

Método de detección

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

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: Windows Installer

Specify an MSI product code: File System
Registry
Windows Installer

Product code: {A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Browse ...

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

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

MSI Property: Version

Operator: Equals

Value:

OK Cancel

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

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

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

Revision #5

Created 12 July 2025 01:36:19 by Julian Rios

Updated 16 July 2025 18:21:51 by Julian Rios