Manage Engine Endpoint Central

Manage Engine Endpoint Central es una tecnología de administración de recursos TI nueva e innovadora

Requisitos previos

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

Debe contar con la capacidad de realizar acciones administrativas en la consola de **Manage Engine** 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 verificar manualmente la instalación del agente.

Los computadores de la organización deben tener previamente el agente del **Endpoint Central** instalado, esto significa que ya un administrador de tecnología ejecutó la instalación del agente y éste se pudo conectar correctamente al servidor donde se encuentra instalado el **Manage Engine**.

En la consola del **Manage Engine** ya existe un **grupo de usuarios o de computadores** y están bien organizados, de tal manera que cuando se lleve a cabo el procedimiento de *NOFRAUD*, se puedan seleccionar de forma correcta los computadores o usuarios que serán objeto de la metodología antifraude.

Debe copiar o descargar el agente de The Fraud Explorer (normalmente llamado ***endpointInstaller.msi***) al equipo desde donde se vayan a ejecutar los procedimientos porque en algún momento se subirán a **Manage Engine**.

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.

Video con todos los pasos

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

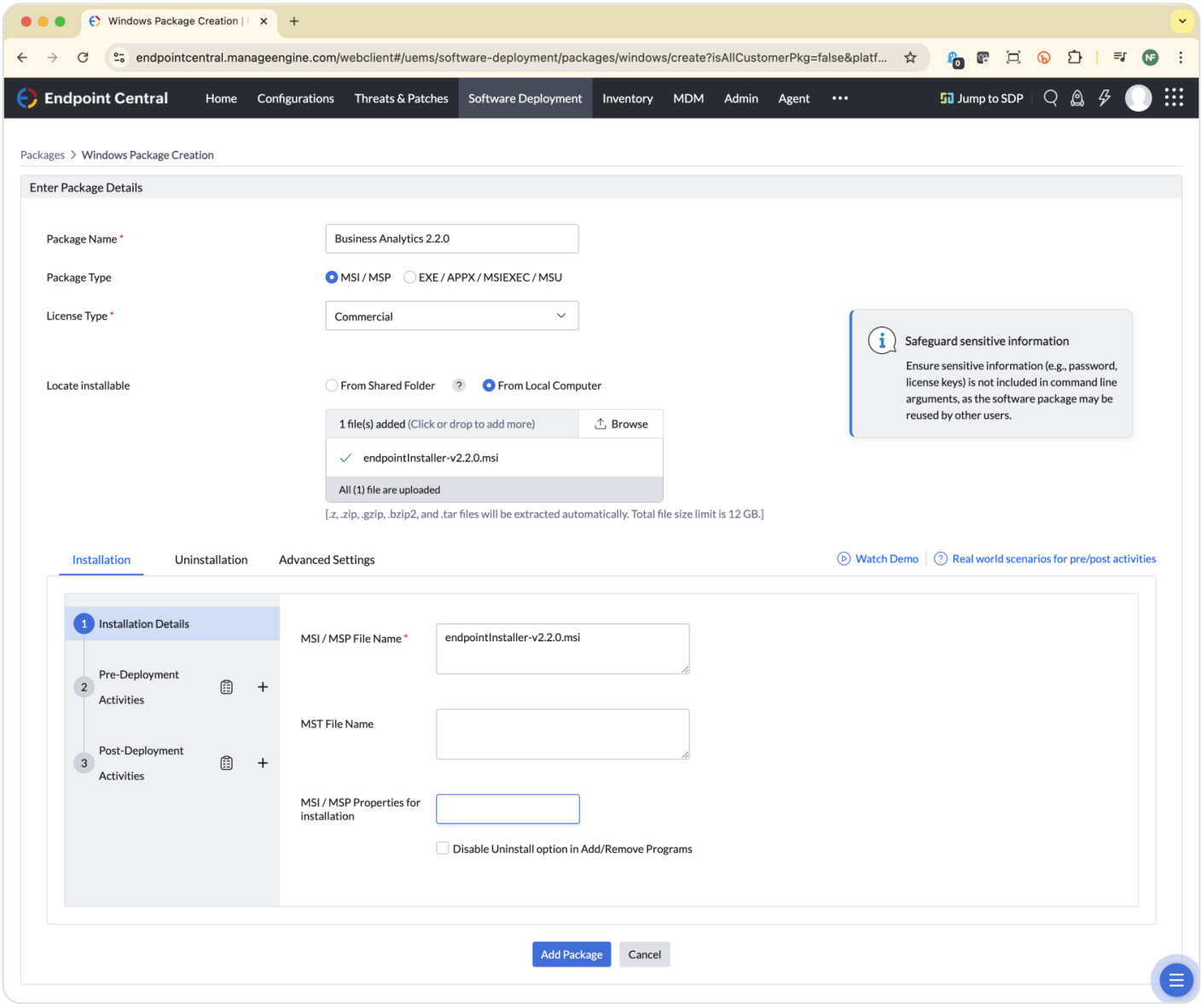
https://www.youtube.com/embed/lxJhzy9gIYg?si=C5NHc-hva1Phka5g

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

Paquete de instalación

Entre a la consola **Endpoint Central**, de clic en **Software Deployment** del menú superior y luego en **Add Package** y **Windows**.



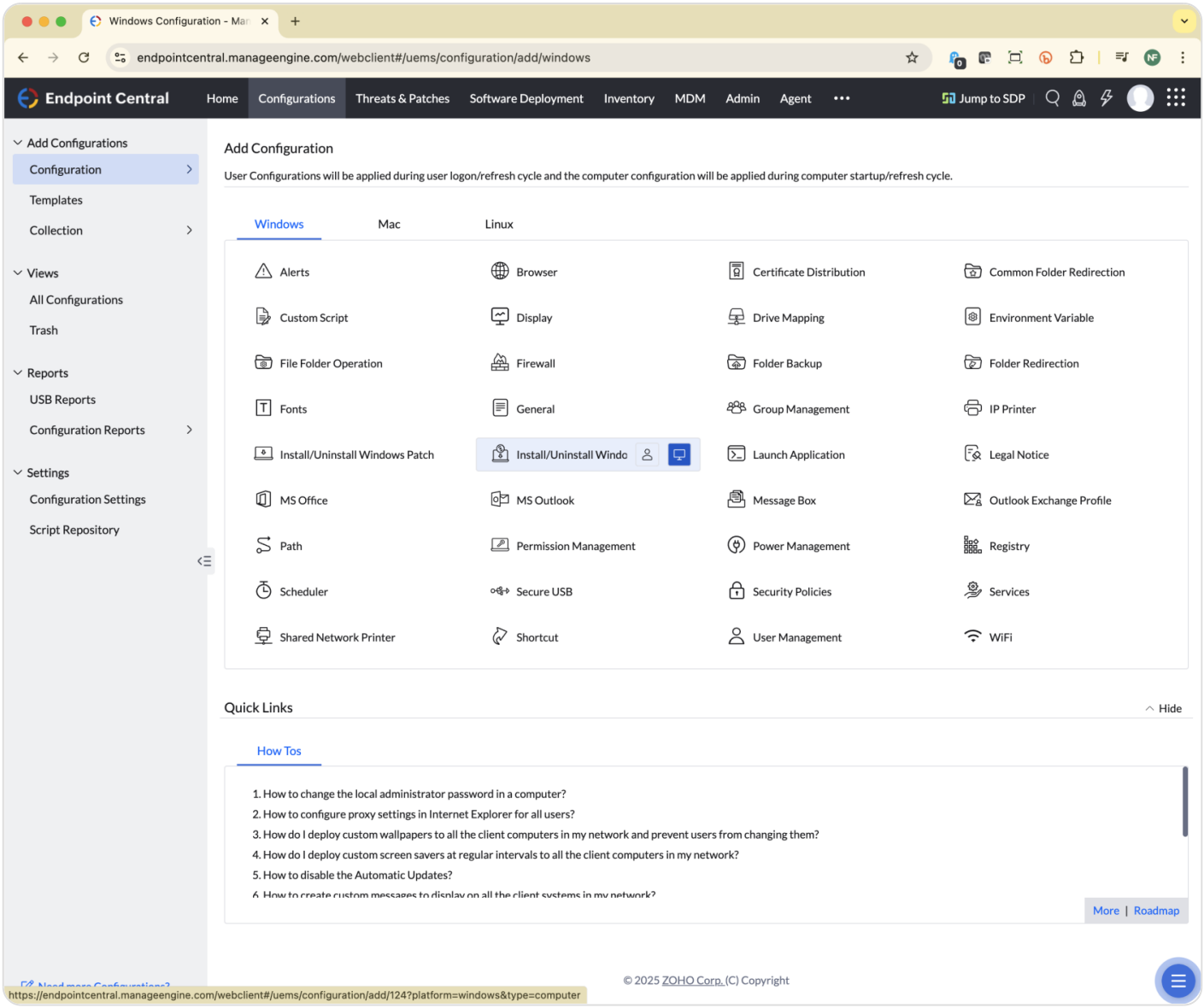
Diligencie el campo **Package Name** y ponga allí **Business Analytics 2.2.0**, en **Package Type** escoja la opción **MSI/MSP**, en **License Type** elija **Commercial**, en **Locate Installable** elija **From Local Computer** y navegue hasta el MSI del agente y para finalizar escriba **endpointInstaller-v2.2.0.msi** (o el nombre del archivo del agente) en el campo **MSI/MSP File Name**. Este nombre de archivo es muy importante porque Endpoint Central lo usará para ejecutar el comando **msiexec.exe** en la máquina destino con éste nombre.

Cuando finalice, de clic en **Add Package** y estará listo para continuar con el siguiente paso.

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

Configuración para la instalación

De clic en **Configurations** en el menú superior y luego de clic en **Create Configuration** y **Windows**, luego seleccione la opción **Install/Uninstall Windows Software** y asegúrese de que selecciona el botón con forma de pantalla y no con forma de usuario.

