# Revisar análisis de Windows de terminales seguros (CSE)

## Contenido



## Introducción

Este documento describe los diferentes tipos de análisis de un conector de Windows.

## Prerequisites

Los requisitos previos para este documento son:

- Extremo de Windows
- Secure Endpoint (CSE) versión v.8.0.1.21164 o posterior
- Acceso a Secure Endpoint Console

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de terminal segura
- Extremo de Windows 10
- Versión de terminal seguro v.8.0.1.21164

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Los análisis se probaron en un entorno de laboratorio con la política establecida en debug.
La exploración de Flash durante la instalación se habilitó mediante la descarga del conector.
Los análisis se ejecutaron desde la GUI de Secure Client y desde Scheduler.

# Análisis completo

Este registro se muestra cuando se solicita un análisis completo desde la interfaz gráfica de usuario (GUI) de CSE.

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: Processing AMP_UI_SCAN action:
```

*Analizar desde la interfaz de usuario*

Aquí, el proceso ScanInitiator comienza el proceso Scan.

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: ScanInitiator::RequestScan: Attempting to start scan: dConnecte
```

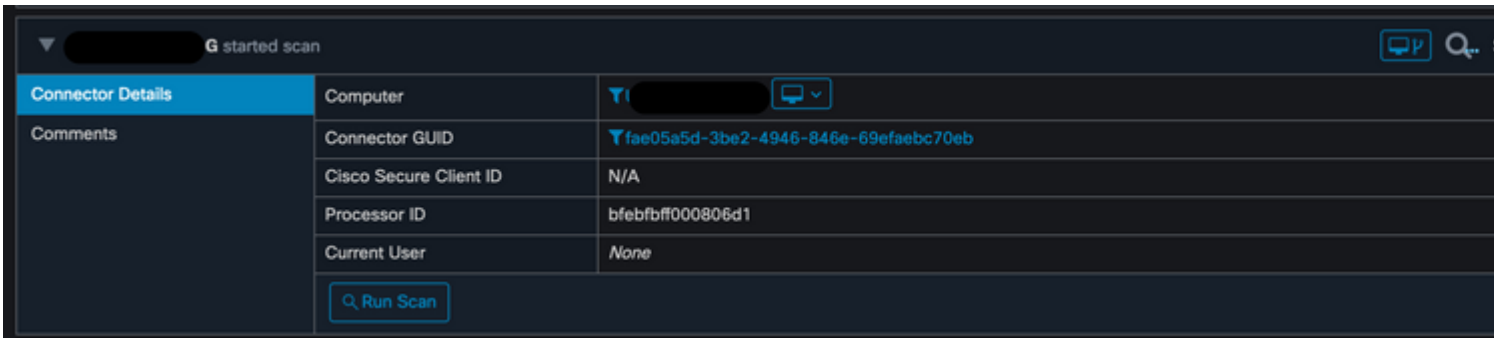
Puede ver que **Análisis completo** es el tipo de Análisis activado en la GUI como se muestra en la imagen.

A continuación, tiene el **Identificador de seguridad** (**SID)**, que es un valor de longitud variable asignado a este evento en particular, este Identificador de seguridad le ayuda a realizar el seguimiento del análisis en los registros.

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: imn::CEventManager::PublishEvent: publis
json={"iclsa":"0","sce":108,"scx":"Full Scan","sid":1407343,"sit":2,"sop":0,"stp":
ui64EventId=7135211821471891460
```

*Evento Publish*

Puede relacionar esto con el evento desde la consola CSE.




*Evento de consola*

A continuación, en los registros, puede ver lo siguiente:

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: PublishScanStartEvent publishing event suc
```

*Publicación correcta*

A continuación, la siguiente acción consiste en realizar el análisis:

En este ejemplo, puede ver cuándo se inicia el análisis y, como en el caso anterior, se proporciona un SID, esta vez, con un valor de **2458015.**

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: Scan::ScanThreadProcess: beginning scan id: 2458015, [type: 1, opt
```

*Inicio de escaneo Flash*

La siguiente acción consiste en publicar el evento en la nube de CSE.

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"ic
Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```

Cuando finalice el análisis, el evento se publicará en la nube.

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"ic
Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```

*Digitalización Finalizar publicación*

El evento se puede ver en el visor de eventos de Windows. Como puede observar, la información es la misma que la información presentada en los registros.

