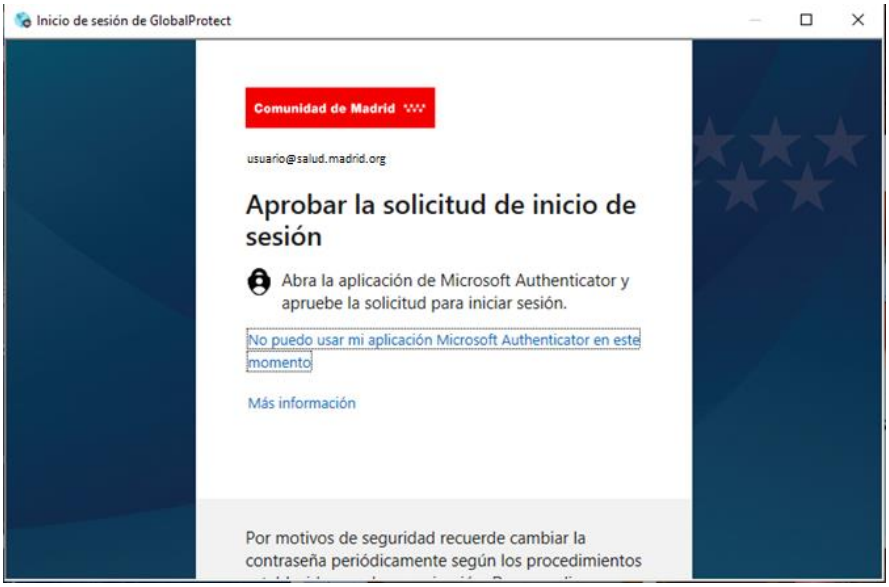


Ilustración 6 Solicitud de segundo factor de autenticación mediante aplicación MS Authenticator

- Este segundo factor de autenticación dependerá del método de autenticación predeterminado seleccionado durante el proceso de *enrolado* del teléfono móvil en el servicio de segundo factor de autenticación de Microsoft. (Si no lo ha realizado, se deberán seguir los pasos indicados en el documento *2FA – Guía de Usuario*).

- Por ejemplo, si el método de autenticación seleccionado es MS-Authenticator, aparecerá un mensaje indicando que se debe aprobar la solicitud de inicio de sesión en la aplicación Authenticator del móvil

Ilustración 7 Solicitud para aprobar el inicio de sesión en MS Authenticator instalado en el móvil.

NOTA: Existe un tiempo de espera para la confirmación/introducción del segundo factor de autenticación. Transcurrido ese tiempo se deniega el inicio de sesión y se finaliza el proceso de conexión. Siendo necesario volver a iniciar todo el proceso de Conexión.

- Una vez introducido el segundo factor de autenticación de forma satisfactoria el proceso de autenticación finaliza y se inicia la conexión VPN.
- La aplicación muestra el progreso del proceso de conexión a la VPN MFA. Durante este proceso se realizan varios chequeos de seguridad en el equipo cliente, así como, la configuración de los parámetros de la VPN.

Ilustración 8 Pantalla con información de proceso de conexión VPN.

- En el caso de que las comprobaciones de seguridad del equipo cliente sean satisfactorias y las configuraciones de la VPN se hayan podido realizar, se establece la conexión, teniendo el usuario acceso a los recursos corporativos autorizados asociados a la pertenencia del mismo a un grupo de Directorio Activo.

NOTA: En el caso de ocurrir cualquier error o no conformidad en el proceso de establecimiento de la VPN se recibirá un mensaje indicando el problema. En este caso la VPN no se establece y el usuario no tiene acceso a los recursos corporativos autorizados.

- Si la conexión se establece satisfactoriamente, la aplicación GlobalProtect muestra un mensaje indicando “Conectado” junto con la información del equipo central al que se ha conectado. El icono GlobalProtect de la barra de tareas cambia su color gris a azul claro para indicar que se está conectado a la VPN.