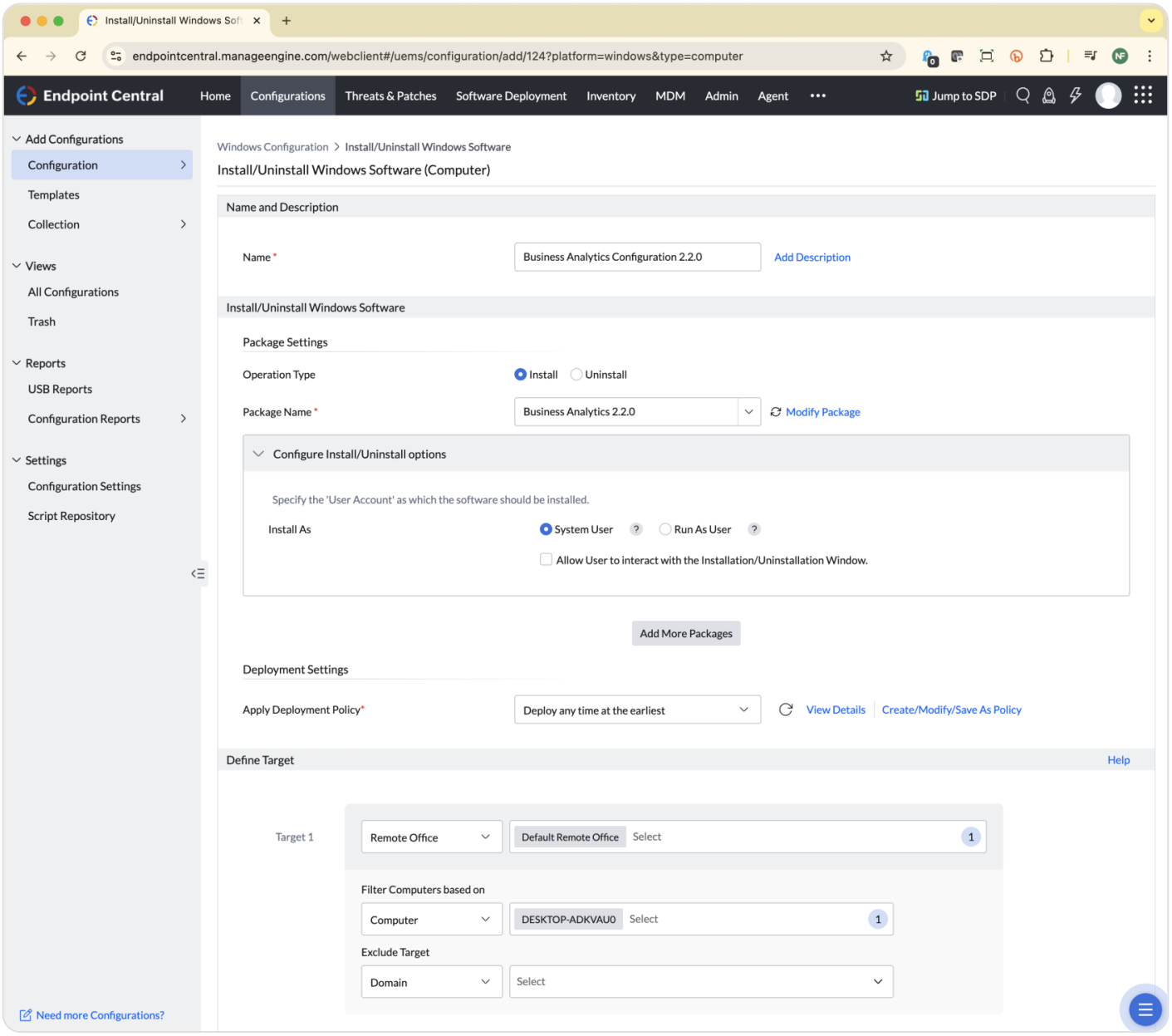


Endpoint Central requiere crear una configuración para realizar un despliegue de software, es decir, separa la creación de un paquete de las acciones a ejecutar sobre él.

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

Deployment del agente

Una vez completado el paso anterior, se le mostrará esta pantalla donde deberá configurar algunas opciones finales para el despliegue del agente.



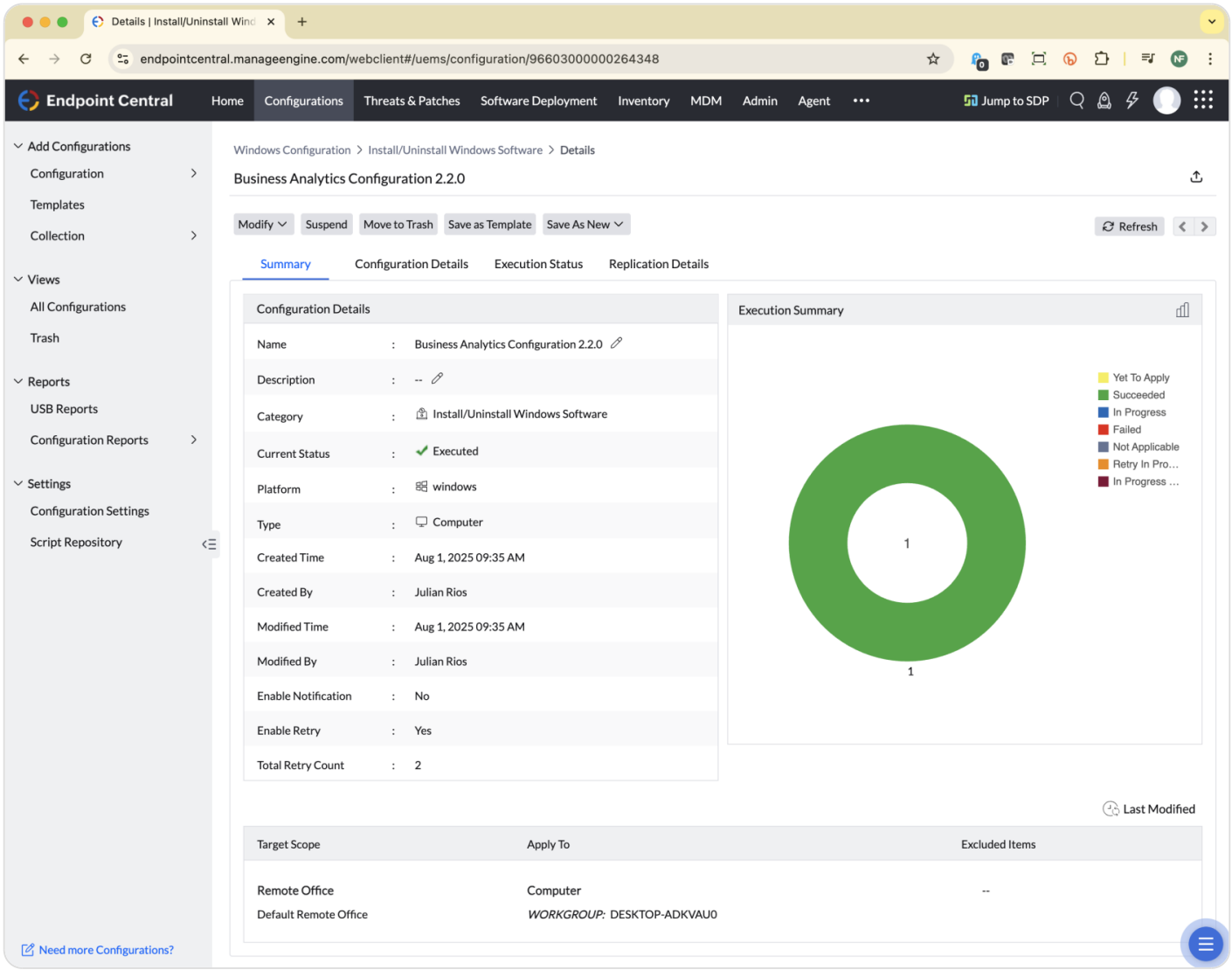
Escriba un nombre para esta configuración, algo como **Business Analytics Configuration 2.2.0**, luego especifique que la operación a llevar a cabo es **Install**, que el paquete es **Business Analytics 2.2.0** (el que se creó en pasos anteriores), que se instale como **System User** y al final en la opción de **Target** elija cuales serán los computadores a los que desea instalarle el agente.

Para finalizar, de clic en el botón **Deploy Immediately**. Esto instalará de manera inmediata el agente en los computadores seleccionados.

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

Monitoreo de la instalación

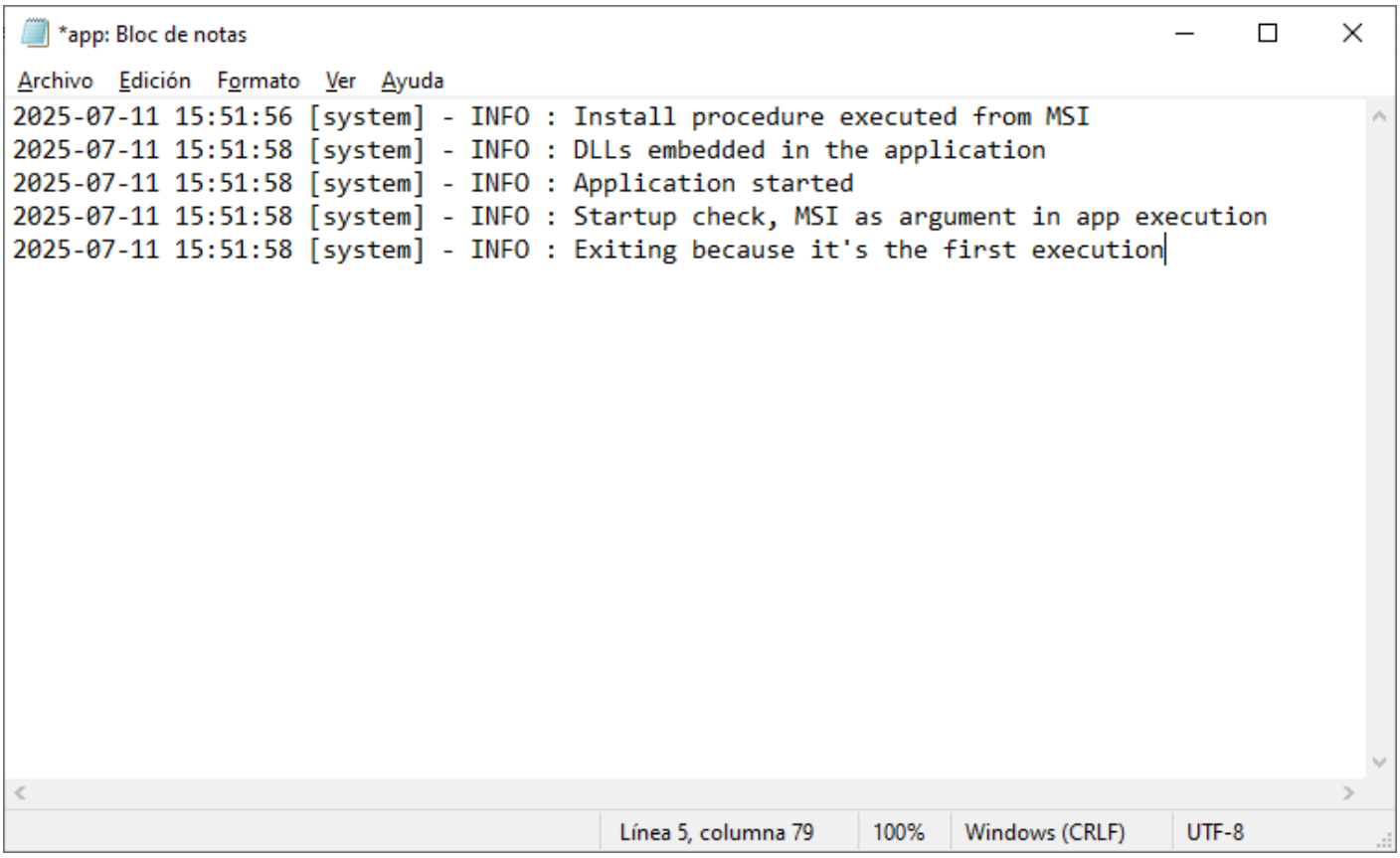
Después de que dé clic en **Deploy Immediately**, aparecerá esta pantalla donde se le mostrará el estado de la instalación.



