

Manage Engine Endpoint Central

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

- [Requisitos previos](#)
- [Video con todos los pasos](#)
- [Paquete de instalación](#)
- [Configuración para la instalación](#)
- [Deployment del agente](#)
- [Monitoreo de la instalación](#)
- [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](#)
- [Crear paquete para actualización](#)
- [Suspende versión anterior](#)
- [Configuración para la actualización](#)
- [Verificación de la actualización](#)
- [PowerShell para verificar actualización](#)
- [Actualización en listado de Aplicaciones](#)
- [Desinstalación del agente](#)
- [Verificación de la desinstalación](#)

Requisitos previos

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

Debe contar con la capacidad de realizar acciones administrativas en la consola de **Manage Engine** y opcionalmente en los computadores de la organización. En teoría, para llevar a cabo el despliegue de nuestro agente no se requiere realizar ninguna acción en los PC de los empleados, sin embargo, en la primera instalación de pruebas quizás quiera verificar manualmente la instalación del agente.

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

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

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

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

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

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

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/lxJhzy9gIYg?si=C5NHc-hva1Phka5g>

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

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

Paquete de instalación

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

Windows Package Creation | X +

endpointcentral.manageengine.com/webclient#/uems/software-deployment/packages/windows/create?isAllCustomerPkg=false&platf...

Endpoint Central Home Configurations Threats & Patches Software Deployment Inventory MDM Admin Agent ... Jump to SDP

Packages > Windows Package Creation

Enter Package Details

Package Name * Business Analytics 2.2.0

Package Type MSI / MSP EXE / APPX / MSIEXEC / MSU

License Type * Commercial

Locate installable From Shared Folder From Local Computer

1 file(s) added (Click or drop to add more) Browse

✓ endpointInstaller-v2.2.0.msi

All (1) file are uploaded

[.z, .zip, .gzip, .bzip2, and .tar files will be extracted automatically. Total file size limit is 12 GB.]

Safeguard sensitive information
Ensure sensitive information (e.g., password, license keys) is not included in command line arguments, as the software package may be reused by other users.

Installation Uninstallation Advanced Settings Watch Demo Real world scenarios for pre/post activities

1 Installation Details

2 Pre-Deployment Activities +

3 Post-Deployment Activities +

MSI / MSP File Name * endpointInstaller-v2.2.0.msi

MST File Name

MSI / MSP Properties for installation

Disable Uninstall option in Add/Remove Programs

Add Package Cancel

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

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

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

Configuración para la instalación

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

The screenshot shows the Endpoint Central web interface. The top navigation bar includes 'Home', 'Configurations', 'Threats & Patches', 'Software Deployment', 'Inventory', 'MDM', 'Admin', and 'Agent'. The left sidebar contains 'Add Configurations', 'Views', 'Reports', and 'Settings'. The main content area is titled 'Add Configuration' and shows a grid of configuration options for Windows, Mac, and Linux. The 'Install/Uninstall Windows Patch' option is highlighted, and the 'Install/Uninstall Windows' button is selected. Below the grid is a 'Quick Links' section with a 'How Tos' link and a list of links to various configuration guides.

Endpoint Central Home Configurations Threats & Patches Software Deployment Inventory MDM Admin Agent ... Jump to SDP

Add Configuration
User Configurations will be applied during user logon/refresh cycle and the computer configuration will be applied during computer startup/refresh cycle.

Windows Mac Linux

- Alerts
- Browser
- Certificate Distribution
- Common Folder Redirection
- Custom Script
- Display
- Drive Mapping
- Environment Variable
- File Folder Operation
- Firewall
- Folder Backup
- Folder Redirection
- Fonts
- General
- Group Management
- IP Printer
- Install/Uninstall Windows Patch
- Install/Uninstall Windows
- Launch Application
- Legal Notice
- MS Office
- MS Outlook
- Message Box
- Outlook Exchange Profile
- Path
- Permission Management
- Power Management
- Registry
- Scheduler
- Secure USB
- Security Policies
- Services
- Shared Network Printer
- Shortcut
- User Management
- WiFi

Quick Links Hide

[How Tos](#)

1. How to change the local administrator password in a computer?
2. How to configure proxy settings in Internet Explorer for all users?
3. How do I deploy custom wallpapers to all the client computers in my network and prevent users from changing them?
4. How do I deploy custom screen savers at regular intervals to all the client computers in my network?
5. How to disable the Automatic Updates?
6. How to create custom messages to display on all the client systems in my network?

[More](#) | [Roadmap](#)

[Need more Configuration?](#)
<https://endpointcentral.manageengine.com/webclient#/uems/configuration/add/124?platform=windows&type=computer>

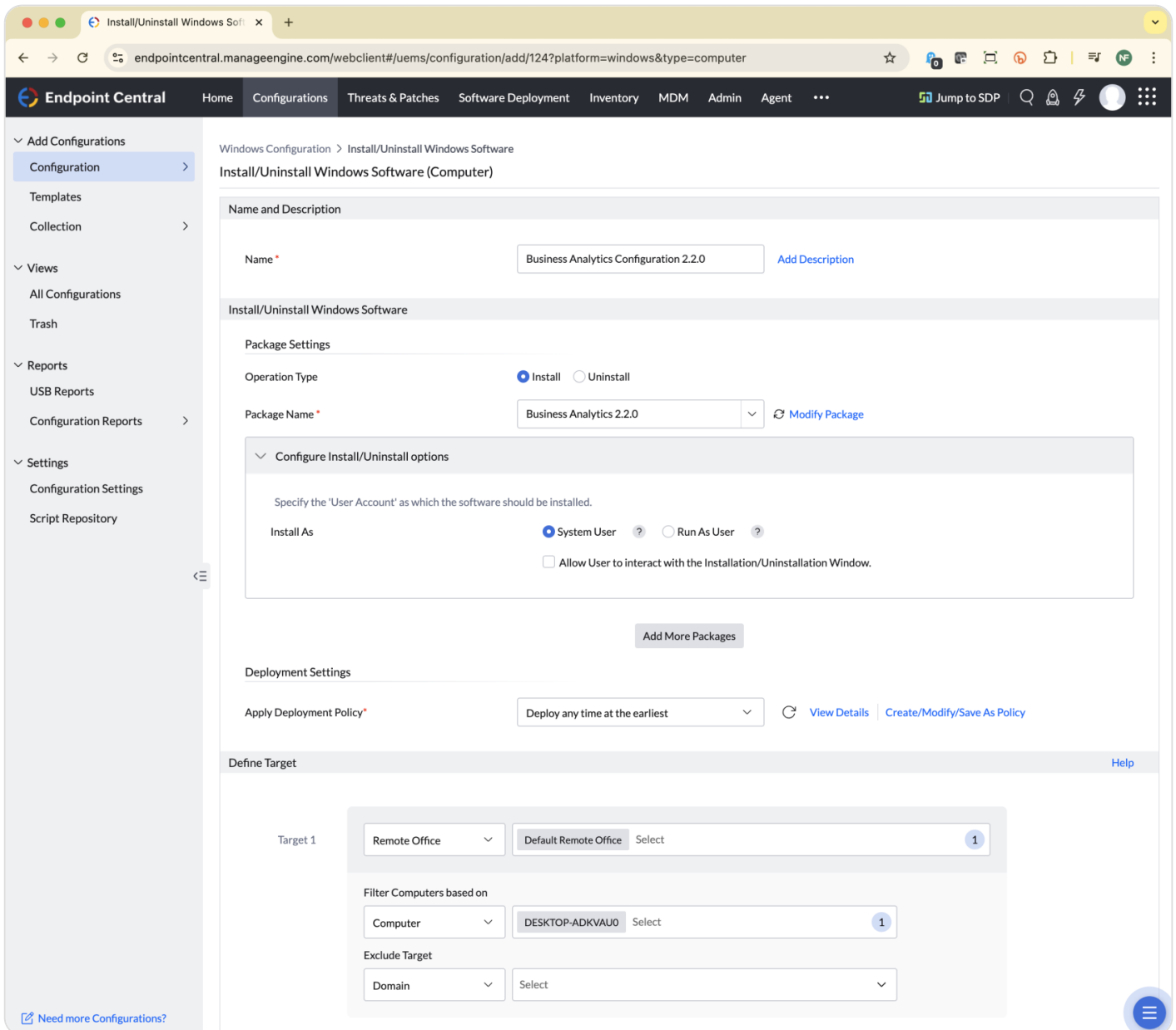
© 2025 ZOH0 Corp. (C) Copyright

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

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

Deployment del agente

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



The screenshot shows the Endpoint Central web interface for configuring the installation of Windows software. The page is titled "Install/Uninstall Windows Software (Computer)".

