

Despliegue del agente antifraude

En esta sección se tratarán todos los procedimientos necesarios para implementar el agente de monitoreo antifraude en una organización.

- Características del agente
- System Center Configuration Manager
 - Requisitos previos
 - Video con todos los pasos
 - Ingreso a SCCM
 - Creación de una Aplicación
 - Información de la Aplicación
 - Sumario de la creación de la Aplicación
 - Configuración de la distribución
 - Tipo de distribución
 - Comandos para instalar y desinstalar
 - Experiencia de usuario
 - Método de detección
 - Despliegue de la Aplicación
 - Selección de usuarios o dispositivos
 - Punto de distribución
 - Acción de despliegue
 - Agendamiento del despliegue
 - Experiencia del usuario
 - Alertas de despliegue
 - Resumen del despliegue
 - Forzar política en PC

- Verificación de la instalación
- Reinicio del PC
- Archivos que crea el agente
- Base de datos del agente
- Entradas de registro de Windows
- Aparición en programas instalados
- ProductID con PowerShell
- Monitoreo del agente
- Inicio del agente
- Actualización del agente
- Información de la actualización
- Resumen de la actualización
- Propiedades de la actualización
- Configurar la supersedencia
- Tipo de despliegue de actualización
- Experiencia de usuario en actualización
- Despliegue de actualización
- Destino de contenido para actualizar
- Acción de actualización
- Agenda de la actualización
- Experiencia para desplegar actualización
- Alertamiento de actualización
- Resumen de actualización
- Verificación de la actualización
- PowerShell para verificar actualización
- Actualización en listado de Aplicaciones
- Desinstalar el agente
- Deployment de la desinstalación
- Acción de desinstalación
- Experiencia de desinstalación
- Resumen de la desinstalación
- Verificación de la desinstalación
- Instalación y desinstalación manual

- Requisitos previos
- Video con todos los pasos
- Instalación del agente
- Verificación de la instalación
- Reinicio del PC
- Revisión de instalación con PowerShell
- Archivos que crea el agente
- Base de datos del agente
- Entradas de registro de Windows
- Aparición en programas instalados
- Monitoreo del agente
- Inicio del agente
- Actualización del agente
- Verificación de la actualización
- PowerShell para verificar actualización
- Actualización en listado de Aplicaciones
- Desinstalación del agente
- Verificación de la desinstalación

- Despliegue con GPO de Active Directory
 - Requisitos previos
 - Video con todos los pasos
 - Abrir Active Directory
 - Grupo de seguridad
 - Creación de la política GPO
 - Nombre de la política GPO
 - Eliminación del filtro por defecto
 - Creación de un nuevo filtro
 - Delegación
 - Delegación del grupo de seguridad
 - Edición de la política
 - Configuración avanzada
 - Propiedades del despliegue
 - Crear el link de la política
 - Aplicar la política con gpupdate

- Aplicar la política en un PC
- Comprobación de la política
- Verificación de la instalación
- Reinicio del PC
- Revisión de instalación con PowerShell
- Archivos que crea el agente
- Base de datos del agente
- Entradas de registro de Windows
- 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

Características del agente

Antes de iniciar cualquier proceso de instalación, actualización o desinstalación, es importante que conozca la estructura del agente para que prepare su infraestructura y permita su funcionamiento. A continuación se realizará una caracterización de sus propiedades:

Conectividad	El agente requiere comunicarse con un servidor externo. Esta comunicación sucede solamente en una vía (agente - > servidor) y lo hace por 2 puertos, uno TCP y uno UDP. Los clientes recibirán un correo indicando cuáles son estos puertos para que procedan a configurar sus Firewalls.
Seguridad en su ejecución	Los antivirus podrían impedir que el agente se ejecute, por ello será importante añadir a la lista de exclusión la carpeta donde se aloja y el MD5 y SHA-1 de su ejecutable.
Carpetas y archivos que se crean	C:\ProgramData\Software es la ruta donde se almacena el ejecutable. C:\Users\usuario\AppData\Local\Software\endpoint.d b3 es la bse de datos. C:\ProgramData\Software\businessAnalytics.exe es el ejecutable. C:\ProgramData\Software\app.log es el archivo de log. C:\ProgramData\Software\uninstall.xml configuración para su desinstalación. C:\ProgramData\Software\configApp.xml configuración del agente. C:\Users\usuario\AppData\Roaming\BusinessAnalytic s aquí se almacenan los archivos que se usan durante la instalación del agente.
Entrada en el registro de Windows	HKEY_LOCAL_MACHINE, SOFTWARE, WOW6432Node, Microsoft, Windows, CurrentVersion, Run.
Espacio en disco duro	1.2 MB (1280 Kb)
Memoria RAM que consume	Entre 8 MB y 17 MB de memoria RAM.
Compatibilidad con Windows	Windows XP 32 y 64 Bits hasta Windows 11, con .NET Framework 4.8

Conociendo estas propiedades, puede proceder con el despliegue del agente.

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

System Center Configuration Manager

El agente de The Fraud Explorer puede ser desplegado de manera masiva y silenciosa en los dispositivos corporativos de una organización a través de su módulo SCEM (System Center Endpoint Manager)

Requisitos previos

Antes de ejecutar cualquier procedimiento en la consola de **Microsoft SCCM** es importante tener en cuenta los siguientes requisitos previos:

Debe contar con la capacidad de realizar acciones administrativas en la consola **SCCM** 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 quipos para no tener que esperar mucho tiempo a que se haga de forma natural.

Los computadores de la organización deben tener previamente el agente **SCCM** instalado, esto significa que ya un administrador de tecnología ejecutó la instalación del agente (CCMSetup.exe) y éste se pudo conectar correctamente al servidor donde se encuentra instalado el **System Center Configuration Manager**.

En la consola **SCCM** ya existe un **colección de usuarios o de dispositivos** y están bien organizados, 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 SCCM o al 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 SCCM 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.

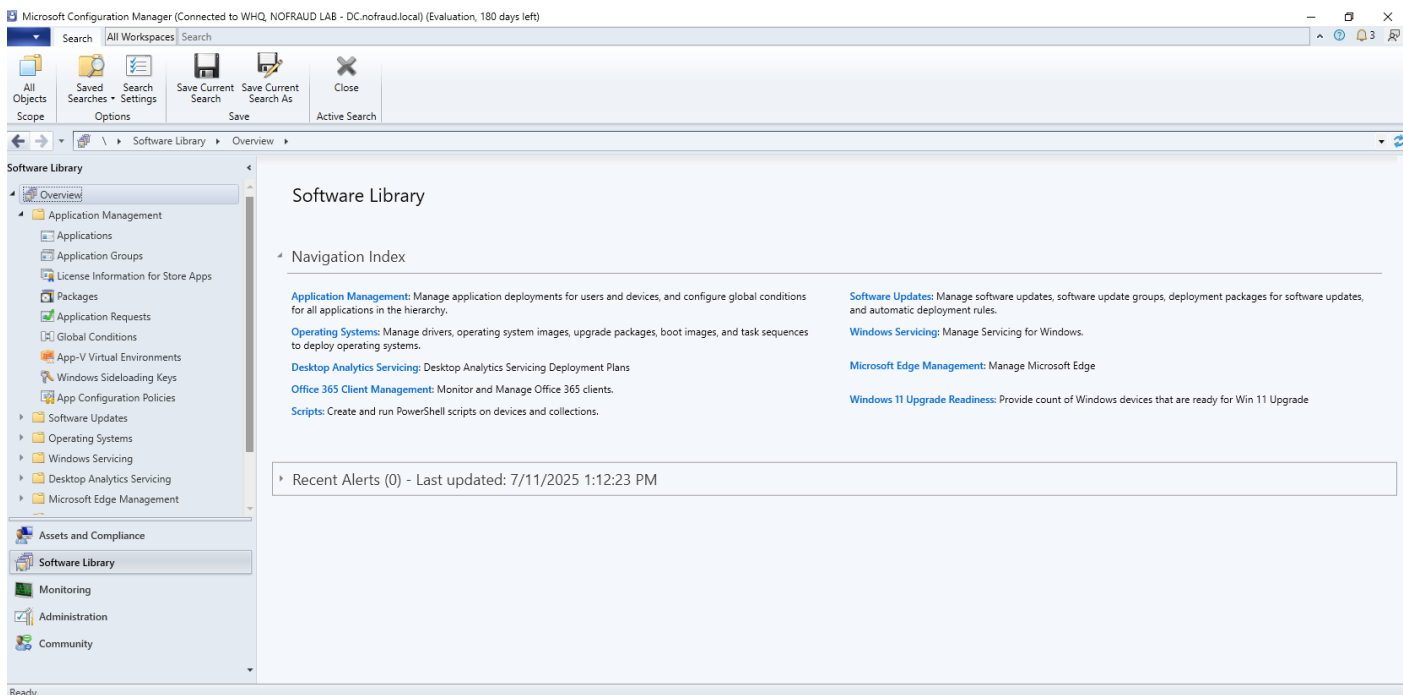
<https://www.youtube.com/embed/jiNtXUC2X2o?si=Z3Bsk-fLaUjC0QuS>

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.

Ingreso a SCCM

En el menú inicio de Windows Server, dar clic en **Configuration Manager Console**. En esta ventana destacan dos entradas en el menú izquierdo inferior: **Software Library** y **Monitoring**. En estas dos opciones radicarán los procedimientos para el despliegue y el monitoreo de las acciones que se ejecuten en la consola.



En este manual se dará por entendido que la organización ya tiene previamente configuradas las colecciones de usuarios y/o dispositivos, por lo que no se entrará en la opción **Assets and Compliance**.

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

Creación de una Aplicación

En la pantalla principal del SCCM, se debe dar clic en **Software Library** y allí dar clic derecho sobre la entrada del menú llamada **Application** y luego en **Create Application**.

Create Application Wizard

General

General

Import Information

Summary

Progress

Completion

Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

☒ Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\Dc\msi\endpointInstaller.msi

Example: \\Server\Share\File

☐ Manually specify the application information

Browse...

< Previous

Next >

Summary

Cancel

En esta ventana se debe seleccionar que el tipo de aplicación a desplegar es **Windows Installer** (msi) y en Location se debe escribir la ruta completa donde se encuentra el instalador. No se debe escribir una ruta local, se debe escribir una ruta de red alcanzable por todas las máquinas de la organización.

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

Información de la Aplicación

Se debe escribir el nombre de la aplicación. Para nuestro caso y para la primera vez que se despliega el software, recomendamos escribir **Business Analytics**.

Create Application Wizard

General Information

General Information

Specify information about this application

Name: Business Analytics

Administrator comments:

Publisher:

Software version:

Optional reference:

Administrative categories:

Select...

Specify the installation program for this application and the required installation rights.

Installation program: msiexec /i "endpointInstaller.msi" /quiet /qn Browse...

☐ Run installation program as 32-bit process on 64-bit clients.

Install behavior: Install for system

< Previous Next > Summary Cancel

En el campo **Intallation program** se debe escribir:

```
msiexec /i "endpointInstaller.msi" /qn /quiet
```

Nótese que se deben escribir las comillas y que la línea termina en /qn /quiet. Estas opciones indicarán al instalador que despliegue el software de manera silenciosa sin interactuar con el

usuario.

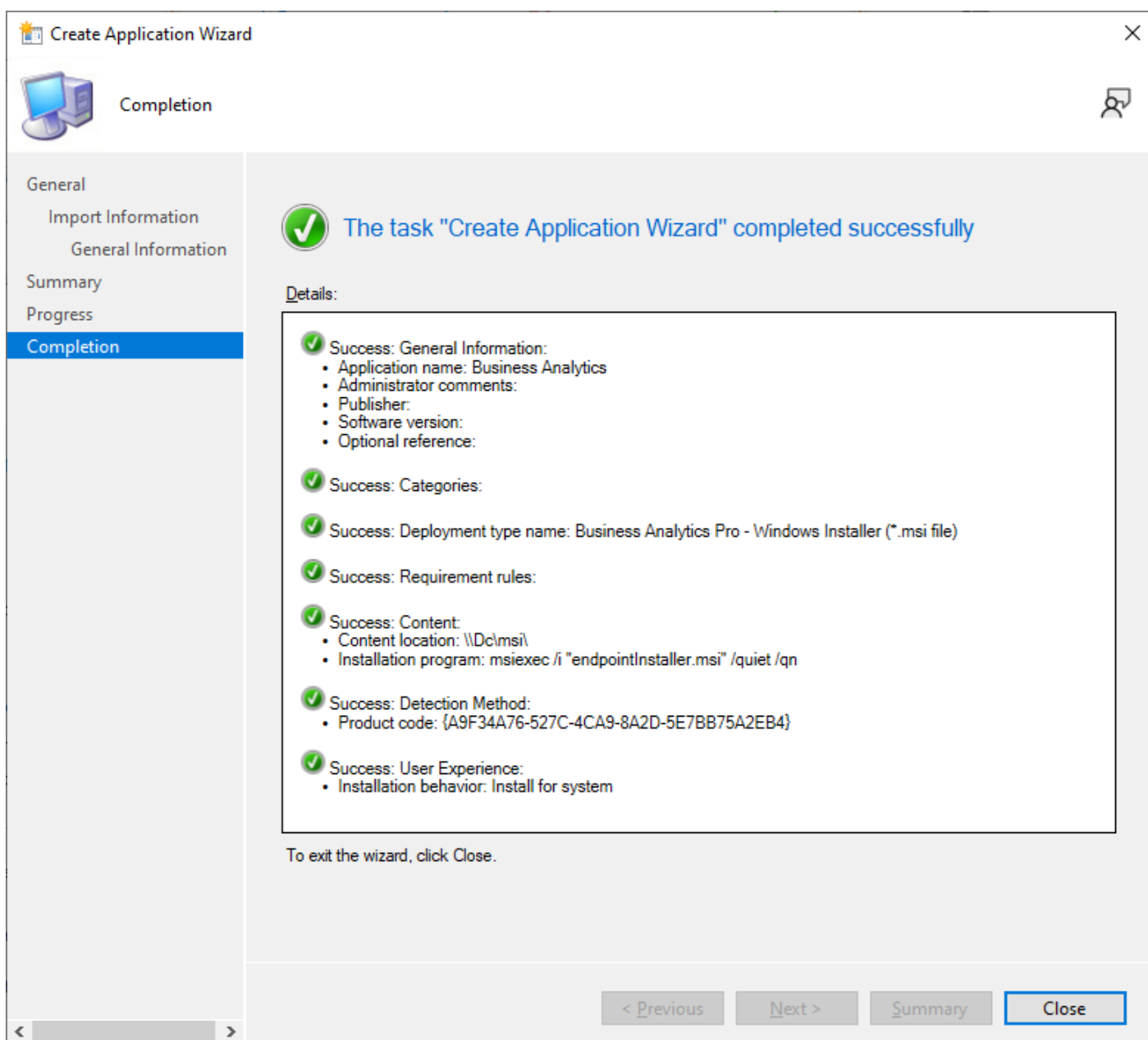
En la opción **Install behavior** se debe seleccionar **Install for System**. Esto hará que el agente se instale con el usuario **system** y que tenga todos los permisos necesarios para que el agente funcione. Aunque el agente de The Fraud Explorer no requiere ejecutarse con permisos administrador, sí se requiere tener este tipo de privilegios para su instalación.

Al agente de The Fraud Explorer corre a nivel de usuario, con permisos del usuario que será monitoreado, es decir, con permisos restringidos al usuario, y no como administrador.

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

Sumario de la creación de la Aplicación

Al finalizar el asistente de creación de la aplicación, se mostrará un resumen, en donde se destaca que SCCM ha detectado automáticamente el **código del producto** y que además será el **método de detección** por defecto para identificar si el software queda o no queda instalado en los PC de los usuarios.

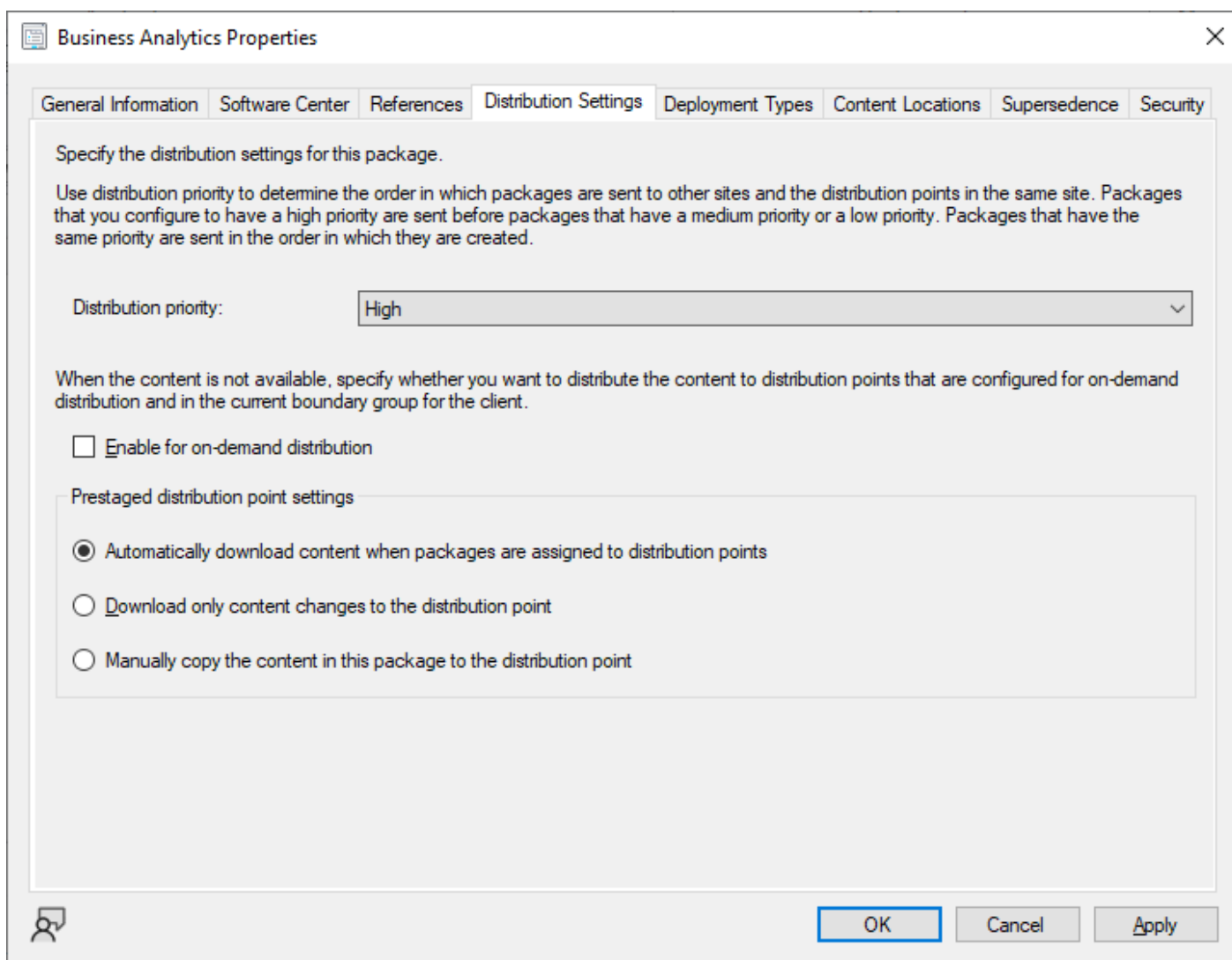


No es necesario indicar otra información por el momento, por ejemplo, la versión, comentarios o fabricante de la aplicación.

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

Configuración de la distribución

Una vez creada la aplicación, se debe dar clic derecho sobre ella y seleccionar **Properties**. Una vez abra la ventana de propiedades, se debe seleccionar la pestaña **Distribution Settings**.



The screenshot shows the 'Business Analytics Properties' dialog box with the 'Distribution Settings' tab selected. The dialog has a title bar with a close button (X) and a tab bar with the following tabs: General Information, Software Center, References, Distribution Settings (active), Deployment Types, Content Locations, Supersedence, and Security. The main content area contains the following text: 'Specify the distribution settings for this package.' followed by a paragraph explaining distribution priority. Below this is a 'Distribution priority:' label and a dropdown menu set to 'High'. Another paragraph explains on-demand distribution settings, followed by an unchecked checkbox labeled 'Enable for on-demand distribution'. A section titled 'Prestaged distribution point settings' contains three radio button options: 'Automatically download content when packages are assigned to distribution points' (selected), 'Download only content changes to the distribution point', and 'Manually copy the content in this package to the distribution point'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons. A help icon is at the bottom left.

Business Analytics Properties

General Information Software Center References **Distribution Settings** Deployment Types Content Locations Supersedence Security

Specify the distribution settings for this package.

Use distribution priority to determine the order in which packages are sent to other sites and the distribution points in the same site. Packages that you configure to have a high priority are sent before packages that have a medium priority or a low priority. Packages that have the same priority are sent in the order in which they are created.

Distribution priority: High

When the content is not available, specify whether you want to distribute the content to distribution points that are configured for on-demand distribution and in the current boundary group for the client.

☐ Enable for on-demand distribution

Prestaged distribution point settings

☒ Automatically download content when packages are assigned to distribution points

☐ Download only content changes to the distribution point

☐ Manually copy the content in this package to the distribution point

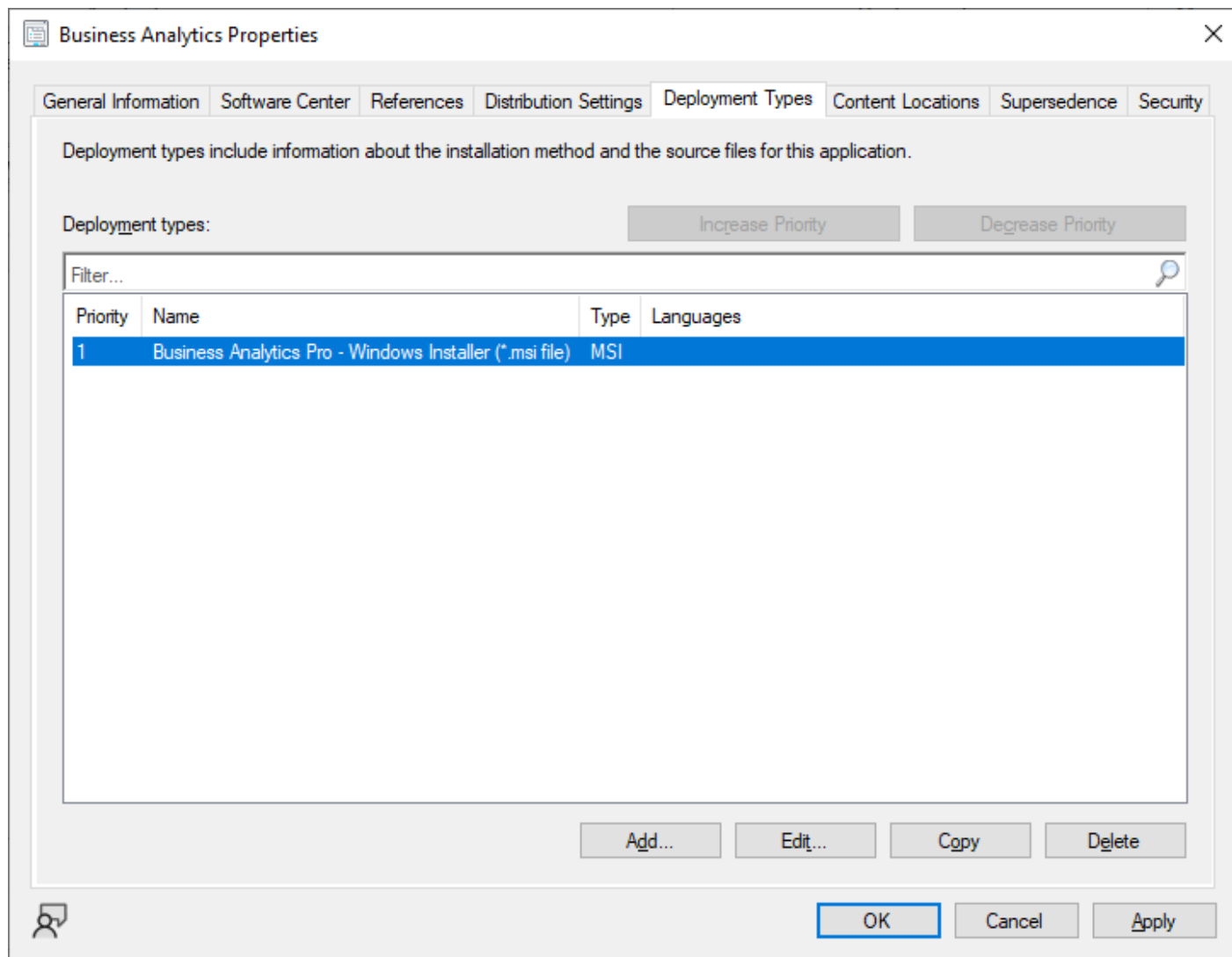
OK Cancel Apply

Se debe seleccionar en **Distribution priority** la opción **High** y en las opciones de **Prestaged distribution point settings** se debe elegir la opción **Automatically download content when packages are assigned to distribution points**.

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

Tipo de distribución

En la misma ventana de propiedades de la aplicación, se debe ir a la pestaña **Deployment Types**, seleccionar la entrada por defecto y luego dar clic en **Edit**.

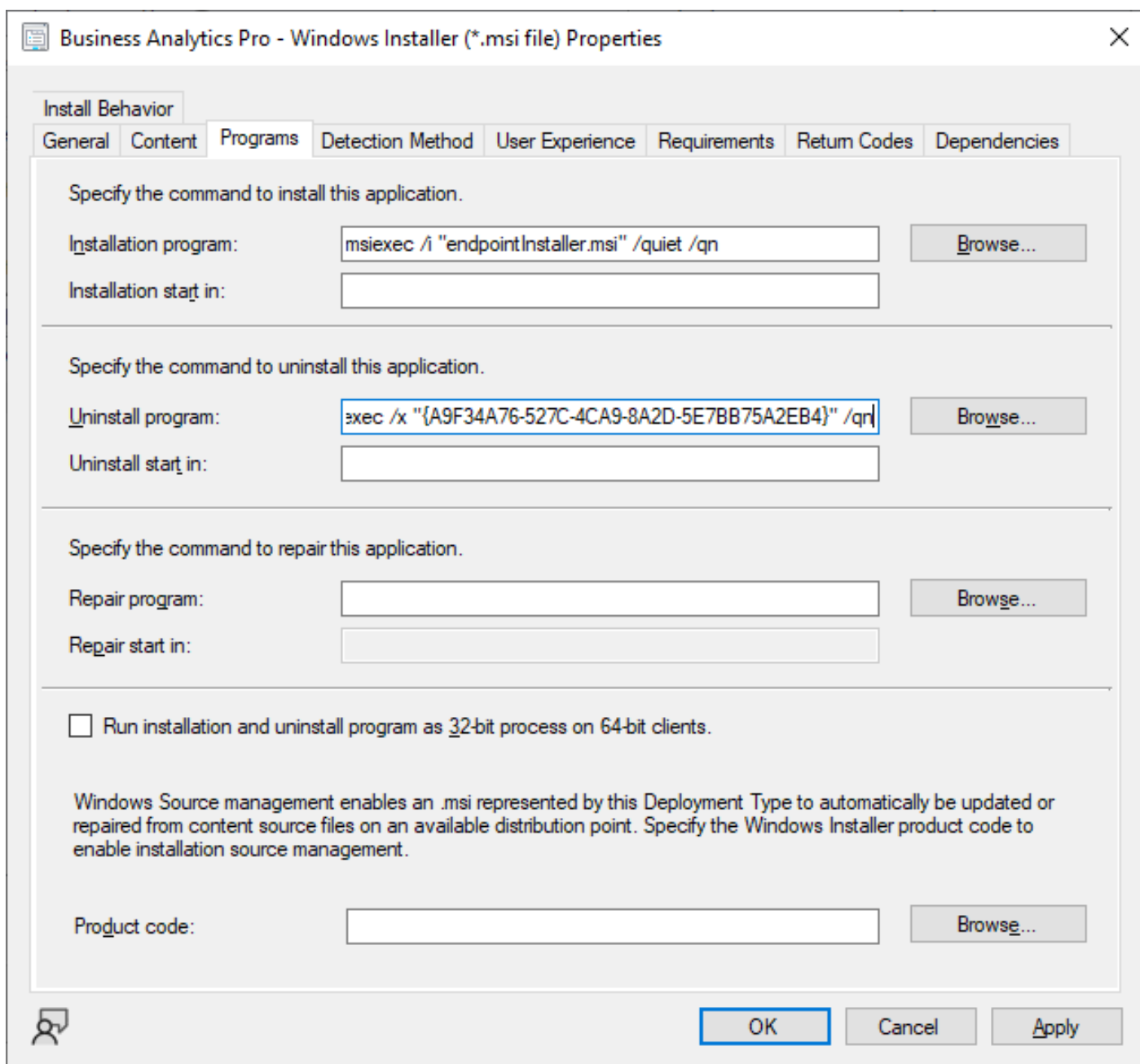


Esto abrirá una nueva ventana en la que se configurarán varias opciones que determinarán el tipo de despliegue que se realizará para el agente.

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

Comandos para instalar y desinstalar

A esta pestaña se llega desde la ventana de propiedades de la aplicación, luego entrando a la pestaña **Deployment Types** y dando clic en **Edit**. Aquí se van a configurar los comandos de instalación y desinstalación del agente MSI.



Business Analytics Pro - Windows Installer (*.msi file) Properties

Install Behavior

General Content **Programs** Detection Method User Experience Requirements Return Codes Dependencies

Specify the command to install this application.

Installation program: Browse...

Installation start in:

Specify the command to uninstall this application.

Uninstall program: Browse...

Uninstall start in:

Specify the command to repair this application.

Repair program: Browse...

Repair start in:

☐ Run installation and uninstall program as 32-bit process on 64-bit clients.

Windows Source management enables an .msi represented by this Deployment Type to automatically be updated or repaired from content source files on an available distribution point. Specify the Windows Installer product code to enable installation source management.

Product code: Browse...

OK Cancel Apply

En el campo **Installation program** se debe asegurar que está escrito:

```
msiexec /i "endpointInstaller.msi" /quiet /qn
```

Y en el campo Uninstall program se debe asegurar que está escrito:

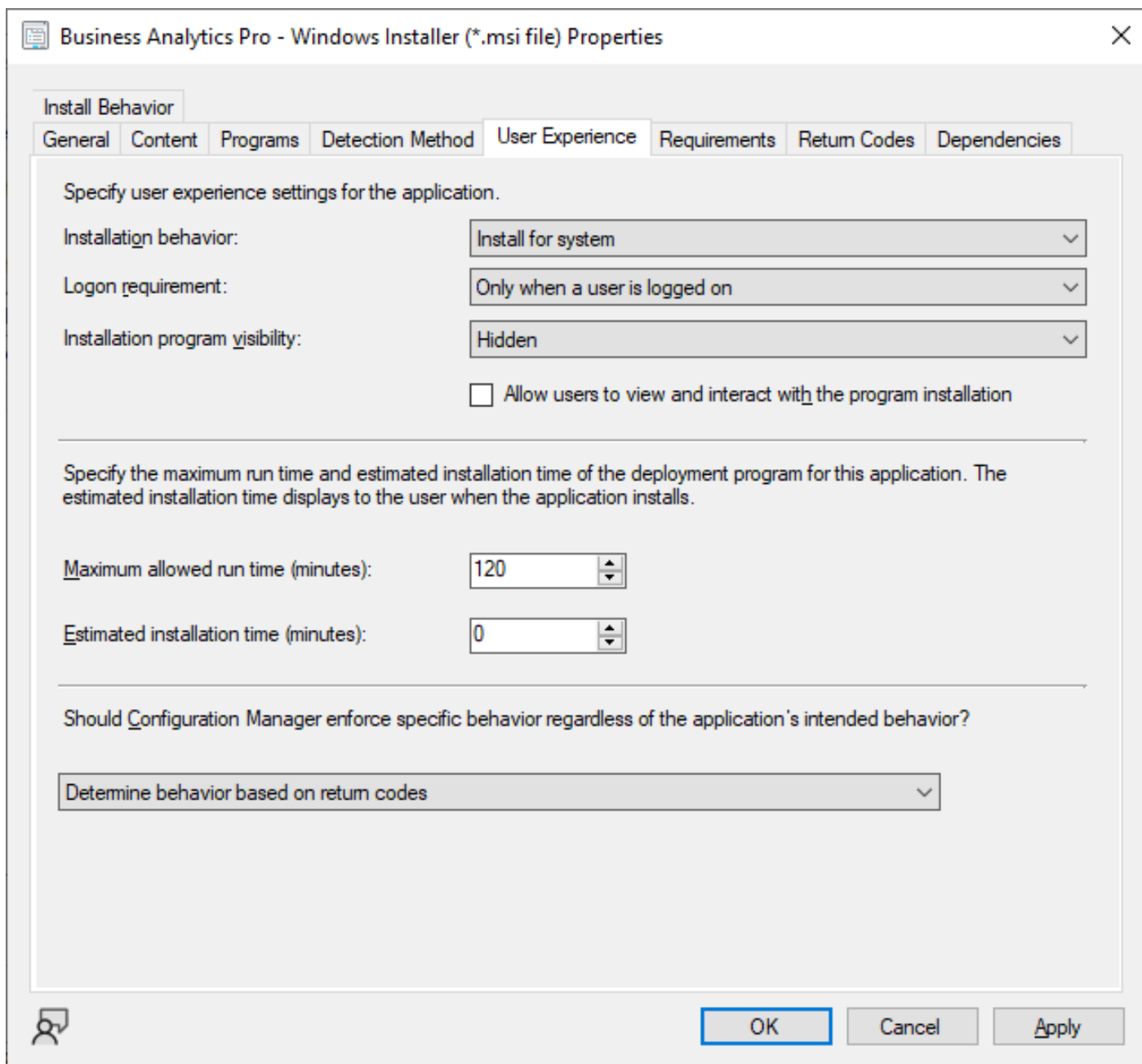
```
msiexec /x "{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}" /qn
```

Nótese las comillas en ambos comandos. Por defecto en el comando de desinstalación no están presentes las comillas ni el /qn.

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

Experiencia de usuario

A esta pestaña se llega desde la ventana de propiedades de la aplicación, luego entrando a la pestaña **Deployment Types** y dando clic en **Edit**. Aquí se va a configurar la experiencia que tendrá el usuario final.



Business Analytics Pro - Windows Installer (*.msi file) Properties

Install Behavior

General Content Programs Detection Method **User Experience** Requirements Return Codes Dependencies

Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Only when a user is logged on

Installation program visibility: Hidden

☐ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 120

Estimated installation time (minutes): 0

Should Configuration Manager enforce specific behavior regardless of the application's intended behavior?

Determine behavior based on return codes

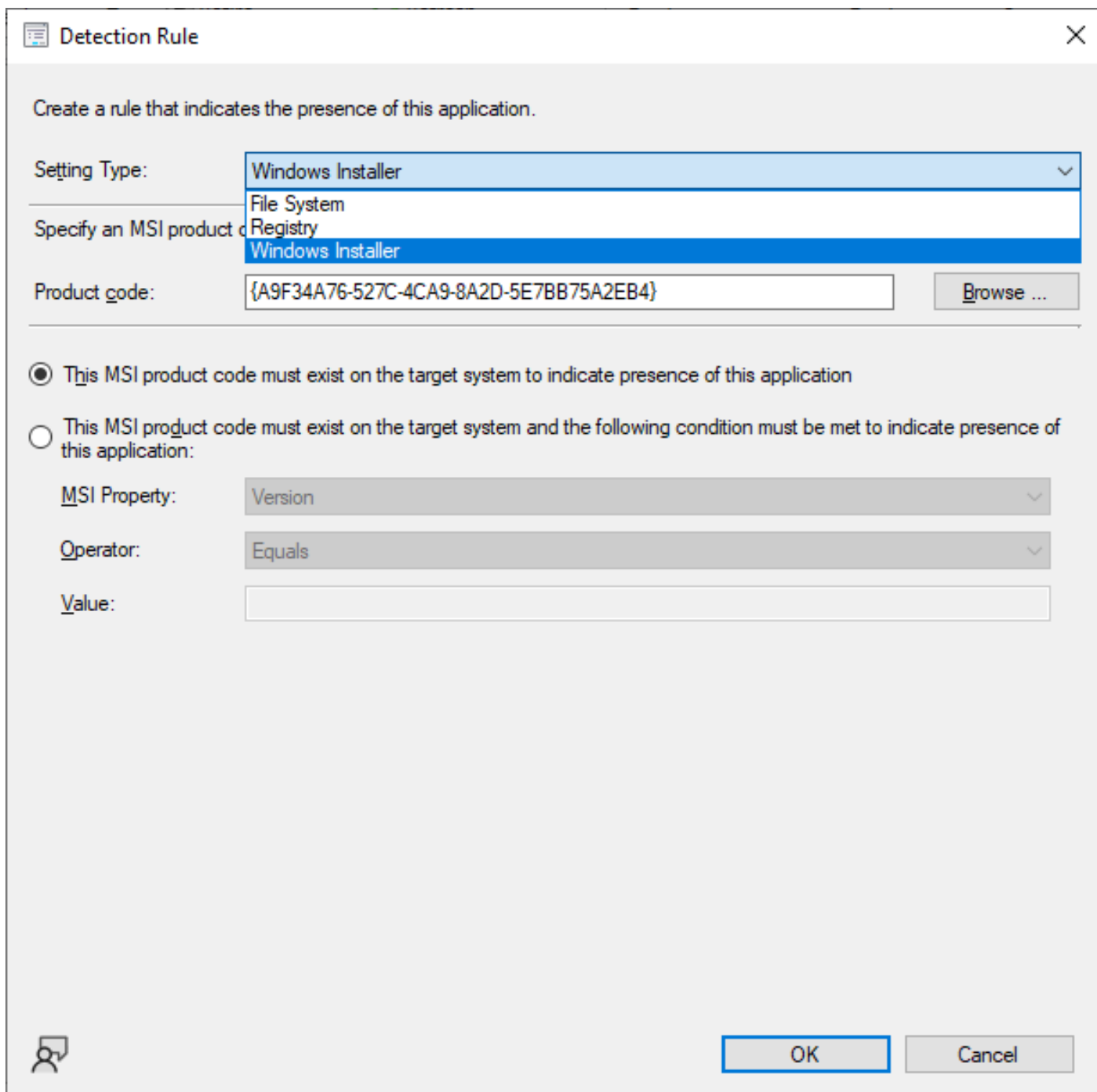
OK Cancel Apply

En **Install behavior** se debe asegurar que está seleccionado **Install for system**. En **Logon requirement** debe estar especificada la opción **Only when a user is logged on** y en **Installation program visibility** se debe seleccionar **Hidden**.

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

Método de detección

A esta pestaña se llega desde la ventana de propiedades de la aplicación, luego entrando a la pestaña **Deployment Types** y dando clic en **Edit**. Aquí se va a configurar el método de detección del MSI de The Fraud Explorer en los computadores de la organización.