Tardará aproximadamente 2 minutos en refrescar esta información. Debería aparecer la operación como **Executed**.

Verificación de la instalación

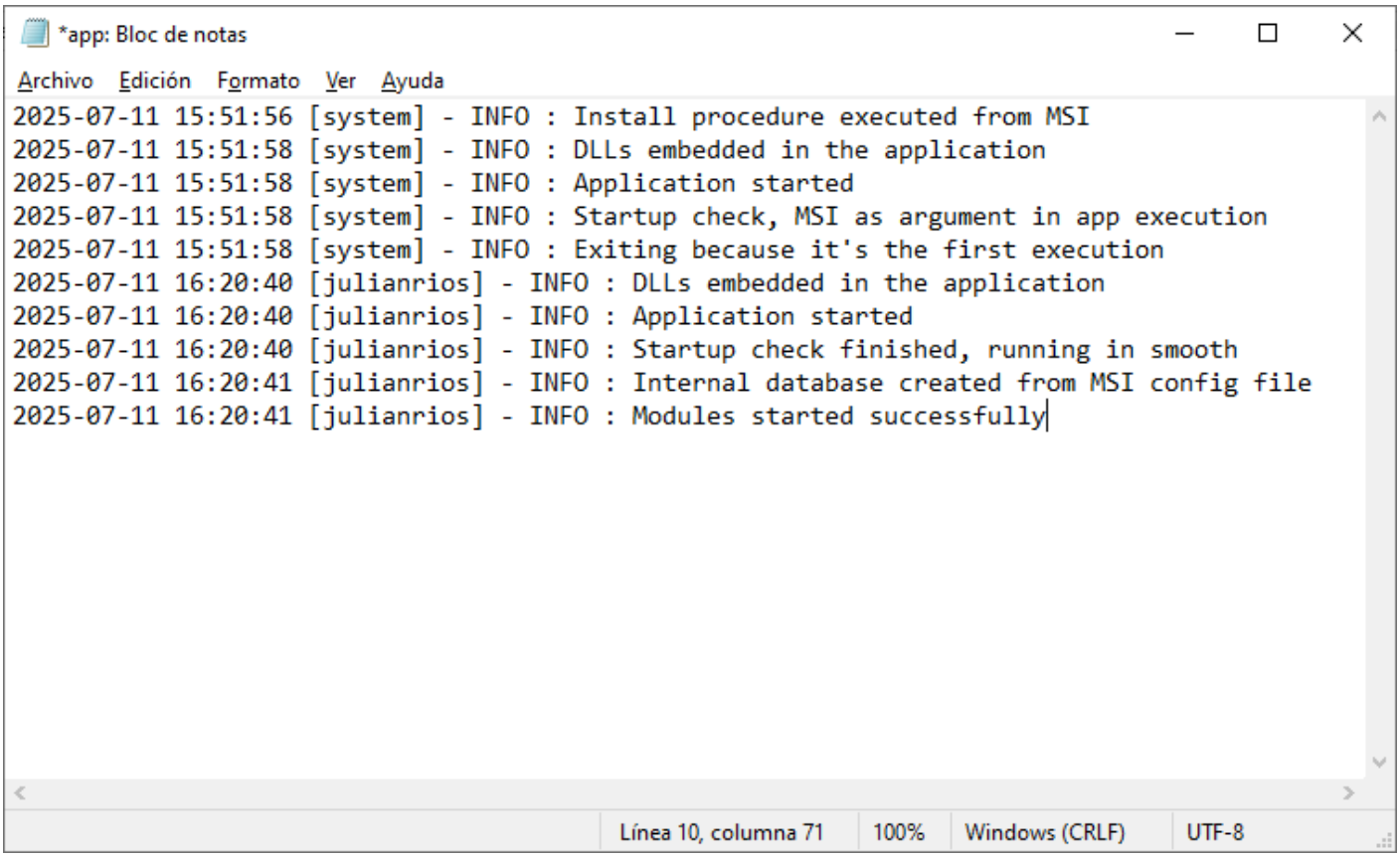
Para verificar la instalación se puede esperar a que en **Microsoft Intune** se muestre el nivel de cumplimiento por aplicación. Sin embargo si queremos verificar directamente en el PC, se debe abrir el archivo de log ubicado en **C:\ProgramData\Software\app.log** con el **blog de notas**.



En este log se puede ver que el usuario que instaló la aplicación es **system** y que además por se la primera ejecución no se inicia el agente. Esto es debido a que el agente está programado para que funcione con privilegios de usuario normal, no con privilegios de administrador ni system por seguridad.

Reinicio del PC

Para que el agente de The Fraud Explorer empiece a funcionar, se debe reiniciar el PC. Una vez reiniciado el PC se puede volver a a abrir el archivo C:\ProgramData\Software\app.log donde se verá información sobre su primera ejecución.

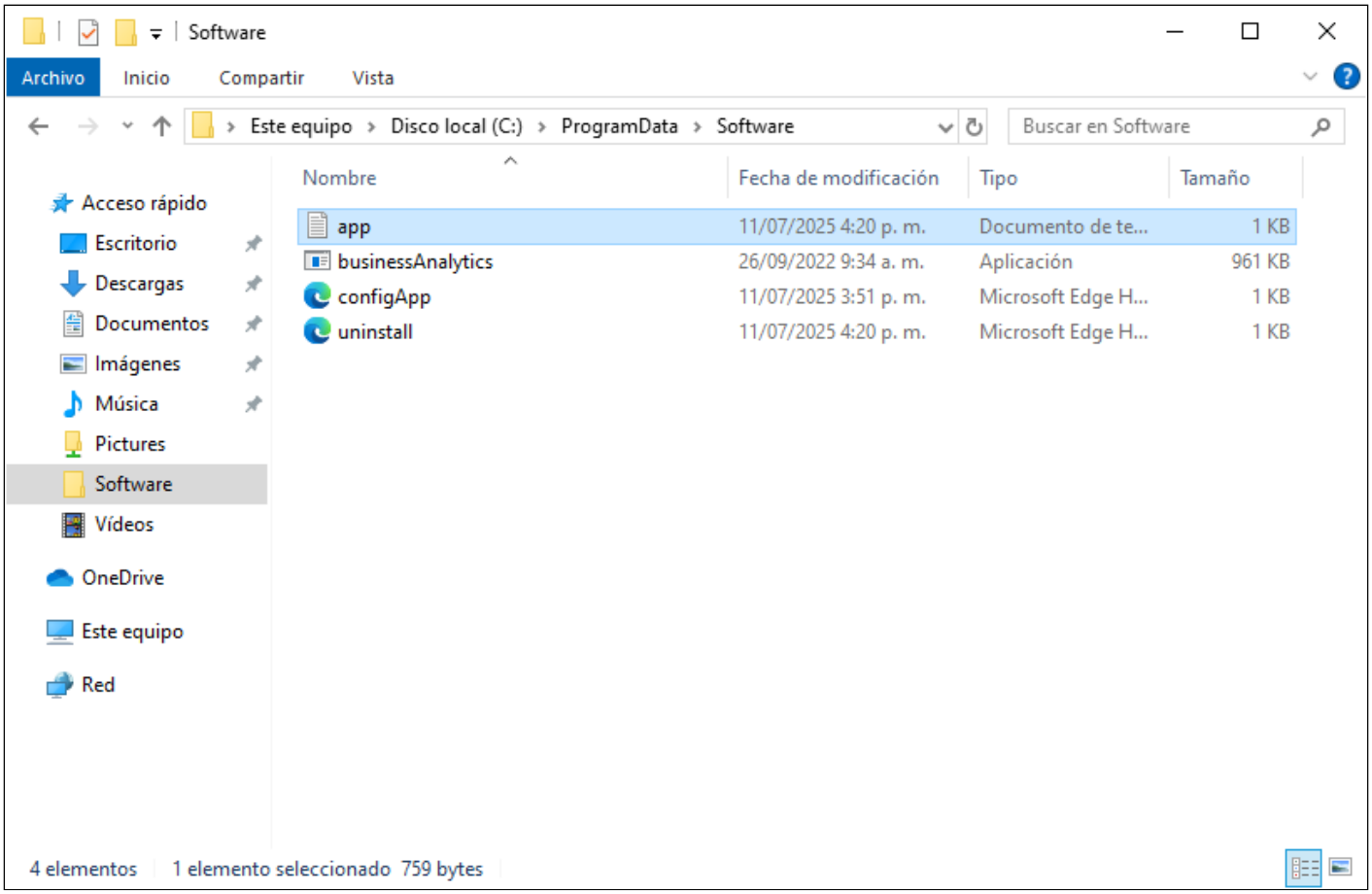


Como se observa, ya la ejecución se hace con un usuario normal sin privilegios elevados y de esa manera el agente de The Fraud Explorer lo detecta y procede a arrancar diciendo **Modules started successfully**.

El agente de The Fraud Explorer está configurado internamente para no permitir que se arranque con usuario administrador ni system.

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**.

