

Despliegue con Microsoft Intune

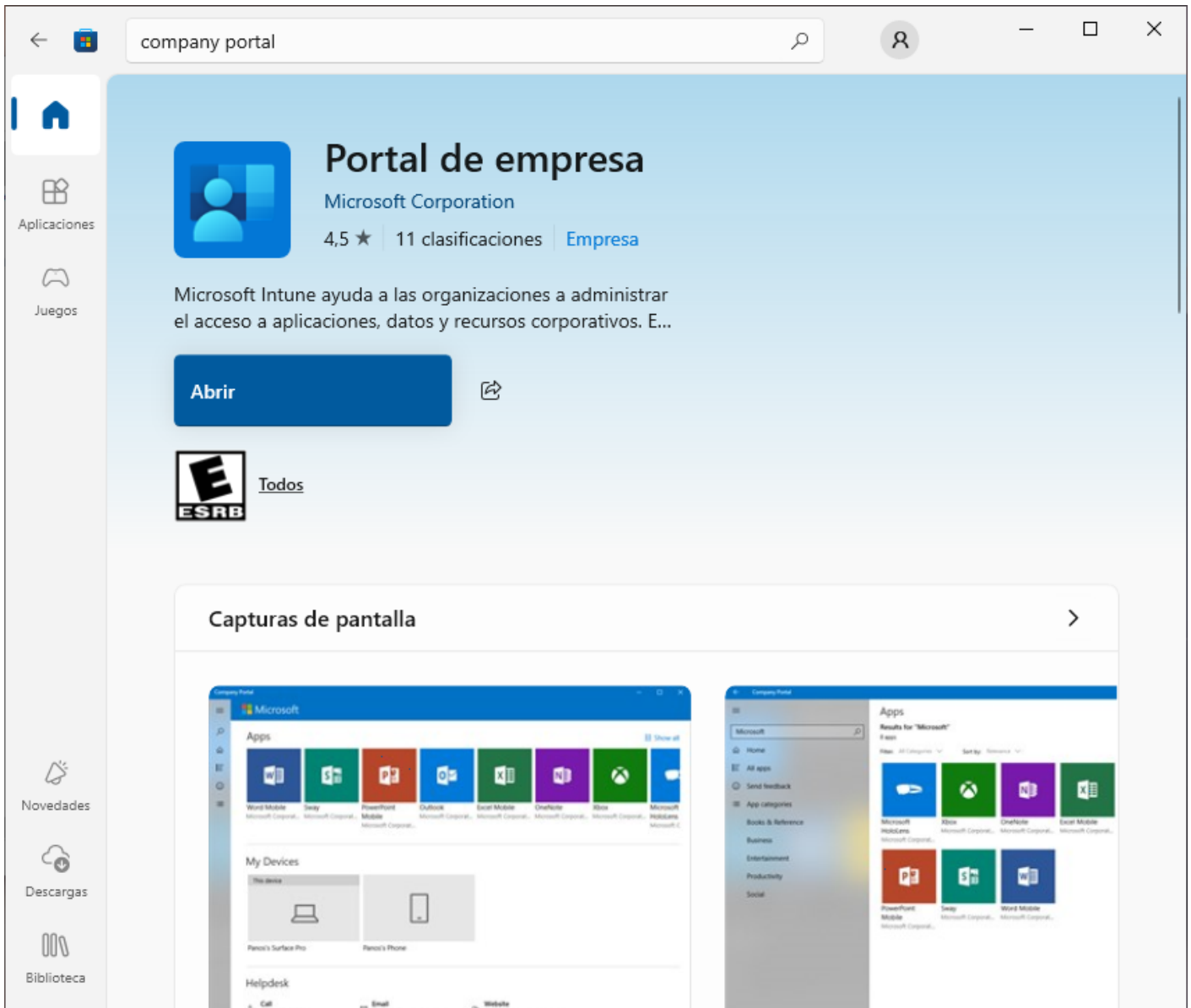
Uso de Microsoft Intune en la nube como MDM para el despliegue del agente en los dispositivos de la organización.

- [Requisitos previos](#)
- [Video con todos los pasos](#)
- [Preparación de carpetas y archivos](#)
- [Empaquetado del agente](#)
- [Creación del paquete IntuneWin](#)
- [Creación de una aplicación](#)
- [Añadir el paquete IntuneWin](#)
- [Información de la aplicación](#)
- [Comando de instalación](#)
- [Requisitos de instalación](#)
- [Regla de detección](#)
- [Asignación de usuarios o máquinas](#)
- [Sincronización de dispositivo](#)
- [Sincronizar cliente Windows](#)
- [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
- Carpeta para actualizar el agente
- Paquete de actualización
- Aplicación para la actualización
- Seleccionar paquete de actualización
- Información de actualización
- Comandos de actualización
- Requerimientos de actualización
- Reglas de detección
- Supersedencia
- Asignaciones para actualización
- Eliminar asignaciones antiguas
- Sincronización de dispositivo
- Sincronizar cliente Windows
- Verificación de la actualización
- PowerShell para verificar actualización
- Actualización en listado de Aplicaciones
- Desinstalación del agente
- Asignación de desinstalación
- Sincronización de dispositivo
- Sincronizar cliente Windows
- Verificación de la desinstalación

Requisitos previos

Su organización debe tener **Microsoft Intune** previamente configurado y con las licencias para los usuarios y/o dispositivos. cada computador debe tener por consiguiente la aplicación **Company Portal** y debe estar correctamente enrolado.



Debe contar con la capacidad de realizar acciones administrativas en **Microsoft Intune** 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.

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/pXzID59q4gs?si=GTaV-4JDDI3Z9Eym>

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

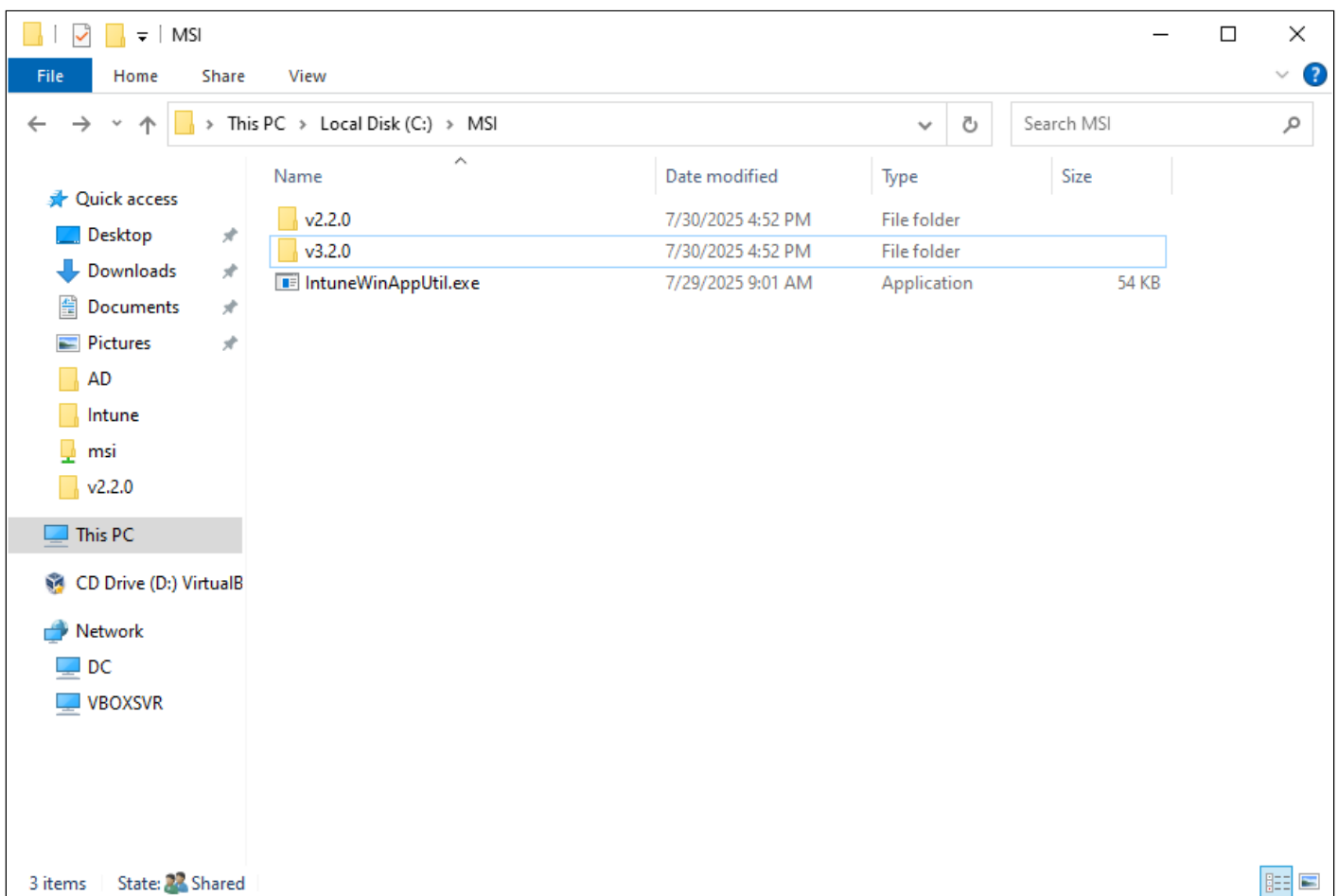
The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Preparación de carpetas y archivos

Microsoft Intune necesita que le proveamos un paquete de instalación (archivo .intunewin) para poder desplegar un MSI (nuestro agente) y ese paquete lo vamos a crear primero estructurando su contenido.

En un computador cualquiera con Windows, cree una carpeta con nombre **MSI** en la unidad raíz, en ella cree una carpeta llamada **v2.2.0** (esta es la versión del agente que vamos a instalar). En el directorio **MSI** descargue la utilidad **WinApp** de Intune de la URL:

```
https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool/raw/master/IntuneWinAppUtil.exe
```

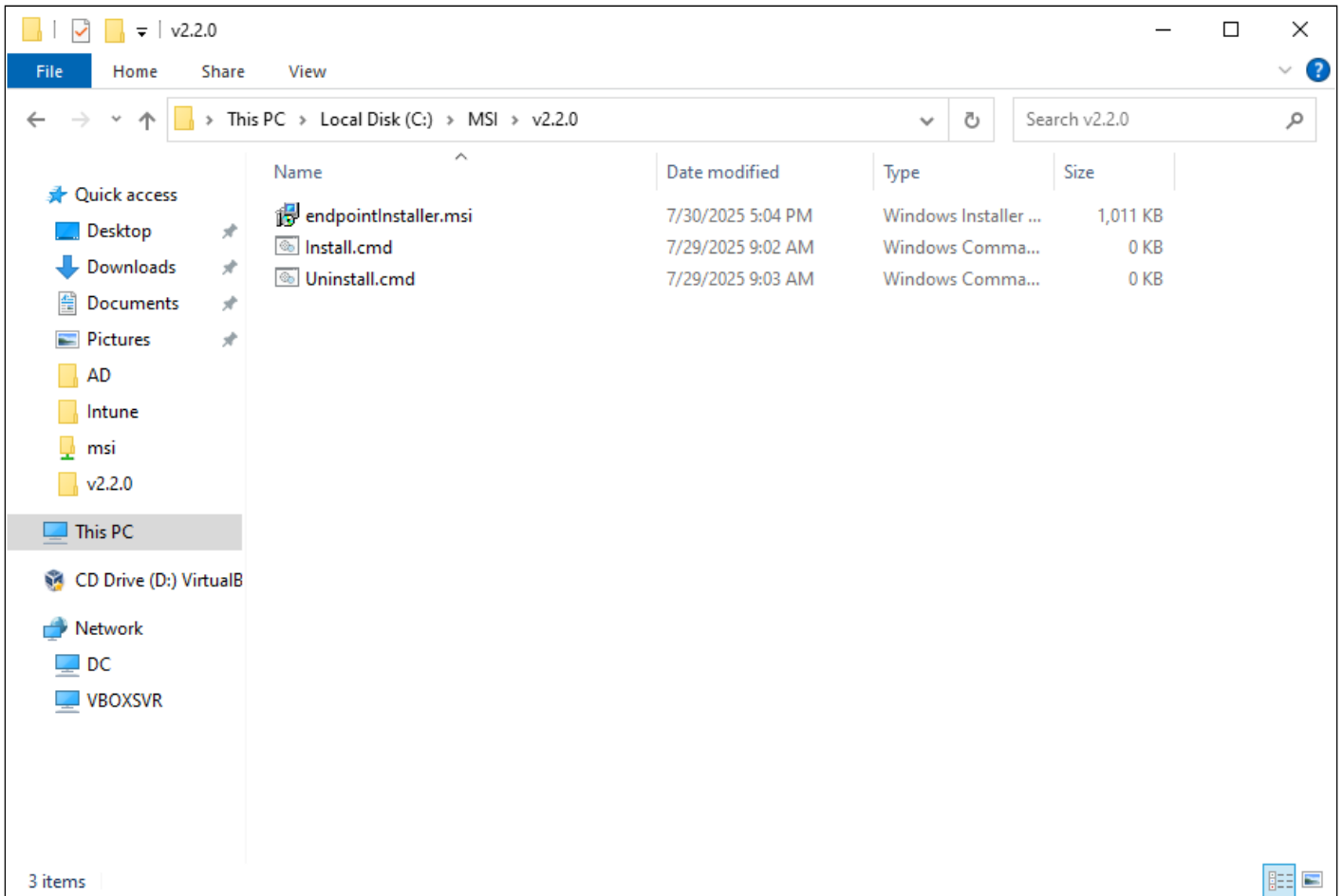


Al final la estructura de carpetas debe lucir así, con una carpeta **MSI** en la raíz y dentro de ella una carpeta **v2.2.0** y el archivo ejecutable **IntuneWinAppUtil.exe**. Si este paso se hizo correctamente ya estamos listos para continuar.

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

Empaquetado del agente

En la carpeta que se creó con nombre **v2.2.0**, coloque el agente **endpointInstaller.msi** y cree dos archivos en blanco, uno llamado **Install.cmd** y otro **Uninstall.cmd**.



Esta estructura es necesaria para crear el empaquetado que soporta **Microsoft Intune**. Si esto está listo, podemos continuar con el siguiente paso.

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

Creación del paquete IntuneWin

Abra una consola **MS-DOS** y navegue hasta la carpeta raíz **MSI**. Una vez allí ejecute el comando:

```
IntuneWinAppUtil.exe
```

Este comando ejecuta la utilidad de **Microsoft Intune** que creará el paquete de instalación con extensión `.intunewin`, compatible con la metodología de despliegue de este producto. Cuando se le pregunte por el **source folder** escriba `v2.2.0`, cuando se le pregunte por el **setup file** escriba `Install.cmd`, cuando se le pregunte por el **output folder** escriba un punto y cuando se le pregunte por el **catalog folder** escriba `N`.

```
Administrator: Command Prompt
C:\MSI>IntuneWinAppUtil.exe
Please specify the source folder: v2.2.0
Please specify the setup file: Install.cmd
Please specify the output folder: .
Do you want to specify catalog folder (Y/N)?N
INFO Validating parameters
INFO Validated parameters within 7 milliseconds
INFO Compressing the source folder 'v2.2.0' to 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO Calculated size for folder 'v2.2.0' is 1035264 within 1 milliseconds
INFO Compressed folder 'v2.2.0' successfully within 79 milliseconds
INFO Checking file type
INFO Checked file type within 13 milliseconds
INFO Encrypting file 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 19 milliseconds
INFO Computing SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\c0262001-b7c8-4e5e-bfeb-9d42734ede53
INFO Computed SHA256 hash for 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\c0262001-b7c8-4e5e-bfeb-9d42734ede53' within 22 milliseconds
INFO Computing SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin
INFO Computed SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin within 18 milliseconds
INFO Copying encrypted file from 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\c0262001-b7c8-4e5e-bfeb-9d42734ede53' to 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO File 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 10 milliseconds
INFO Generating detection XML file 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage\Metadata\Detection.xml'
INFO Generated detection XML file within 32 milliseconds
INFO Compressing folder 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage' to '.\Install.intunewin'
INFO Calculated size for folder 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage' is 674174 within 0 milliseconds
INFO Compressed folder 'C:\Users\Administrator\AppData\Local\Temp\7da198fe-8ec6-4678-97ac-b5215af6ab75\IntuneWinPackage' successfully within 54 milliseconds
INFO Removing temporary files
INFO Removed temporary files within 12 milliseconds
INFO File '.\Install.intunewin' has been generated successfully

[=====] 100%
INFO Done!!!

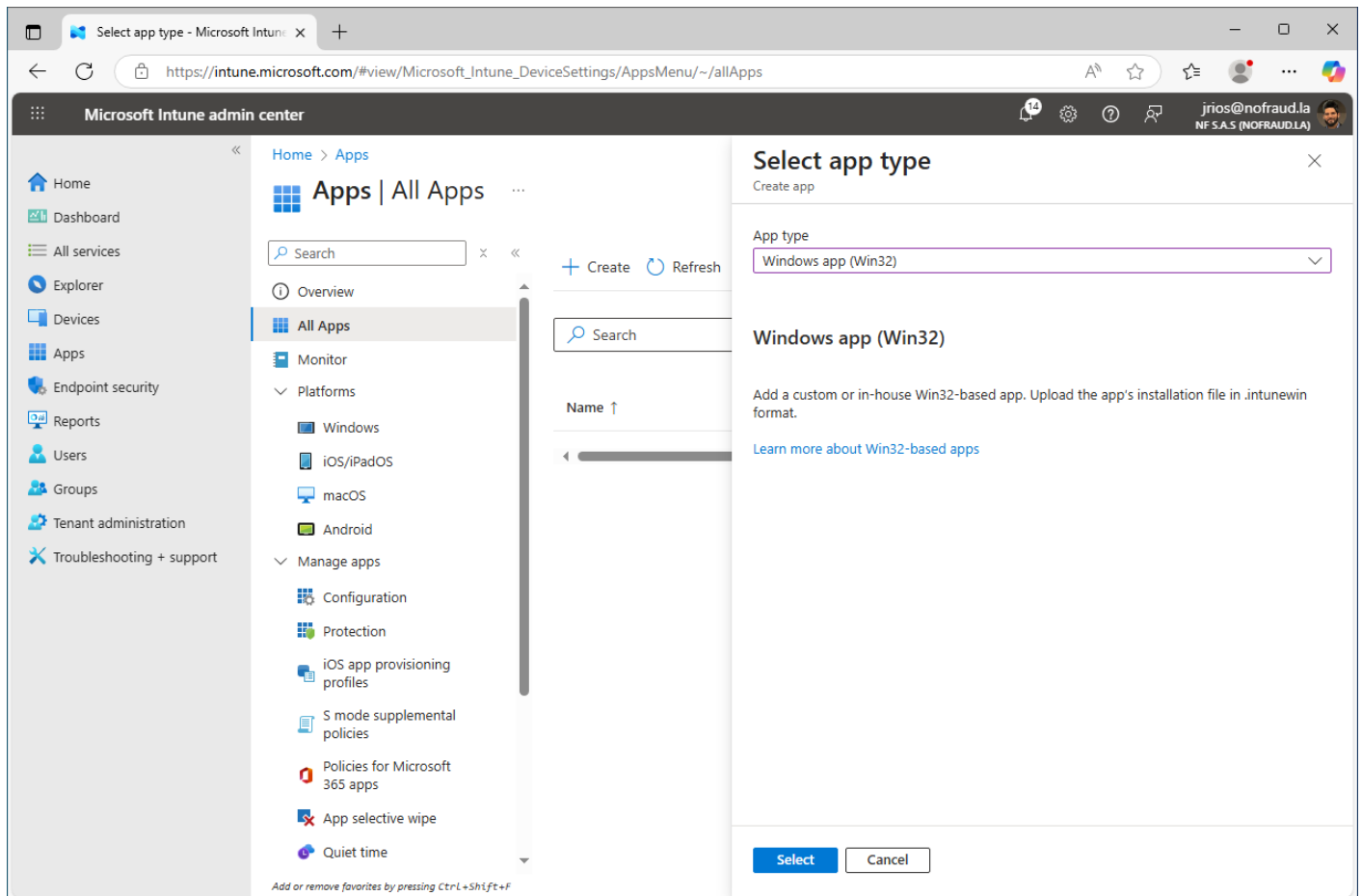
C:\MSI>
```

Esto creará un archivo llamado **Install.intunewin** en la carpeta **MSI**. Este archivo es el paquete de instalación compatible con **Microsoft Intune** de nuestro agente en su versión 2.2.0. Renombre este archivo a **endpointInstaller-v2.2.0.intunewin** para mayor recordación.

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

Creación de una aplicación

Ingresa a la consola administrativa de **Microsoft Intune**. Una vez allí, en la parte izquierda seleccione **Apps**, luego **All Apps** y de clic en **Create**.