- Name and Description:** The "Name" field is set to "Business Analytics Configuration 2.2.0".
- Package Settings:**
 - Operation Type:** "Install" is selected.
 - Package Name:** "Business Analytics 2.2.0" is selected.
 - Configure Install/Uninstall options:**
 - Install As:** "System User" is selected.
 - "Allow User to interact with the Installation/Uninstallation Window." is unchecked.
- Deployment Settings:** "Apply Deployment Policy" is set to "Deploy any time at the earliest".
- Define Target:**
 - Target 1:** "Remote Office" is selected, with "Default Remote Office" as the value.
 - Filter Computers based on:** "Computer" is selected, with "DESKTOP-ADKVAU0" as the value.
 - Exclude Target:** "Domain" is selected, with "Select" as the value.

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

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

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

Monitoreo de la instalación

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

The screenshot displays the Endpoint Central web interface. The main content area shows the details for a configuration named "Business Analytics Configuration 2.2.0". The configuration is in the "Executed" state, as indicated by a green checkmark and a donut chart showing 100% completion. The interface includes a navigation sidebar on the left, a top menu, and a main content area with tabs for Summary, Configuration Details, Execution Status, and Replication Details.

Configuration Details:

- Name: Business Analytics Configuration 2.2.0
- Description: --
- Category: Install/Uninstall Windows Software
- Current Status: Executed
- Platform: windows
- Type: Computer
- Created Time: Aug 1, 2025 09:35 AM
- Created By: Julian Rios
- Modified Time: Aug 1, 2025 09:35 AM
- Modified By: Julian Rios
- Enable Notification: No
- Enable Retry: Yes
- Total Retry Count: 2

Execution Summary:

- Yet To Apply: 0
- Succeeded: 1
- In Progress: 0
- Failed: 0
- Not Applicable: 0
- Retry In Progress: 0
- In Progress: 0

Target Scope:

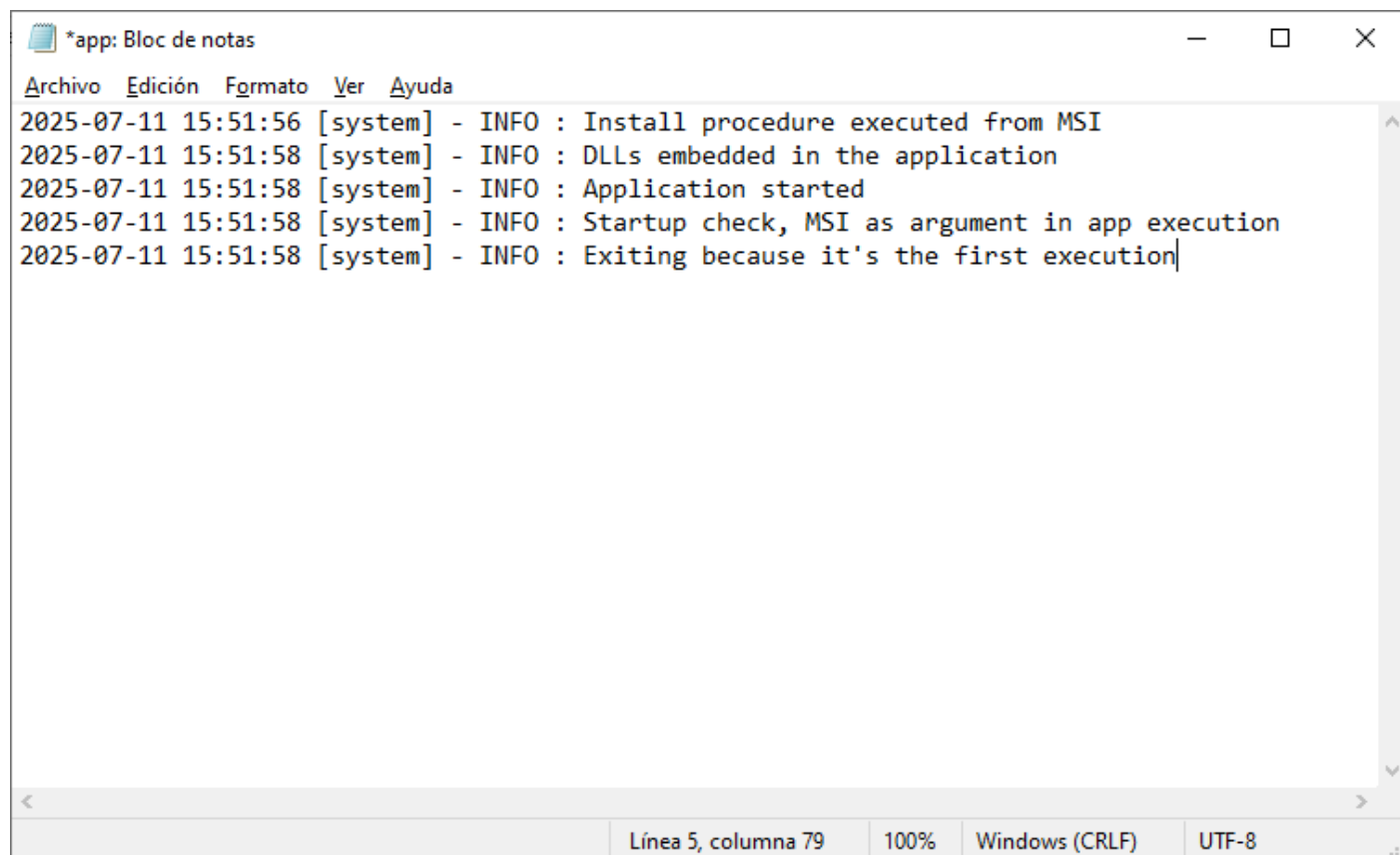
Target Scope	Apply To	Excluded Items
Remote Office	Computer	--
Default Remote Office	WORKGROUP: DESKTOP-ADKVAUO	--

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

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



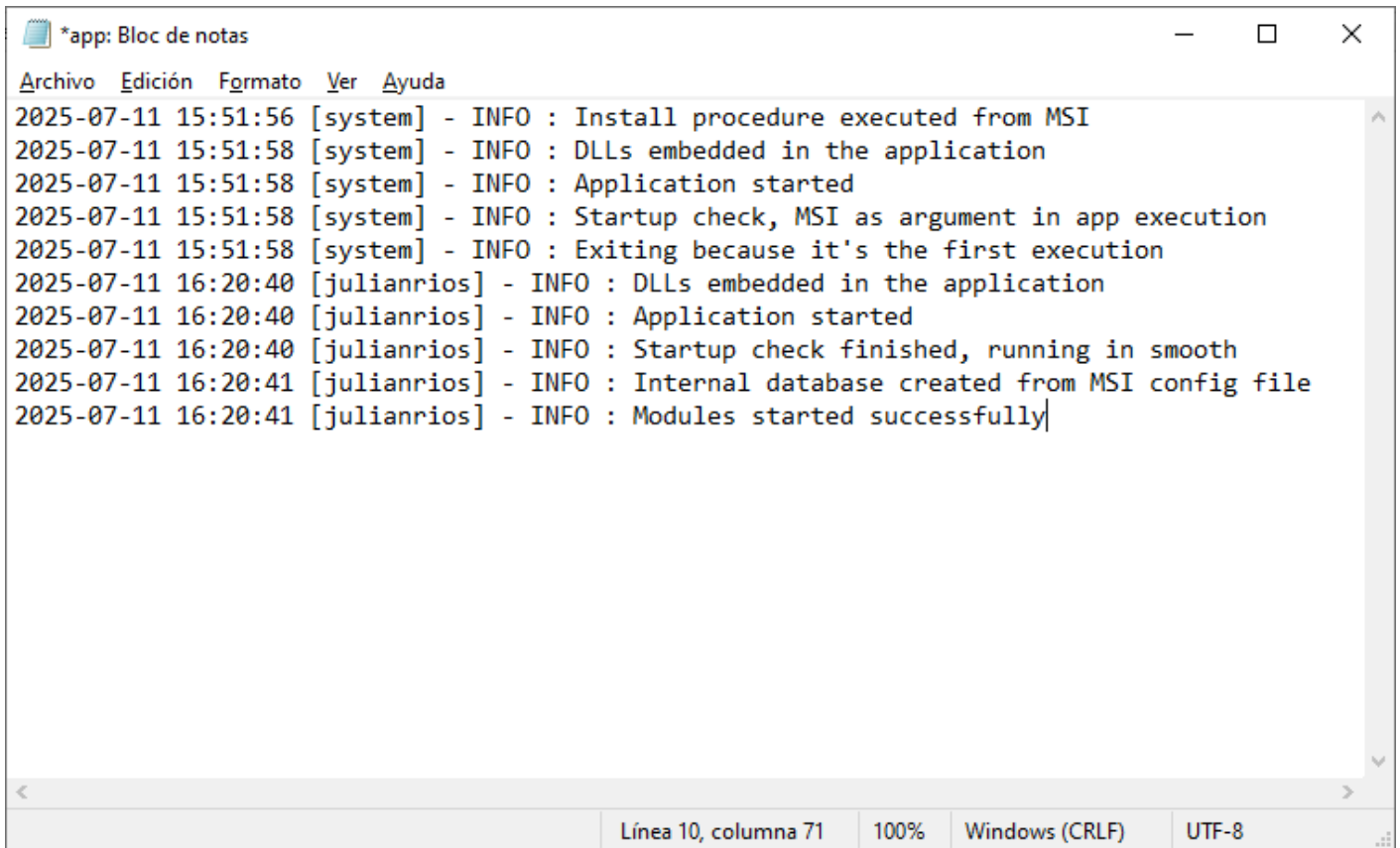
```
*app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup check, MSI as argument in app execution
2025-07-11 15:51:58 [system] - INFO : Exiting because it's the first execution
Línea 5, columna 79 100% Windows (CRLF) UTF-8
```

