

# HAR-logbestanden van SecureX-console verzamelen

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem:](#)

[Oplossing:](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u HAR-logs (HTTP Archive) kunt verzamelen vanuit een browser.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

### Probleem:

TAC gebruikt HAR-logbestanden om problemen met betrekking tot de SecureX-console op te lossen.

Met de informatie in de HAR-logbestanden kan TAC de API-vragen die aan de SecureX-backend server zijn gesteld, beoordelen en een probleem efficiënt isoleren.

### Oplossing:

Stap 1. Navigeer naar de SecureX-console.

Stap 2. Navigeer naar het gedeelte waar de problemen worden gepresenteerd en klik met de

rechtermuisknop.

### Step 3. Selecteer Inspect.

The screenshot shows the Cisco SecureX dashboard with the 'Insights' tab selected. The main content area displays 'Source Health' with a 75% progress indicator, 'Types' (0 Devices), and 'Status' (0 Managed, 0 Unmanaged). A browser context menu is open over the 'Inspect' button, with 'Inspect' highlighted. The menu options include: Back, Forward, Reload, Bookmark Page, Save Page As..., Save Page to Pocket, Select All, Take Screenshot, View Page Source, Inspect Accessibility Properties, Inspect, and Block element... The dashboard also shows a 'Filters' section with various search and filter options.

### Step 4. Navigeer naar het network tabblad.

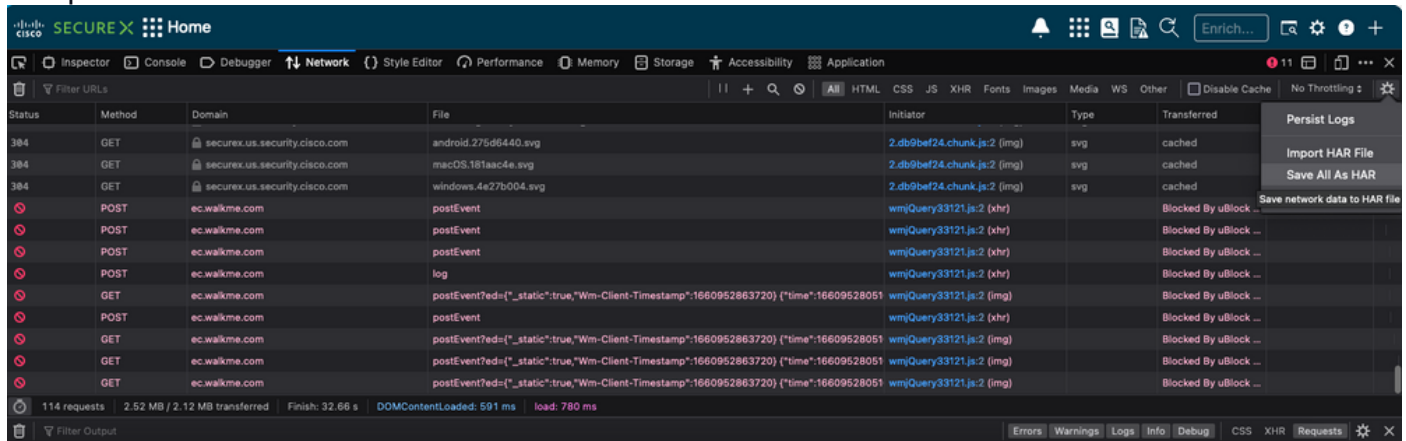
The screenshot shows the Cisco SecureX dashboard with the 'Network' tab selected in the browser's developer tools. The 'Network' tab is active, displaying a list of requests. The first request is a 200 status OPTIONS request to visibility.amp.cisco.com for the file notifications. The second request is a 200 status GET request to visibility.amp.cisco.com for the file notifications, initiated by ats-ribbon.js:1 (xhr) in JSON format. The developer tools also show the 'Console' tab with a 'Cross-Origin Request Blocked' error message.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	OPTIONS	visibility.amp.cisco.com	notifications	xhr	plain	936 B	18 B	71 ms
200	GET	visibility.amp.cisco.com	notifications	ats-ribbon.js:1 (xhr)	json	900 B	2 B	98 ms

Step 5. Reproduceer het probleem of herlaad de pagina zodat alle vragen in de logs kunnen worden opgenomen.

Step 6. Selecteer het pictogram Engine en selecteer save All as HAR om de logbestanden op uw

computer te archiveren.



Stap 7. Zodra u het HAR-bestand hebt gemaakt, uploadt u het bestand naar het [Support Case Manager](#) in uw TAC-case.

## Gerelateerde informatie

- [Officiële SecureX-documentatie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## 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.