

Windows-Scans für sichere Endgeräte (CSE) überprüfen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vollständige Suche](#)

[Flash-Scan](#)

[Geplante Scans](#)

[Zeitgesteuerte Vollständige Suche](#)

[Andere Scans](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument werden die verschiedenen Scantypen eines Windows-Connectors beschrieben.

Voraussetzungen

Dieses Dokument setzt Folgendes voraus:

- Windows-Endpunkt
- Secure Endpoint (CSE) Version v.8.0.1.21164 oder höher
- Zugriff auf die Konsole für sichere Endgeräte

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Konsole für sichere Endgeräte
- Windows 10-Endgerät
- Secure Endpoint Version v.8.0.1.21164

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Scans wurden in einer Laborumgebung getestet, wobei die Richtlinie auf debug festgelegt war.
Der Flash-Scan bei der Installation wurde über Connector-Download aktiviert.
Die Scans wurden über die Secure Client-GUI und den Scheduler ausgeführt.

Vollständige Suche

Dieses Protokoll veranschaulicht, wenn eine vollständige Suche über die grafische Benutzeroberfläche (GUI) von CSE angefordert wird.

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

Scannen über die Benutzeroberfläche

Hier startet der ScanInitiator-Prozess den Scan-Prozess.

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

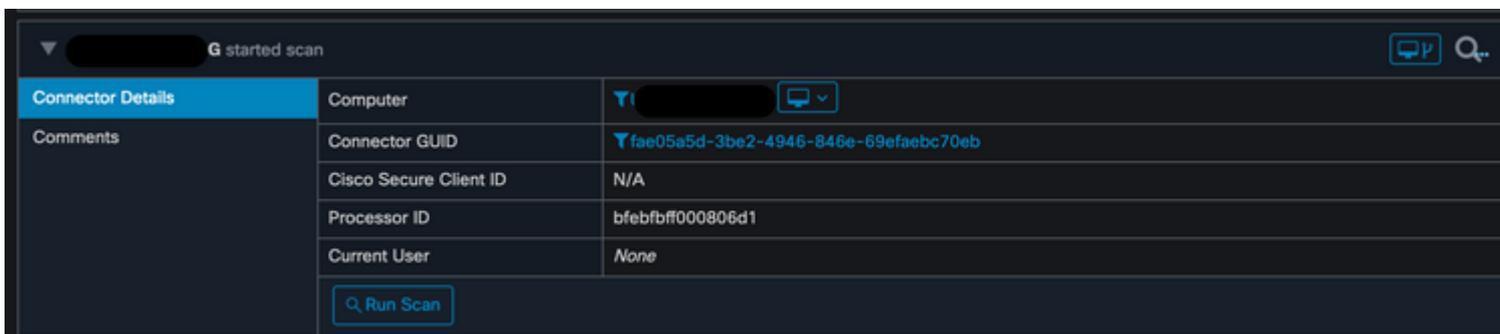
Sie können sehen, dass **Vollständige Suche** die Art der auf der GUI ausgelösten Suche ist, wie im Bild gezeigt.

Als Nächstes haben Sie die **Sicherheits-ID (Security Identifier, SID)**, die ein Wert variabler Länge ist, der diesem bestimmten Ereignis zugewiesen ist. Diese Sicherheits-ID hilft Ihnen, den Scan in den Protokollen zu verfolgen.

```
(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
```

Veröffentlichungsereignis

Sie können dies mit dem Ereignis in der CSE-Konsole abgleichen.



The screenshot shows a table with the following details:

Connector Details	Computer	Ti [dropdown]
Comments	Connector GUID	fae05a5d-3be2-4946-846e-69efaebc70eb
	Cisco Secure Client ID	N/A
	Processor ID	bfebfbff000806d1
	Current User	None
	<input type="button" value="Run Scan"/>	

Konsolenergebnis

Als Nächstes sehen Sie in den Protokollen Folgendes:

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

Veröffentlichung erfolgreich

Als Nächstes führen Sie den Scan aus:

In diesem Beispiel sehen Sie, wann der Scan gestartet wird. Wie zuvor wird dieses Mal eine SID mit dem Wert 2458015 **vergeben**.

