Despliegue con GPO de Active Directory

Se mostrarán los procedimiento para llevar a cabo la instalación, actualización y desinstalación del agente usando el GPO de Active Directory.

- Aparición en programas instalados
- Monitoreo del agente
- Inicio del agente
- Actualización del agente
- Qué se actualizará
- Propiedades de la actualización
- Inventario de aplicaciones
- Verificación de la actualización
- PowerShell para verificar actualización
- Actualización en listado de Aplicaciones
- Desinstalación del agente
- Verificación de la desinstalación

Requisitos previos

Antes de ejecutar cualquier procedimiento en el **Active Directory** es importante tener en cuenta los siguientes requisitos previos:

Debe contar con la capacidad de realizar acciones administrativas en **Active Directory** y opcionalmente en los computadores de la organización. En teoría, para llevar a cabo el despliegue de nuestro agente no se requiere realizar ninguna acción en los PC de los empleados, sin embargo, en la primera instalación de pruebas quizás quiera forzar la actualización de la política en alguno de los equipos para no tener que esperar mucho tiempo a que se haga de forma natural.

Los computadores de la organización deben estar previamente unidos al dominio, esto significa que ya un administrador de tecnología pasó por el PC y lo ingresó al dominio de la organización y este PC está inventariado en el directorio activo y el empleado cuenta con un usuario de red válido.

En el **Active Directory** ya existe una unidad organizacional bien estructurada, de tal manera que cuando se lleve a cabo el procedimiento de *NOFRAUD*, se puedan seleccionar de forma correcta los dispositivos o usuarios que serán objeto de la metodología antifraude.

Debe copiar o descargar el agente de The Fraud Explorer (normalmente llamado ***endpointInstaller.msi***) al servidor de controlador de dominio desde donde se compartirá a todos los equipos de la organización para que se pueda llevar a cabo su instalación. Es muy importante que de ahora en adelante, cuando el **Active Directory** le pida la ruta del paquete MSI en relación con nuestro agente, use una ruta de red y no una ruta local, es decir, debe usar algo como \\dc.nofraud.la\MSI\endpointInstaller.msi y no C:\MSI\endpointInstaller.msi.

El agente de The Fraud Explorer es compatible con sistemas operativos Windows de 32 y 64 bits, desde Windows 7 en adelante, sin embargo, nuestro agente requiere que el **Framework .NET 4.8** de Microsoft esté previamente instalado en los PC donde se llevará a cabo el despliegue. El Framework .NET viene por defecto instalado en Windows y si el sistema operativo cuenta con los últimos parches es altamente probable que este requisito se cumpla de forma automática y no deba realizar nada. El único escenario donde debería instalarlo manualmente es en caso de que los sistemas operativos no estén actualizados. Puede ejecutar el siguiente comando en una consola PowerShell para saber qué versión se encuentra instalada:

```
reg query "HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP\v4\Full" /v Release
```

Si se cumplen estos requisitos, estamos listos para continuar con la aplicación de los procedimientos.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Video con todos los pasos

En vez de seguir los pasos documentados, también puede optar por visualizar este video.

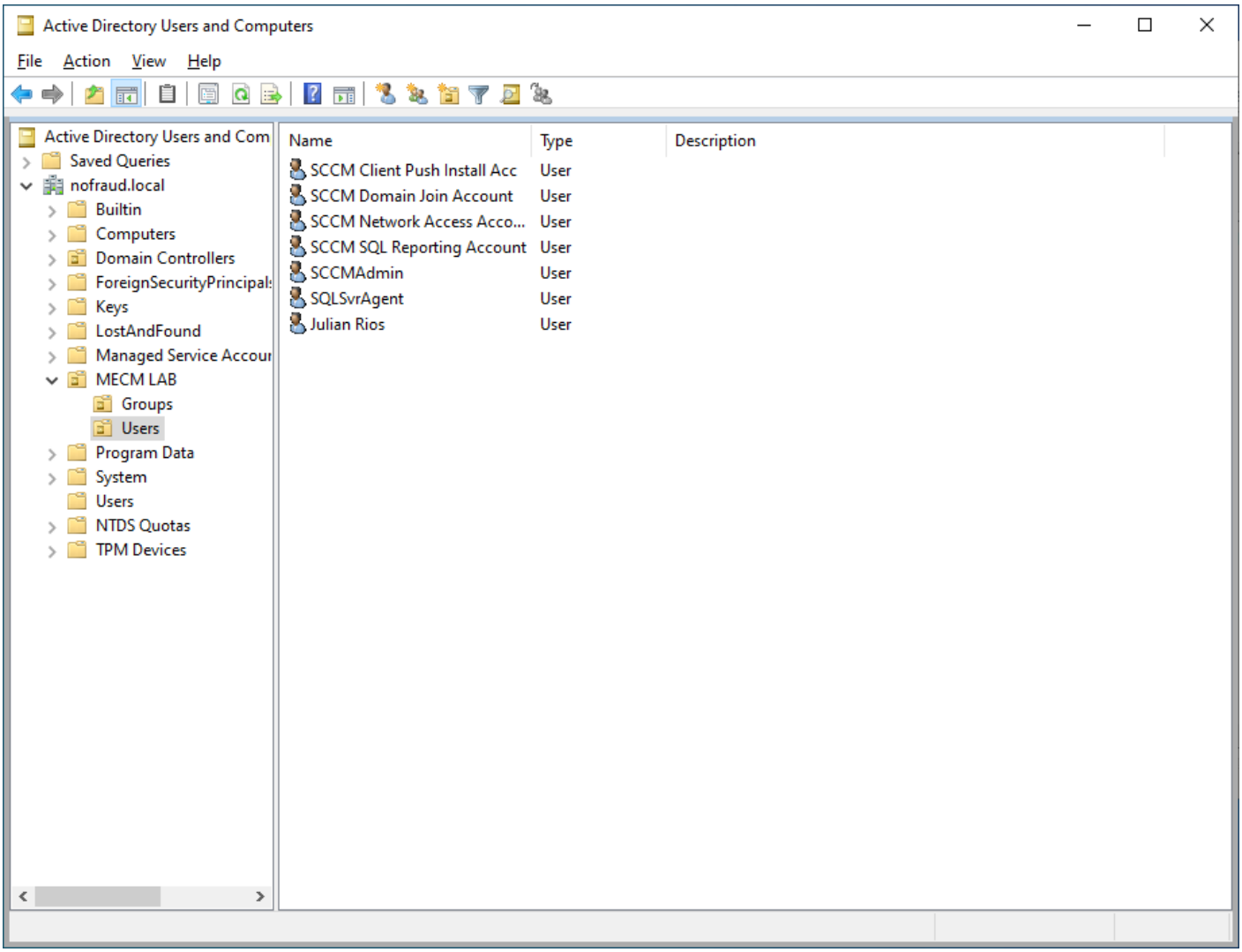
https://www.youtube.com/embed/3f_auPBiPk0?si=AD8aFwC9YYew5vg0

El video contiene todos los pasos de la guía ejecutados de forma práctica y cada uno de los pasos está separado por capítulos.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Abrir Active Directory

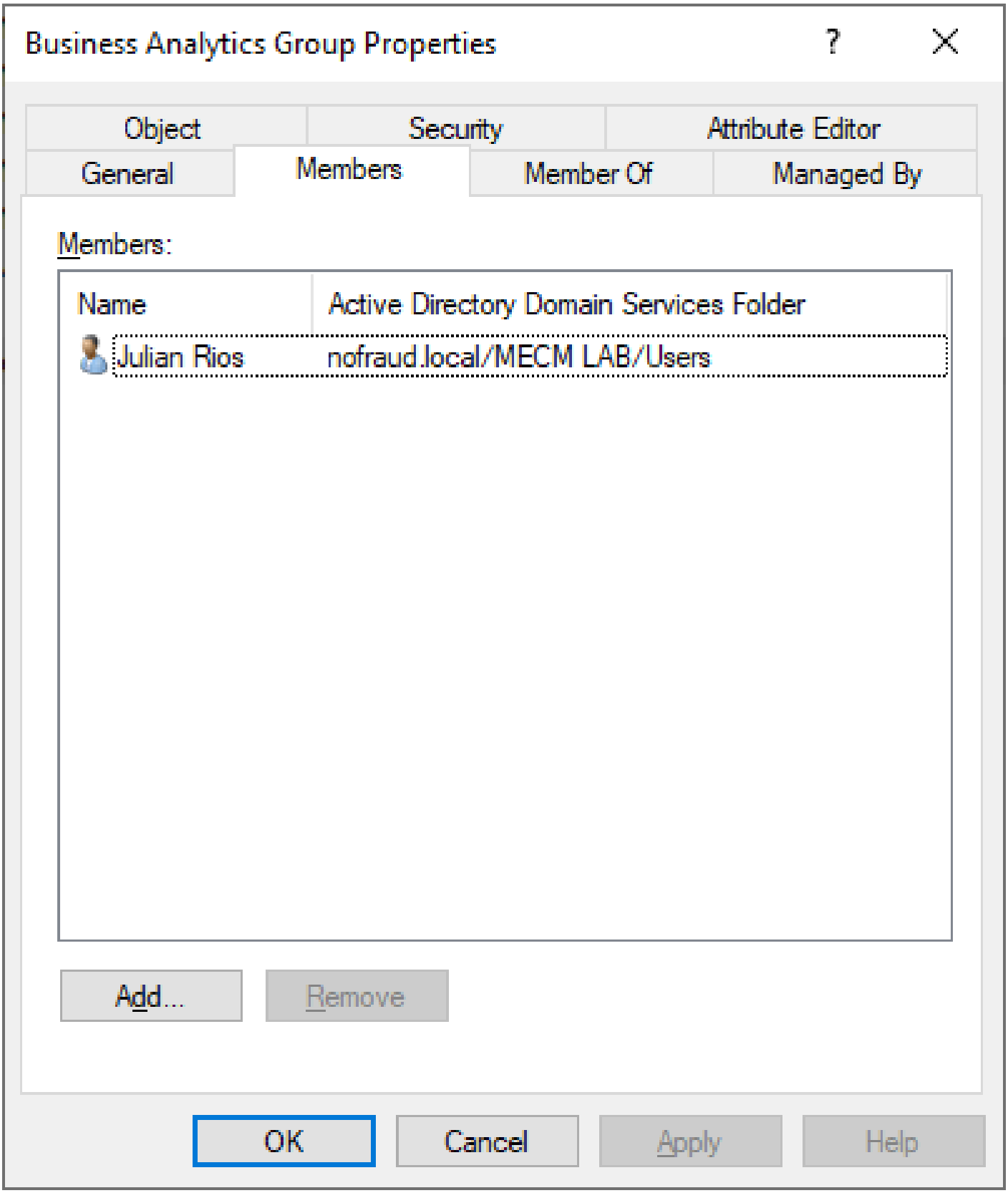
Abra la aplicación **Active Directory users and Computers** en el controlador de dominio y haga clic en la unidad organizativa OU donde se encuentran todos los usuarios.



No importa si existen usuarios que no tendrán la política, más adelante se creará un filtro de seguridad que tendrá una regla para que solamente ciertos usuarios la tengan.

Grupo de seguridad

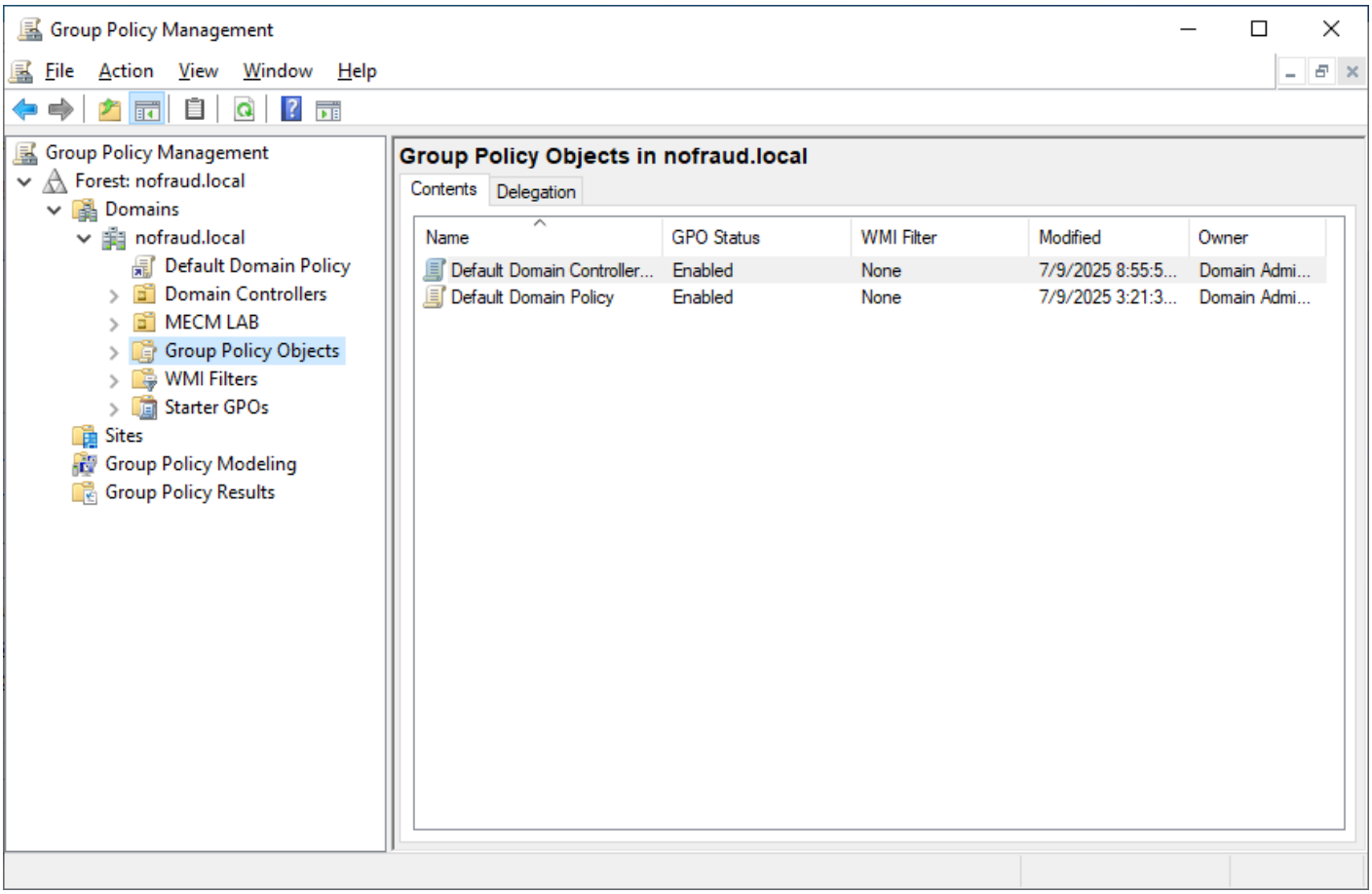
En la OU donde se encuentran todos los usuarios de la organización, cree un **Security Group** con scope **Global** y añada a él los usuarios que serán objeto de la aplicación de la política en la pestaña miembros.



Para crear un grupo de clic derecho en la OU y posteriormente de clic en **New** y luego **Group**.

Creación de la política GPO

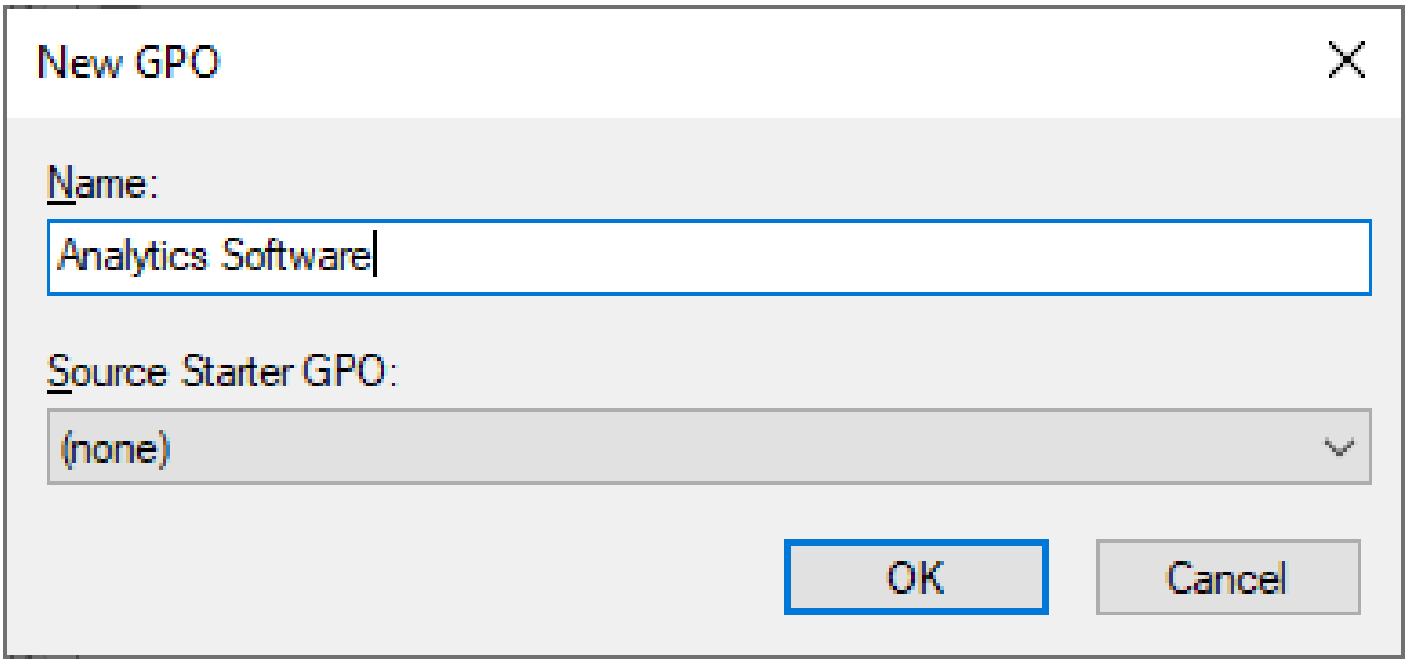
Abra la aplicación **Group Policy Management** para construir la política. Seleccione el bosque por defecto y llegue a la entrada **Group Policy Objects**.