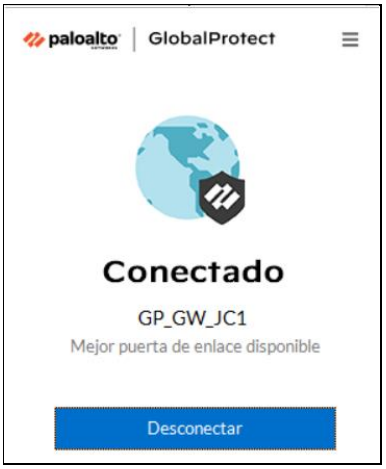


Ilustración 9 Mensaje de establecimiento de VPN correcto en el agente GlobalProtect

Ilustración 10 Aspecto del icono de GlobalProtect con VPN establecida

5 Verificación de la conformidad

- El servicio de acceso remoto se ha diseñado para que se evalúe la conformidad de seguridad (*posture)* del equipo remoto según los requisitos de seguridad definidos que determinan si el equipo cumple con un nivel de seguridad considerado aceptable.
- El resultado de la evaluación de la postura de seguridad determina si el equipo cumple con los requisitos mínimos de seguridad y por tanto está autorizado para acceder a los recursos corporativos a través de la VPN.
- La evaluación de seguridad se realiza durante la fase de conexión remota. Una vez que el usuario se registra, el servicio de acceso remoto identifica el entorno al que pertenece el usuario, así como el grupo de DA del que es miembro para determinar las medidas de seguridad mínimas que debe cumplir el equipo remoto.
- Para ello, el agente GlobalProtect recopila la información necesaria del equipo remoto. Si el resultado de la evaluación es favorable, se concede el acceso remoto a los recursos autorizados.
- En caso de no ser favorable, el usuario recibe un mensaje indicando que no cumple con la Postura de Seguridad para el entorno al que pertenece, además de información sobre la medida de seguridad que no cumple. En este caso, la conexión VPN se mantiene establecida, pero se deniega el acceso remoto a los recursos corporativos.

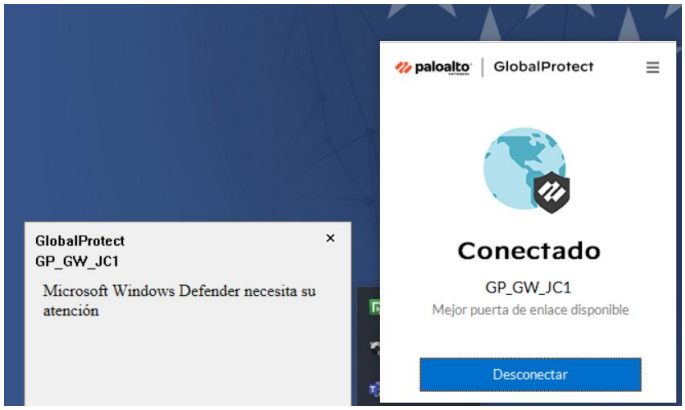


Ilustración 11 Posible mensaje de aviso sobre el estado de seguridad del equipo local

- Para obtener más detalle sobre el estado de la conexión debemos acceder al menú de configuración del Agente GlobalProtect

Ilustración 12 Acceso a Menú de Configuración Agente GlobalProtect

- Desde aquí, accedemos a la pestaña de “Notificaciones” para visualizar todos los avisos de seguridad recibidos.
- Como vemos en el siguiente ejemplo, se indica al usuario que el Servicio “Microsoft Windows Defender” no cumple con el estado de seguridad definido y necesita ser revisado.