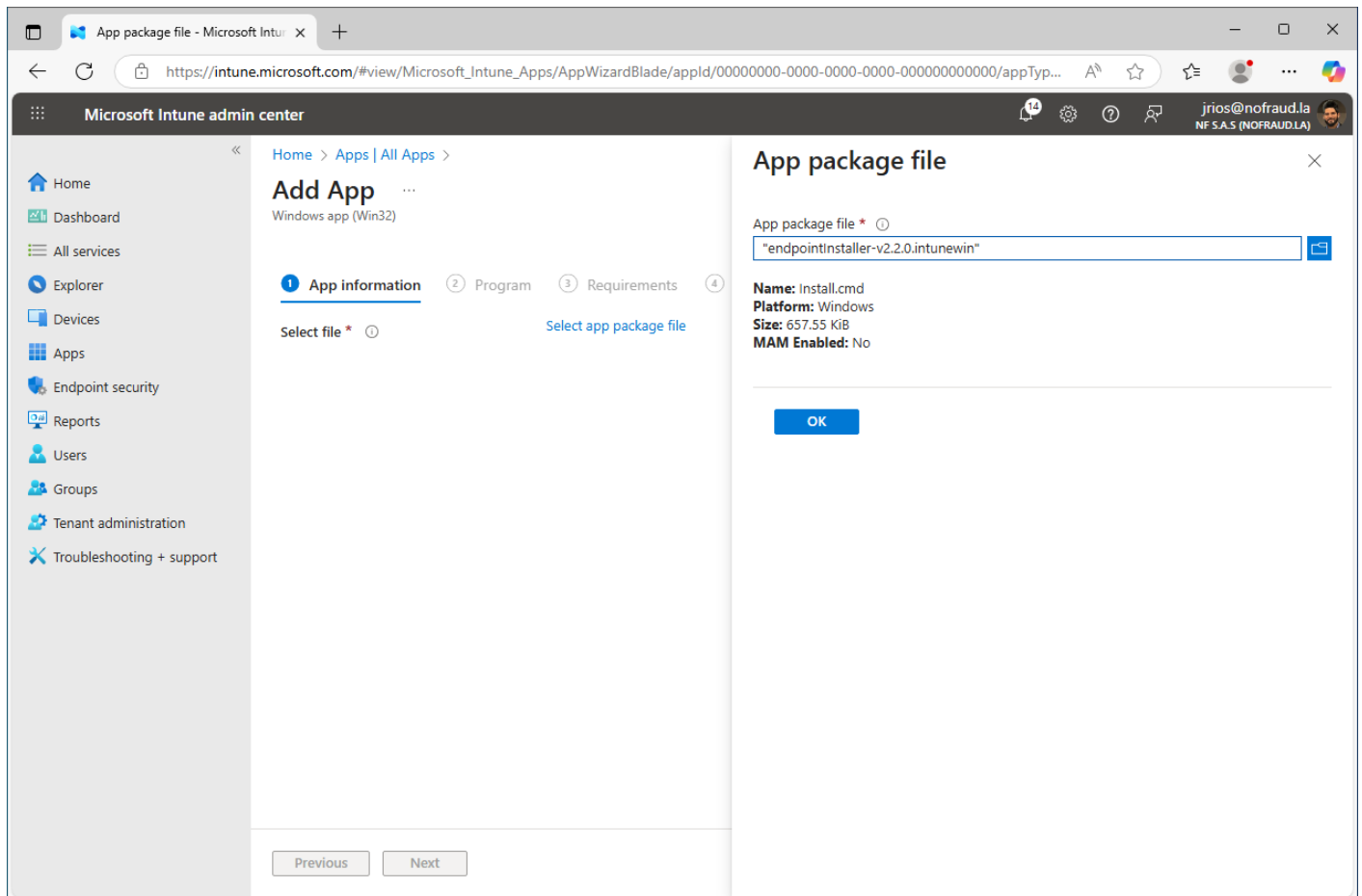


Luego seleccione el tipo de aplicación **Windows app (Win32)** y de clic en el botón **Select**.

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

Añadir el paquete IntuneWin

Navegue en sus archivos y carpetas para seleccionar el archivo **endpointInstaller-v2.2.0.intunewin** y añádalo como paquete de instalación.

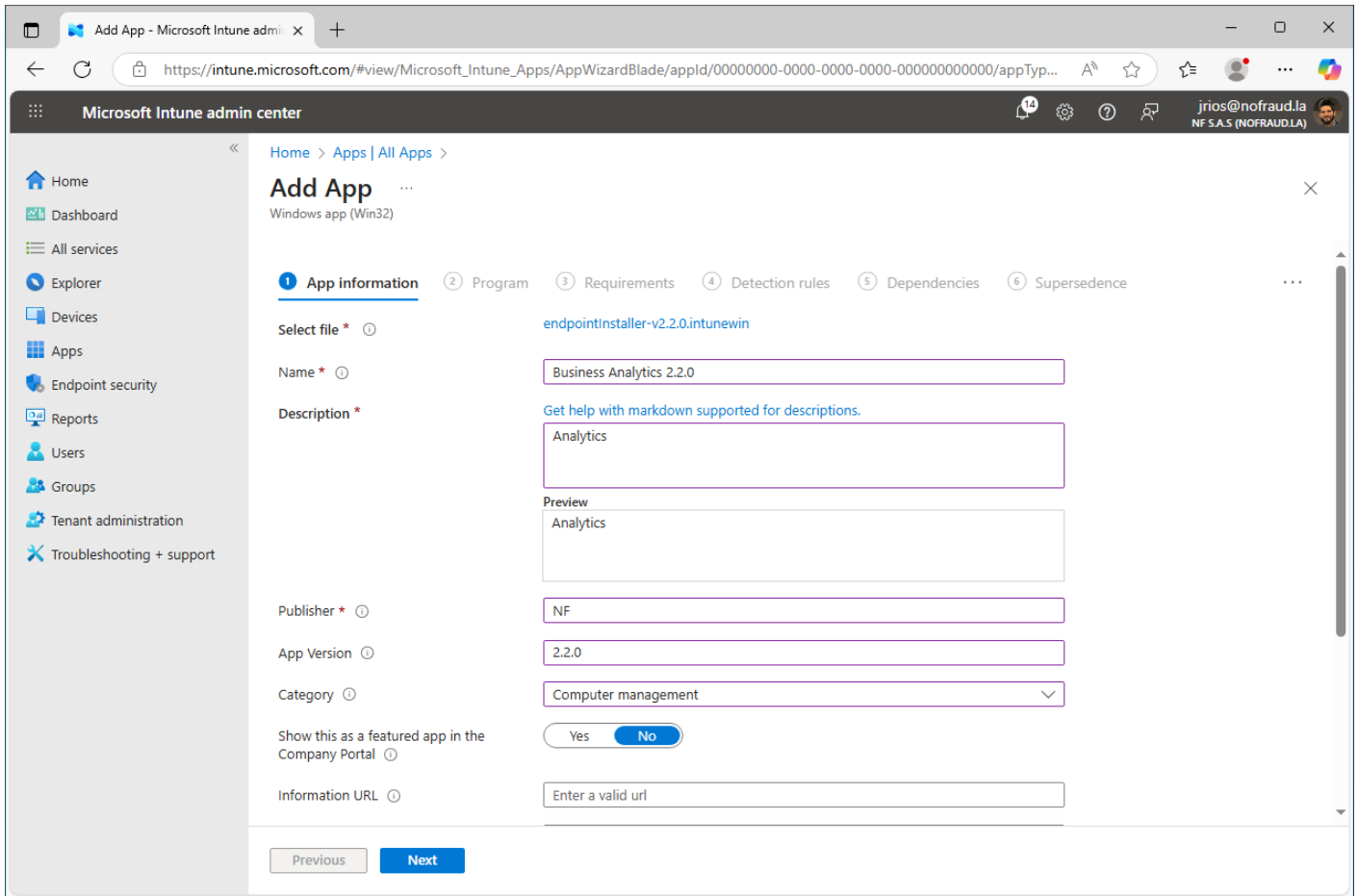


Automáticamente se detectará que el paquete es válido y corresponde al formato propietario de **Microsoft intune**.

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

Información de la aplicación

Escriba el nombre Business Analytics y llene la descripción y otros campos con datos informativos.



The screenshot shows the 'Add App' wizard in the Microsoft Intune Admin Center. The 'App information' step is selected, and the following fields are filled:

- Select file: endpointinstaller-v2.2.0.intunewin
- Name: Business Analytics 2.2.0
- Description: Analytics
- Preview: Analytics
- Publisher: NF
- App Version: 2.2.0
- Category: Computer management
- Show this as a featured app in the Company Portal: No
- Information URL: Enter a valid url

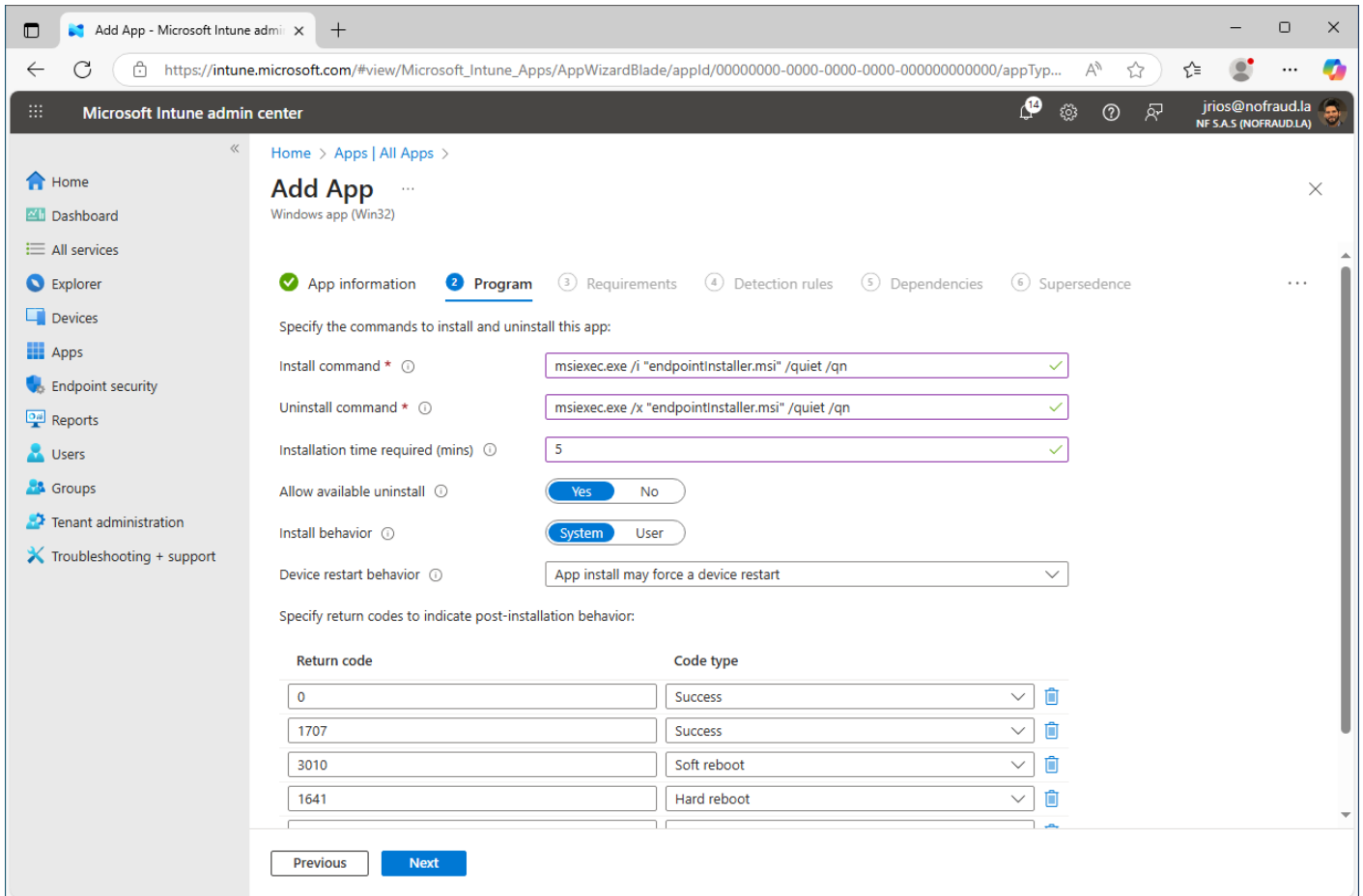
Navigation buttons 'Previous' and 'Next' are visible at the bottom.

Asegúrese de que la opción de **mostrar esta aplicación en el portal de empresa** esté deshabilitada.

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

Comando de instalación

Escriba el comando de instalación y desinstalación como se muestra en la imagen. Asegúrese de que endpointInstaller.msi esté dentro de comillas dobles.



Microsoft Intune admin center

Home > Apps | All Apps >

Add App

Windows app (Win32)

App information **2 Program** 3 Requirements 4 Detection rules 5 Dependencies 6 Supersede

Specify the commands to install and uninstall this app:

Install command *

Uninstall command *

Installation time required (mins)

Allow available uninstall Yes No

Install behavior System User

Device restart behavior

Specify return codes to indicate post-installation behavior:

Return code	Code type
<input type="text" value="0"/>	<input type="text" value="Success"/>
<input type="text" value="1707"/>	<input type="text" value="Success"/>
<input type="text" value="3010"/>	<input type="text" value="Soft reboot"/>
<input type="text" value="1641"/>	<input type="text" value="Hard reboot"/>

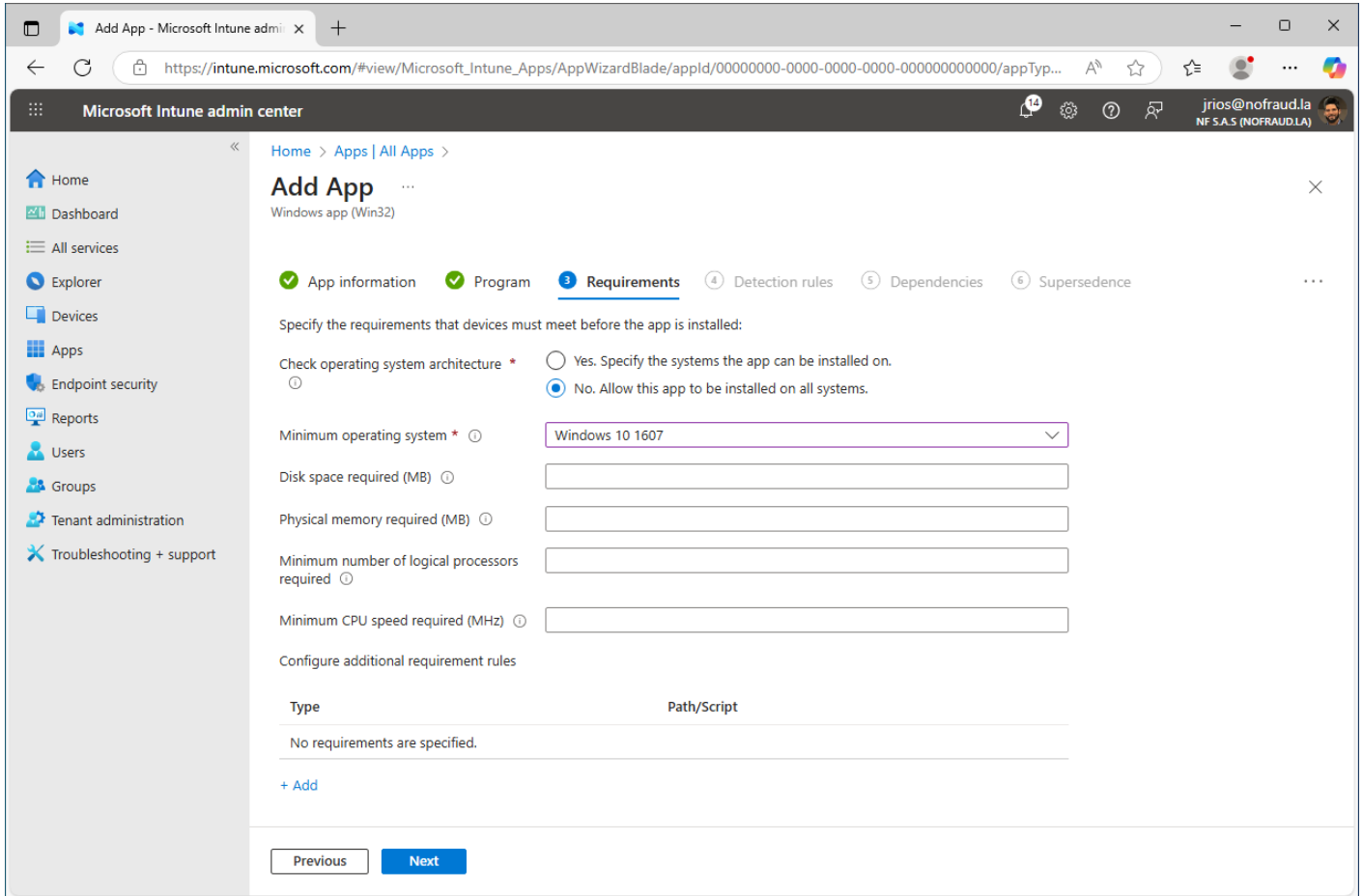
Previous Next

Cambie a 5 minutos el tiempo necesario de instalación para la aplicación y asegúrese de que el **Install Behavior** este marcado en **System**.

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

Requisitos de instalación

Microsoft Intune requiere que se le especifique cuál es la versión del sistema operativo compatible con nuestra aplicación. En este caso elegimos Windows 10 en su versión 1607, que es la versión mínima que soporta **Microsoft Intune**.



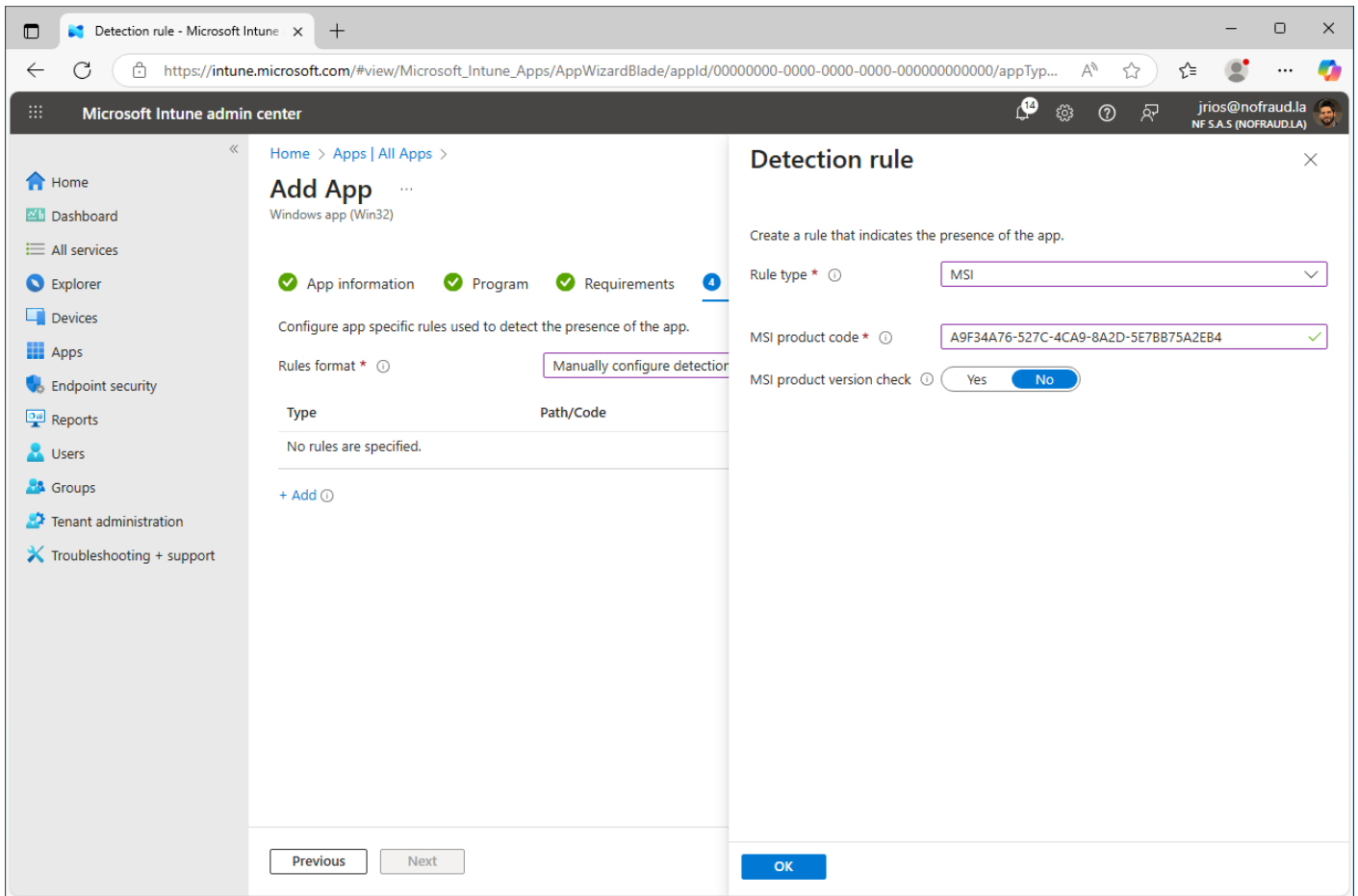
The screenshot shows the 'Add App' wizard in the Microsoft Intune Admin Center, specifically the 'Requirements' step. The wizard is for a 'Windows app (Win32)'. The 'Requirements' step is highlighted with a blue circle and the number '3'. The wizard has six steps: 1. App information, 2. Program, 3. Requirements, 4. Detection rules, 5. Dependencies, and 6. Supersedeance. The 'Requirements' step is currently active. The wizard asks to specify the requirements that devices must meet before the app is installed. There are two radio buttons for 'Check operating system architecture': 'Yes. Specify the systems the app can be installed on.' (unselected) and 'No. Allow this app to be installed on all systems.' (selected). Below this, there are several input fields: 'Minimum operating system' (set to 'Windows 10 1607'), 'Disk space required (MB)', 'Physical memory required (MB)', 'Minimum number of logical processors required', and 'Minimum CPU speed required (MHz)'. At the bottom, there is a table for 'Configure additional requirement rules' with columns for 'Type' and 'Path/Script'. The table is currently empty, with the text 'No requirements are specified.' below it. There is a '+ Add' button below the table. At the bottom of the wizard, there are 'Previous' and 'Next' buttons.