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](https://www.nofraud.com). 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

Línea 10, columna 71  100%  Windows (CRLF)  UTF-8
```

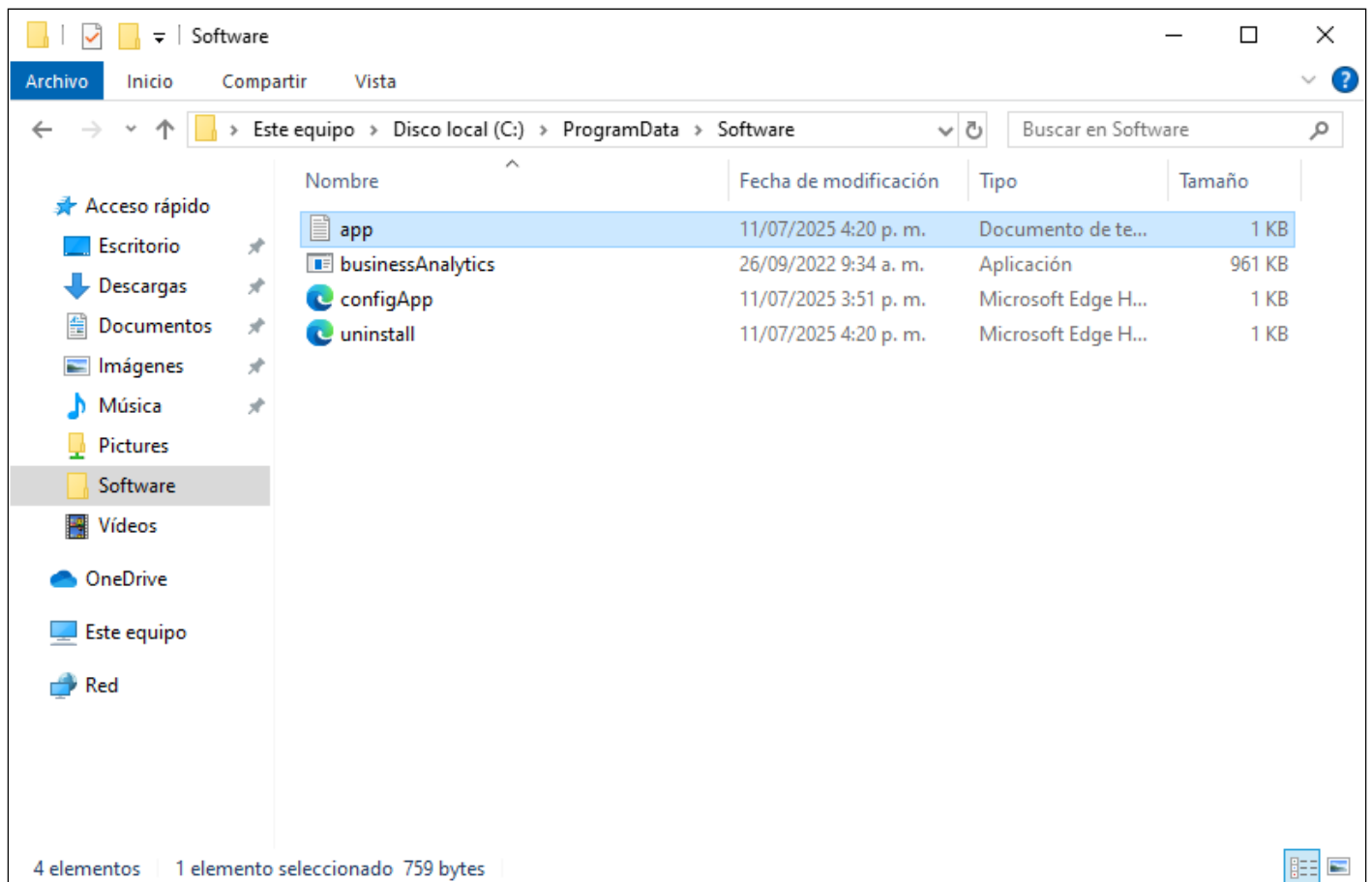
Como se observa, ya la ejecución se hace con un usuario normal sin privilegios elevados y de esa manera el agente de The Fraud Explorer lo detecta y procede a arrancar diciendo **Modules started successfully**.

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**.

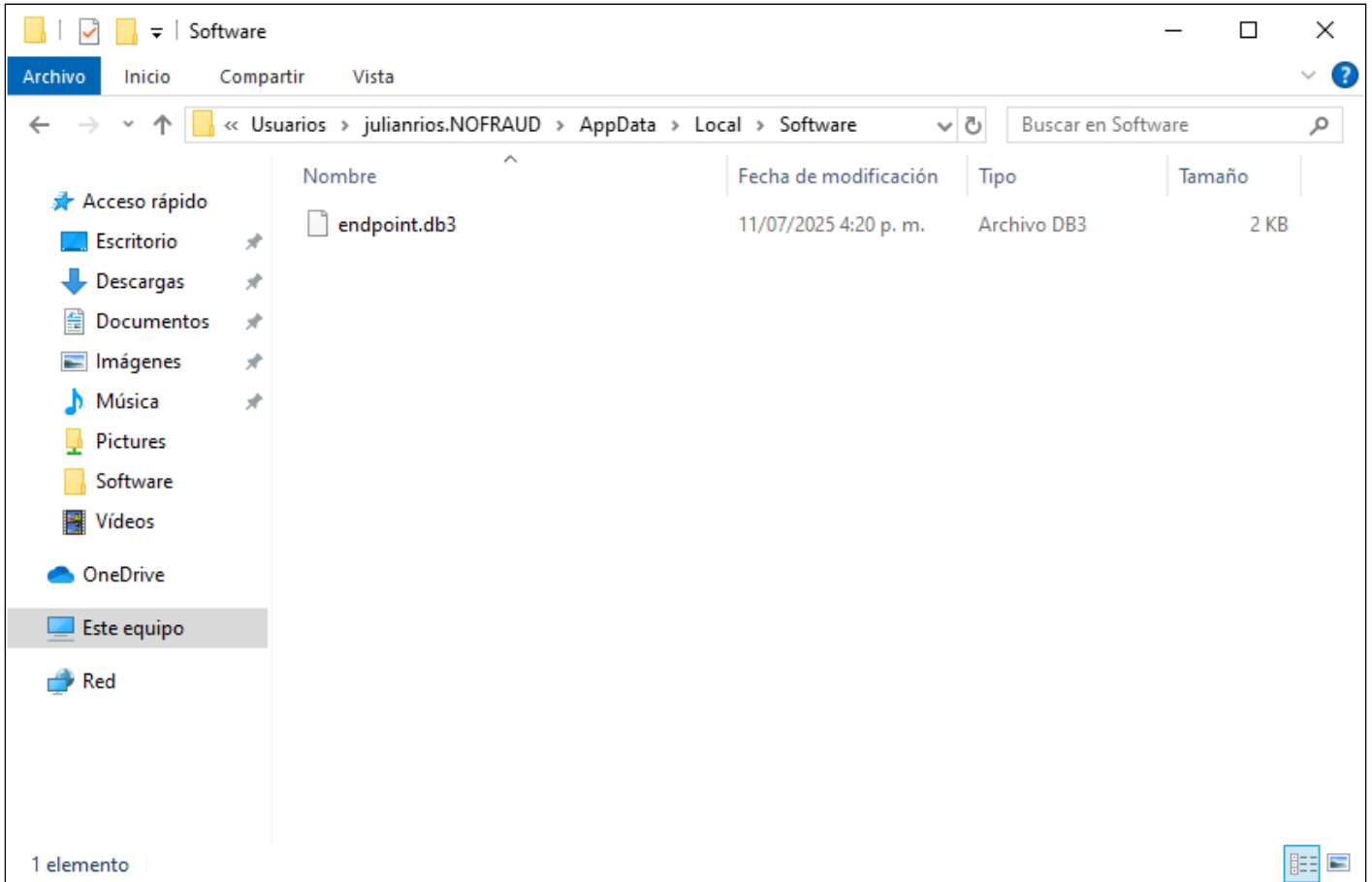


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

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.