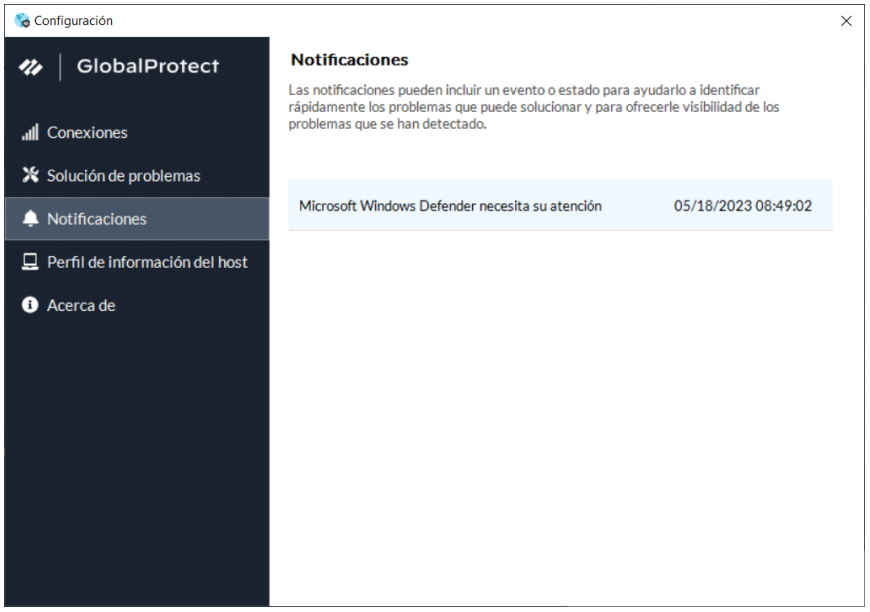


Ilustración 13 Menú de Notificaciones Agente GlobalProtect

6 Depuración de errores

- El Agente GlobalProtect permite recopilar información de registros de actividades para realizar depuraciones de errores.
- Para ello, desde el menú configuración accedemos a la sección “Solución de Problemas”, seleccionamos la opción “Logs de depuración” y pulsamos “Recopilar registros”.

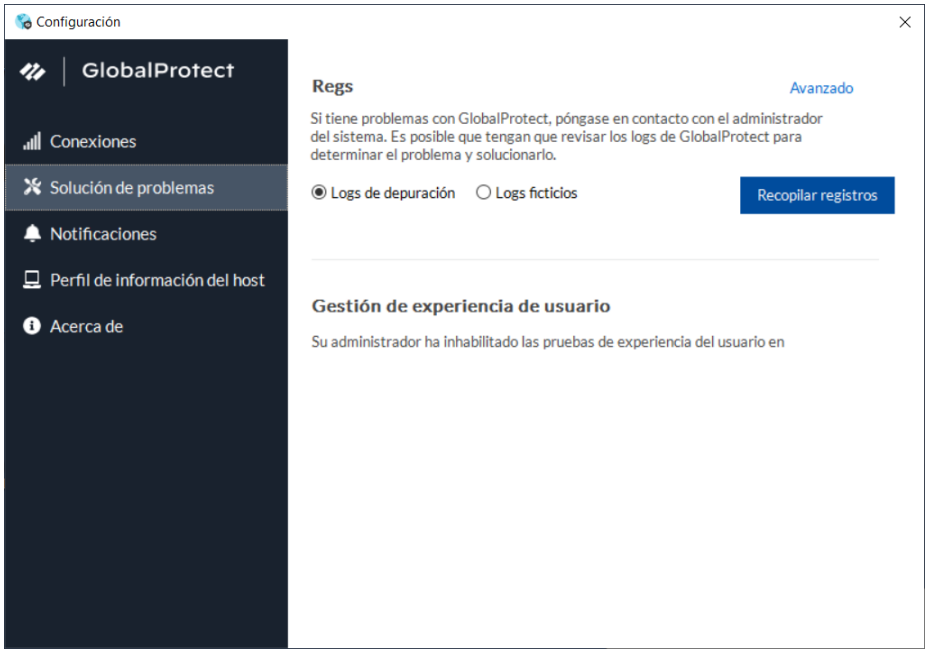
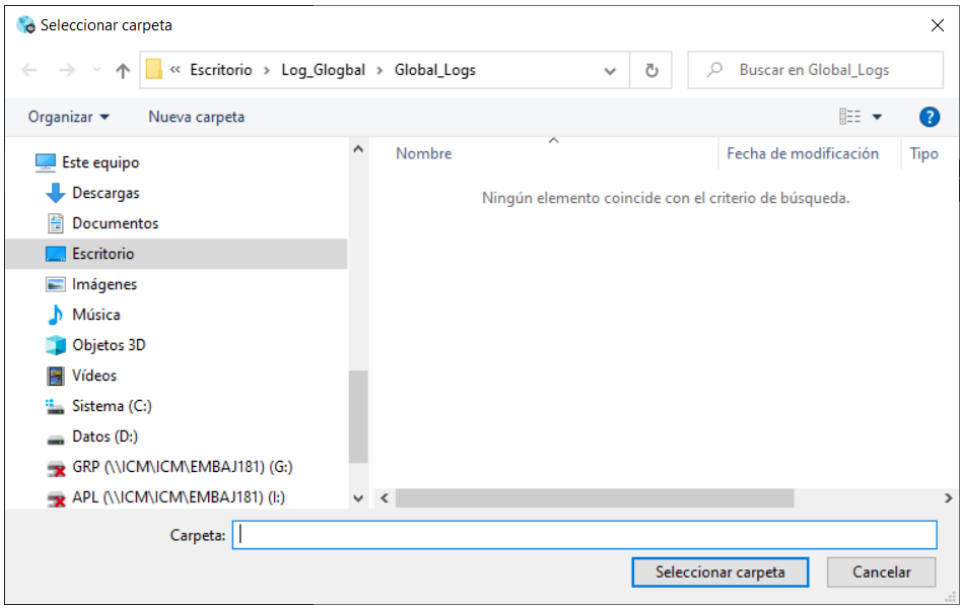