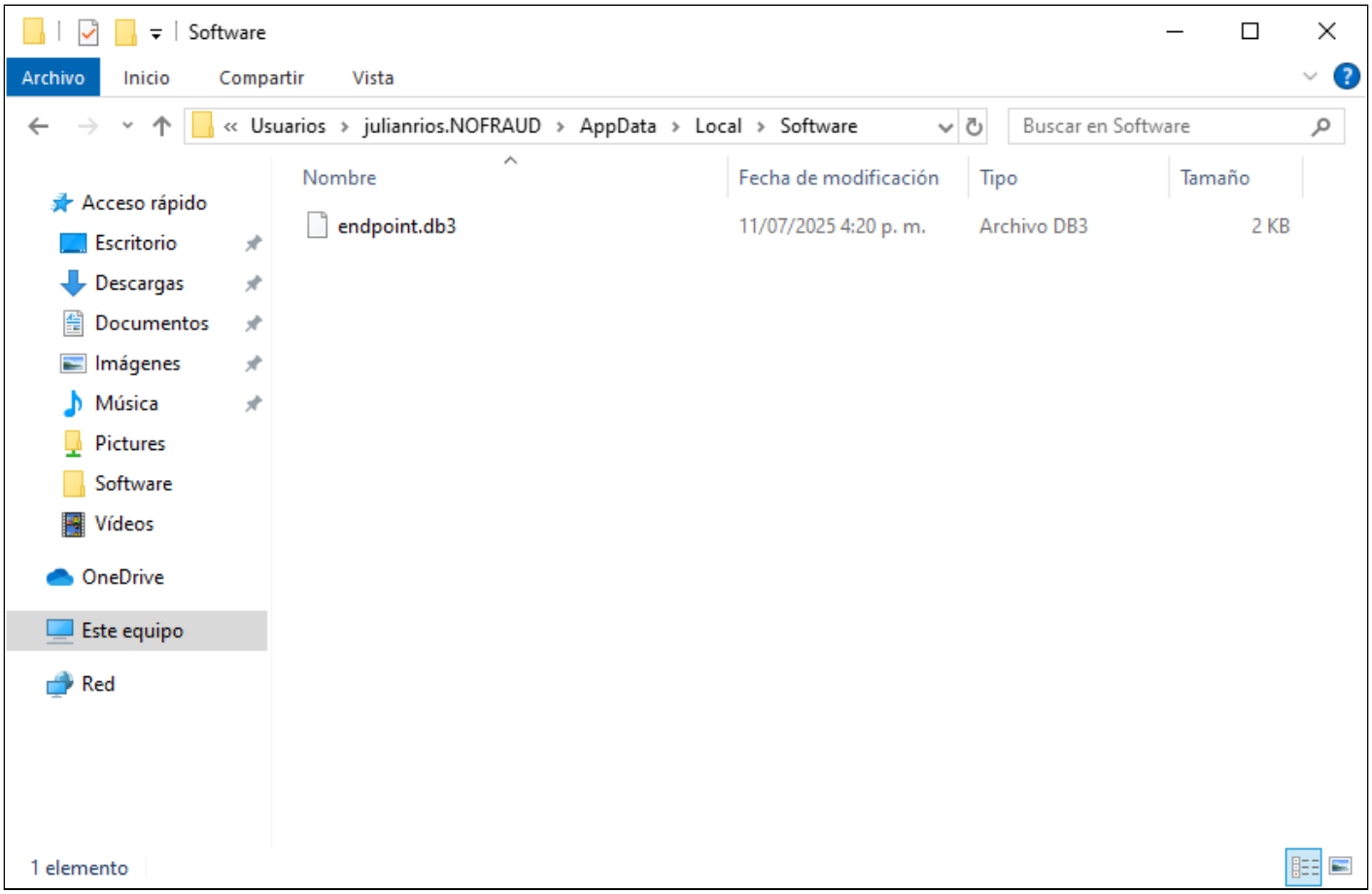


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe** .

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.

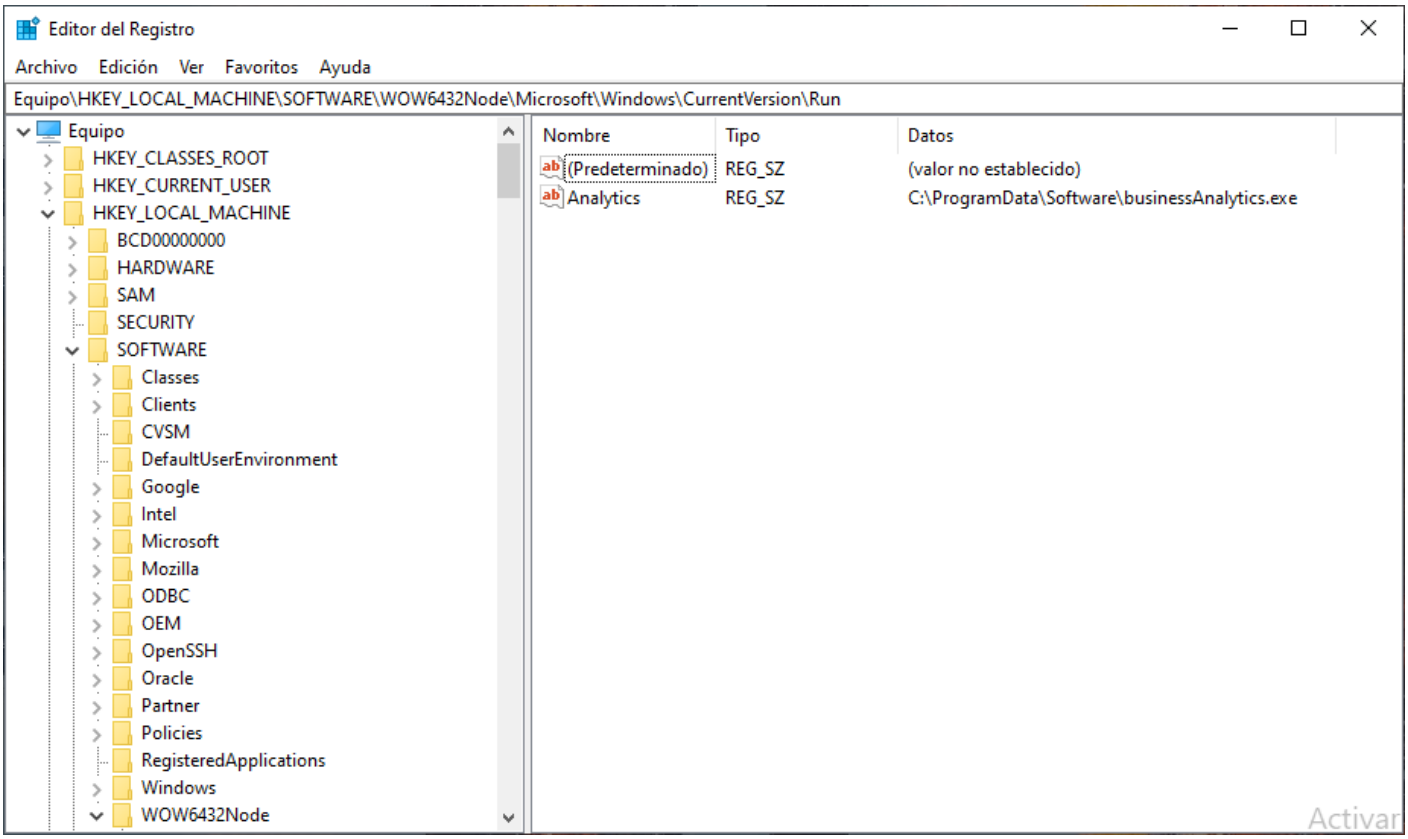


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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**.

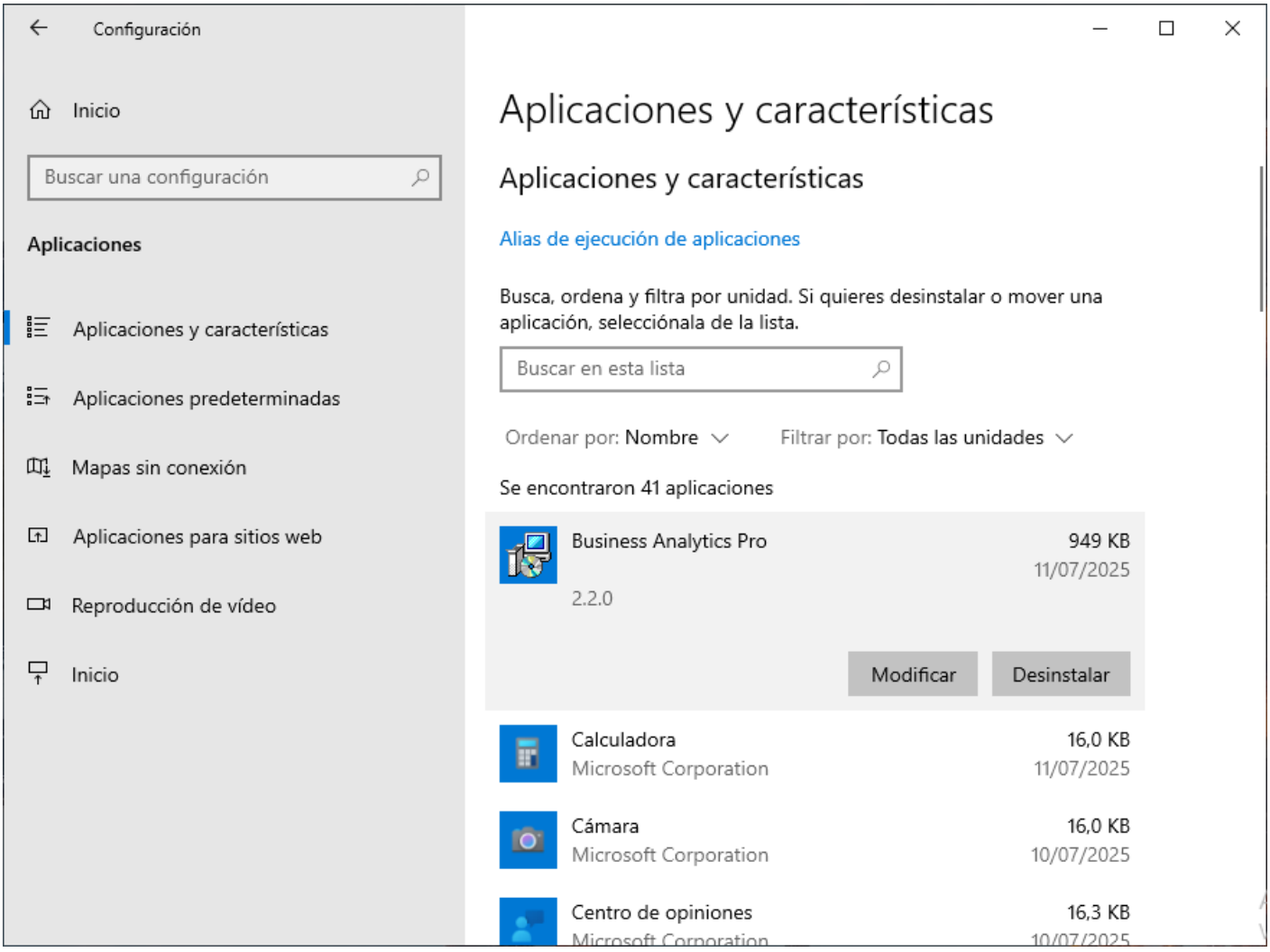


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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**.