Se deja en blanco cualquier otra información, como espacio en disco, memoria o procesadores y se da clic en **Next**.

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

Regla de detección

La regla de detección se usa para que Microsoft Intune pueda identificar si la aplicación está instalada o no en los computadores. En esta ocasión se debe seleccionar que la regla estará basada en el código del producto del MSI del agente antifraude.



The screenshot shows the Microsoft Intune admin center interface. The main content area is titled "Add App" and is for a "Windows app (Win32)". The "Requirements" step is selected, and the "Detection rule" dialog is open. The dialog contains the following fields:

- Rule type: MSI
- MSI product code: A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4
- MSI product version check: No

The dialog also includes a "Manually configure detection" link and an "OK" button at the bottom right.

Para saber cuál es el código del producto, puede usar la herramienta **Microsoft Orca**, aunque en NOFRAUD se le entregará toda esta información a la hora de iniciar el proyecto.

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

Asignación de usuarios o máquinas

Existen 3 secciones en las asignaciones, una llamada **Required**, otra llamada **Available for enrolled devices** y otra **Uninstall**. Dependiendo de la operación a realizar, se agregan usuarios o máquinas a una de ellas. En este caso, se agregarán todas las máquinas a la categoría **Required** porque se requiere que esta aplicación se instale en todas las máquinas.

The screenshot shows the Microsoft Intune Admin Center interface for adding an application. The 'Assignments' tab is active, displaying a table for 'Required' assignments. The table has the following structure:

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Install
Included	All devices	None	None	Show all toast notifications	As soon as possible	As soon as possible

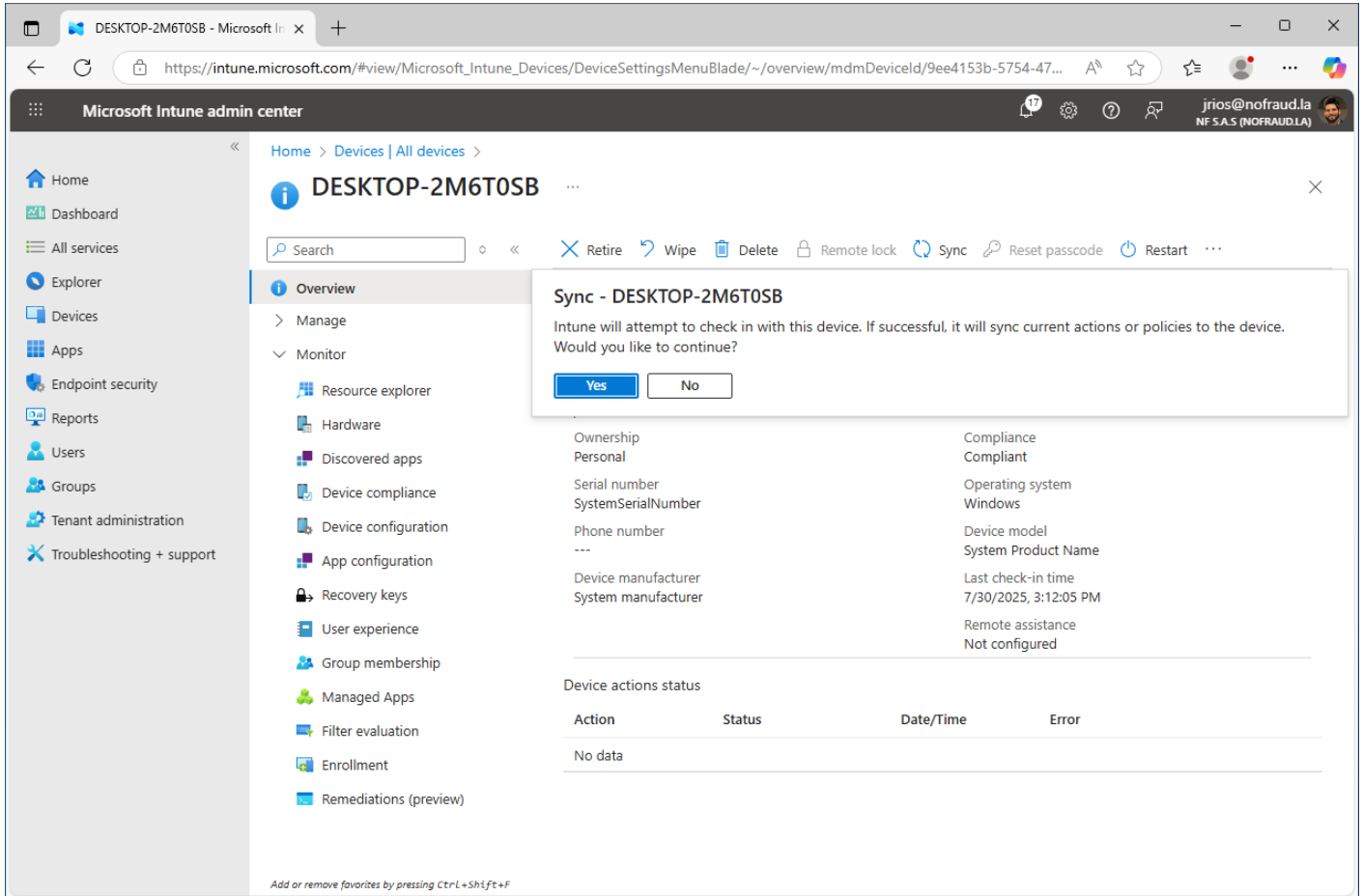
Below the table, there are sections for 'Available for enrolled devices' (currently empty) and 'Uninstall'. Navigation buttons 'Previous' and 'Next' are visible at the bottom.

En su organización podrá suceder que no se quiera desplegar el agente antifraude a todas las máquinas, por ello, deberá crear un grupo y agregar como miembros aquellos dispositivos o usuarios que serán objeto de la metodología antifraude.

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

Sincronización de dispositivo

Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'DESKTOP-2M6T0SB' and includes a search bar and action buttons: Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, and Restart. A 'Sync - DESKTOP-2M6T0SB' dialog box is open, asking for confirmation to sync current actions or policies to the device. Below the dialog, the device's metadata is displayed in two columns:

Ownership	Compliance
Personal	Compliant
Serial number	Operating system
SystemSerialNumber	Windows
Phone number	Device model
---	System Product Name
Device manufacturer	Last check-in time
System manufacturer	7/30/2025, 3:12:05 PM
	Remote assistance
	Not configured

Below the metadata, there is a 'Device actions status' table:

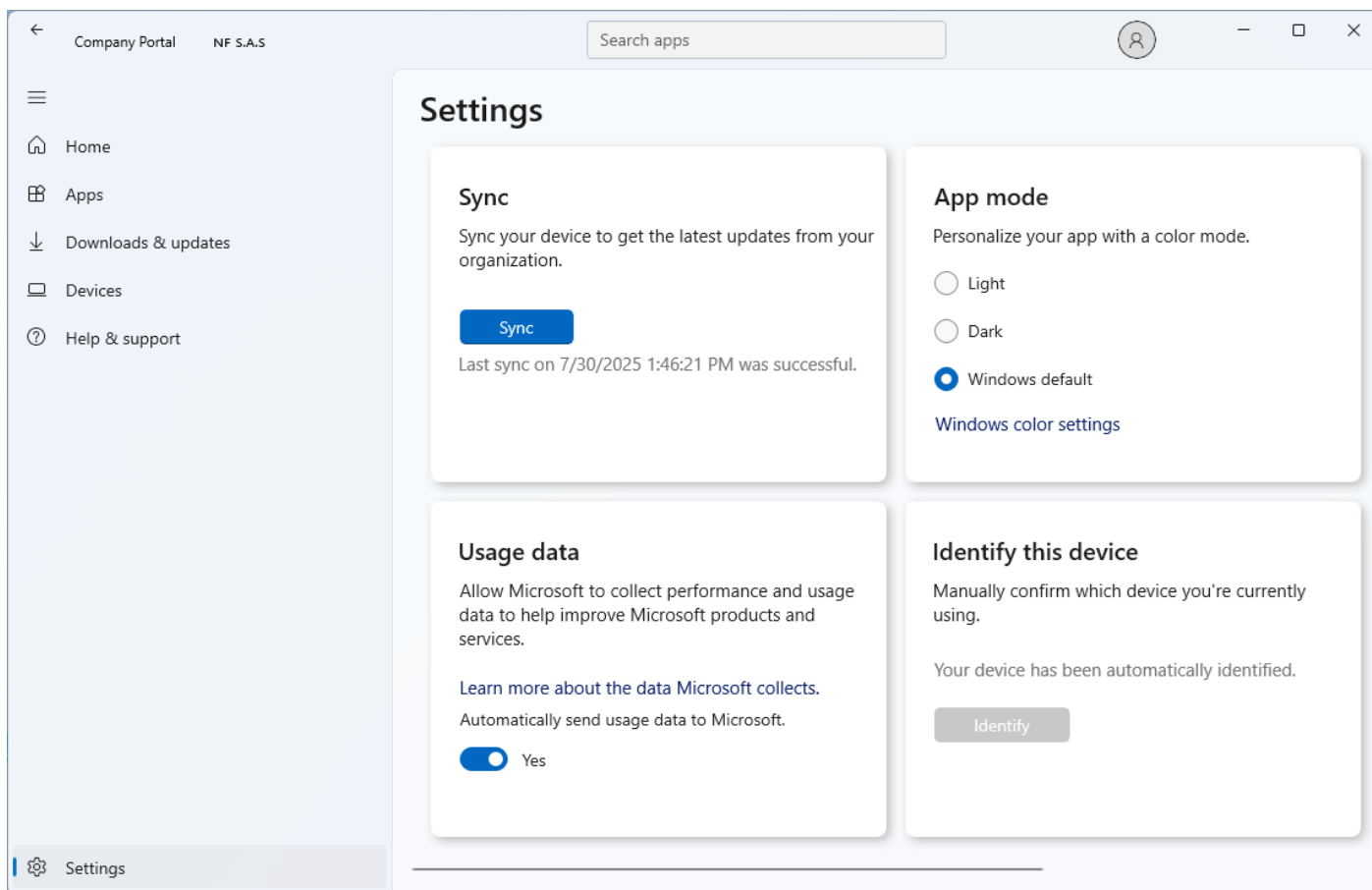
Action	Status	Date/Time	Error
No data			

El siguiente paso será forzar la sincronización del lado de las máquinas.

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

Sincronizar cliente Windows

Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.



Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política e instalará el agente antifraude de manera inmediata en esta máquina.

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

Monitoreo de la instalación

Para monitorear el estado de la instalación, de clic en en **Apps, All Apps** y seleccione **Business Analytics**. Allí aparecerá un gráfico de torta indicando un resumen de las operaciones.

The screenshot displays the Microsoft Intune admin center interface. The main content area shows the details for 'Business Analytics 2.2.0' under 'Client Apps'. The 'Overview' tab is selected, showing a 'Device status' donut chart. The chart indicates that 1 device is installed, 0 are not installed, 0 have failed, 0 are install pending, and 0 are not applicable. The total number of devices is 1.

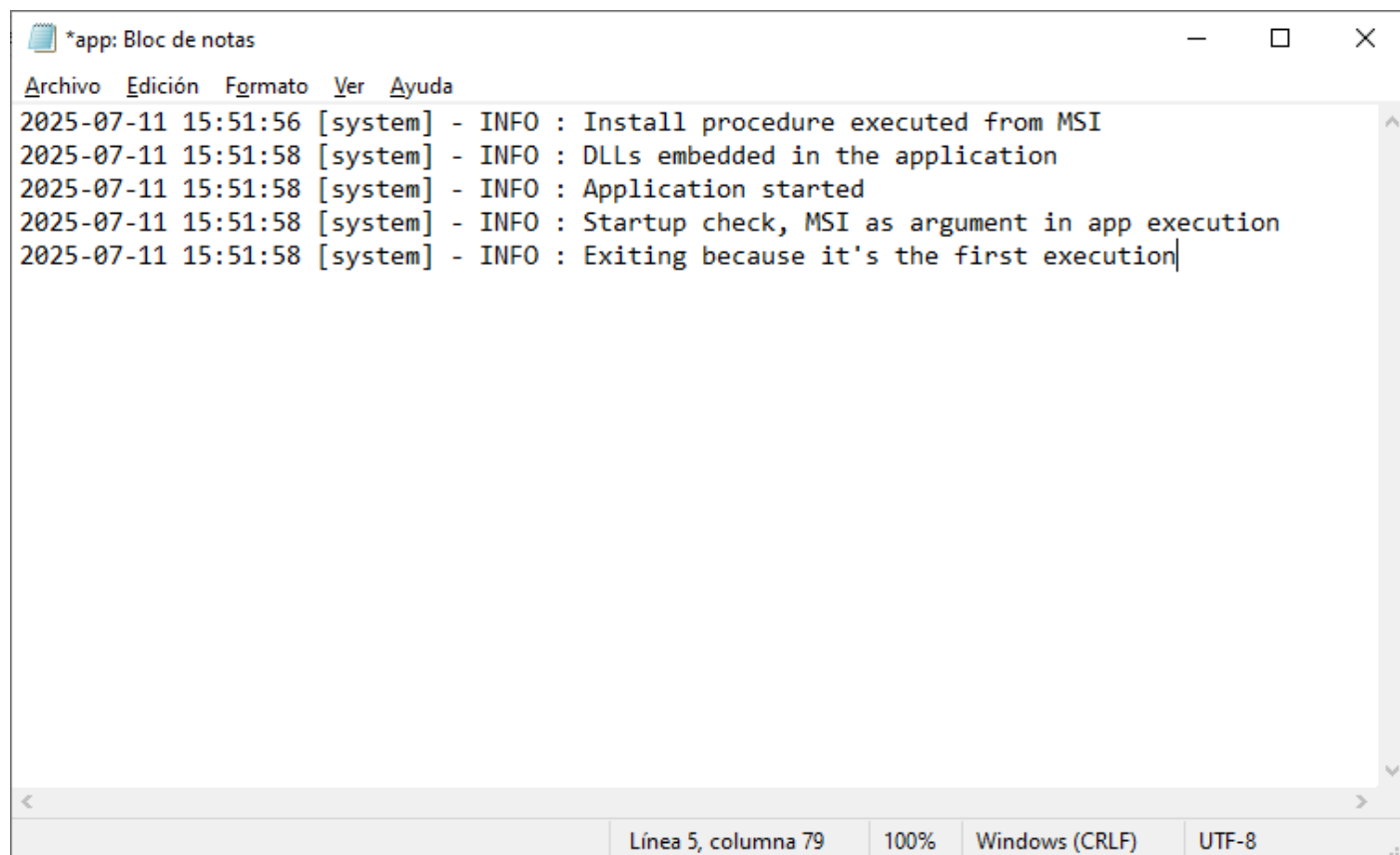
Category	Count
Installed	1
Not Installed	0
Failed	0
Install Pending	0
Not Applicable	0
TOTAL	1

Este gráfico no se actualiza de manera inmediata, puede tardar un rato en aparecer que la aplicación ya fue desplegada con éxito.

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
```

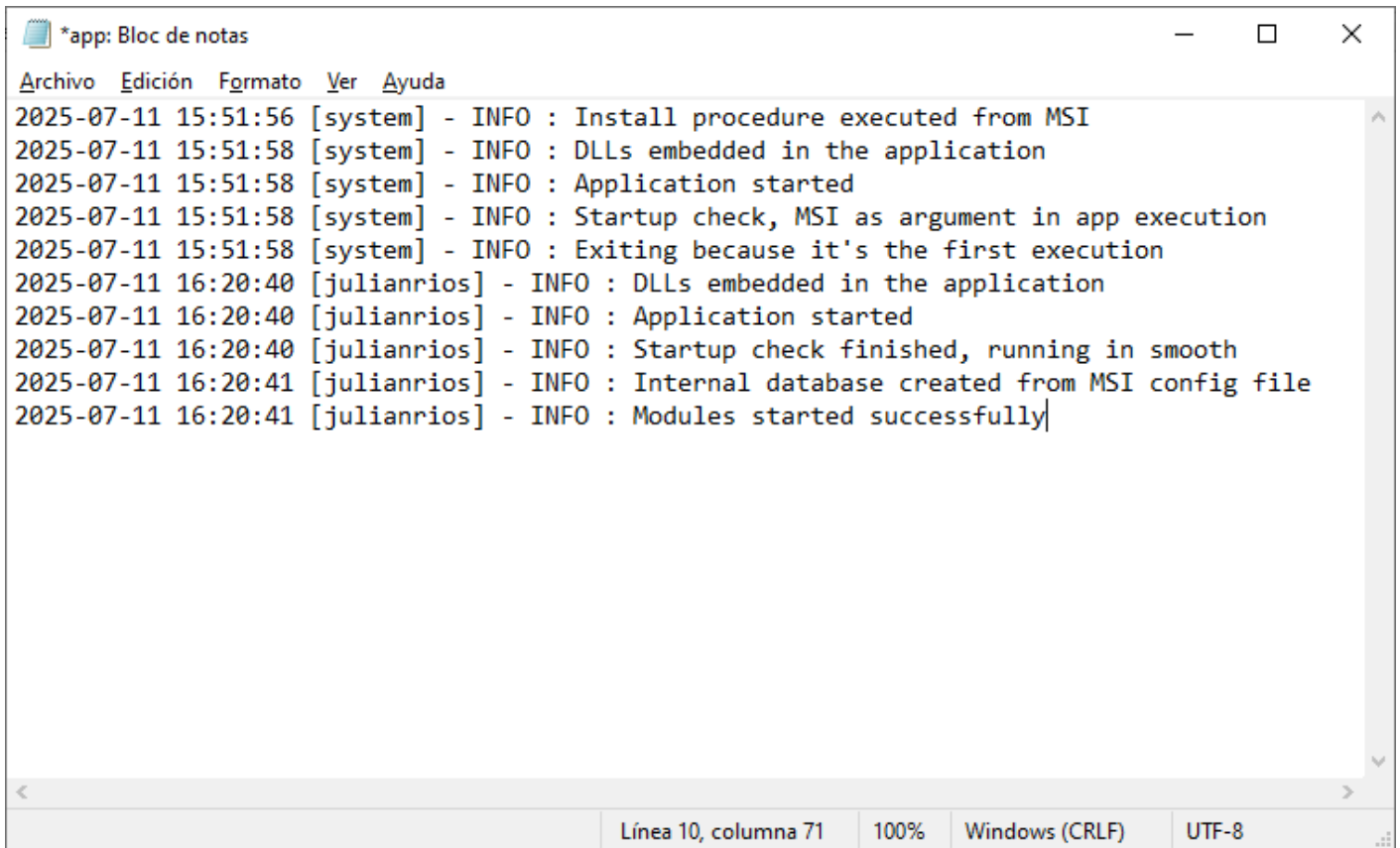
Línea 5, columna 79 100% Windows (CRLF) UTF-8

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
```

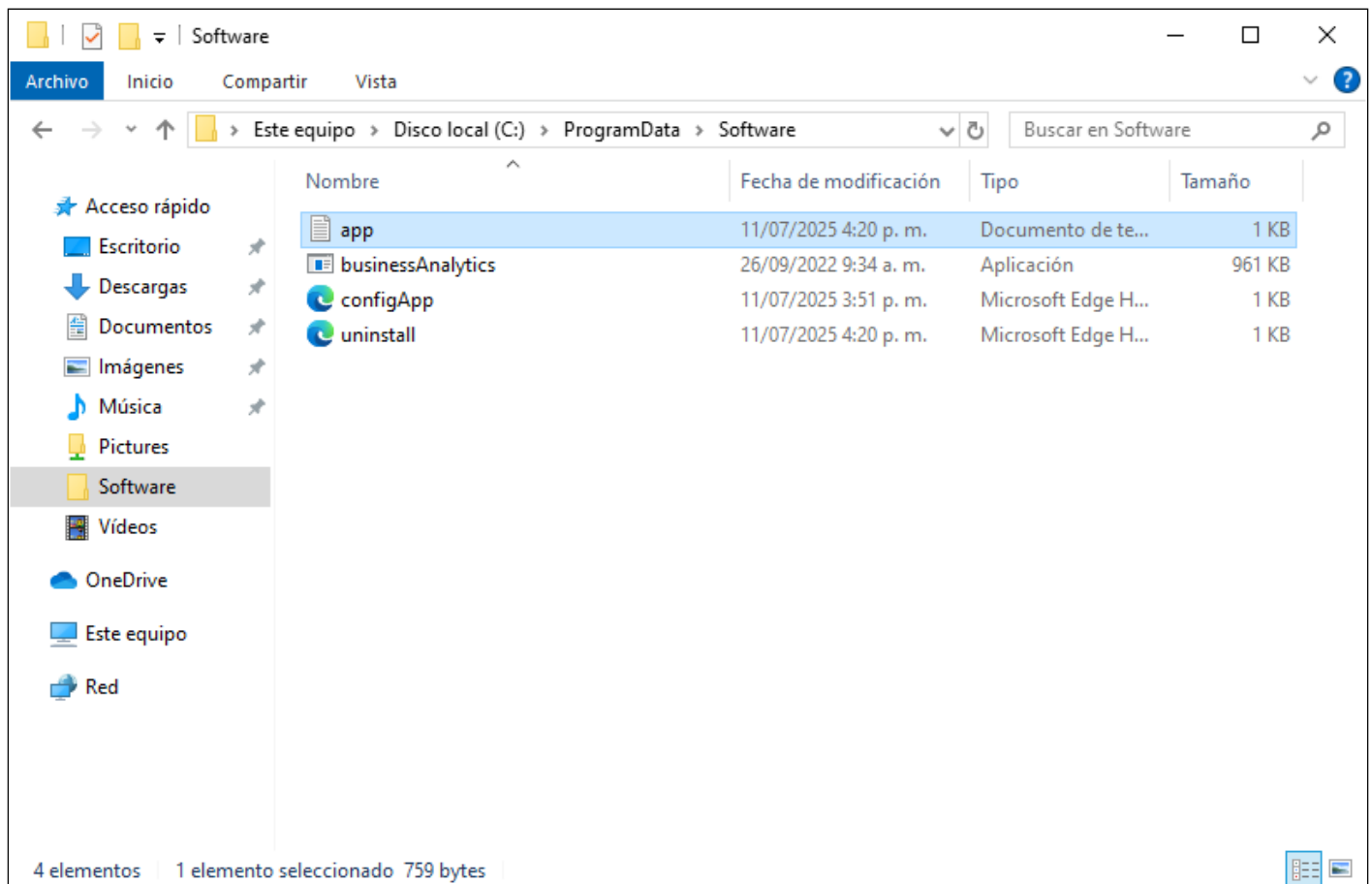
Como se observa, ya la ejecución se hace con un usuario normal sin privilegios elevados y de esa manera el agente de The Fraud Explorer lo detecta y procede a arrancar diciendo **Modules started successfully**.