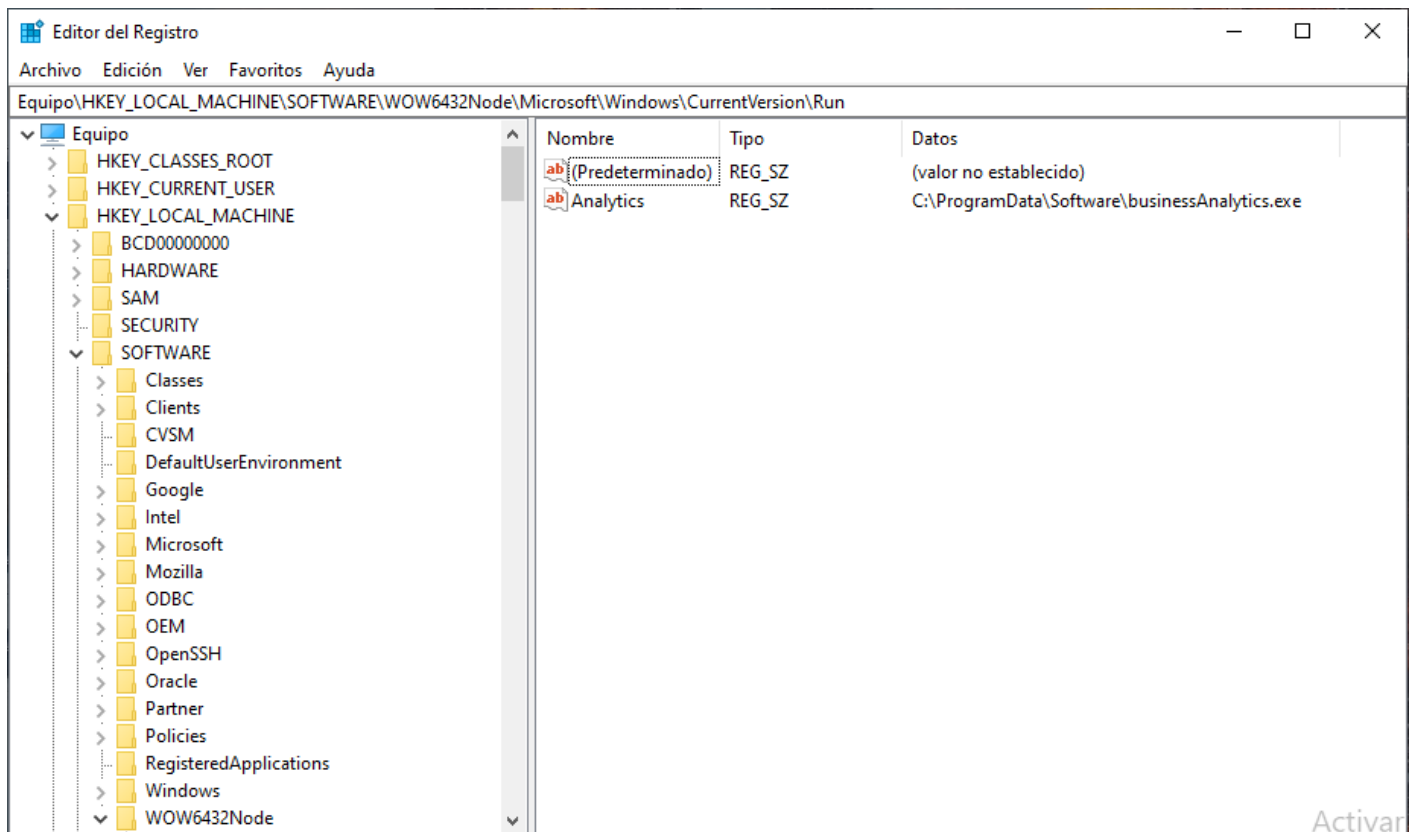


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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.**

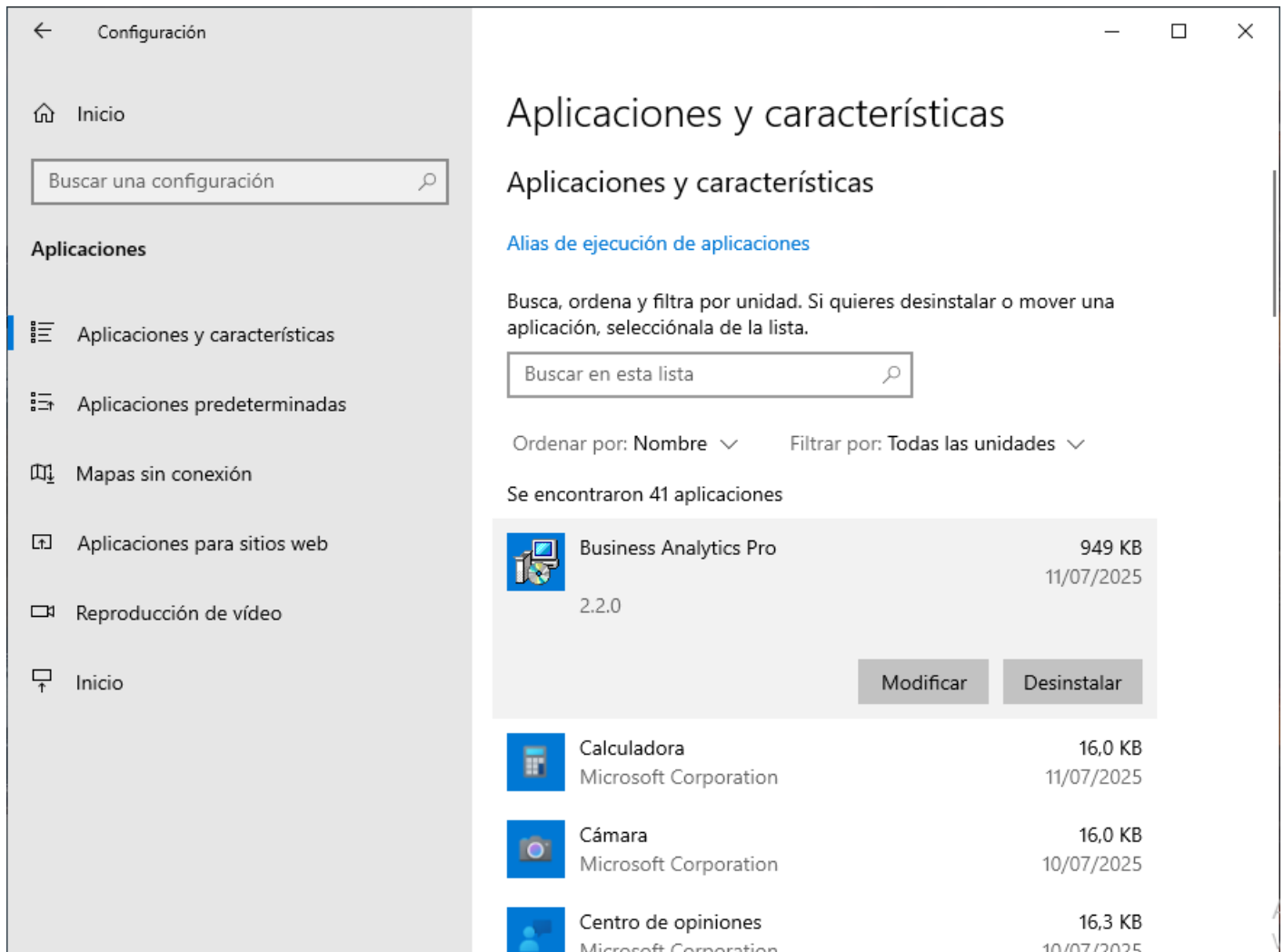


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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**.



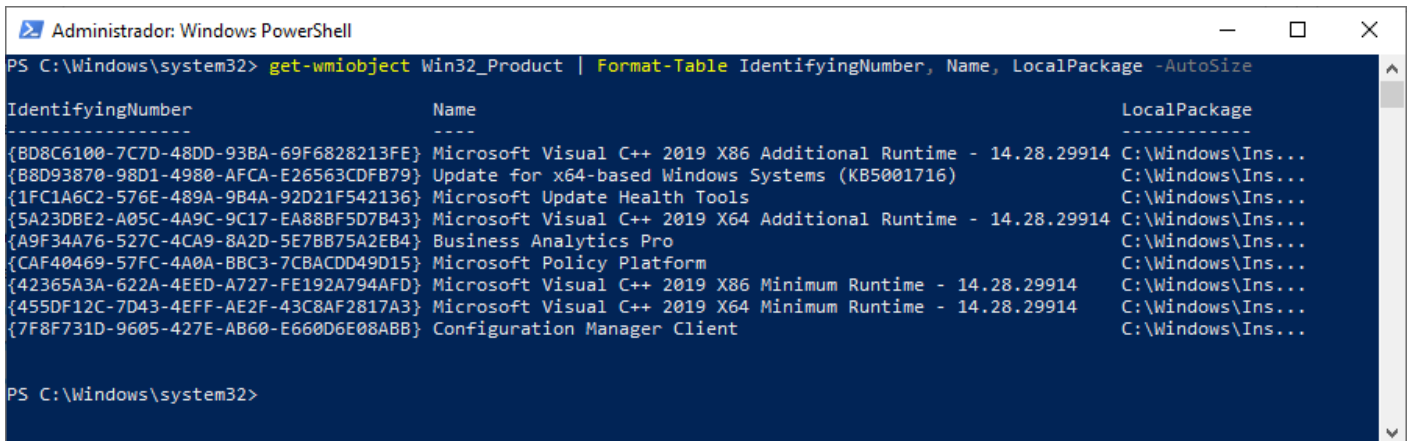
Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se reemplaza la actual con la nueva versión.

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
```



```
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...

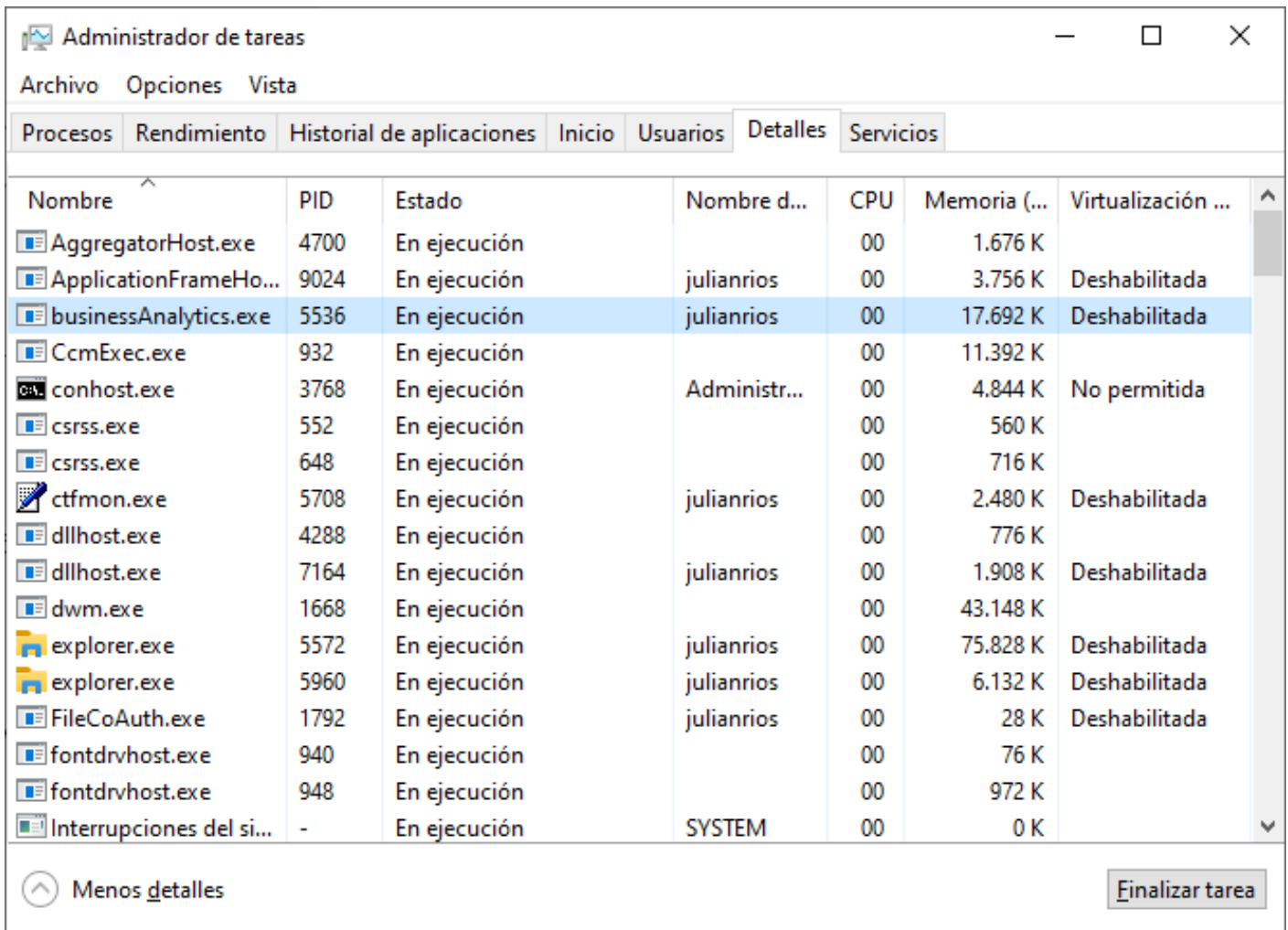
PS C:\Windows\system32>
```

