

Revisar verificações do Windows do Secure Endpoint (CSE)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Verificação completa](#)

[Varredura em Flash](#)

[Varreduras programadas](#)

[Verificação Completa agendada](#)

[Outras varreduras](#)

[Troubleshoot](#)

Introduction

Este documento descreve os diferentes tipos de varreduras de um conector do Windows.

Prerequisites

Os pré-requisitos para este documento são:

- Ponto de Extremidade do Windows
- Secure Endpoint (CSE) versão v.8.0.1.21164 ou posterior
- Acesso ao console de endpoint seguro

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Console de endpoint seguro
- Ponto de Extremidade do Windows 10
- Secure Endpoint versão v.8.0.1.21164

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As varreduras foram testadas em um ambiente de laboratório com a Política definida para depuração.
A varredura flash na instalação foi ativada por meio de download do Connector.
As varreduras foram executadas na GUI do Secure Client e no Agendador.

Verificação completa

Esse registro demonstra quando uma verificação completa é solicitada na interface gráfica do usuário (GUI) do CSE.

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

Digitalizar a partir da interface do usuário

Aqui, o processo ScanInitiator inicia o processo Scan.

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

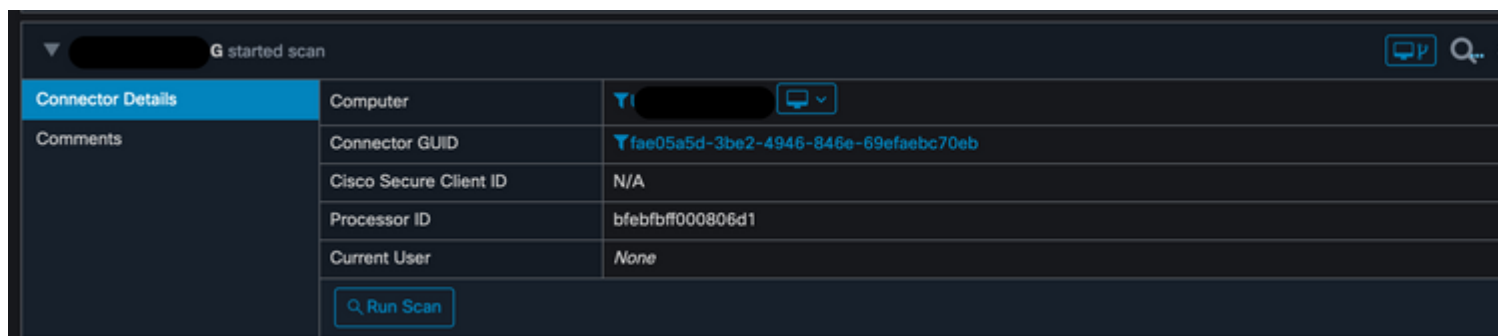
Você pode ver que **Varredura completa** é o tipo de Varredura acionada na GUI, como mostrado na imagem.

Em seguida, você tem o **Identificador de Segurança (SID)**, que é um valor de tamanho variável atribuído a esse evento específico, esse Identificador de Segurança ajuda a controlar a varredura nos logs.

```
(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
```

Publicar evento

Você pode fazer a correspondência disso com o evento no console do CSE.



Evento de console

Em seguida, nos logs, você pode ver isso:

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

Publicação Bem-sucedida

Em seguida, a próxima ação é, na verdade, executar a varredura:

Neste exemplo, você pode ver quando a Varredura é iniciada e, como anteriormente, um SID é fornecido, desta vez, com um valor de **2458015**.

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

Início da varredura flash

A próxima ação é publicar o evento na nuvem do 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
```

Quando a Varredura é concluída, o Evento é publicado na nuvem.

```
(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
```

Verificação Concluir Publicação

O evento pode ser visto no Visualizador de Eventos do Windows. Como você pode observar, as informações são as mesmas apresentadas nos logs.