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**.

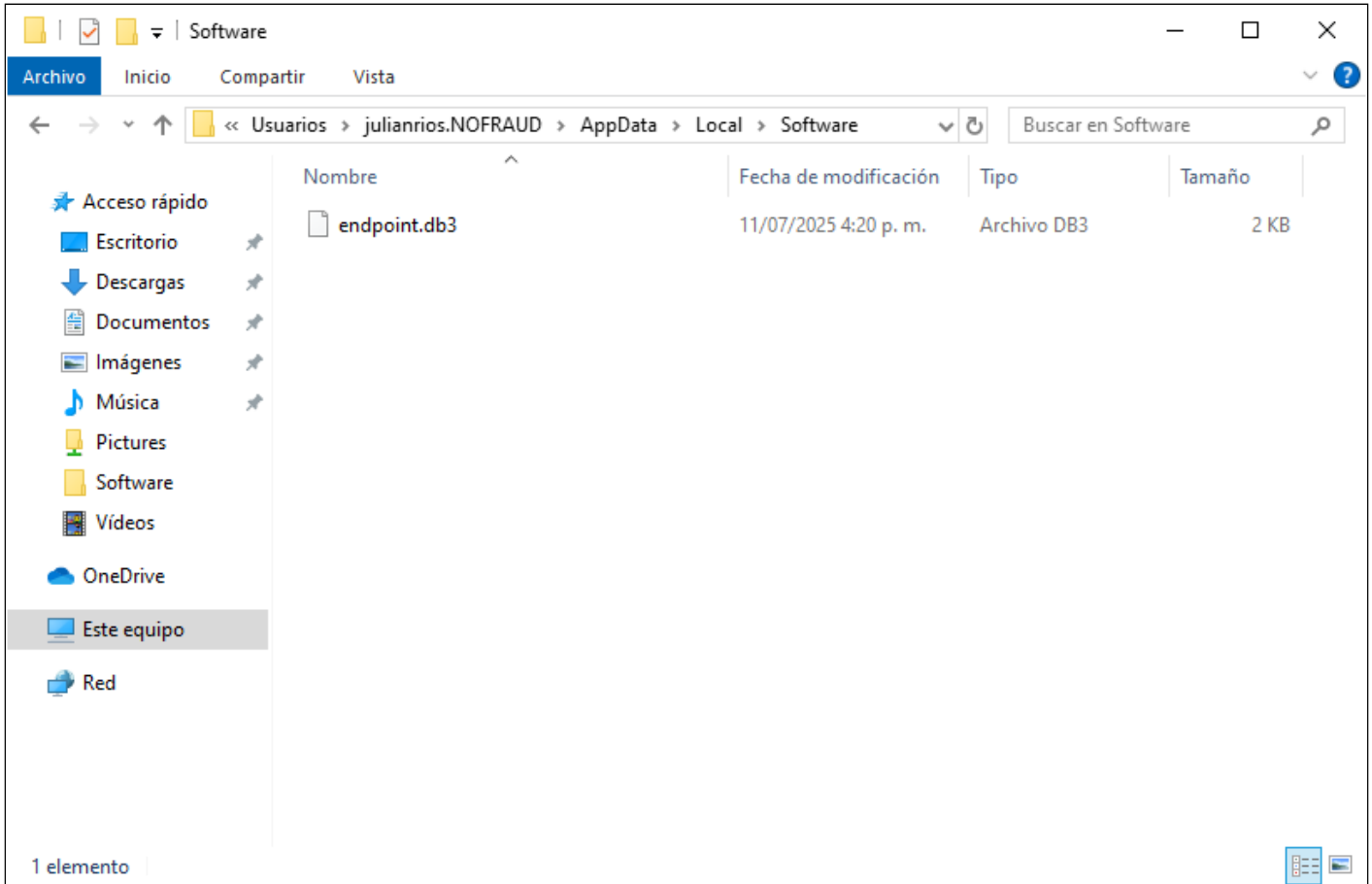


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

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.

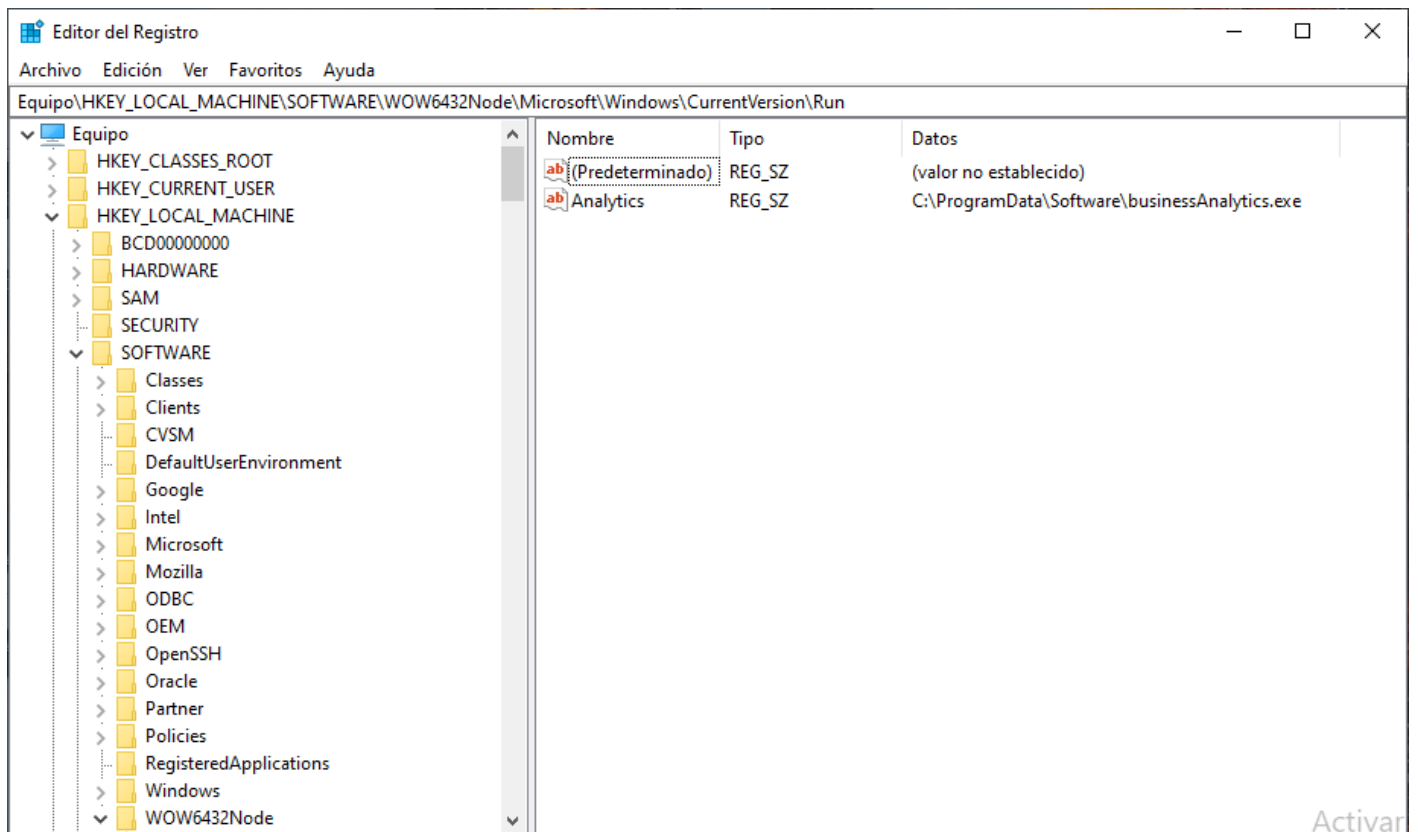


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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.**

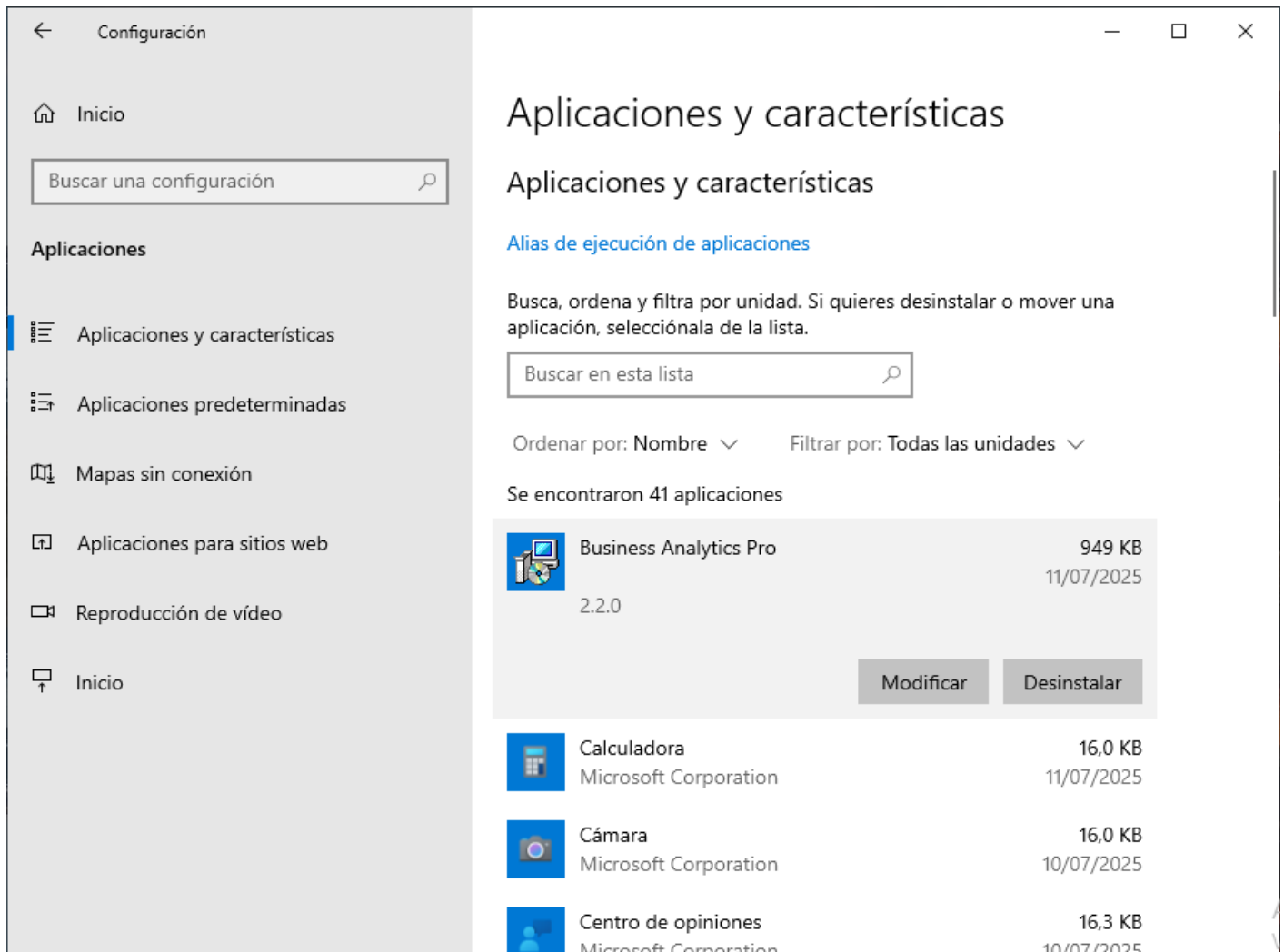


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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**.



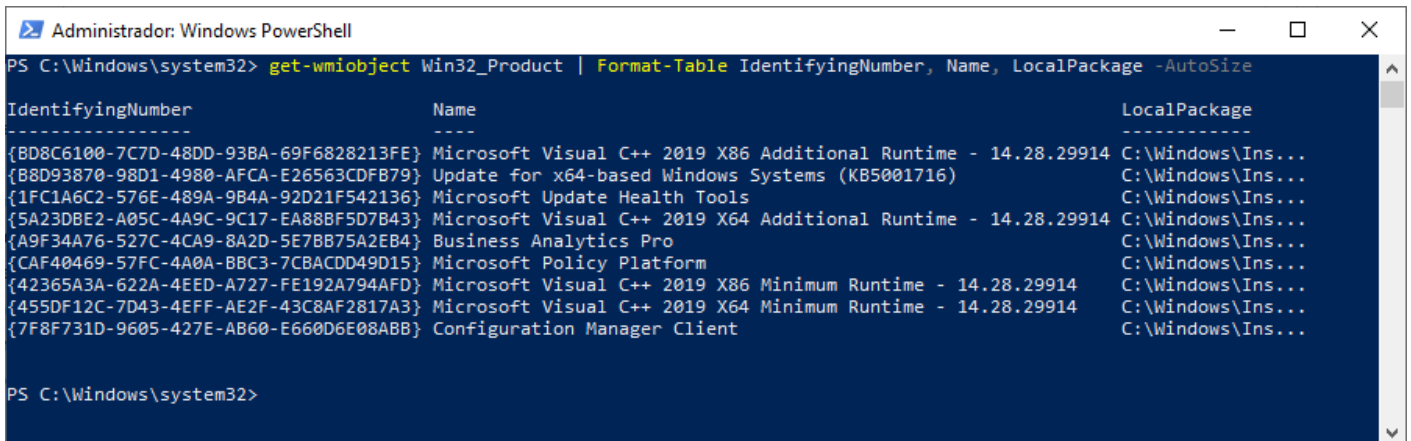
Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se reemplaza la actual con la nueva versión.

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...