De clic derecho sobre **Group Policy Object** y luego seleccione **New**.

Nombre de la política GPO

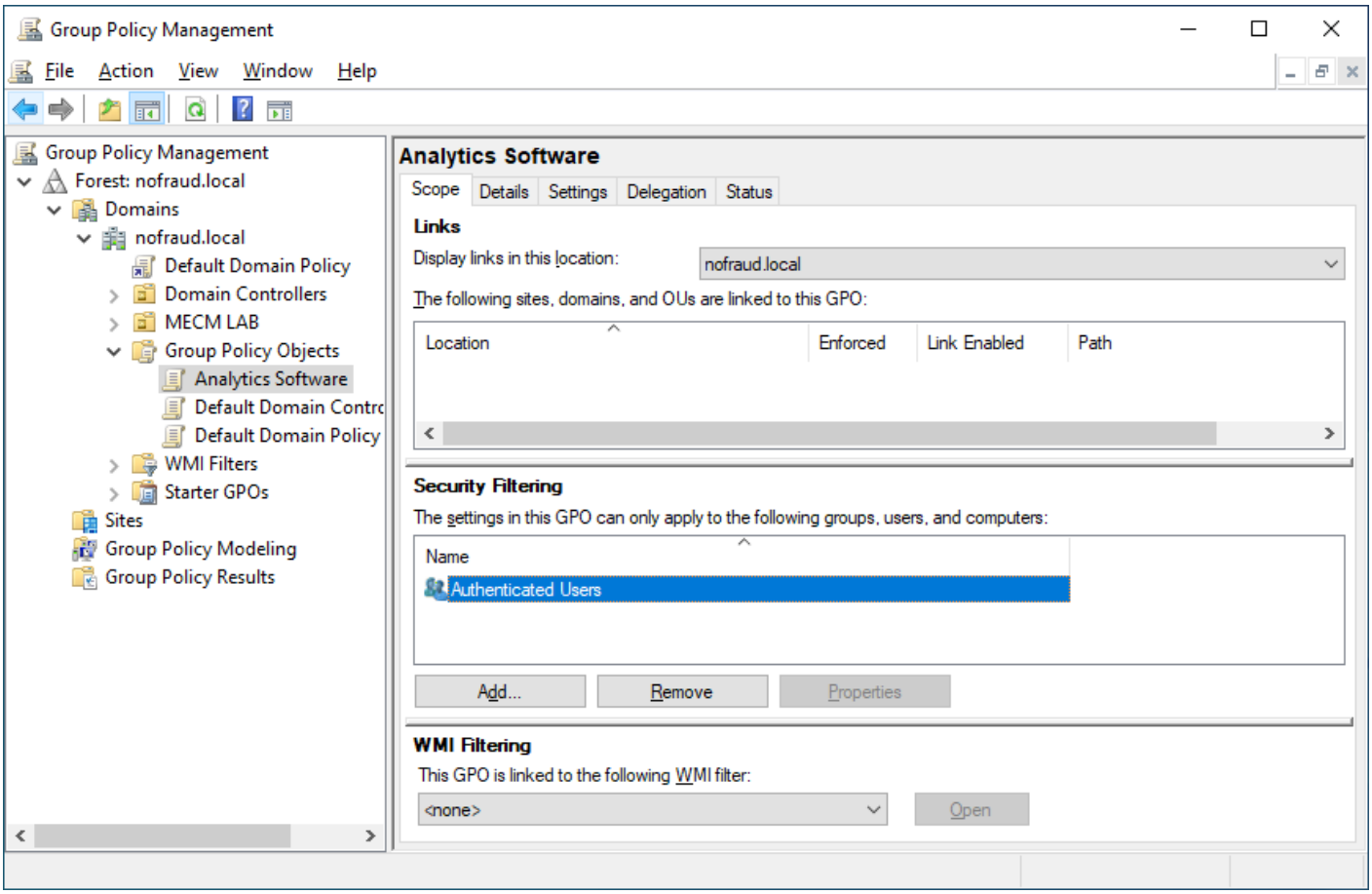
Escriba un nombre para la nueva política de GPO.



Se recomienda usar el nombre **Analytics Software**.

Eliminación del filtro por defecto

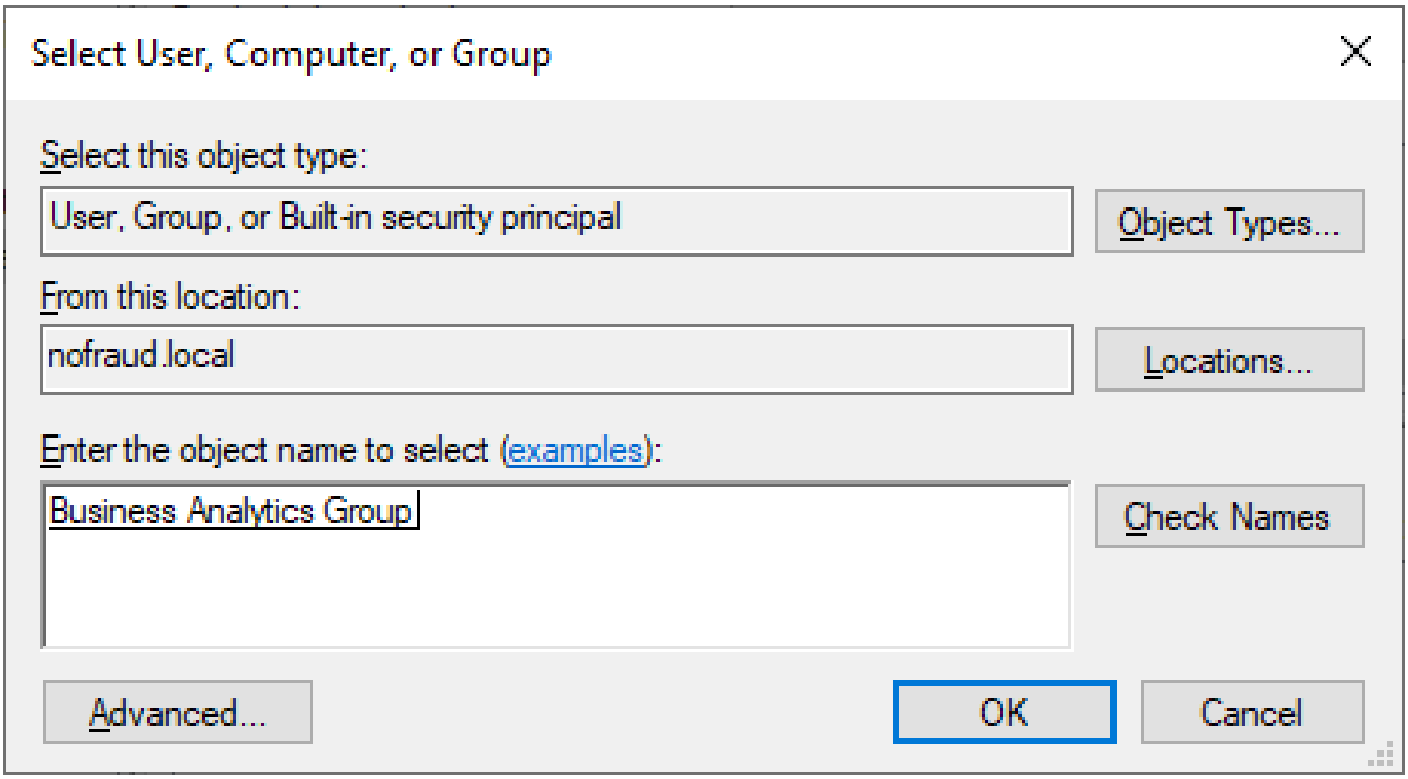
Después de ponerle un nombre a la política, se regresa a la pantalla principal del **Group Policy Management**. Allí, de clic en la entrada **Authenticated Users** dentro del **Security Filtering** y luego presione el botón **Remove**.



Esto eliminará el filtro por defecto para la aplicación de la política. Normalmente la política se aplica a todos los usuarios que se autentiquen en Windows, pero lo que se quiere es poder seleccionar usuarios y ponerlos en un grupo y solo a estos aplicarles la política.

Creación de un nuevo filtro

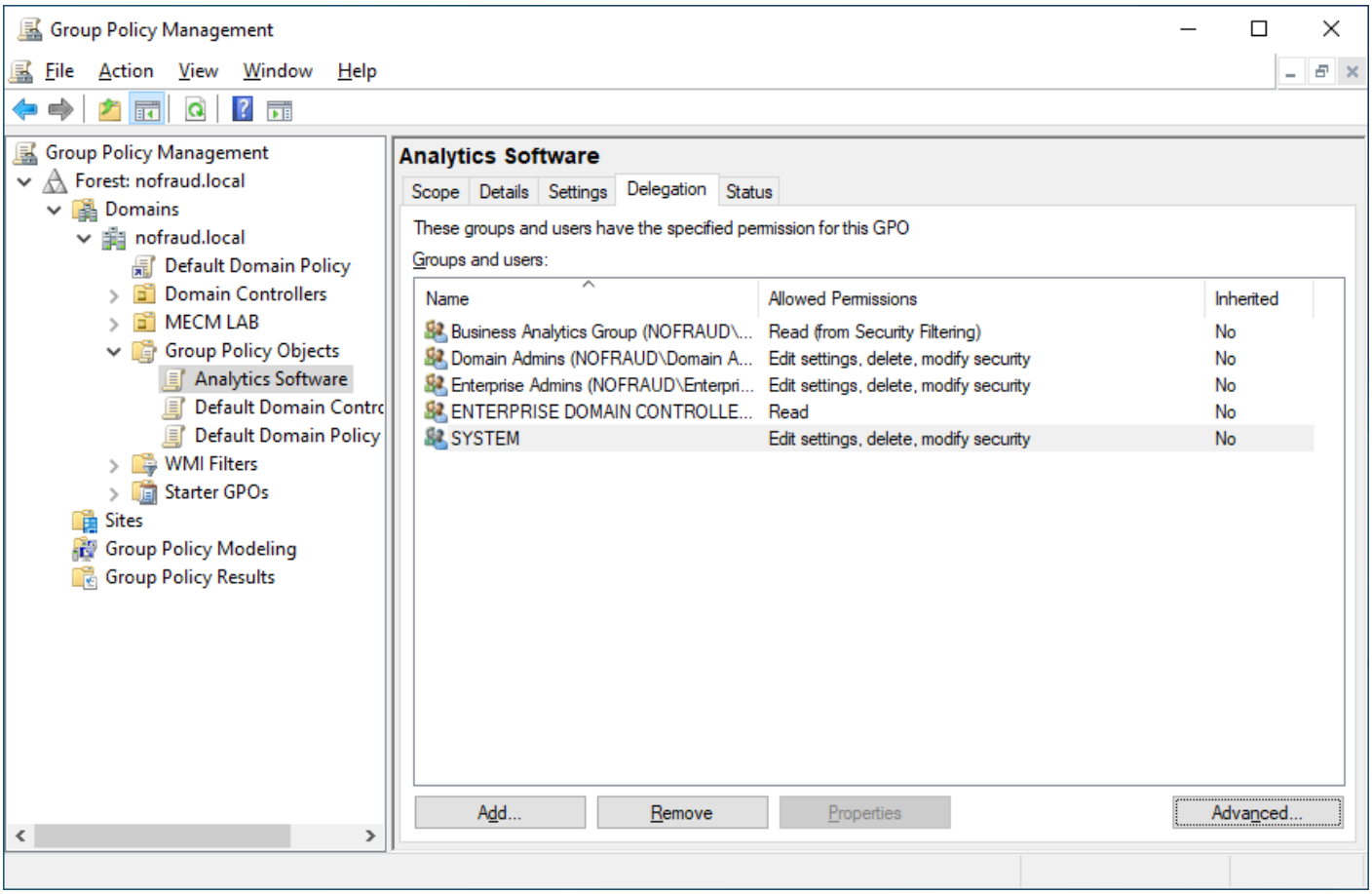
En la pantalla principal del **Group Policy Management**, de clic en **Add** en la sección de **Security Filtering**.



Allí, escriba el nombre del grupo de seguridad que creó con anterioridad y al que agregó como miembros los usuarios a los que desea que se les aplique ésta política.

Delegación

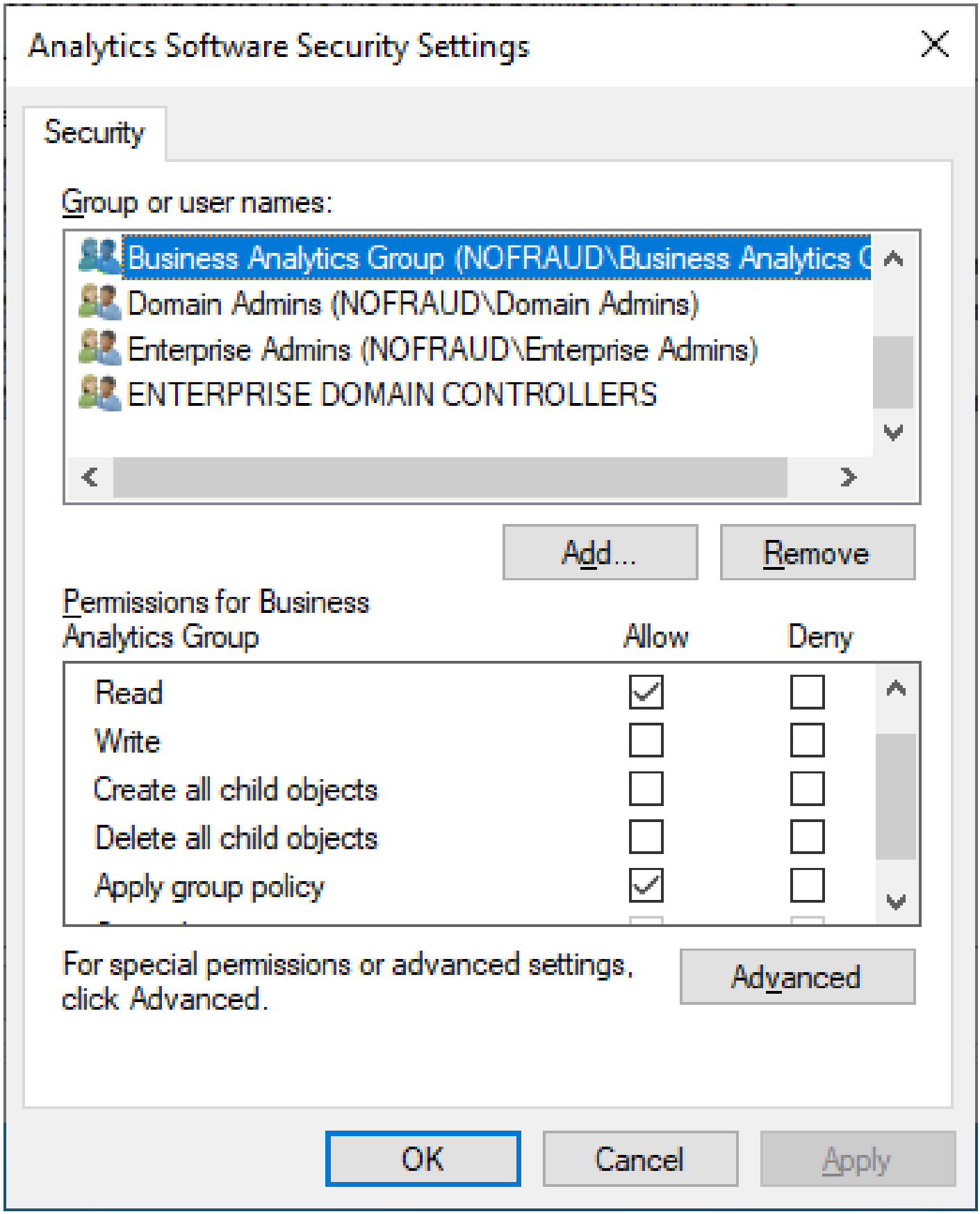
Estando parados en la política recién creada **Analytics Software**, dar clic en la pestaña **Delegation** y luego en el botón **Advanced**.