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**.



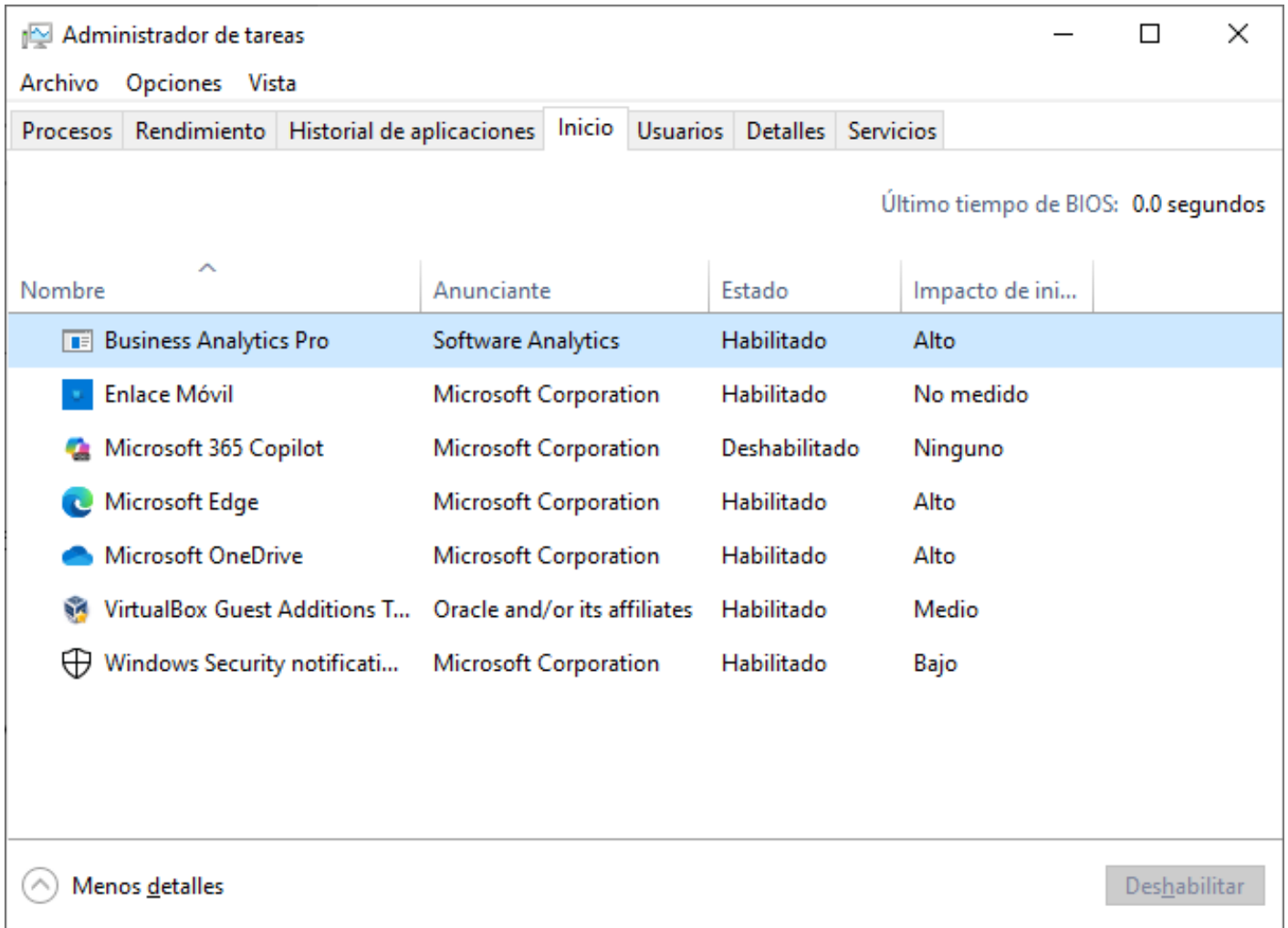
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00	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	

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.

Crear paquete para actualización

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

Endpoint Central

Home Configurations Threats & Patches Software Deployment Inventory MDM Admin Agent

Jump to SDP

Packages > Windows Package Creation

Enter Package Details

Package Name * Business Analytics 3.2.0

Package Type MSI / MSP EXE / APPX / MSIEXEC / MSU

License Type * Commercial

Locate installable From Shared Folder From Local Computer

1 file(s) added (Click or drop to add more) Browse

✓ endpointInstaller-v3.2.0.msi

All (1) file are uploaded

[.z, .zip, .gzip, .bzip2, and .tar files will be extracted automatically. Total file size limit is 12 GB.]

Safeguard sensitive information
Ensure sensitive information (e.g., password, license keys) is not included in command line arguments, as the software package may be reused by other users.