```
- <EventData>
    <Data Name="JsonEvent">{"dios":0,"ds":0,"hi":0,"scx":"Flash Scan","sdds":0,"sdfs":10951,"sdps":215,"sid":2458015,"s
      </Data>
    <Data Name="EventTypeId">554696715</Data>
    <Data Name="TimeStamp">133058605022030000</Data>
    <Data Name="EventId">7135602410092756997</Data>
    <Data Name="Description">EVENT_SCAN_COMPLETED_CLEAN</Data>
  </EventData>
</Event>
```

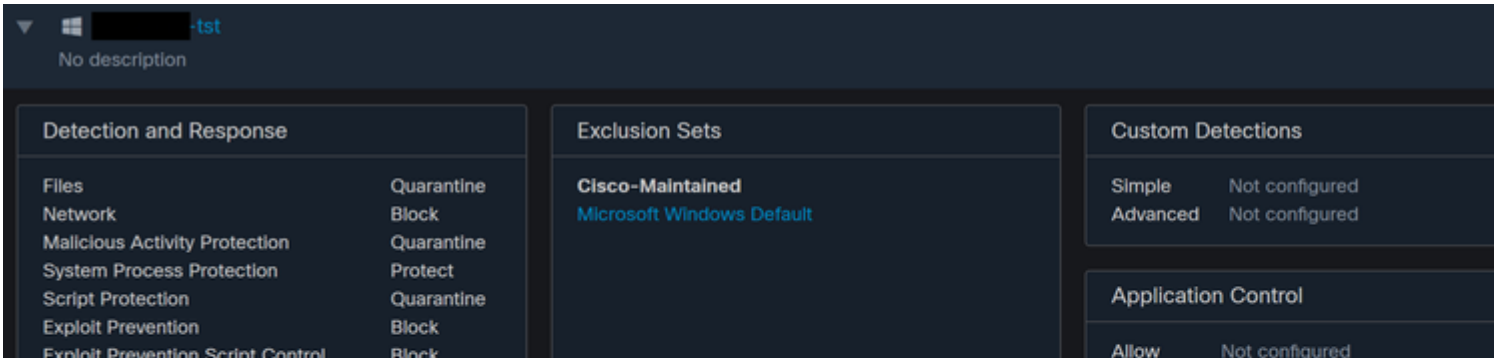