Se configurará qué grupos tienen permisos para la aplicación de la política.

Delegación del grupo de seguridad

Después de darle clic en **Advanced** en la ventana pasada de **Delegación**, se llega a esta ventana donde deberá darle clic en el botón **Add** y agregar **Authenticated Users** a la lista de Grupos. Asegúrese de que este grupo solamente tiene la opción **Read** habilitada como permitida y los demás deshabilitados.

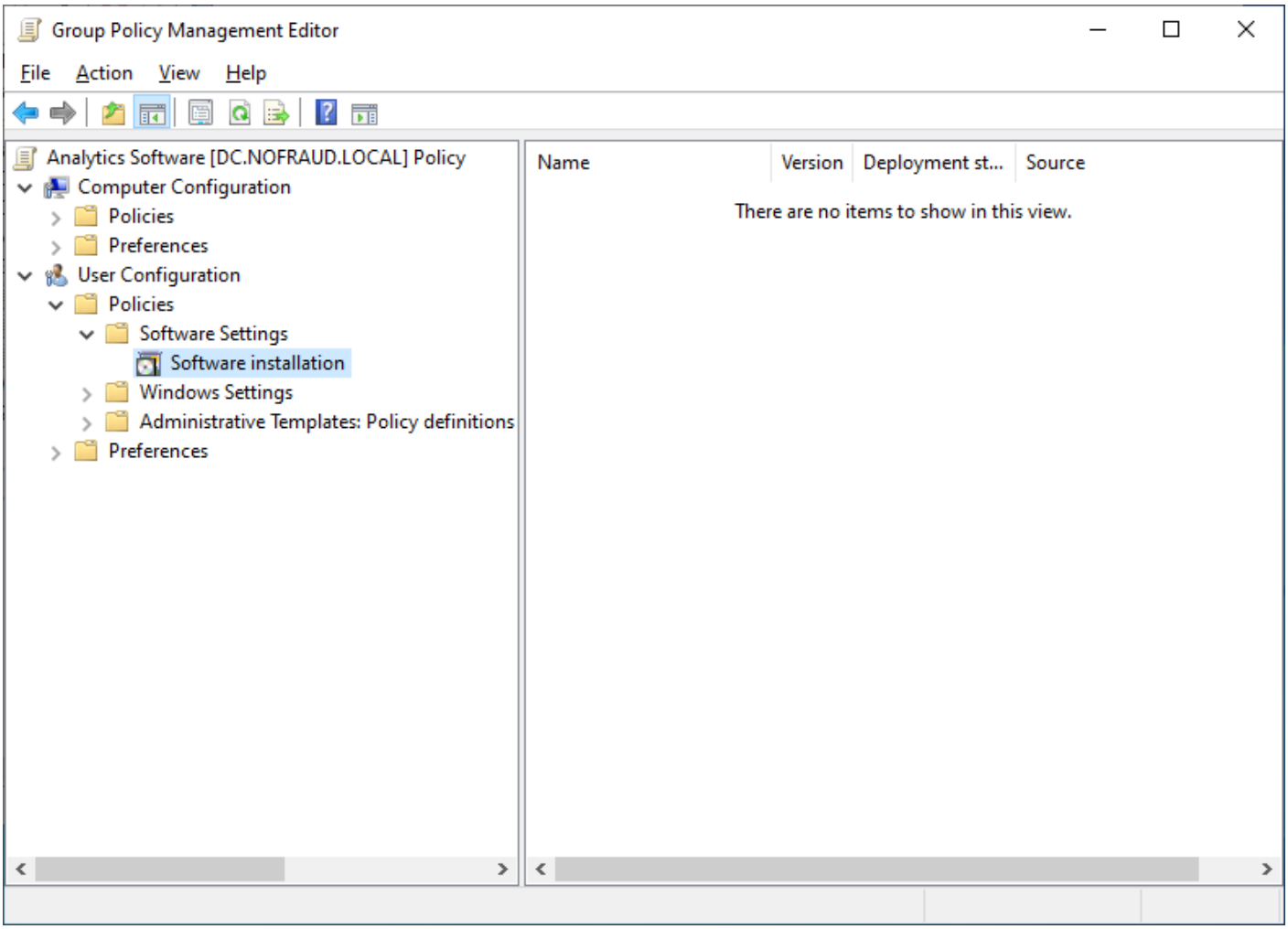


Para finalizar, asegúrese de que el grupo de seguridad creado en el directorio activo, en este caso **Business Analytics Group**, tenga las opciones de **Read** y **Apply group policy** habilitadas.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Edición de la pólitica

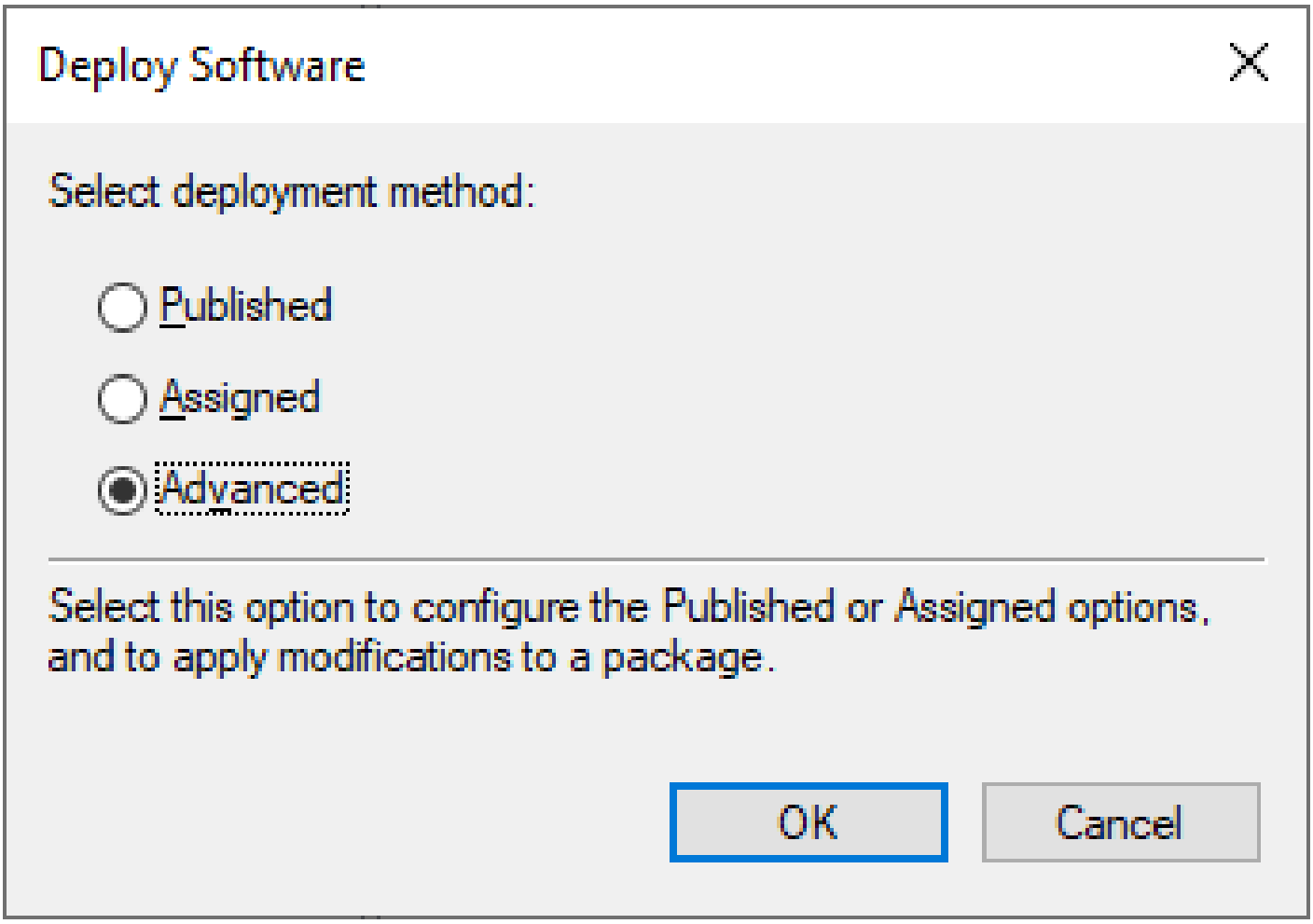
Edite la política dando clic derecho sobre ella y luego en **Edit**.



Aparecerá esta ventana donde deberá crear una entrada en **Software Installation** dando clic en **User Configuration**, **Policies**, **Software Setings**, **Software Installation**, **New** y cuando se le pregunte por el archivo MSI del agente, ubíquelo en la ruta de red, no en la ruta local del servidor.

Configuración avanzada

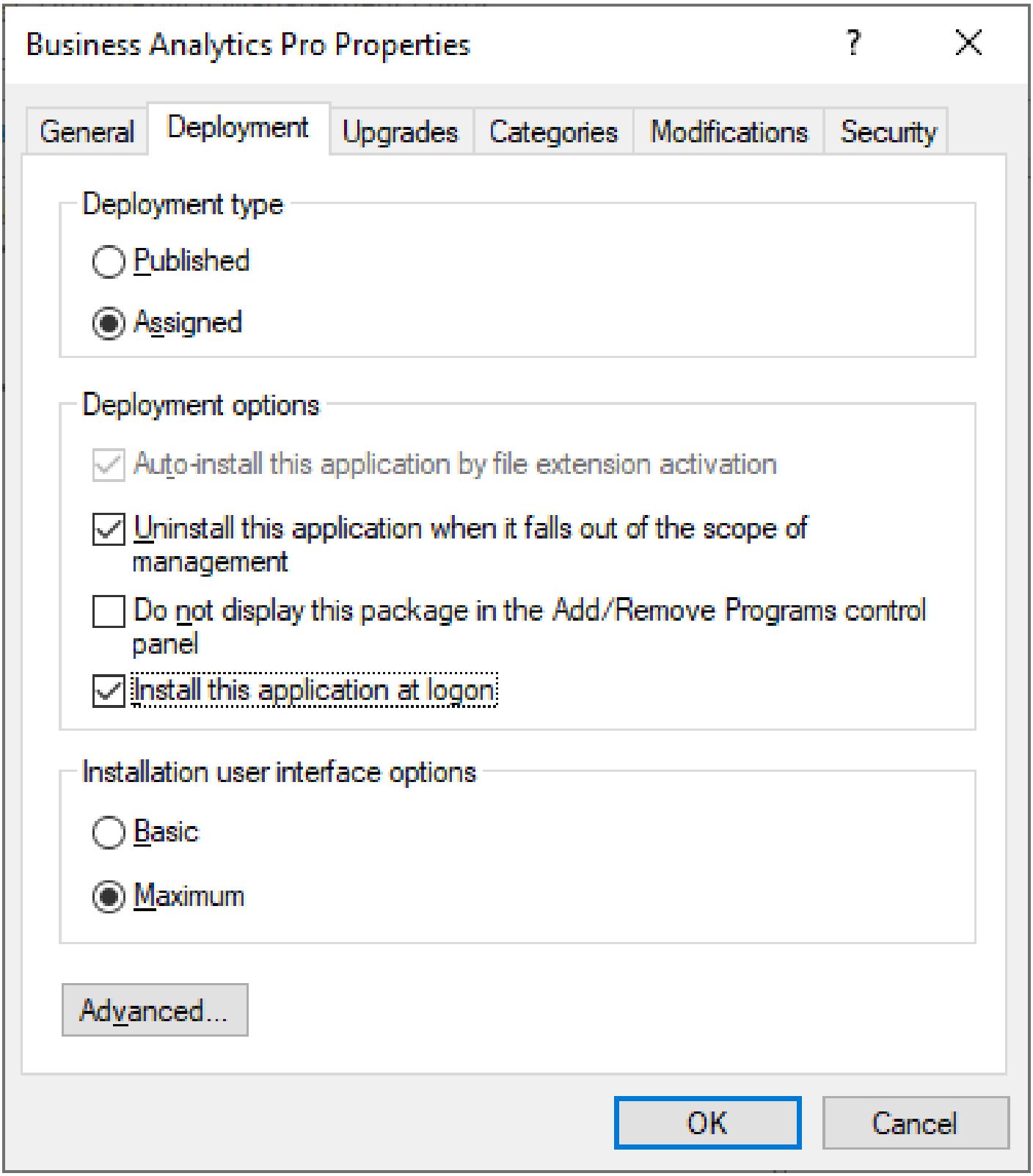
Seleccione que desea configurar el despliegue de manera avanzada.



Más adelante se configurarán el resto de opciones, por el momento de clic en OK.

Propiedades del despliegue

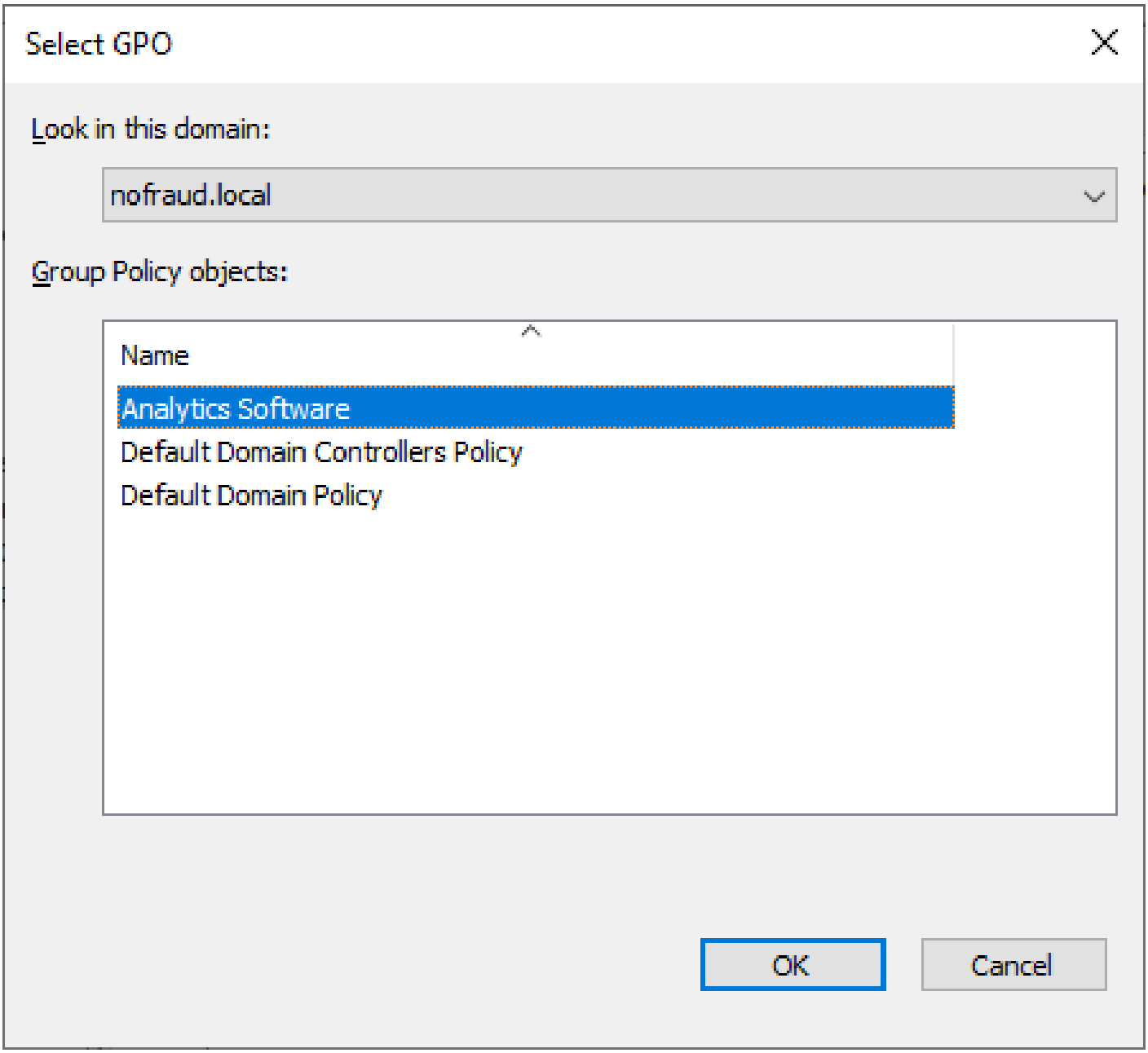
En la ventana de propiedades seleccione la pestaña **Deployment**. Aquí verifique que el tipo de despliegue sea **Assigned** y que en las opciones estén activadas las casillas **Uninstall this application when it falls out of the scope of management** y **Install this application at logon**.



De clic en OK. Con esto la política quedó correctamente configurada y solo faltaría asignarla (linkearla) a una unidad organizativa.