The screenshot shows the 'Detection Rule' dialog box in System Center Configuration Manager. The dialog has a title bar with a close button (X) and a subtitle 'Create a rule that indicates the presence of this application.' Below this, there are three main sections. The first section, 'Setting Type:', has a dropdown menu with 'Windows Installer' selected. Below this, 'Specify an MSI product code:' has a text box containing '{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}' and a 'Browse ...' button. The second section has two radio buttons. The first is selected and labeled 'This MSI product code must exist on the target system to indicate presence of this application'. The second is labeled 'This MSI product code must exist on the target system and the following condition must be met to indicate presence of this application:'. Below the second radio button, there are three fields: 'MSI Property:' with a dropdown showing 'Version', 'Operator:' with a dropdown showing 'Equals', and 'Value:' with an empty text box. At the bottom right, there are 'OK' and 'Cancel' buttons. At the bottom left, there is a small icon of a person with a speech bubble.

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: Windows Installer

Specify an MSI product code: {A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Browse ...

☒ This MSI product code must exist on the target system to indicate presence of this application

☐ This MSI product code must exist on the target system and the following condition must be met to indicate presence of this application:

MSI Property: Version

Operator: Equals

Value:

OK Cancel

Por defecto, SCCM detecta que el agente de The Fraud Explorer está instalado si en el computador existe un paquete con el código de producto que previamente se ha inventariado de manera automática. Esta opción se debe dejar así, sin modificar.

Sin embargo, podrían existir problemas en algunos computadores donde por determinadas circunstancias ya no es posible localizar el software a través del código de producto. Se recomienda que en estos casos se use el método **File System** y se use la ruta **C:\ProgramData\Software\businessAnalytics.exe** para que SCCM sepa que el agente de The Fraud Explorer está instalado y pueda ejecutar acciones futuras sobre él, como actualizaciones o desinstalaciones.

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

Despliegue de la Aplicación

A esta ventana se llega dando clic derecho sobre la aplicación recientemente creada y luego en la opción **Deploy**.

Deploy Software Wizard

General

Specify general information for this deployment

Software: Business Analytics Browse...

Collection: Browse...

☐ Use default distribution point groups associated to this collection

☒ Automatically distribute content for dependencies

Comments (optional):

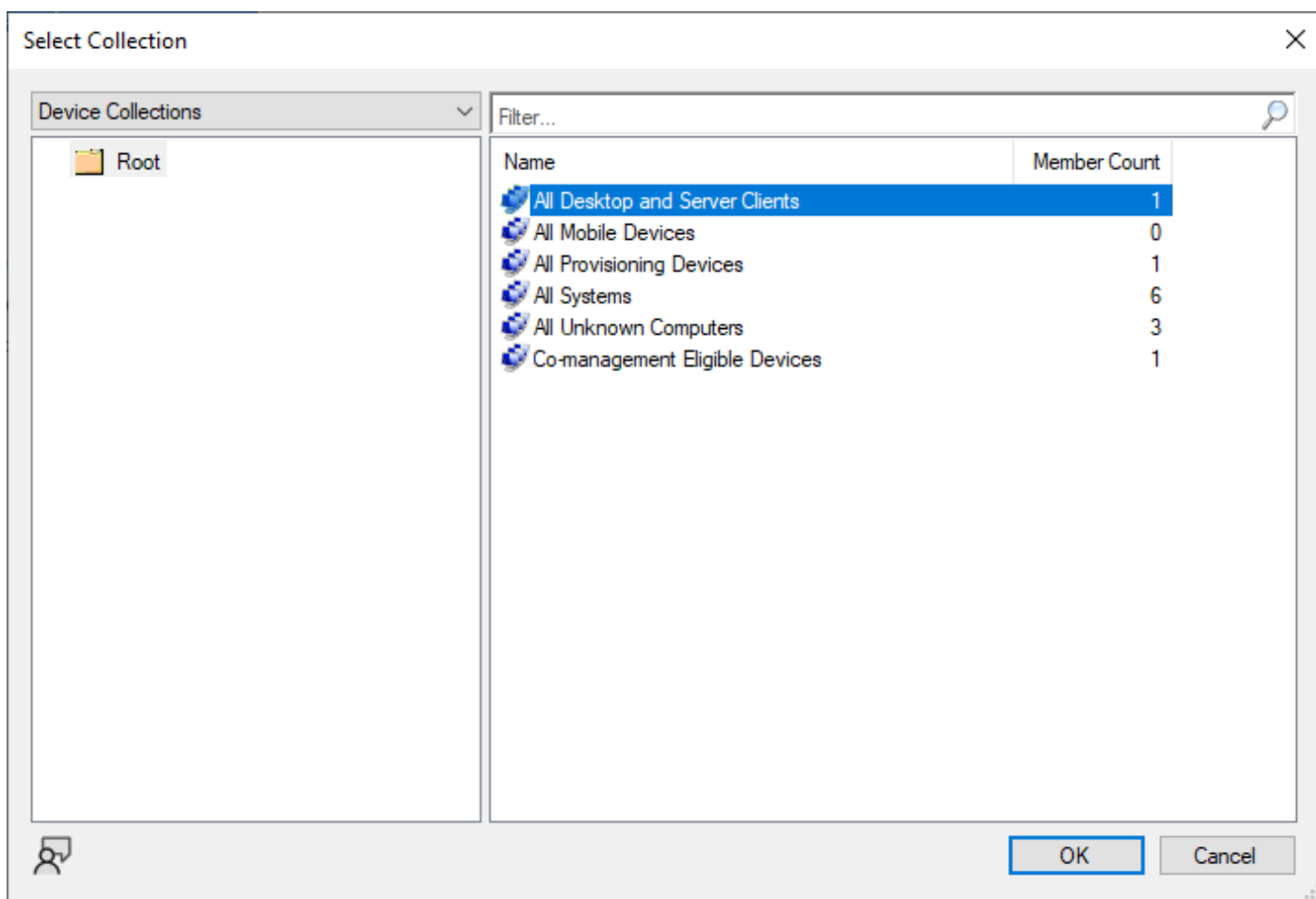
< Previous Next > Summary Cancel

En esta opción (Deploy) se configurarán las opciones de despliegue de la aplicación y se seleccionarán a cuales usuarios o dispositivos se les instalará el agente de The Fraud Explorer.

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

Selección de usuarios o dispositivos

Una vez estando en la opción **Deploy**, se procede a dar clic en **Browse** y se llega a esta ventana donde se debe seleccionar a qué dispositivos o usuarios se les instalará el agente de The Fraud Explorer.



Previo a esta ventana, como requisito previo, deberá haber organizado sus dispositivos y usuarios de tal forma que se permita seleccionar fácilmente el grupo de usuarios que se desea monitorear.

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

Punto de distribución

Siguiendo con la opción de **Deploy**, se deberá seleccionar el **punto de distribución** donde será distribuido el contenido.

Deploy Software Wizard

Content

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

Name	Type
There are no items to show in this view.	

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Filter...

Name	Description	Associations
DC.NOFRAUD.LOCAL	Distribution point	

Add Remove

< Previous Next > Summary Cancel

En una instalación normal, solo se tendrá un único punto o distribución. Para seleccionarlo debe dar clic en **Add** y luego marcar la casilla del **Distribution Point**.

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

Acción de despliegue

Procediendo con la configuración del **Deploy**, se selecciona la acción que ejecutará este despliegue. En este caso se selecciona la acción **Install** y el propósito **Required**.

Deploy Software Wizard

Deployment Settings

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify settings to control this deployment

Action: Install

Purpose: Required

☐ Allow end users to attempt to repair this application

☒ When a resource is no longer a member of the collection, uninstall this application

☐ Pre-deploy software to the user's primary device

☐ Send wake-up packets

☐ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

< Previous **Next >** Summary Cancel

Se marca la casilla **When a resource is no longer a member of the collection, uninstall this application**. Esta opción permite que cuando un usuario o un dispositivo no pertenezca a la colección seleccionada en los pasos anteriores, se envíe la acción de desinstalación del agente de The Fraud Explorer.

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

Agendamiento del despliegue

En esta ventana se puede configurar un horario y fecha específica para el despliegue de la acción de Instalación.

Deploy Software Wizard

Scheduling

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify the schedule for this deployment

This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.

Time based on: UTC

☐ Schedule the application to be available at:
7/11/2025 8:40 PM

Installation deadline:
☒ As soon as possible after the available time
☐ Schedule at:
7/11/2025 8:40 PM

☐ Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.

< Previous Next > Summary Cancel

Para el caso del agente de The Fraud Explorer, se recomienda que no se realice agendamiento o programación, sino que se realice de manera inmediata.

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

Experiencia del usuario

La experiencia del usuario en la pantalla **Deploy** se refiere a aquellos comportamientos que se le mostrarán y se le permitirán al usuario realizar con nuestro instalador. Para una instalación silenciosa y desatendida, se recomienda elegir la opción **Hide in Software Center and all notifications**.

Deploy Software Wizard

User Experience

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify the user experience for the installation of this software:

Specify user experience setting for this deployment

User notifications:
Hide in Software Center and all notifications

☐ When software changes are required, show a dialog window to the user instead of a toast notification

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

☐ Software Installation
☐ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

☒ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

< Previous **Next >** Summary Cancel

Con esta configuración, el agente de SCCM en el dispositivo del usuario no mostrará ningún mensaje de instalación o desinstalación del agente de The Fraud Explorer.

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

Alertas de despliegue

En esta pantalla se pueden configurar alertas que informen sobre problemas o inconvenientes en la ejecución de la acción de despliegue.

Deploy Software Wizard

Alerts

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify Configuration Manager and Operations Manager alert options

Configuration Manager generates alerts when this application is deployed.

Threshold for successful deployment

☐ Create a deployment alert when the threshold is lower than the following:

Percent success: 1

After: 7/18/2025 1:40 PM

Threshold for failed deployment

☐ Create a deployment alert when the threshold is higher than the following:

Percent failure: 0

Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.

☐ Enable System Center Operations Manager maintenance mode

☐ Generate System Center Operations Manager alert when a software installation fails

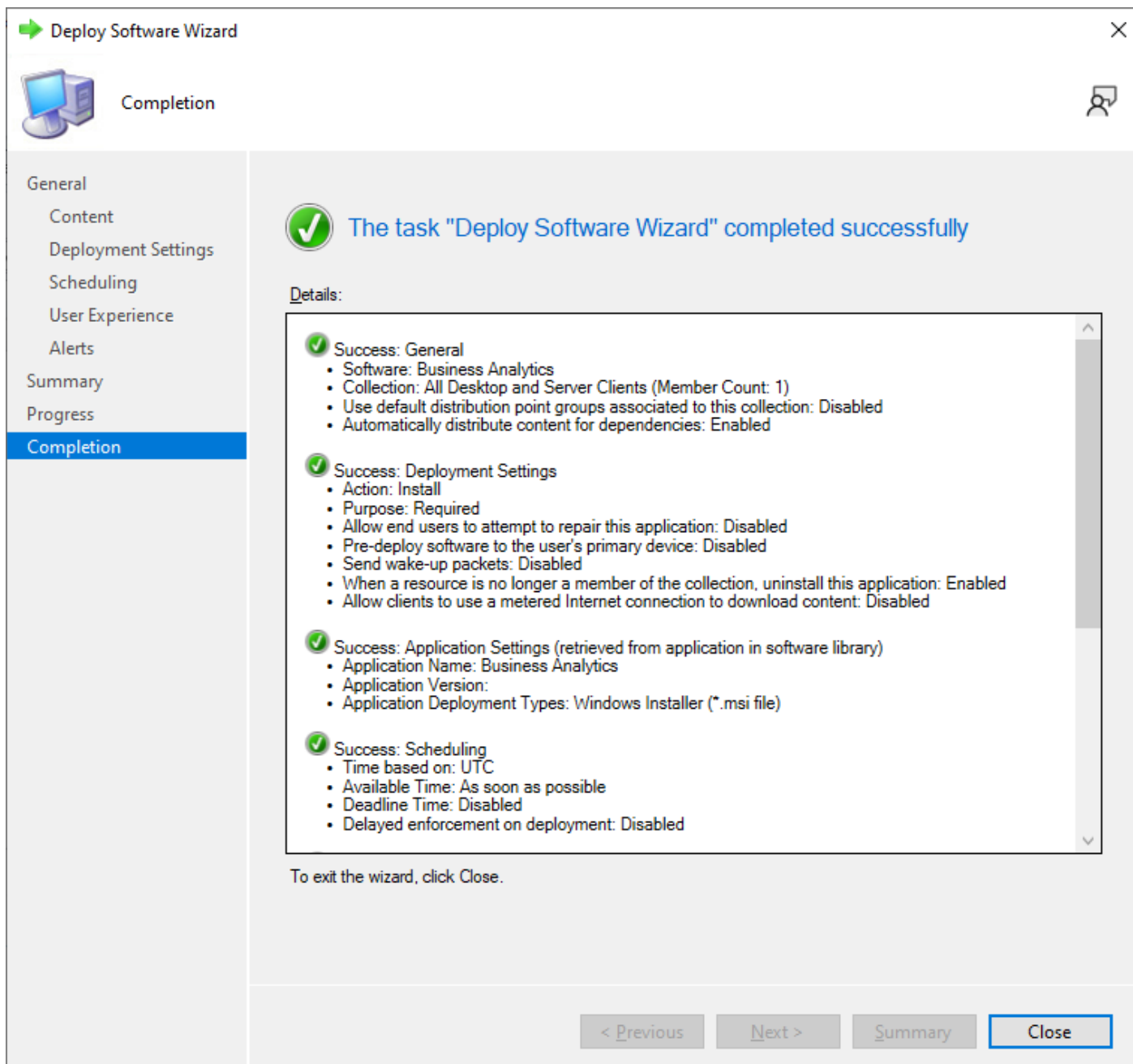
< Previous Next > Summary Cancel

Se recomienda no configurar alertas para el despliegue de la solución The Fraud Explorer y dejar las opciones por defecto de la ventana que no envían alertas.

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

Resumen del despliegue

Al finalizar se obtiene este resumen de las operaciones que fueron ejecutadas de forma exitosa.



The screenshot shows the 'Deploy Software Wizard' window in System Center Configuration Manager. The window title is 'Deploy Software Wizard' with a green arrow icon. The 'Completion' tab is selected in the left-hand navigation pane, which also includes 'General', 'Content', 'Deployment Settings', 'Scheduling', 'User Experience', 'Alerts', 'Summary', and 'Progress'. The main area displays a large green checkmark icon and the text 'The task "Deploy Software Wizard" completed successfully'. Below this, a 'Details:' section contains a scrollable list of success messages:

- ✓ Success: General
 - Software: Business Analytics
 - Collection: All Desktop and Server Clients (Member Count: 1)
 - Use default distribution point groups associated to this collection: Disabled
 - Automatically distribute content for dependencies: Enabled
- ✓ Success: Deployment Settings
 - Action: Install
 - Purpose: Required
 - Allow end users to attempt to repair this application: Disabled
 - Pre-deploy software to the user's primary device: Disabled
 - Send wake-up packets: Disabled
 - When a resource is no longer a member of the collection, uninstall this application: Enabled
 - Allow clients to use a metered Internet connection to download content: Disabled
- ✓ Success: Application Settings (retrieved from application in software library)
 - Application Name: Business Analytics
 - Application Version:
 - Application Deployment Types: Windows Installer (*.msi file)
- ✓ Success: Scheduling
 - Time based on: UTC
 - Available Time: As soon as possible
 - Deadline Time: Disabled
 - Delayed enforcement on deployment: Disabled

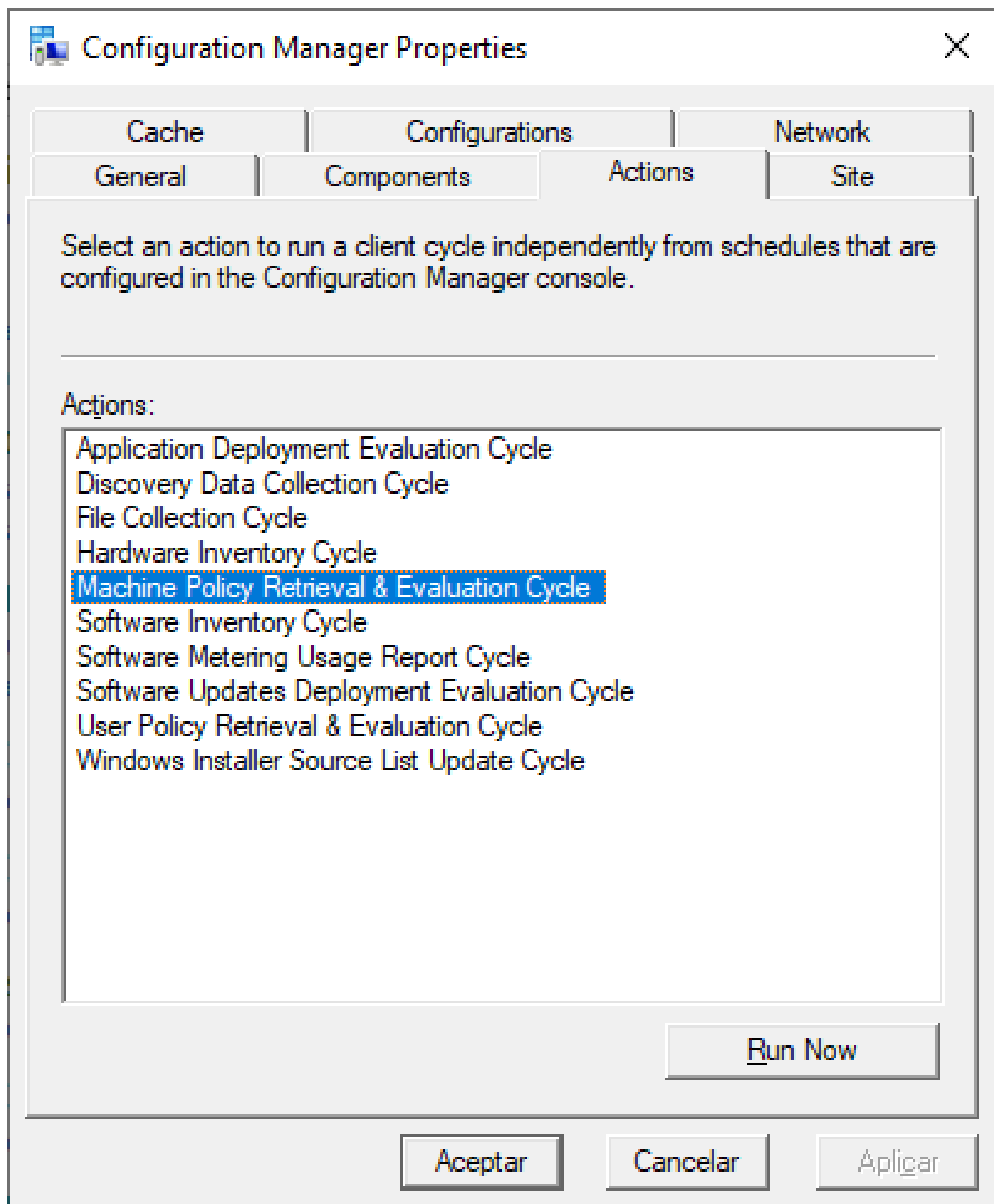
Below the details, it says 'To exit the wizard, click Close.' At the bottom right, there are four buttons: '< Previous' (disabled), 'Next >' (disabled), 'Summary' (disabled), and 'Close' (active).

Aquí se debe verificar que la acción a ejecutar sea **Install**, que el propósito sea **Required** y que no se le muestre ningún tipo de mensaje o alerta al usuario en su dispositivo.

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

Forzar política en PC

No hay necesidad de forzar la política de despliegue que se acabó de crear en el SCCM, sin embargo, si queremos que se ejecute de inmediato, es decir, que se instale nuestro agente, podemos forzar su ejecución.

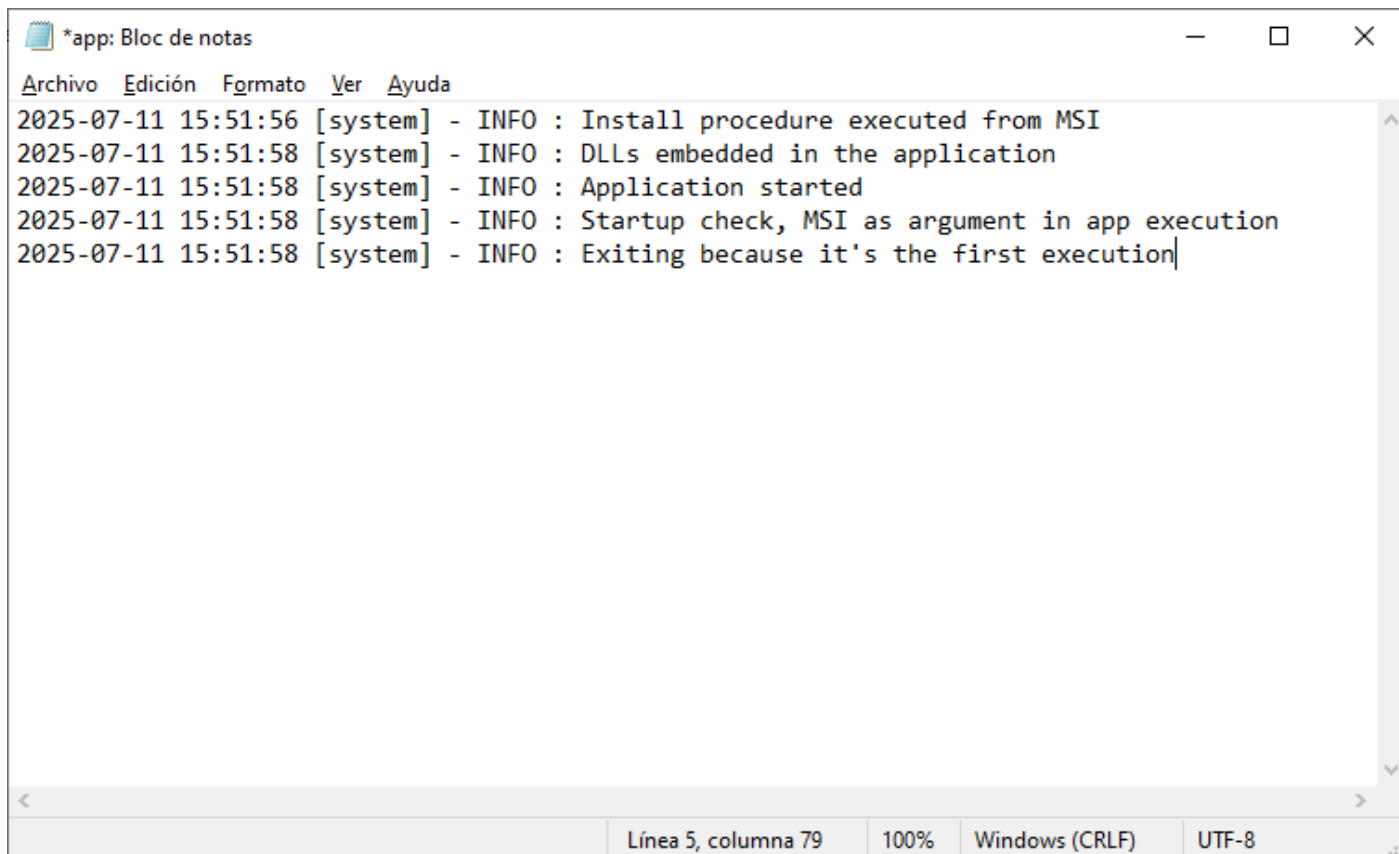


Se debe entrar al **Panel de Control** de Windows, dar clic en **Sistema y Seguridad** y luego en **Configuration Manager**. En la ventana que se abre, se ingresa a la pestaña **Actions** y allí se da clic en **Machine Policy Retrieval & Evaluation Cycle** y luego clic en **Run Now**.

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

Verificación de la instalación

Para verificar la instalación se puede esperar a que en el SCCM, en el centro de Monitoreo, se muestre el nivel de cumplimiento. 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**.



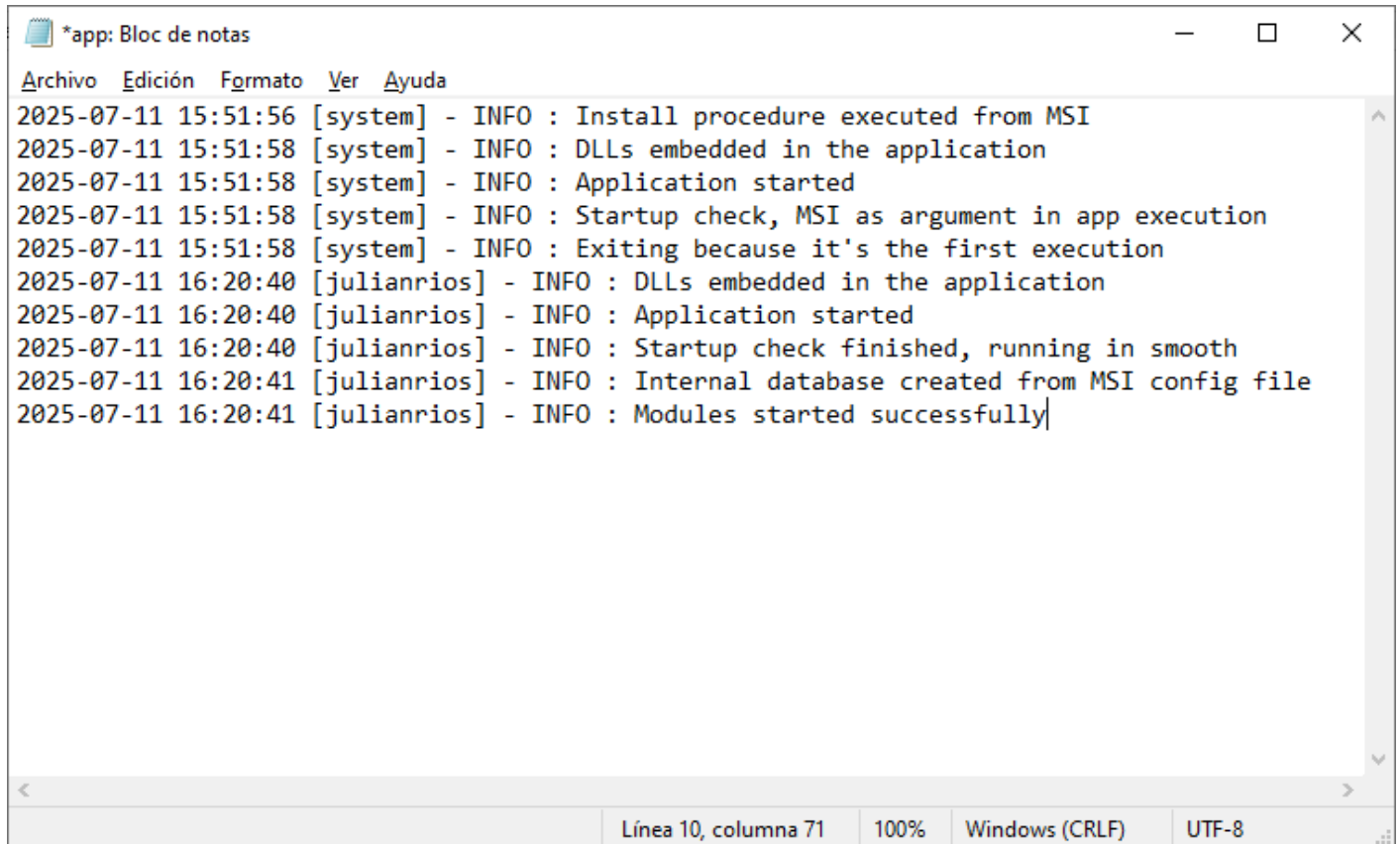
```
*app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup check, MSI as argument in app execution
2025-07-11 15:51:58 [system] - INFO : Exiting because it's the first execution
```

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.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones. Este software está siendo desarrollado por [NOFRAUD.la](#). Este contenido es privado y únicamente está disponible para clientes de NOFRAUD. Está prohibida su publicación en fuentes abiertas o disponibles al público.

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 abrir el archivo C:\ProgramData\Software\app.log donde se verá información sobre su primera ejecución.



```
*app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup check, MSI as argument in app execution
2025-07-11 15:51:58 [system] - INFO : Exiting because it's the first execution
2025-07-11 16:20:40 [julianrios] - INFO : DLLs embedded in the application
2025-07-11 16:20:40 [julianrios] - INFO : Application started
2025-07-11 16:20:40 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-11 16:20:41 [julianrios] - INFO : Internal database created from MSI config file
2025-07-11 16:20:41 [julianrios] - INFO : Modules started successfully
```

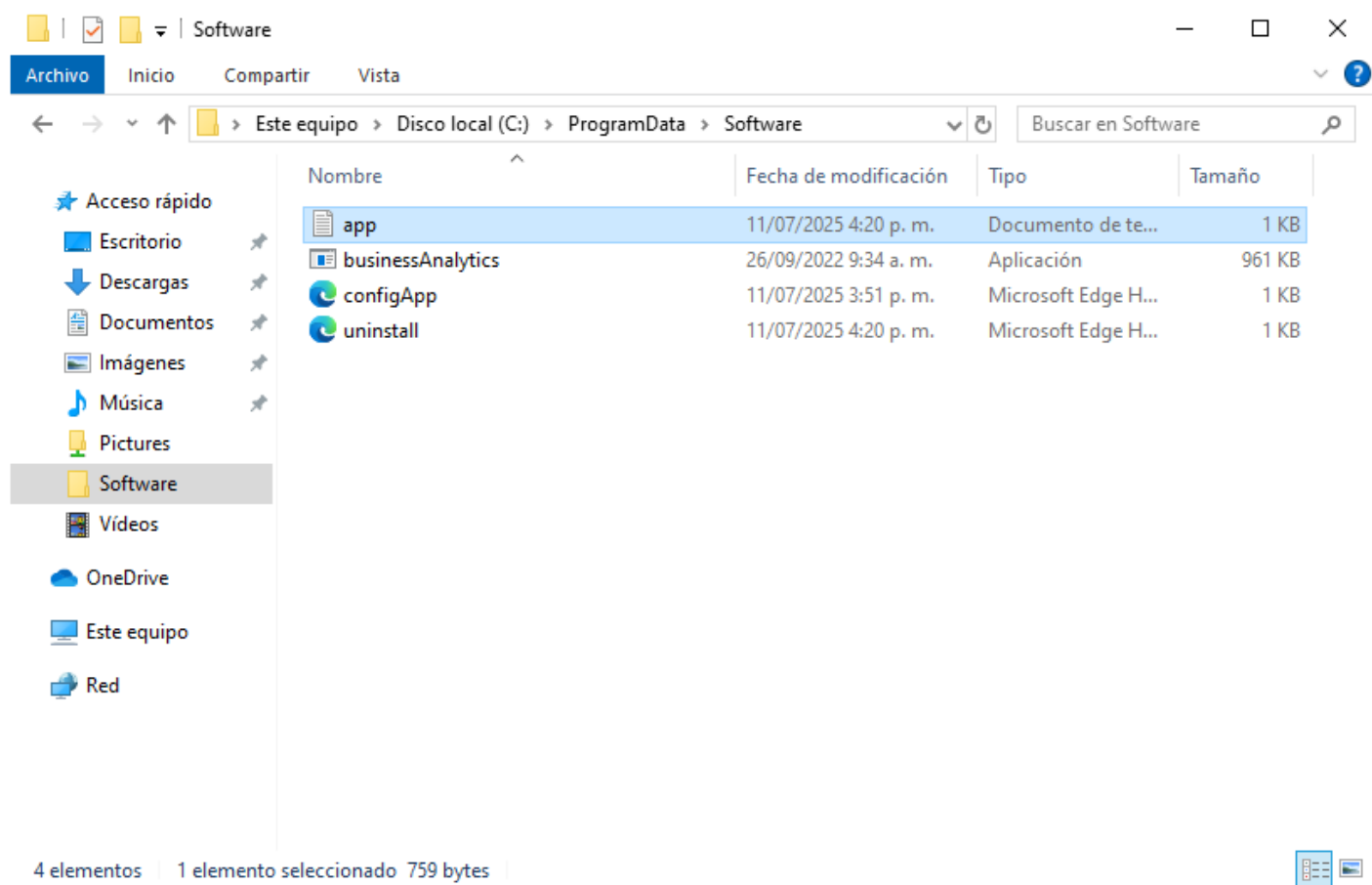
Como se observa, ya la ejecución se hace con un usuario normal sin privilegios elevados y de esa manera el agente de The Fraud Explorer lo detecta y procede a arrancar diciendo **Modules started successfully**.

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

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

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**.

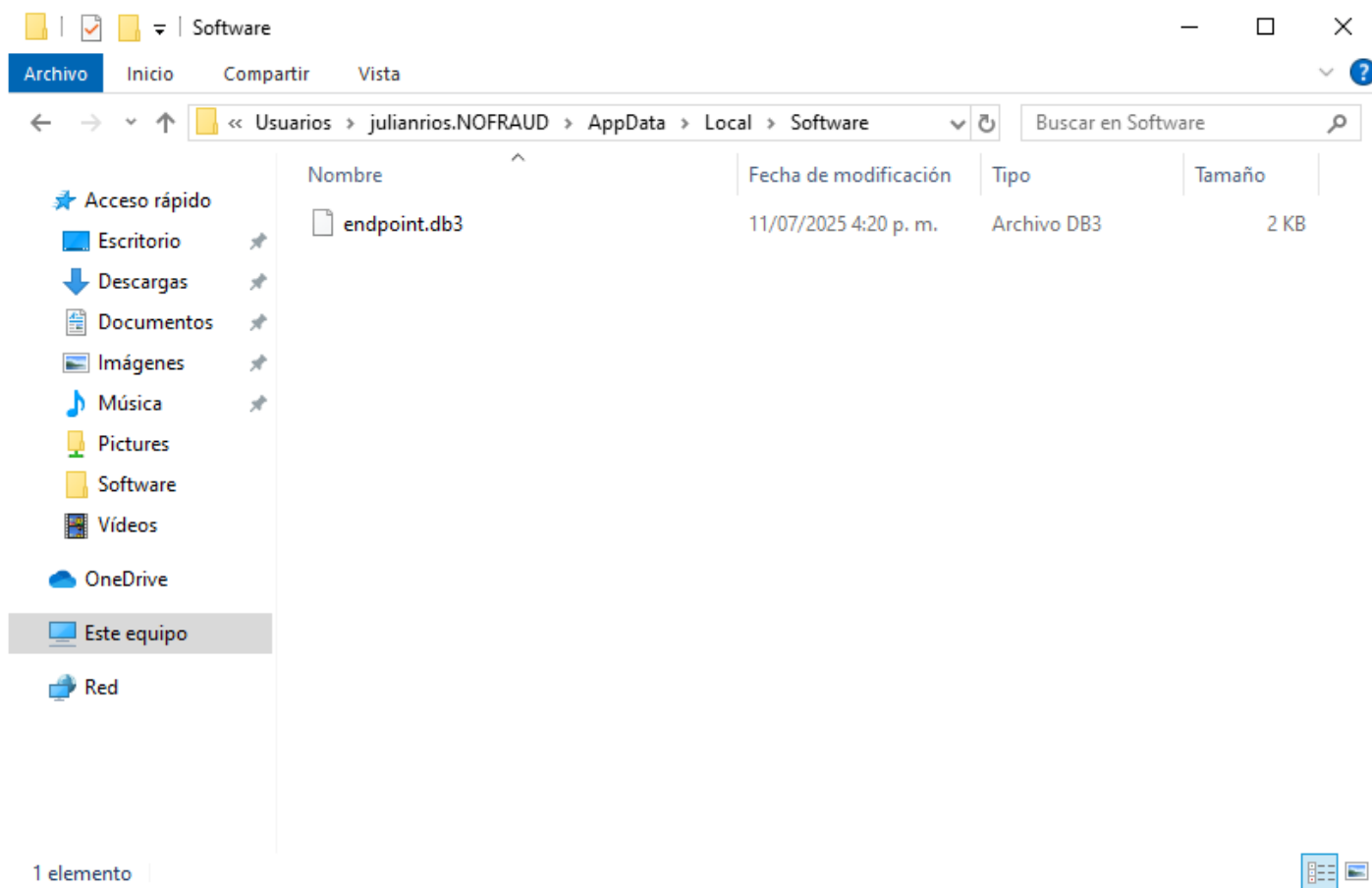


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

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.

