

# Beoordeel Secure Endpoint (CSE) Windows-scans

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Volledig scannen](#)

[Flash scan](#)

[Geplande scans](#)

[Geplande volledige scan](#)

[Andere scans](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft de verschillende typen scans van een Windows-connector.

## Voorwaarden

De voorwaarden voor dit document zijn:

- Windows-endpoint
- Secure Endpoint (CSE) versie v.8.0.1.21164 of hoger
- Toegang tot Secure Endpoint-console

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Endpoint-console
- Windows 10-endpoint
- Secure Endpoint versie v.8.0.1.21164

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

De scans werden getest op een lab-omgeving met Policy ingesteld om te debuggen. Flash scan on install was ingeschakeld via Connector download.

De scans zijn uitgevoerd vanuit de Secure Client GUI en vanuit de Scheduler.

## **Volledig scannen**

Dit logbestand toont aan wanneer een volledige scan wordt aangevraagd via de GUI (Graphic User Interface - grafische gebruikersinterface) van CSE.

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

Scannen vanaf gebruikersinterface

Hier begint het ScanInitiator-proces met het scanproces.

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

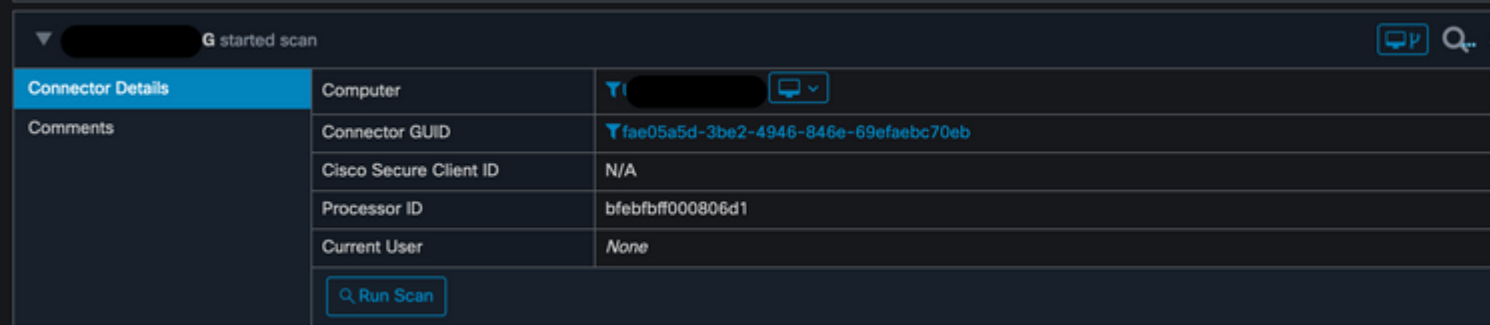
U kunt zien dat **Full Scan** het type Scannen is dat op de GUI is geactiveerd, zoals in de afbeelding wordt weergegeven.

Vervolgens hebt u de **Security Identifier (SID)**, die een waarde is van variabele lengte toegewezen aan deze bepaalde gebeurtenis, deze Security Identifier helpt u de scan in de logbestanden te volgen.

```
(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
```

Publicatiegebeurtenis

U kunt dit afstemmen op de gebeurtenis vanuit de CSE-console.



The screenshot shows a table with the following data:

Connector Details	
Computer	[redacted]
Connector GUID	fae05a5d-3be2-4946-846e-69efaebc70eb
Cisco Secure Client ID	N/A
Processor ID	bfebfbf000806d1
Current User	None

Below the table is a button labeled "Run Scan".

Console-gebeurtenis

Daarna, in de logboeken, kunt u dit zien:

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

Geslaagd publiceren

Dan is de volgende actie eigenlijk het scannen:

In dit voorbeeld kunt u zien wanneer het Scannen start, en zoals eerder, wordt deze keer een SID gegeven, met een waarde van **2458015**.

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

Flash scan start

De volgende actie is om het evenement te publiceren naar de CSE cloud.

```
(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
```

Wanneer de scan is voltooid, wordt de Event gepubliceerd in de cloud.

```
(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
```

Scannen Voltooien publiceren

De gebeurtenis is te zien in de Windows Event viewer. Zoals u kunt opmerken, is de informatie hetzelfde als de informatie die in de logboeken wordt gepresenteerd.

```
- <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>
```

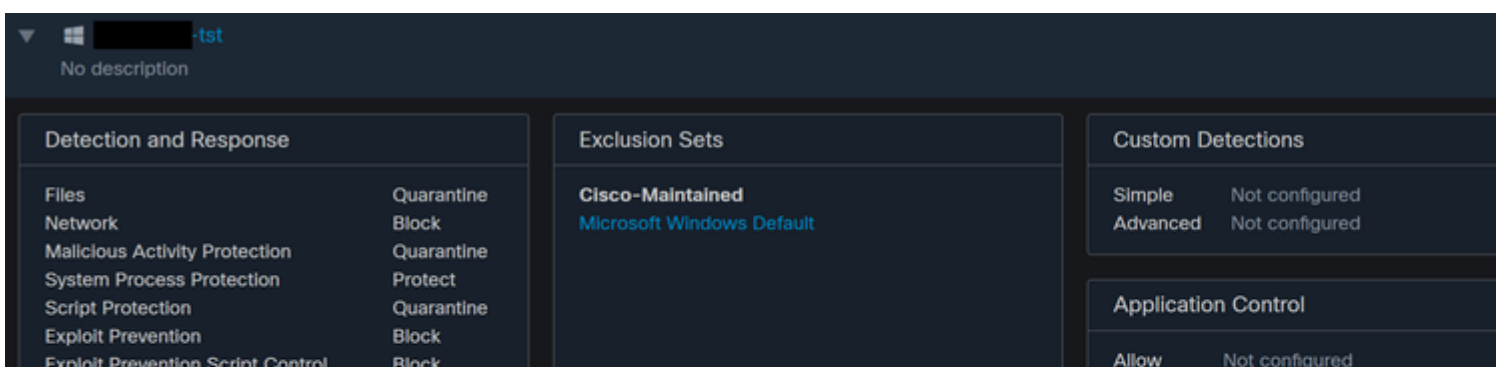
JSON Event

## Geplande scans

Wanneer het gaat om Geplande scans, moet u zich bewust zijn van een reeks aspecten.

Nadat een scan is gepland, verandert het serienummer.

Op dit punt is het testbeleid niet voorzien van geplande scans.



## Product Updates

### Advanced Settings

#### Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbital

Engines

TETRA

Network

Scheduled Scans

*Geavanceerde instellingen*

Klik op **New (Nieuw)**.

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

Schedule

+ New

*Nieuwe scanconfiguratie*

De opties zijn:

- Scaninterval
- Scantijd
- Scantype

Klik op **Toevoegen** nadat u de scan hebt geconfigureerd.

## Scheduled Scan

Scan Interval

Daily

Scan Time

0

00

Scan Type

Full Scan

*Geplande scanconfiguratie*

**Sla** uw beleidswijzigingen op. Er verschijnt een pop-up die uw wijzigingen bevestigt.



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>

```

Cloudweergave

Als de scan is voltooid, kunt u de gebeurtenis zien die wordt gepubliceerd in de cloud.

```

(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

```

Scannen Voltooien publiceren

## Geplande volledige scan

In de Windows-gebeurtenisviewer wordt **Event Scan gestart**, zoals in de afbeelding wordt getoond.

```

- <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>

```

Als het klaar is, kun je het gepubliceerde evenement vergelijken.

```

(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

```

U kunt dit zien in de gebeurtenisviewer vanuit 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

```

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.