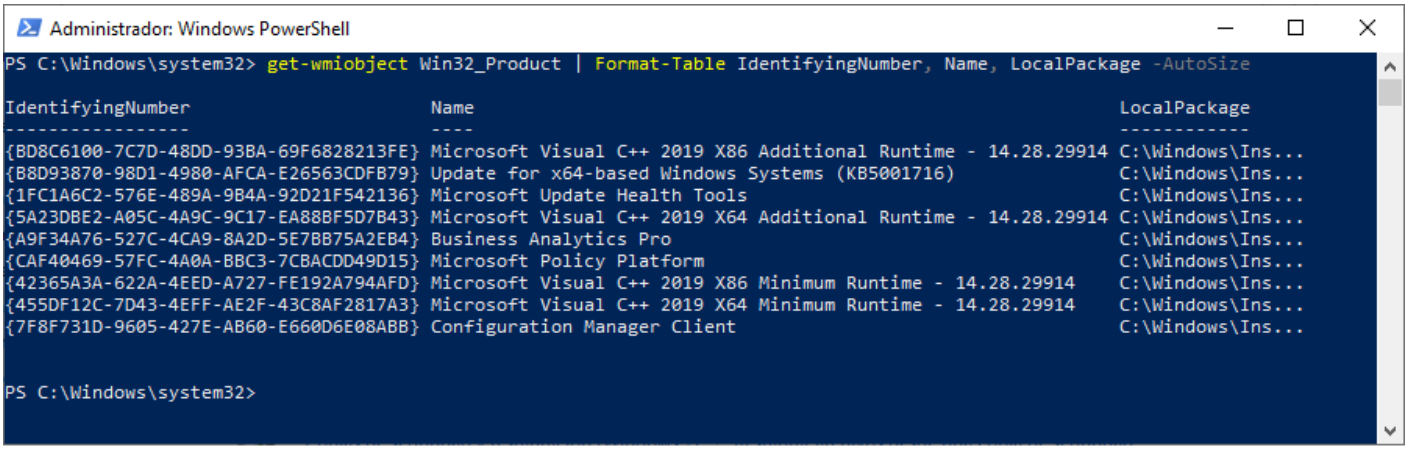
Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se re-emplaza la actual con la nueva versión.

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

ProductID con PowerShell

Se puede verificar la instalación del agente de The Fraud Explorer a bajo nivel con **PowerShell**. Para ello debe ejecutar el siguiente comando en modo administrador:

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

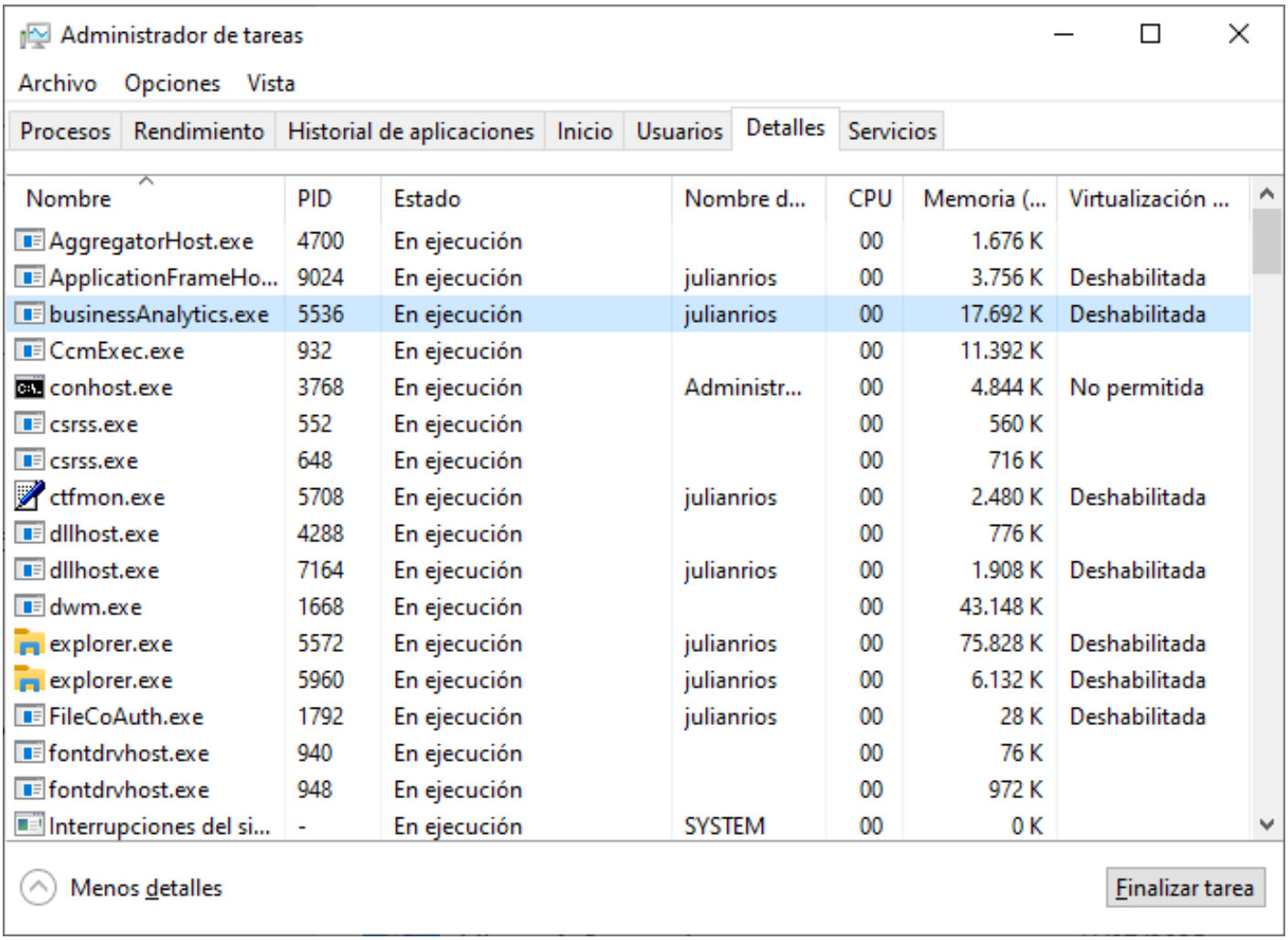


El comando mostrará información relevante como el nombre del producto, el ID del producto y la ubicación del archivo MSI dentro del caché de archivos de instalación de Windows.

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

Monitoreo del agente

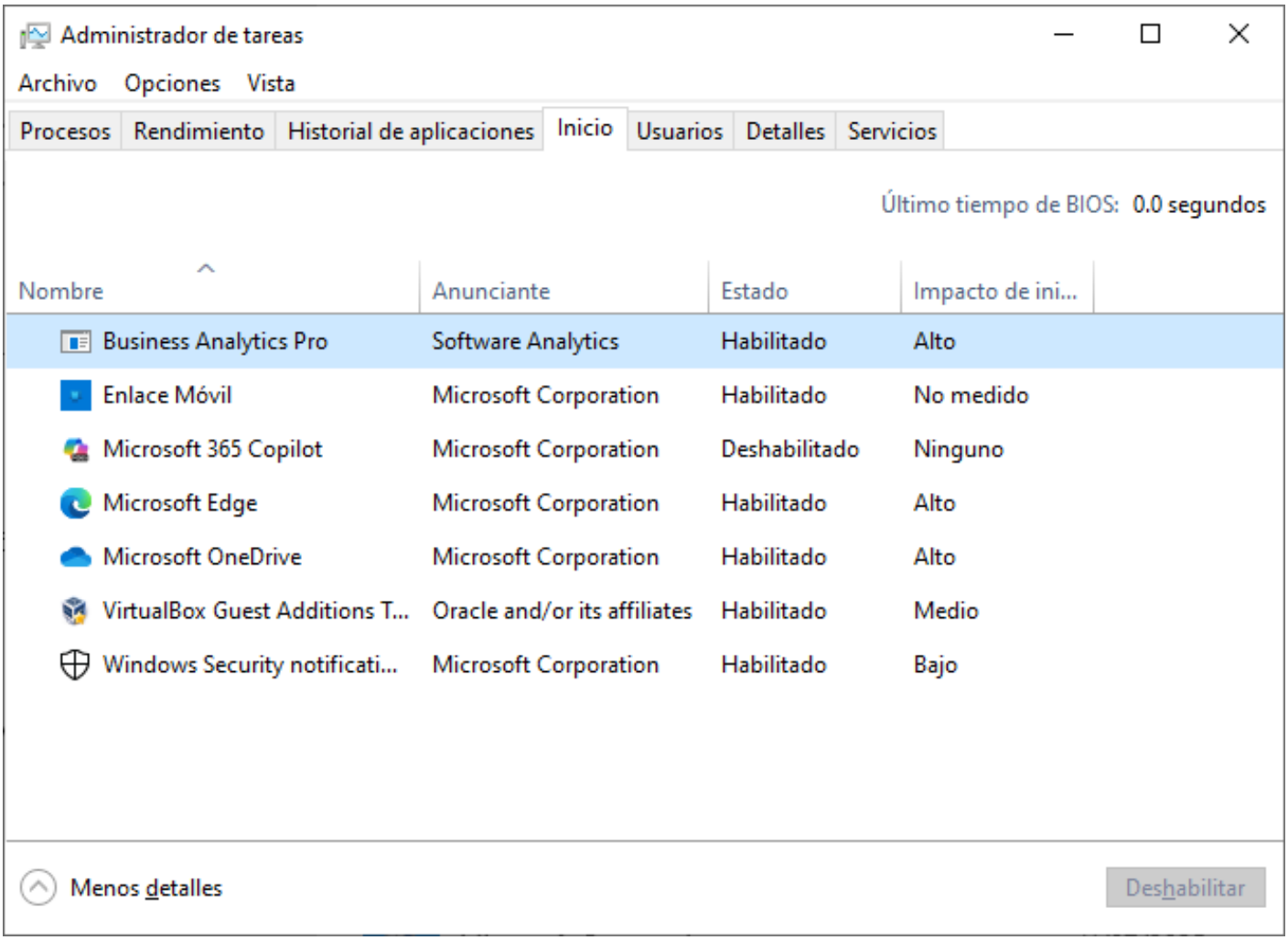
En el PC del usuario, se puede abrir el **Administrador de tareas** y en la pestaña **Detalles** buscar el ejecutable **businessAnalytics.exe**.



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**.