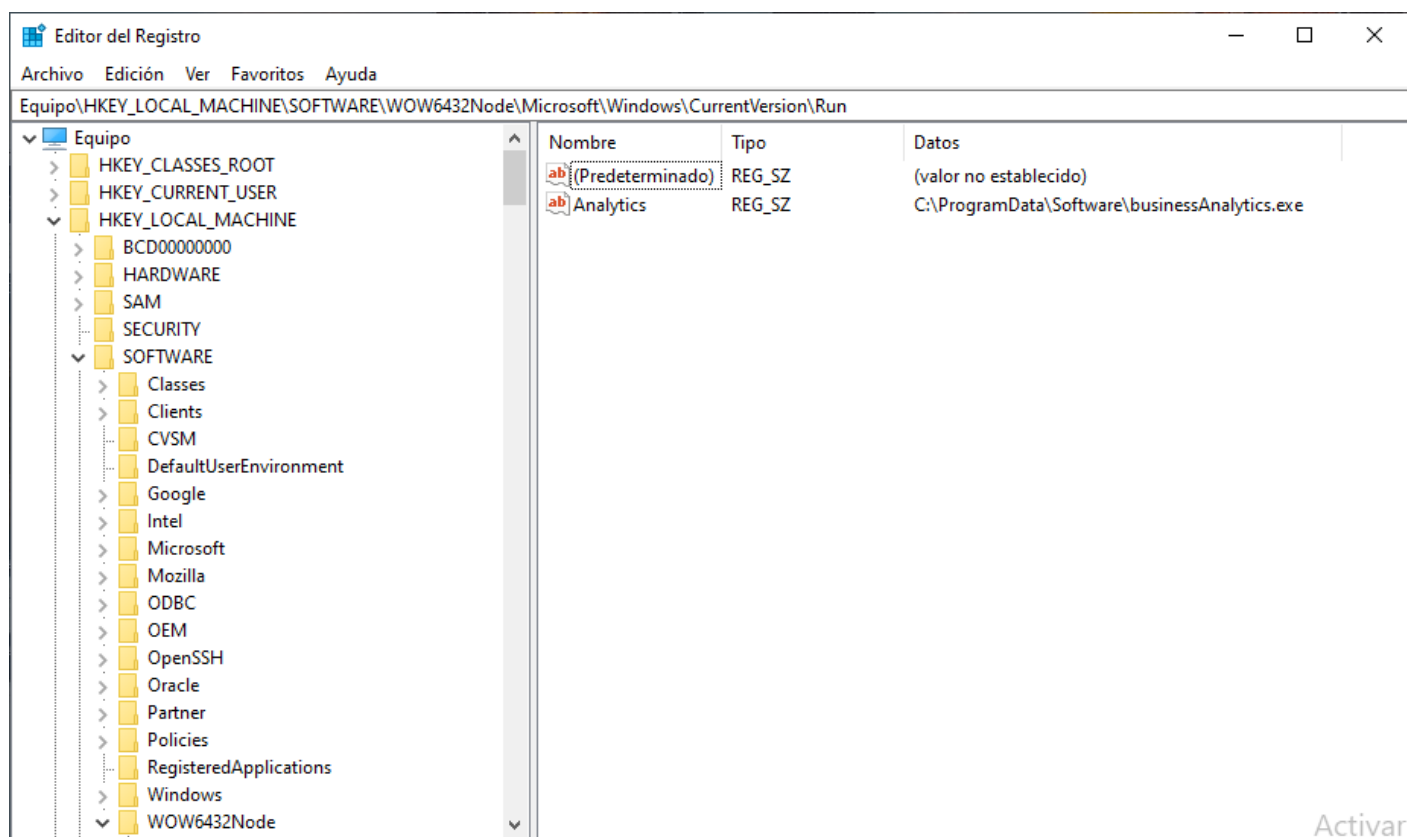


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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.**

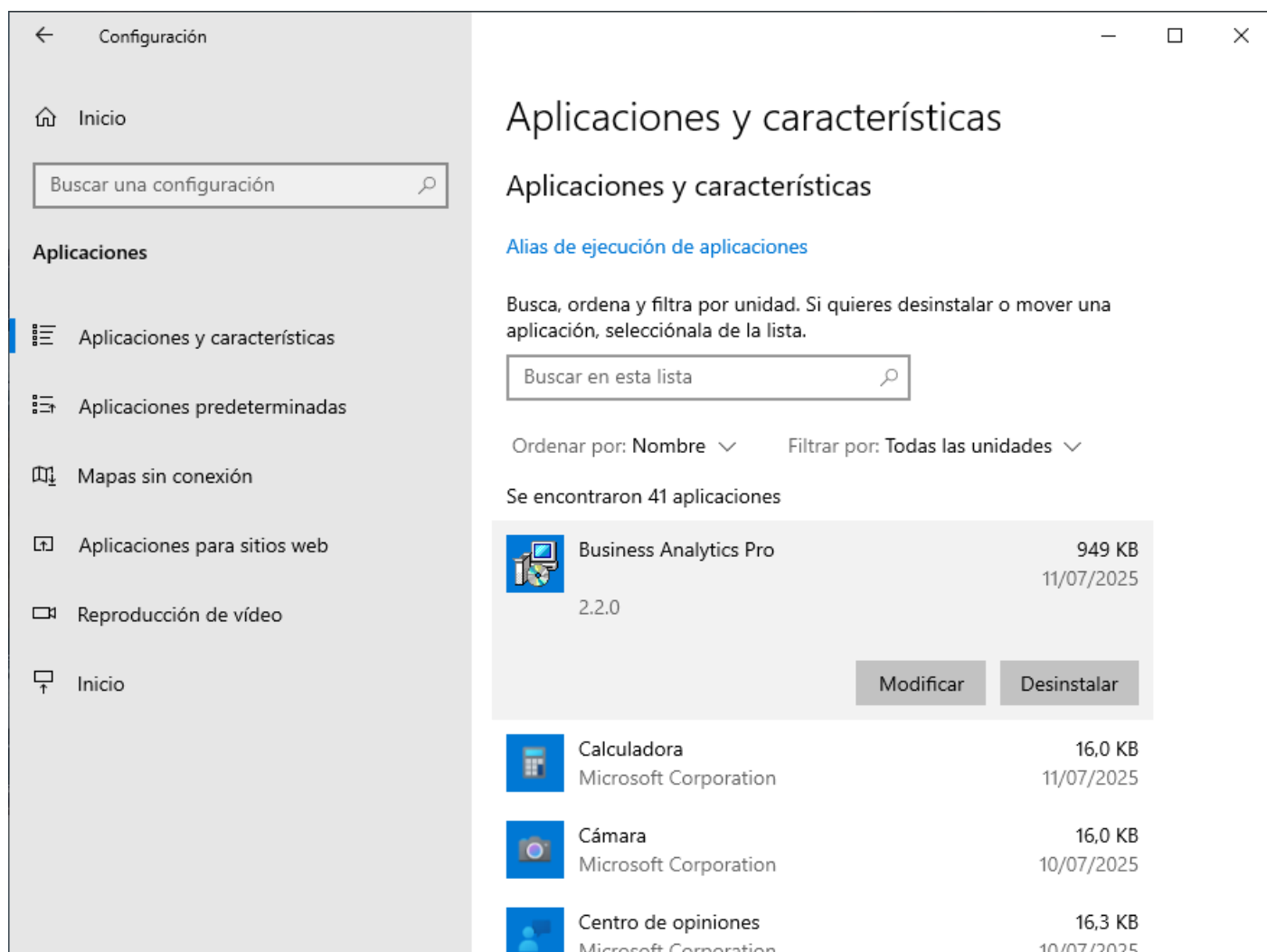


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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**.



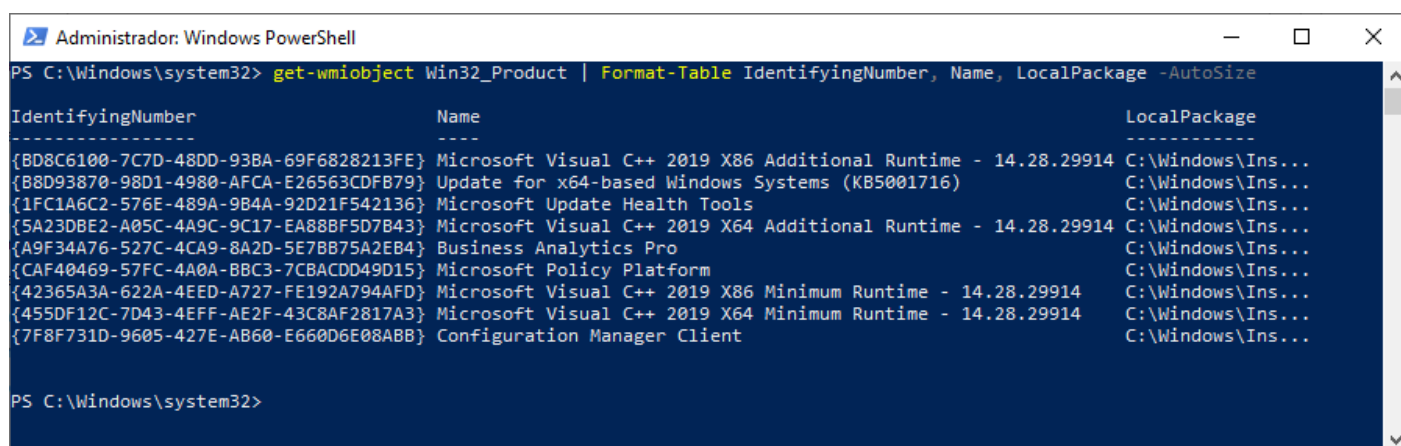
Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se reemplaza la actual con la nueva versión.

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
```



```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

```
PS C:\Windows\system32>
```

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**.

Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00	11.392 K	
conhost.exe	3768	En ejecución	Administr...	00	4.844 K	No permitida
csrss.exe	552	En ejecución		00	560 K	
csrss.exe	648	En ejecución		00	716 K	
ctfmon.exe	5708	En ejecución	julianrios	00	2.480 K	Deshabilitada
dllhost.exe	4288	En ejecución		00	776 K	
dllhost.exe	7164	En ejecución	julianrios	00	1.908 K	Deshabilitada
dwm.exe	1668	En ejecución		00	43.148 K	
explorer.exe	5572	En ejecución	julianrios	00	75.828 K	Deshabilitada
explorer.exe	5960	En ejecución	julianrios	00	6.132 K	Deshabilitada
FileCoAuth.exe	1792	En ejecución	julianrios	00	28 K	Deshabilitada
fontdrvhost.exe	940	En ejecución		00	76 K	
fontdrvhost.exe	948	En ejecución		00	972 K	
Interrupciones del si...	-	En ejecución	SYSTEM	00	0 K	

Menos detalles Finalizar tarea

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.

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

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**.

Administrador de tareas

ArchivoOpcionesVista

ProcesosRendimientoHistorial de aplicacionesInicioUsuariosDetallesServicios

Último tiempo de BIOS: 0.0 segundos

Nombre	Anunciante	Estado	Impacto de ini...
Business Analytics Pro	Software Analytics	Habilitado	Alto
Enlace Móvil	Microsoft Corporation	Habilitado	No medido
Microsoft 365 Copilot	Microsoft Corporation	Deshabilitado	Ninguno
Microsoft Edge	Microsoft Corporation	Habilitado	Alto
Microsoft OneDrive	Microsoft Corporation	Habilitado	Alto
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Habilitado	Medio
Windows Security notificati...	Microsoft Corporation	Habilitado	Bajo

Menos detalles

Deshabilitar

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.

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

Actualización del agente

En el módulo de Aplicaciones, donde se había creado la primera llamada **Business Analytics**, debe ahora crear una nueva que será usada para actualizar la anterior. No se crearán dos aplicaciones diferentes, sino que se le enseñará al SCCM que hay una nueva versión de una aplicación ya existente y que una precede a otra.

Create Application Wizard

General

General

Import Information

Summary

Progress

Completion

Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

☒ Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\Dc\\msi\\endpoint\\Installer-v3.2.0.msi

Example: \\Server\\Share\\File

☐ Manually specify the application information

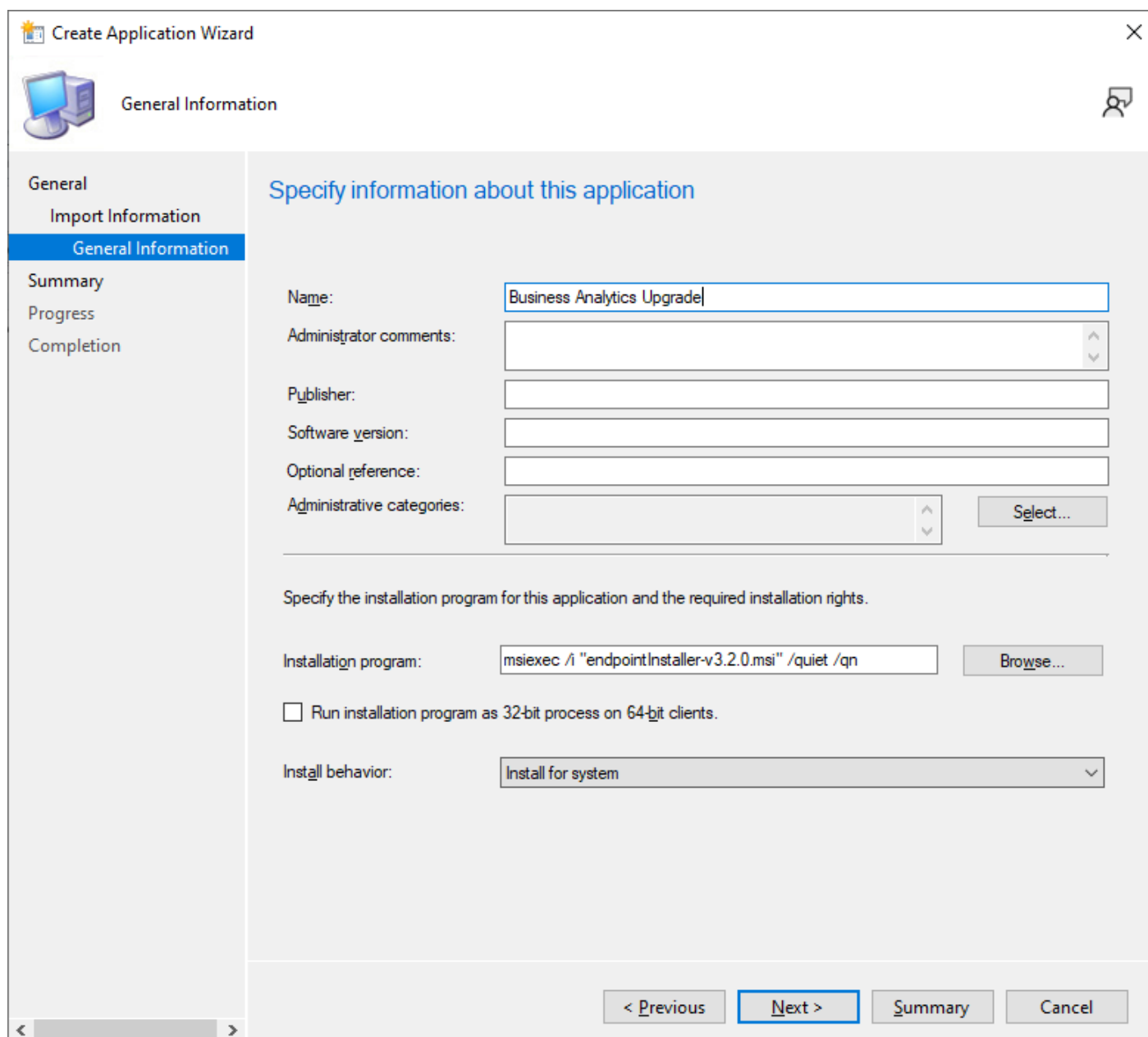
< Previous Next > Summary Cancel

Se dará clic derecho sobre **Applications** y luego en **Create Application**. En la ventana inicial deberá seleccionar el agente con una versión superior al anterior.

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

Información de la actualización

En la ventana donde se le pide proporcionar más información, deberá colocar un nombre que distinga esta aplicación de la anterior, por ejemplo **Business Analytics Upgrade**.



The screenshot shows the 'Create Application Wizard' window with the 'General Information' tab selected. The window title is 'Create Application Wizard'. The left sidebar contains the following options: General, Import Information, General Information (selected), Summary, Progress, and Completion. The main area is titled 'Specify information about this application' and contains the following fields:

- Name:** Business Analytics Upgrade
- Administrator comments:** (empty text box)
- Publisher:** (empty text box)
- Software version:** (empty text box)
- Optional reference:** (empty text box)
- Administrative categories:** (empty list box with a 'Select...' button)

Below these fields, there is a section titled 'Specify the installation program for this application and the required installation rights.' containing:

- Installation program:** msiexec /i "endpointInstaller-v3.2.0.msi" /quiet /qn (with a 'Browse...' button)
- ☐ Run installation program as 32-bit process on 64-bit clients.
- Install behavior:** Install for system (dropdown menu)

At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Summary', and 'Cancel'.

En el campo de texto de **Installation program** deberá especificar el comando para instalar la nueva versión:

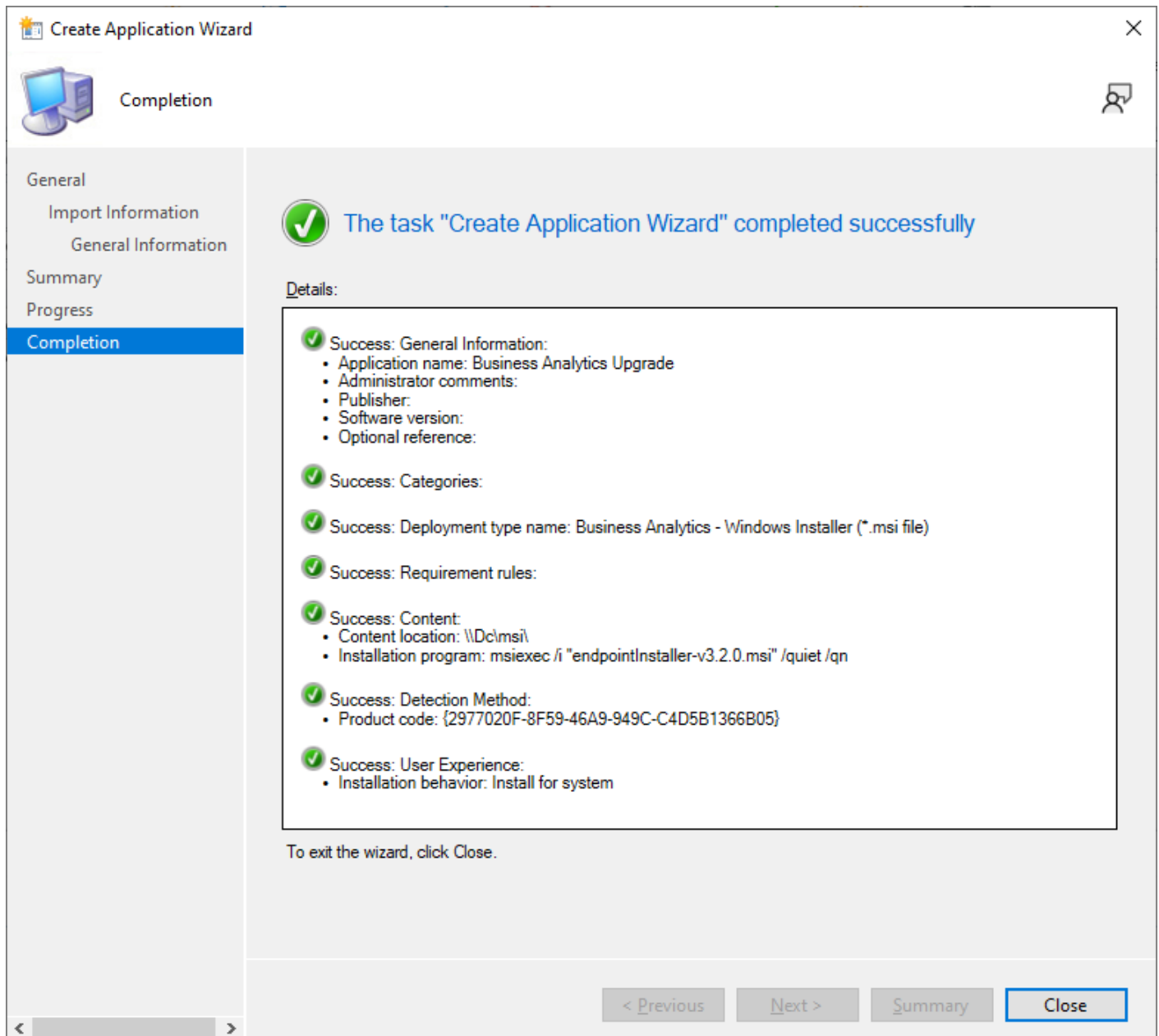
```
msiexec /i "endpointInstallation-v3.2.0.msi" /quiet /qn
```

Deberá luego seleccionar en **Install behavior** la opción **Install for system**, porque igual que la aplicación original, el nuevo agente también requiere que se ejecute la instalación con un rol privilegiado.

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

Resumen de la actualización

El resumen de la aplicación creada para actualizar la anterior luce así.

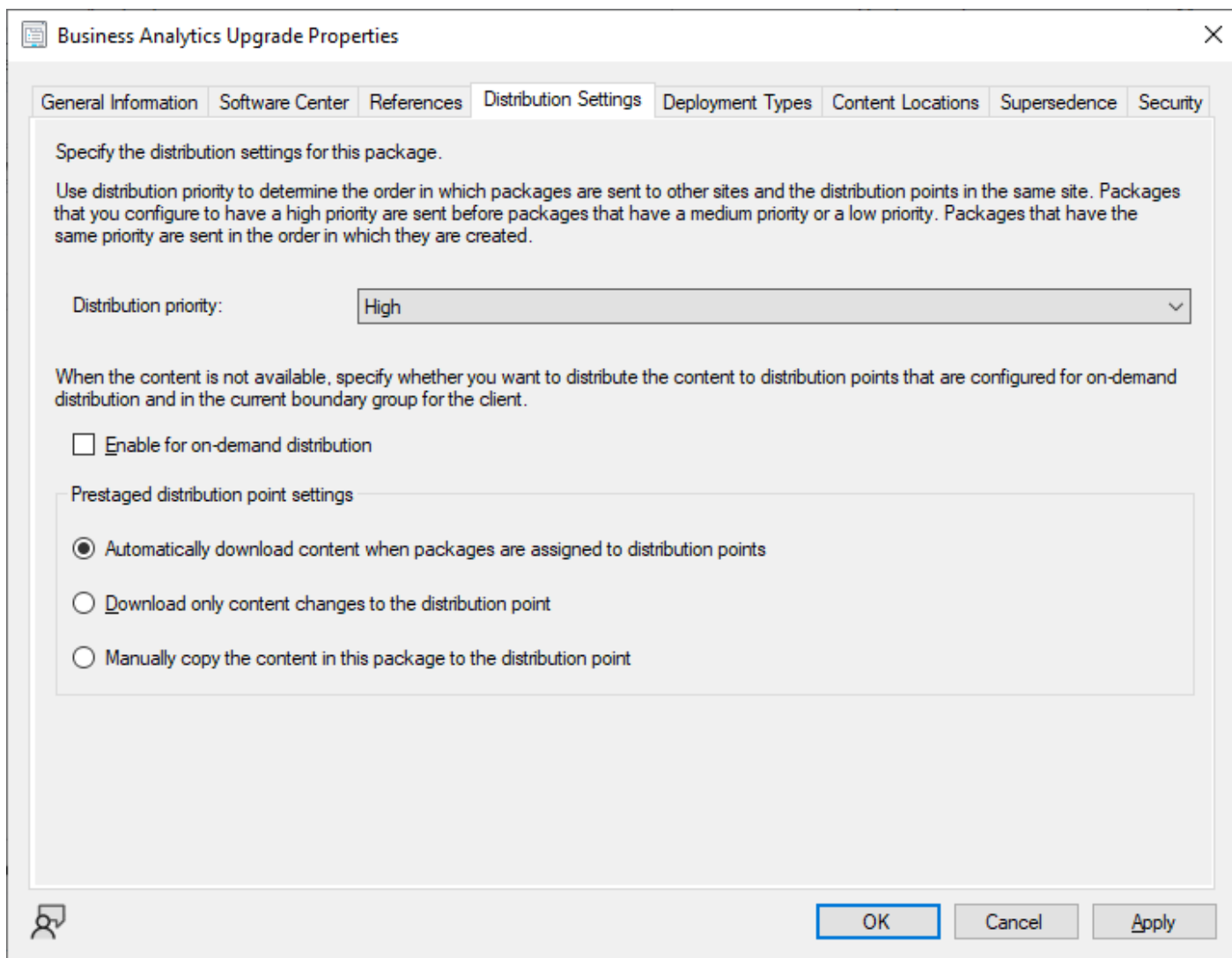


Se destaca que el código del producto es diferente al anterior paquete MSI. Internamente cuando el MSI se instala, busca versiones anteriores del mismo paquete y si las encuentra sobre-escribe la instalación anterior y modifica la información del paquete para que no queden duplicados o repetidos.

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

Propiedades de la actualización

Una vez finalizada la creación de la aplicación para la actualización, se procede a dar clic derecho sobre ella y luego en la pestaña **Distribution Settings** deberá seleccionar **High** en **Distribution priority**.



The screenshot shows the 'Business Analytics Upgrade Properties' dialog box with the 'Distribution Settings' tab selected. The dialog has a title bar with a close button (X) and a tab bar with the following tabs: General Information, Software Center, References, Distribution Settings (active), Deployment Types, Content Locations, Supersedence, and Security.

Inside the 'Distribution Settings' tab, there is a section titled 'Specify the distribution settings for this package.' followed by a descriptive paragraph: 'Use distribution priority to determine the order in which packages are sent to other sites and the distribution points in the same site. Packages that you configure to have a high priority are sent before packages that have a medium priority or a low priority. Packages that have the same priority are sent in the order in which they are created.'

Below this text is a 'Distribution priority:' label followed by a dropdown menu currently set to 'High'.

Further down, there is a text block: 'When the content is not available, specify whether you want to distribute the content to distribution points that are configured for on-demand distribution and in the current boundary group for the client.'

Below this is a checkbox labeled 'Enable for on-demand distribution' which is currently unchecked.

At the bottom of the main content area is a section titled 'Prestaged distribution point settings' containing three radio button options:

- ☒ Automatically download content when packages are assigned to distribution points
- ☐ Download only content changes to the distribution point
- ☐ Manually copy the content in this package to the distribution point

The dialog box has a standard footer with an icon on the left and three buttons on the right: 'OK' (highlighted with a blue border), 'Cancel', and 'Apply'.

Para terminar, deberá seleccionar la opción **Automatically download content when packages are assigned to distribution points**.

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

Configurar la supersedencia

En la ventana de propiedades de la actualización, deberá dar clic en la pestaña **Supersedence** para configurar la relación que existe entre esta actualización y la versión anterior del agente.

Specify Supersedence Relationship

Specify the deployment types to be replaced by this application.

Current Application:

Business Analytics Upgrade

Superseded Application:

Business Analytics

Browse...

Specify the new deployment type to replace the deployment types of the superseded application. The new deployment type will upgrade the installed, superseded deployment type unless you select the Uninstall checkbox. In that case, The previous deployment type will be uninstalled and the new deployment type will be newly installed.

Old Deployment Type	Technology	New Deployment Type	Uninstall
Business Analytics Pro - Windows Inst...	MSI	Business Analytics - Windows Installe ▾	<input type="checkbox"/>

OK

Cancel

En la ventana que aparece deberá escoger **Business Analytics - Windows Installer** en la columna **New Deployment Type** y deberá dejar la casilla de **Uninstall** no activa (sin activar).

Tipo de despliegue de actualización

Estando en la ventana de propiedades de la actualización y luego dando clic en la pestaña **Deployment Type** y editándola, se entrará en esta ventana en la cual deberá especificar los comandos de instalación y desinstalación del nuevo agente.

The screenshot shows the 'Business Analytics - Windows Installer (*.msi file) Properties' dialog box with the 'Programs' tab selected. The dialog has several tabs: 'General', 'Content', 'Programs', 'Detection Method', 'User Experience', 'Requirements', 'Return Codes', and 'Dependencies'. The 'Programs' tab contains three sections for specifying commands:

- Specify the command to install this application.**
 - Installation program: `msiexec /i "endpointInstaller-v3.2.0.msi" /quiet /qn`
 - Installation start in: (empty text box)
- Specify the command to uninstall this application.**
 - Uninstall program: `iexec /x "{2977020F-8F59-46A9-949C-C4D5B1366B05}" /qn`
 - Uninstall start in: (empty text box)
- Specify the command to repair this application.**
 - Repair program: (empty text box)
 - Repair start in: (empty text box)

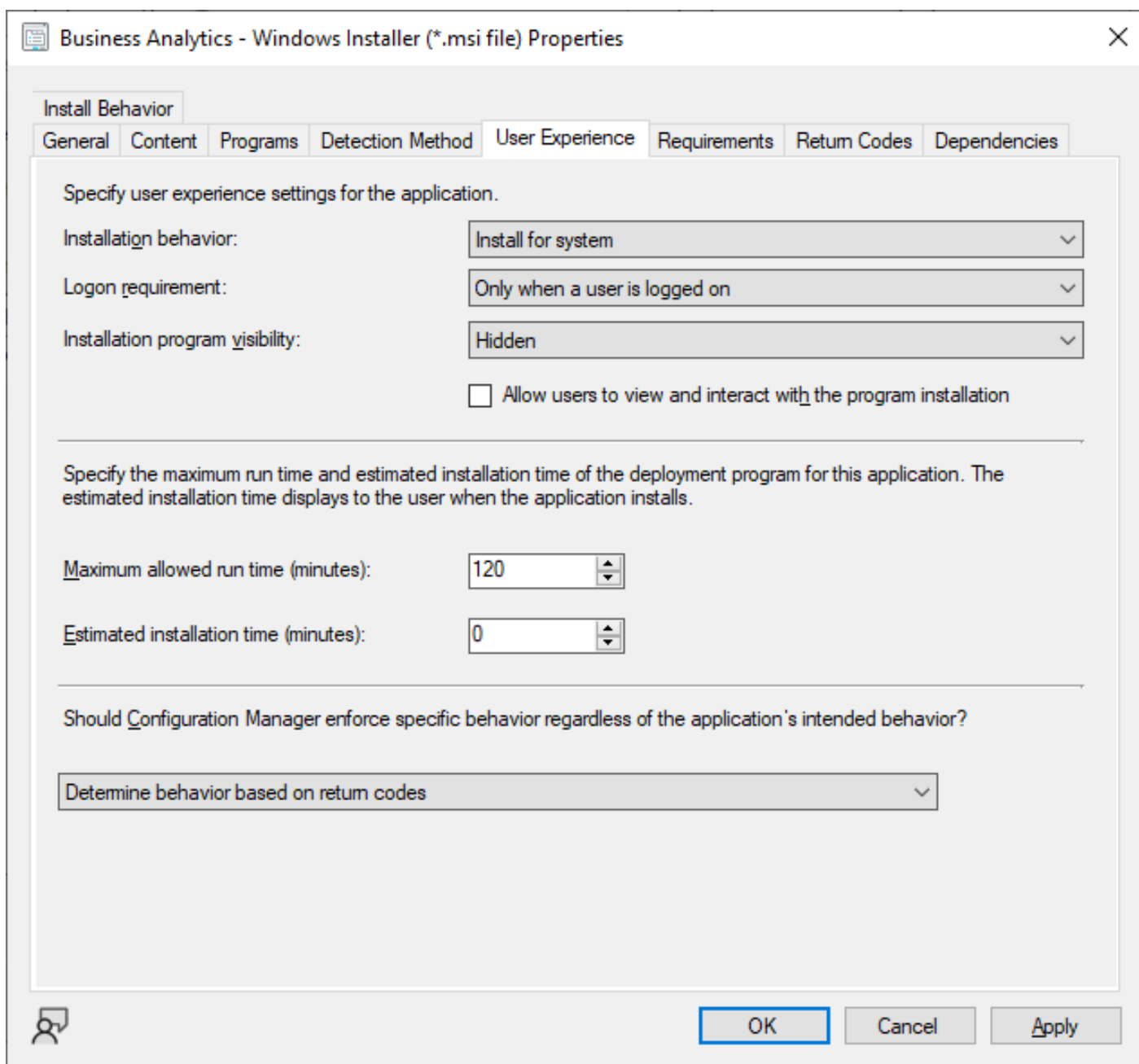
Below these sections is a checkbox labeled 'Run installation and uninstall program as 32-bit process on 64-bit clients.' which is currently unchecked. At the bottom, there is a text box for 'Product code:' and a 'Browse...' button. The dialog also features 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

En la pestaña **Programs** deberá asegurarse de que el campo **Uninstall program** contenga las comillas alrededor del ID del producto y que termine en /qn.

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

Experiencia de usuario en actualización

En la misma ventana que la anterior (**Deployment Type - Edit**) deberá dar clic en la pestaña **User Experience** para configurar la forma en que se le muestra información al usuario.



Business Analytics - Windows Installer (*.msi file) Properties

Install Behavior

General Content Programs Detection Method **User Experience** Requirements Return Codes Dependencies

Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Only when a user is logged on

Installation program visibility: Hidden

☐ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 120

Estimated installation time (minutes): 0

Should Configuration Manager enforce specific behavior regardless of the application's intended behavior?

Determine behavior based on return codes

OK Cancel Apply

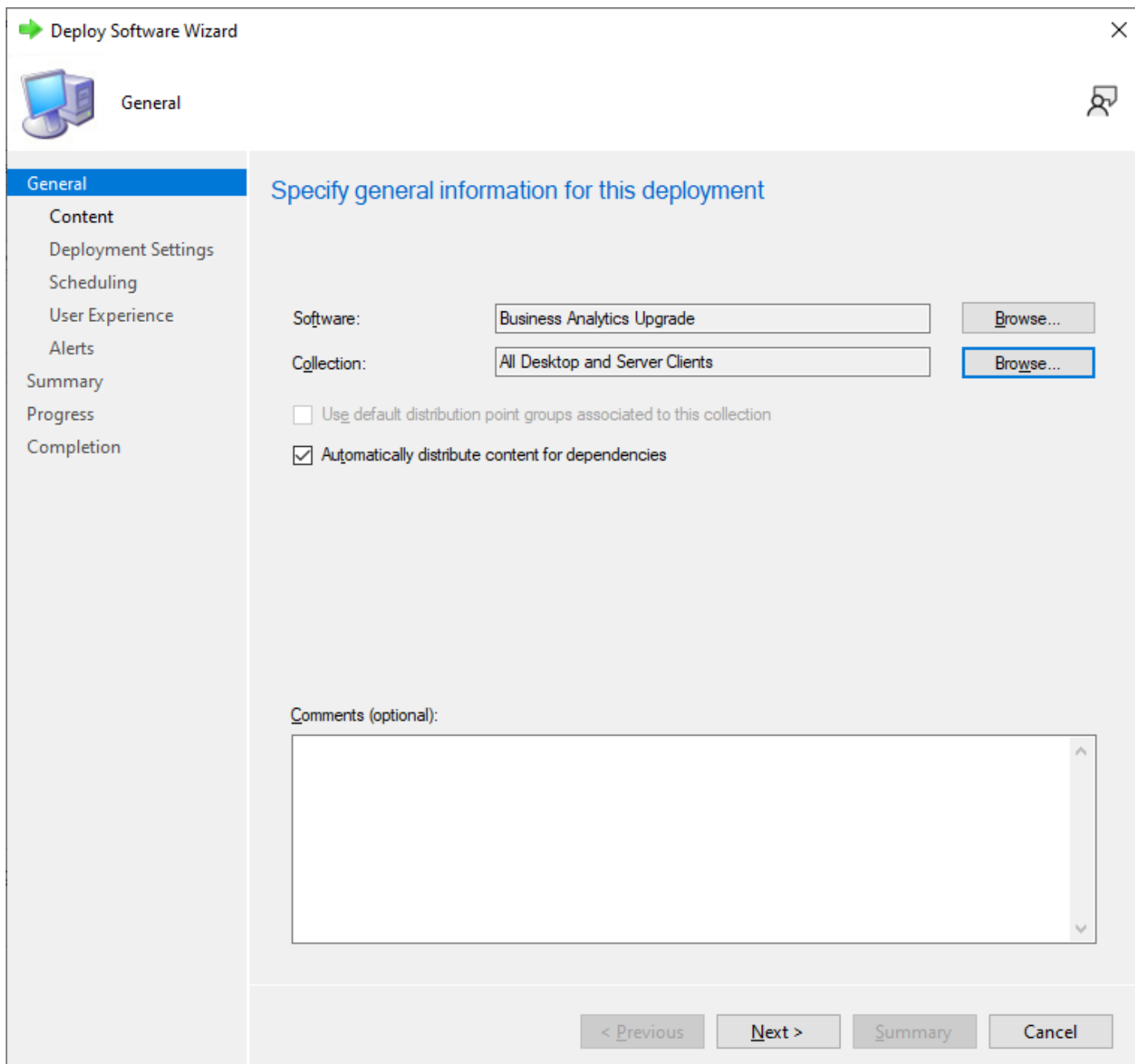
Deberá seleccionar en **Install behavior** la opción **Install for system**, en **Logon requirement** la opción **Only when a user is logged on** y por último en **Installation program visibility** escoger

Hidden.

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

Despliegue de actualización

Una vez creada la aplicación para la actualización, se procede a dar clic derecho sobre ella y luego en **Deploy**.



The screenshot shows the 'Deploy Software Wizard' window. The title bar includes a green arrow icon and the text 'Deploy Software Wizard'. The window is divided into a left sidebar and a main content area. The sidebar contains a 'General' tab (selected) and a list of steps: Content, Deployment Settings, Scheduling, User Experience, Alerts, Summary, Progress, and Completion. The main content area is titled 'Specify general information for this deployment'. It contains two text boxes: 'Software:' with the value 'Business Analytics Upgrade' and 'Collection:' with the value 'All Desktop and Server Clients'. Each text box has a 'Browse...' button to its right. Below these are two checkboxes: 'Use default distribution point groups associated to this collection' (unchecked) and 'Automatically distribute content for dependencies' (checked). At the bottom of the main area is a 'Comments (optional):' label above a large text area. At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

Deploy Software Wizard

General

Specify general information for this deployment

Software: Business Analytics Upgrade Browse...

Collection: All Desktop and Server Clients Browse...

☐ Use default distribution point groups associated to this collection

☒ Automatically distribute content for dependencies

Comments (optional):

< Previous Next > Summary Cancel

En esta ventana deberá seleccionar la colección de usuarios o dispositivos a los cuales se les hará la actualización del agente.

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

Destino de contenido para actualizar

En esta ventana deberá asegurarse de seleccionar el **Distribution Point** donde será descargado el contenido.

Deploy Software Wizard

Content

General

Content

Deployment Settings

Scheduling

User Experience

Alerts

Summary

Progress

Completion

Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

Name	Type
There are no items to show in this view.	

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Filter...

Name	Description	Associations
DC.NOFRAUD.LOCAL	Distribution point	

Add

Remove

< Previous

Next >

Summary

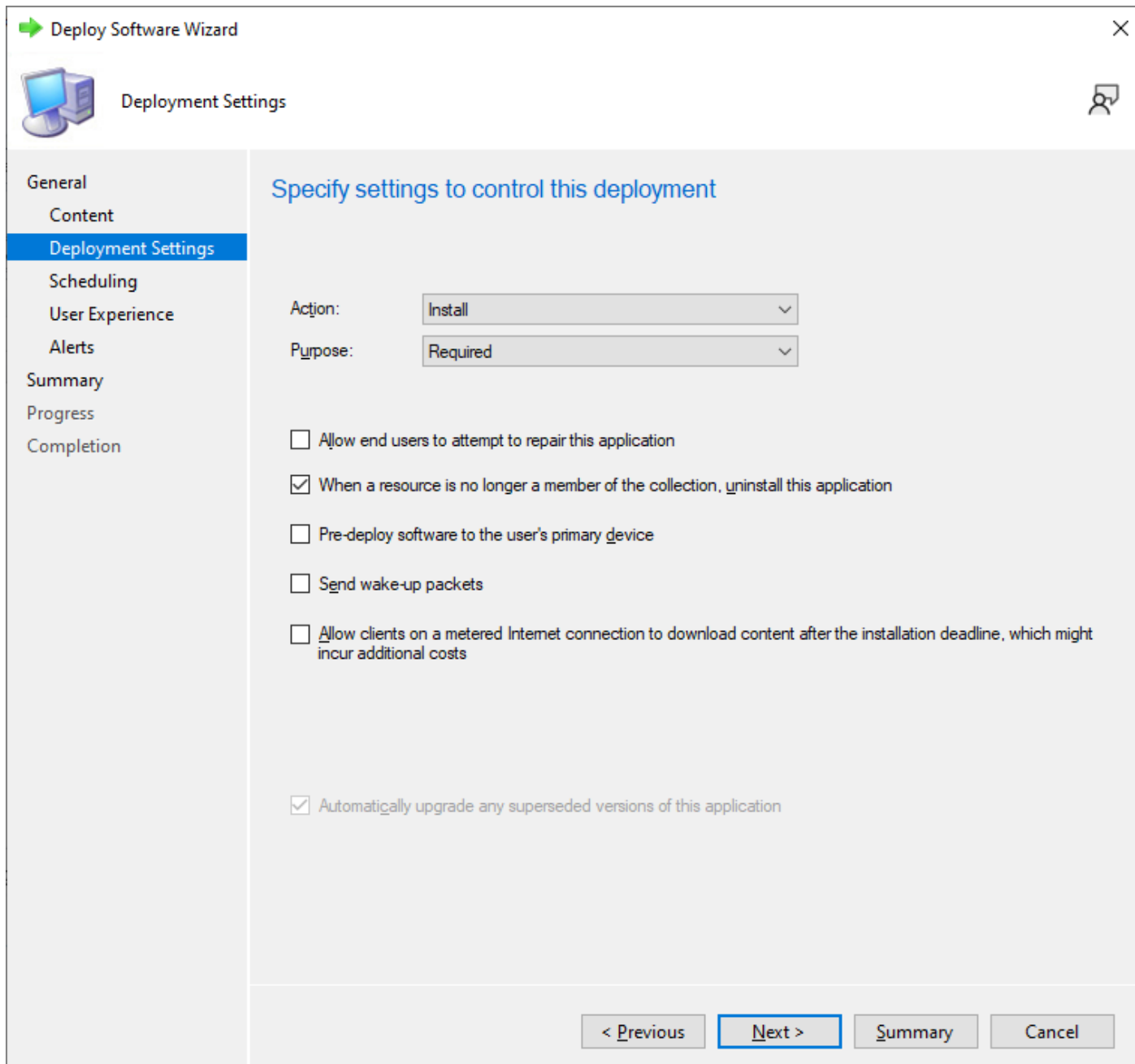
Cancel

Normalmente existe solo un **Distribution Point**, por lo que se recomienda seleccionar el que trae por defecto cuando se da clic en **Add** y luego en **Distribution Point**.