Crear el link de la política

En la pantalla principal del **Group Policy Management** de clic derecho en la unidad organizativa donde se encuentran todos los usuarios de la organización y donde también está el grupo de seguridad creado y de clic en **Link an existing GPO**.



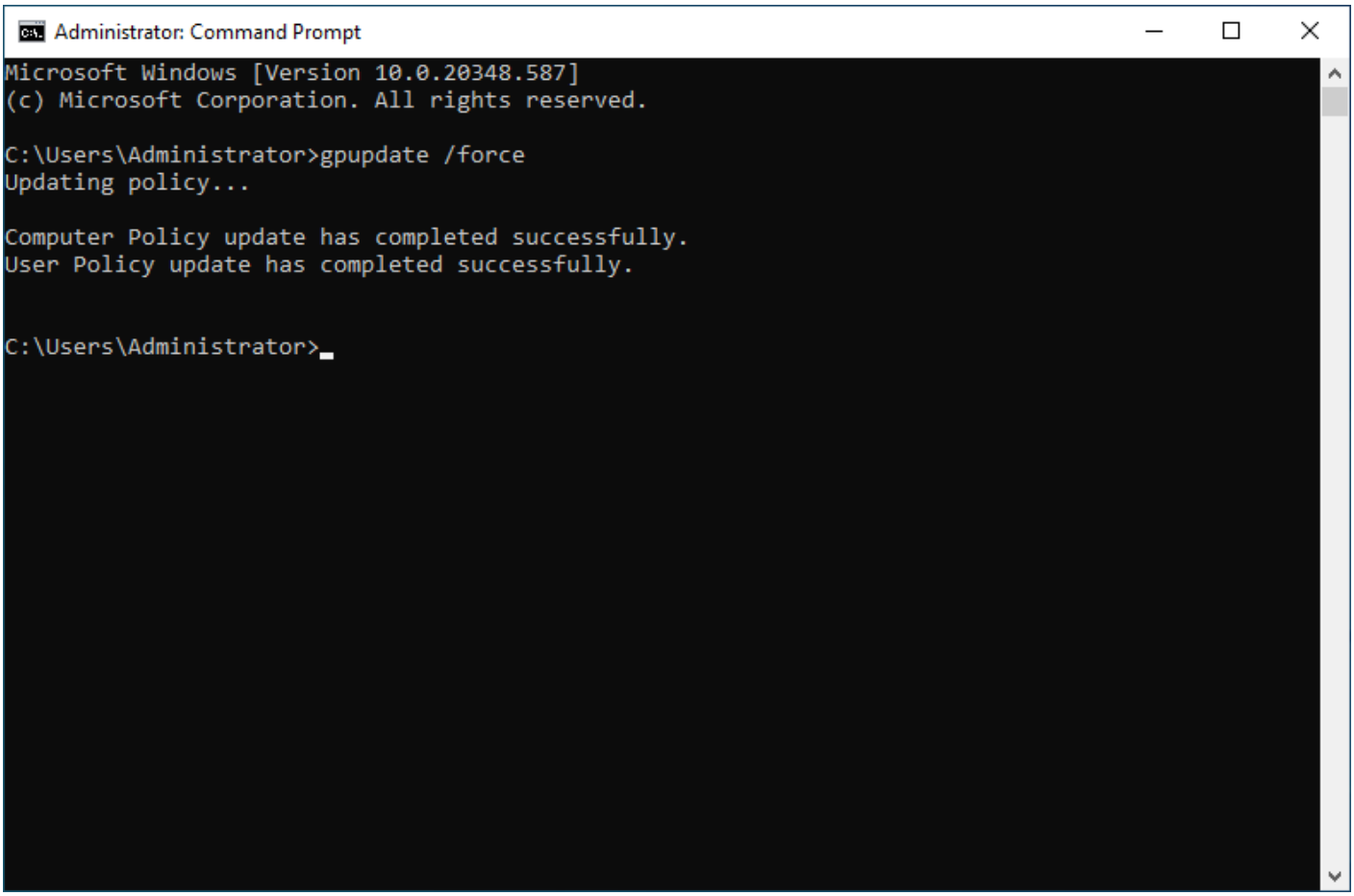
En la lista que se abre, asegúrese de seleccionar la política que acabamos de crear, en este caso la llamada **Analytics Software**. En caso de querer aplicar esta política a otras OU, debe hacer el mismo link para cada OU.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Aplicar la política con gpupdate

Abra una consola de **MS-DOS** en el servidor de controlador de dominio y ejecute el comando:

```
gpupdate /force
```

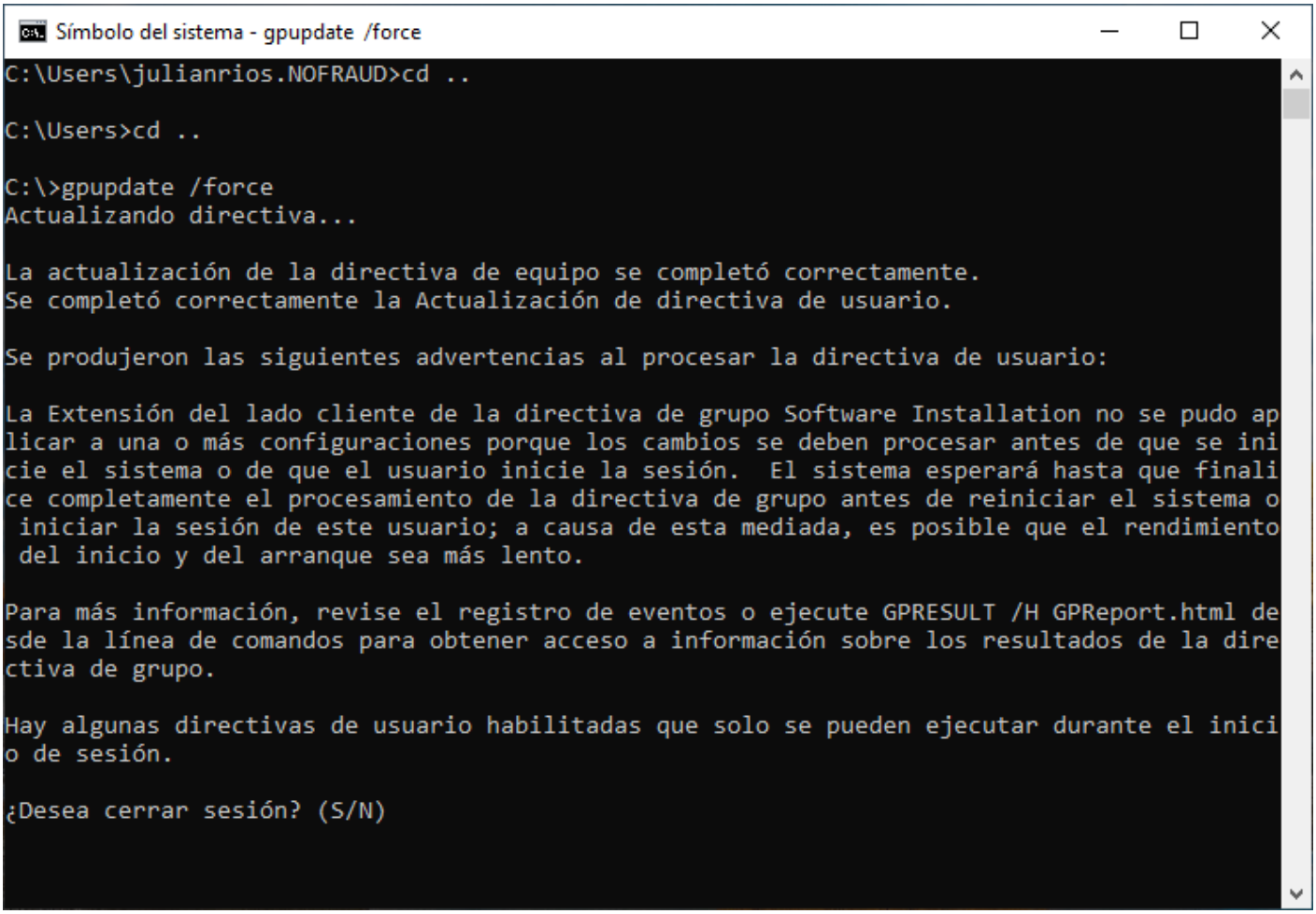


Este comando forzará la aplicación de la política desde el servidor Windows.

Aplicar la política en un PC

En el PC que quiera realizar la prueba, abra una consola de **MS-DOS** con los permisos tradicionales (sin administrador) y ejecute el comando:

```
gpupdate /force
```

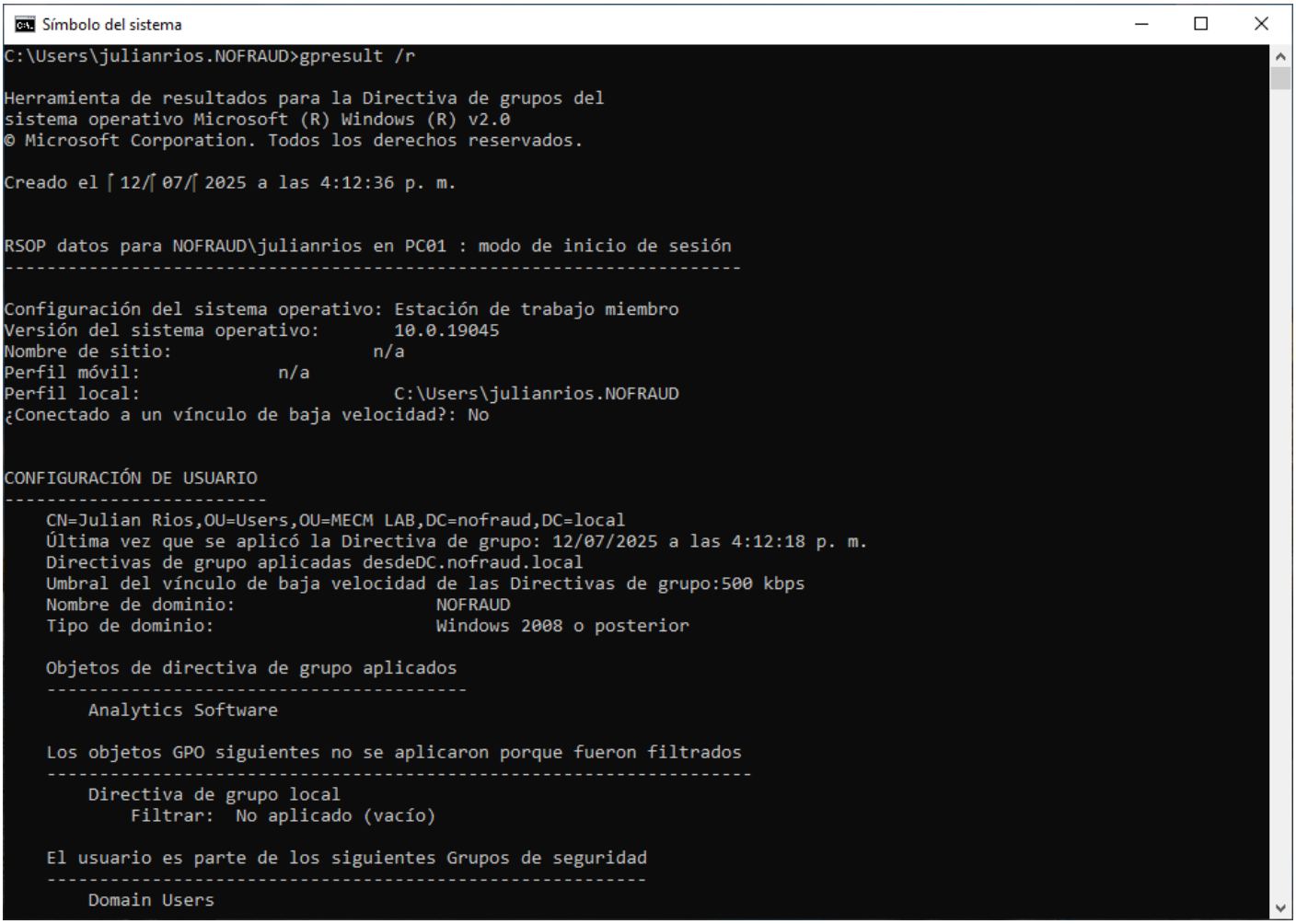


Este comando irá al servidor de controlador de dominio y preguntará si existe una nueva política para este usuario. En caso afirmativo solicitará que se reinicie la sesión en Windows. Debe decir que SI.

Comprobación de la política

En el PC donde esté haciendo la prueba de despliegue de la política, abra una consola de **MS-DOS** con el usuario normal y ejecute el comando:

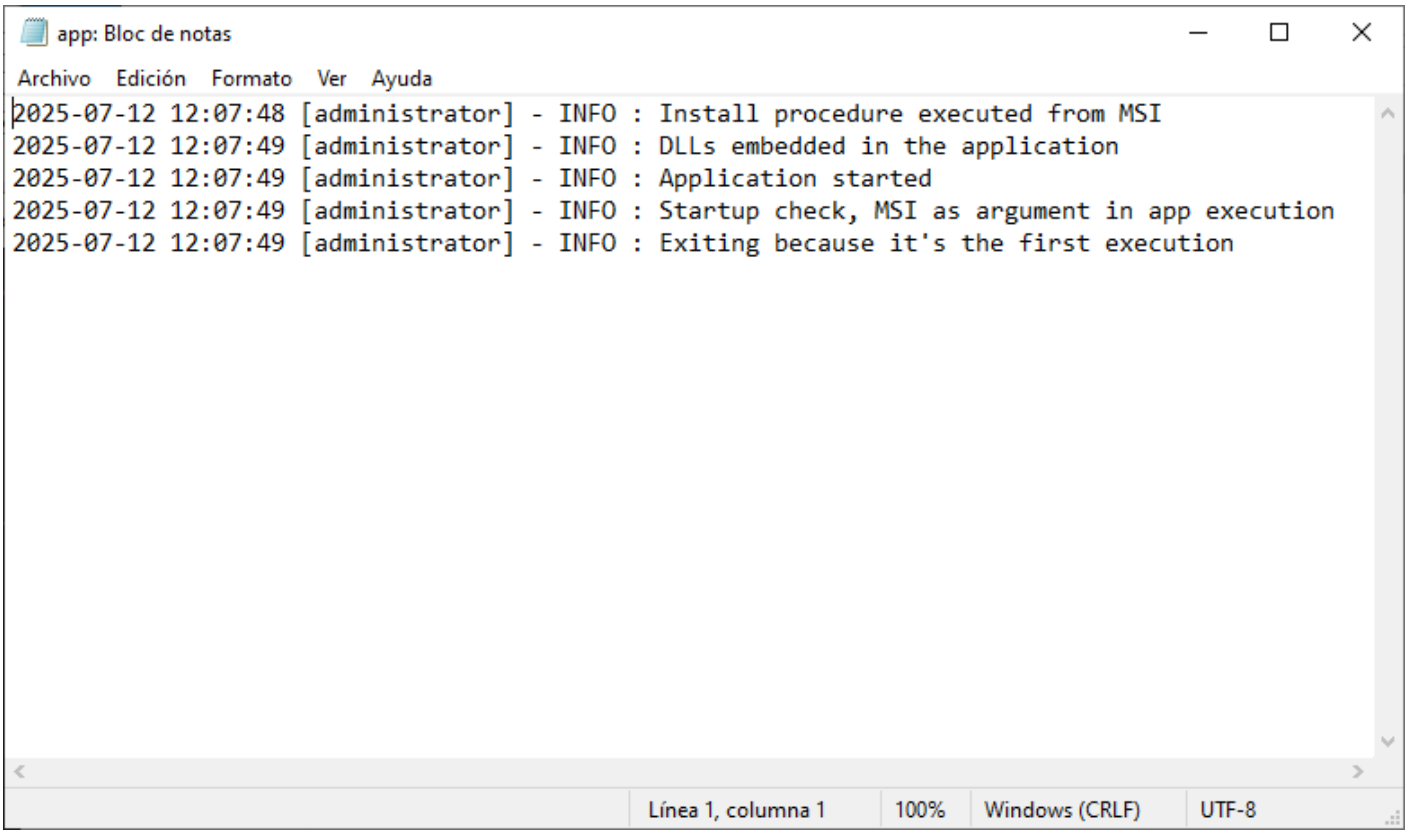
```
gpresult /r
```



Debe aparecer en la sección **Objetos de directiva de grupo aplicados** el nombre de la política que creamos.