Installation Uninstallation Advanced Settings Watch Demo Real world scenarios for pre/post activities

1 Installation Details

2 Pre-Deployment Activities +

3 Post-Deployment Activities +

MSI / MSP File Name * endpointInstaller-v3.2.0.msi

MST File Name

MSI / MSP Properties for installation

Disable Uninstall option in Add/Remove Programs

Add Package Cancel

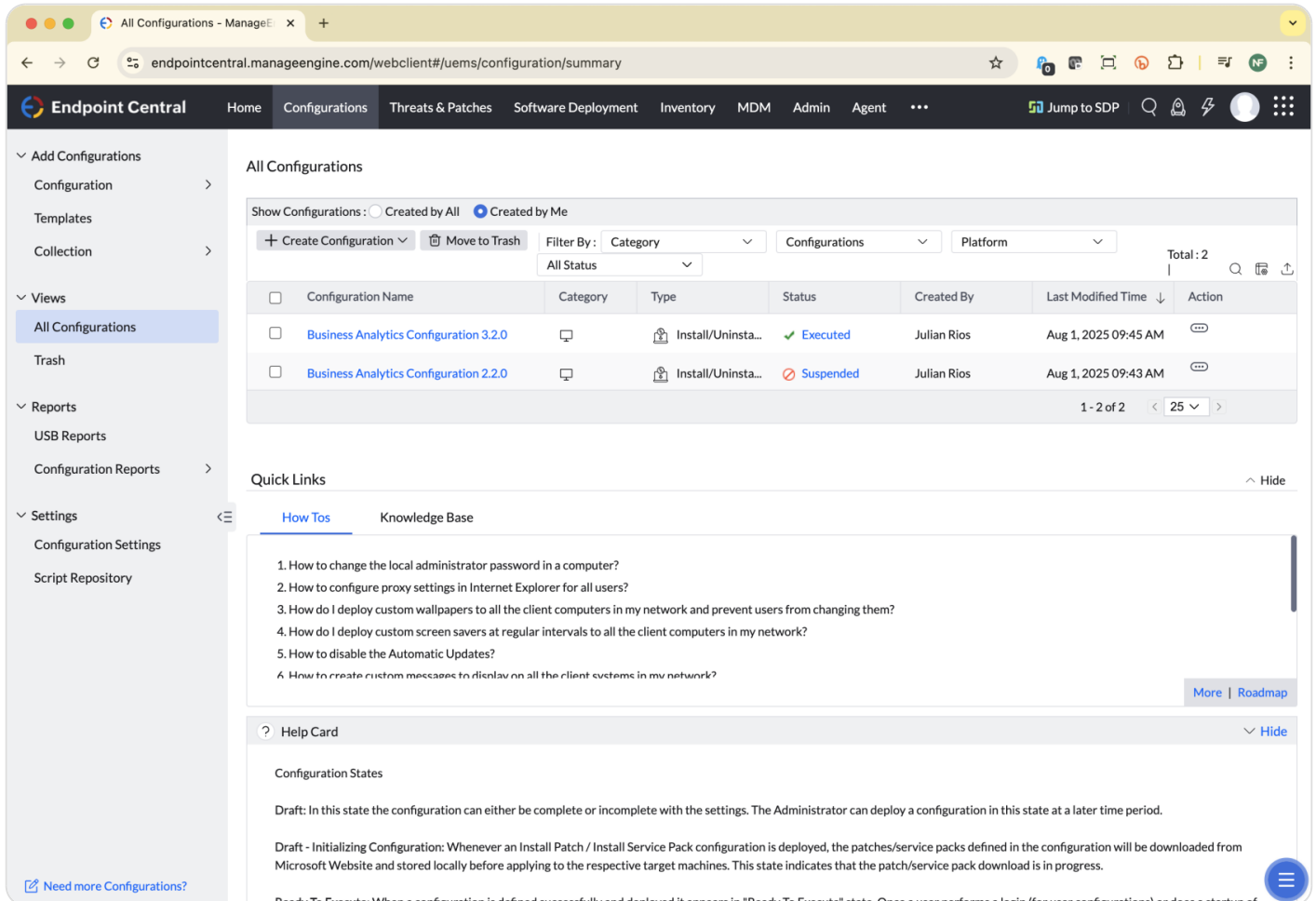
En **Package Name** escribir **Business Analytics 3.2.0** (o la versión actual), en **Package Type** escoger **MSI/MSP**, en **Locate Installable** escoger **From Local Computer** y subir el archivo MSI del agente, en **MSI/MSP File Name** escribir exactamente el nombre del archivo MSI que acaba de subir,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

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

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

Suspender version anterior

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



The screenshot shows the 'All Configurations' page in the Endpoint Central web interface. The page displays a table of configurations with columns for Configuration Name, Category, Type, Status, Created By, Last Modified Time, and Action. Two configurations are listed: 'Business Analytics Configuration 3.2.0' (Executed) and 'Business Analytics Configuration 2.2.0' (Suspended). The 'Suspended' status is highlighted in red. Below the table, there are 'Quick Links' and a 'Help Card' section.

Configuration Name	Category	Type	Status	Created By	Last Modified Time	Action
Business Analytics Configuration 3.2.0	Computer	Install/Uninstall	Executed	Julian Rios	Aug 1, 2025 09:45 AM	...
Business Analytics Configuration 2.2.0	Computer	Install/Uninstall	Suspended	Julian Rios	Aug 1, 2025 09:43 AM	...

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

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.

Configuración para la actualización

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

The screenshot shows the Endpoint Central web interface for configuring 'Install/Uninstall Windows Software'. The page is divided into several sections:

- Name and Description:** The 'Name' field is set to 'Business Analytics Configuration 3.2.0'. There is a link for 'Add Description'.
- Package Settings:** The 'Operation Type' is set to 'Install' (radio button selected). The 'Package Name' is 'Business Analytics 3.2.0' with a 'Modify Package' link.
- Configure Install/Uninstall options:** The 'Install As' section has 'System User' selected (radio button). There is an option for 'Run As User' and a checkbox for 'Allow User to interact with the Installation/Uninstallation Window' which is currently unchecked.
- Deployment Settings:** The 'Apply Deployment Policy' is set to 'Deploy any time at the earliest'. There are links for 'View Details' and 'Create/Modify/Save As Policy'.
- Define Target:** A target named 'Target 1' is defined with 'Remote Office' set to 'Default Remote Office' and 'Filter Computers based on' set to 'Computer' with the value 'DESKTOP-ADKVAU0'. There is an 'Exclude Target' section with 'Domain' set to 'Select'.

At the bottom left, there is a link 'Need more Configurations?' and at the bottom right, there is a 'Help' button.

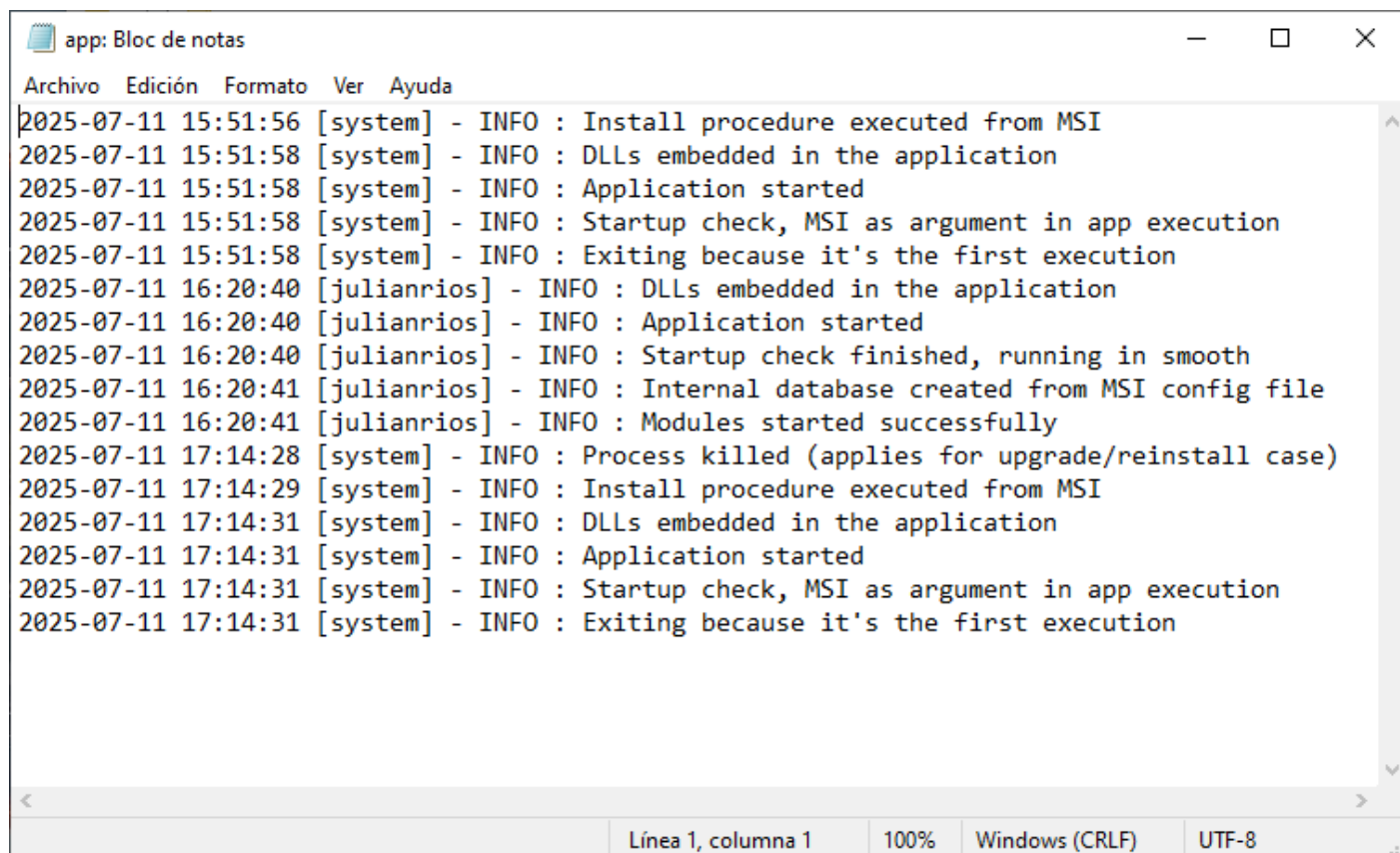
En **Name** escriba **Business Analytics Configuration 3.2.0** (o el nombre que prefiera), en **Operation Type** seleccione **Install**, en **Install As** seleccione **System User** y en **Target** seleccione el grupo objetivo de PCs que serán objeto de la metodología antifraude.