*Evento JSON*

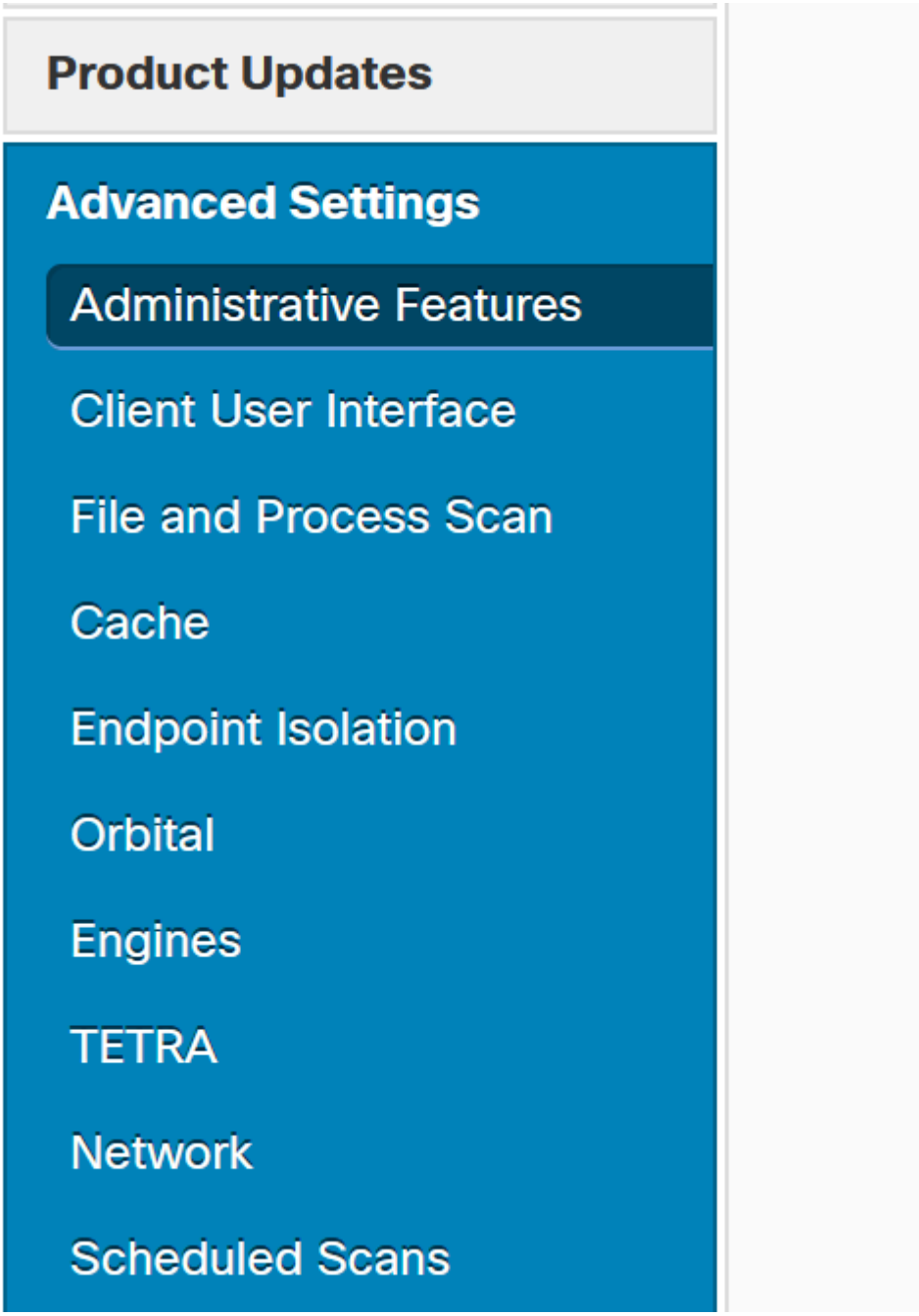
# Exploraciones programadas

Cuando se trata de análisis programados, debe tener en cuenta una serie de aspectos.

Después de programar un análisis, se produce un cambio en el número de serie.

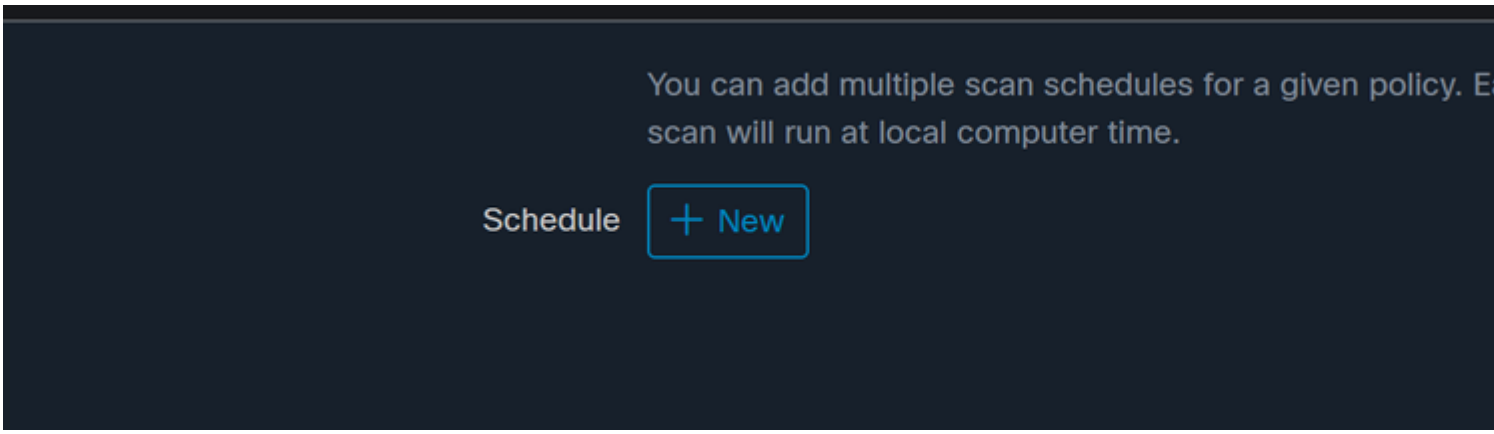
Aquí, la política de prueba no tiene ningún análisis programado.






*Configuración avanzada*