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

Starten des Flash-Scans

Als Nächstes muss die Veranstaltung in der CSE-Cloud veröffentlicht werden.

```
(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
```

Wenn der Scan abgeschlossen ist, wird das Ereignis in der Cloud veröffentlicht.

```
(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
```

Veröffentlichen des Scan-Abschlusses

Das Ereignis wird in der Windows-Ereignisanzeige angezeigt. Wie Sie feststellen können, sind die Informationen die gleichen wie die Informationen in den Protokollen dargestellt.

```
- <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>
```

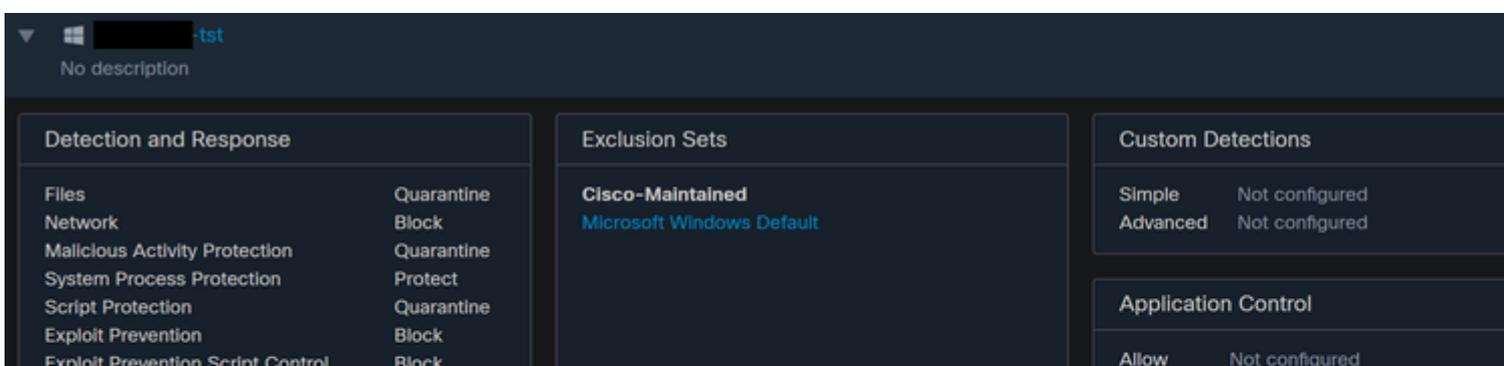
JSON-Veranstaltung

Geplante Scans

Bei der zeitgesteuerten Suche müssen Sie eine Reihe von Aspekten berücksichtigen.

Nachdem eine Suche geplant wurde, wird die Seriennummer geändert.

In diesem Fall enthält die Testrichtlinie keine zeitgesteuerten Scans.



Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbital

Engines

TETRA

Network

Scheduled Scans

Erweiterte Einstellungen

Klicken Sie auf **Neu**.

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

Schedule

+ New

Neue Suchkonfiguration

Folgende Optionen sind verfügbar:

- Scan-Intervall
- Suchzeit
- Suchtyp

Nachdem Sie die Suche konfiguriert haben, klicken Sie auf **Hinzufügen**.

Scheduled Scan

Scan Interval

Daily

Scan Time

0

00

Scan Type

Full Scan

Konfiguration der zeitgesteuerten Suche

Speichern Sie Ihre Richtlinienänderungen. Ein Popup-Fenster wird angezeigt, das Ihre Änderungen bestätigt.



Policy "

-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>

```

Cloud-Ansicht

Sobald der Scan abgeschlossen ist, können Sie das in der Cloud veröffentlichte Ereignis sehen.

```

(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

```

Veröffentlichen des Scan-Abschlusses

Geplante vollständige Suche

In der Windows-Ereignisanzeige wird **Event Scan Started** angezeigt, wie im Bild dargestellt.

```

- <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>

```

Anschließend können Sie die veröffentlichte Veranstaltung vergleichen.

```

(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

```

Sie können dies in der Ereignisanzeige von Windows aus sehen.

```

- <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

```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.