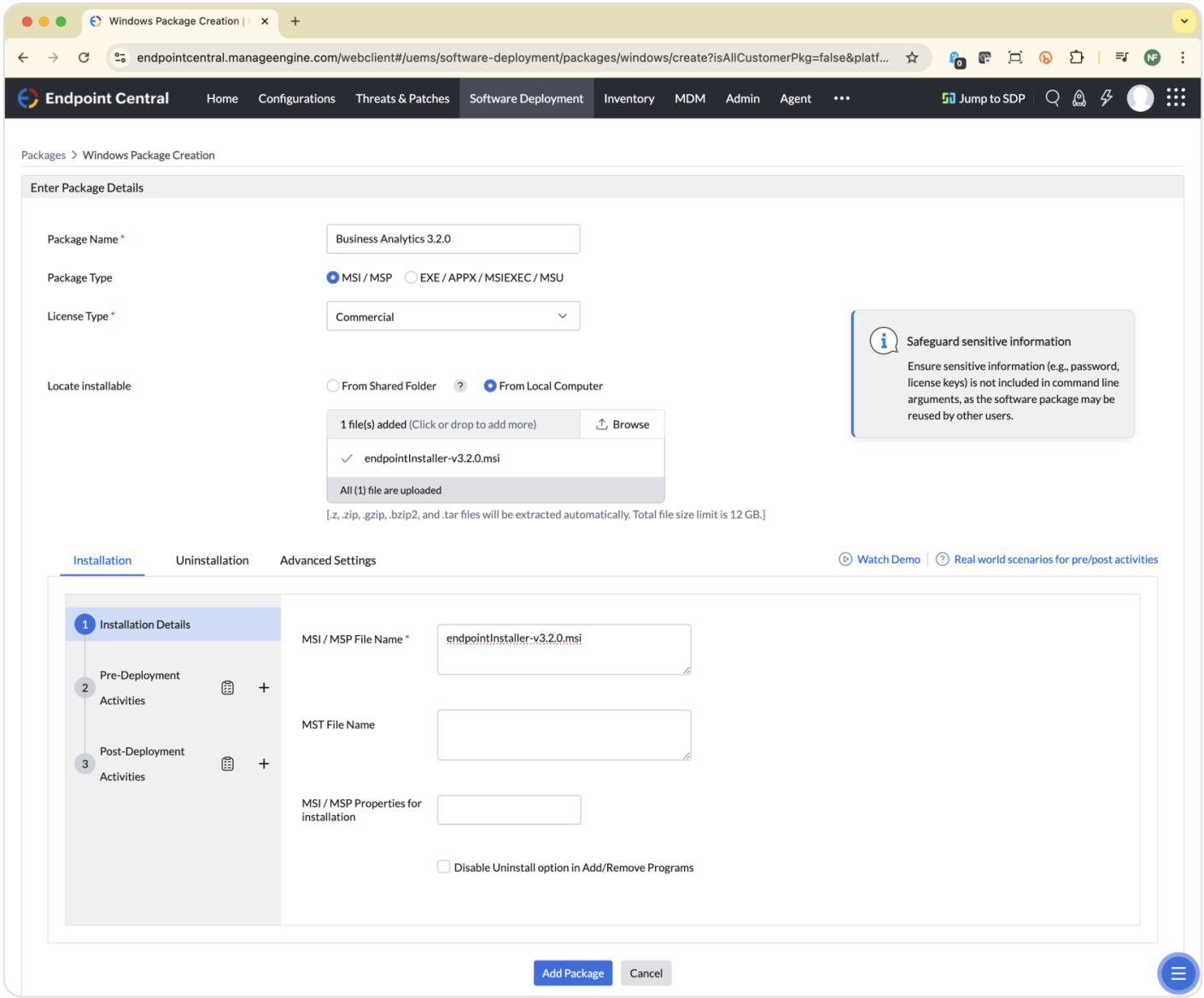


En esta ventana se muestran todas las aplicaciones que arrancan cuando el usuario inicia sesión con su cuenta en Windows. El agente de The Fraud Explorer no arranca como servicio y no interfiere en el proceso de arranque de sistema operativo.

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.

Crear paquete para actualización

Para actualizar la versión del agente antifraude se debe crear un nuevo paquete siguiendo los mismos pasos que el paquete anterior. Debe dar clic en **Software Deployment** del menú superior, **Add Package**, **Windows** y diligenciar como se indica a continuación.



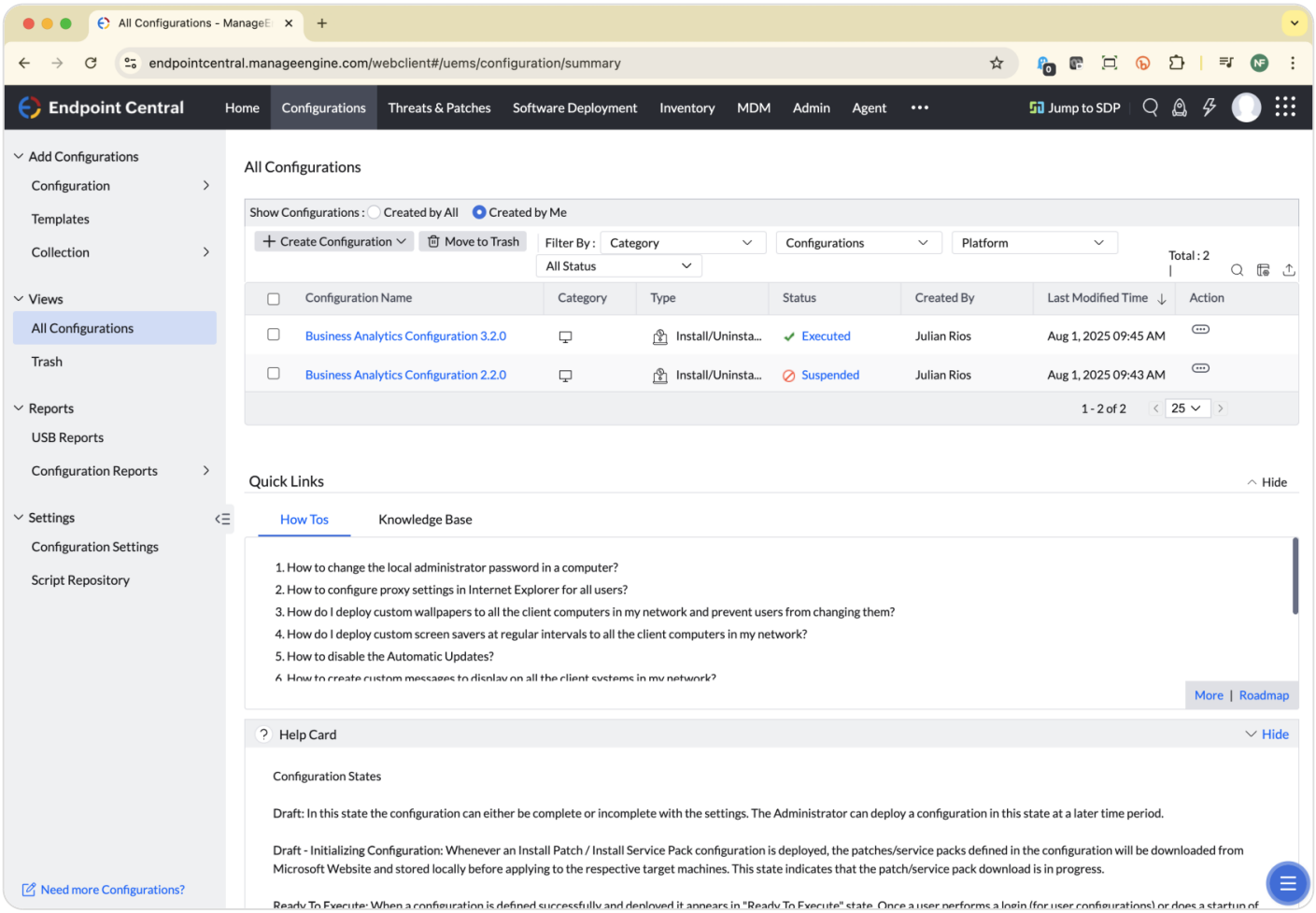
En **Package Name** escribir **Business Analytics 3.2.0** (o la versión actual), en **Package Type** escoger **MSI/MSP**, en **Locate Installable** escoger **From Local Computer** y subir el archivo MSI del agente, en **MSI/MSP File Name** escribir exactamente el nombre del archivo MSI que acaba de subir, en este caso **endpointInstaller-v3.2.0.msi.** Es muy importante que no se equivoque escribiendo el nombre del archivo puesto que este nombre será usado por el comando **msiexec.exe** para instalar el agente.

Para finalizar de clic en **Add Package** y estará listo para continuar con el siguiente paso.

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

Suspender version anterior

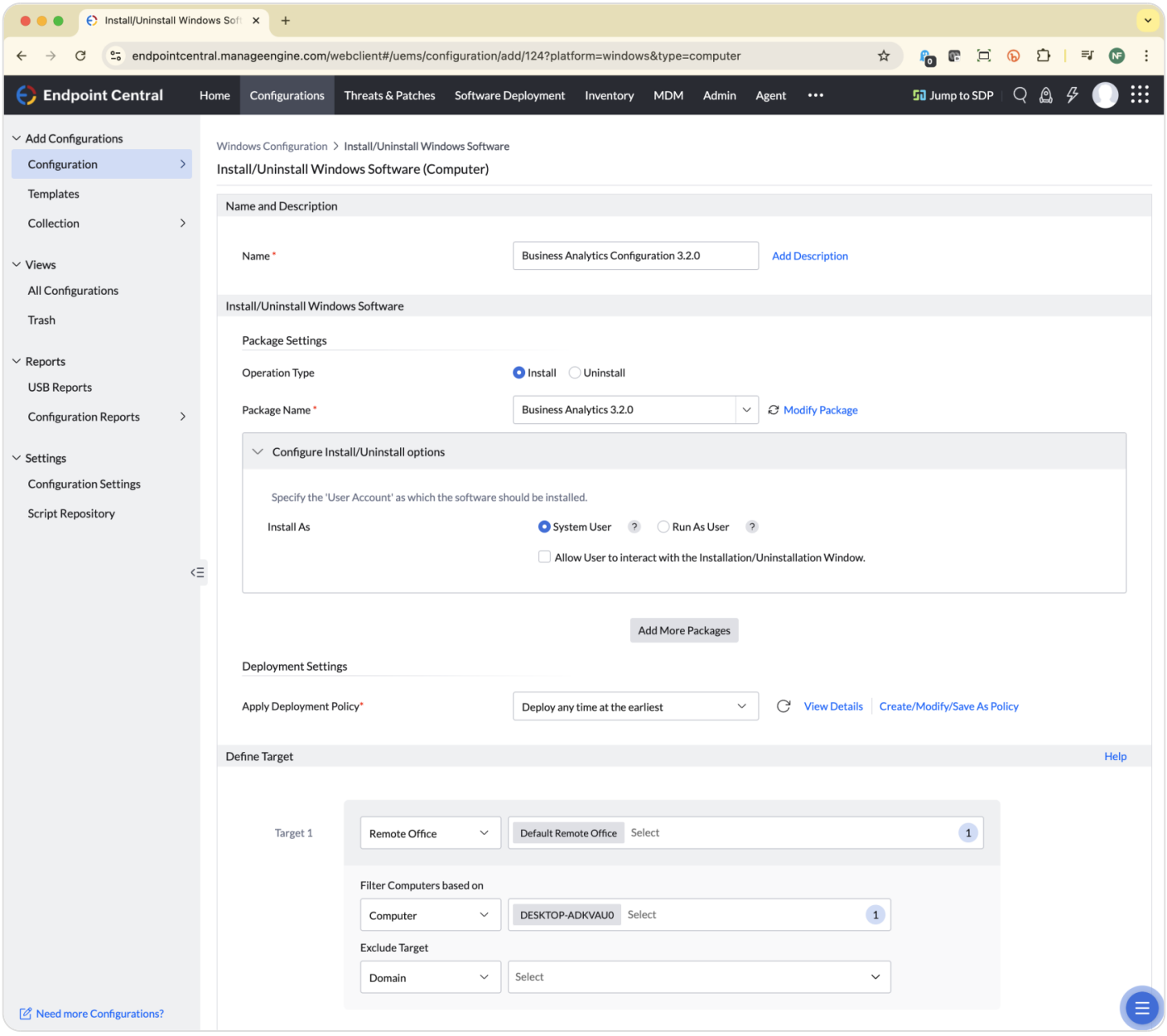
Para evitar conflictos al momento de gestionar instalaciones y actualizaciones, se recomienda suspender la configuración de los agentes con versiones anteriores y dejar activa solamente la versión actual.