```
- <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>
```

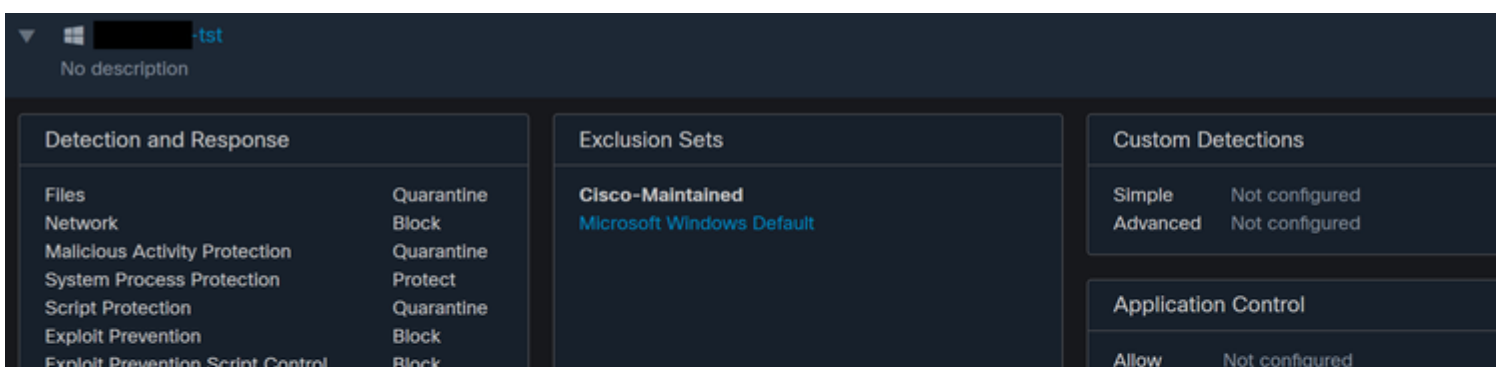
Evento JSON

Varreduras programadas

Quando se trata de varreduras programadas, você deve estar ciente de um conjunto de aspectos.

Depois que uma varredura é programada, ocorre uma alteração no número de série.

Aqui, a política de teste não tem nenhuma varredura programada.



Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbital

Engines

TETRA

Network

Scheduled Scans

Configurações avançadas

Clique em **New**.

You can add multiple scan schedules for a given policy. Each scan will run at local computer time.

Schedule

+ New

Nova Configuração de Verificação

As opções são:

- Intervalo de verificação
- Tempo de Verificação
- Tipo de Verificação

Depois de configurar a Varredura, clique em **Adicionar**.

Scheduled Scan

Scan Interval

Daily

Scan Time

0

00

Scan Type

Full Scan

Configuração da varredura programada

Salve suas alterações de política, uma janela pop-up será exibida confirmando suas alterações.



Policy "[REDACTED]-tst" successfully updated.


```
- <EventData>
  <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop":3,"sdds":0,"sdfs":11575,"sdps":218,"sios":0,"stp":1}, ui64EventId=7135963775756140548
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059446390220000</Data>
  <Data Name="EventId">7135963775756140548</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

Exibição em nuvem

Quando a verificação for concluída, você poderá ver o evento publicado na nuvem.

```
(86641515, +0 ms) Aug 25 18:44:24 [3116]: imn::CEventManager::PublishEvent: publishing type=554696715, json={"iclsa":"0","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop":3,"sdds":0,"sdfs":11575,"sdps":218,"sios":0,"stp":1}, ui64EventId=7135963775756140548
```

Verificação Concluir Publicação

Verificação completa agendada

O visualizador de eventos do Windows mostra **Event Scan Started**, como mostrado na imagem.

```
- <EventData>
  <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,"sdds":46012,"sdfs":280196,"sdps":224,"sios":0,"stp":5}, ui64EventId=7135966352736518152
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059452390500000</Data>
  <Data Name="EventId">7135966352736518152</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

Quando terminar, você poderá comparar o evento publicado.

```
(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEventManager::PublishEvent: publishing type=1091567628, json={"iclsa":"0","sce":108,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,"sdds":46012,"sdfs":280196,"sdps":224,"sios":0,"stp":5}, ui64EventId=7135966352736518152
```

Você pode ver isso no visualizador de eventos do Windows.

```
- <EventData>
  <Data Name="JsonEvent">{"dios":0,"ds":2,"hi":0,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,"sdds":46012,"sdfs":280196,"sdps":224,"sios":0,"stp":5}, ui64EventId=7135966352736518152
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059452390500000</Data>
  <Data Name="EventId">7135966352736518152</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.