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

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.



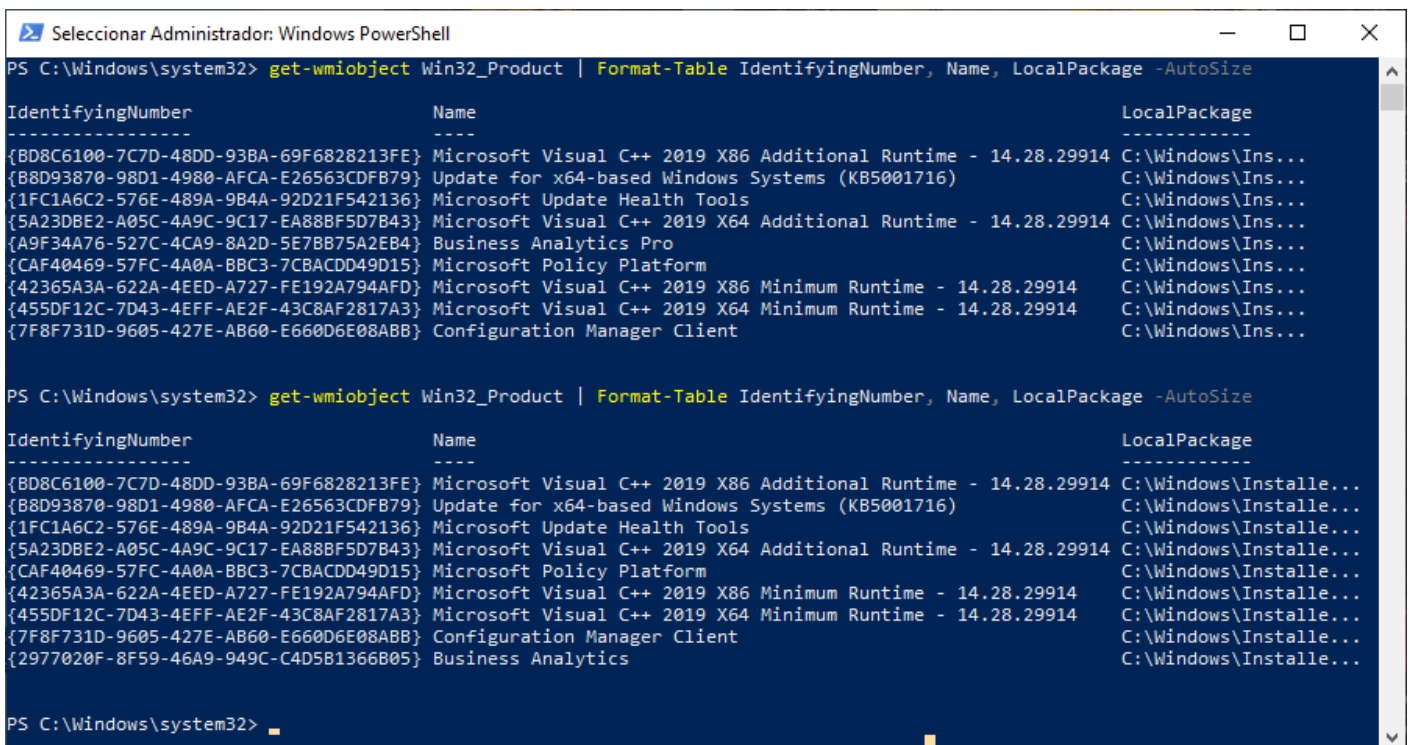
```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup 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
Línea 1, columna 1 100% Windows (CRLF) UTF-8
```

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

PowerShell para verificar actualización

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

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



```
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...

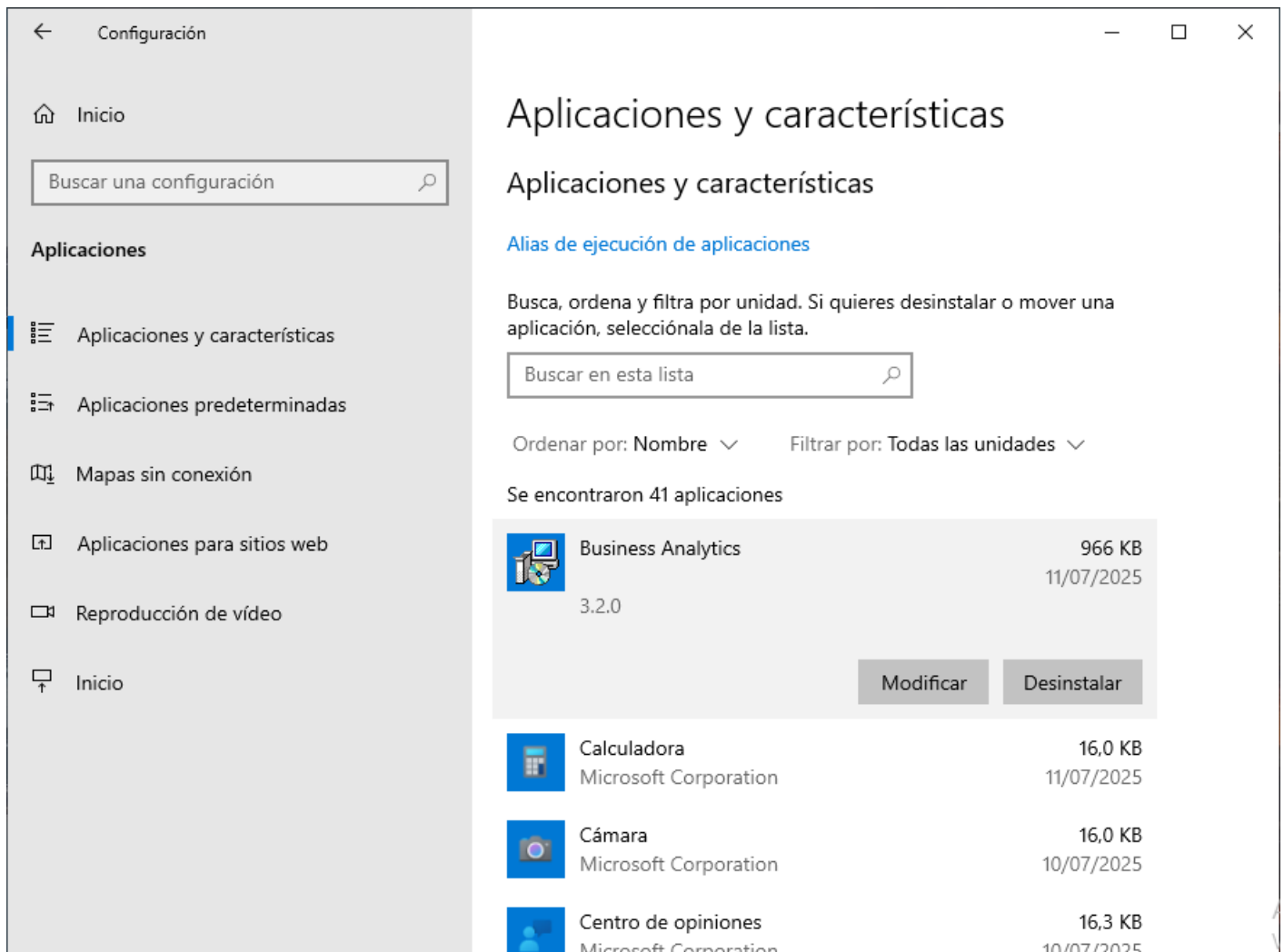
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
IdentifyingNumber      Name                                          LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 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-C4D5B1366805} Business Analytics C:\Windows\Installe...
```

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.