Haga clic en **New.**

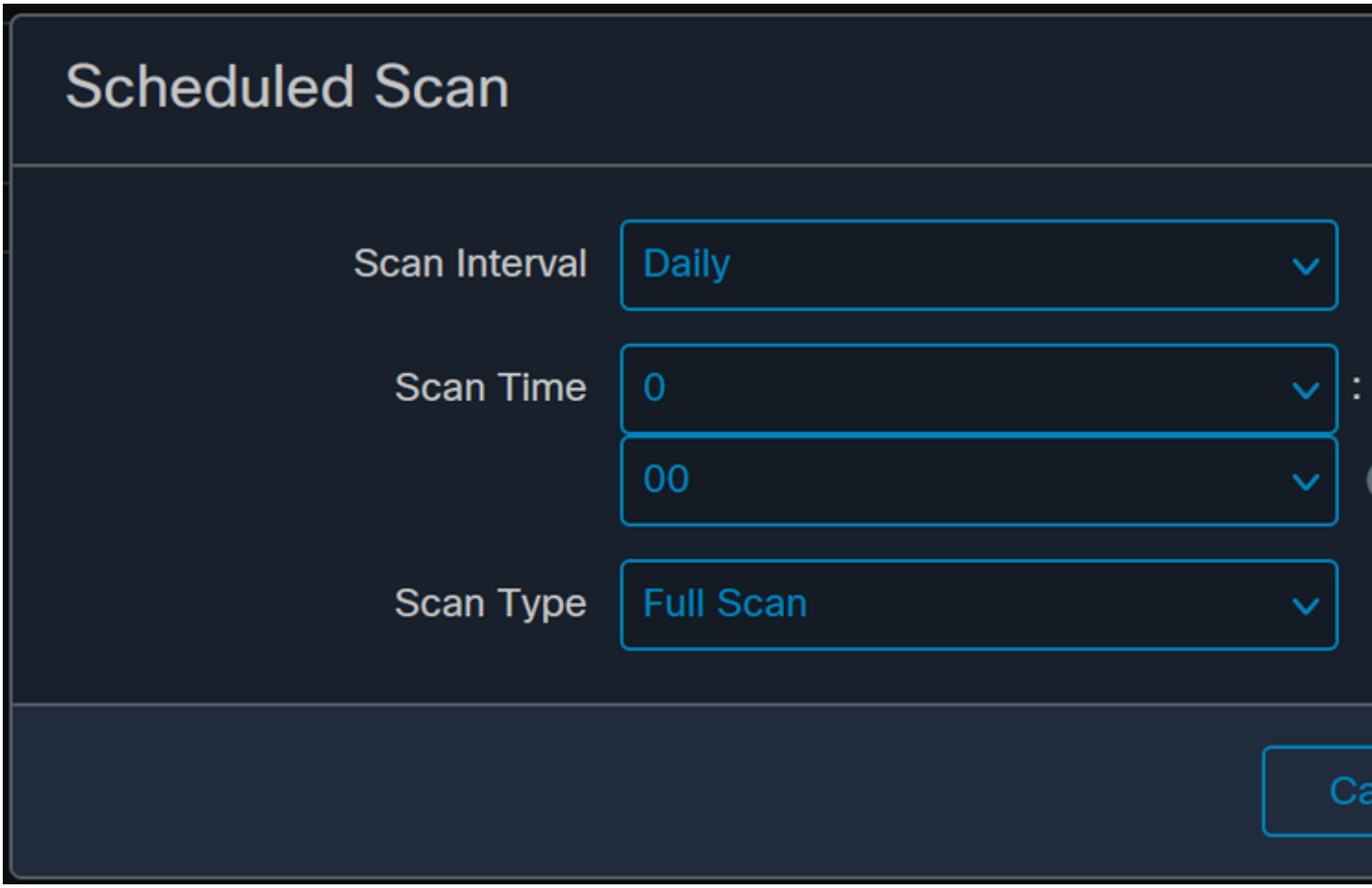



*Nueva configuración de análisis*

Las opciones son:

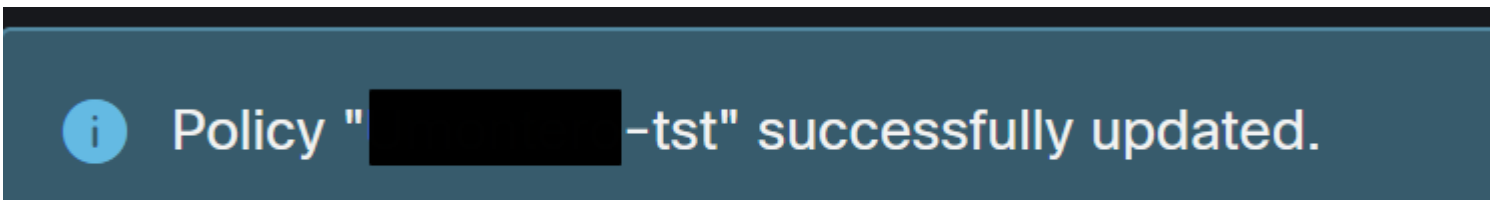
- Intervalo de análisis
- Tiempo de escaneo
- Tipo de análisis

Una vez configurado el análisis, haga clic en **Agregar**.




*Configuración de análisis programada*

**Guarde** los cambios de directiva y aparecerá una ventana emergente que confirma los cambios.