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

Acción de actualización

En la ventana de acciones, se deberá seleccionar **Install** y el propósito de la acción será **Required**



The screenshot shows the 'Deploy Software Wizard' window with the 'Deployment Settings' tab selected. The left sidebar lists the following steps: General, Content, **Deployment Settings**, Scheduling, User Experience, Alerts, Summary, Progress, and Completion. The main area is titled 'Specify settings to control this deployment' and contains the following settings:

- Action: **Install** (selected in the dropdown)
- Purpose: **Required** (selected in the dropdown)
- ☐ Allow end users to attempt to repair this application
- ☒ When a resource is no longer a member of the collection, uninstall this application
- ☐ Pre-deploy software to the user's primary device
- ☐ Send wake-up packets
- ☐ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
- ☒ Automatically upgrade any superseded versions of this application

At the bottom, there are four buttons: '< Previous', **Next >** (highlighted with a blue border), 'Summary', and 'Cancel'.

Al final deberá activar la casilla que dice **When a resource is no longer a member of the collection, uninstall this application**. Esto lo que significa es que cuando el usuario o el dispositivo se saquen de la colección automáticamente se le enviará la orden de desinstalar el agente.

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

Agenda de la actualización

En la ventana de agendar la actualización se puede programar para cuándo se realiza.

Deploy Software Wizard

Scheduling

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify the schedule for this deployment

This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.

Time based on: UTC

☐ Schedule the application to be available at:
7/11/2025 10:10 PM

Installation deadline:
☒ As soon as possible after the available time
☐ Schedule at:
7/11/2025 10:10 PM

☐ Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.

< Previous Next > Summary Cancel

Se recomienda no activar el agendamiento y dejar que se actualice de forma inmediata.

Experiencia para desplegar actualización

En esta ventana se configura la experiencia del usuario para que no se le muestre ningún tipo de aviso ni tenga ninguna interacción con la actualización del agente.

The screenshot shows the 'Deploy Software Wizard' window, specifically the 'User Experience' tab. The left sidebar contains a list of configuration options: General, Content, Deployment Settings, Scheduling, User Experience (selected), Alerts, Summary, Progress, and Completion. The main area is titled 'Specify the user experience for the installation of this software:'. It includes a section 'Specify user experience setting for this deployment' with a 'User notifications:' dropdown menu set to 'Hide in Software Center and all notifications'. Below this is a checkbox 'When software changes are required, show a dialog window to the user instead of a toast notification'. Another section 'When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:' contains checkboxes for 'Software Installation' and 'System restart (if required to complete the installation)'. A section 'Write filter handling for Windows Embedded devices' has a checked checkbox 'Commit changes at deadline or during a maintenance window (requires restarts)'. A note states: 'If this option is not selected, content will be applied on the overlay and committed later.' At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted), 'Summary', and 'Cancel'.

Deploy Software Wizard

User Experience

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify the user experience for the installation of this software:

Specify user experience setting for this deployment

User notifications:
Hide in Software Center and all notifications

☐ When software changes are required, show a dialog window to the user instead of a toast notification

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

☐ Software Installation
☐ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

☒ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

< Previous Next > Summary Cancel

Se deberá elegir la opción **Hide in Software Center and all notifications** para que no se le presente al usuario ninguna alerta al momento de llevar a cabo la actualización.

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

Alertamiento de actualización

Se pueden configurar alertas en caso de que la actualización falle o no se lleve a cabo.

The screenshot shows the 'Deploy Software Wizard' window with the 'Alerts' tab selected. The left sidebar contains a navigation pane with the following items: General, Content, Deployment Settings, Scheduling, User Experience, Alerts (highlighted), Summary, Progress, and Completion. The main area is titled 'Specify Configuration Manager and Operations Manager alert options'. It contains two sections for thresholds: 'Threshold for successful deployment' and 'Threshold for failed deployment'. Each section has a checkbox to 'Create a deployment alert when the threshold is lower/higher than the following:'. The 'successful deployment' section has a 'Percent success' spinner set to 1, and the 'failed deployment' section has a 'Percent failure' spinner set to 0. Both sections also have 'After' fields with date and time pickers. At the bottom, there are three checkboxes: 'Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.', 'Enable System Center Operations Manager maintenance mode', and 'Generate System Center Operations Manager alert when a software installation fails'. The bottom right of the window has four buttons: '< Previous', 'Next >' (highlighted), 'Summary', and 'Cancel'.

Deploy Software Wizard

Alerts

General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion

Specify Configuration Manager and Operations Manager alert options

Configuration Manager generates alerts when this application is deployed.

Threshold for successful deployment

☐ Create a deployment alert when the threshold is lower than the following:

Percent success: 1

After: 7/18/2025 3:10 PM

Threshold for failed deployment

☐ Create a deployment alert when the threshold is higher than the following:

Percent failure: 0

Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.

☐ Enable System Center Operations Manager maintenance mode

☐ Generate System Center Operations Manager alert when a software installation fails

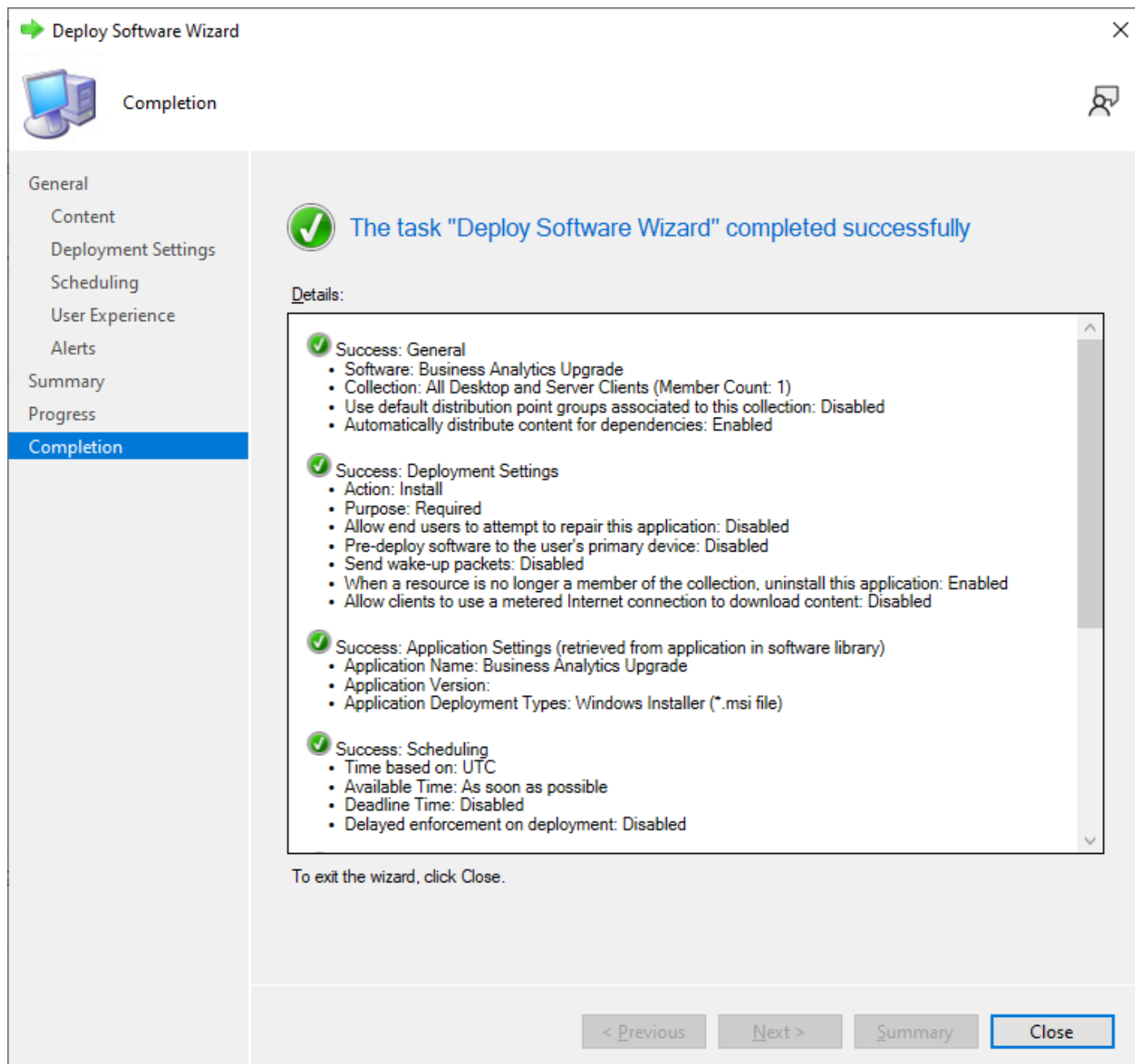
< Previous Next > Summary Cancel

Se recomienda no configurar ninguna alerta y proceder con las opciones por defecto.

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

Resumen de actualización

Al finalizar el proceso de actualización se mostrará un resumen donde se consolida toda la información sobre las configuraciones seleccionadas.

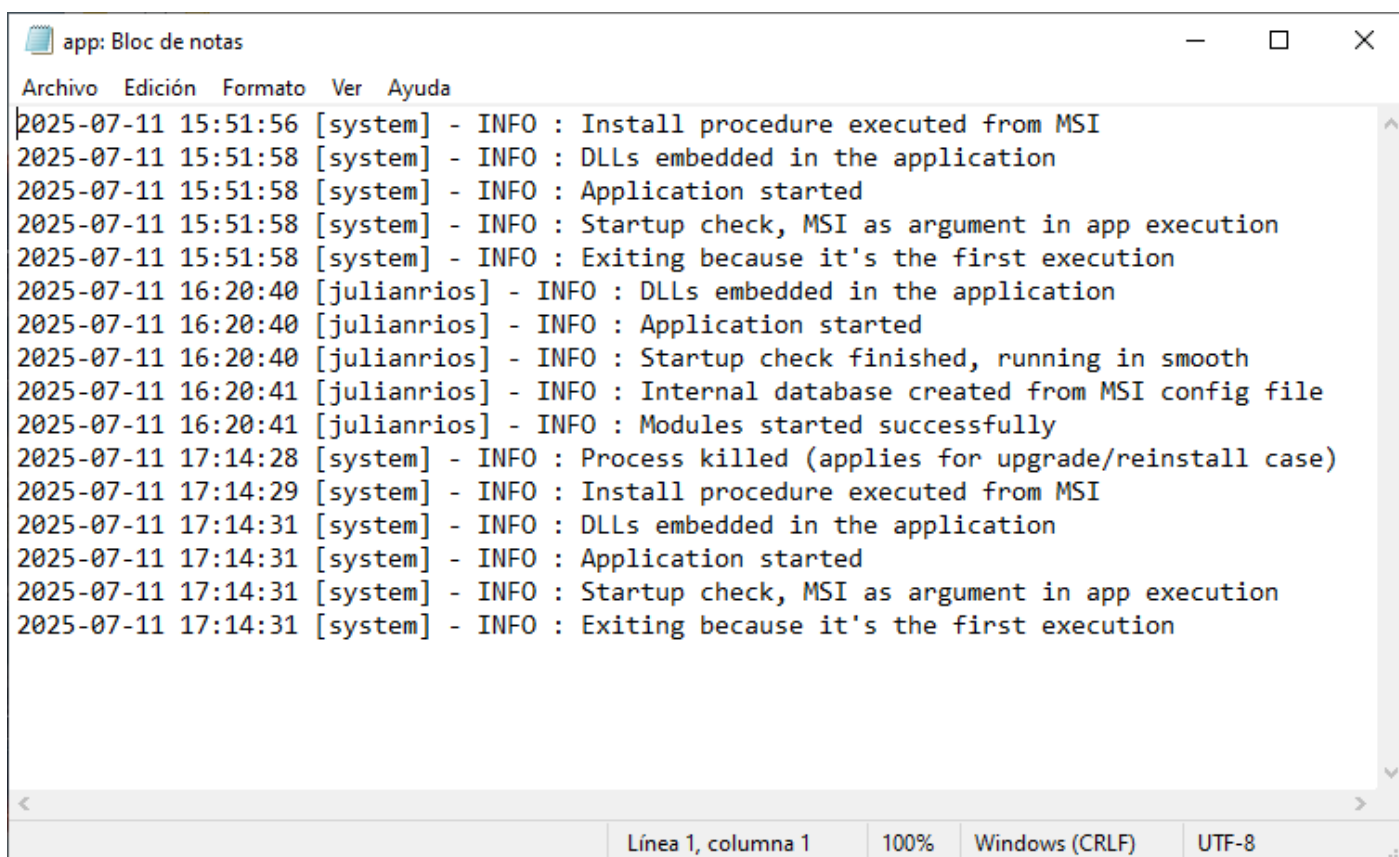


En esta pantalla es importante asegurarse de que la acción elegida fue **Install** y de que el propósito fue **Required**.

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

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.



```
app: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup check, MSI as argument in app execution
2025-07-11 15:51:58 [system] - INFO : Exiting because it's the first execution
2025-07-11 16:20:40 [julianrios] - INFO : DLLs embedded in the application
2025-07-11 16:20:40 [julianrios] - INFO : Application started
2025-07-11 16:20:40 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-11 16:20:41 [julianrios] - INFO : Internal database created from MSI config file
2025-07-11 16:20:41 [julianrios] - INFO : Modules started successfully
2025-07-11 17:14:28 [system] - INFO : Process killed (applies for upgrade/reinstall case)
2025-07-11 17:14:29 [system] - INFO : Install procedure executed from MSI
2025-07-11 17:14:31 [system] - INFO : DLLs embedded in the application
2025-07-11 17:14:31 [system] - INFO : Application started
2025-07-11 17:14:31 [system] - INFO : Startup check, MSI as argument in app execution
2025-07-11 17:14:31 [system] - INFO : Exiting because it's the first execution
```

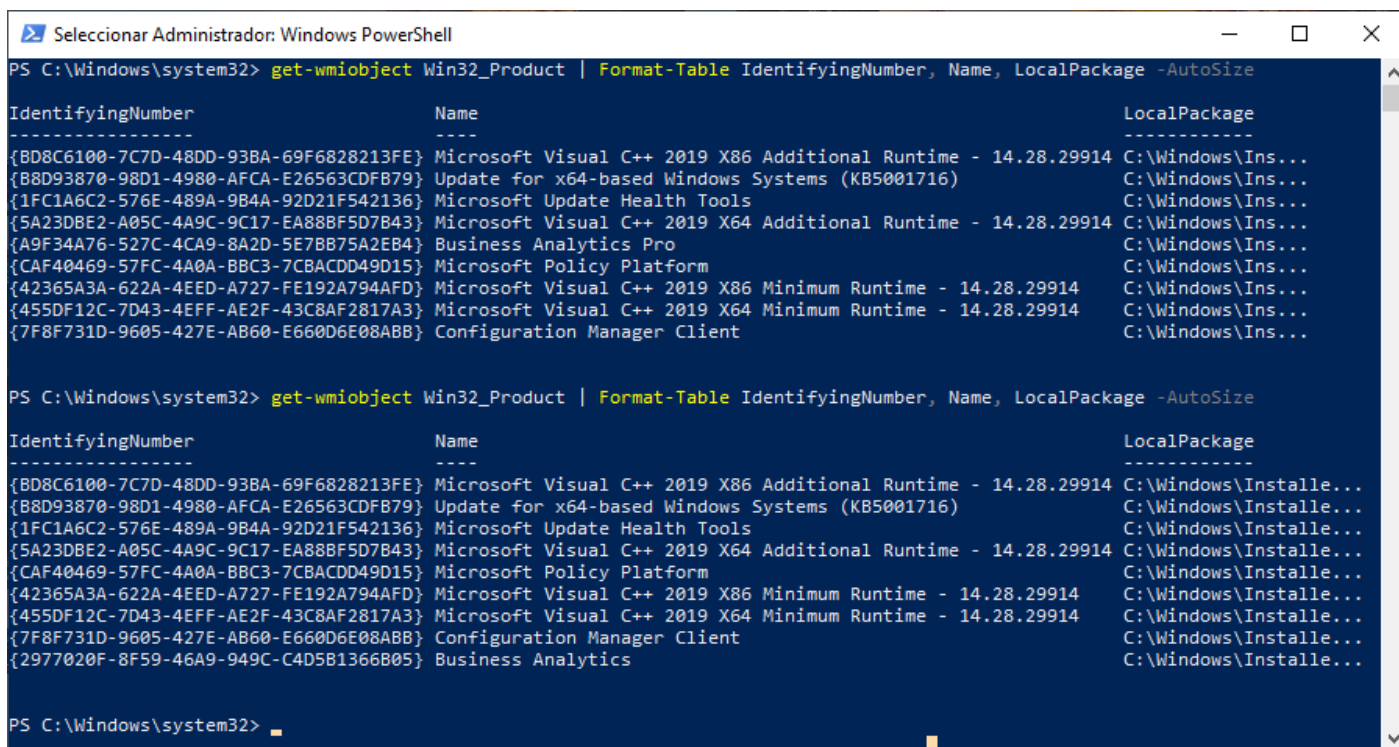
Deberá aparecer el mensaje **Process killed (applies for upgrade/reinstall case)** y se mostrará la usuario **system** como el ejecutor de esa actividad.

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

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
```



```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05}	Business Analytics	C:\Windows\Installe...

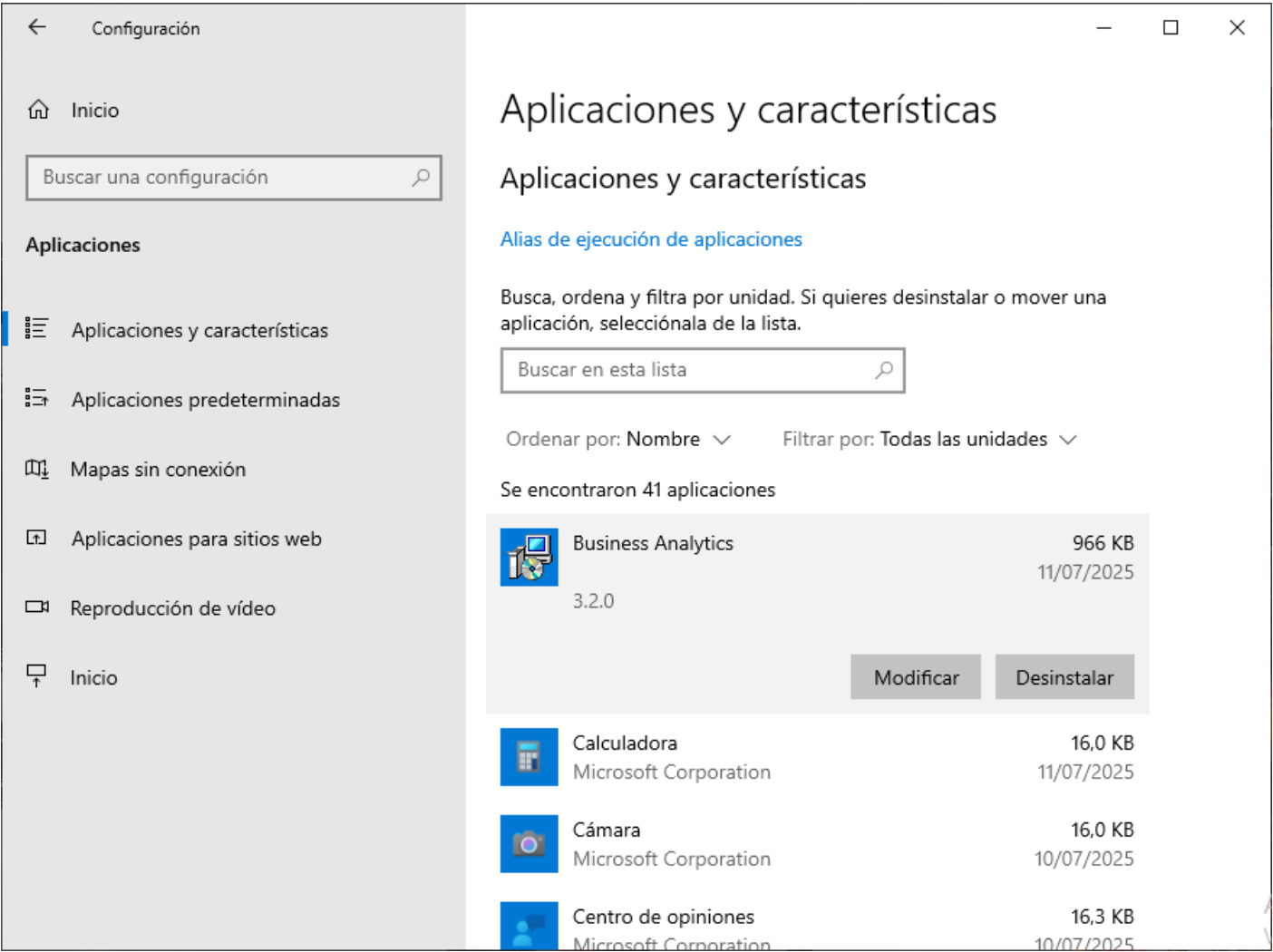
```
PS C:\Windows\system32>
```

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

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

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.

Desinstalar el agente

Para desinstalar el agente se debe primero eliminar el **Deployment** de instalación o actualización del agente, para esto, se da clic en la última aplicación creada previamente y luego en la parte inferior entrar a la pestaña **Deployments**, seleccionar la entrada que aparece, darle clic derecho y luego en **Delete**.

Microsoft Configuration Manager (Connected to WHQ, NOFRAUD LAB - DC.nofraud.local) (Evaluation, 180 days left)

Home Deployment Folder All Workspaces Search

Enable Delete Disable Collection Refresh Properties

Deployment Properties

Software Library Overview Application Management Applications

Applications 2 items

Search current node + subfolders

Icon	Name	Deployment Types	Deployments	Status
	Business Analytics	1	1	Active
	Business Analytics Upgrade	1	1	Active

Business Analytics Upgrade

Icon	Collection	Deployment Start Time	Purpose	Compliance %	Action	Requires Approval
	All Desktop and Server Clients	7/11/2025 10:13 PM	Required	0.0	Install	No

Summary Deployment Types Deployments Phased Deployments Task Sequences Application Groups

Debe eliminar el deployment, no la aplicación y esto es debido a que no pueden existir dos deployments que se contraríen el uno al otro (uno instala y otro desinstala).

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

Deployment de la desinstalación

Para crear un **Deploy** de desinstalación, de clic derecho sobre la última aplicación creada (la última versión del agente) y luego en la opción Deploy.

Deploy Software Wizard

General

Specify general information for this deployment

Software: Business Analytics Upgrade Browse...

Collection: All Desktop and Server Clients Browse...

☐ Use default distribution point groups associated to this collection

☒ Automatically distribute content for dependencies

Comments (optional):

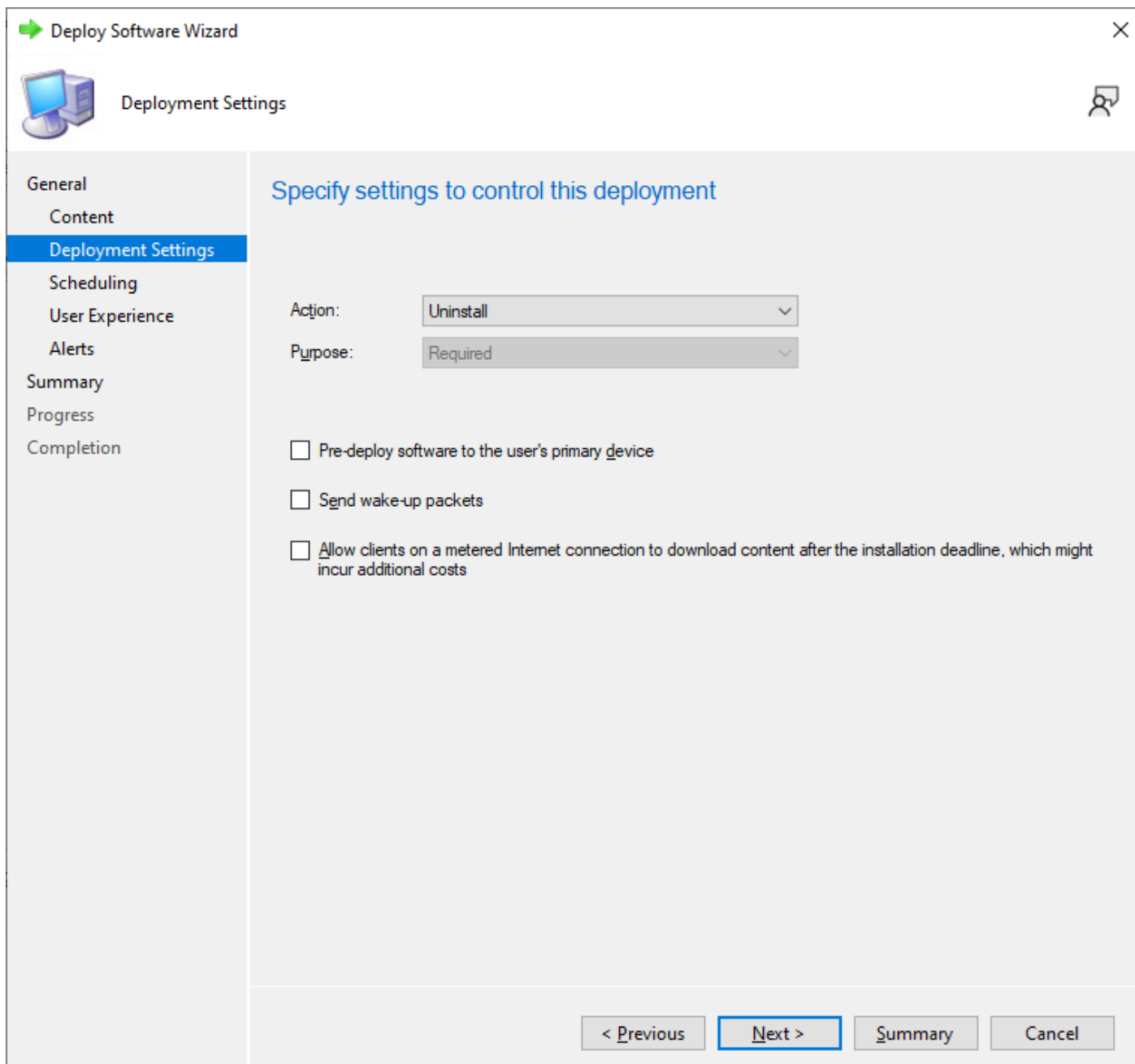
< Previous Next > Summary Cancel

En la ventana de **Deploy** seleccione la colección de usuario o dispositivos en los cuales se llevará a cabo la desinstalación del agente.

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

Acción de desinstalación

Se debe seleccionar la acción **Uninstall** para continuar con la desinstalación del agente.



The screenshot shows the 'Deploy Software Wizard' window, specifically the 'Deployment Settings' tab. The left sidebar contains a list of steps: General, Content, Deployment Settings (highlighted), Scheduling, User Experience, Alerts, Summary, Progress, and Completion. The main area is titled 'Specify settings to control this deployment'. It features two dropdown menus: 'Action' set to 'Uninstall' and 'Purpose' set to 'Required'. Below these are three unchecked checkboxes: 'Pre-deploy software to the user's primary device', 'Send wake-up packets', and 'Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs'. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Summary', and 'Cancel'.

Setting	Value
Action:	Uninstall
Purpose:	Required

- ☐ Pre-deploy software to the user's primary device
- ☐ Send wake-up packets
- ☐ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

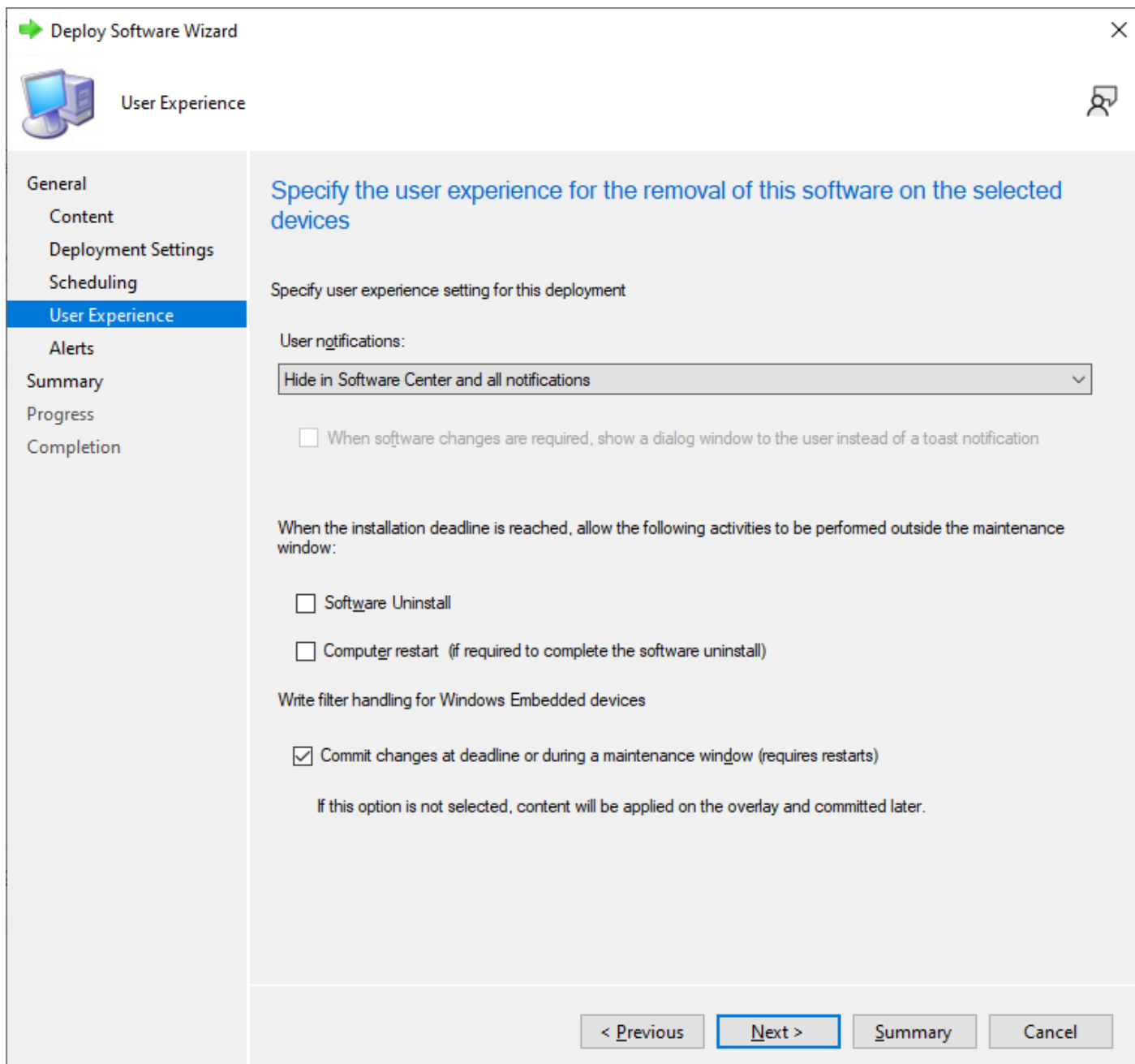
Navigation buttons: < Previous, **Next >**, Summary, Cancel

En esta ventana la opción de **Purpose** está deshabilitada debido a que una desinstalación por defecto tiene un propósito único y este es el requerido.

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

Experiencia de desinstalación

En esta ventana se configura qué tipo de información se le mostrará al usuario cuando se ejecute la desinstalación del agente en su máquina.



The screenshot shows the 'Deploy Software Wizard' window, specifically the 'User Experience' tab. The window has a title bar with a green arrow icon and the text 'Deploy Software Wizard'. Below the title bar is a navigation pane on the left with the following options: General, Content, Deployment Settings, Scheduling, User Experience (selected), Alerts, Summary, Progress, and Completion. The main area of the window is titled 'Specify the user experience for the removal of this software on the selected devices'. It contains the following settings:

- 'Specify user experience setting for this deployment': A dropdown menu set to 'Hide in Software Center and all notifications'.
- 'User notifications': A checkbox labeled 'When software changes are required, show a dialog window to the user instead of a toast notification' which is unchecked.
- 'When the installation deadline is reached, allow the following activities to be performed outside the maintenance window': Two checkboxes, 'Software Uninstall' and 'Computer restart (if required to complete the software uninstall)', both of which are unchecked.
- 'Write filter handling for Windows Embedded devices': A checkbox labeled 'Commit changes at deadline or during a maintenance window (requires restarts)' which is checked.
- A note below the checked checkbox: 'If this option is not selected, content will be applied on the overlay and committed later.'

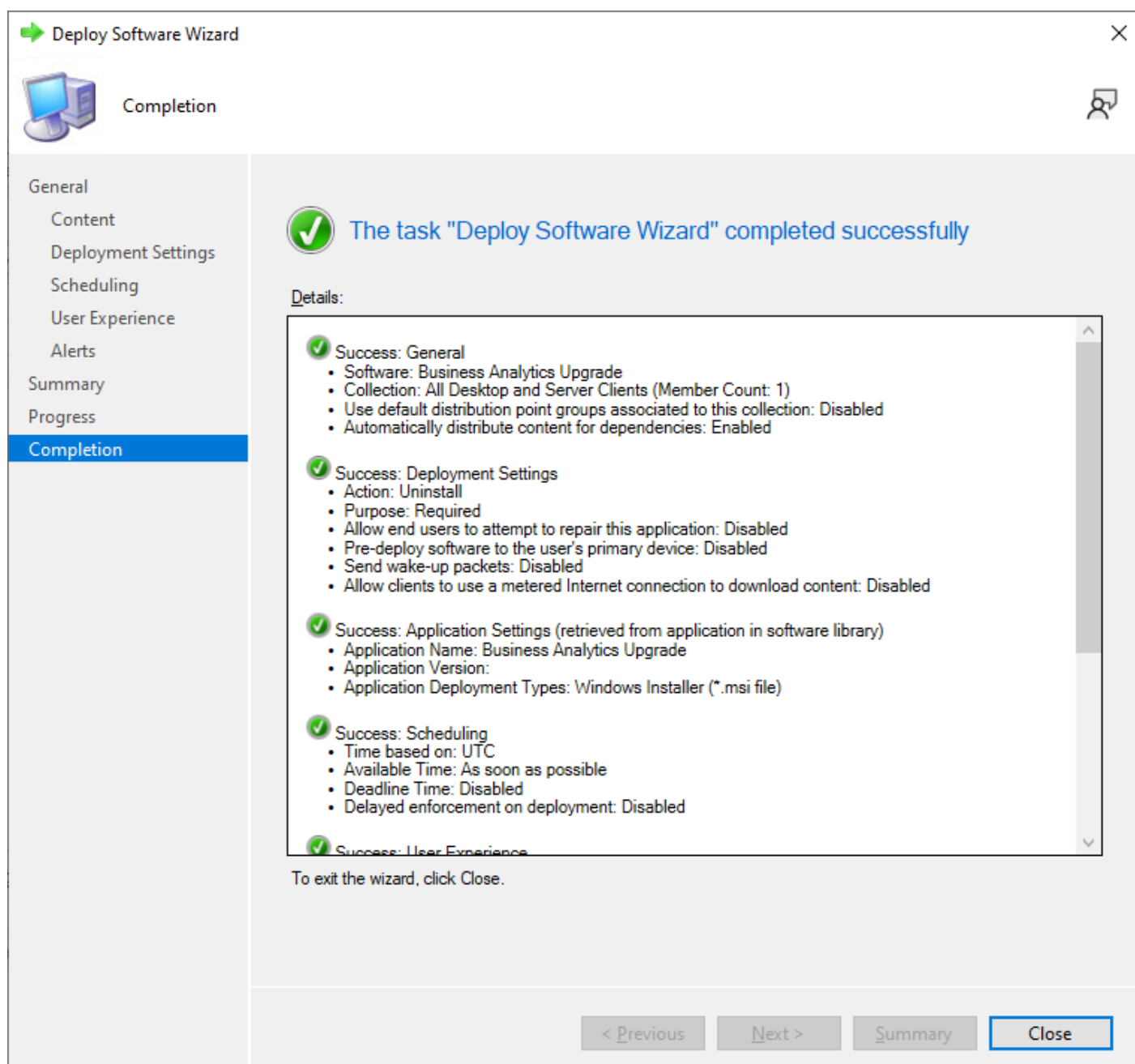
At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Summary', and 'Cancel'.

Se recomienda establecer la opción **Hide in Software Center and all notifications** para que el usaurio no sea molestado con avisos de desinstalación del agente.

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

Resumen de la desinstalación

Para finalizar, se muestra un resumen de la acción de desinstalación que se acabó de configurar.



Aquí se debe revisar que efectivamente quede bien señalada que la acción es **Uninstall**.

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

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
```

The screenshot shows a Windows PowerShell console window titled 'Administrador: Windows PowerShell'. The command is executed three times, showing the list of installed products. The output is formatted as a table with three columns: IdentifyingNumber, Name, and LocalPackage.

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05}	Business Analytics	C:\Windows\Installe...

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...