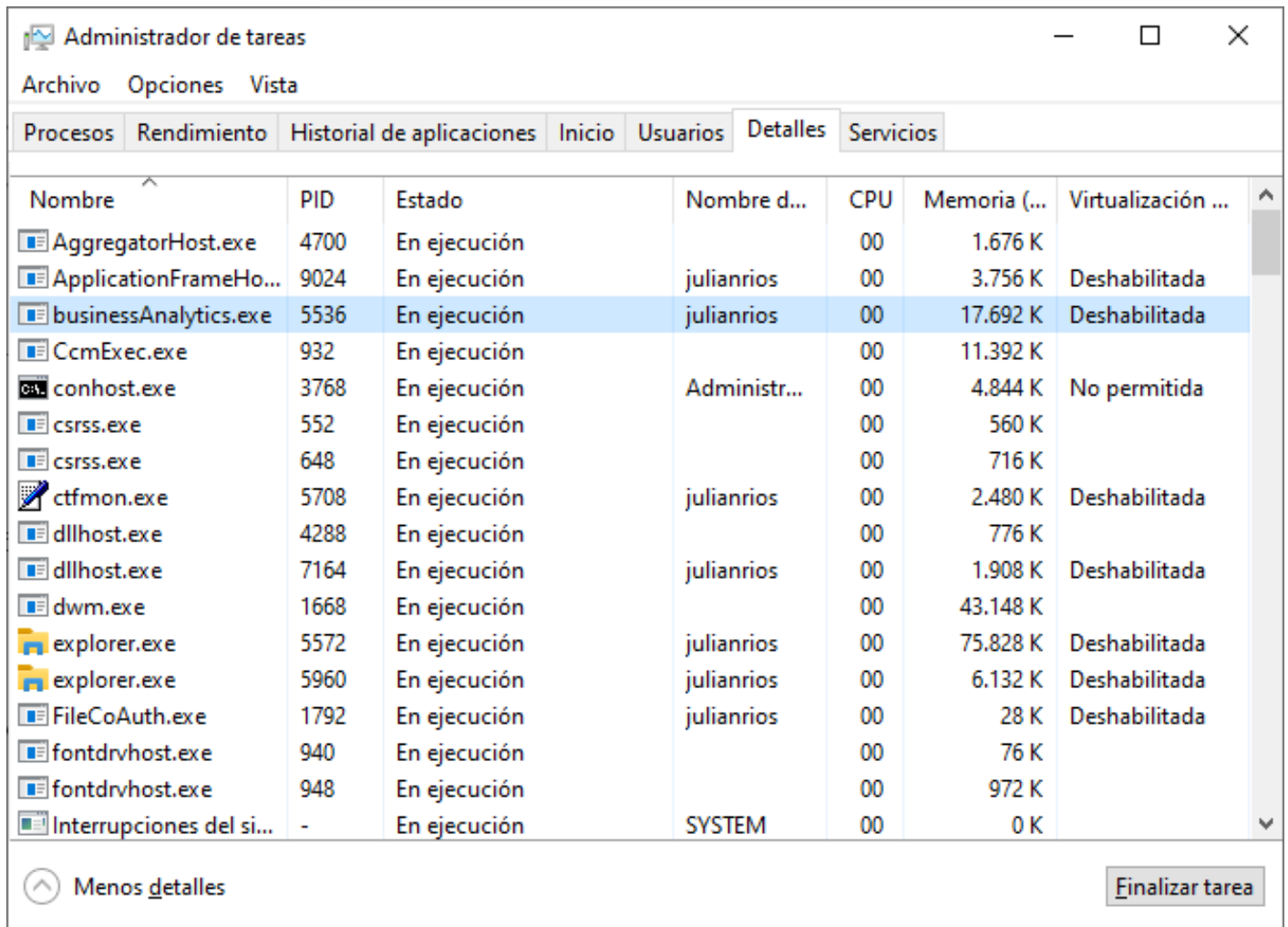
PS C:\Windows\system32>
```

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**.



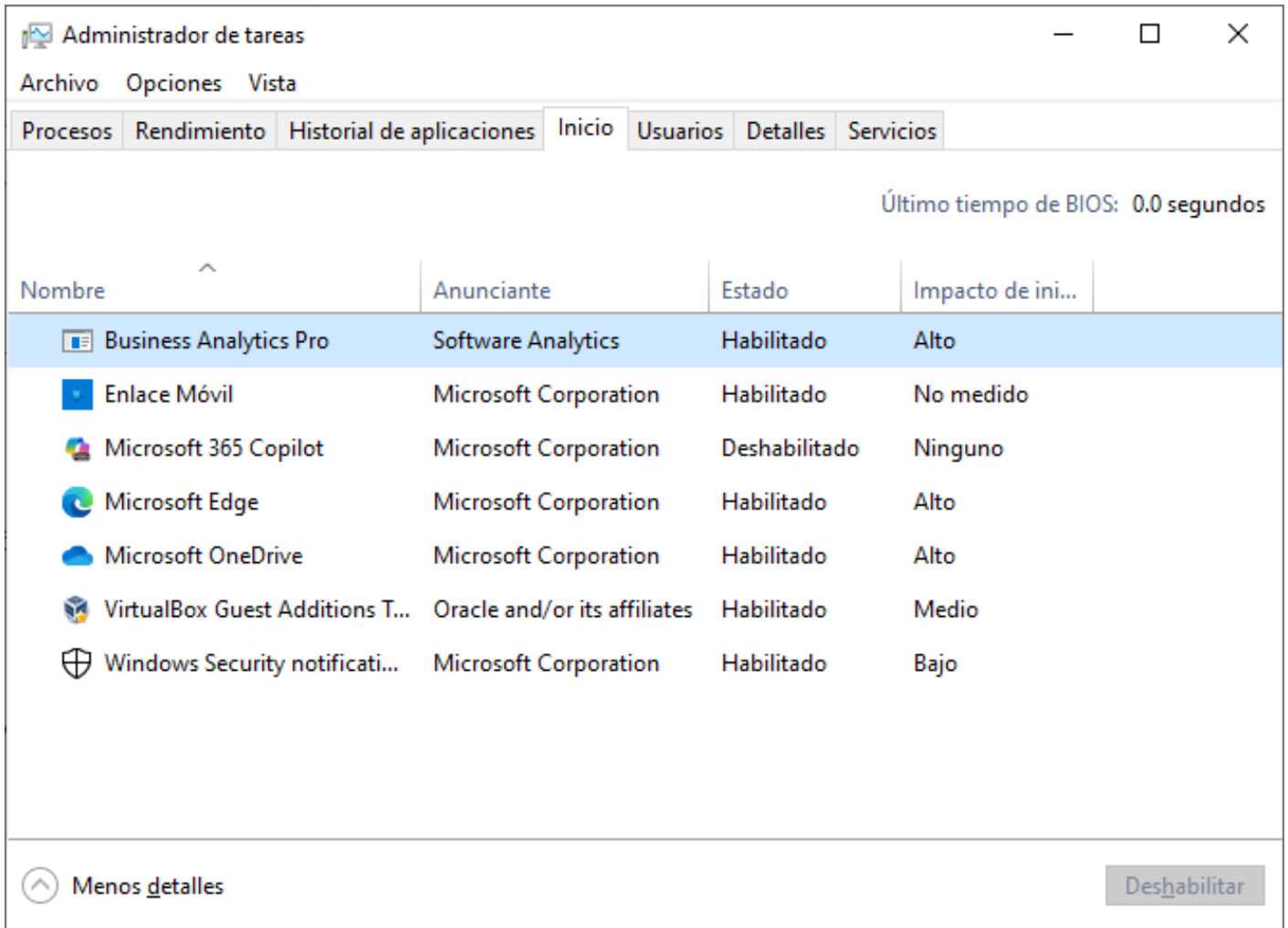
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00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

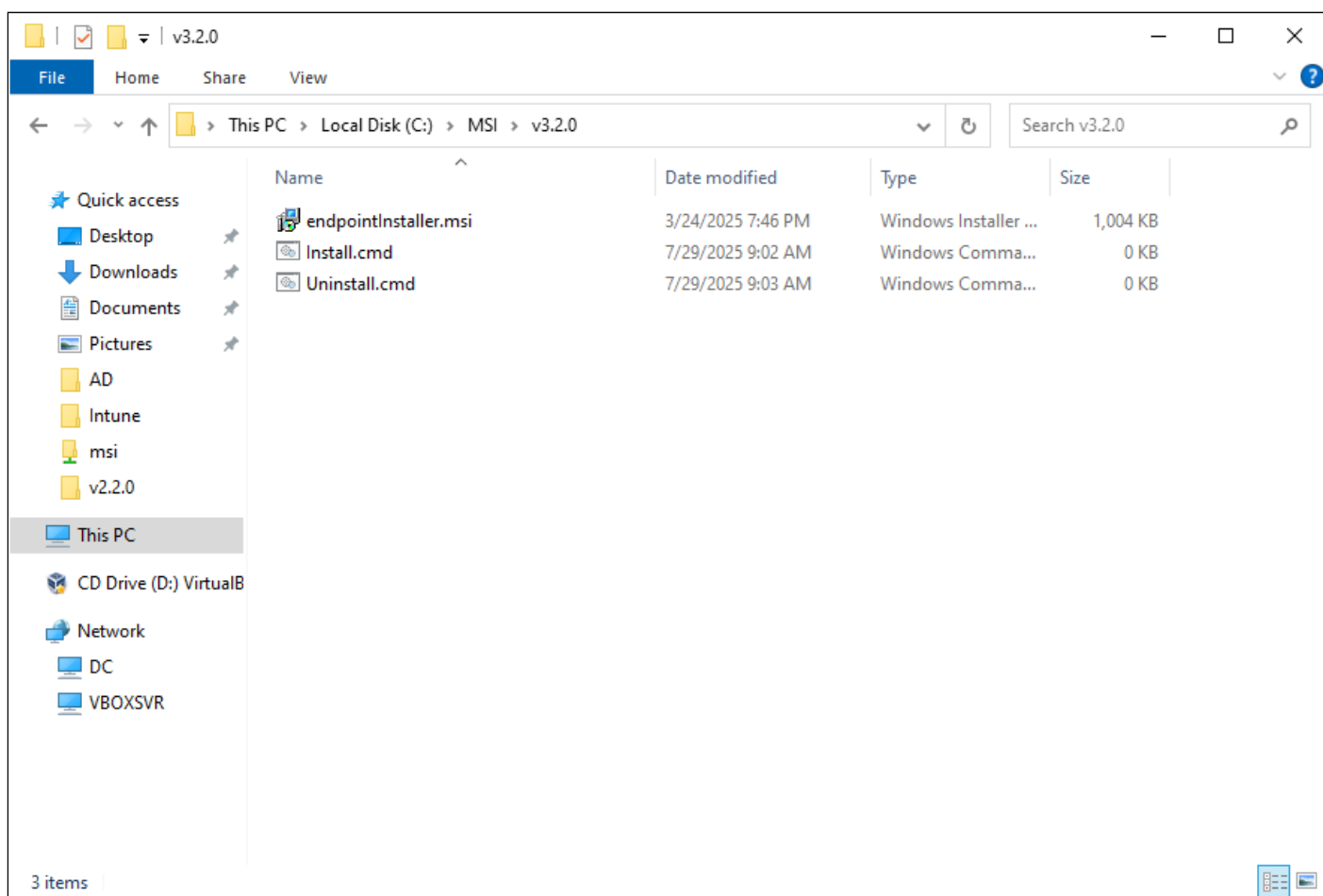
En caso de tener problemas con el arranque de Windows, puede descartar directamente que sea el agente de The Fraud Explorer, porque el agente se ejecuta en la etapa final cuando se ha cargado completamente el explorador de Windows.

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

Carpeta para actualizar el agente

Se debe crear la carpeta del nuevo agente con la nueva versión. Para este caso se llamará **v3.2.0** y en ella se colocará el archivo MSI del agente **endpointInstaller.msi** y se deberán crear dos archivos en blanco, uno llamado **Install.cmd** y el otro **Uninstall.cmd**.

Esta carpeta se crea así para cumplir con las normas del tipo de paquete **IntuneWin**, que se necesita crear para hacer nuestro agente antifraude compatible con **Microsoft Intune**.

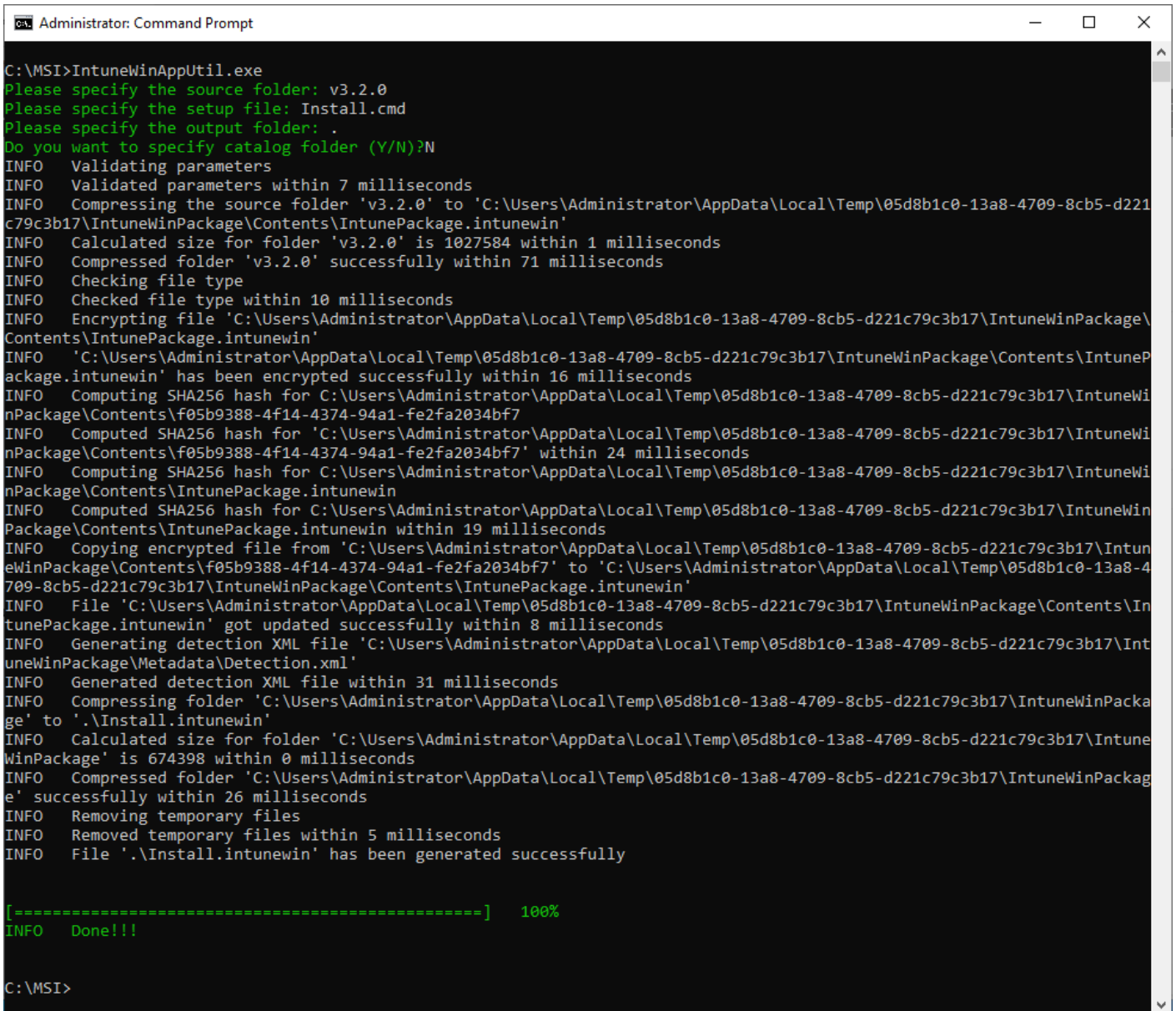


Una vez creada esta estructura, se podrá proceder a crear el paquete como se indica a continuación.

Paquete de actualización

Se debe abrir una consola MS-DOS y navegar hasta la carpeta C:\MSI donde se encuentra la estructura de carpetas compatibles con los paquetes de Microsoft Intune. Una vez allí se ejecuta el comando:

```
IntuneWinAppUtil.exe
```



```
Administrator: Command Prompt
C:\MSI>IntuneWinAppUtil.exe
Please specify the source folder: v3.2.0
Please specify the setup file: Install.cmd
Please specify the output folder: .
Do you want to specify catalog folder (Y/N)?N
INFO Validating parameters
INFO Validated parameters within 7 milliseconds
INFO Compressing the source folder 'v3.2.0' to 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO Calculated size for folder 'v3.2.0' is 1027584 within 1 milliseconds
INFO Compressed folder 'v3.2.0' successfully within 71 milliseconds
INFO Checking file type
INFO Checked file type within 10 milliseconds
INFO Encrypting file 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 16 milliseconds
INFO Computing SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\05b9388-4f14-4374-94a1-fe2fa2034bf7
INFO Computed SHA256 hash for 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\05b9388-4f14-4374-94a1-fe2fa2034bf7' within 24 milliseconds
INFO Computing SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin
INFO Computed SHA256 hash for C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin within 19 milliseconds
INFO Copying encrypted file from 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\05b9388-4f14-4374-94a1-fe2fa2034bf7' to 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO File 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 8 milliseconds
INFO Generating detection XML file 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage\Metadata\Detection.xml'
INFO Generated detection XML file within 31 milliseconds
INFO Compressing folder 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage' to '.\Install.intunewin'
INFO Calculated size for folder 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage' is 674398 within 0 milliseconds
INFO Compressed folder 'C:\Users\Administrator\AppData\Local\Temp\05d8b1c0-13a8-4709-8cb5-d221c79c3b17\IntuneWinPackage' successfully within 26 milliseconds
INFO Removing temporary files
INFO Removed temporary files within 5 milliseconds
INFO File '.\Install.intunewin' has been generated successfully

[=====] 100%
INFO Done!!!