Verificación de la instalación

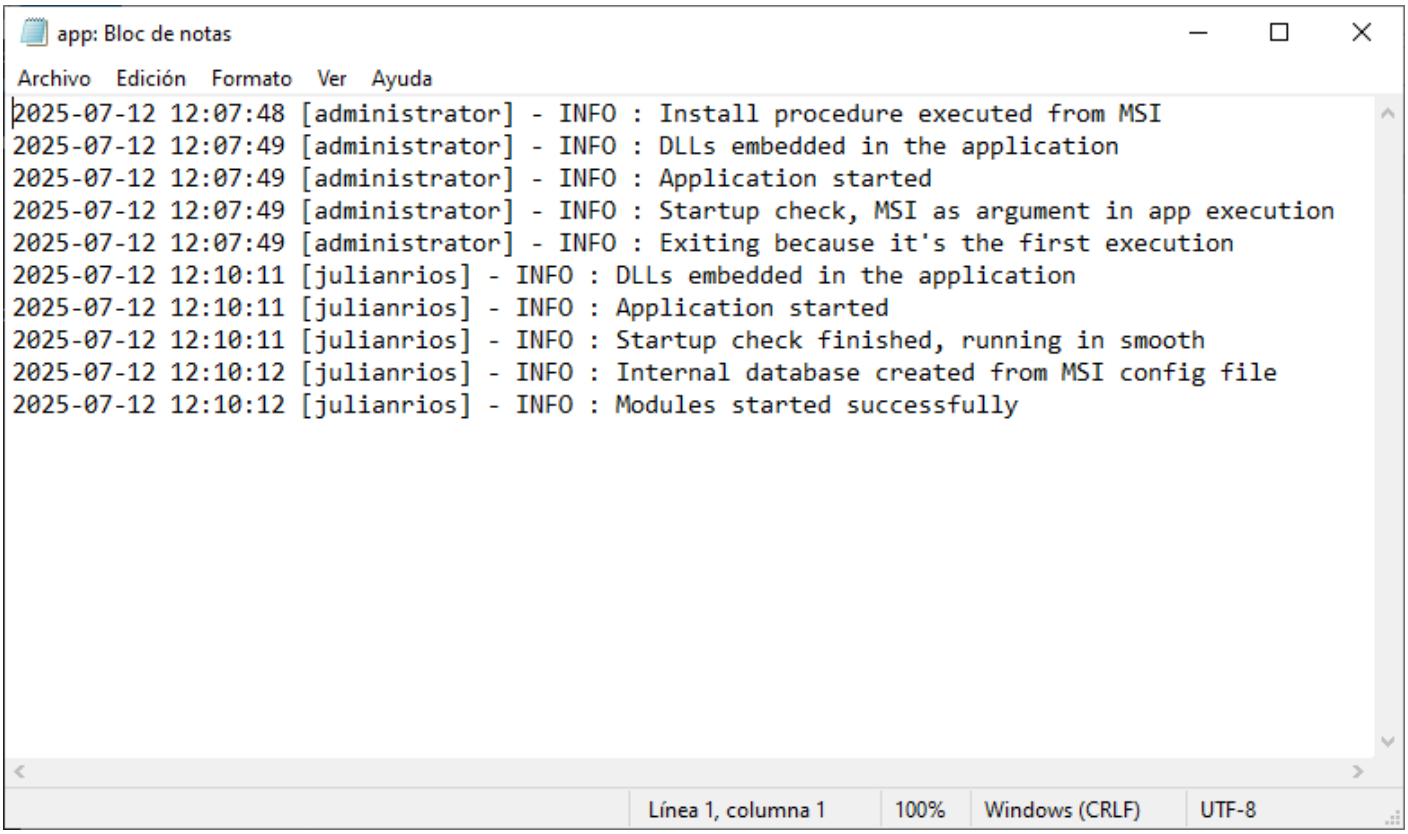
El instalador crea sus archivos en la carpeta **C:\ProgramData\Software** y allí se encuentra un archivo de log llamado **app.log**. Si lo abre deberá ver este tipo de entradas donde se indica que le usuario administrador acaba de realizar la instalación del agente.



El agente solo usa el usuario **administrador** para instalar el aplicativo, no para correrlo.

Reinicio del PC

Cuando se reinicia el PC, el agente arranca con los permisos del usuario restringido, como se observa en el archivo **C:\ProgramData\Software\app.log**.

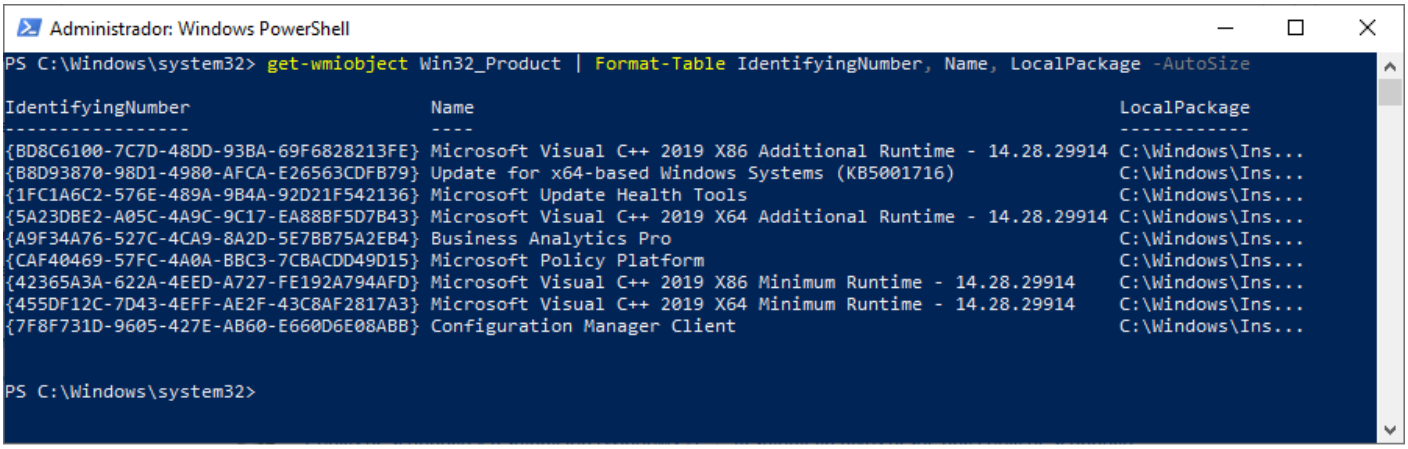


En este archivo de log se encontrará toda información relevante de inicio, parada, actualización, desinstalación e incluso errores que pueda presentar el agente durante su ejecución.

Revisión de instalación con PowerShell

Puede ejecutar este comando en una consola de **PowerShell** para obtener mayor información sobre el producto instalado:

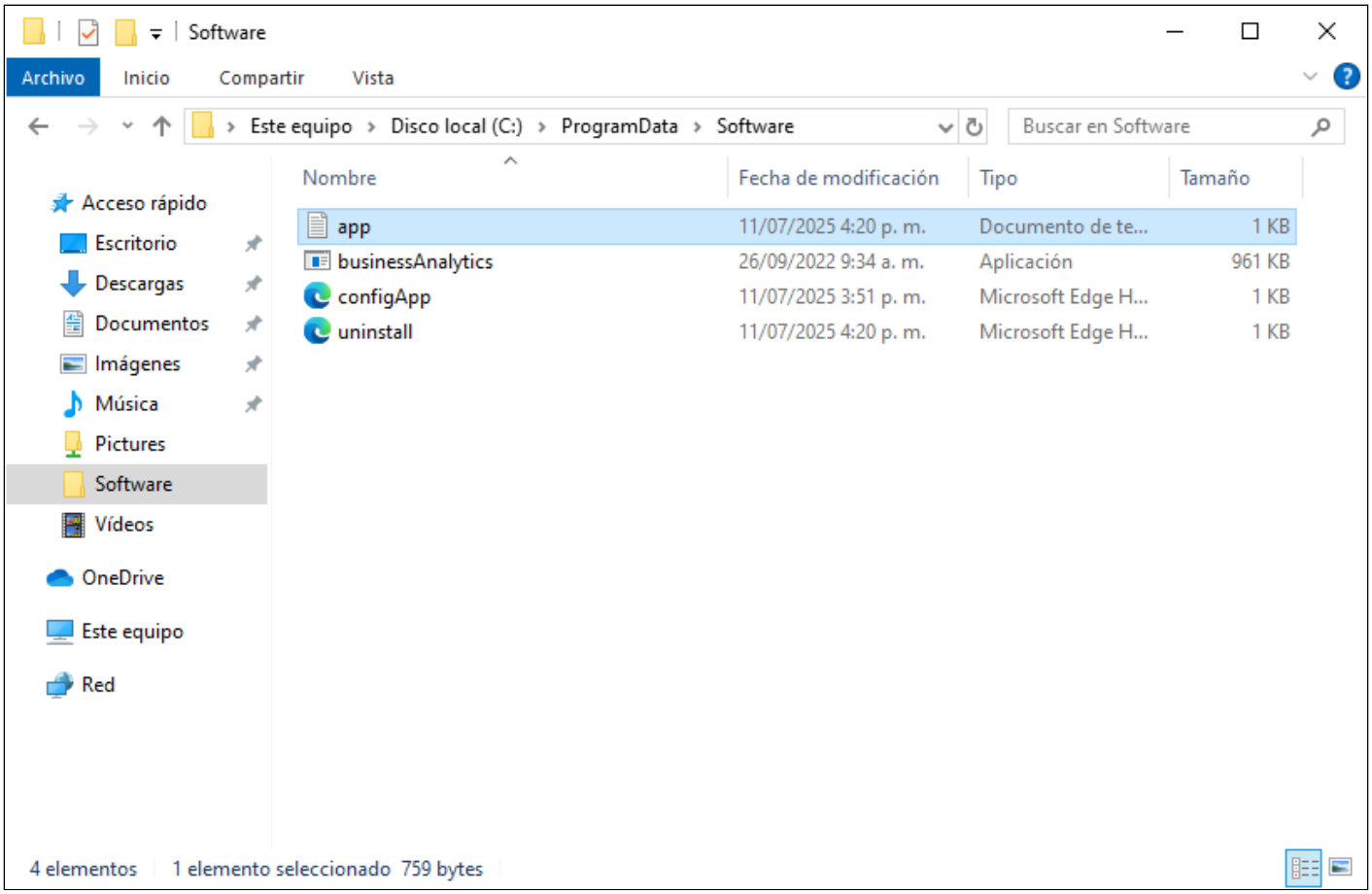
```
wmi-object Win32-Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



En esta pantalla se muestra información de valor como el ID del producto y la ruta local que ha creado Windows para almacenar en caché el MSI del agente.

Archivos que crea el agente

En la carpeta **C:\ProgramData\Software** se almacena el archivo ejecutable del agente de The Fraud Explorer llamado **businessAnalytics.exe**. Junto a él también se encuentra un archivo de los llamado **app.log**, un archivo de configuración llamado **configApp.xml** y un archivo con instrucciones internas para la desinstalación llamado **uninstall.xml**.

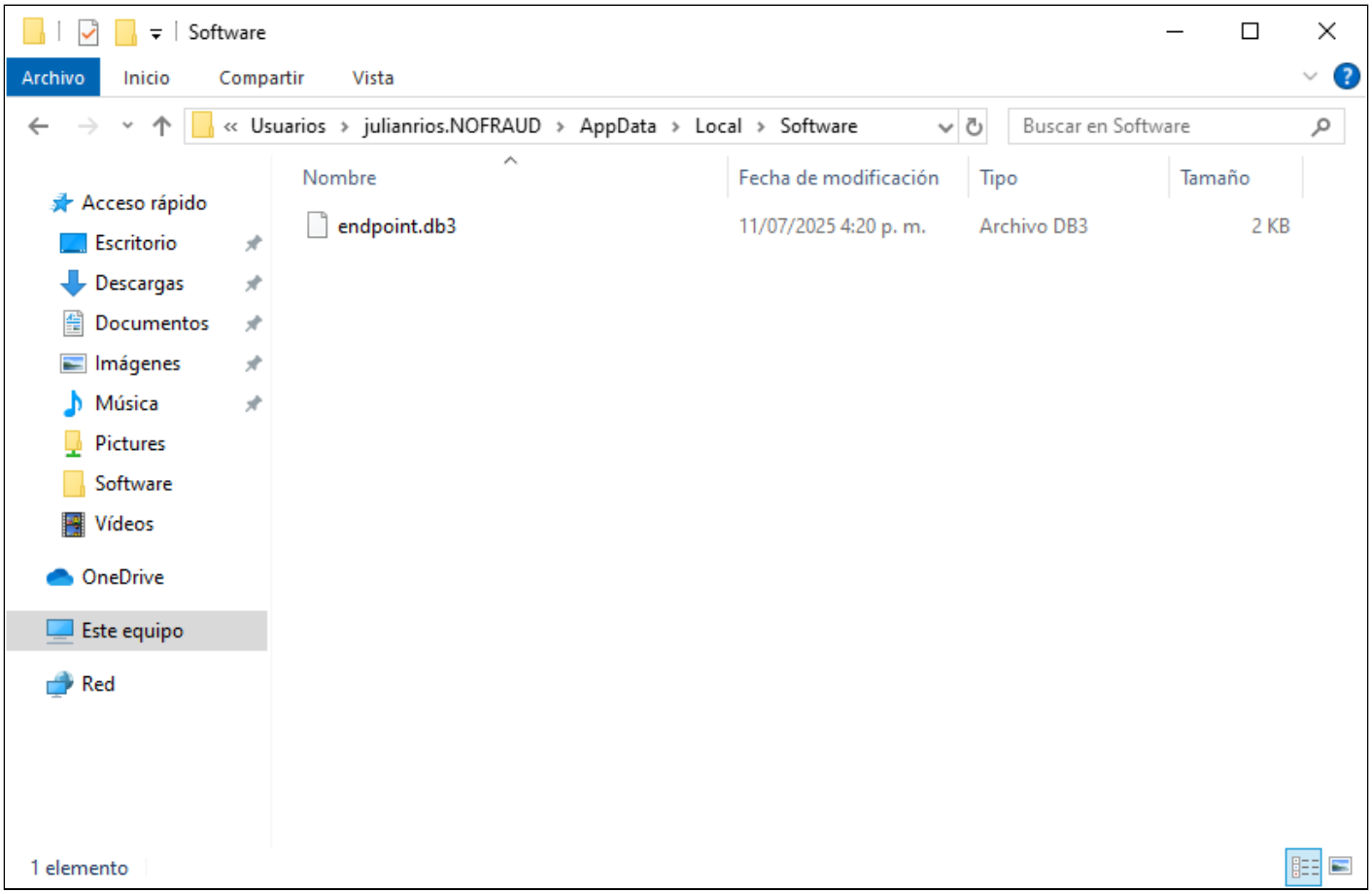


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe** .

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Base de datos del agente

Internamente el agente de The Fraud Explorer almacena su configuración en un archivo cifrado llamado **endpoint.db3** y localizado en la carpeta **C:\Users\empleado\AppData\Local\Software**. Esta carpeta depende al final del usuario que será monitoreado.

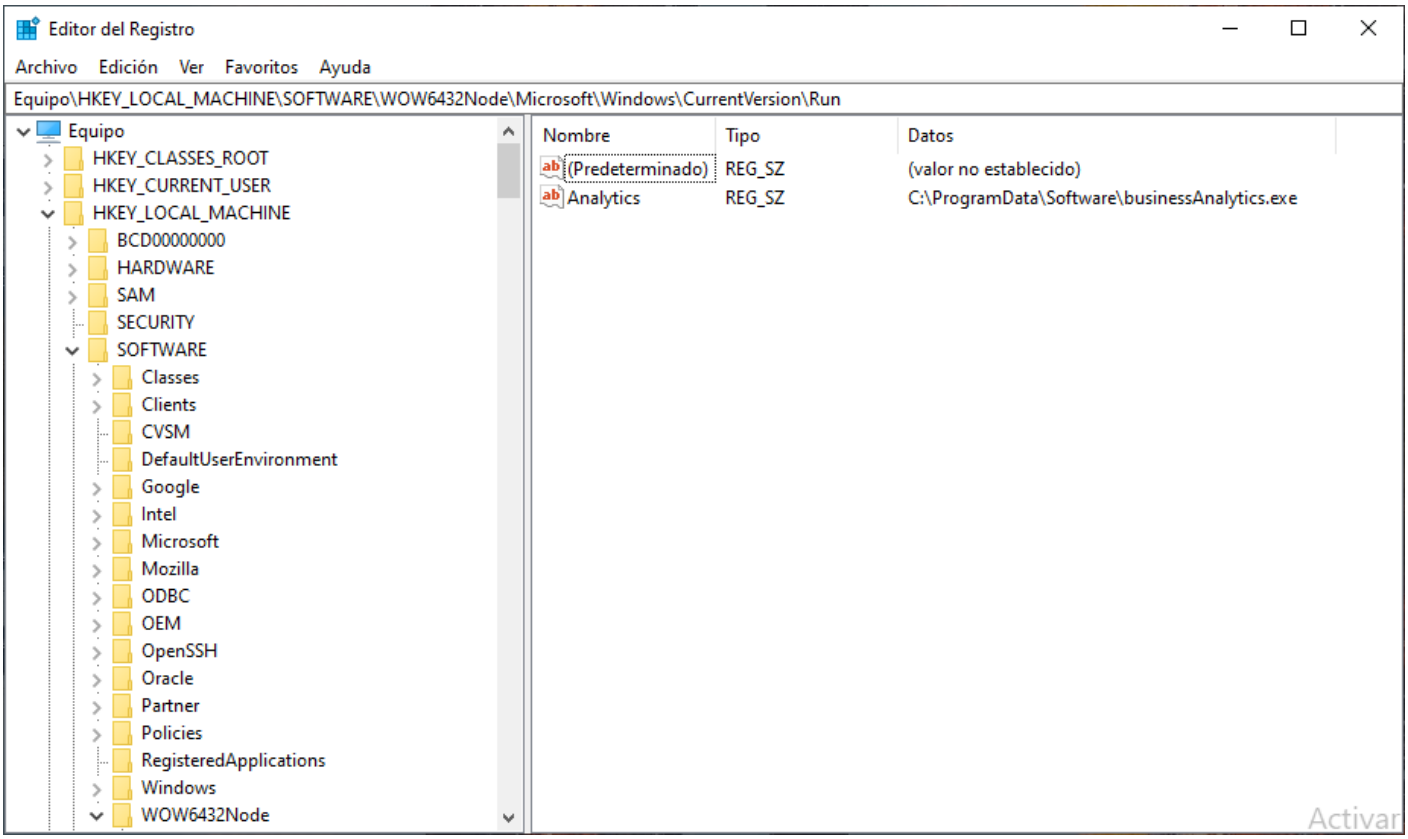


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Entradas de registro de Windows

El agente de The Fraud Explorer crea una entrada en el registro de Windows en la ruta **HKEY_LOCAL_MACHINE, SOFTWARE, WOW6432Node, Microsoft, Windows, CurrentVersion, Run**.

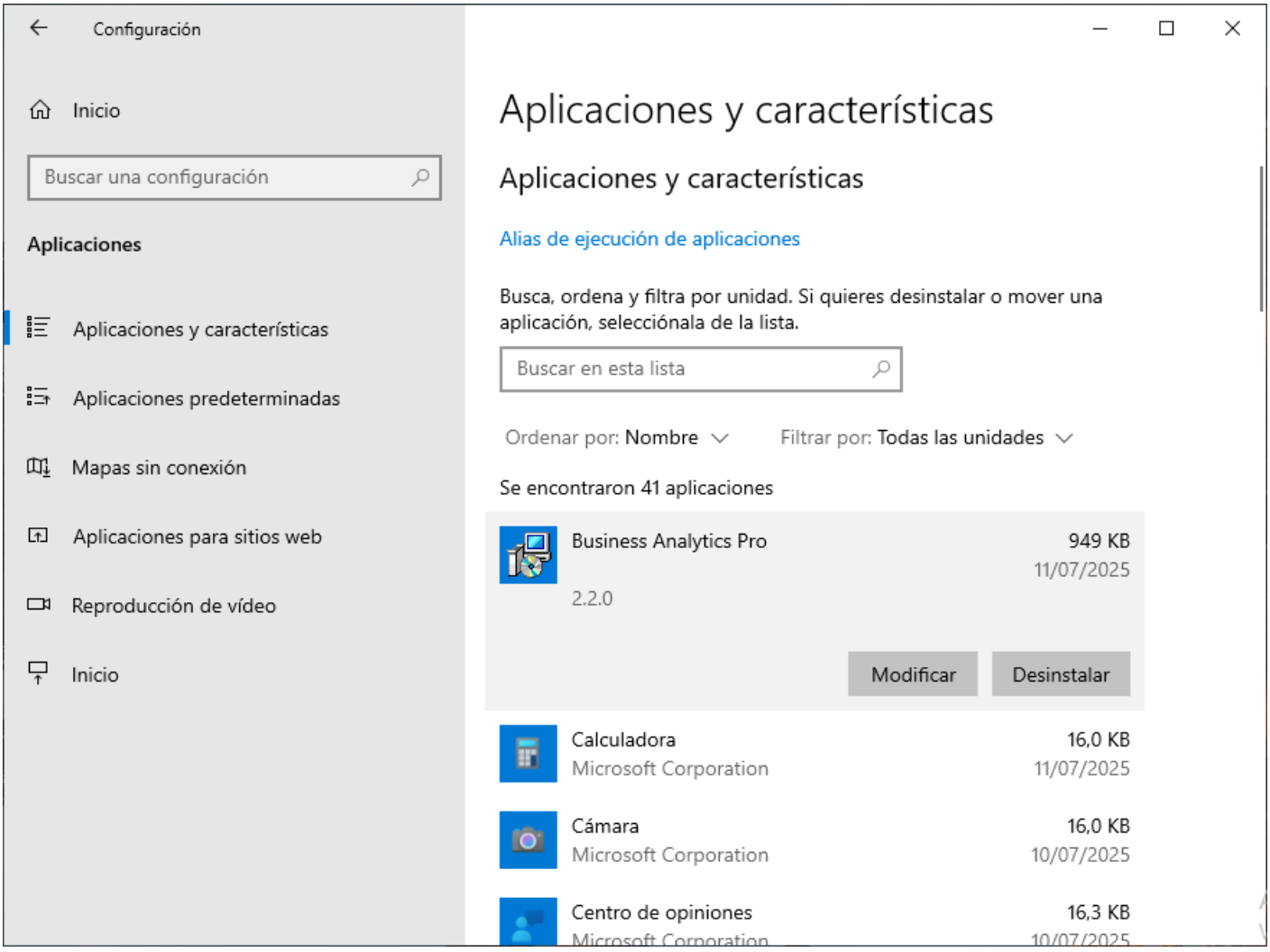


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Aparición en programas instalados

Si se entra al panel de control y allí se ingresa a las aplicaciones y características del equipo, se verá que aparece el agente de The Fraud Explorer con el nombre **Business Analytics**.

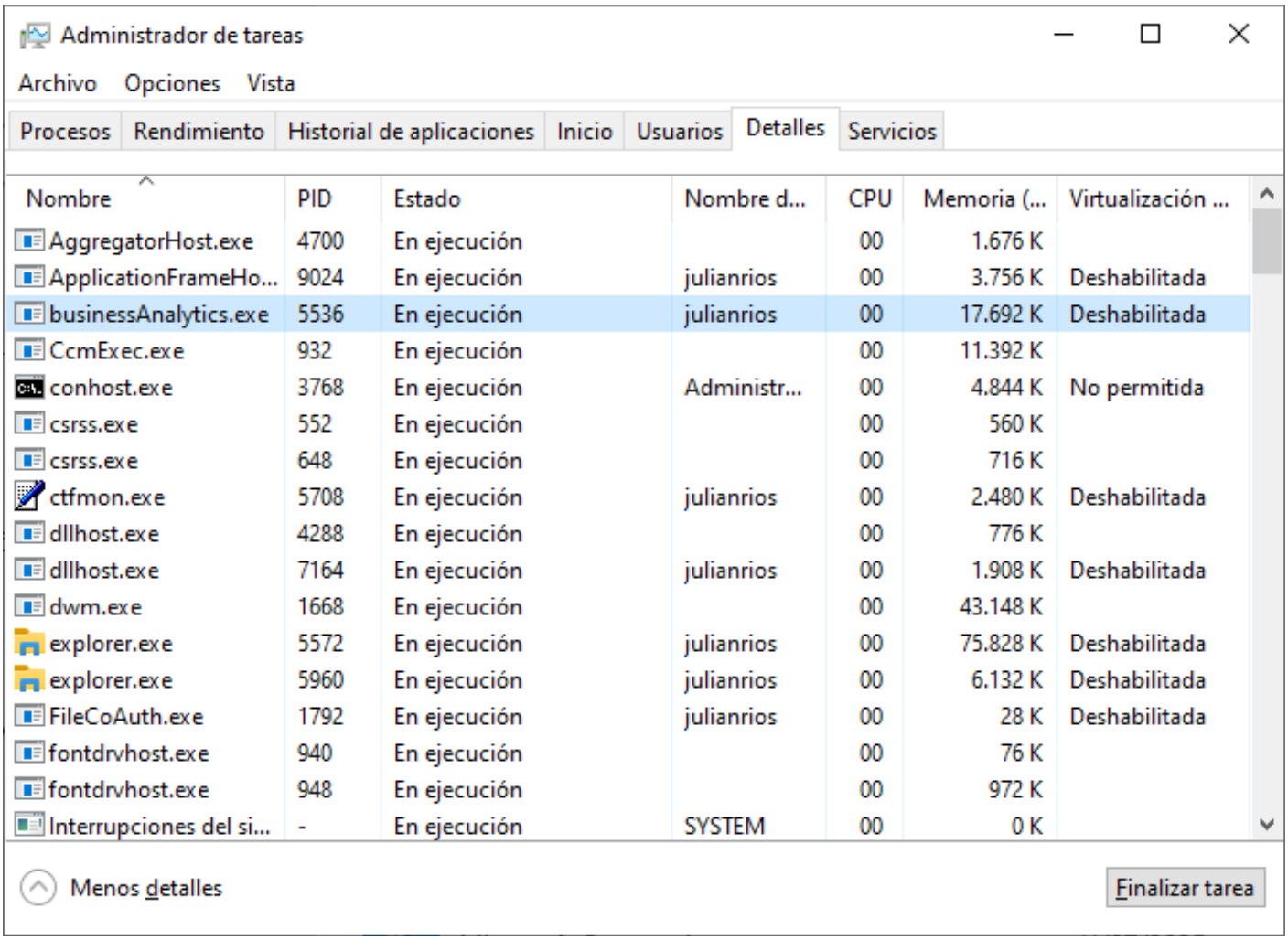


Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se re-emplaza la actual con la nueva versión.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Monitoreo del agente

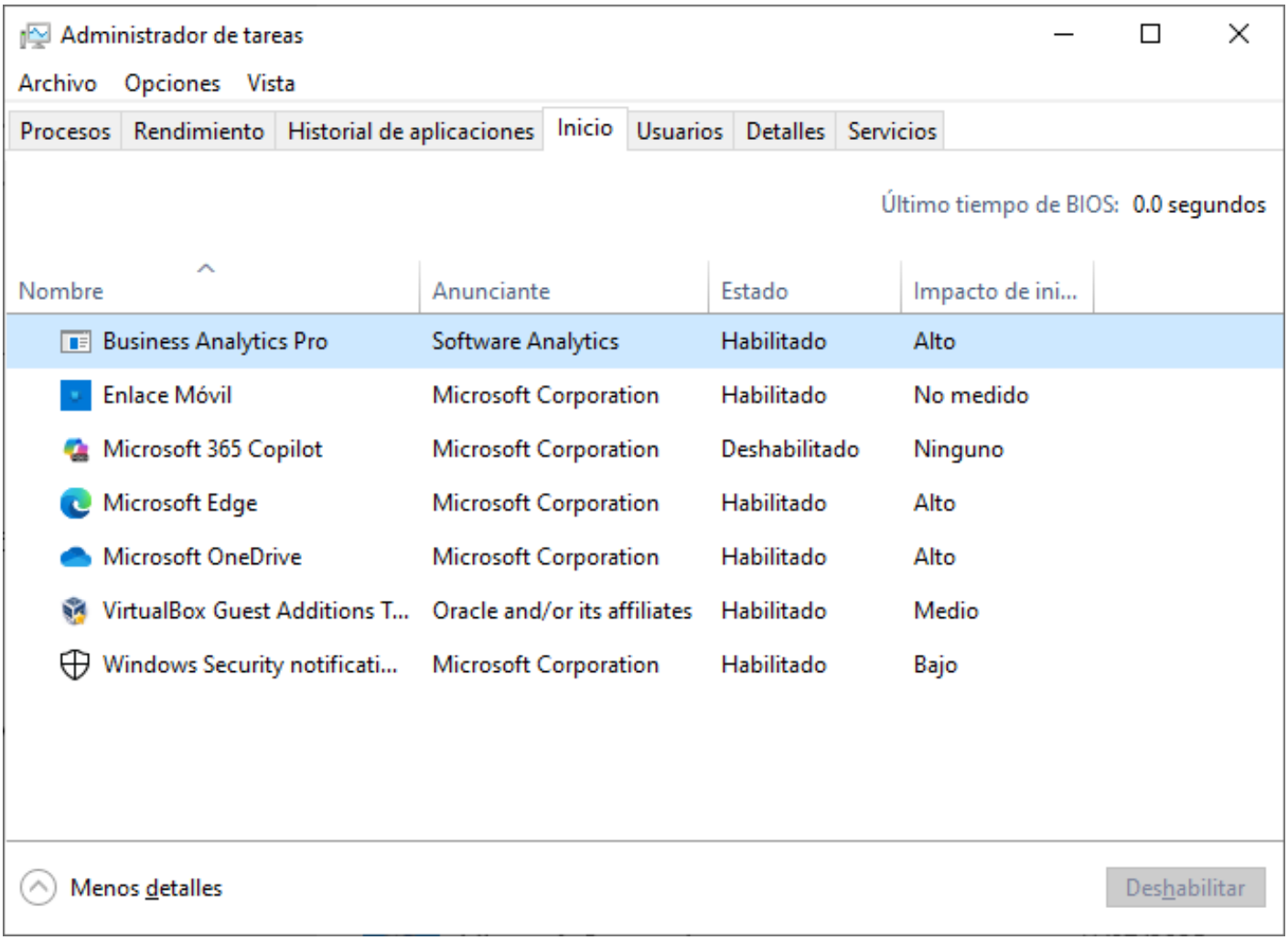
En el PC del usuario, se puede abrir el **Administrador de tareas** y en la pestaña **Detalles** buscar el ejecutable **businessAnalytics.exe**.



El ejecutable se arranca con los privilegios del usuario que será monitoreado. Se pueden ver además los consumos de recursos que hace el agente. Cuando recién arranca, el agente puede consumir 17 MB de memoria RAM, pero una vez termina de arrancar su uso es de aproximadamente 8 MB.

Inicio del agente

Al crear la entrada en el registro de Windows, automáticamente el agente puede verse en la misma ventana del **Administrador de tareas**, en la pestaña **Inicio**.



En esta ventana se muestran todas las aplicaciones que arrancan cuando el usuario inicia sesión con su cuenta en Windows. El agente de The Fraud Explorer no arranca como servicio y no interfiere en el proceso de arranque de sistema operativo.