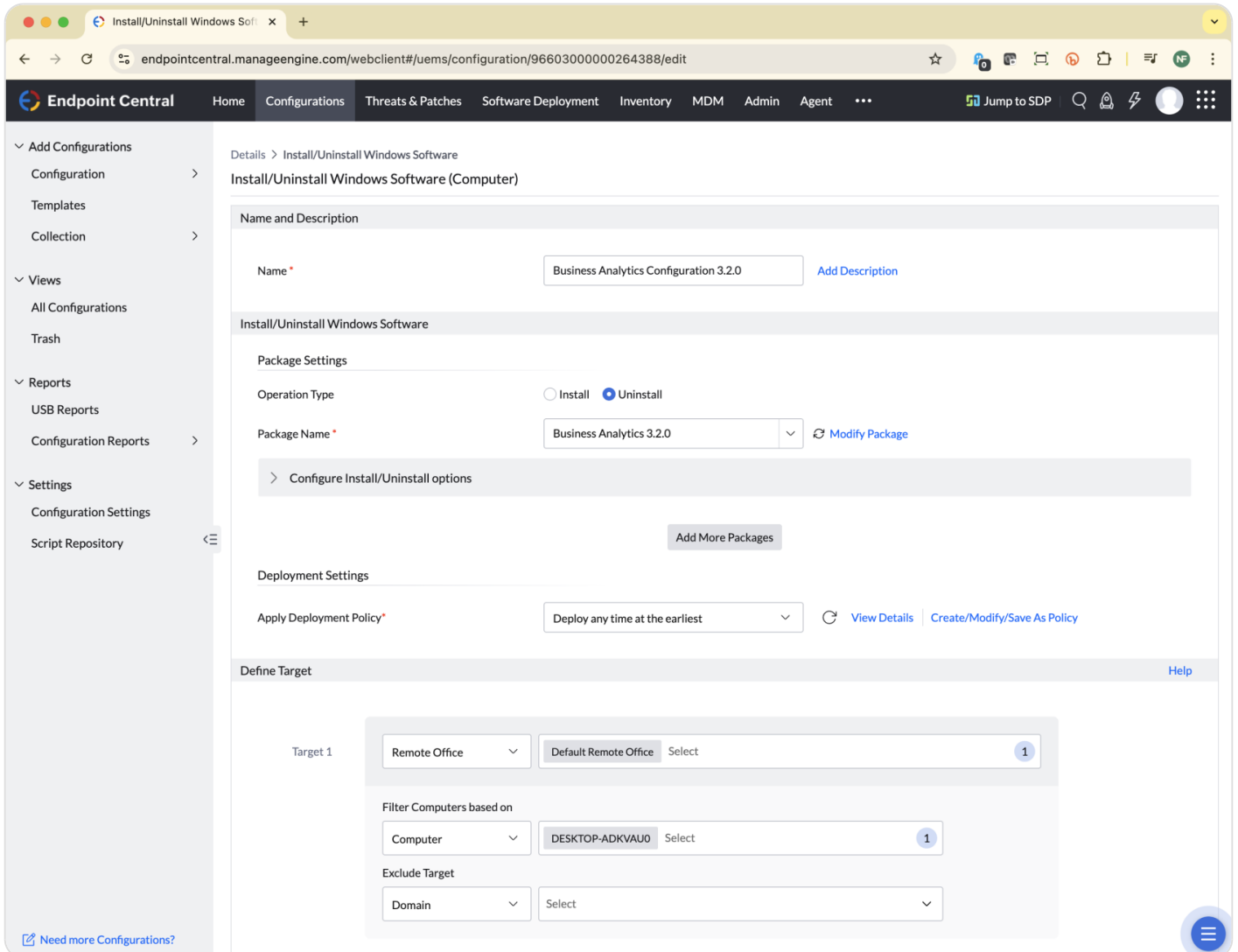


Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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

Desinstalación del agente

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



The screenshot displays the Endpoint Central web interface for configuring software deployment. The main content area is titled "Install/Uninstall Windows Software (Computer)".

- Name and Description:** The "Name" field is set to "Business Analytics Configuration 3.2.0".
- Package Settings:**
 - Operation Type:** The "Uninstall" radio button is selected.
 - Package Name:** Set to "Business Analytics 3.2.0".
 - A button labeled "Configure Install/Uninstall options" is visible.
 - An "Add More Packages" button is located below the package name field.
- Deployment Settings:**
 - Apply Deployment Policy:** Set to "Deploy any time at the earliest".
 - Buttons for "View Details" and "Create/Modify/Save As Policy" are present.
- Define Target:**
 - Target 1:** Includes a "Remote Office" dropdown set to "Default Remote Office" and a "Filter Computers based on" dropdown set to "Computer" with "DESKTOP-ADKVAU0" selected.
 - An "Exclude Target" dropdown is set to "Domain".

A "Need more Configurations?" link is visible in the bottom left corner, and a help icon is in the bottom right corner.

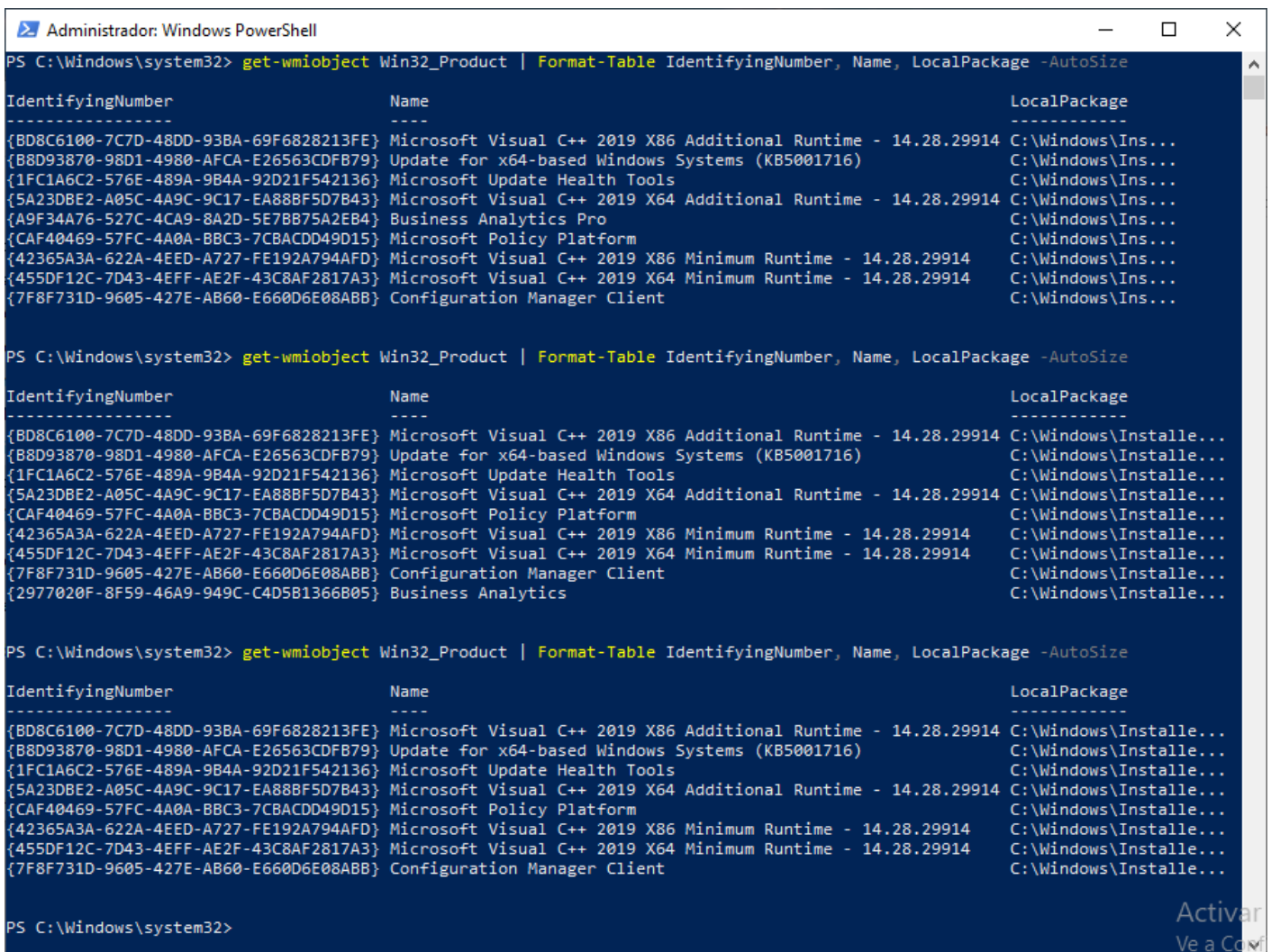
De clic en el botón **Deploy Immediately** y esto desinstalará la última versión del agente en los computadores.

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-C4D5B1366805} 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 configuración de desinstalación en **Endpoint Central**, ya no aparece la aplicación Business Analytics.