```
PS C:\Windows\system32>
```

Como se observa, después de crear la acción de desinstalación en el SCCM, ya no aparece la aplicación Business Analytics.

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

Instalación y desinstalación manual

En esta entrada se mostrará cómo realizar una instalación manual del agente en un PC, así como su actualización y desinstalación.

Requisitos previos

Antes de ejecutar de **manera manual** un procedimiento de instalación, actualización o desinstalación del agente es importante tener en cuenta los siguientes requisitos previos:

Debe contar con la capacidad de realizar acciones administrativas en el PC debido a que se debe abrir la consola MS-DOS en el equipo del usuario con privilegios de administrador.

Encuentre la manera de tener acceso al PC del usuario, ya sea de forma presencial (física) o de forma remota. Que la instalación sea manual no quiere decir que necesariamente requiera de una presencia física en el computador.

En la instalación manual no se requiere que el PC o el usuario pertenezcan a un dominio o que tengan un agente instalado SCCM u otro. Se puede llevar a cabo la instalación incluso en equipos con versiones de sistema operativo Home.

Debe copiar o descargar el agente de The Fraud Explorer (normalmente llamado **endpointInstaller.msi**) al PC para que se pueda llevar a cabo su instalación. Para esta instalación manual, se debe descargar de forma manual el MSI del agente de The Fraud Explorer al computador. Puede descargar el agente a través de una carpeta compartida en Onedrive o incluso accediendo a una ruta de red donde tenga el MSI compartido.

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.

Instalación y desinstalación manual

Video con todos los pasos

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

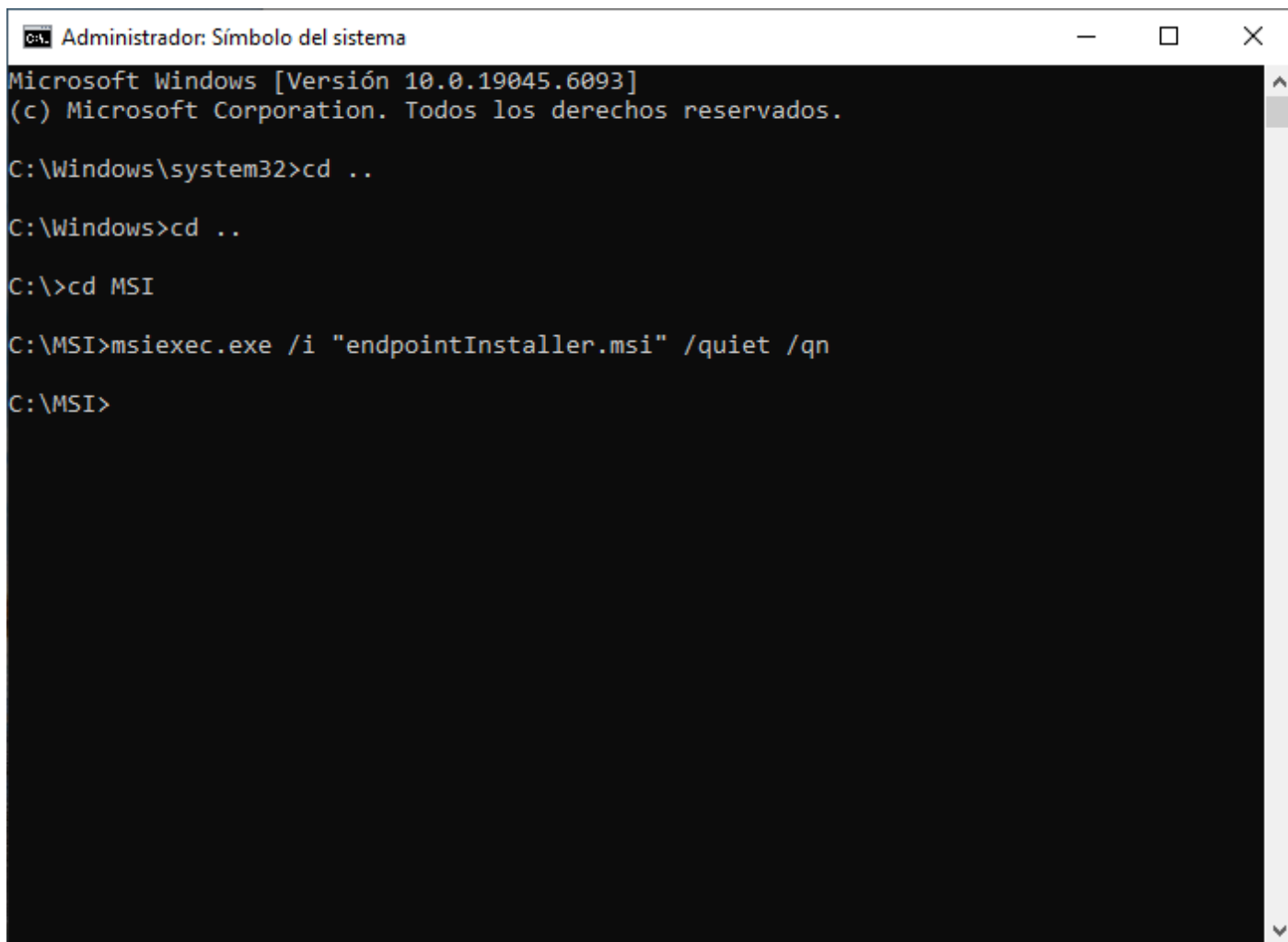
<https://www.youtube.com/embed/87HNEWn-4Ts?si=YyKvfKAHeRWmqj6g>

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.

Instalación del agente

Abra una consola **MS-DOS** en modo administrador. Estos comandos no funcionan en una consola **MS-DOS** que no se abra en modo administrador.



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.6093]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd MSI

C:\MSI>msiexec.exe /i "endpointInstaller.msi" /quiet /qn

C:\MSI>
```

Vaya a la ruta donde ha descargado el MSI del agente de The Fraud Explorer y ejecute el siguiente comando:

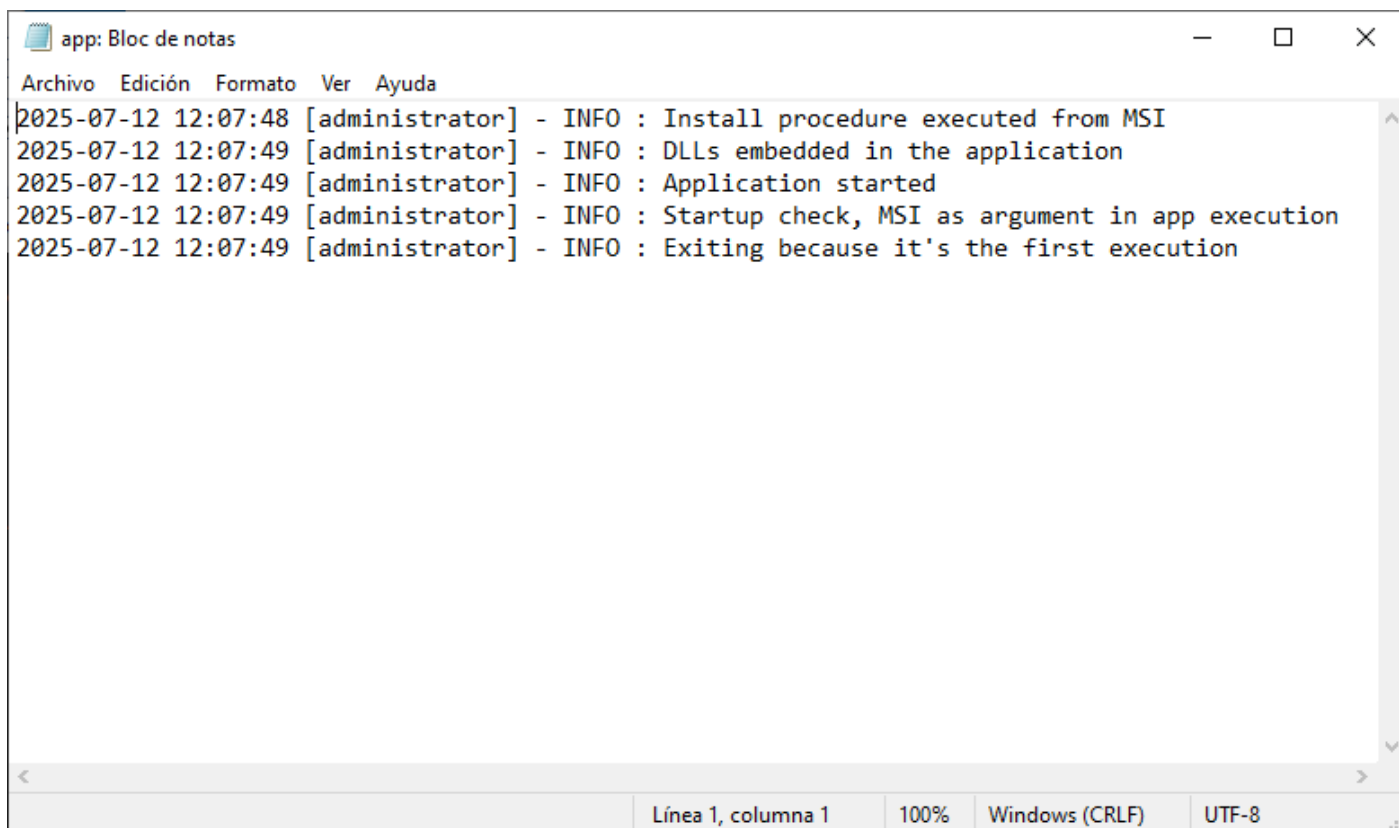
```
msiexec.exe /i "endpointInstaller.exe" /quiet /qn
```

Este comando instalará de manera silenciosa el agente en el computador del usuario.

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

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.



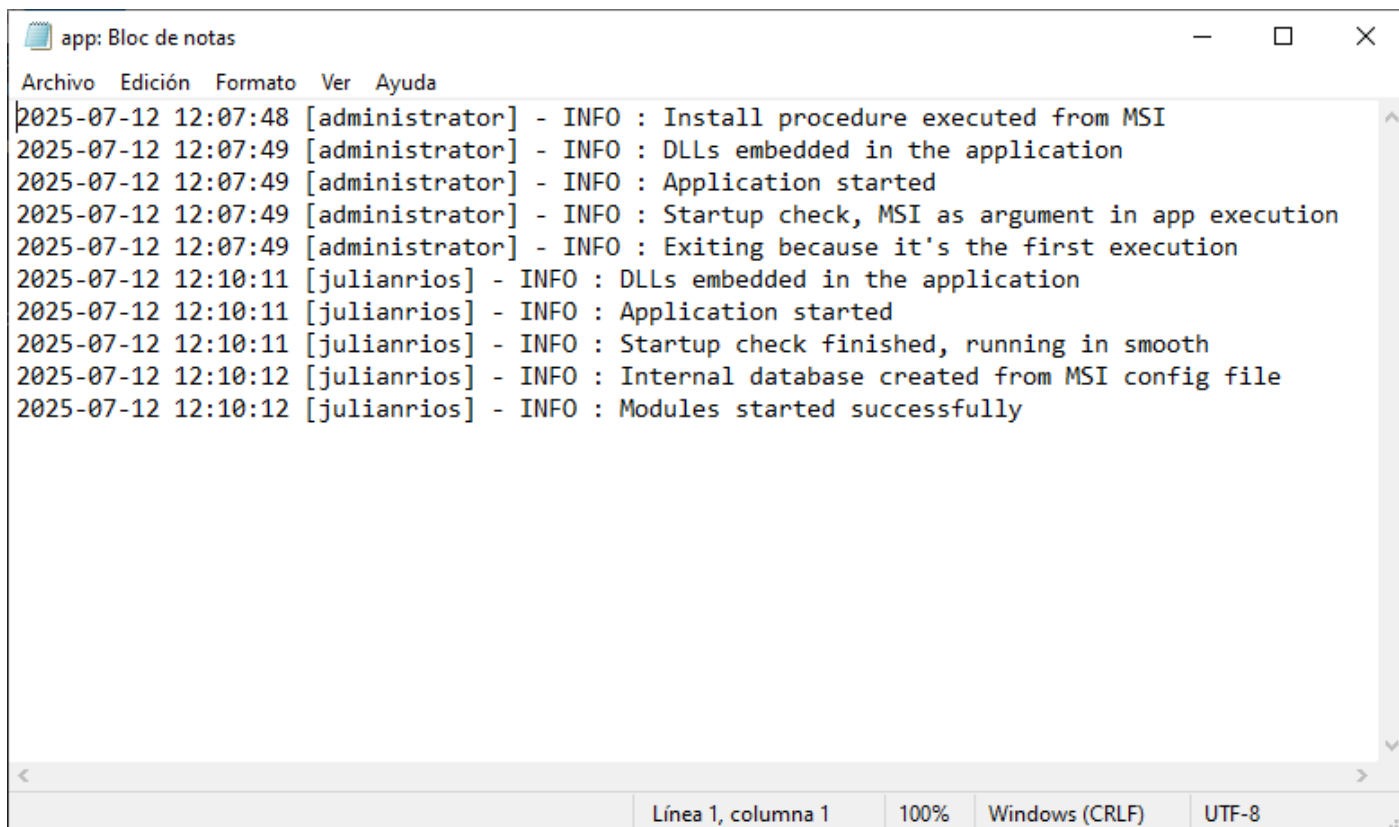
```
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
```

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

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

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**.



```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
```

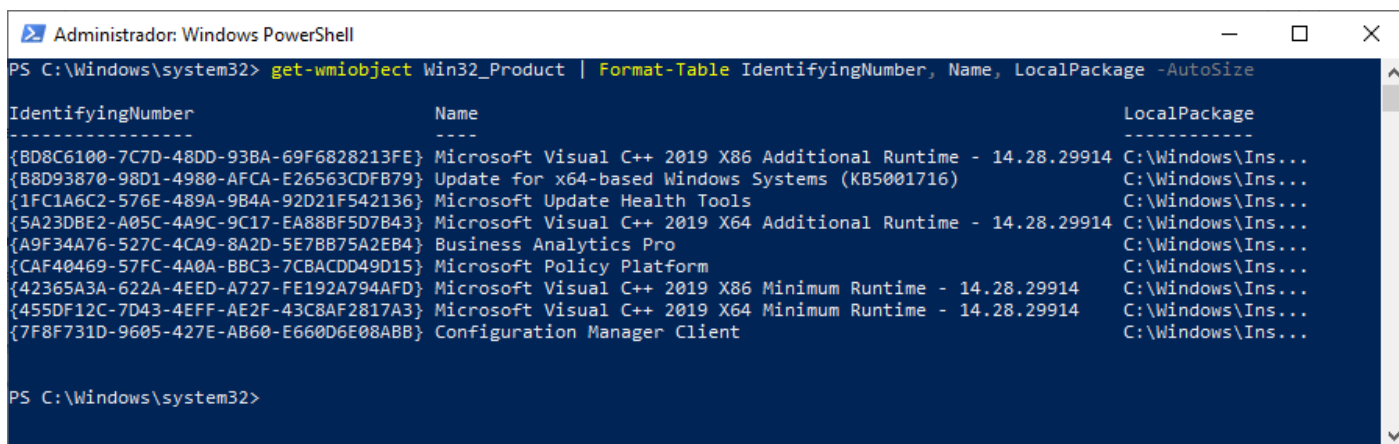
En este archivo de log se encontrará toda información relevante de inicio, parada, actualización, desinstalación e incluso errores que pueda presentar el agente durante su ejecución.

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

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
```



```
Administrador: Windows PowerShell
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Business Analytics Pro C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Ins...

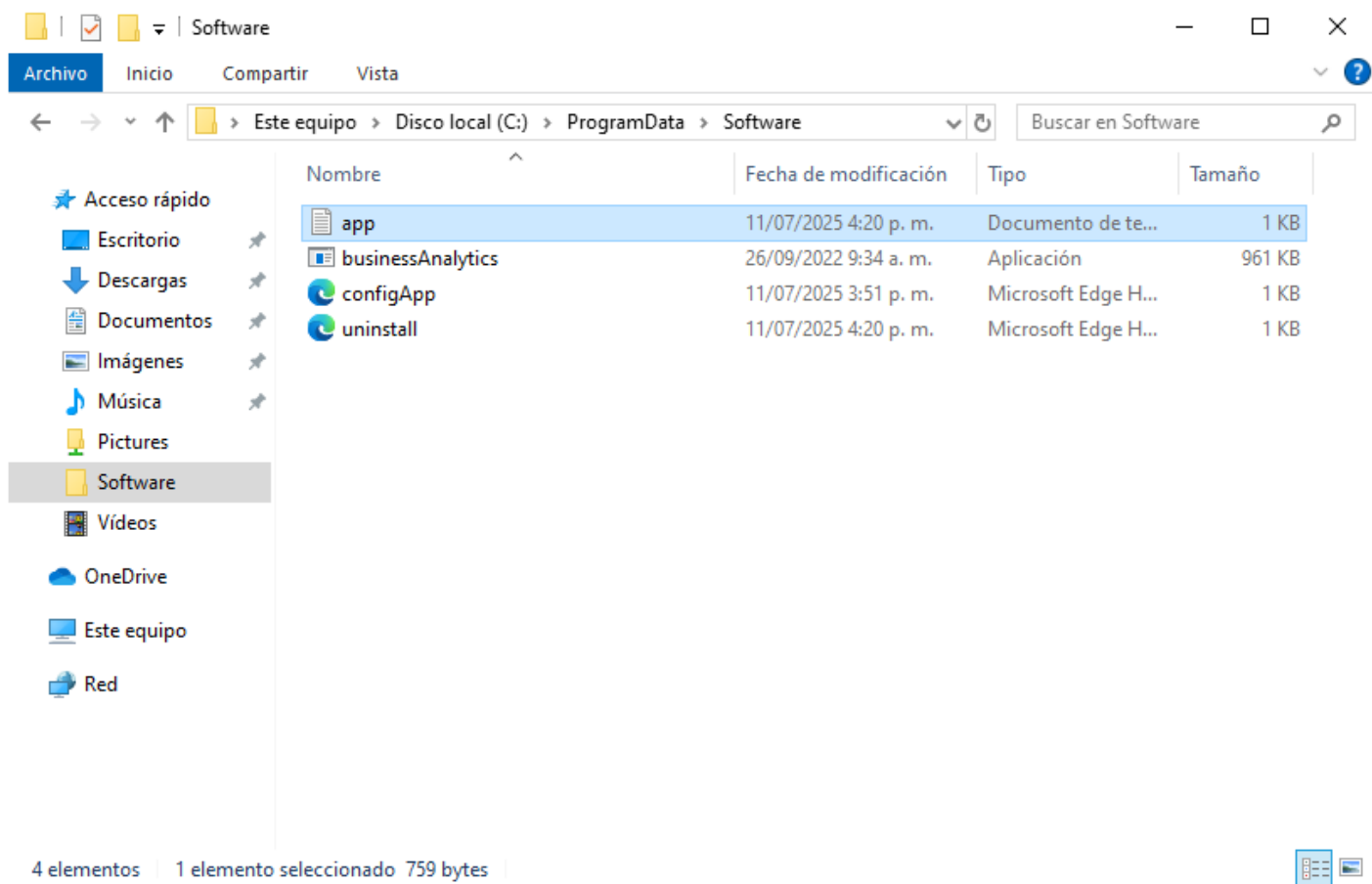
PS C:\Windows\system32>
```

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.

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

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**.

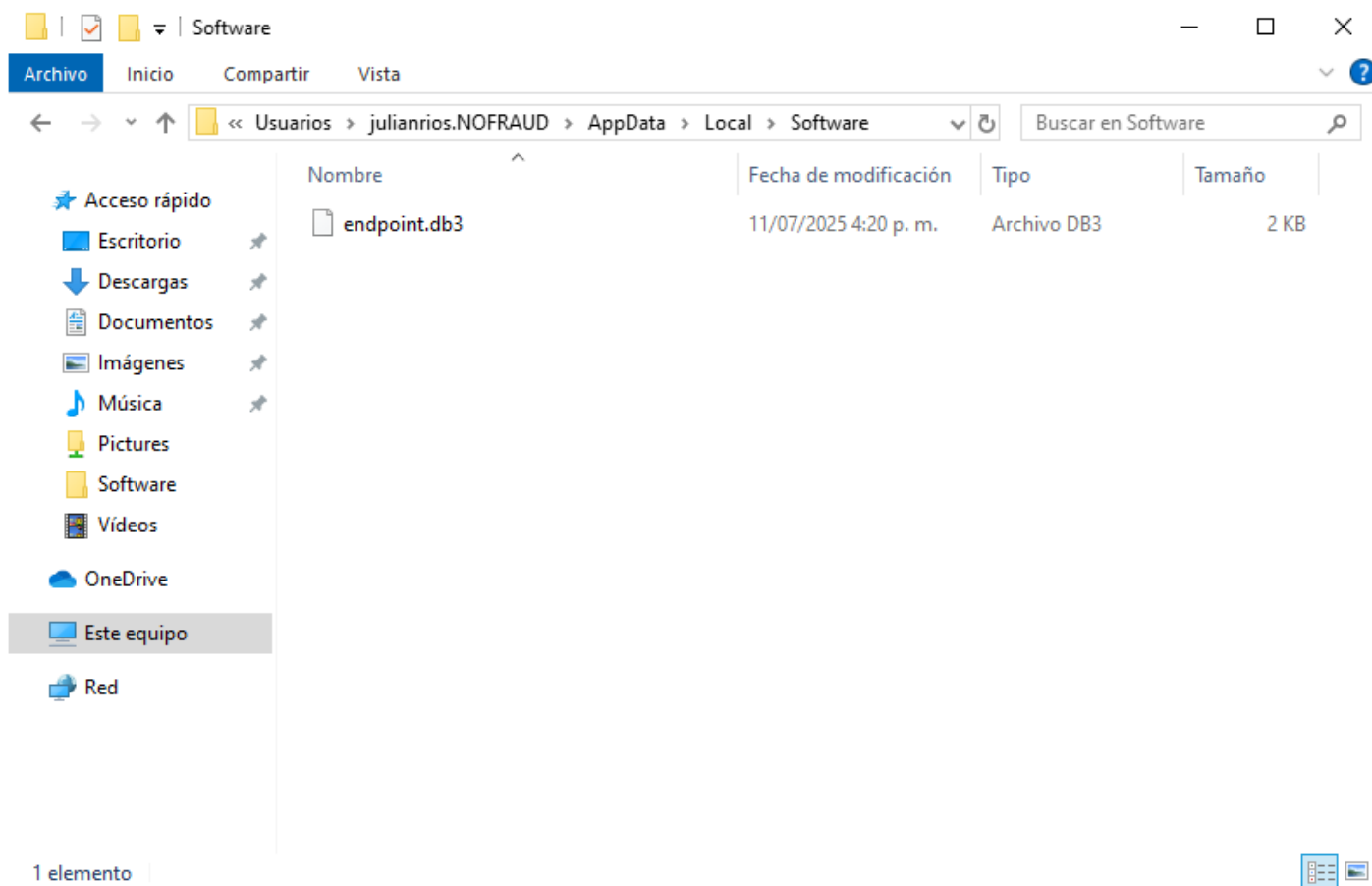


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

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.

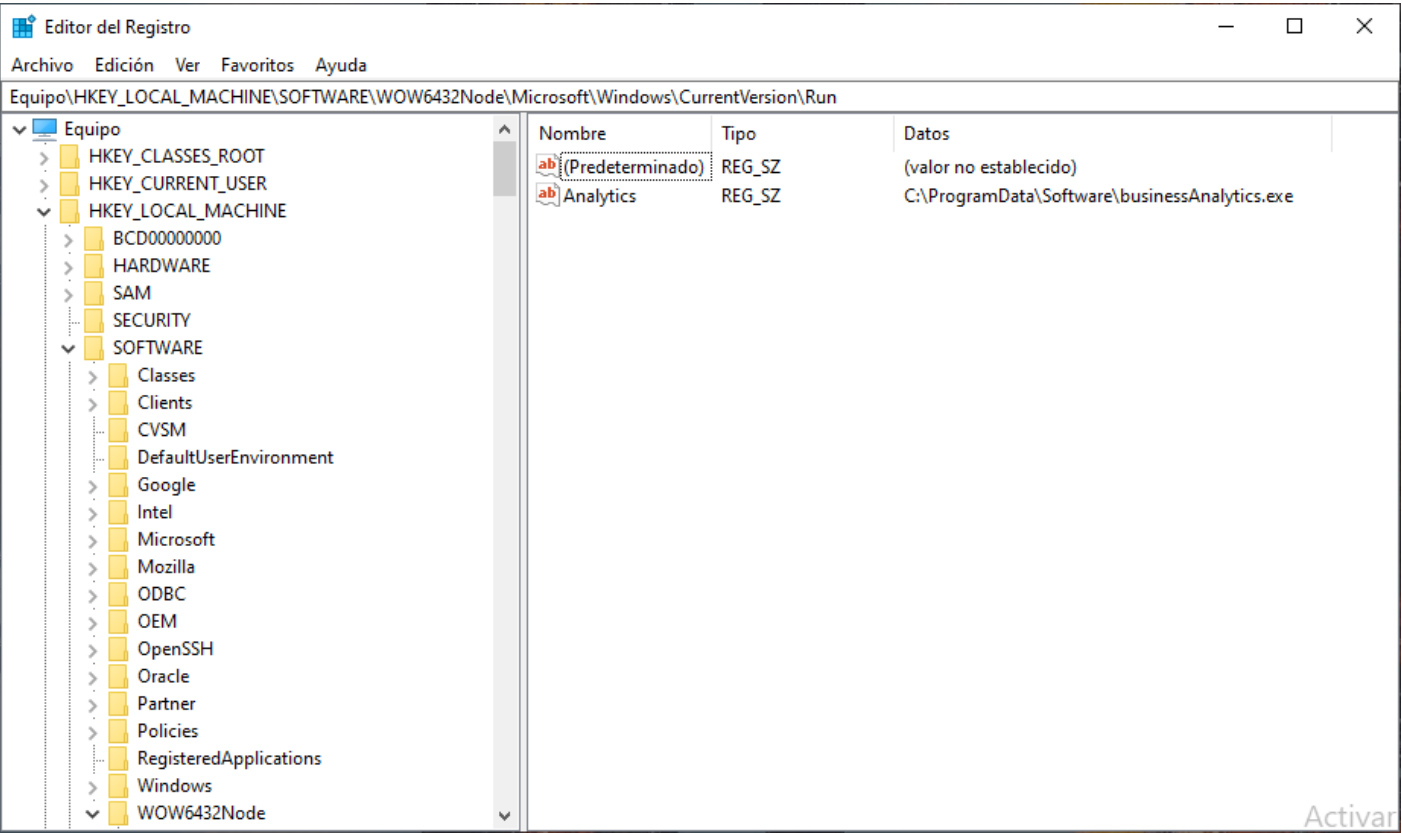


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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.**

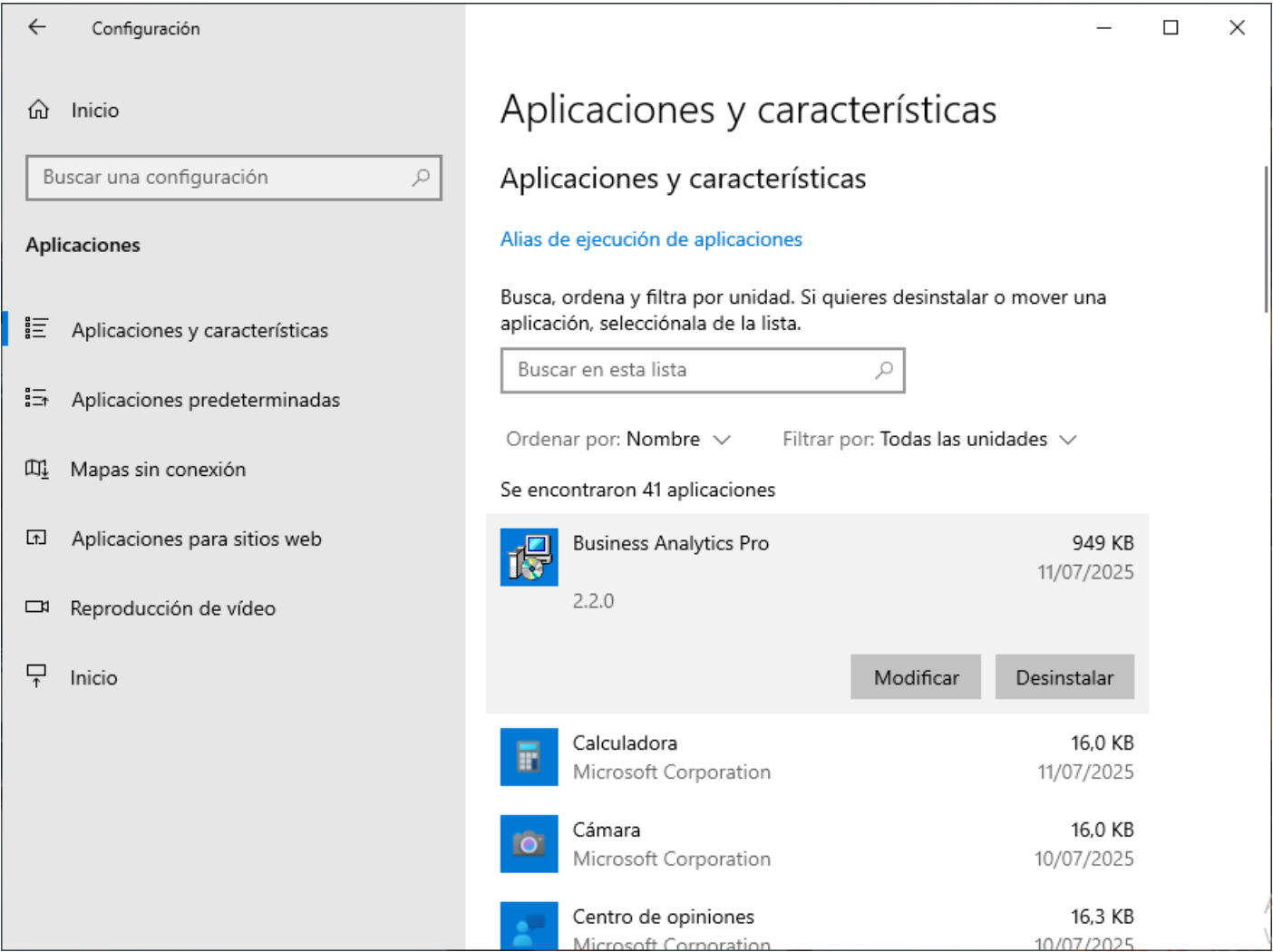


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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 reemplaza 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**.

Administrador de tareas

ArchivOpcionesVista

ProcesosRendimientoHistorial de aplicacionesInicioUsuariosDetallesServicios

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00	11.392 K	
conhost.exe	3768	En ejecución	Administr...	00	4.844 K	No permitida
csrss.exe	552	En ejecución		00	560 K	
csrss.exe	648	En ejecución		00	716 K	
ctfmon.exe	5708	En ejecución	julianrios	00	2.480 K	Deshabilitada
dllhost.exe	4288	En ejecución		00	776 K	
dllhost.exe	7164	En ejecución	julianrios	00	1.908 K	Deshabilitada
dwm.exe	1668	En ejecución		00	43.148 K	
explorer.exe	5572	En ejecución	julianrios	00	75.828 K	Deshabilitada
explorer.exe	5960	En ejecución	julianrios	00	6.132 K	Deshabilitada
FileCoAuth.exe	1792	En ejecución	julianrios	00	28 K	Deshabilitada
fontdrvhost.exe	940	En ejecución		00	76 K	
fontdrvhost.exe	948	En ejecución		00	972 K	
Interrupciones del si...	-	En ejecución	SYSTEM	00	0 K	

Menos detalles

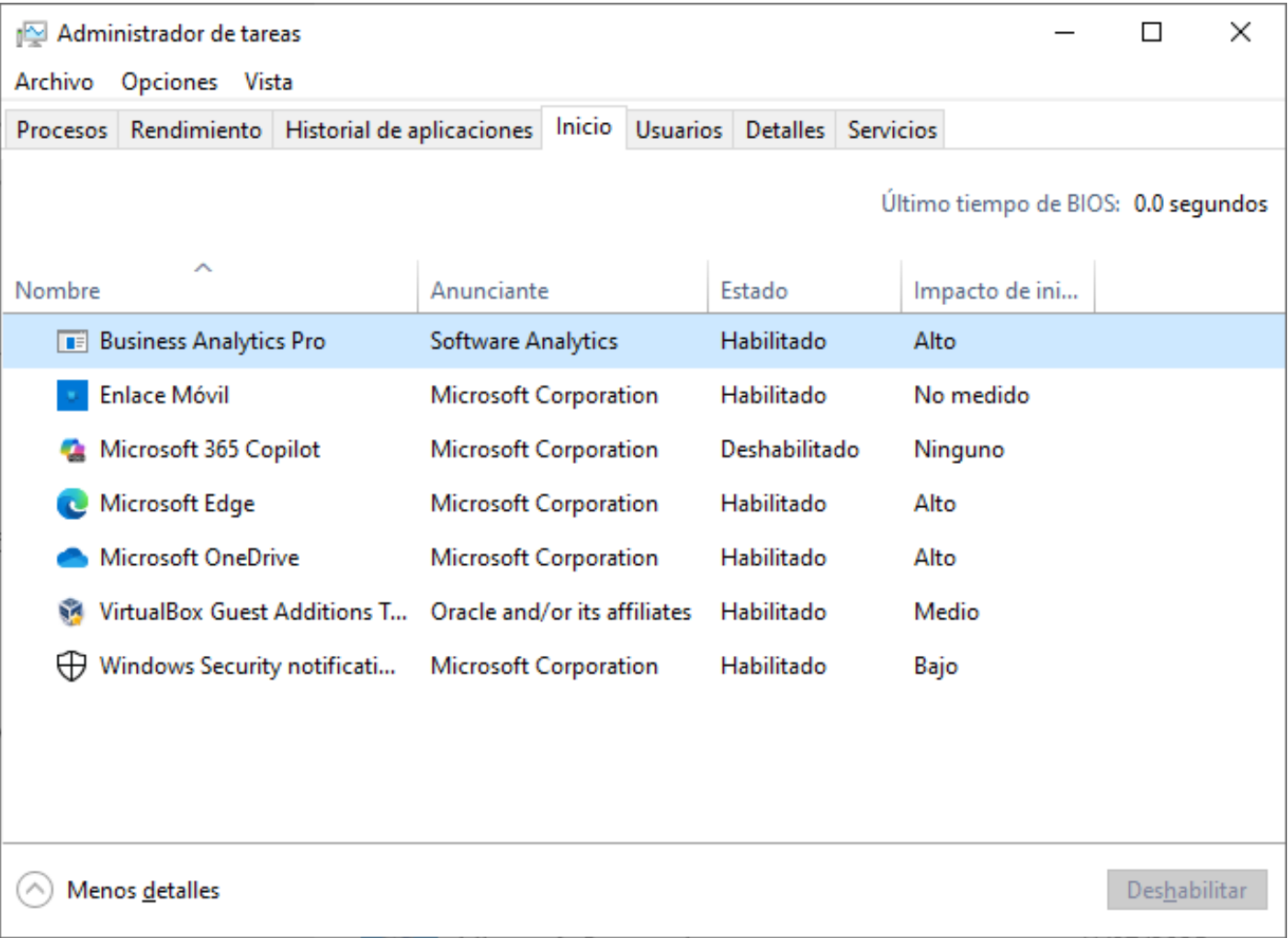
Finalizar tarea

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.

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

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**.



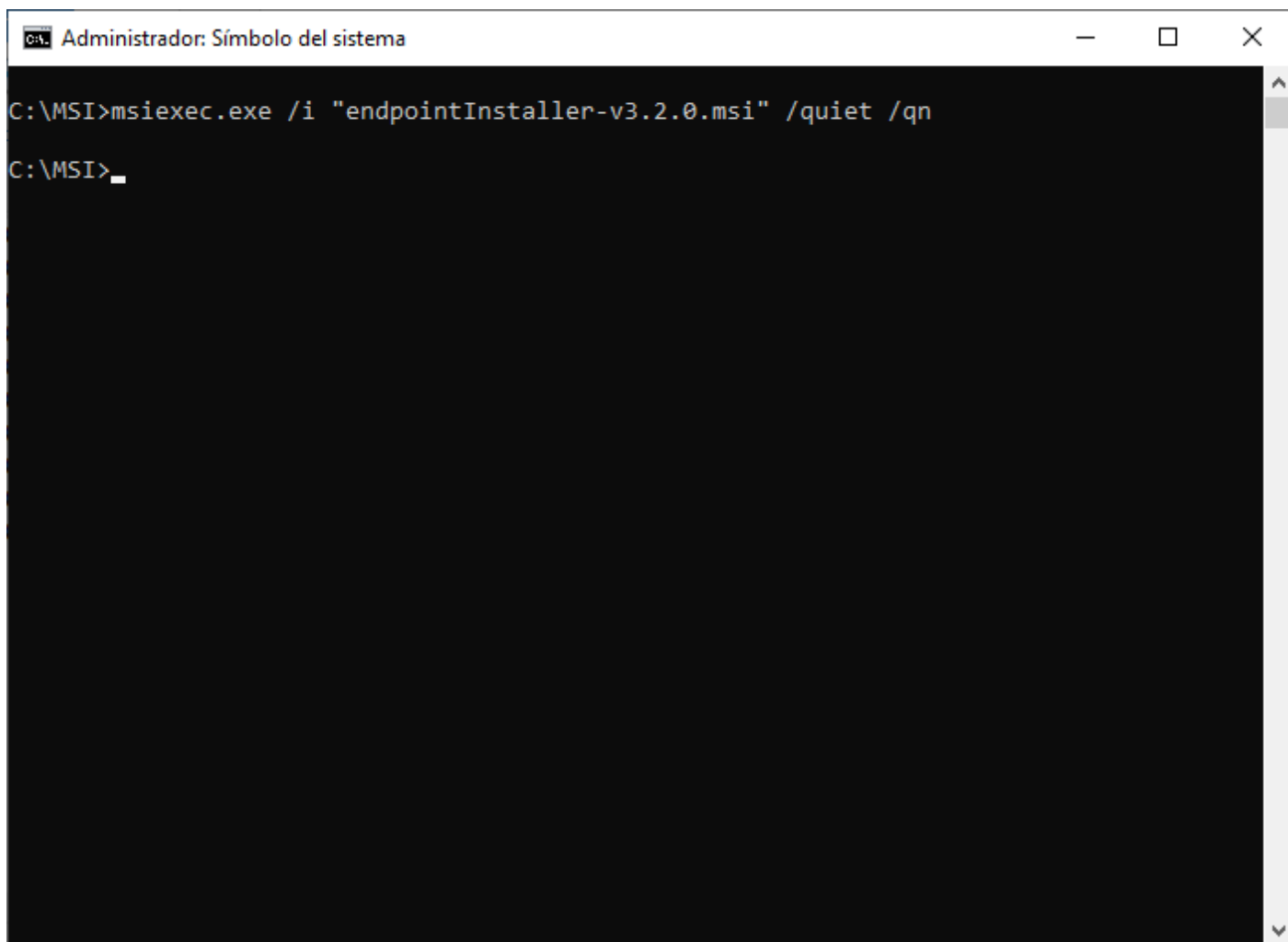
En esta ventana se muestran todas las aplicaciones que arrancan cuando el usuario inicia sesión con su cuenta en Windows. El agente de The Fraud Explorer no arranca como servicio y no interfiere en el proceso de arranque de sistema operativo.

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.

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

Actualización del agente

Para actualizar el agente deberá abrir una consola de **MS-DOS** en modo **administrador** y ejecutar exactamente el mismo comando que se usó para instalarlo, con la diferencia que acá deberá especificar el MSI de la nueva versión del agente.



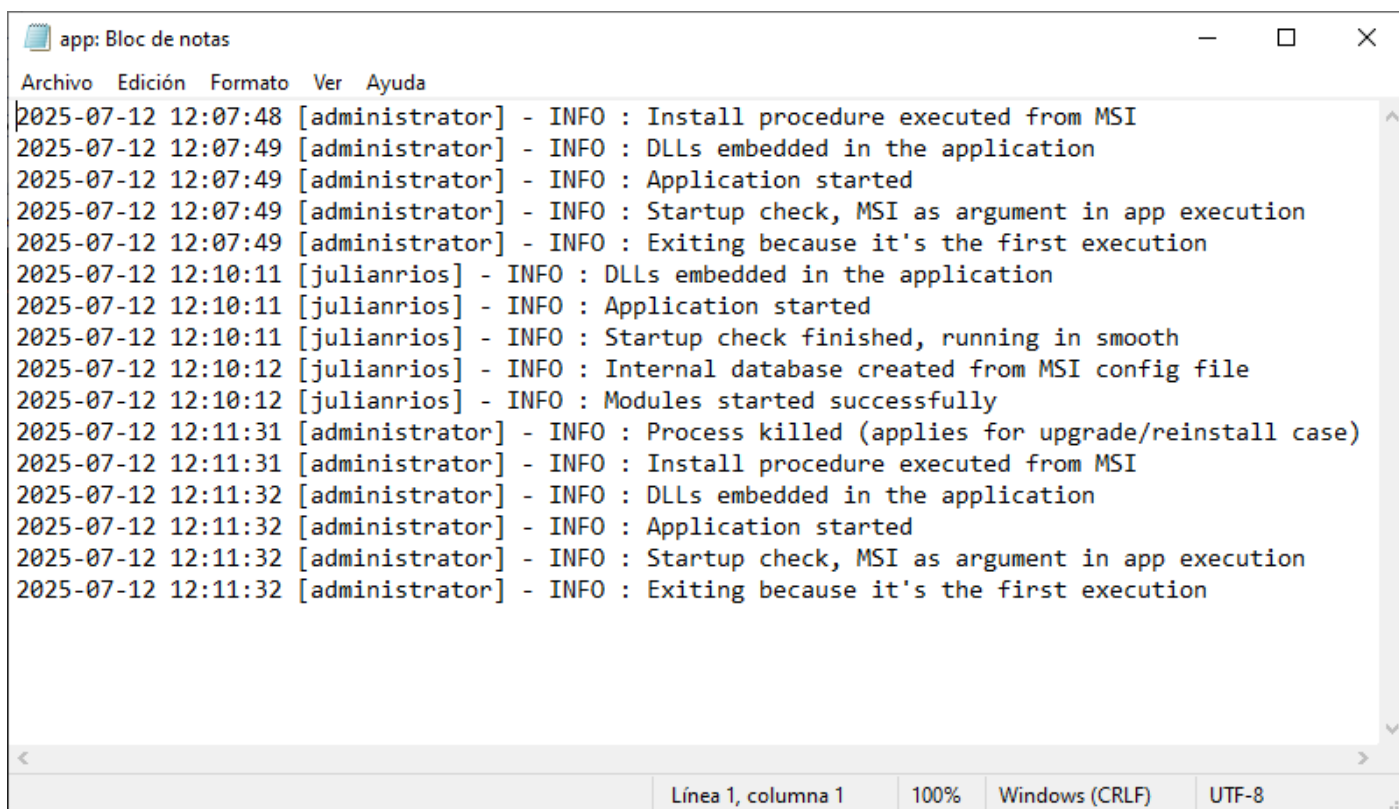
```
C:\MSI>msiexec.exe /i "endpointInstaller-v3.2.0.msi" /quiet /qn
C:\MSI>
```

Internamente el MSI busca versiones anteriores del mismo agente, lo reemplaza y copia los nuevos archivos a la carpeta **C:\ProgramData\Software** donde normalmente se almacenan.

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

Verificación de la actualización

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