Para suspender una configuración, seleccione los **tres puntos** de la columna **Action** y de clic en la opción **Suspend** del menú desplegable.

Configuración para la actualización

De clic en **Configurations** en la parte superior del menú, luego en **Create Configuration**, **Windows** y asegúrese de seleccionar la opción **Install/Uninstall Windows Software** con el ícono de la pantalla y no del usuario. Una vez hecho esto le aparecerá la siguiente ventana donde deberá diligenciar los datos como se indica.

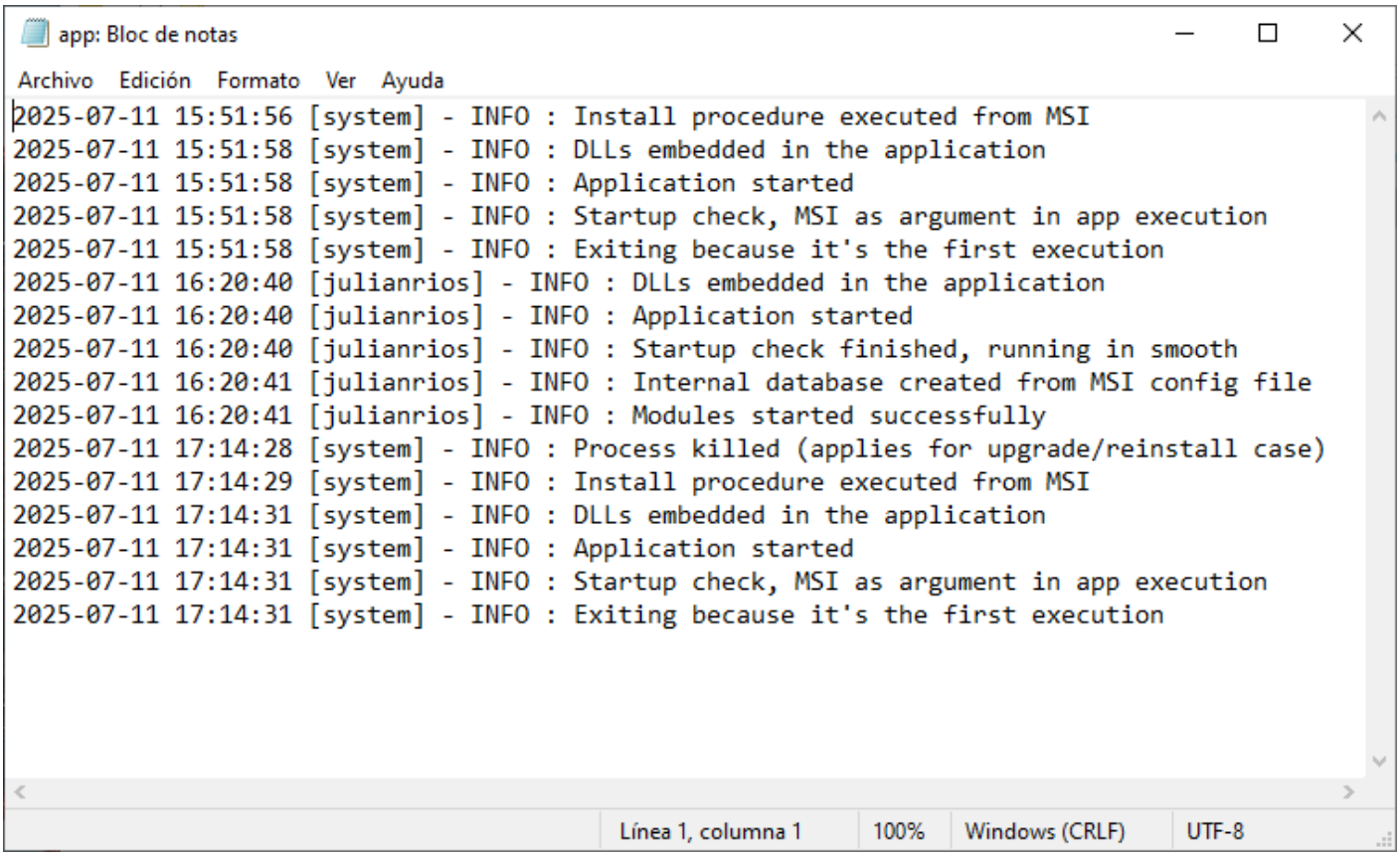


En **Name** escriba **Business Analytics Configuration 3.2.0** (o el nombre que prefiera), en **Operation Type** seleccione **Install**, en **Install As** seleccione **System User** y en **Target** seleccione el grupo objetivo de PCs que serán objeto de la metodología antifraude.

Al finalizar de clic en el botón **Deploy Immediately**. Esto desplegará automáticamente el agente en los PCs destino. El proceso de actualización se manera internamente en el MSI, es decir, una vez instalado, el MSI detecta versiones anteriores del agente instaladas y hace todo lo necesario para no generar duplicados.

Verificación de la actualización

En el PC del usuario donde se llevó a cabo la actualización, se puede abrir el archivo **C:\ProgramData\Software\app.log** para verificar que la actualización se haya llevado a cabo con éxito.

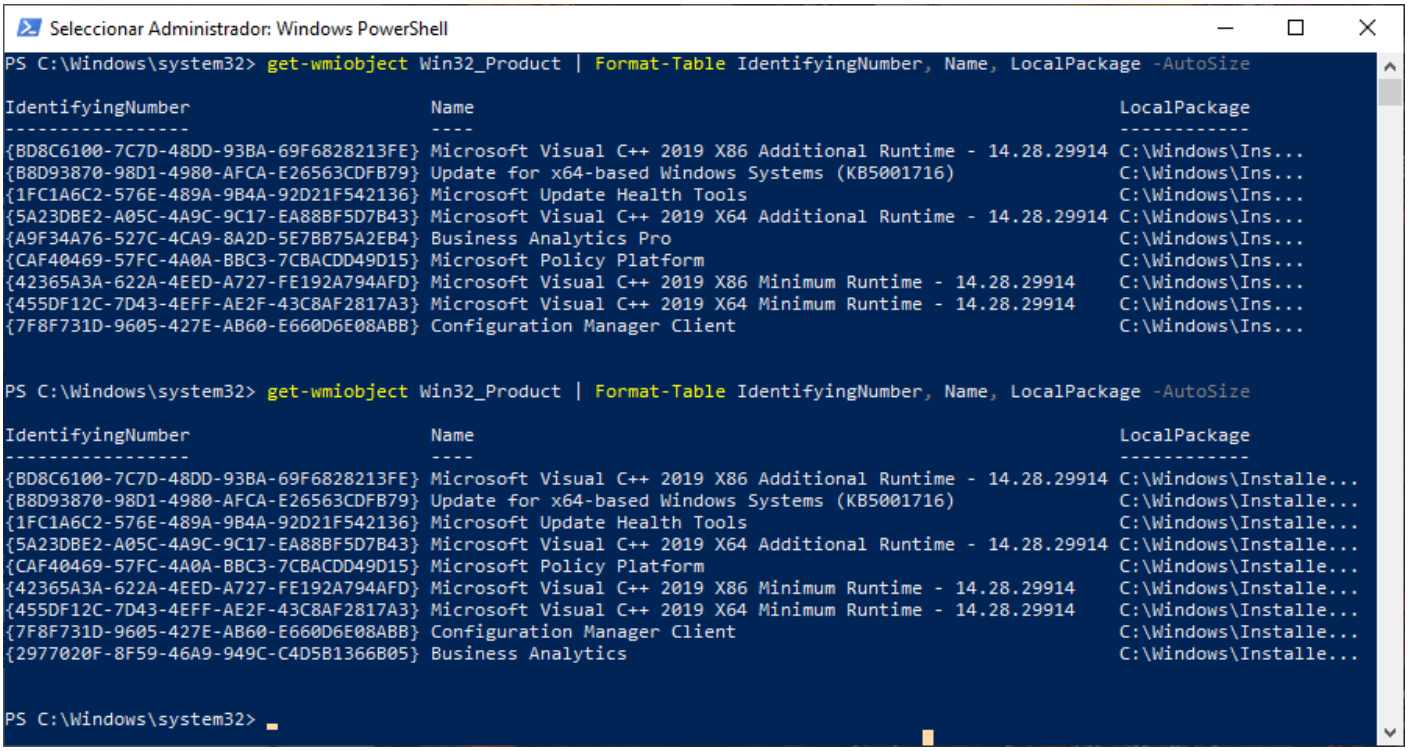


Deberá aparecer el mensaje **Process killed (applies for upgrade/reinstall case)** y se mostrará la usuario **system** como el ejecutor de esa actividad.