Ilustración 14 Menú de solución de problemas del Agente GlobalProtect

- Indicamos el directorio dónde se guardarán los registros recopilados.



- Una vez seleccionada la carpeta destino, se exportan los ficheros con la información necesaria para la depuración de los errores.

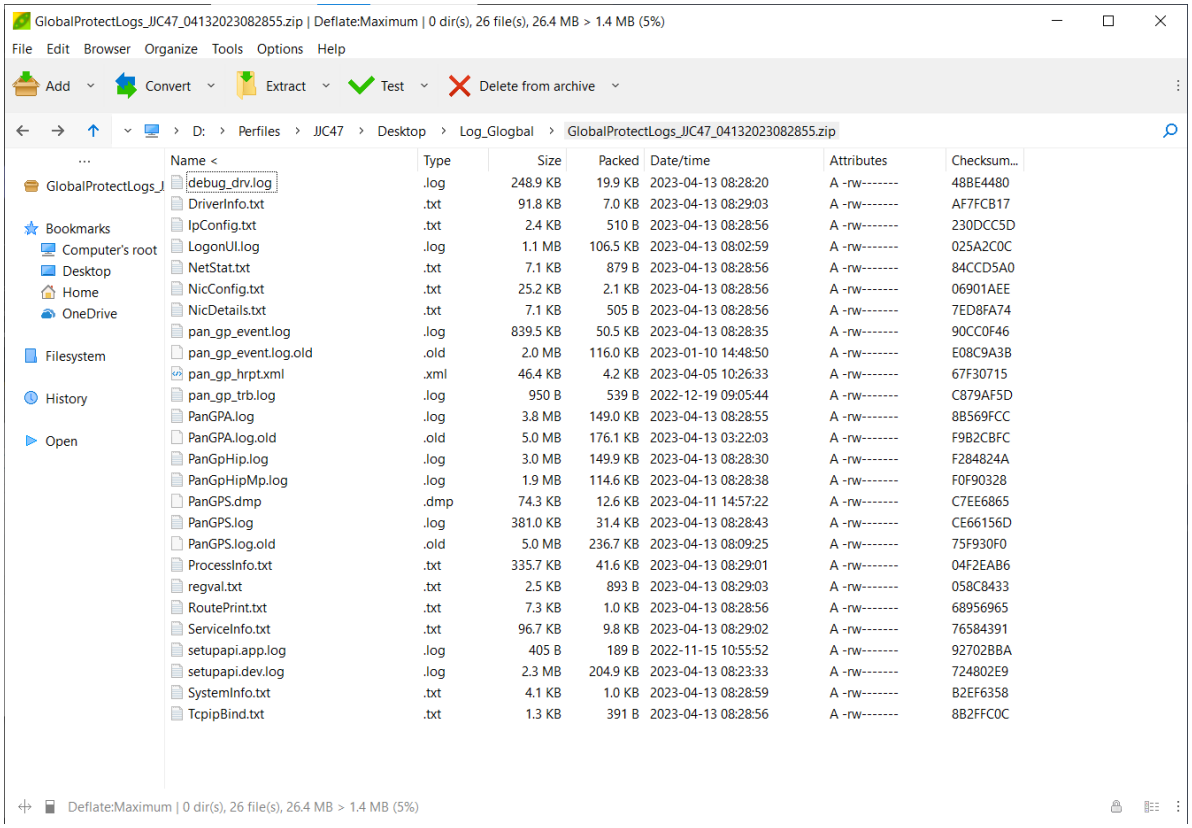


Ilustración 15 Ficheros generados para la depuración de errores desde el Agente GlobalProtect

- Cada uno de estos ficheros recoge información del proceso de conexión, autenticación, estado, etc.. del Agente GlobalProtect y se utilizan para detectar la causa del problema.

FIN DEL DOCUMENTO