```
- <EventData>
    <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop
    <Data Name="EventTypeId">554696714</Data>
    <Data Name="TimeStamp">133059446390220000</Data>
    <Data Name="EventId">7135963775756140548</Data>
    <Data Name="Description">EVENT_SCAN_STARTED</Data>
  </EventData>
</Event>
```


*Cloud View*

Una vez finalizado el análisis, podrá ver el evento publicado en la nube.


```
(86641515, +0 ms) Aug 25 18:44:24 [3116]: imn::CEventManager::PublishEvent: publishing type=554696715, json={"
Scan","sdds":0,"sdfs":11575,"sdps":218,"sid":86616093,"sios":0,"sit":4,"sop":3,"sspc":0,"stp":1}, ui64EventId=
```


*Digitalización Finalizar publicación*

# Análisis completo programado

El visor de eventos de Windows muestra **Event Scan Started**, como se muestra en la imagen.


```
- <EventData>
    <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,
    <Data Name="EventTypeId">554696714</Data>
    <Data Name="TimeStamp">133059452390500000</Data>
    <Data Name="EventId">7135966352736518152</Data>
    <Data Name="Description">EVENT_SCAN_STARTED</Data>
  </EventData>
</Event>
```


Una vez finalizado, puede comparar el evento publicado.


```
(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEventManager::PublishEvent: publishing type=1091567628, json={
Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,"stp":5}, ui64Even
```


Puede ver esto en el visor de eventos de Windows.


```
- <EventData>
    <Data Name="JsonEvent">{"dios":0,"ds":2,"hi":0,"scx":"Full
      Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).