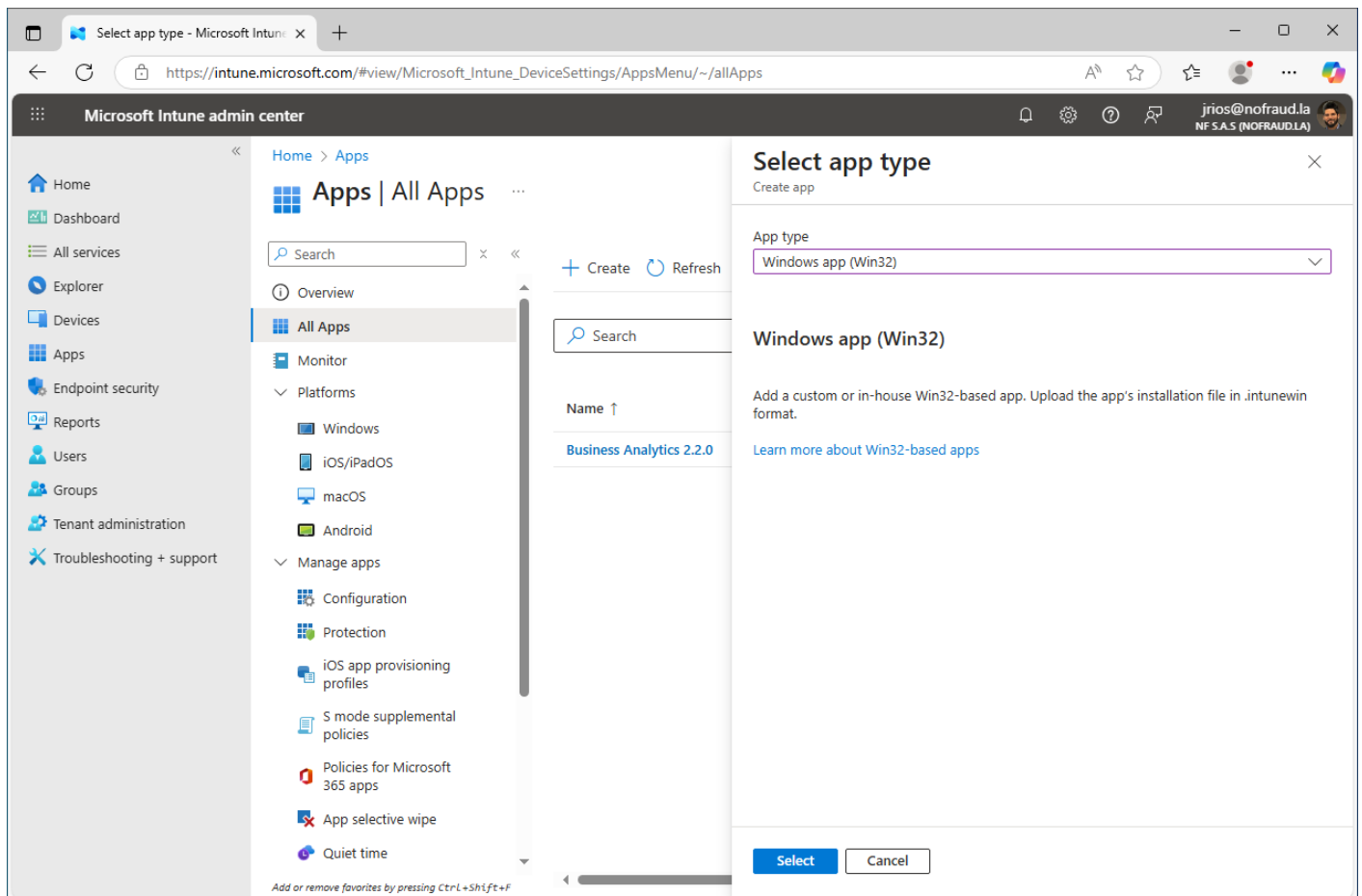
C:\MSI>
```

Cuando pregunte por la carpeta origen, escriba **v3.2.0**, cuando pregunte por el archivo de configuración escriba **Install.cmd**, cuando pregunte por la carpeta de destino escriba **un punto** y al final escriba **N** cuando se le pregunte por el catálogo. Este proceso creará un archivo llamado **Install.intunewin** que deberá ser renombrado a **endpointInstaller-v3.2.0.intunewin** para mejor recordación.

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

Aplicación para la actualización

En la plataforma de **Microsoft Intune**, dar clic en **Apps**, **All Apps** y luego en el botón **Create**.

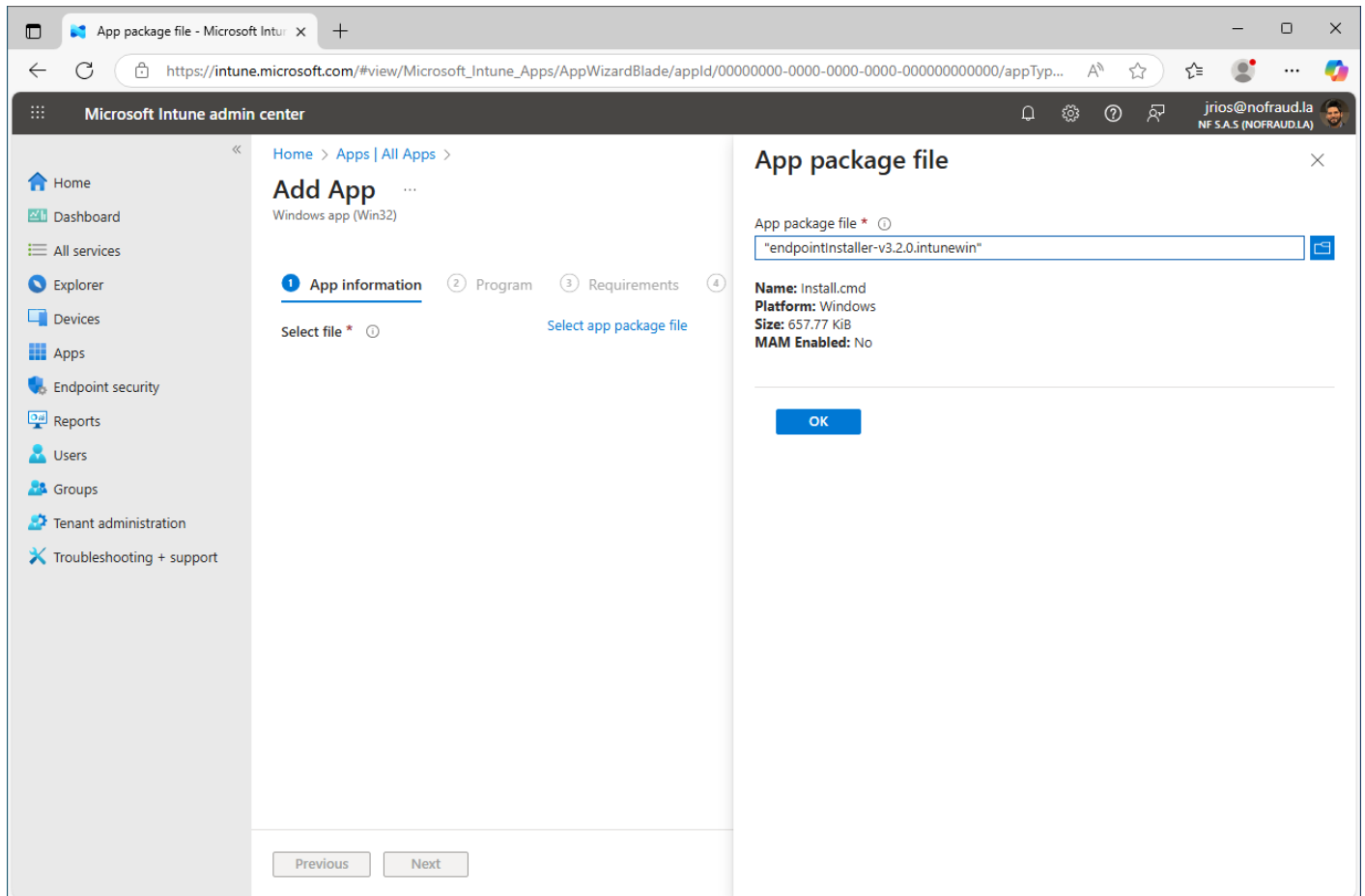


Allí seleccione que la aplicación es de tipo **Windows app (Win32)** y de clic en **Select**.

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

Seleccionar paquete de actualización

Seleccione el archivo que acabó de crear llamado **endpointInstaller-v3.2.0.intunewin**.

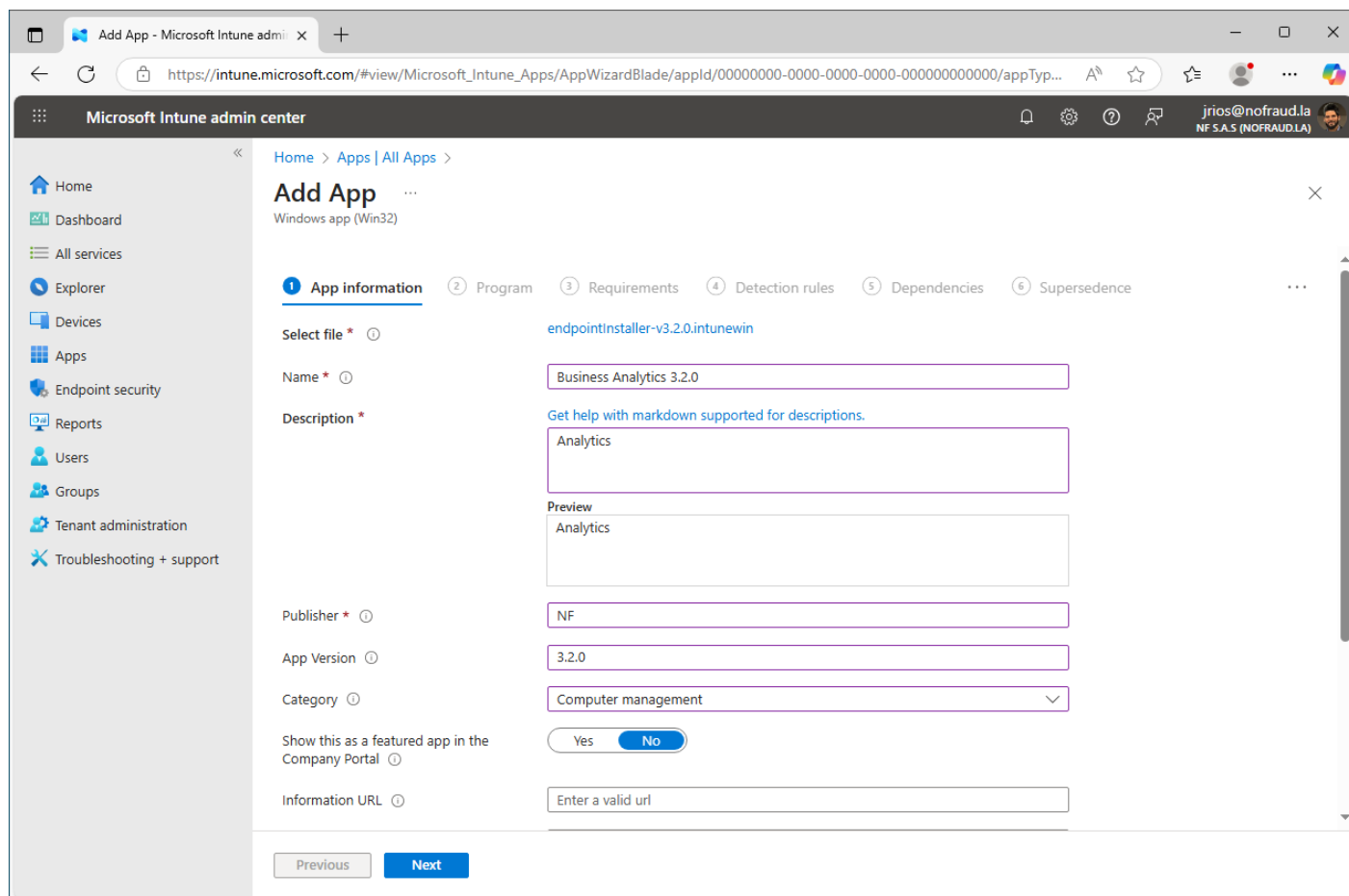


De clic en **OK** para continuar con el proceso.

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

Información de actualización

Escriba el nombre **Business Analytics 3.2.0** en el campo de nombre para diferenciar esta aplicación de la anterior.



The screenshot shows the 'Add App' wizard in the Microsoft Intune Admin Center. The 'App information' step is selected, and the following fields are visible:

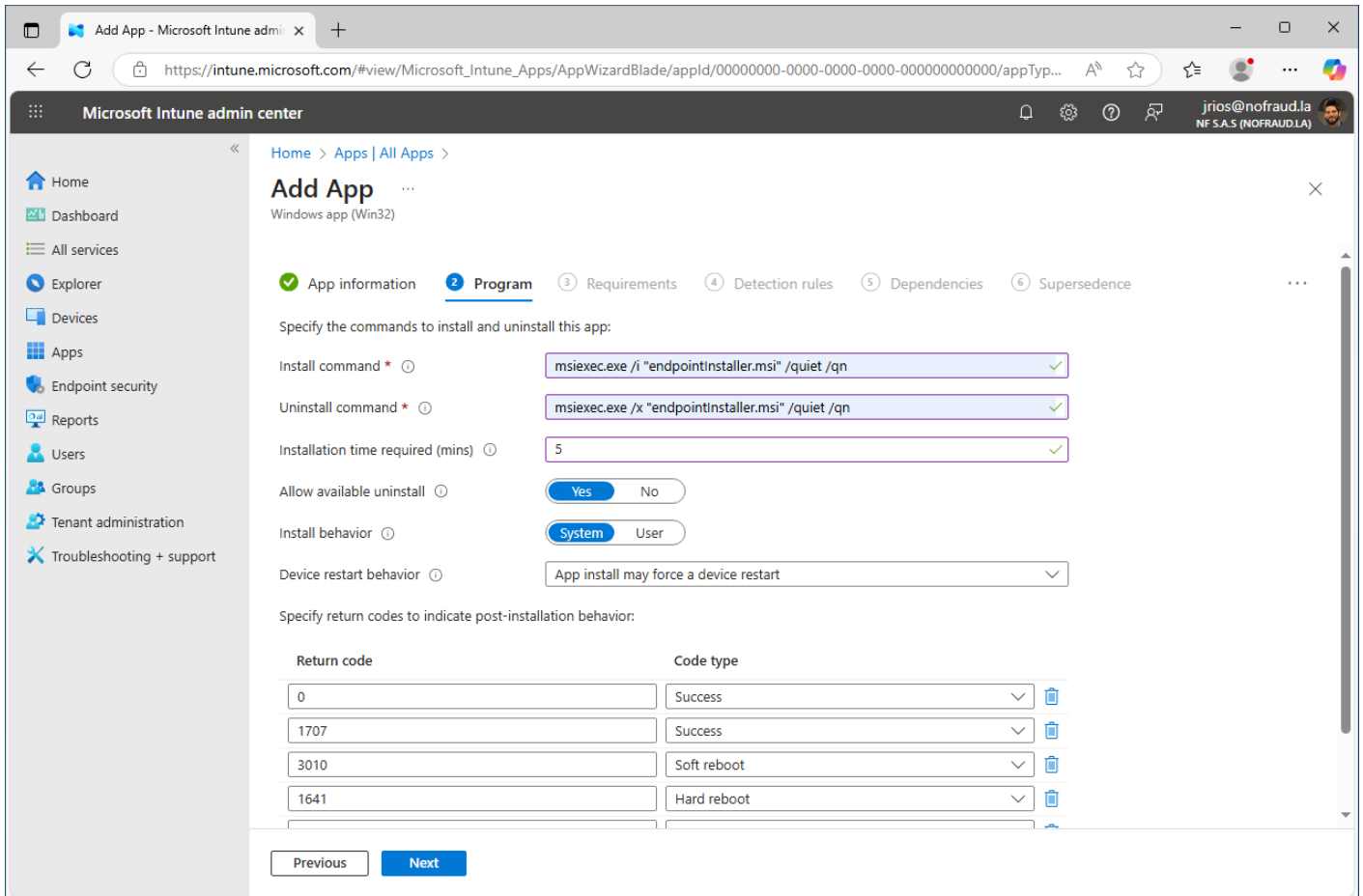
- Select file:** endpointinstaller-v3.2.0.intunewin
- Name:** Business Analytics 3.2.0
- Description:** Analytics
- Publisher:** NF
- App Version:** 3.2.0
- Category:** Computer management
- Show this as a featured app in the Company Portal:** No (selected)
- Information URL:** Enter a valid url

Asegúrese de que la opción de mostrar esta aplicación en el portal de compañía este deshabilitada.

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

Comandos de actualización

Asegúrese de escribir los comandos de instalación y desinstalación como se muestra en la imagen abajo.



Microsoft Intune admin center

Home > Apps | All Apps >

Add App

Windows app (Win32)

App information **2 Program** 3 Requirements 4 Detection rules 5 Dependencies 6 Supersede

Specify the commands to install and uninstall this app:

Install command *

Uninstall command *

Installation time required (mins)

Allow available uninstall Yes No

Install behavior System User

Device restart behavior

Specify return codes to indicate post-installation behavior:

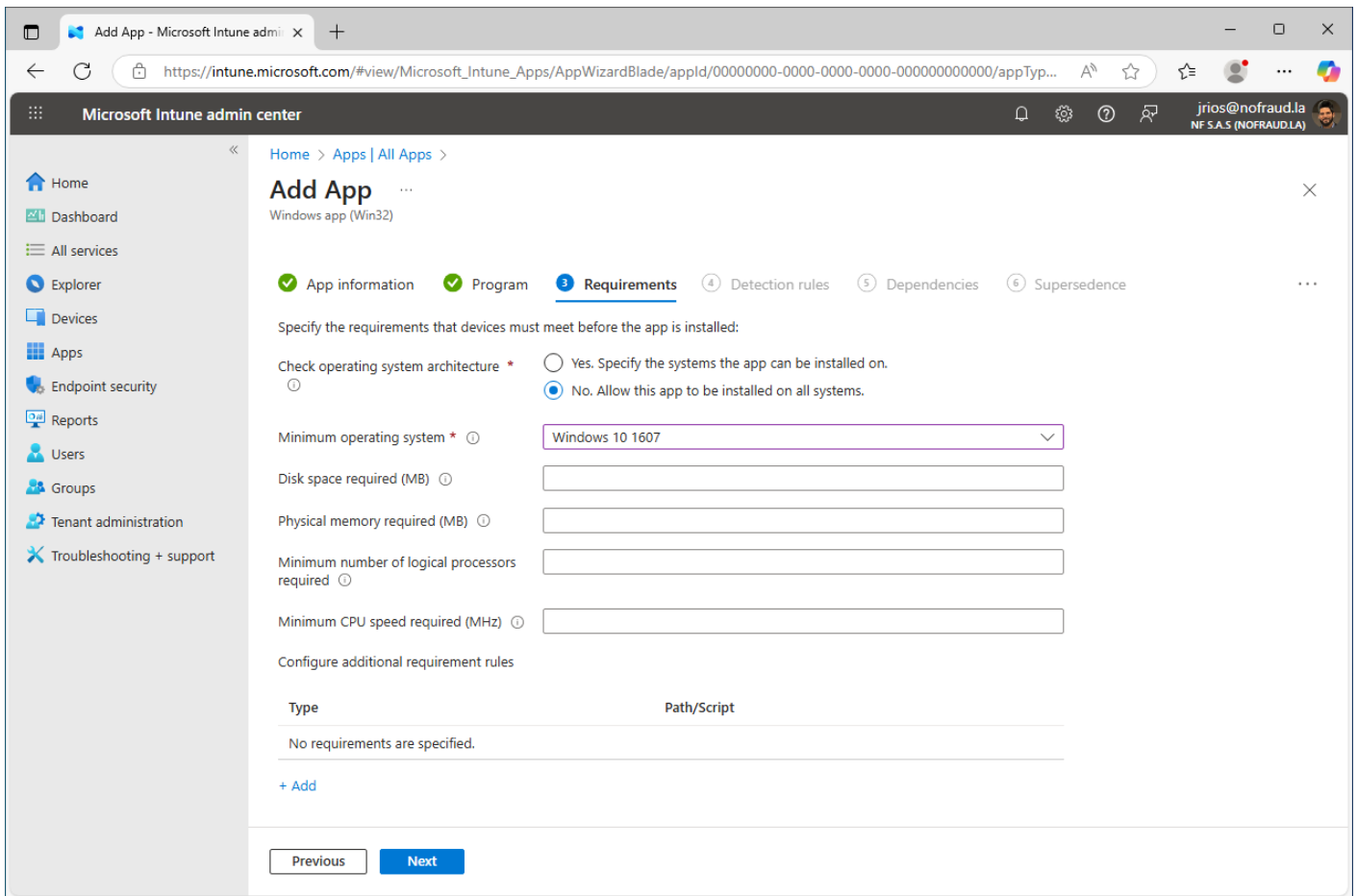
Return code	Code type
<input type="text" value="0"/>	<input type="text" value="Success"/>
<input type="text" value="1707"/>	<input type="text" value="Success"/>
<input type="text" value="3010"/>	<input type="text" value="Soft reboot"/>
<input type="text" value="1641"/>	<input type="text" value="Hard reboot"/>

Asegúrese también de que la opción de **Install Behavior** esté marcada como **System**.

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

Requerimientos de actualización

Microsoft Intune exige seleccionar como requerimiento una versión de Windows mínima, para este caso se selecciona Windows 10 1607.



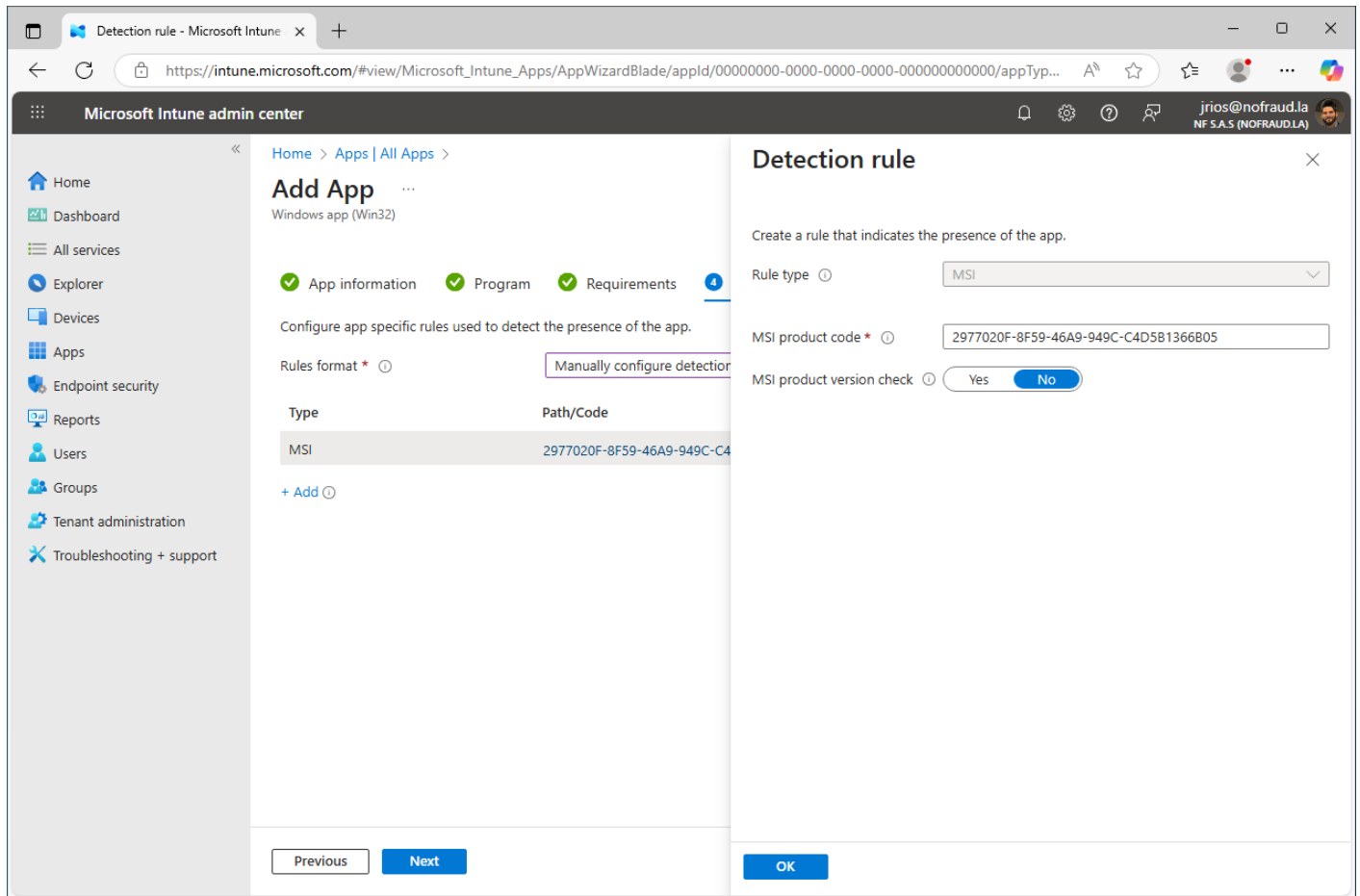
The screenshot shows the 'Add App' wizard in the Microsoft Intune Admin Center, specifically the 'Requirements' step. The wizard is titled 'Add App' and is for a 'Windows app (Win32)'. The progress bar shows that 'App information' and 'Program' are completed, while 'Requirements' is the current step. The instructions state: 'Specify the requirements that devices must meet before the app is installed:'. There are two radio button options for 'Check operating system architecture *': 'Yes. Specify the systems the app can be installed on.' (unselected) and 'No. Allow this app to be installed on all systems.' (selected). Below this, there are several input fields for requirements: 'Minimum operating system *' (set to 'Windows 10 1607'), 'Disk space required (MB)', 'Physical memory required (MB)', 'Minimum number of logical processors required', and 'Minimum CPU speed required (MHz)'. At the bottom, there is a table for 'Configure additional requirement rules' with columns for 'Type' and 'Path/Script', and a note that 'No requirements are specified.' with a '+ Add' link. Navigation buttons 'Previous' and 'Next' are at the bottom.

El resto de opciones se deja en blanco y se da clic en el botón **Next**.

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

Reglas de detección

Microsoft Intune necesita que se le especifique cuál será la regla de detección mediante la cual se averiguará si la aplicación queda instalada o no. En este caso se especifica que la regla es a través del **código del producto** del MSI.



The screenshot shows the Microsoft Intune admin center interface. The main content area is titled "Add App" and is for a "Windows app (Win32)". It features a progress bar with four steps: "App information", "Program", "Requirements", and "Rules format" (which is currently active). Below the progress bar, there is a section for "Rules format" with a dropdown menu set to "Manually configure detection". A table below this section lists the app's details:

Type	Path/Code
MSI	2977020F-8F59-46A9-949C-C4D5B1366B05

At the bottom of the table, there is a "+ Add" button. To the right of the table, there is a "Detection rule" panel with the following configuration:

- Rule type: MSI
- MSI product code: 2977020F-8F59-46A9-949C-C4D5B1366B05
- MSI product version check: No

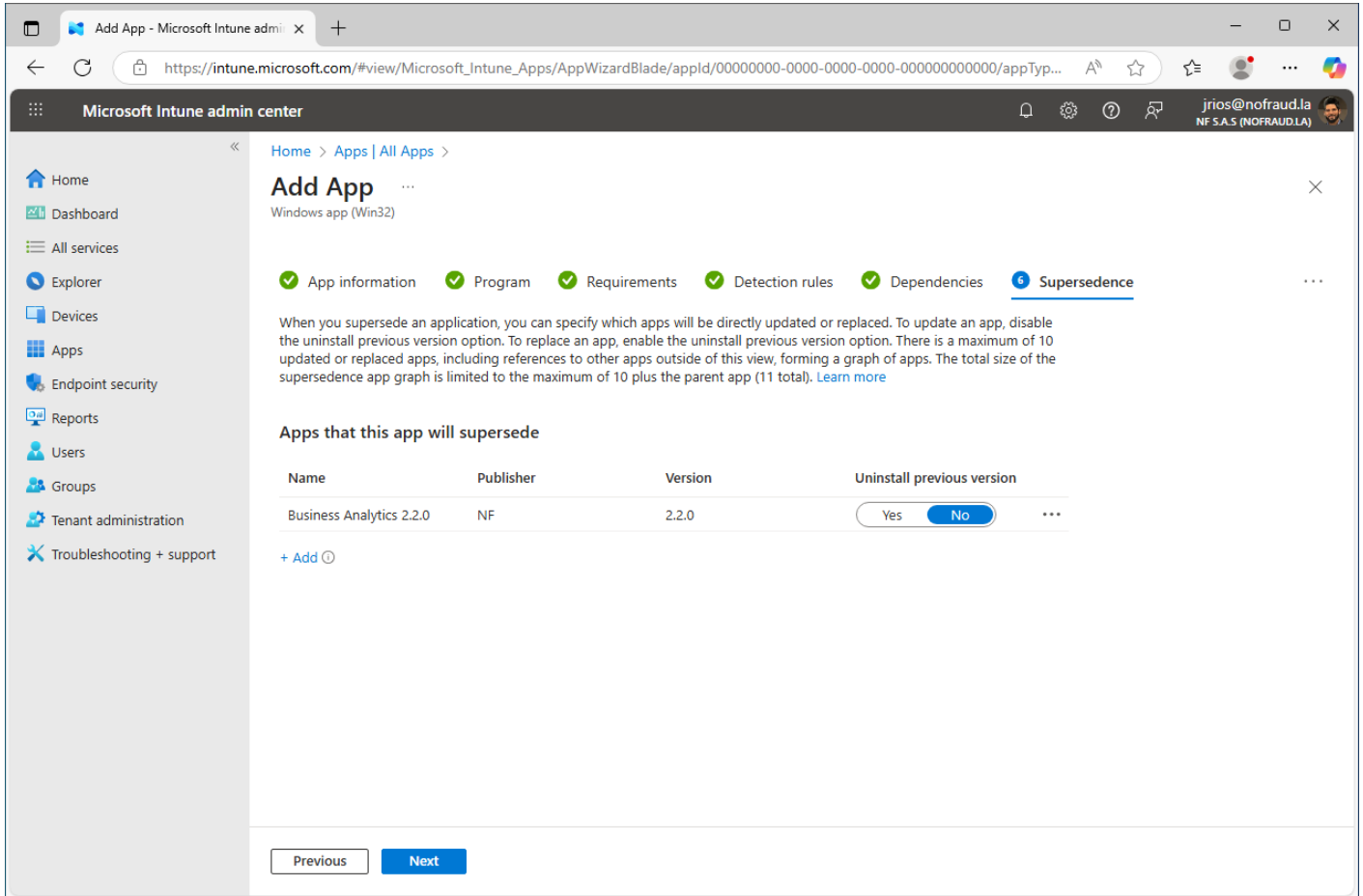
Navigation buttons include "Previous", "Next", and "OK".

Este código del producto es proporcionado por NOFRAUD al momento de iniciar el proyecto, sin embargo, también puede usar la aplicación **Microsoft Orca** para abrir el MSI y ver el código del producto.

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

Supersedencia

Esta es la parte donde se le especifica a **Microsoft Intune** que la aplicación que se está creando es la versión más actual de otra que ya existe. Se debe dar clic en **añadir** y seleccionar **Business Analytics 2.2.0** (la versión anterior).



The screenshot shows the 'Add App' wizard in the Microsoft Intune Admin Center, specifically the 'Supersede' step. The breadcrumb navigation is 'Home > Apps | All Apps >'. The page title is 'Add App' with a sub-header 'Windows app (Win32)'. There are five progress indicators: 'App information', 'Program', 'Requirements', 'Detection rules', and 'Dependencies' are all marked with green checkmarks. 'Supersede' is the current step, marked with a blue circle and a plus sign. Below the progress indicators, there is a text block explaining the supersede process: 'When you supersede an application, you can specify which apps will be directly updated or replaced. To update an app, disable the uninstall previous version option. To replace an app, enable the uninstall previous version option. There is a maximum of 10 updated or replaced apps, including references to other apps outside of this view, forming a graph of apps. The total size of the supersedence app graph is limited to the maximum of 10 plus the parent app (11 total). [Learn more](#)'. Below this text is a table titled 'Apps that this app will supersede' with columns for Name, Publisher, Version, and Uninstall previous version. The table contains one row: 'Business Analytics 2.2.0' by publisher 'NF' with version '2.2.0'. The 'Uninstall previous version' column has a 'Yes' button (disabled) and a 'No' button (active). At the bottom of the wizard, there are 'Previous' and 'Next' buttons.

Name	Publisher	Version	Uninstall previous version
Business Analytics 2.2.0	NF	2.2.0	Yes No

Debe asegurarse de que no se desinstale la versión anterior. Esto no significa que quedarán dos versiones instaladas, esto lo que significa es que el proceso de actualización se llevará a cabo por el MSI y no por **Microsoft Intune**.

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

Asignaciones para actualización

En la pantalla de asignaciones, seleccione en la categoría **Required** el grupo de usuarios o dispositivos al cual desea realizarle la actualización del agente.

Microsoft Intune admin center

Home > Apps | All Apps >

Add App

Windows app (Win32)

Program Requirements Detection rules Dependencies Supersedence **Assignments**

Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device. If the app is not removed prior to retiring the device, the end user will need to take explicit action on the device to remove the app.

Required

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Install
Included	All devices	None	None	Show all toast notifications	As soon as possible	As soon as possible

+ Add group + Add all users + Add all devices

Available for enrolled devices

Group mode	Group	Filter mode	Filter	Auto-update	End user notifications	Availability
No assignments						

+ Add group + Add all users + Add all devices

Uninstall

Previous Next

En este caso, se seleccionó **Add all devices**, pero en su ambiente lo más seguro es que el agente no se haya instalado en todos los dispositivos, por lo cual deberá elegir el grupo que creó al momento de instalar por primera vez el agente. Con esto ya estaría creada la aplicación para la actualización.

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

Eliminar asignaciones antiguas

Entre a la aplicación de la versión anterior del agente, de clic en **Properties** y luego en **Assignments Edit**.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options like Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Business Analytics 2.2.0 | Properties' and includes a search bar and a list of tabs: Overview, Manage, Properties (selected), and Monitor. The Properties section is divided into several categories: Minimum CPU speed required (MHz), Additional requirement rules, Detection rules, Dependencies, Supersedence, and Assignments. The Assignments section is expanded, showing a table with the following data:

Group mode	Group	Filter mode	Filter	End user notification
Required				
Included	All devices	None	None	Show all toast notific

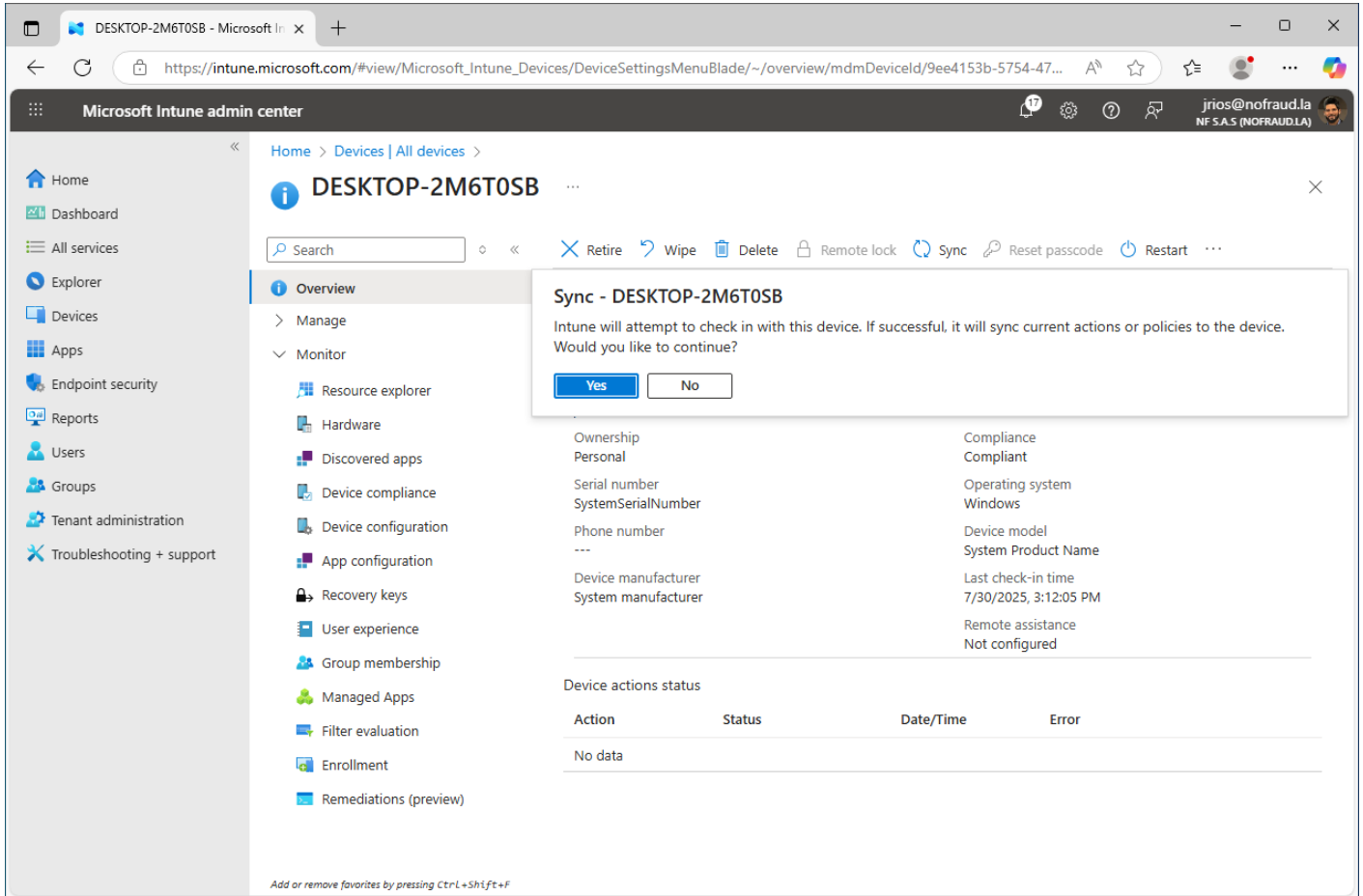
Below the table, there are sections for 'Available for enrolled devices' and 'Uninstall'.

Asegúrese de eliminar la asignación de esta aplicación para que no interfiera en futuras acciones de desinstalación.

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

Sincronización de dispositivo

Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'DESKTOP-2M6T0SB' and includes a search bar and action buttons: Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, and Restart. A 'Sync - DESKTOP-2M6T0SB' dialog box is open, asking for confirmation to sync current actions or policies to the device. Below the dialog, the device's metadata is displayed in two columns:

Ownership	Compliance
Personal	Compliant
Serial number	Operating system
SystemSerialNumber	Windows
Phone number	Device model
---	System Product Name
Device manufacturer	Last check-in time
System manufacturer	7/30/2025, 3:12:05 PM
	Remote assistance
	Not configured

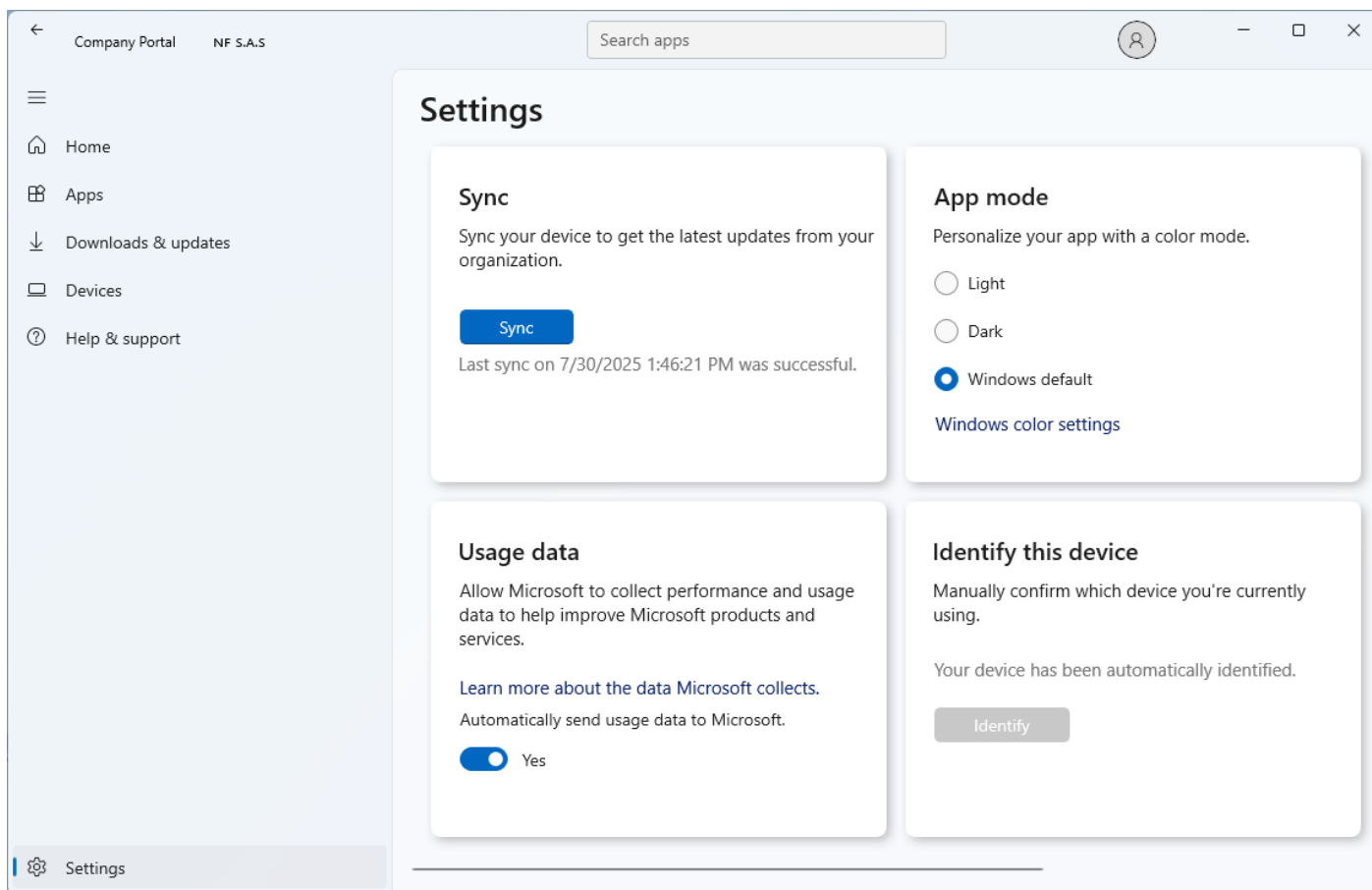
Below the metadata, there is a 'Device actions status' table with columns for Action, Status, Date/Time, and Error. The table currently shows 'No data'.

El siguiente paso será forzar la sincronización del lado de las máquinas.

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

Sincronizar cliente Windows

Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.

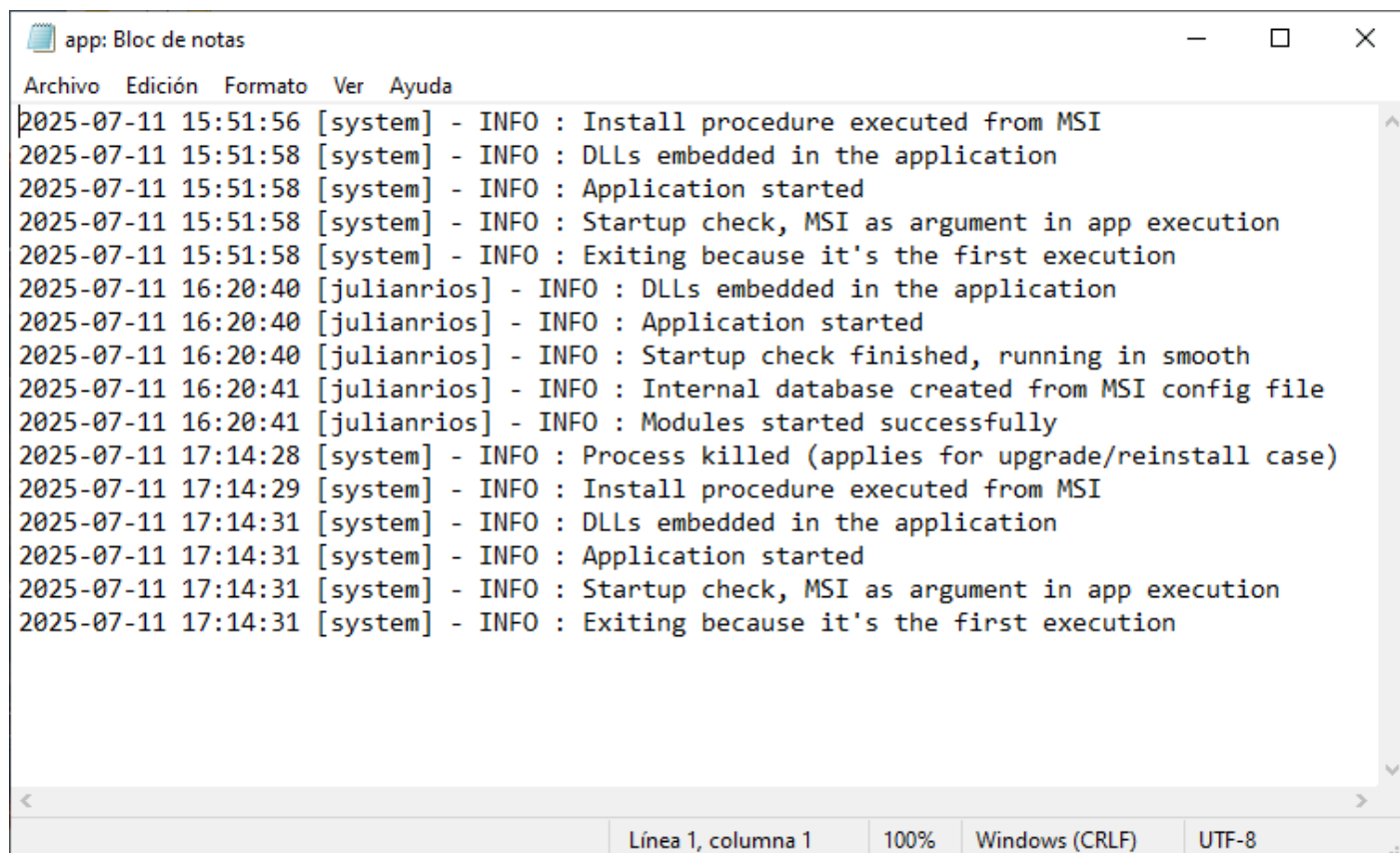


Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política y actualizará el agente antifraude de manera inmediata en esta máquina.

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.



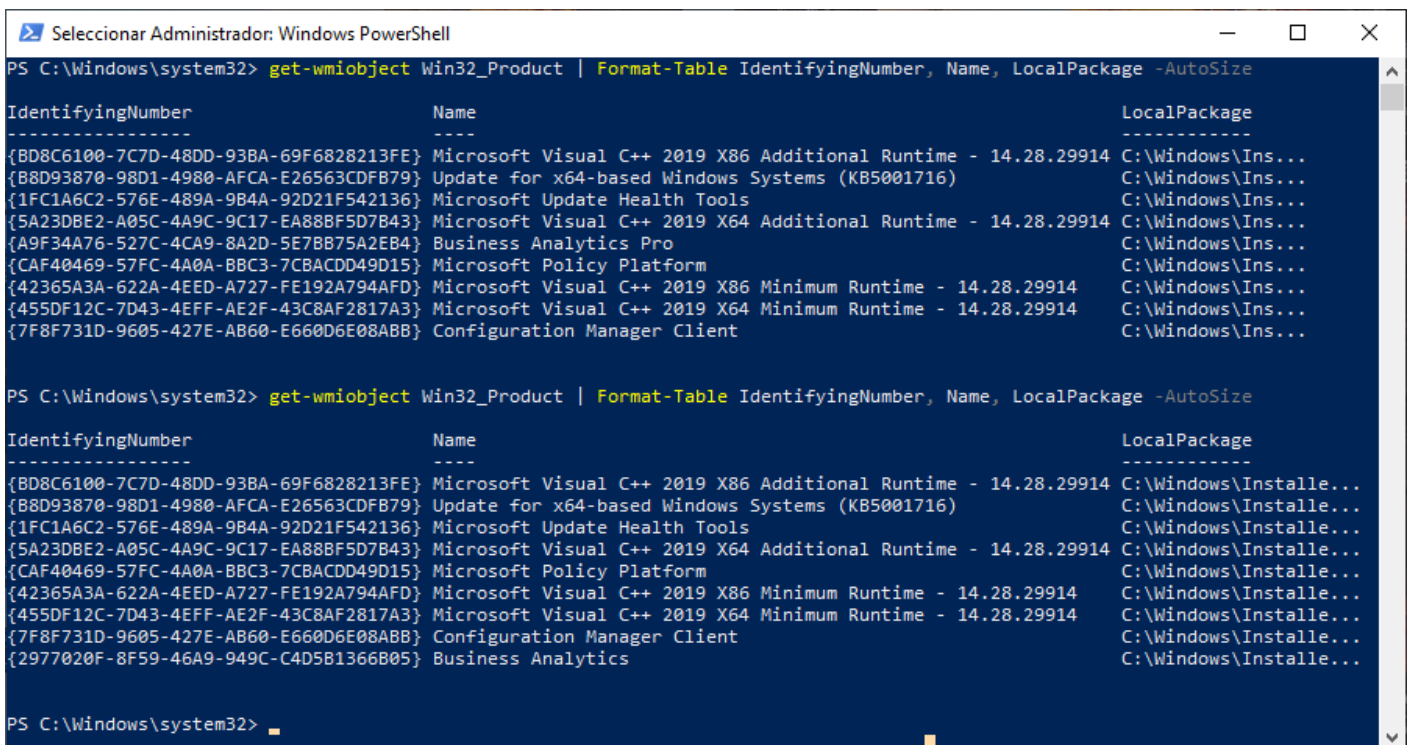
```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-11 15:51:56 [system] - INFO : Install procedure executed from MSI
2025-07-11 15:51:58 [system] - INFO : DLLs embedded in the application
2025-07-11 15:51:58 [system] - INFO : Application started
2025-07-11 15:51:58 [system] - INFO : Startup 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...