```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
2025-07-12 12:11:31 [administrator] - INFO : Process killed (applies for upgrade/reinstall case)
2025-07-12 12:11:31 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:11:32 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:11:32 [administrator] - INFO : Application started
2025-07-12 12:11:32 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:11:32 [administrator] - INFO : Exiting because it's the first execution
Línea 1, columna 1 100% Windows (CRLF) UTF-8
```

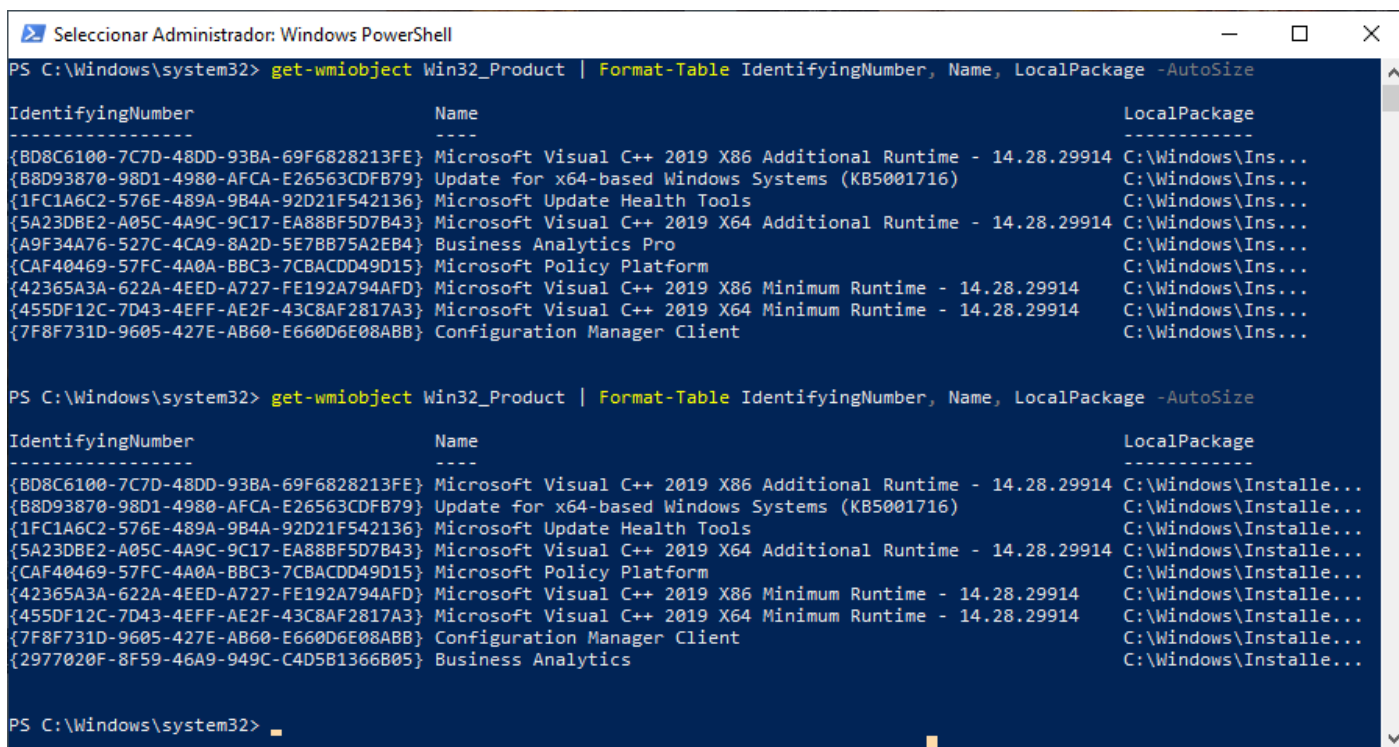
Se puede comprobar que se actualizó por la presencia de la entrada **Process killed (applies for upgrade/reinstall case)**.

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

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
```



```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05}	Business Analytics	C:\Windows\Installe...

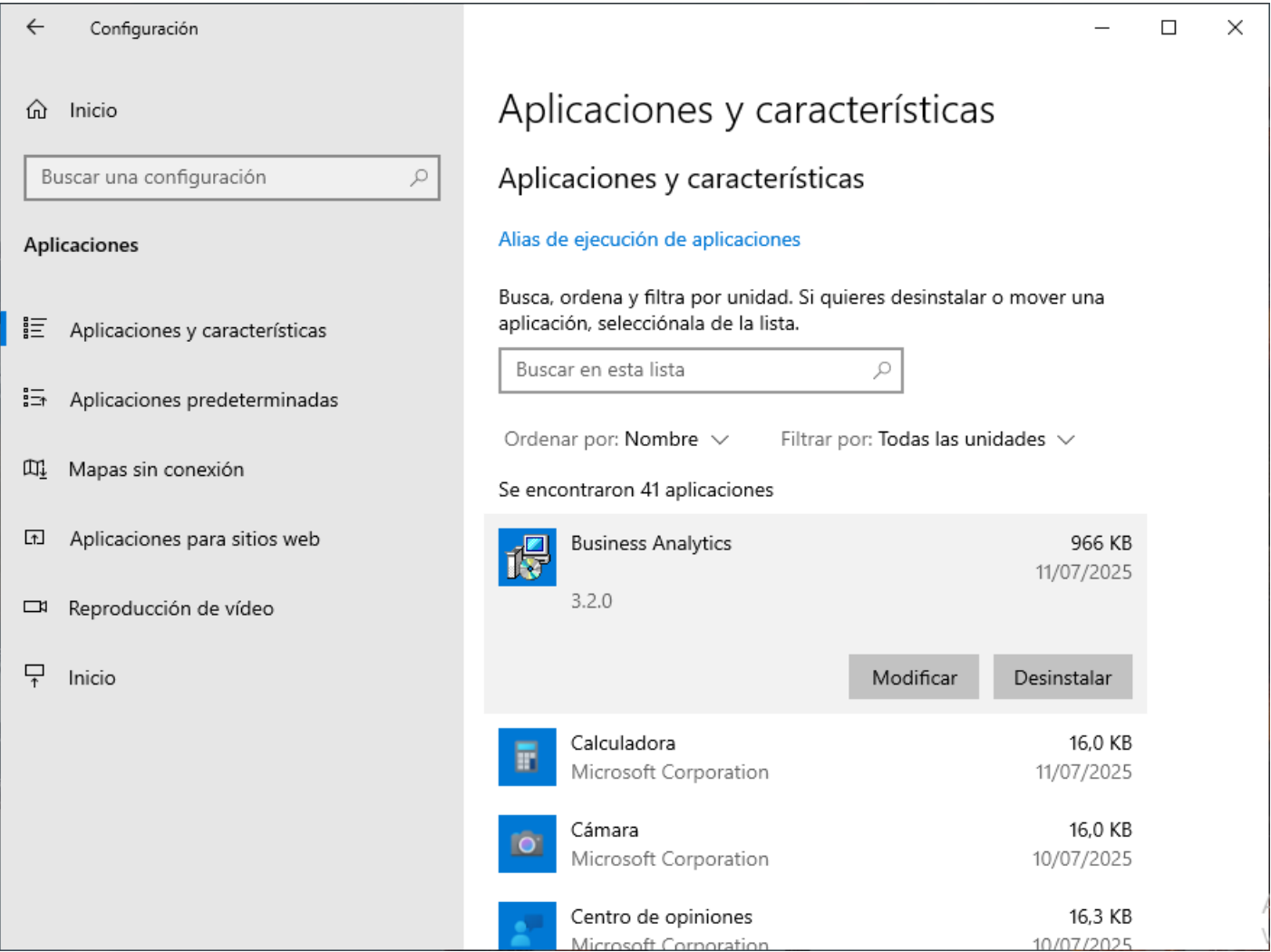
```
PS C:\Windows\system32>
```

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

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

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.



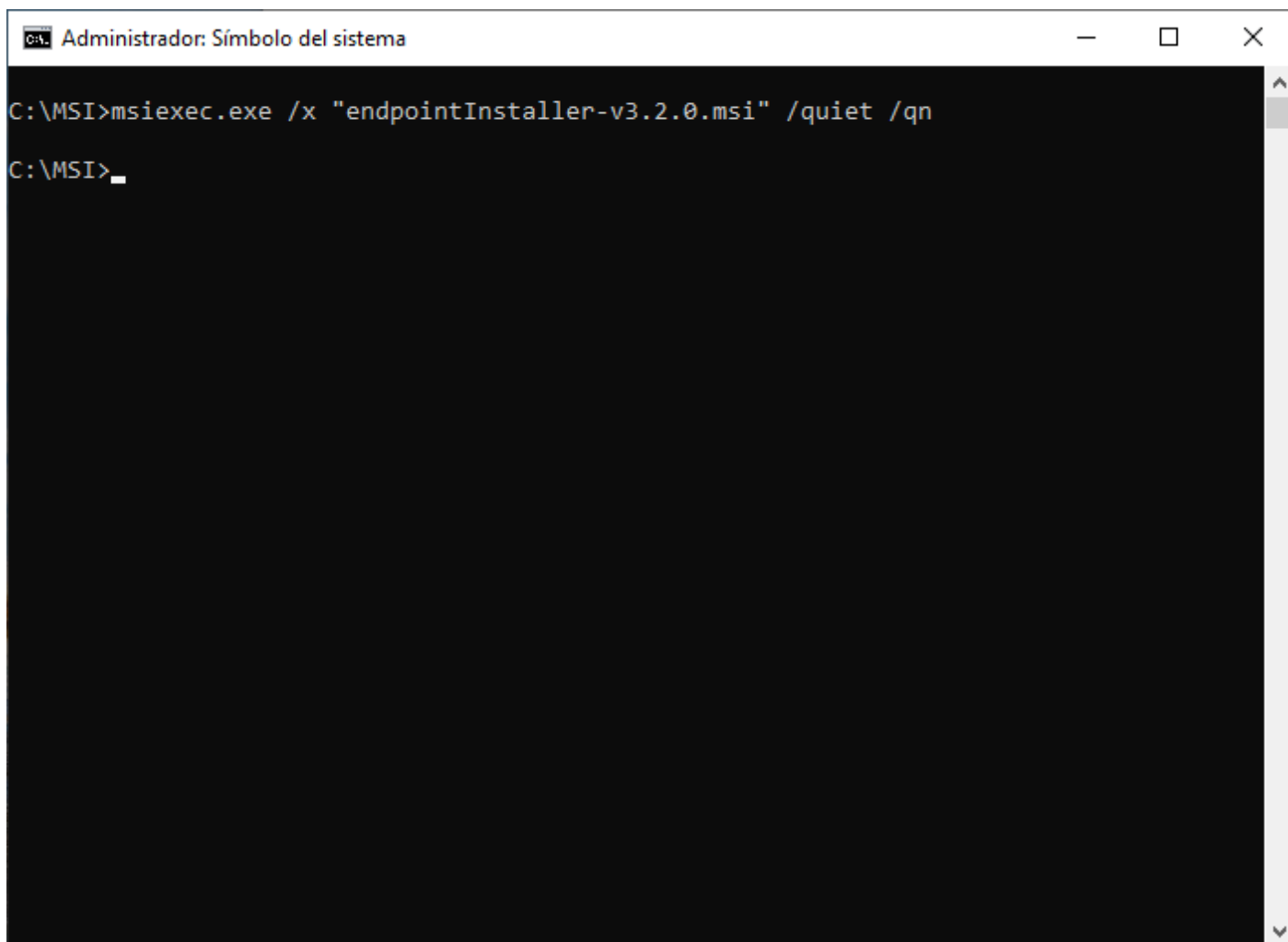
Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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

Desinstalación del agente

En una consola **MS-DOS** en modo **administrador** deberá ejecutar el comando:

```
msiexec.exe /x "endpointInstaller-v3.2.0.msi" /quiet /qn
```

A screenshot of a Windows command prompt window. The title bar at the top reads "Administrador: Símbolo del sistema". The window has standard Windows window controls (minimize, maximize, close) on the right. The command prompt shows the directory "C:\MSI" and the command "msiexec.exe /x "endpointInstaller-v3.2.0.msi" /quiet /qn" has been entered and executed. The prompt now shows "C:\MSI>" with a cursor.

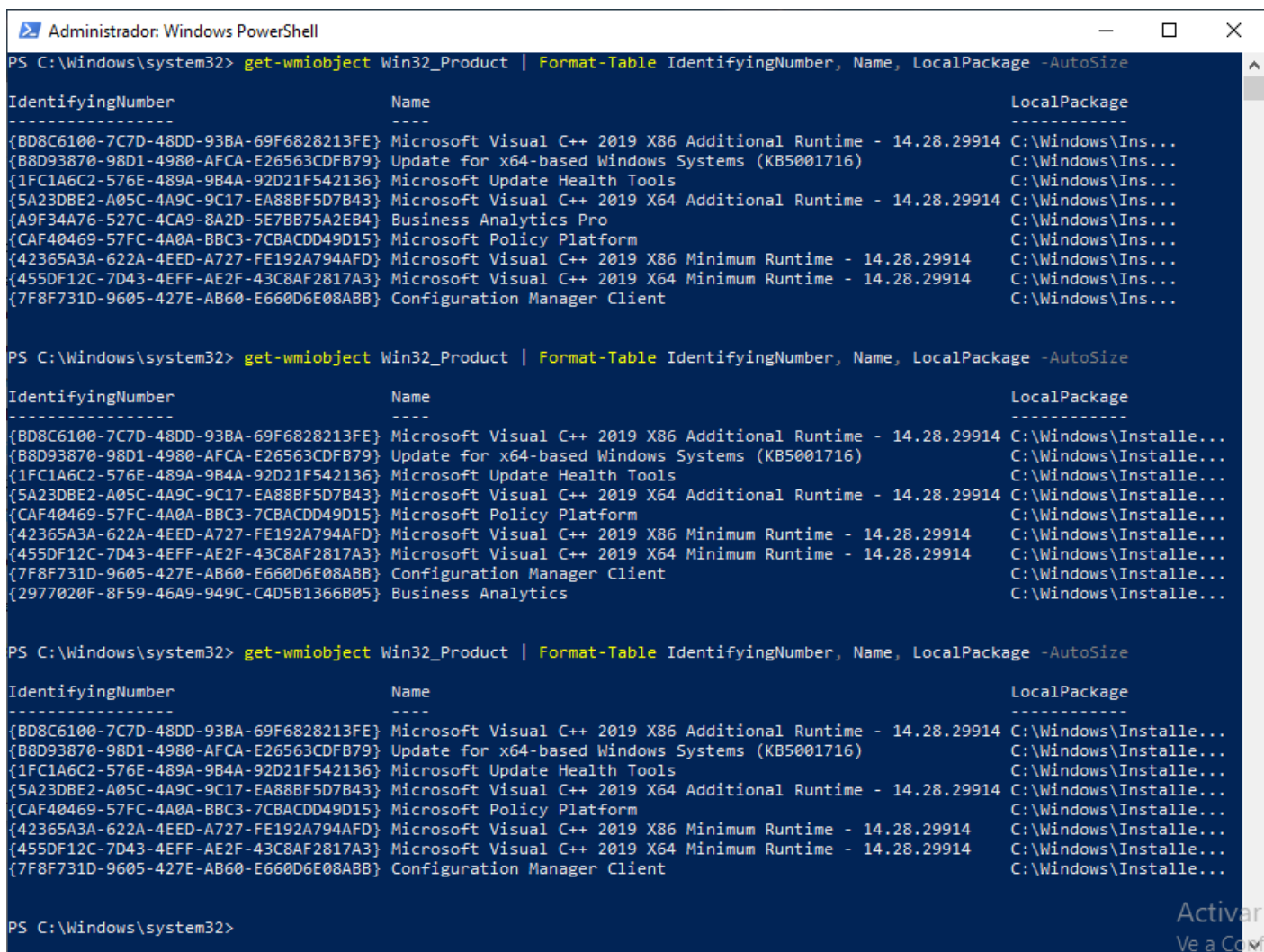
Este comando desinstalará el agente en modo silencioso, eliminando todos los archivos asociados al agente, incluyendo la base de datos y la entrada en el registro de Windows.

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

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
```



```
Administrador: Windows PowerShell
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Business Analytics Pro C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Ins...

PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05} Business Analytics C:\Windows\Installe...

PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Installe...

PS C:\Windows\system32>
```

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

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

Despliegue con GPO de Active Directory

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

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 organizada, 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.

Despliegue con GPO de Active Directory

Video con todos los pasos

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

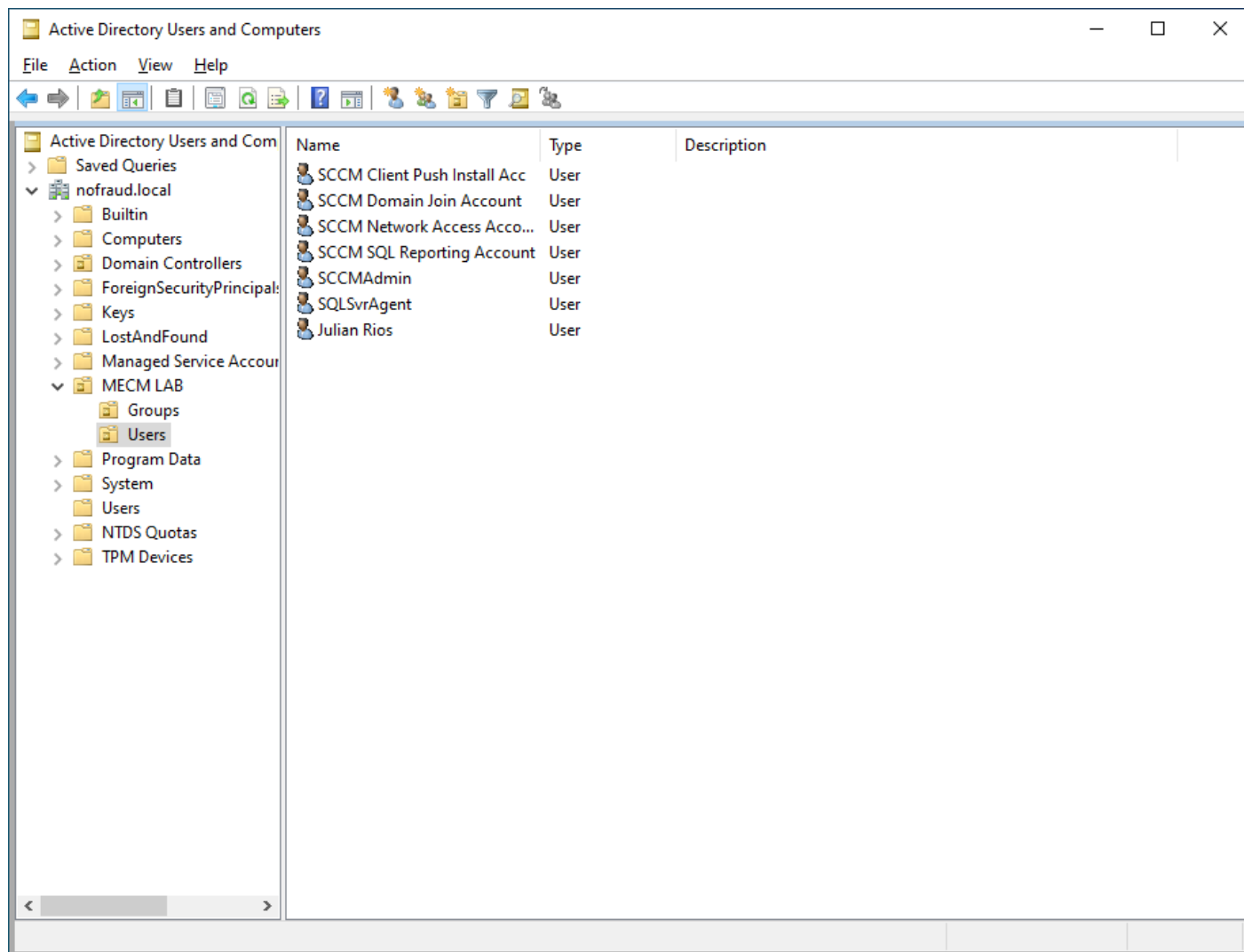
https://www.youtube.com/embed/3f_auPBiPk0?si=AD8aFwC9YYew5vg0

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.

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

Despliegue con GPO de Active Directory

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.

Business Analytics Group Properties?×

Object

General

Security


Members

Attribute Editor

Member Of

Managed By

Members:

Name	Active Directory Domain Services Folder
 Julian Rios	nofraud.local/MECM LAB/Users

Add...

Remove

OK

Cancel

Apply

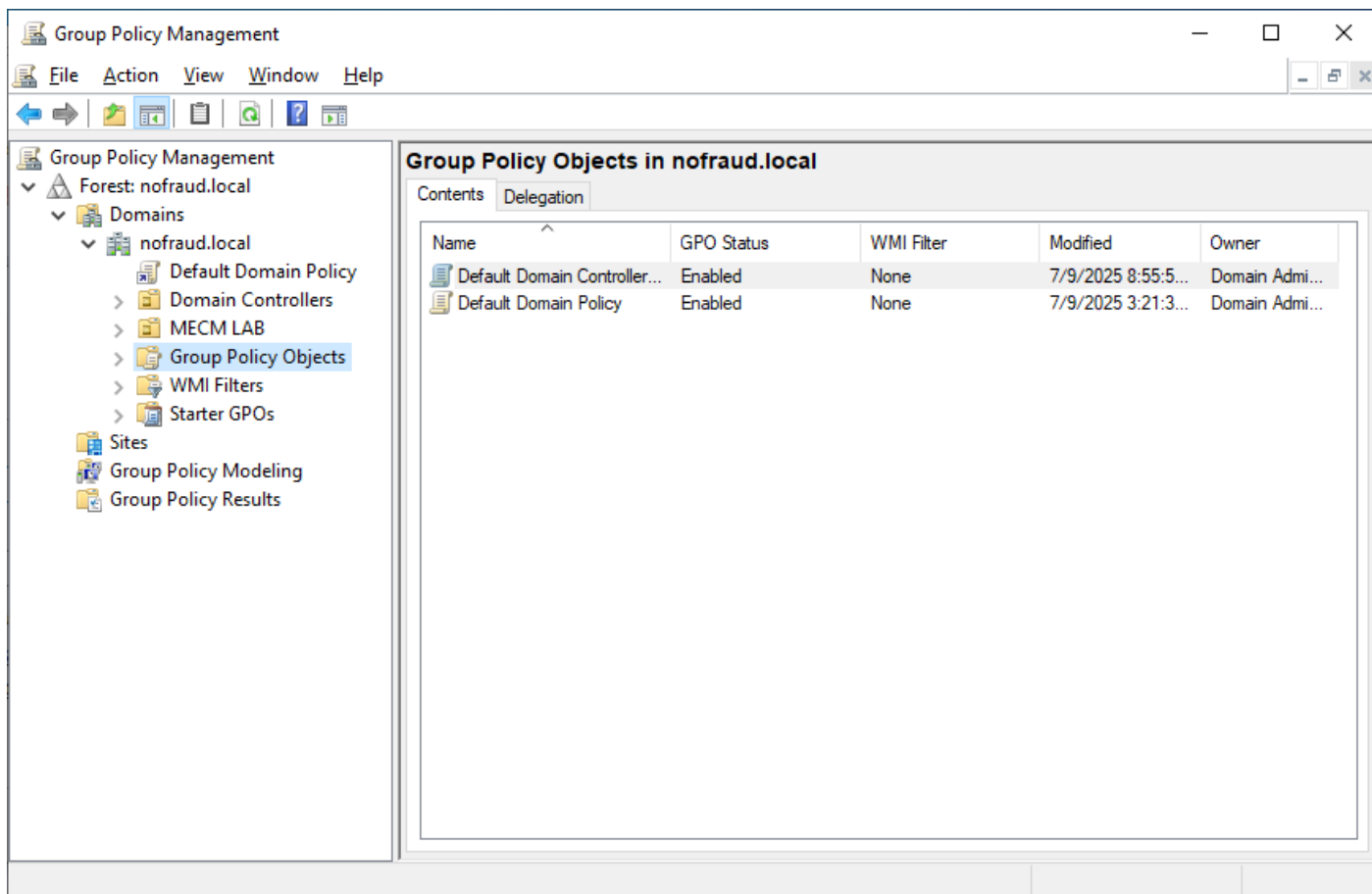
Help

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

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

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**.

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

Nombre de la política GPO

Escriba un nombre para la nueva política de GPO.

New GPO

X

Name:

Analytics Software

Source Starter GPO:

(none)

OK

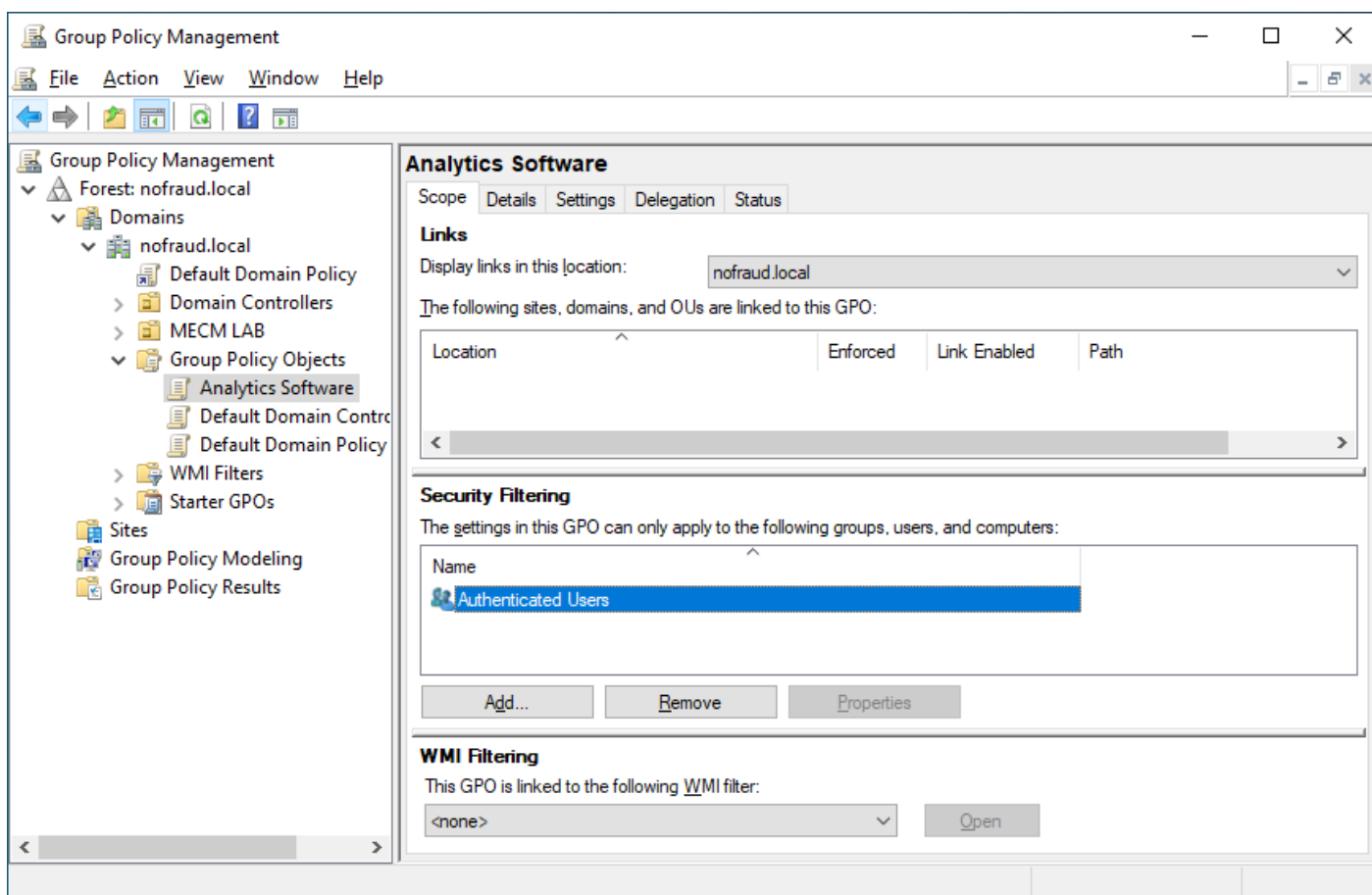
Cancel

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

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

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**.

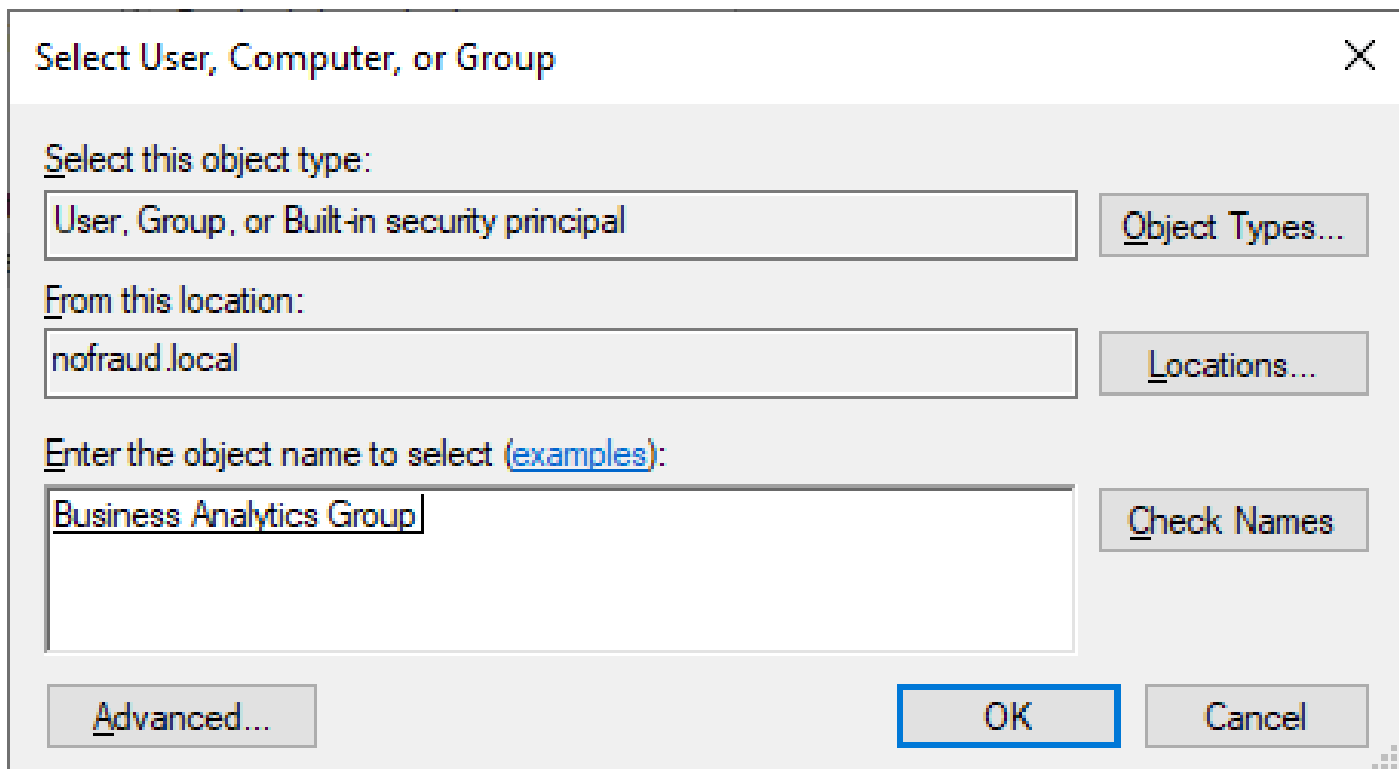


Esto eliminará el filtro por defecto para la aplicación de la política. Normalmente la política se aplica a todos los usuarios que se autenticquen en Windows, pero lo que se quiere es poder seleccionar usuarios y ponerlos en un grupo y solo a estos aplicarles la política.

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

Creación de un nuevo filtro

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



Select User, Computer, or Group

Select this object type:

User, Group, or Built-in security principal

Object Types...

From this location:

nofraud.local

Locations...

Enter the object name to select (examples):

Business Analytics Group

Check Names

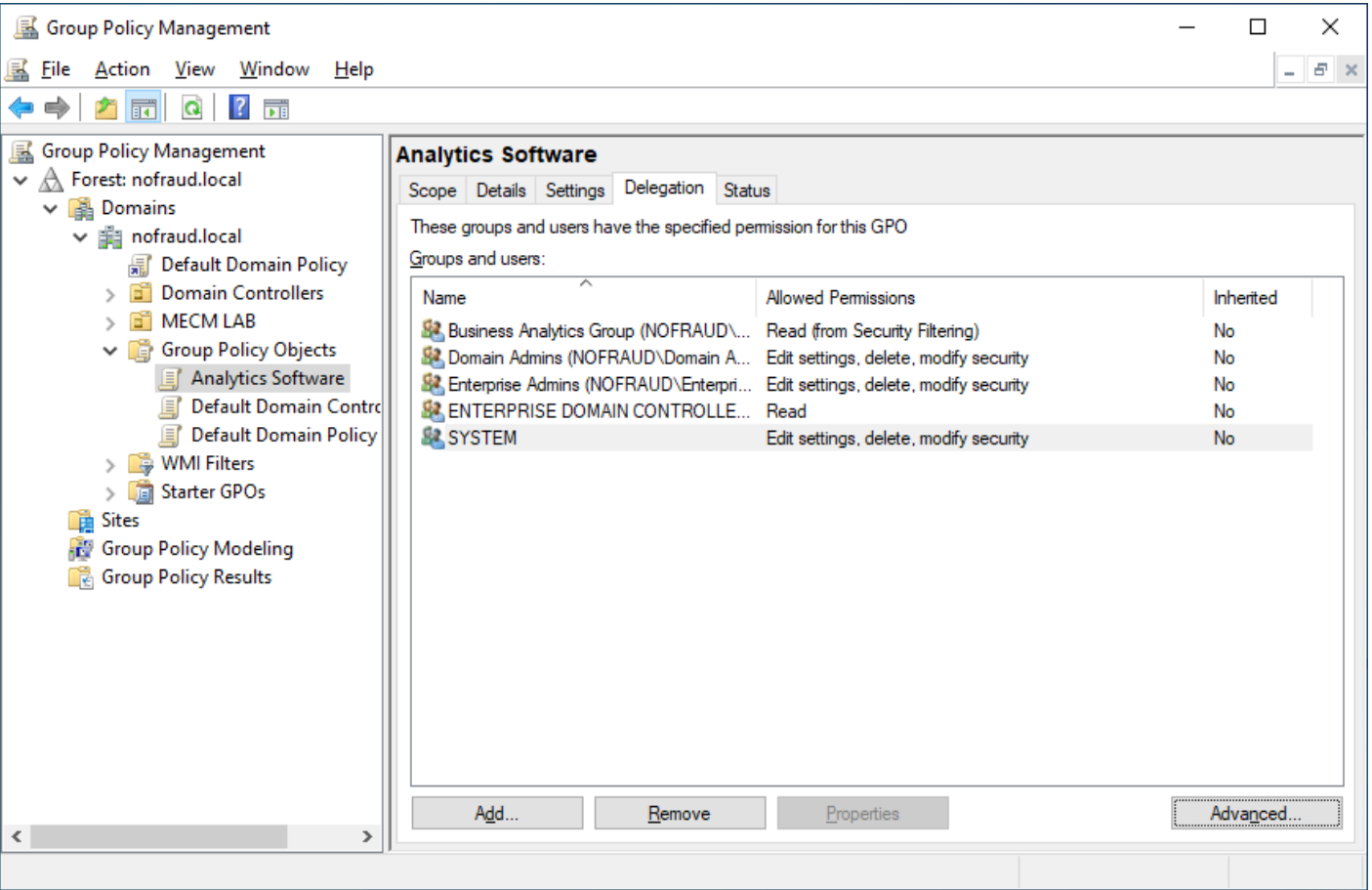
Advanced... OK Cancel

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.