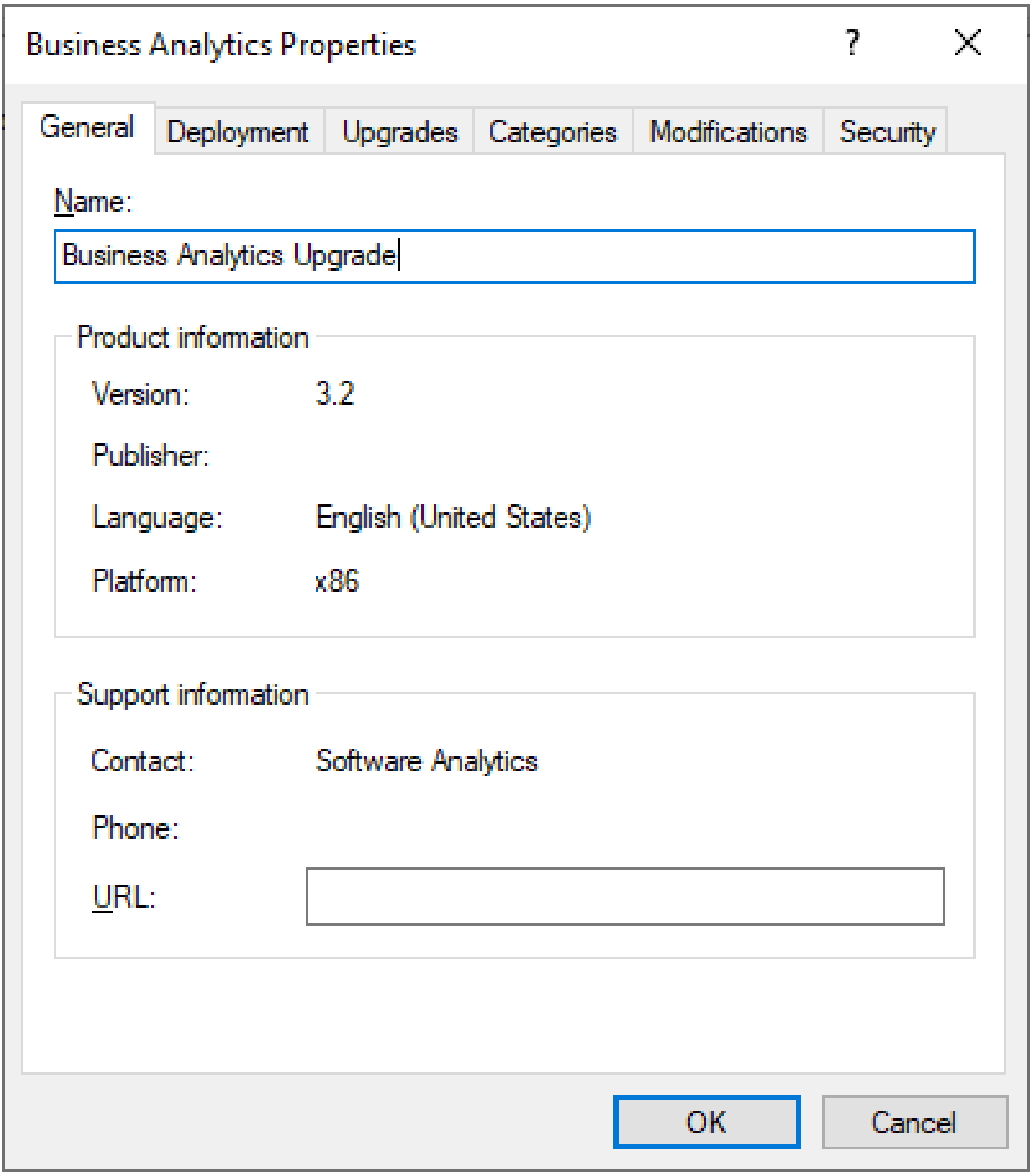
En caso de tener problemas con el arranque de Windows, puede descartar directamente que sea el agente de The Fraud Explorer, porque el agente se ejecuta en la etapa final cuando se ha cargado completamente el explorador de Windows.

Actualización del agente

Para actualizar el agente, ingrese de nuevo al **Group Policy Management**, de clic derecho en la política GPO creada en **Group Policy Objects** y luego en **Edit**.

En **User Configuration**, **Policies**, **Software Settings**, **Software Installation**, de clic en **New Package**. Cuando sele pida especificar el MSI del agente, seleccione la nueva versión y asegúrese de que especifica una ruta de red en vez de una ruta local.

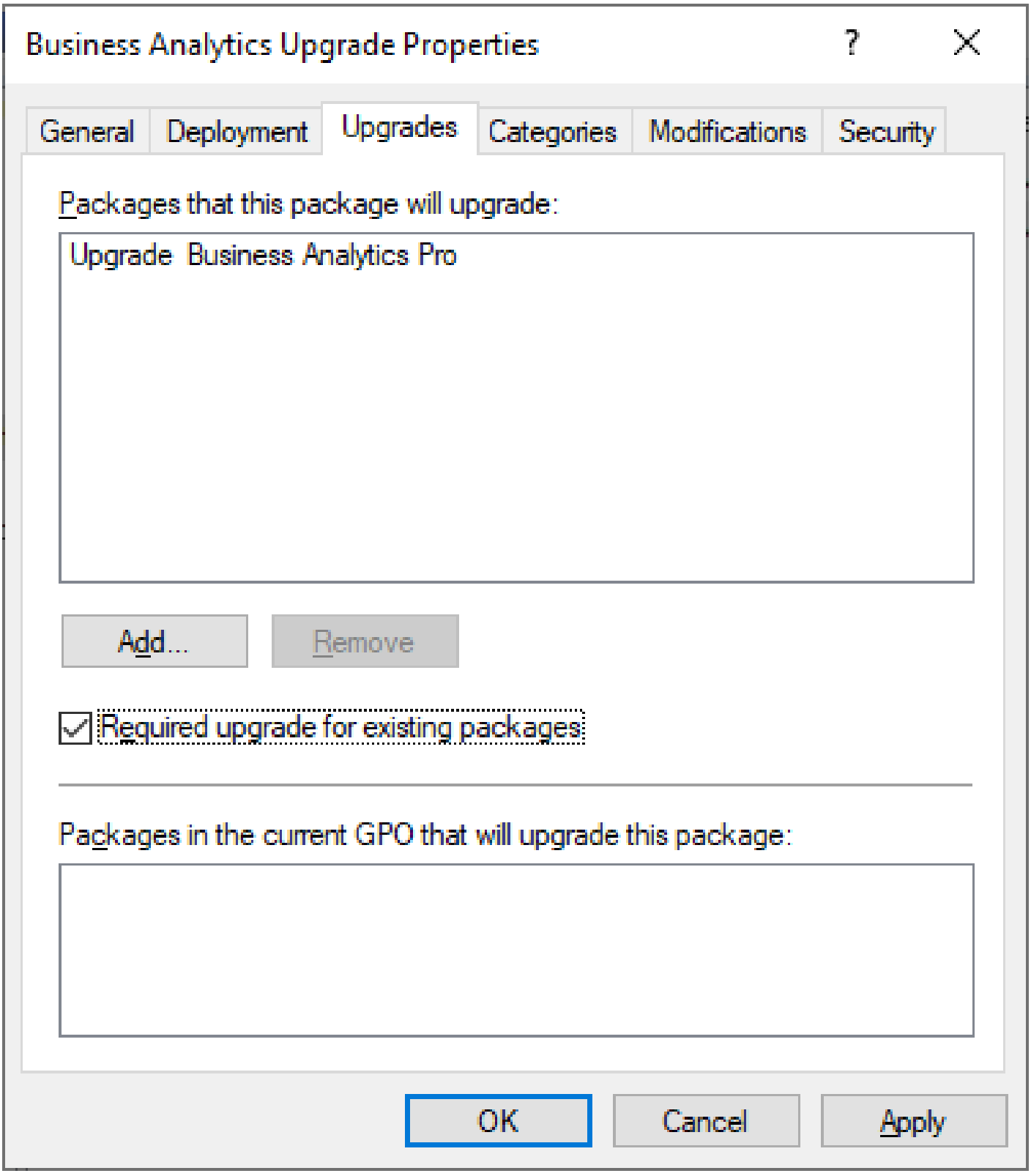
Cuando se le pida especificar si desea ser **Asignado** o **Publicado**, no seleccione ninguna y seleccione la ultima opción de configuración **Avanzada**.



Elija un nombre que diferencie esta aplicación de la anterior. Puede usar al final la palabra **Upgrade** como referencia.

Qué se actualizará

En las propiedades de la actualización elija que este paquete actualiza un paquete anterior, como se muestra en la imagen a continuación.

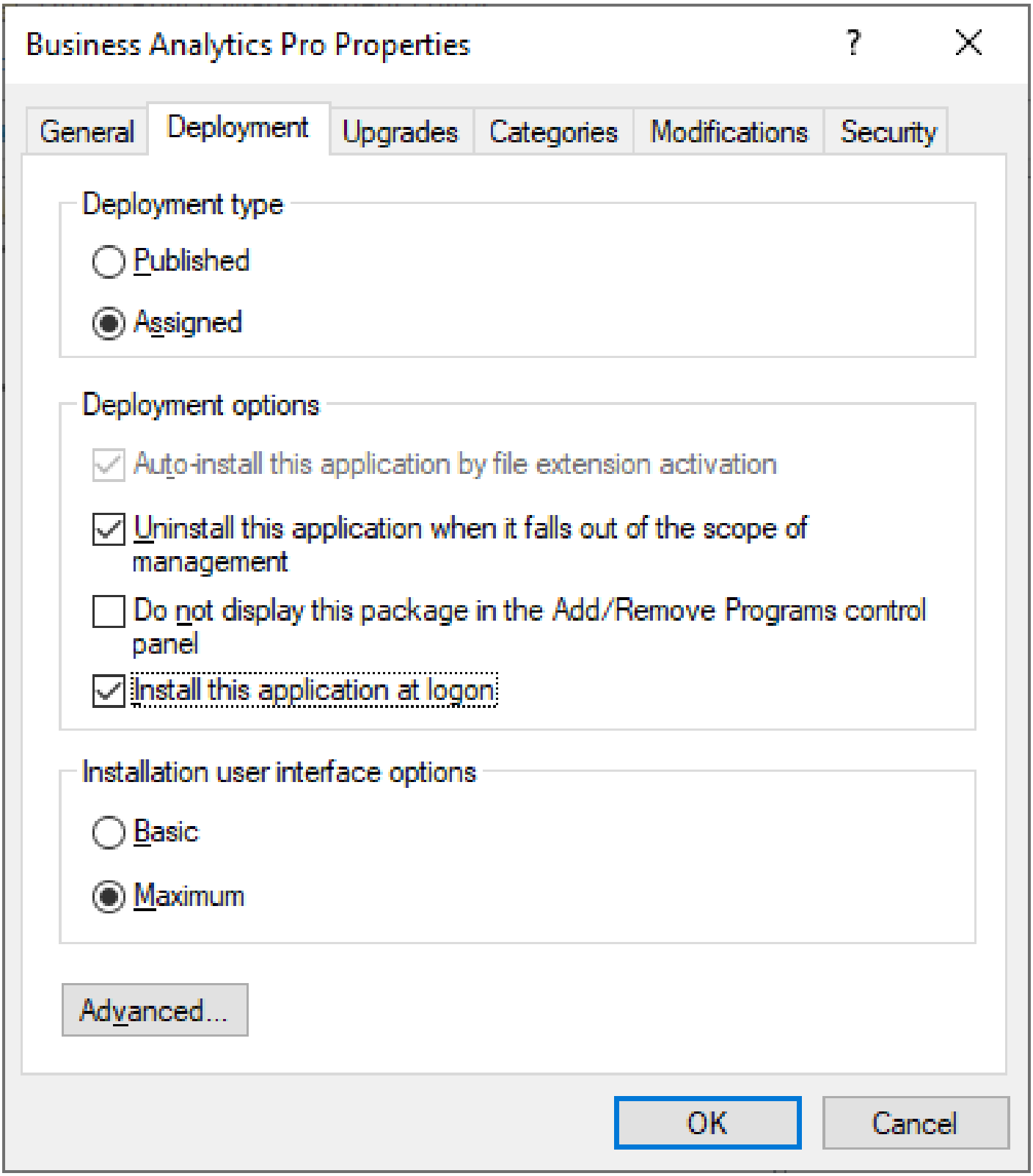


Active la casilla **Required upgrade for existing packages** y aplique la configuración.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Propiedades de la actualización

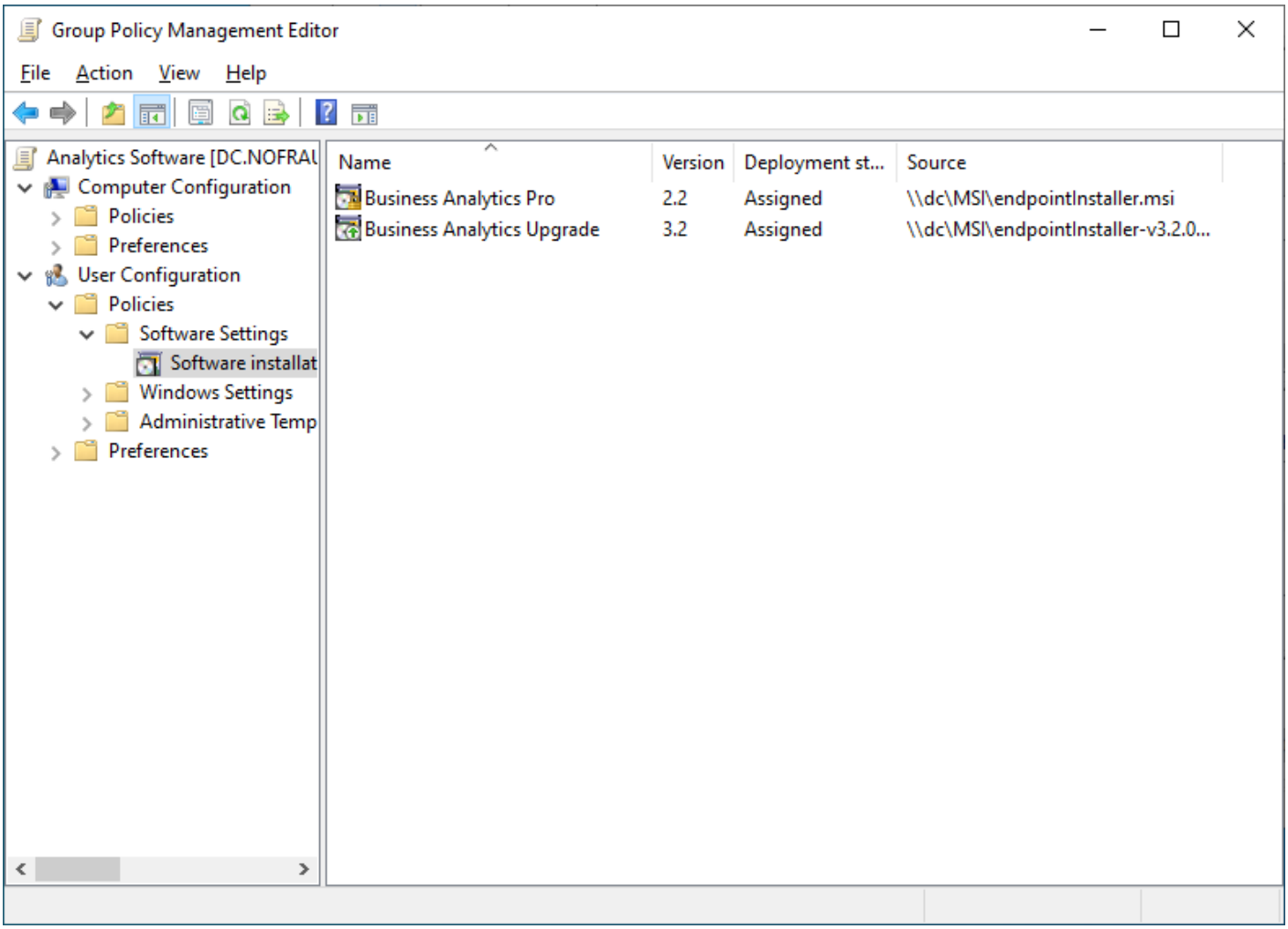
En la ventana de propiedades seleccione la pestaña **Deployment**. Aquí verifique que el tipo de despliegue sea **Assigned** y que en las opciones estén activadas las casillas **Uninstall this application when it falls out of the scope of management** y **Install this application at logon**.



De clic en OK. Con esto la política quedó correctamente configurada la actualización.

Inventario de aplicaciones

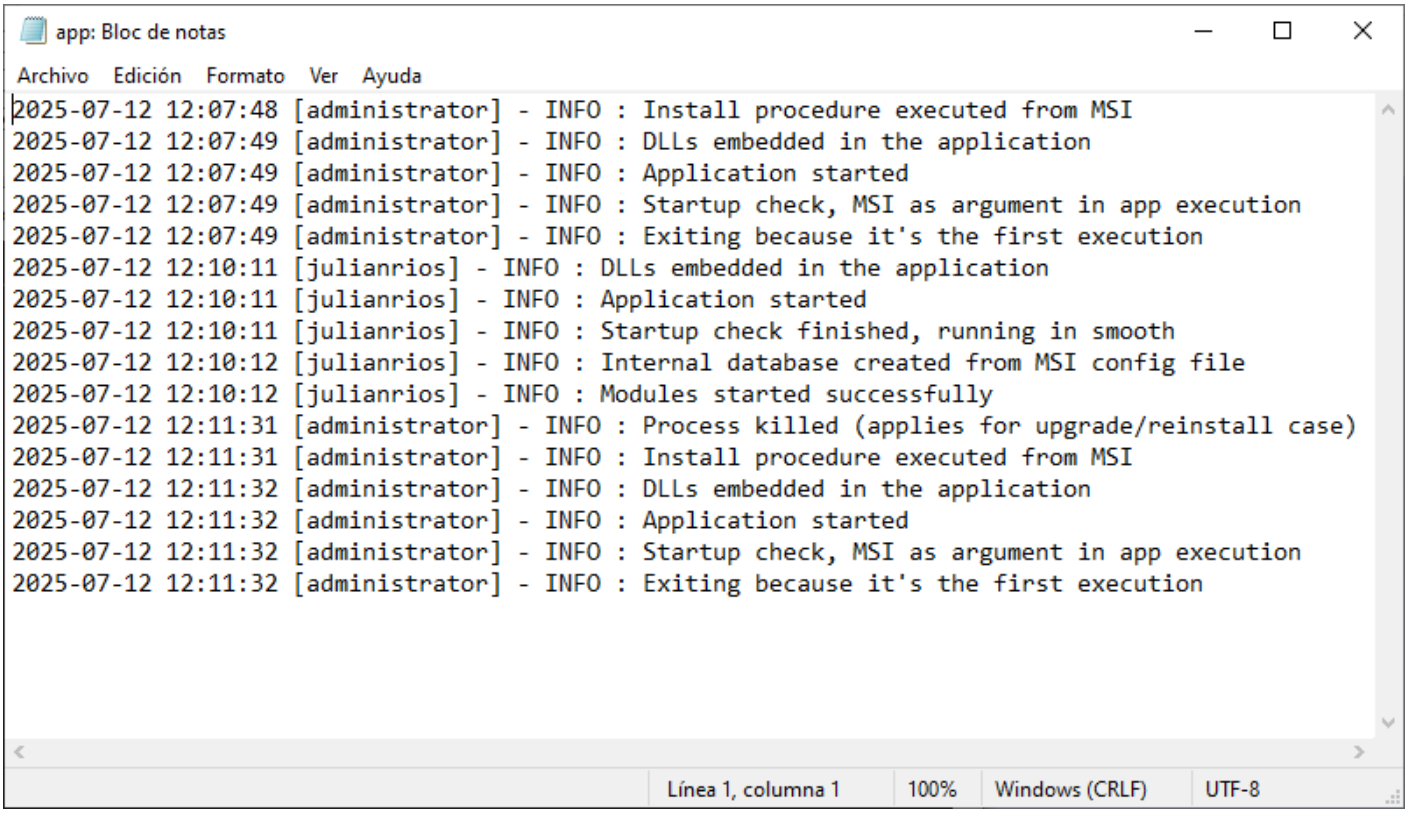
En este momento deberían aparecer estas dos entradas, una que muestra la primera versión del agente y otra que muestra una versión más actualizada.



En los iconos se ve que la segunda entrada tiene una flecha verde hacia arriba, lo significa que se trata de una actualización.

Verificación de la actualización

En el archivo C:\ProgramData\Software\app.log se observará el proceso de actualización ejecutado.

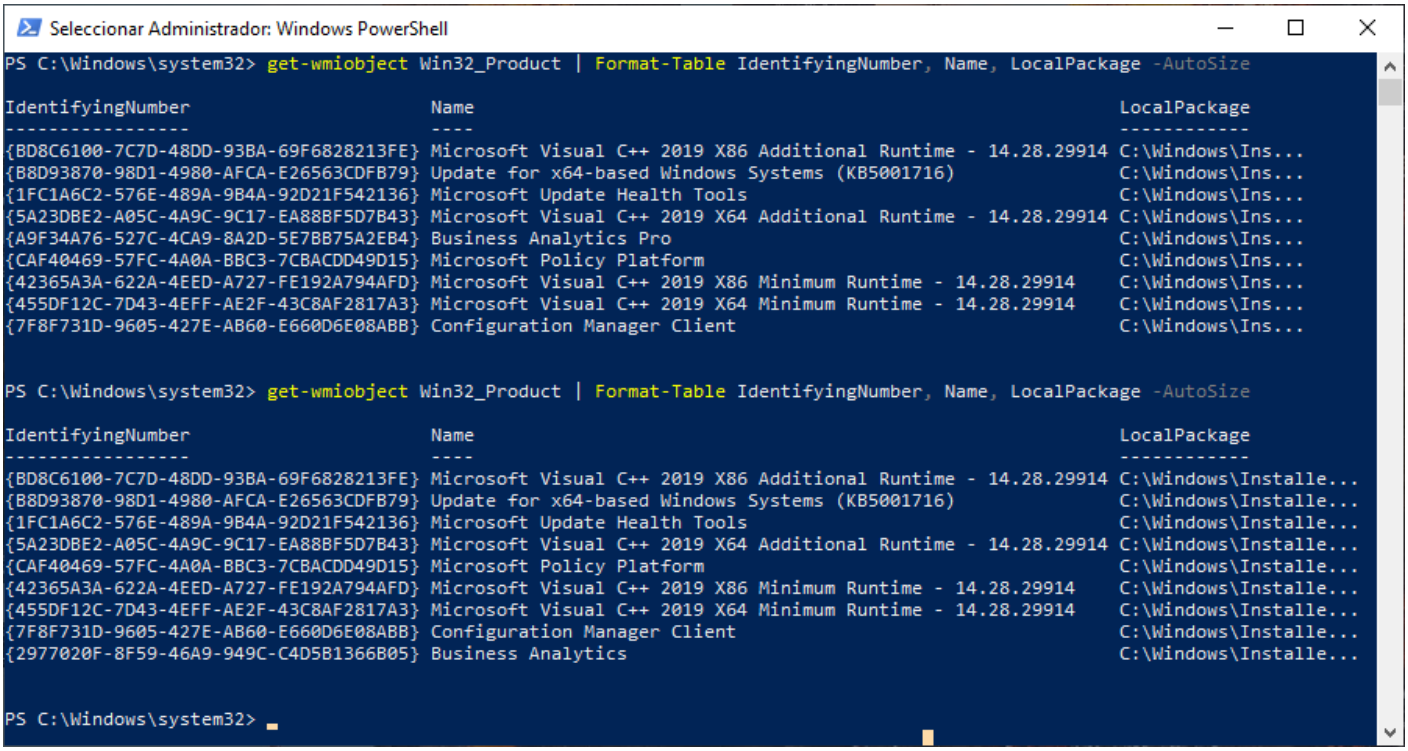


Se puede comprobar que se actualizó por la presencia de la entrada **Process killed (applies for upgrade/reinstall case)**.

PowerShell para verificar actualización

Si se vuelve a ejecutar el siguiente comando en el **PowerShell**, se dará cuenta de que la versión anterior ya no existe y se ha reemplazado por la nueva versión:

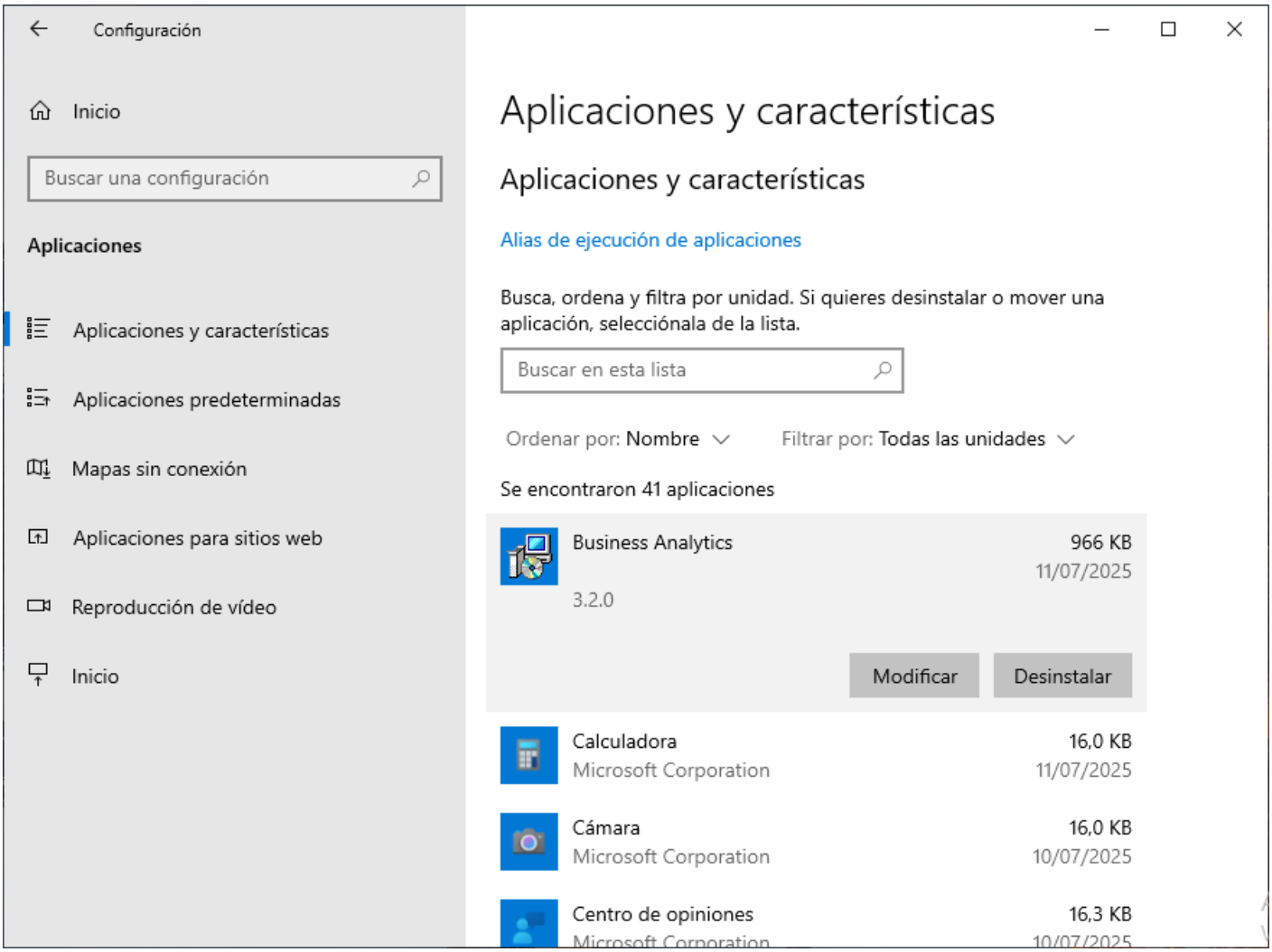
```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