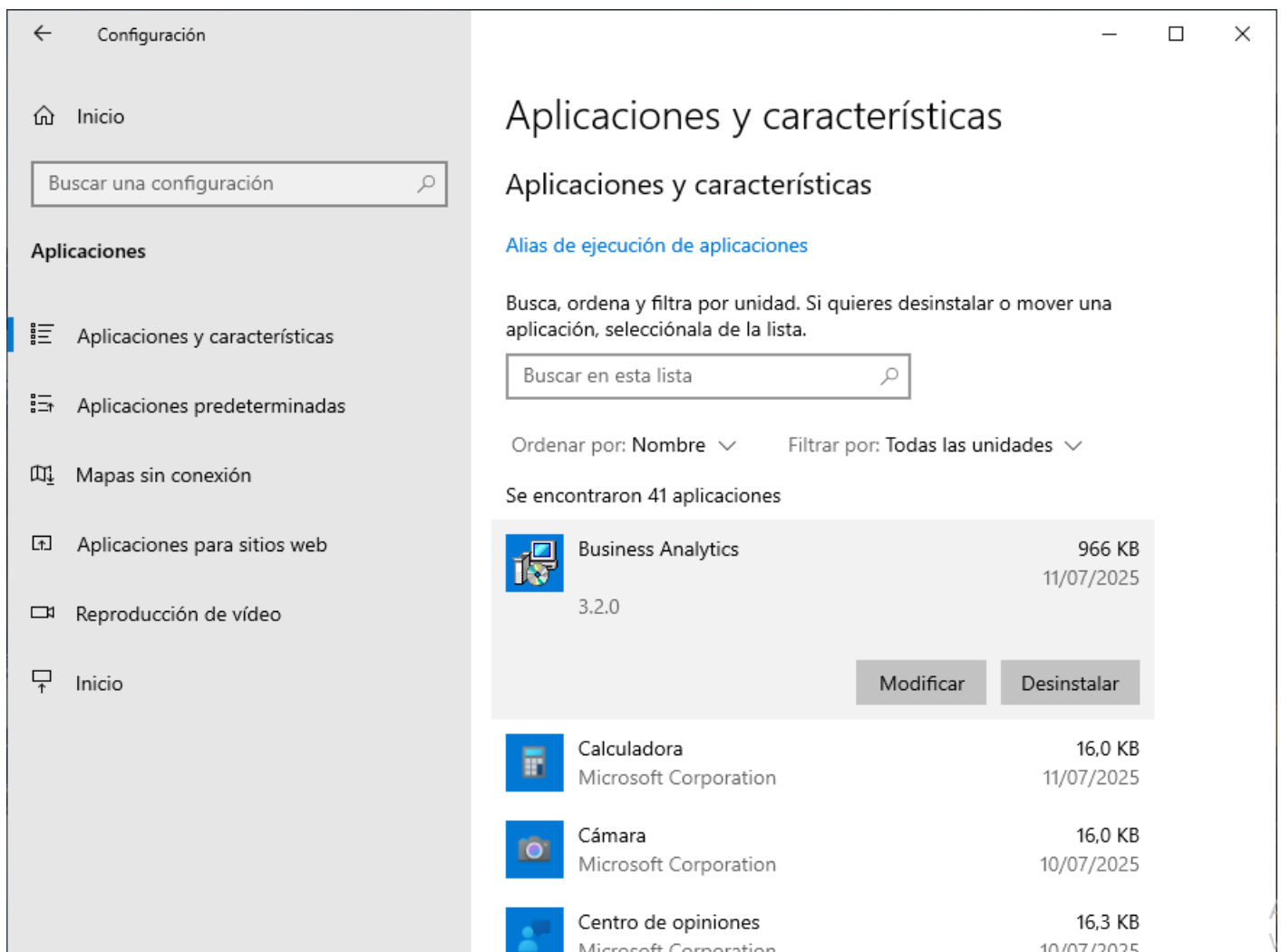
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
IdentifyingNumber      Name                                                                 LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional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