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

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.

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

Despliegue con GPO de Active Directory

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.


Analytics Software Security Settings


X


Security

Group or user names:

 Business Analytics Group (NOFRAUD\Business Analytics G

 Domain Admins (NOFRAUD\Domain Admins)

 Enterprise Admins (NOFRAUD\Enterprise Admins)

 ENTERPRISE DOMAIN CONTROLLERS

<

>

Add...

Remove

Permissions for Business Analytics Group

	Allow	Deny	
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	^
Write	<input type="checkbox"/>	<input type="checkbox"/>	
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>	
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>	
Apply group policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	v

For special permissions or advanced settings, click Advanced.

Advanced

OK

Cancel

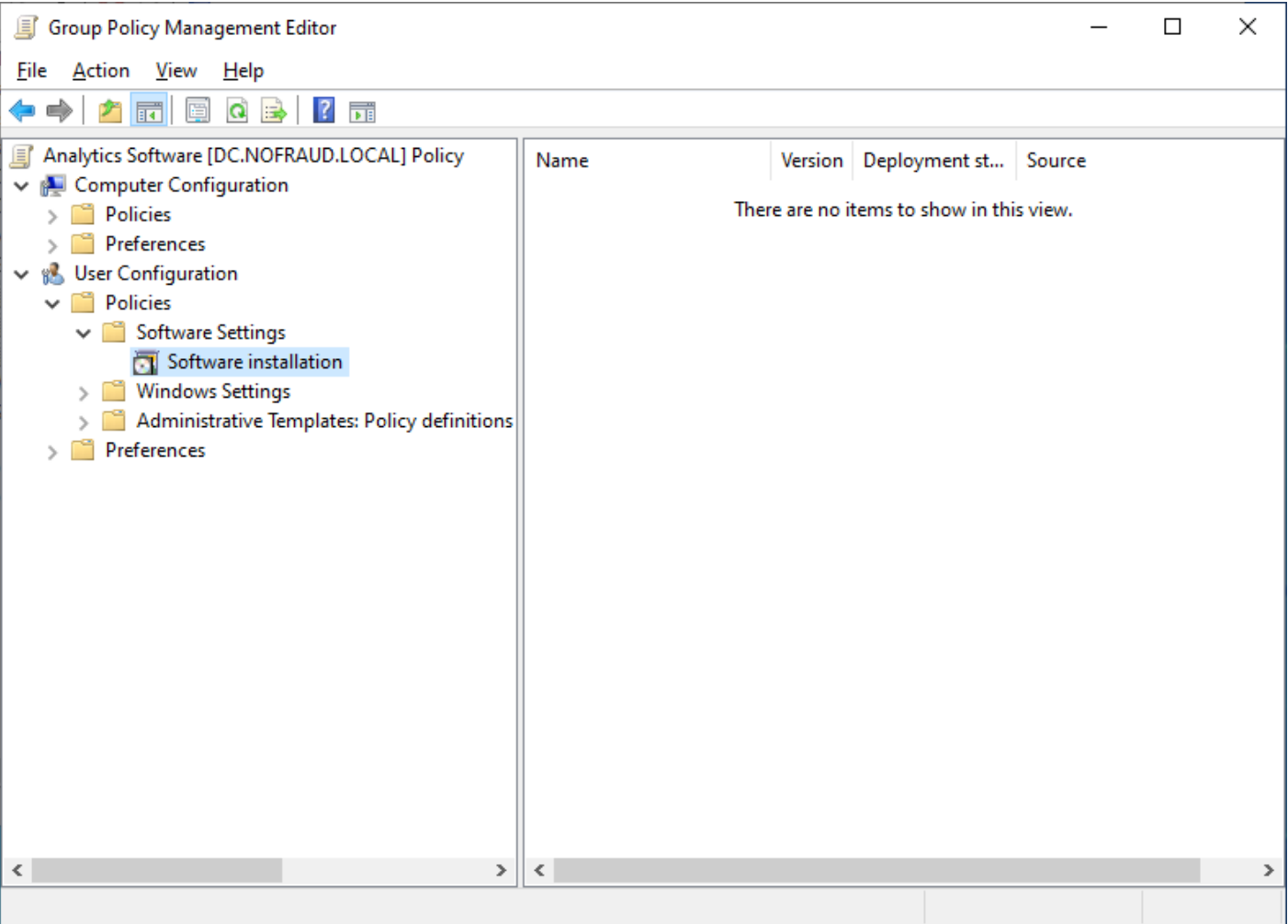
Apply

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 política

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

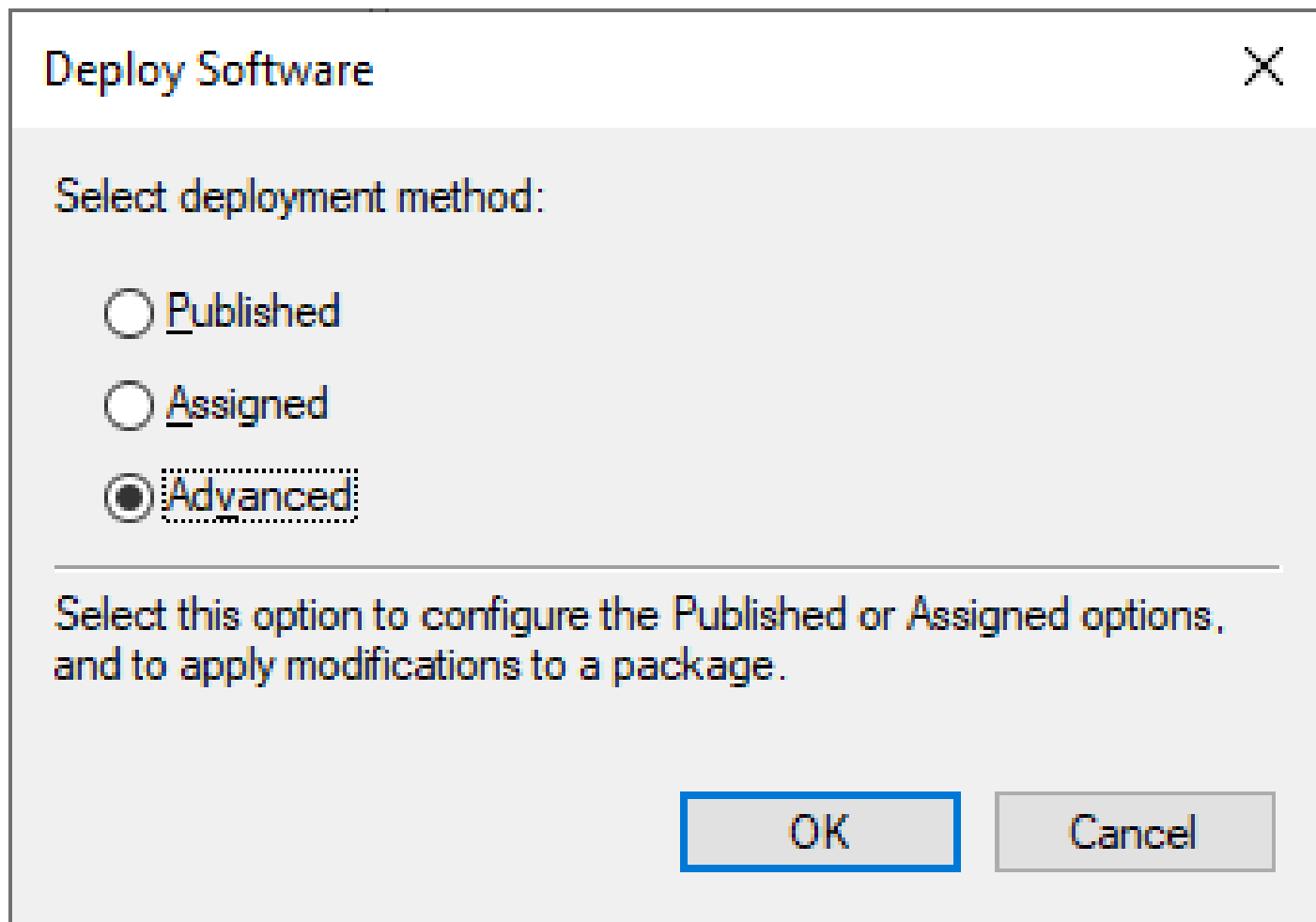


Aparecerá esta ventana donde deberá crear una entrada en **Software Installation** dando clic en **User Configuration, Policies, Software Setings, Software Installation, New** y cuando se le pregunte por el archivo MSI del agente, ubíquelo en la ruta de red, no en la ruta local del servidor.

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

Configuración avanzada

Seleccione que desea configurar el despliegue de manera avanzada.



Deploy Software

Select deployment method:

☐ Published

☐ Assigned

☒ Advanced

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

OK Cancel

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

Despliegue con GPO de Active Directory

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**.

Business Analytics Pro Properties

General Deployment Upgrades Categories Modifications Security

Deployment type

☐ Published

☒ Assigned

Deployment options

☒ Auto-install this application by file extension activation

☒ Uninstall this application when it falls out of the scope of management

☐ Do not display this package in the Add/Remove Programs control panel

☒ Install this application at logon

Installation user interface options

☐ Basic

☒ Maximum

Advanced...

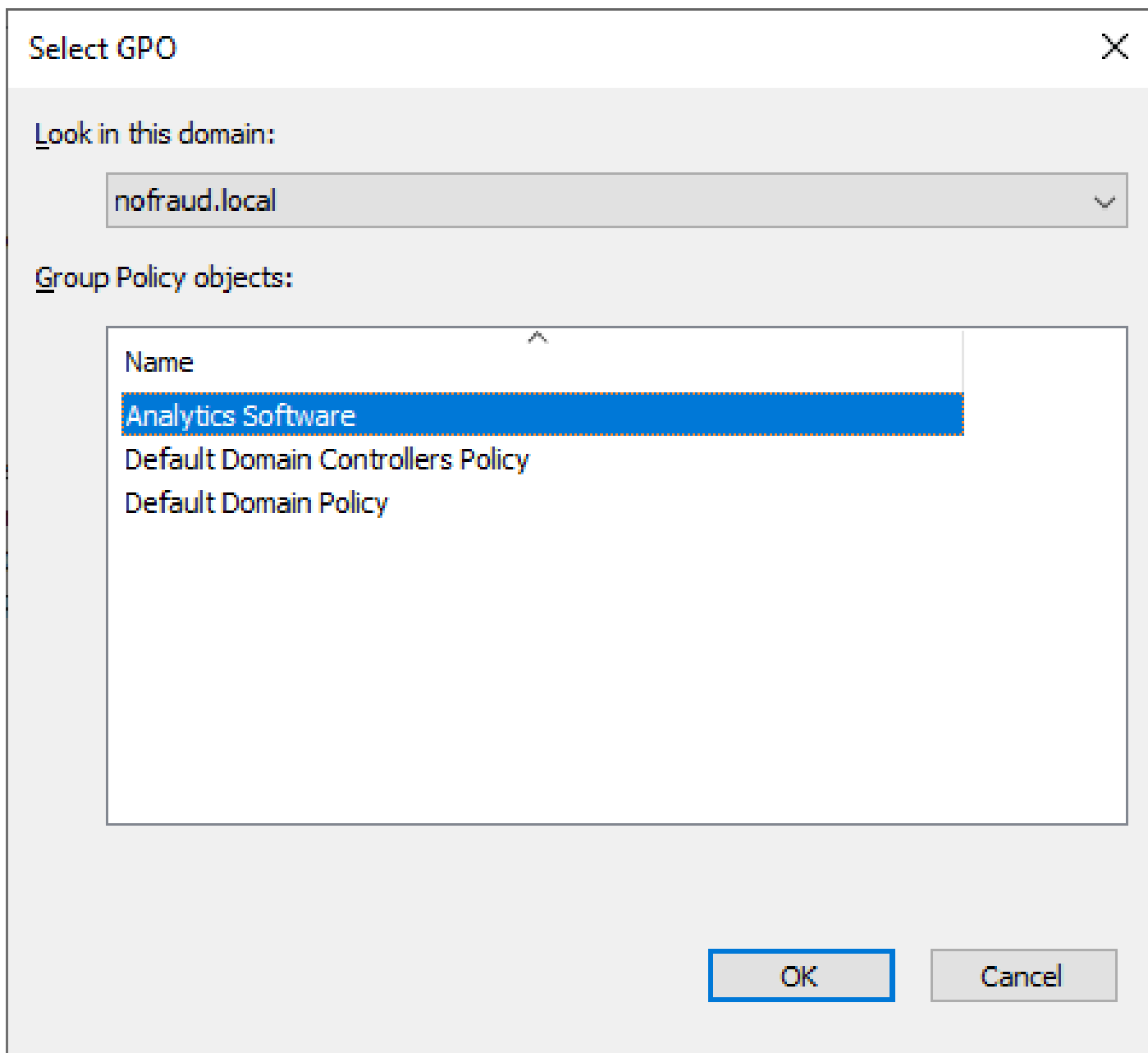
OK Cancel

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

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

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.

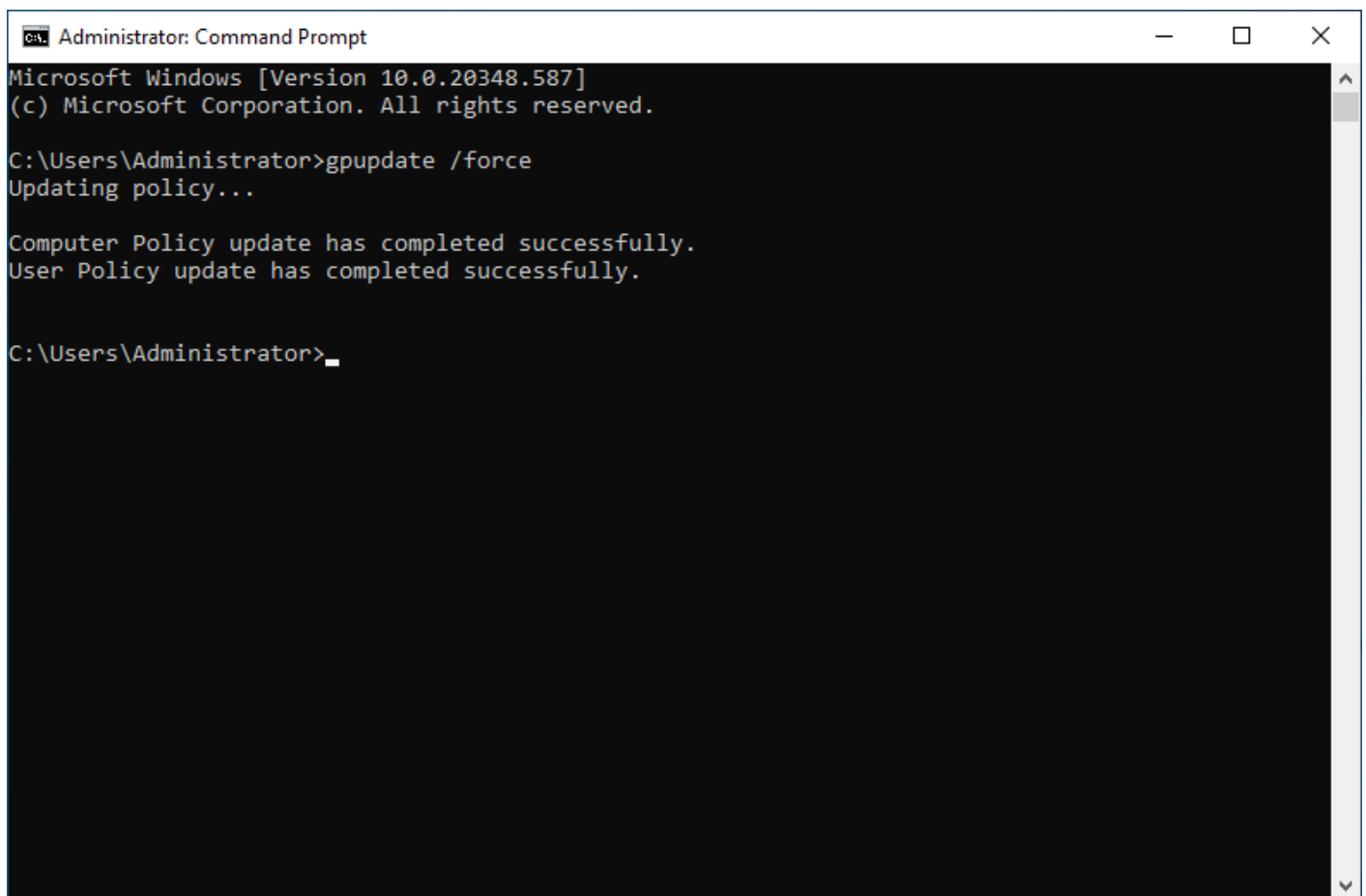
The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Despliegue con GPO de Active Directory

Aplicar la política con gpupdate

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

```
gpupdate /force
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

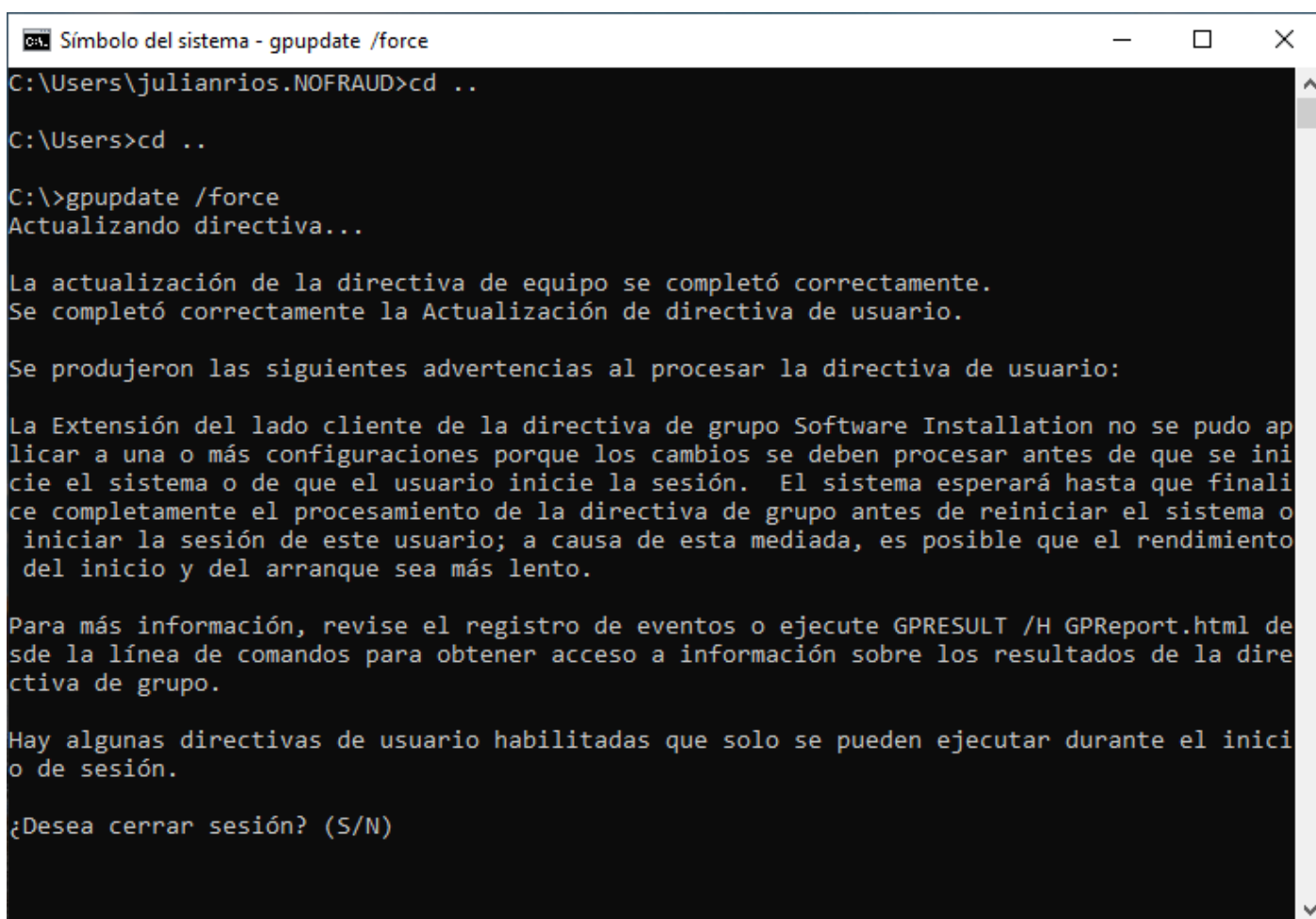
Este comando forzará la aplicación de la política desde el servidor Windows.

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

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
```



```
Símbolo del sistema - gpupdate /force
C:\Users\julianrios.NOFRAUD>cd ..
C:\Users>cd ..
C:\>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

Se produjeron las siguientes advertencias al procesar la directiva de usuario:

La Extensión del lado cliente de la directiva de grupo Software Installation no se pudo ap
licar a una o más configuraciones porque los cambios se deben procesar antes de que se ini
cie el sistema o de que el usuario inicie la sesión. El sistema esperará hasta que finali
ce completamente el procesamiento de la directiva de grupo antes de reiniciar el sistema o
iniciar la sesión de este usuario; a causa de esta mediada, es posible que el rendimiento
del inicio y del arranque sea más lento.

Para más información, revise el registro de eventos o ejecute GPRESULT /H GPREport.html de
sde la línea de comandos para obtener acceso a información sobre los resultados de la dire
ctiva de grupo.

Hay algunas directivas de usuario habilitadas que solo se pueden ejecutar durante el inici
o de sesión.

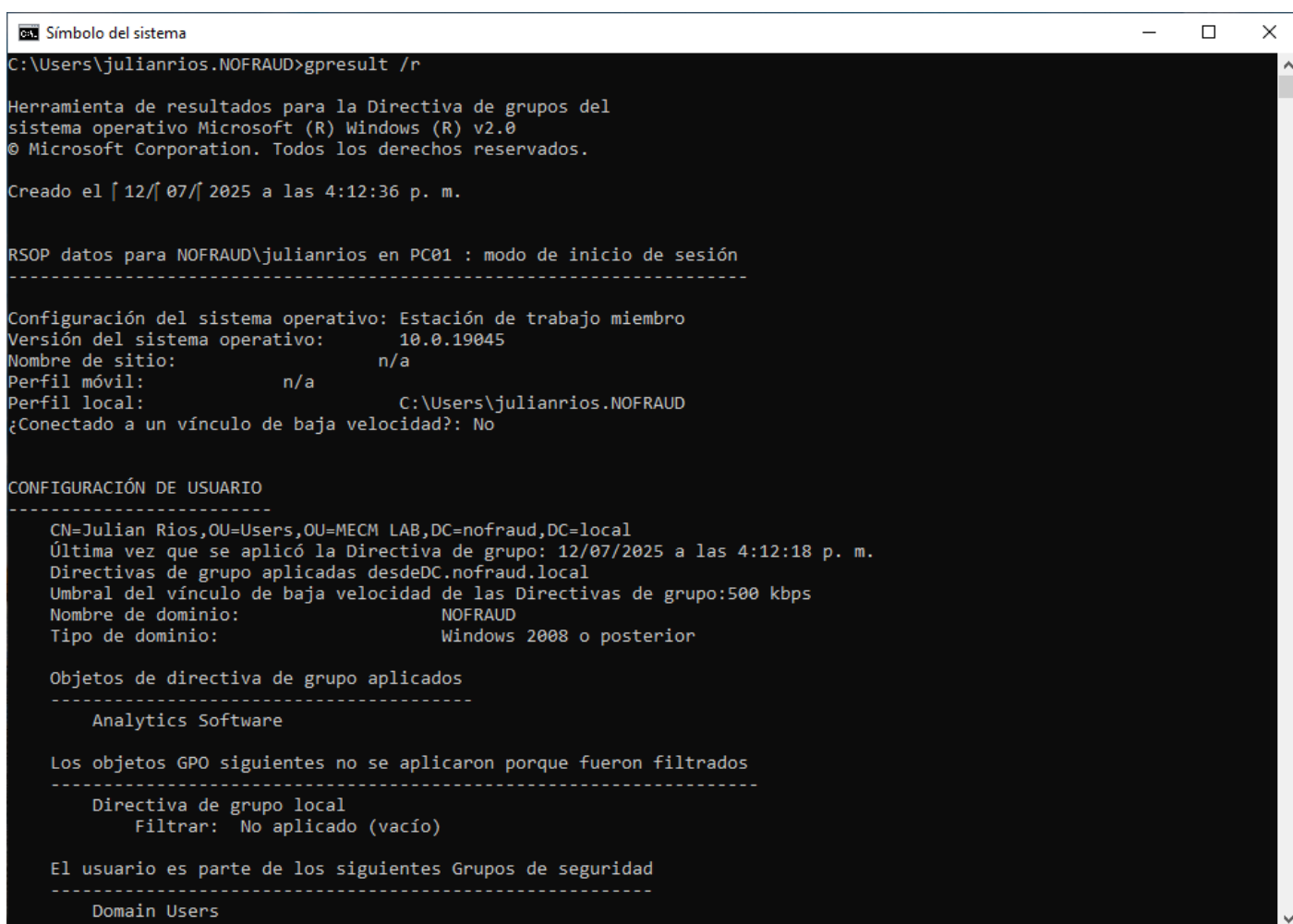
¿Desea cerrar sesión? (S/N)
```

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
```



```
Símbolo del sistema
C:\Users\julianrios.NOFRAUD>gpresult /r

Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
© Microsoft Corporation. Todos los derechos reservados.

Creado el [12/07/2025 a las 4:12:36 p. m.]

RSOP datos para NOFRAUD\julianrios en PC01 : modo de inicio de sesión
-----

Configuración del sistema operativo: Estación de trabajo miembro
Versión del sistema operativo:      10.0.19045
Nombre de sitio:                    n/a
Perfil móvil:                        n/a
Perfil local:                       C:\Users\julianrios.NOFRAUD
¿Conectado a un vínculo de baja velocidad?: No

CONFIGURACIÓN DE USUARIO
-----
CN=Julian Rios,OU=Users,OU=MECM LAB,DC=nofraud,DC=local
Última vez que se aplicó la Directiva de grupo: 12/07/2025 a las 4:12:18 p. m.
Directivas de grupo aplicadas desdeDC.nofraud.local
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio:                  NOFRAUD
Tipo de dominio:                    Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
    Analytics Software

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
    Directiva de grupo local
        Filtrar: No aplicado (vacío)

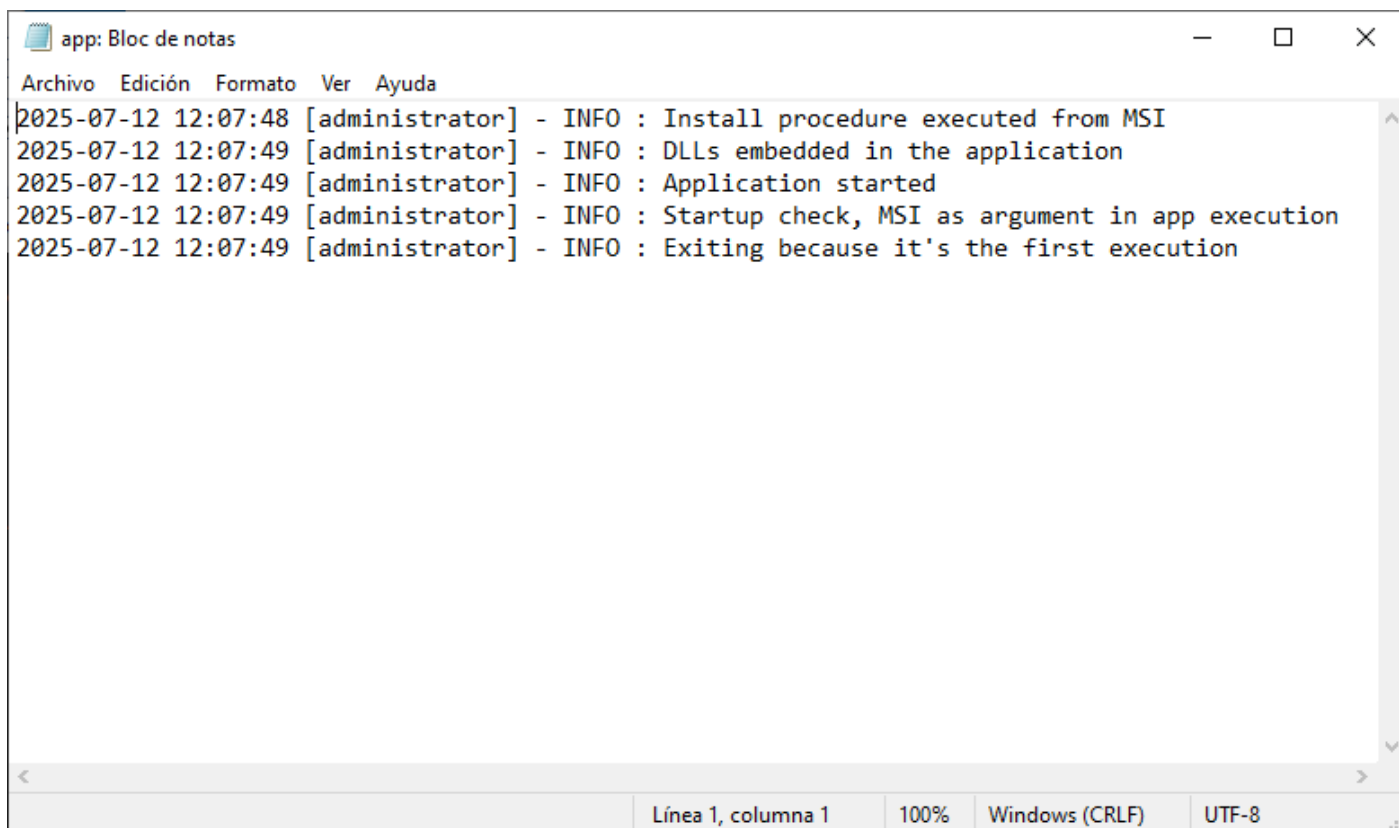
El usuario es parte de los siguientes Grupos de seguridad
-----
    Domain Users
```

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

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

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.



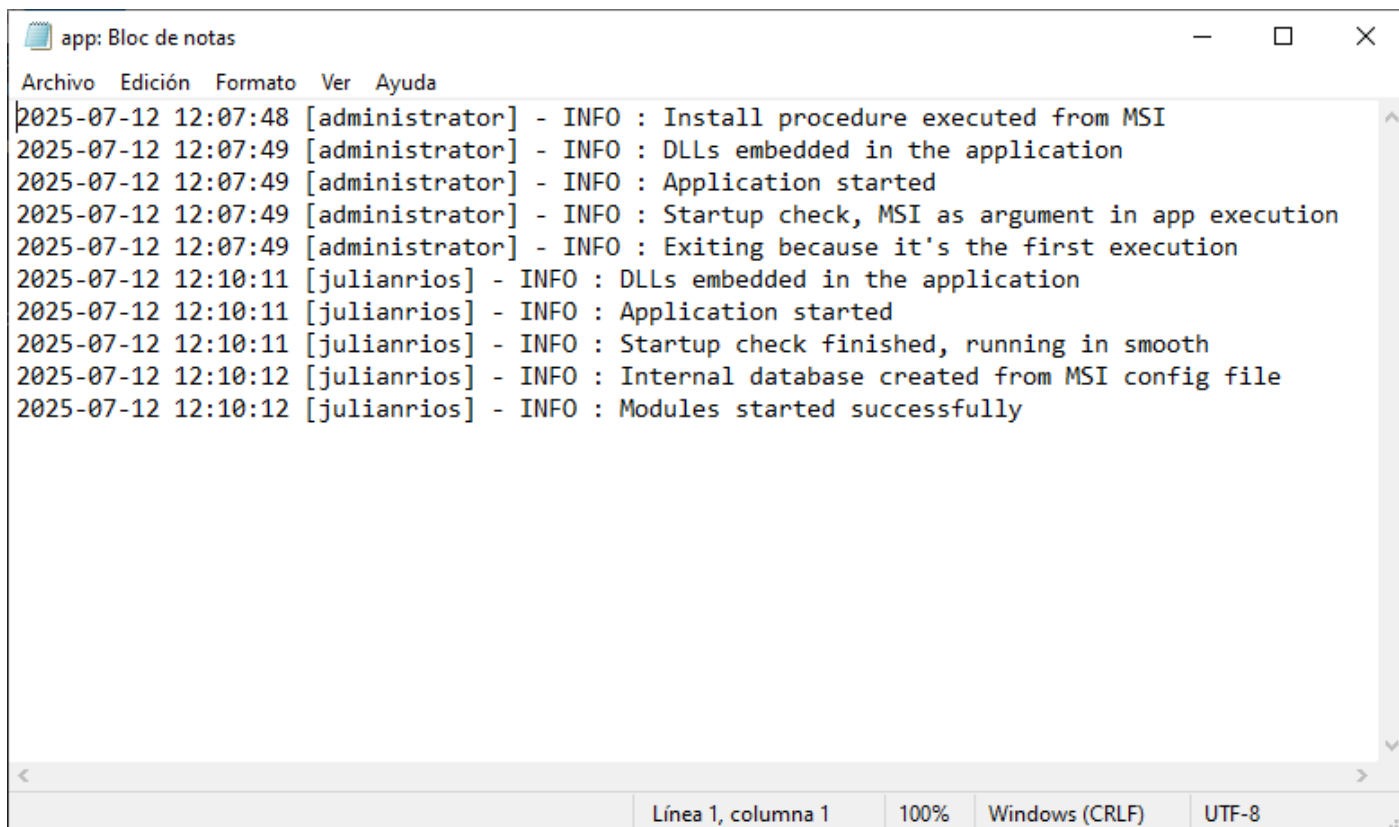
```
app: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
```

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

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

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**.



```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
Línea 1, columna 1 100% Windows (CRLF) UTF-8
```

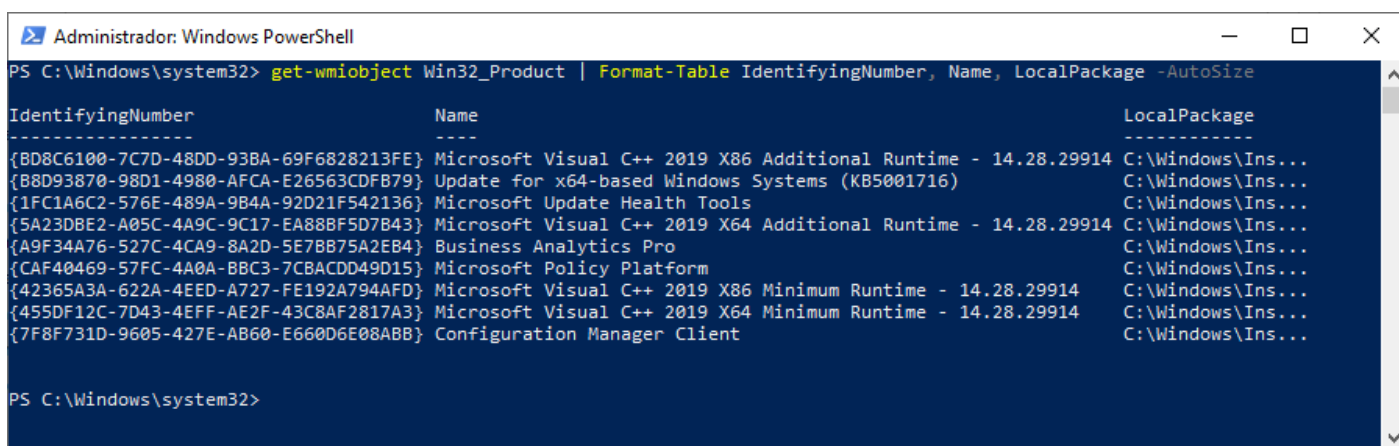
En este archivo de log se encontrará toda información relevante de inicio, parada, actualización, desinstalación e incluso errores que pueda presentar el agente durante su ejecución.

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

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
```



```
Administrador: Windows PowerShell
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Business Analytics Pro C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Ins...

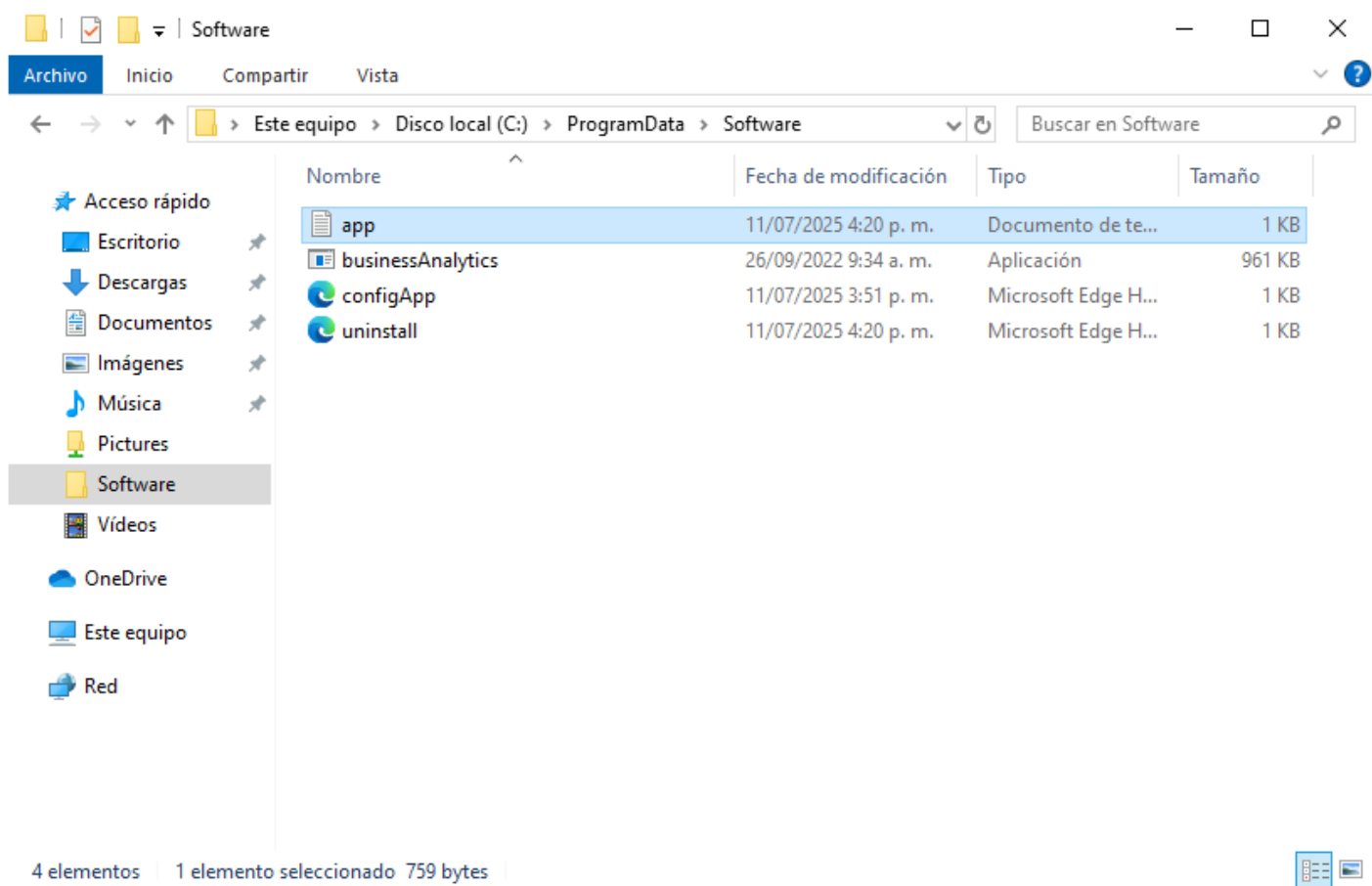
PS C:\Windows\system32>
```

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.