Adicionalmente se muestra el nuevo código del producto, que es diferente al anterior.

Actualización en listado de Aplicaciones

Adicionalmente, si abre el Panel de control en el PC del usuario y da clic en **Aplicaciones y características**, verá que solo existe una entrada en el listado de aplicaciones referente al agente de The Fraud Explorer.



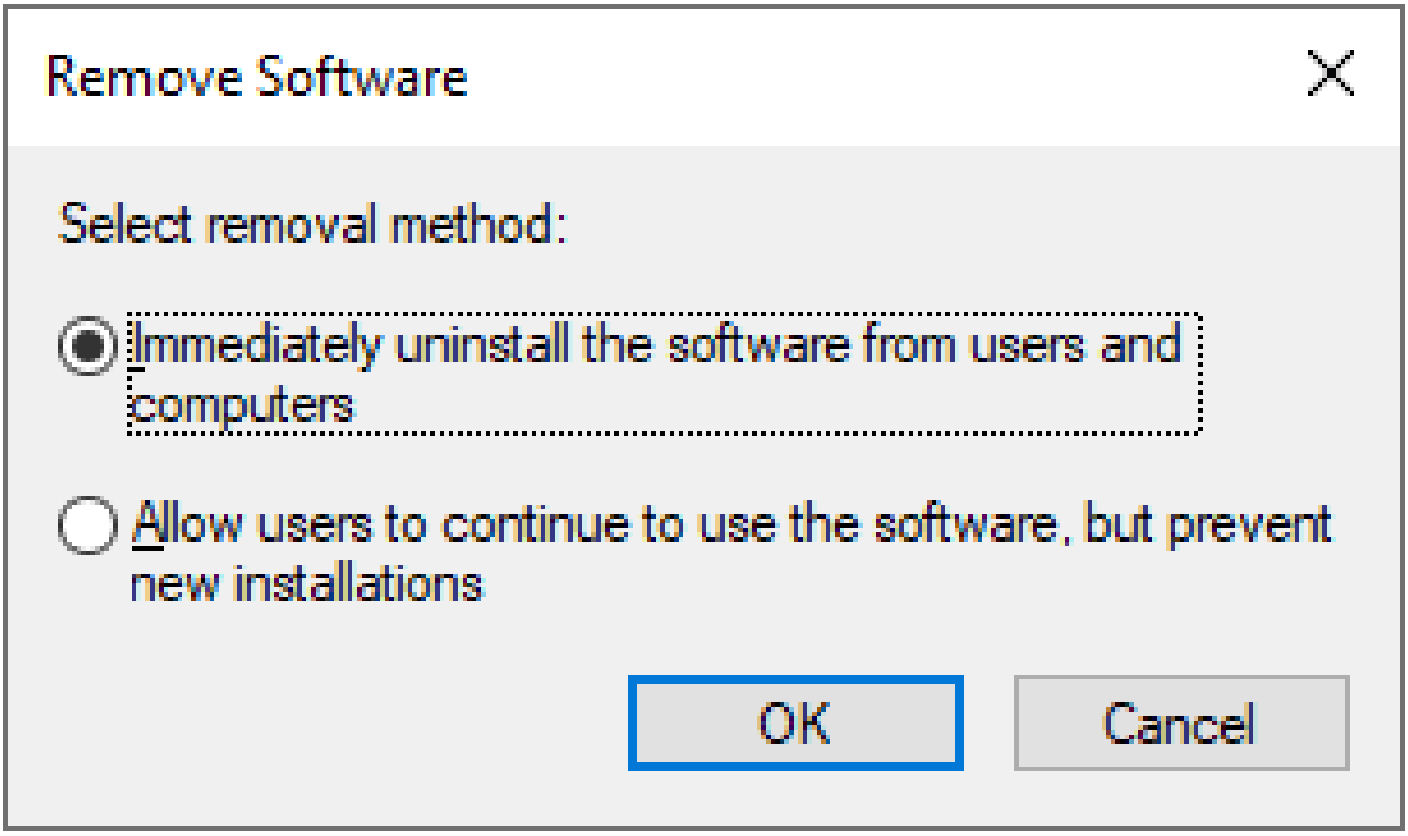
Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Desinstalación del agente

Para desinstalar el agente, debe entrar al **Group Policy Management**, seleccionar la política creada **Analytics Software** y dar clic derecho y luego en **Edit**.

Ubíquese en la ruta **User Configuration**, **Policies**, **Software Settings**, **Software Installation**, de clic derecho sobre el software asignado y luego en **All Tasks** y **Remove**.

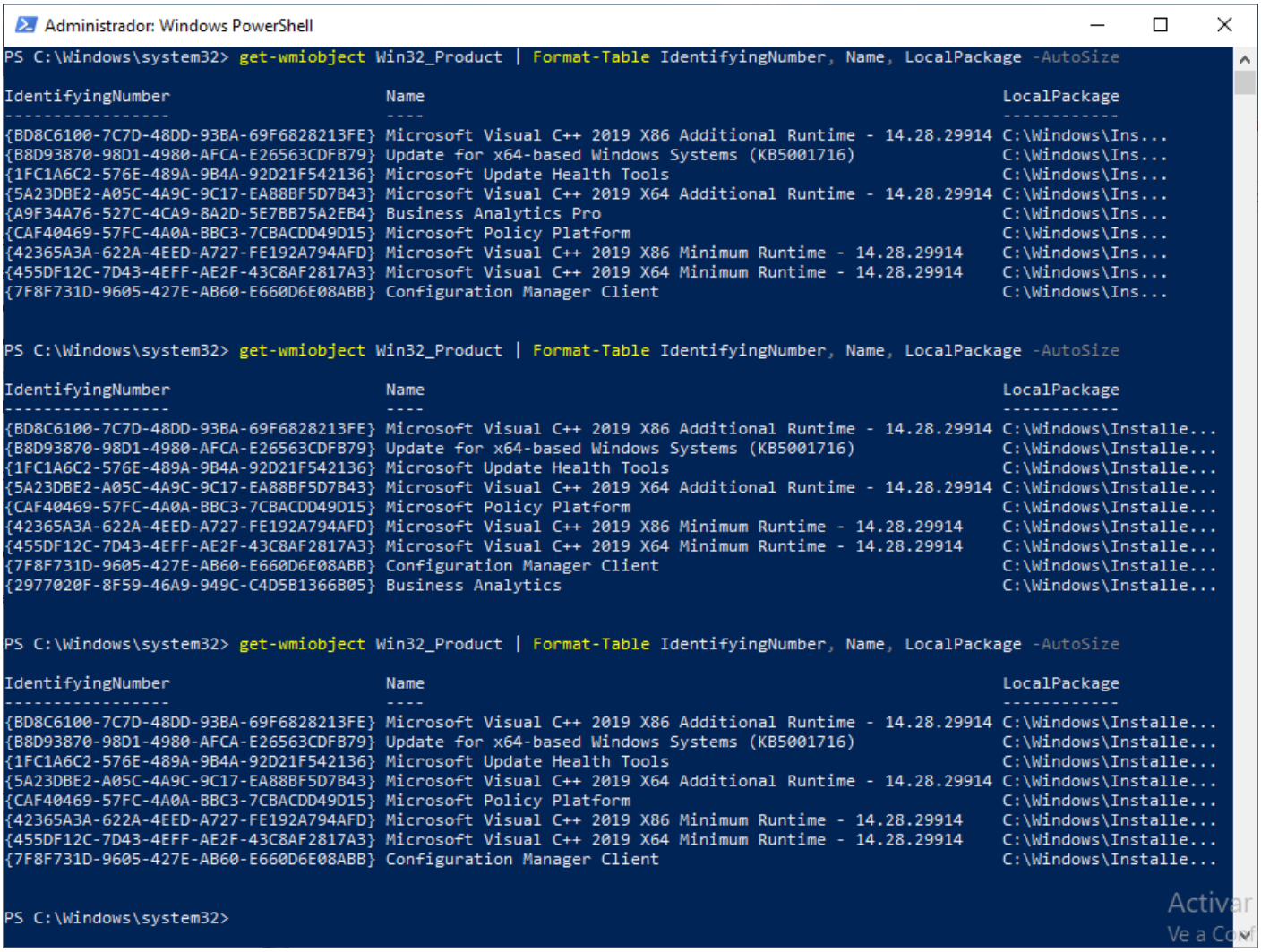


Seleccione la primera opción y de clic en OK. Esto desinstalará el agente en el próximo reinicio de los PC.

Verificación de la desinstalación

Para verificar en un PC de usuario, se puede volver a ejecutar el comando en la consola de **PowerShell** que muestra el listado de las aplicaciones instaladas:

```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



Como se observa, después de ejecutar el comando de desinstalación, ya no aparece la aplicación Business Analytics.