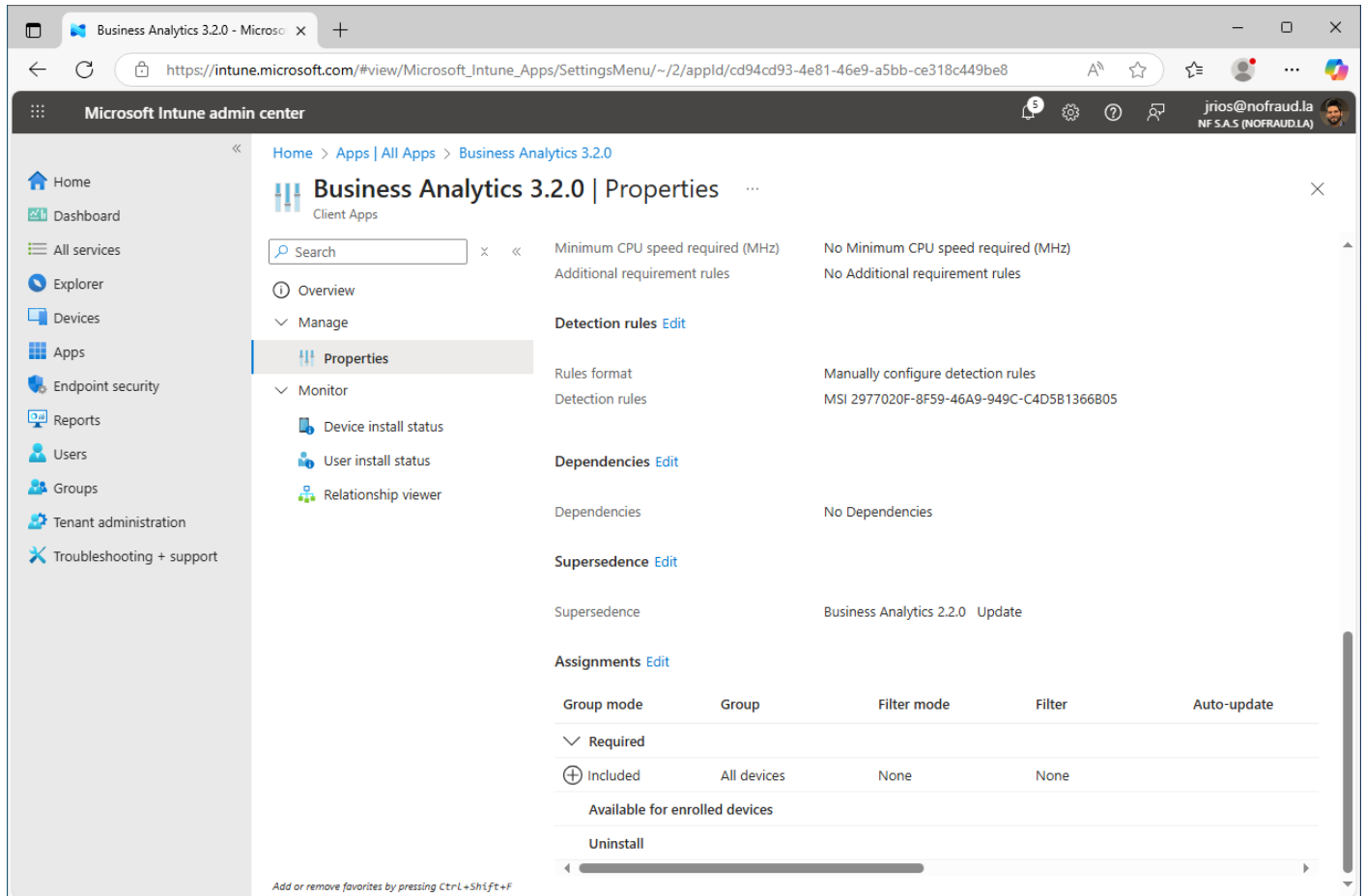


Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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

Desinstalación del agente

De clic en **Apps**, **All Apps** y seleccione la última versión del agente instalada. De clic en **Properties** y en **Assignments Edit**.



The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Business Analytics 3.2.0 | Properties' and includes a search bar and a list of configuration options:

- Minimum CPU speed required (MHz): No Minimum CPU speed required (MHz)
- Additional requirement rules: No Additional requirement rules
- Detection rules Edit
 - Rules format: Manually configure detection rules
 - Detection rules: MSI 2977020F-8F59-46A9-949C-C4D5B1366B05
- Dependencies Edit
 - Dependencies: No Dependencies
- Supersedence Edit
 - Supersedence: Business Analytics 2.2.0 Update
- Assignments Edit
 - Group mode: Required
 - Group: All devices
 - Filter mode: None
 - Filter: None
 - Available for enrolled devices: [checked]
 - Uninstall: [button]

A continuación ponga mucha atención a la operación que se realizará sobre las asignaciones.

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

Asignación de desinstalación

Se debe borrar de **Required** las entradas que previamente se añadieron. Luego, se deben crear en la categoría **Uninstall** las asignaciones de acuerdo al objetivo de desinstalación.

The screenshot shows the Microsoft Intune admin center interface. The main content area is titled "Edit application" for a "Windows app (Win32)" named "Business Analytics 3.2.0". The interface is divided into three sections:

- Required:** This section is currently empty, showing a table with columns for "Filter", "End user notifications", "Availability", "Installation deadline", "Restart grace period", and "Delivery optimization". Below the table are links to "+ Add group", "+ Add all users", and "+ Add all devices".
- Available for enrolled devices:** This section shows "No assignments" and a table with columns for "Group mode", "Group", "Filter mode", "Filter", "Auto-update", "End user notifications", and "Availability". Below the table are links to "+ Add group", "+ Add all users", and "+ Add all devices".
- Uninstall:** This section is active, showing a table with columns for "Group mode", "Group", "Filter mode", "Filter", "End user notifications", "Availability", and "Install". The table contains one entry: "Included" for "All devices" with "None" for filter mode and "None" for filter. The "End user notifications" column has a link "Show all toast notifications". Below the table are links to "+ Add group", "+ Add all users", and "+ Add all devices".

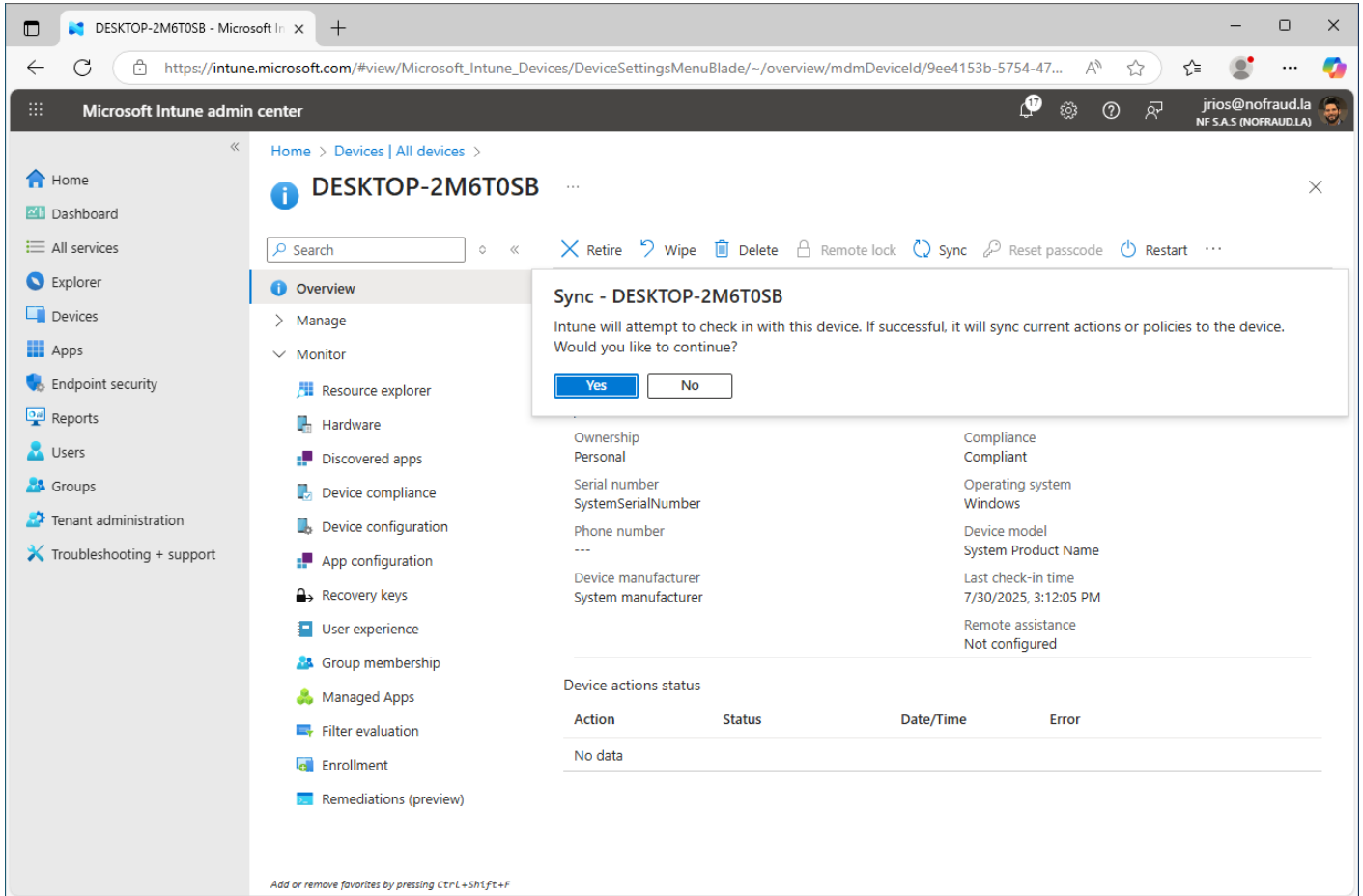
At the bottom of the page, there are two buttons: "Review + save" (highlighted in blue) and "Cancel".

Dar clic en **Review + save** y con esto ya estaría lista la política de desinstalación del agente.

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

Sincronización de dispositivo

Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'DESKTOP-2M6T0SB' and includes a search bar and action buttons: Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, and Restart. A 'Sync - DESKTOP-2M6T0SB' dialog box is open, asking for confirmation to sync current actions or policies to the device. Below the dialog, device details are displayed in two columns:

Property	Value
Ownership	Personal
Serial number	SystemSerialNumber
Phone number	---
Device manufacturer	System manufacturer
Compliance	Compliant
Operating system	Windows
Device model	System Product Name
Last check-in time	7/30/2025, 3:12:05 PM
Remote assistance	Not configured

Below the details, there is a 'Device actions status' table:

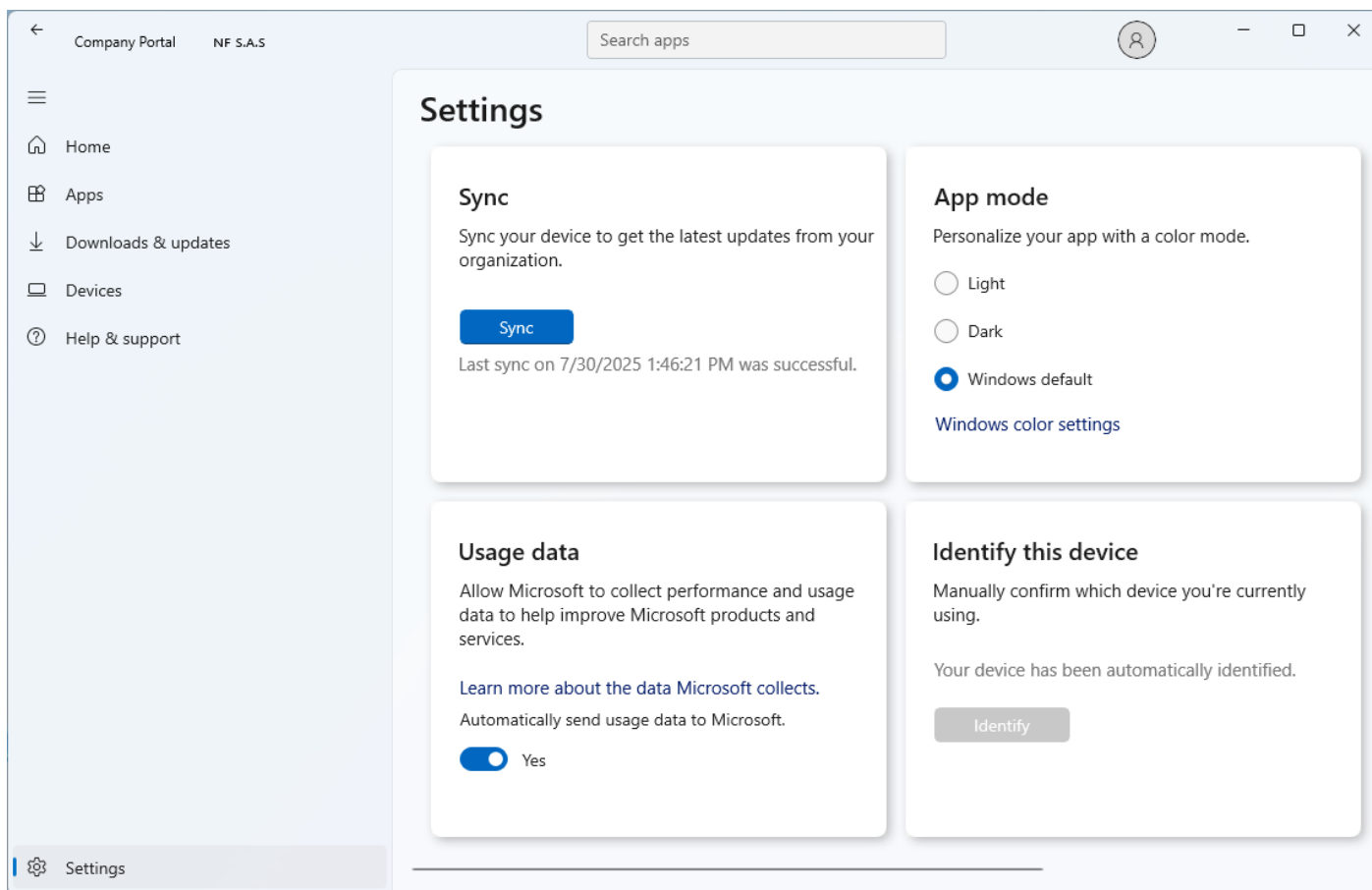
Action	Status	Date/Time	Error
No data			

El siguiente paso será forzar la sincronización del lado de las máquinas.

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

Sincronizar cliente Windows

Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.



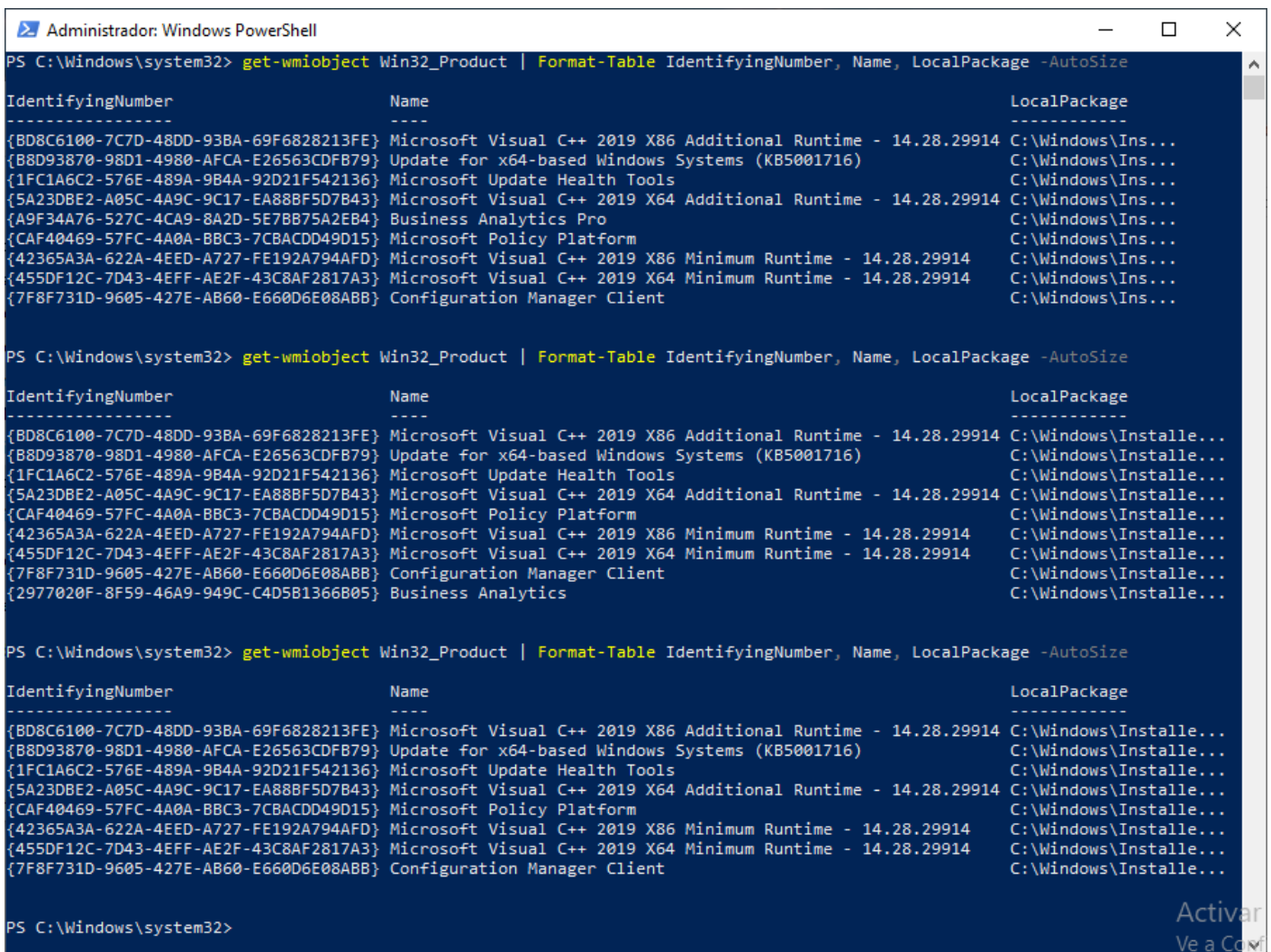
Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política y desinstalará el agente antifraude de manera inmediata en esta máquina.

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 acción de desinstalación en **Microsoft Intune**, ya no aparece la aplicación Business Analytics.