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

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**.

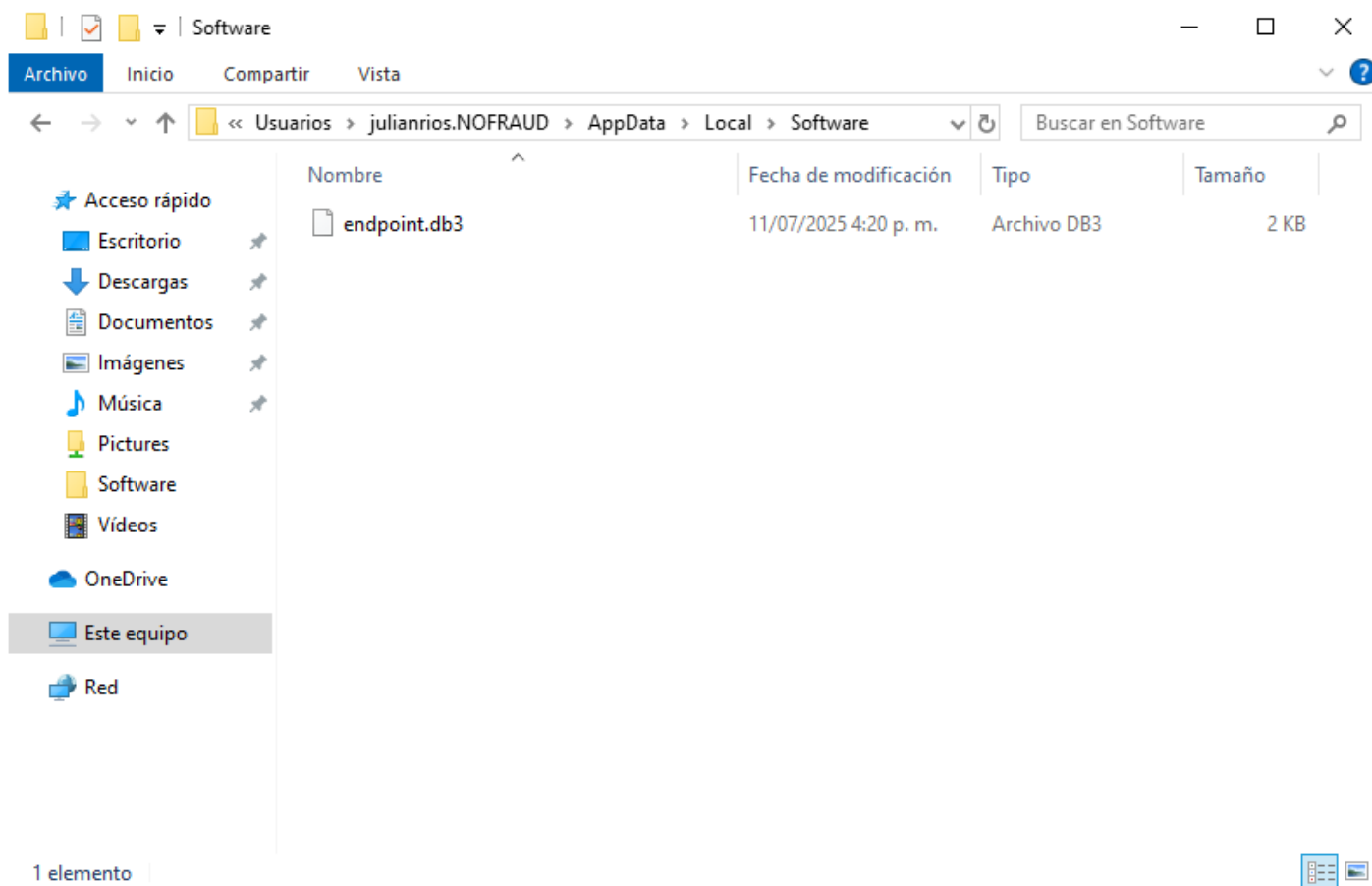


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

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.

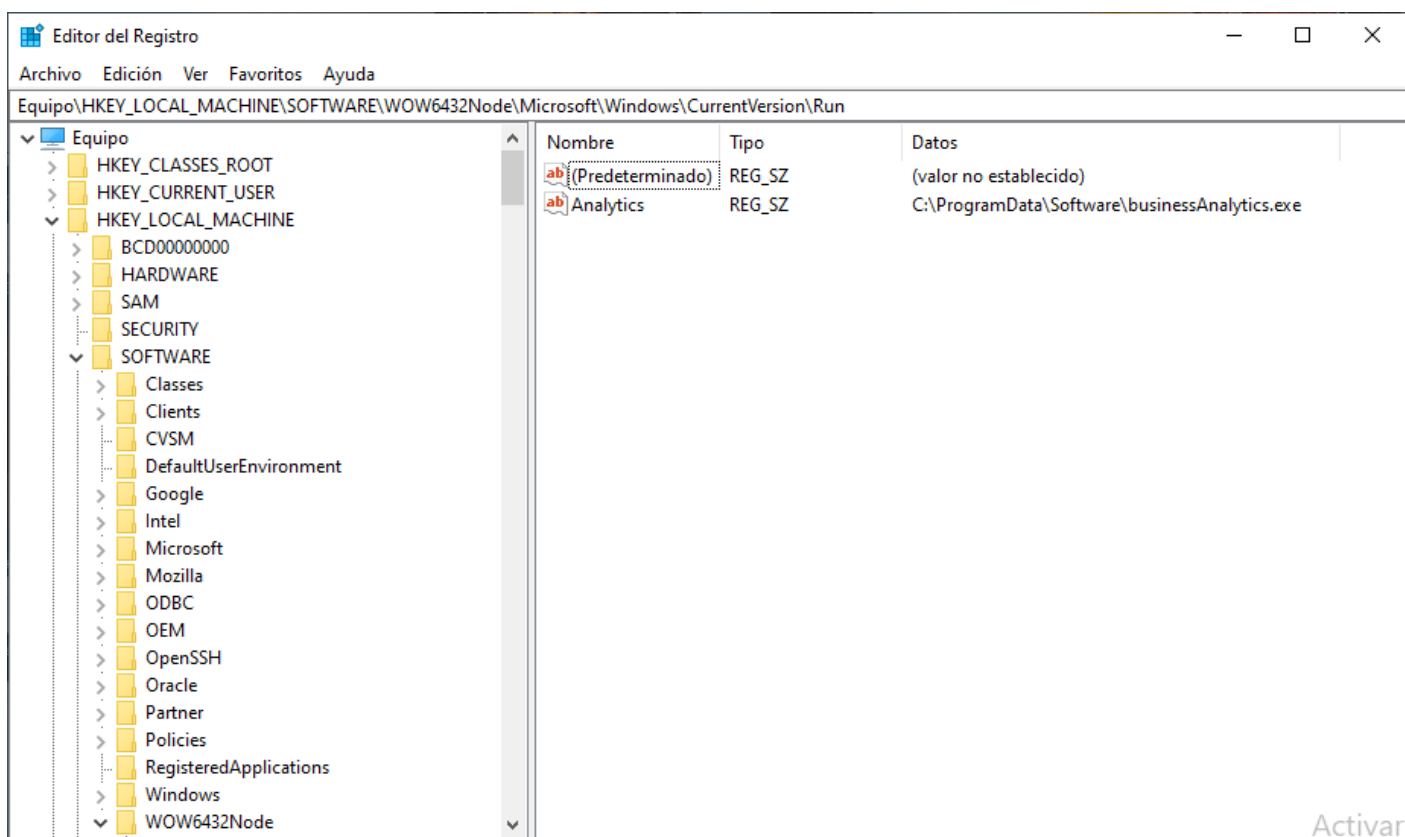


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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**.

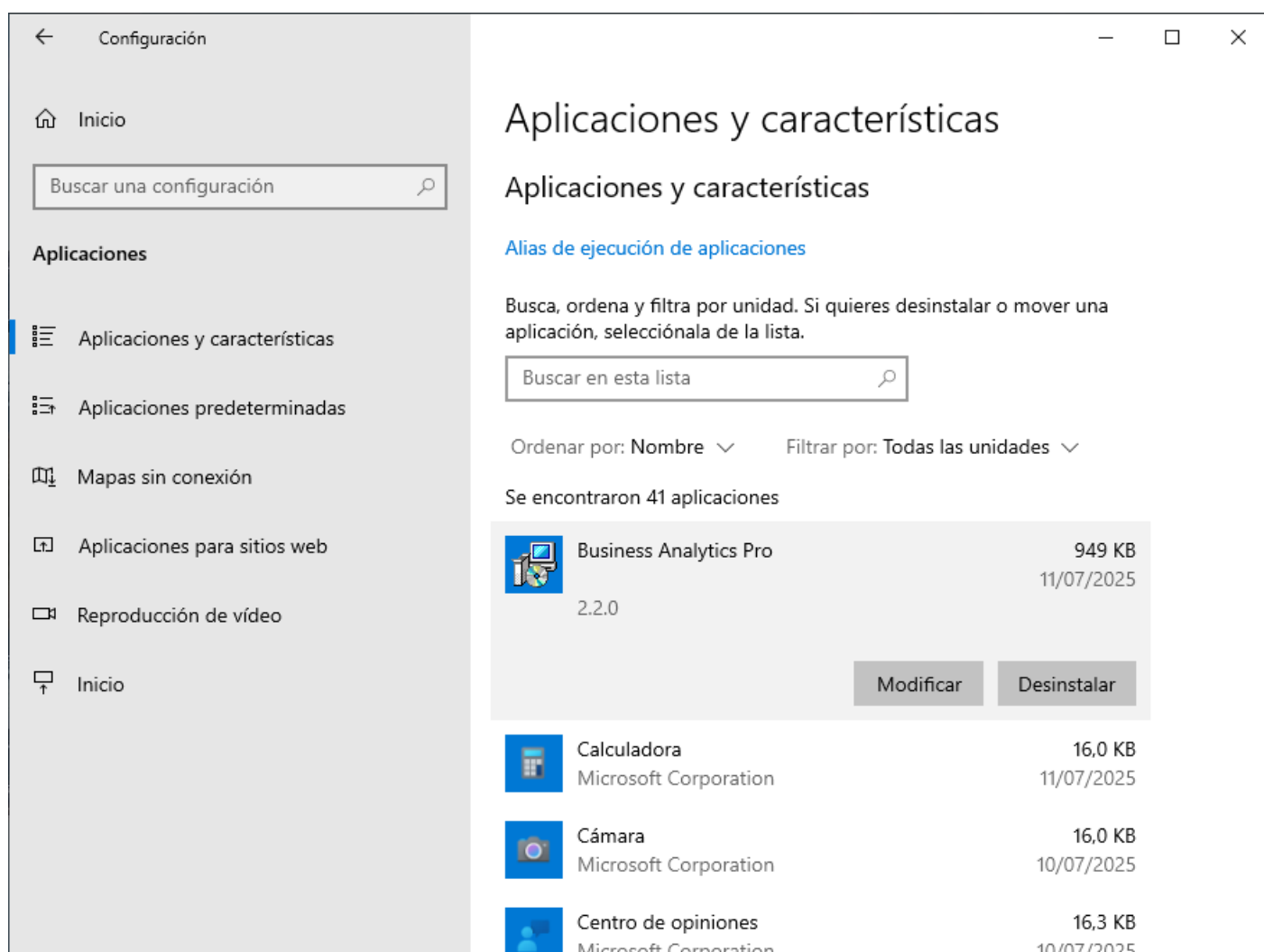


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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 reemplaza 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**.

Administrador de tareas

ArchivOpcionesVista

ProcesosRendimientoHistorial de aplicacionesInicioUsuariosDetallesServicios

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00	11.392 K	
conhost.exe	3768	En ejecución	Administr...	00	4.844 K	No permitida
csrss.exe	552	En ejecución		00	560 K	
csrss.exe	648	En ejecución		00	716 K	
ctfmon.exe	5708	En ejecución	julianrios	00	2.480 K	Deshabilitada
dllhost.exe	4288	En ejecución		00	776 K	
dllhost.exe	7164	En ejecución	julianrios	00	1.908 K	Deshabilitada
dwm.exe	1668	En ejecución		00	43.148 K	
explorer.exe	5572	En ejecución	julianrios	00	75.828 K	Deshabilitada
explorer.exe	5960	En ejecución	julianrios	00	6.132 K	Deshabilitada
FileCoAuth.exe	1792	En ejecución	julianrios	00	28 K	Deshabilitada
fontdrvhost.exe	940	En ejecución		00	76 K	
fontdrvhost.exe	948	En ejecución		00	972 K	
Interrupciones del si...	-	En ejecución	SYSTEM	00	0 K	

Menos detalles

Finalizar tarea

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.

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

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**.

Administrador de tareas

ArchivoOpcionesVista

ProcesosRendimientoHistorial de aplicacionesInicioUsuariosDetallesServicios

Último tiempo de BIOS: 0.0 segundos

Nombre	Anunciante	Estado	Impacto de ini...
Business Analytics Pro	Software Analytics	Habilitado	Alto
Enlace Móvil	Microsoft Corporation	Habilitado	No medido
Microsoft 365 Copilot	Microsoft Corporation	Deshabilitado	Ninguno
Microsoft Edge	Microsoft Corporation	Habilitado	Alto
Microsoft OneDrive	Microsoft Corporation	Habilitado	Alto
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Habilitado	Medio
Windows Security notificati...	Microsoft Corporation	Habilitado	Bajo

Menos detalles

Des_habilitar

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.

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

Despliegue con GPO de Active Directory

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 se le 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**.

Business Analytics Properties

?

X

General

Deployment

Upgrades

Categories

Modifications

Security

Name:

Business Analytics Upgrade

Product information

Version:

3.2

Publisher:

Language:

English (United States)

Platform:

x86

Support information

Contact:

Software Analytics

Phone:

URL:

OK

Cancel

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

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

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.

The image shows a Windows-style dialog box titled "Business Analytics Upgrade Properties". It has a standard title bar with a question mark and a close button (X). Below the title bar is a tabbed interface with five tabs: "General", "Deployment", "Upgrades" (which is currently selected), "Categories", and "Security".

Inside the "Upgrades" tab, there is a section titled "Packages that this package will upgrade:". Below this title is a list box containing one item: "Upgrade Business Analytics Pro".

Below the list box are two buttons: "Add..." and "Remove".

Below the buttons is a checkbox that is checked, with the label "Required upgrade for existing packages:". A horizontal line separates this section from the one below.

Below the line is another section titled "Packages in the current GPO that will upgrade this package:". Below this title is an empty list box.

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue border.

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.

Despliegue con GPO de Active Directory

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**.

Business Analytics Pro Properties

General Deployment Upgrades Categories Modifications Security

Deployment type

☐ Published

☒ Assigned

Deployment options

☒ Auto-install this application by file extension activation

☒ Uninstall this application when it falls out of the scope of management

☐ Do not display this package in the Add/Remove Programs control panel

☒ Install this application at logon

Installation user interface options

☐ Basic

☒ Maximum

Advanced...

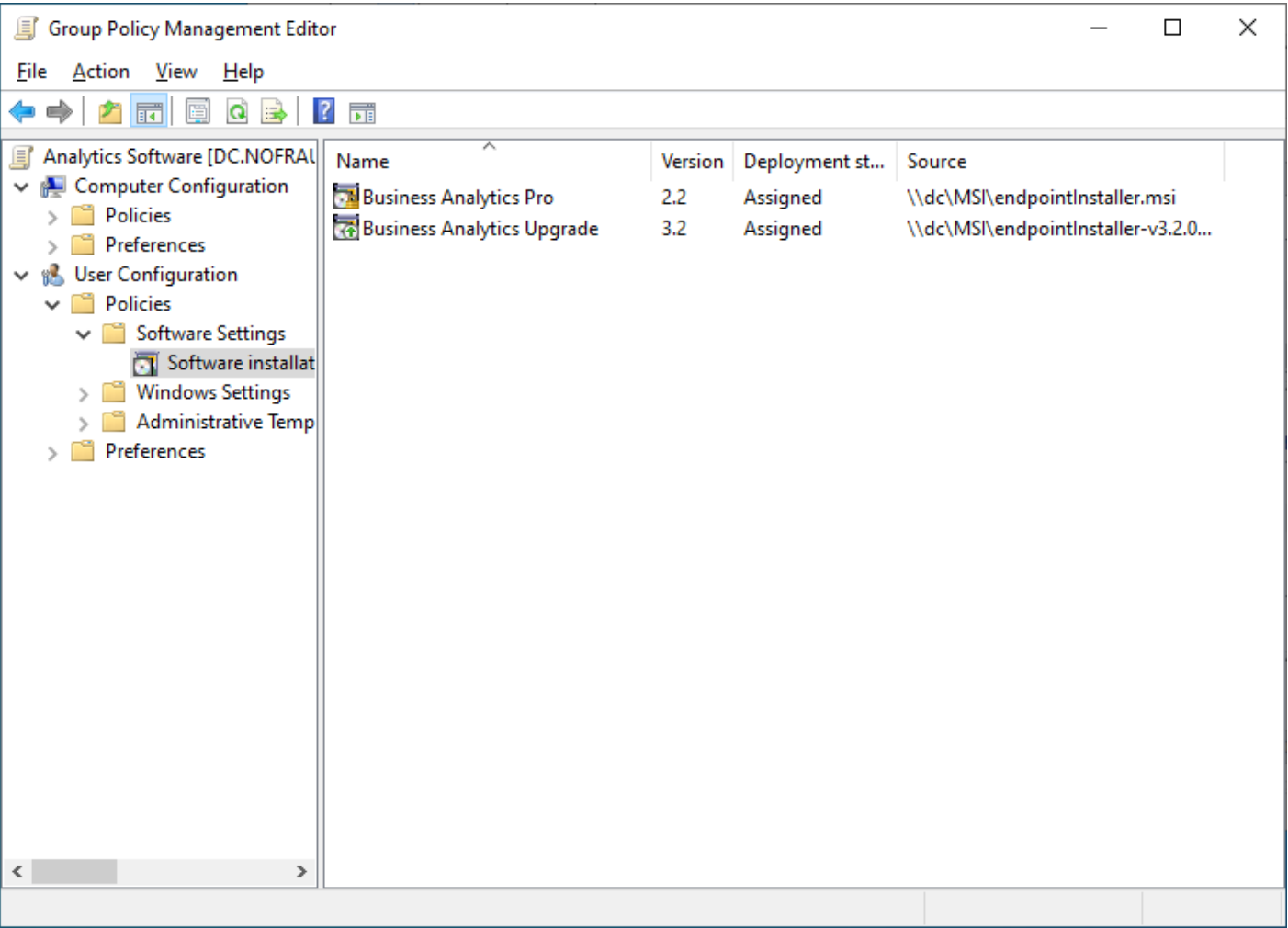
OK Cancel

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

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

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.

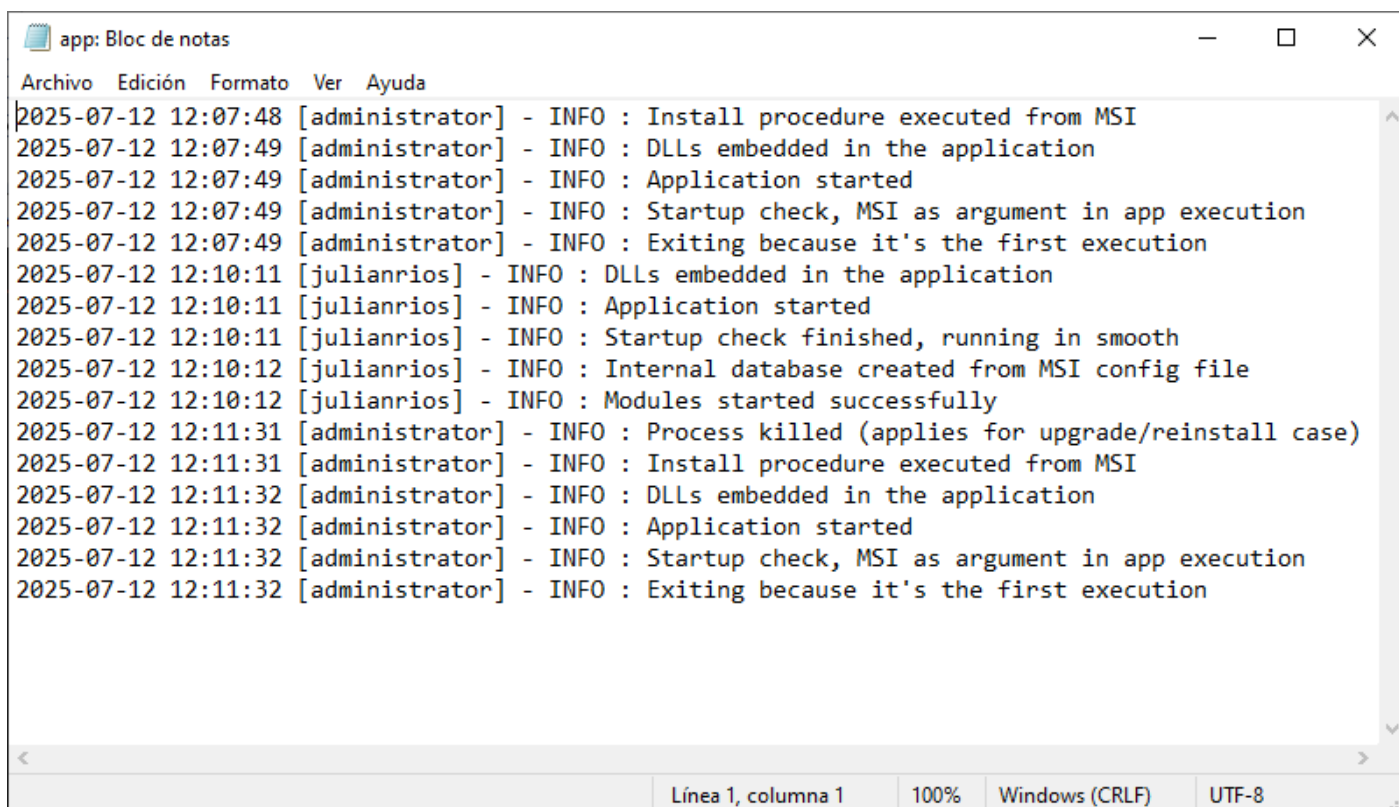


En los iconos se ve que la segunda entrada tiene una flecha verde hacia arriba, lo significa que se trata de una actualización.

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

Verificación de la actualización

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



```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
2025-07-12 12:11:31 [administrator] - INFO : Process killed (applies for upgrade/reinstall case)
2025-07-12 12:11:31 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:11:32 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:11:32 [administrator] - INFO : Application started
2025-07-12 12:11:32 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:11:32 [administrator] - INFO : Exiting because it's the first execution
Línea 1, columna 1 100% Windows (CRLF) UTF-8
```

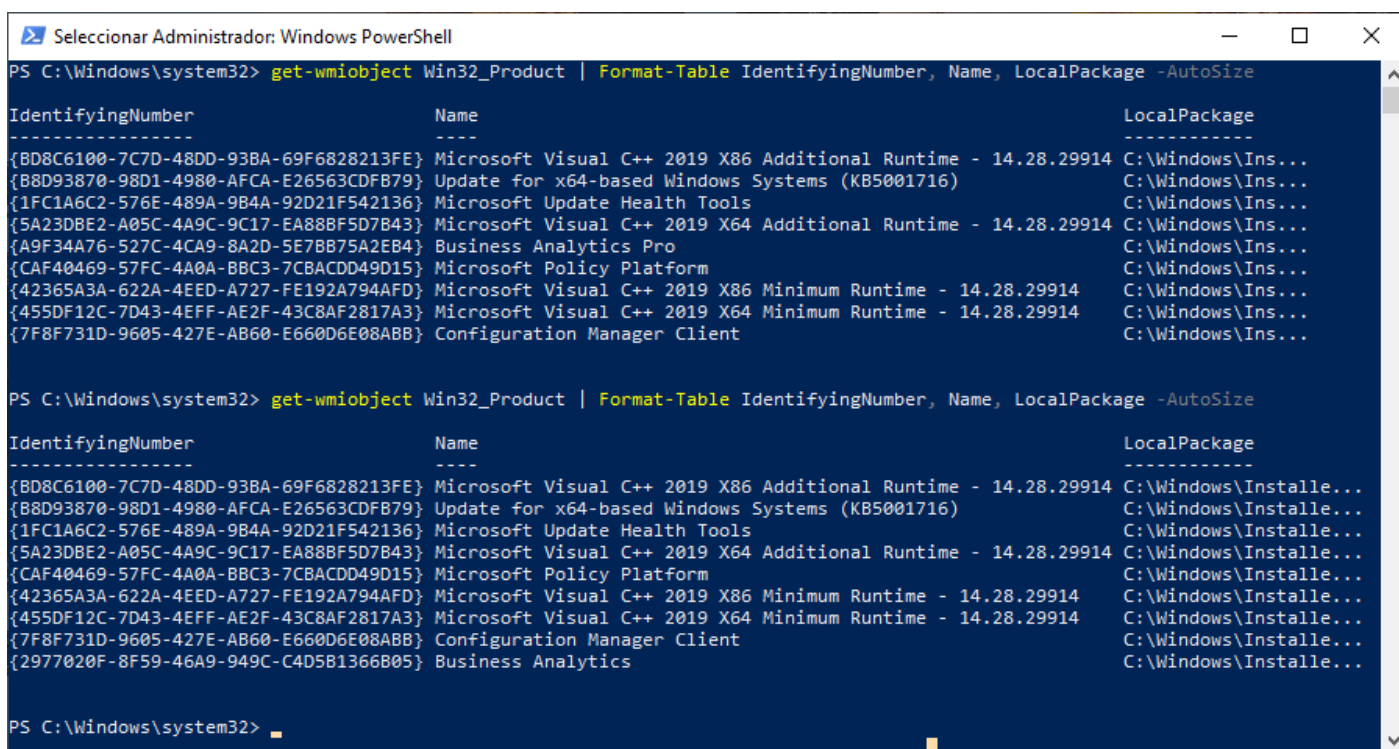
Se puede comprobar que se actualizó por la presencia de la entrada **Process killed (applies for upgrade/reinstall case)**.

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

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
```



```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

```
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05}	Business Analytics	C:\Windows\Installe...

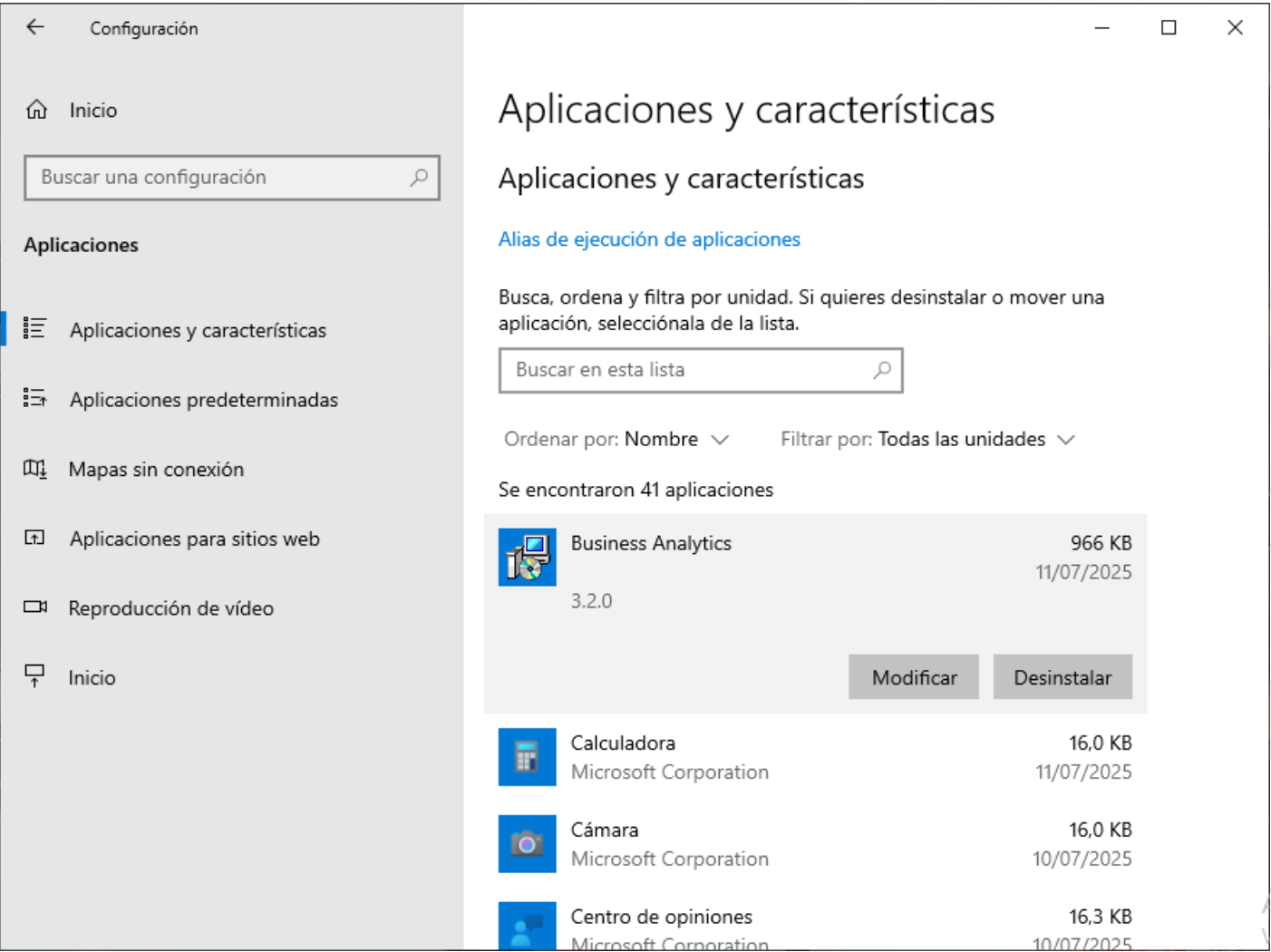
```
PS C:\Windows\system32>
```

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

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

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.



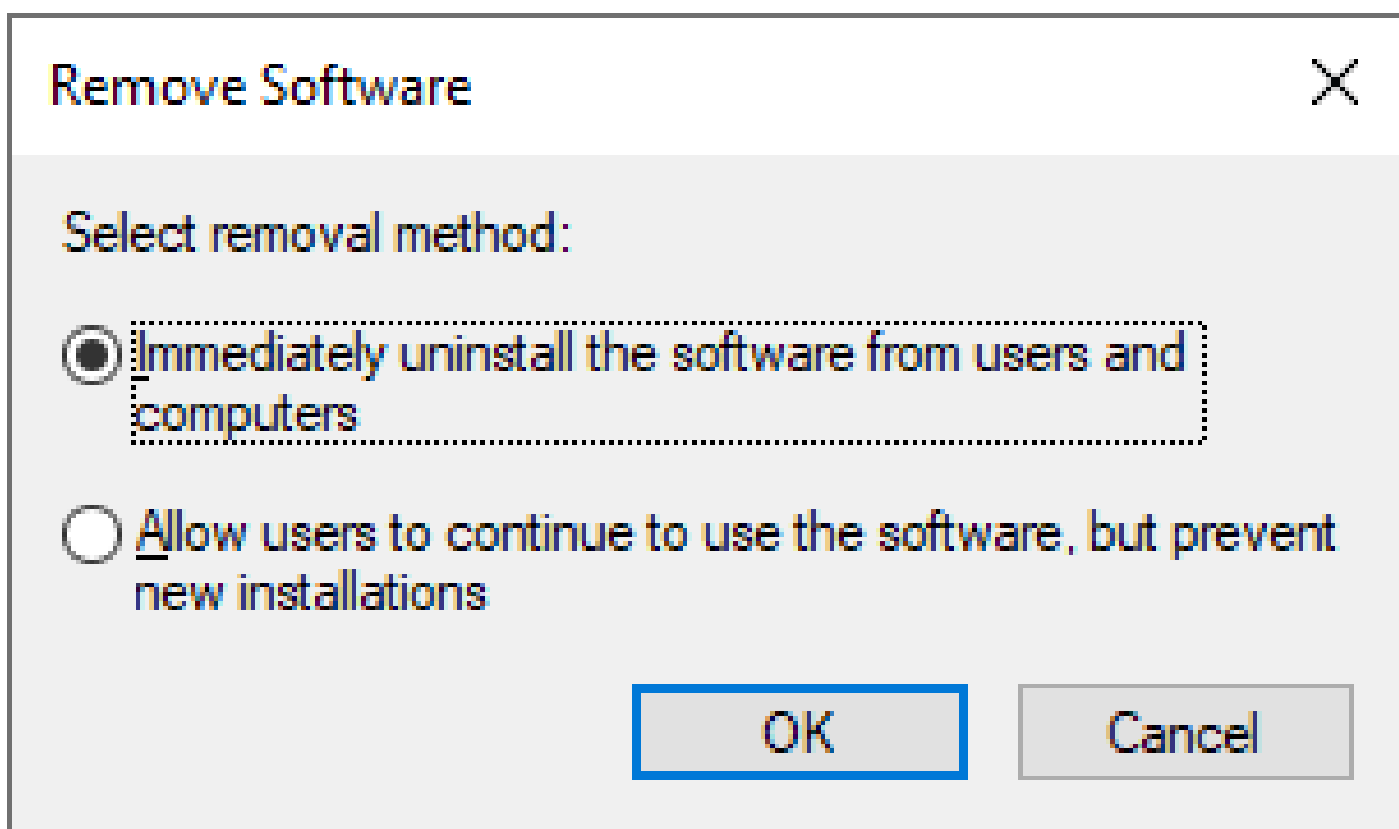
Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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**.

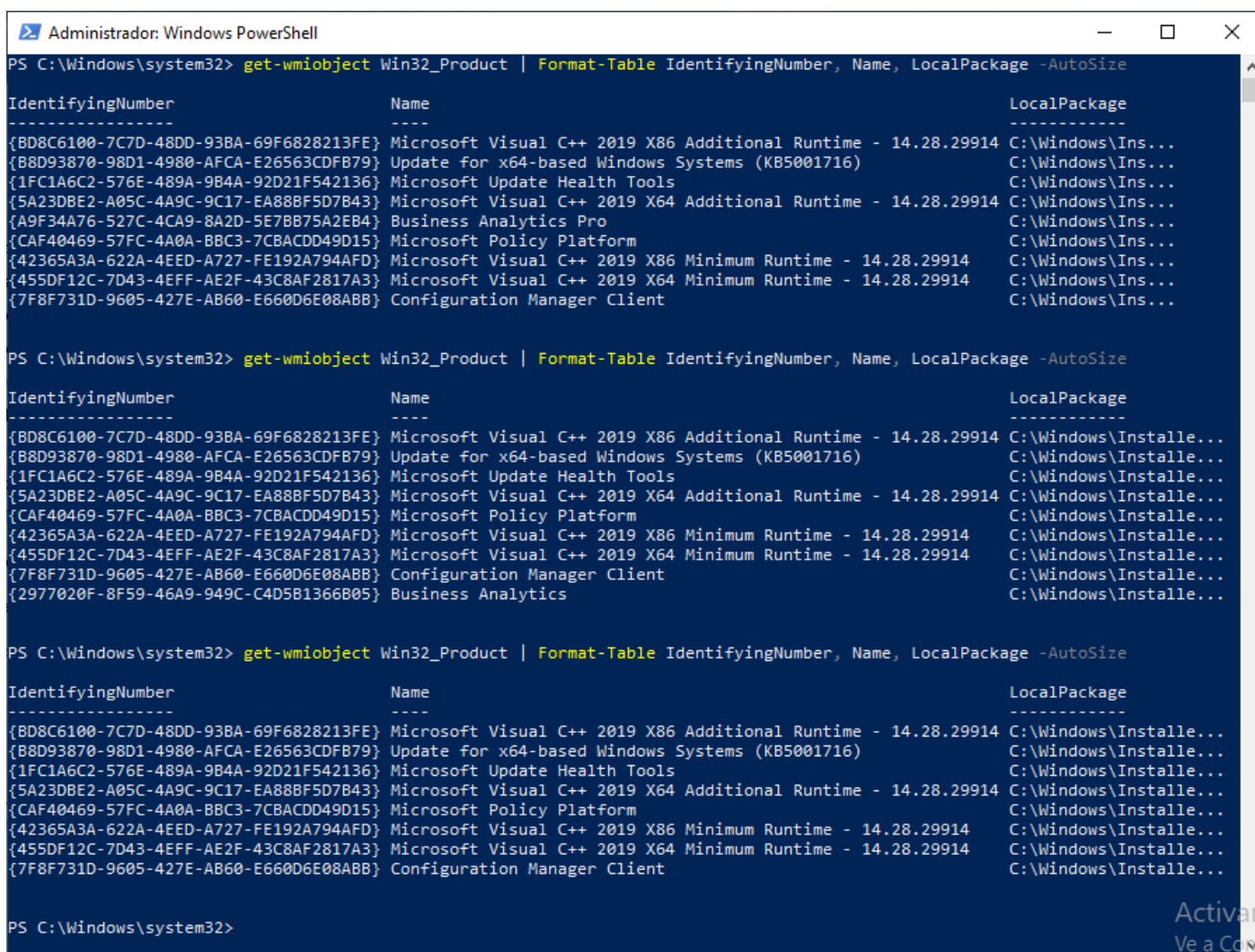


Seleccione la primera opción y de clic en OK. Esto desinstalará el agente en el próximo reinicio de los PC.

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
```



```
Administrador: Windows PowerShell
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Business Analytics Pro C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Ins...

PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366B05} Business Analytics C:\Windows\Installe...

PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Installe...

PS C:\Windows\system32>
```

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