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:

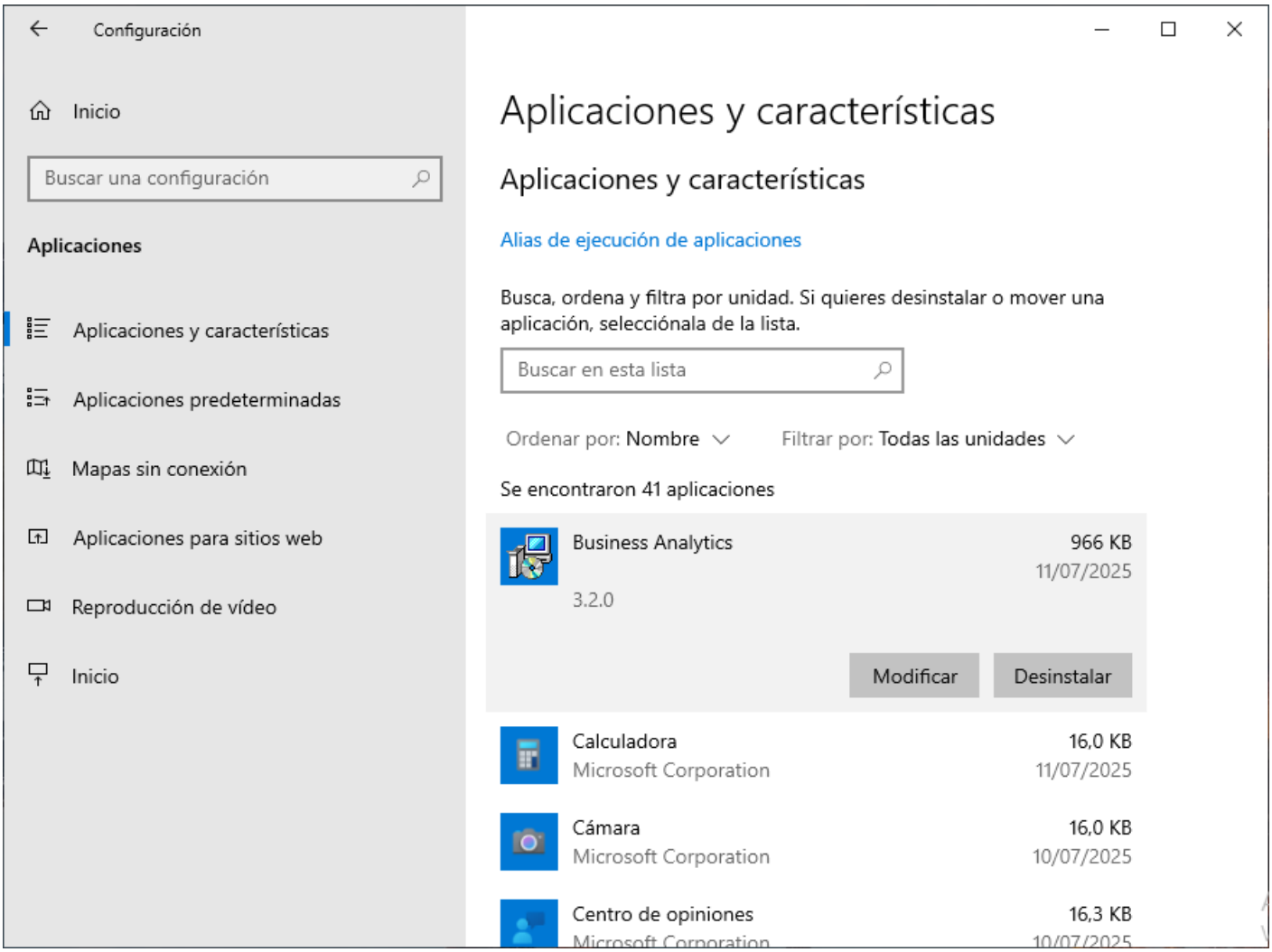
```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



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.

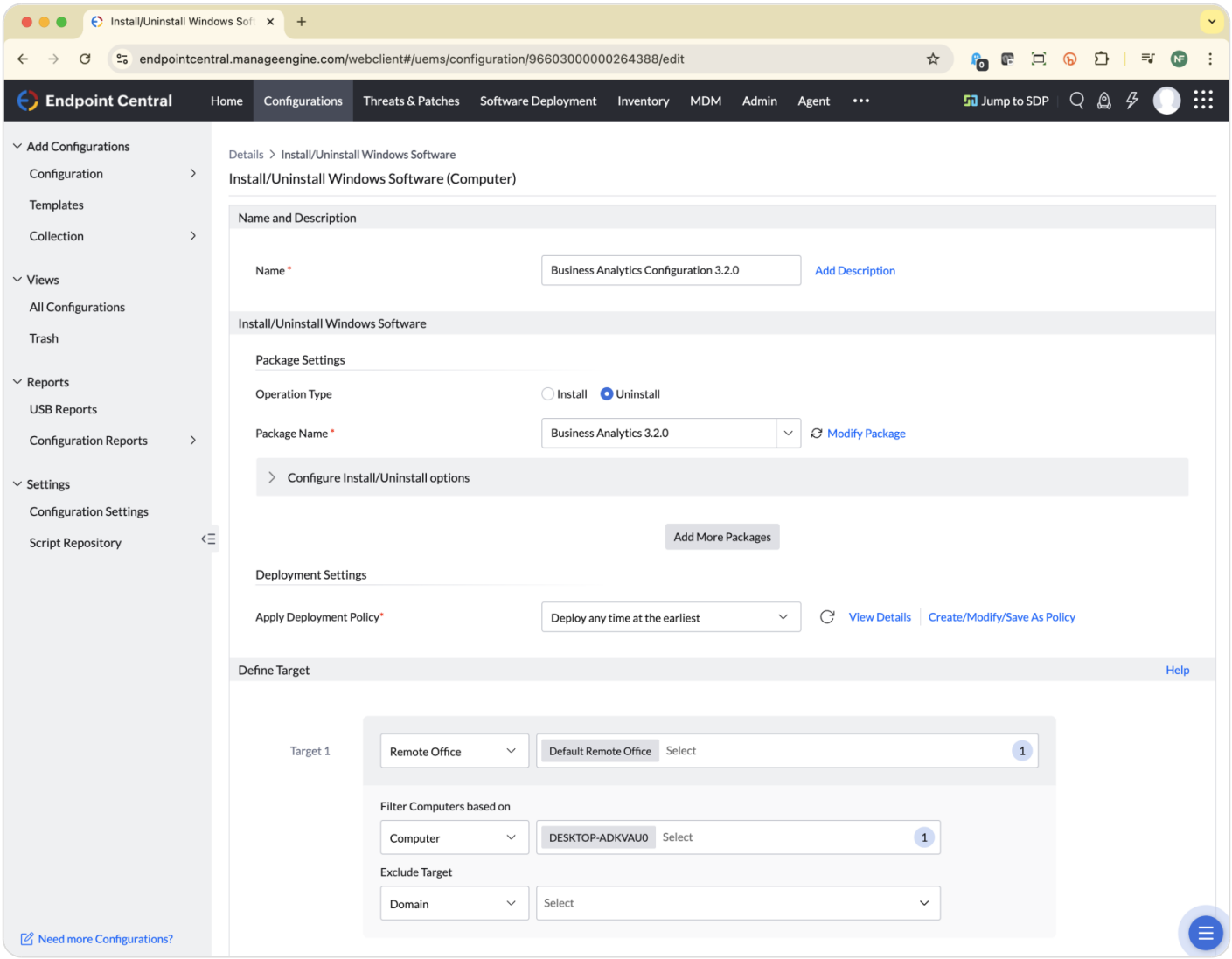


Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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

Desinstalación del agente

Sobre la última configuración guardada, edítela y cambie el tipo de operación de **Install** a **Uninstall**.

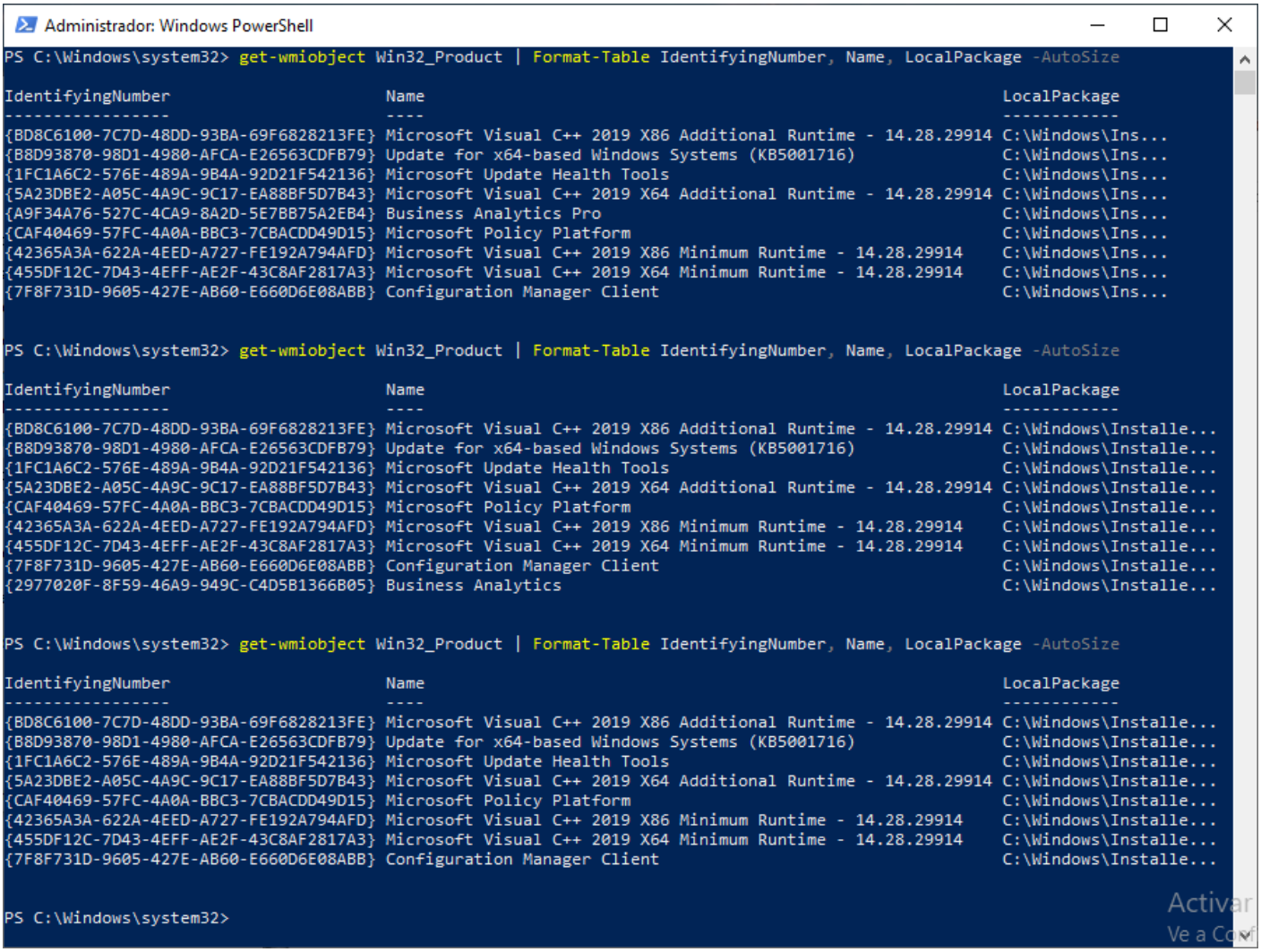


De clic en el botón **Deploy Immediately** y esto desinstalará la última versión del agente en los computadores.

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 crear la configuración de desinstalación en **Endpoint Central**, ya no aparece la aplicación Business Analytics.