

# Secure met Advanced Malware Protection (AMP) voor endpoints en integratiegids

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Generate API Credentials in AMP console](#)

[SecureX-lintje in AMP-console inschakelen](#)

[Opnemen van de Advanced Malware Protection voor endpoints in SecureX](#)

[Verifiëren](#)

[Problemen oplossen](#)

[API-client heeft geen schrijftoegang \[403\]](#)

[Fout: Onbekende API-toets of client-ID \[401\]](#)

[Video-handleiding](#)

## Inleiding

Dit document beschrijft het proces dat vereist is om Cisco SecureX met Cisco Advanced Malware Protection (AMP) te integreren en te controleren voor endpoints.

Bijgedragen door Yeraldin Sanchez en Uriel Torres, bewerkt door Jorge Navarrete, Cisco TAC-engineers.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Advanced Malware Protection voor endpoints
- Basisnavigatie in de SecureX-console
- Optioneel virtualisatie van afbeeldingen

### Gebruikte componenten

- Advanced Malware Protection voor endpoints versie 5.4.2008-04
- Advanced Malware Protection voor endpoints
- SecureX-console versie 1.5.4
- SecureX-beheeraccount

- Microsoft Edge versie 8.0.52.52

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

Cisco Advanced Malware Protection (AMP) voor endpoints is een kernonderdeel van het beveiligingsplatform voor endpoints en wordt uitgevoerd als een preventieve en onderzoekstool dat detectie- en/of reactiefuncties voor Windows-, MacOS-, Linux-, Android- en iOS-apparaten ondersteunt, biedt de Advanced Malware Protection voor endpoints 5 tegels.

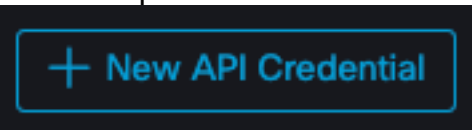
- **Door AMP herkende compromissen:** Een reeks parameters die compromissen samenvat die door AMP worden gedetecteerd
- **Samenvatting van AMP-computers:** Een reeks parameters die de status van AMP-computers samenvat
- **AMP Summary:** A set metriek die AMP-detectie en -respons samenvat
- **AMP-wachtrijen:** Een verzameling metriek die AMP Quarantines per keer samenvat
- **MITER ATT&CK Tactics gedetecteerd door AMP:** Een verzameling parameters die MITER ATT&CK-tactieken samenvat die door AMP zijn gedetecteerd

## Configureren

### Generate API Credentials in AMP console

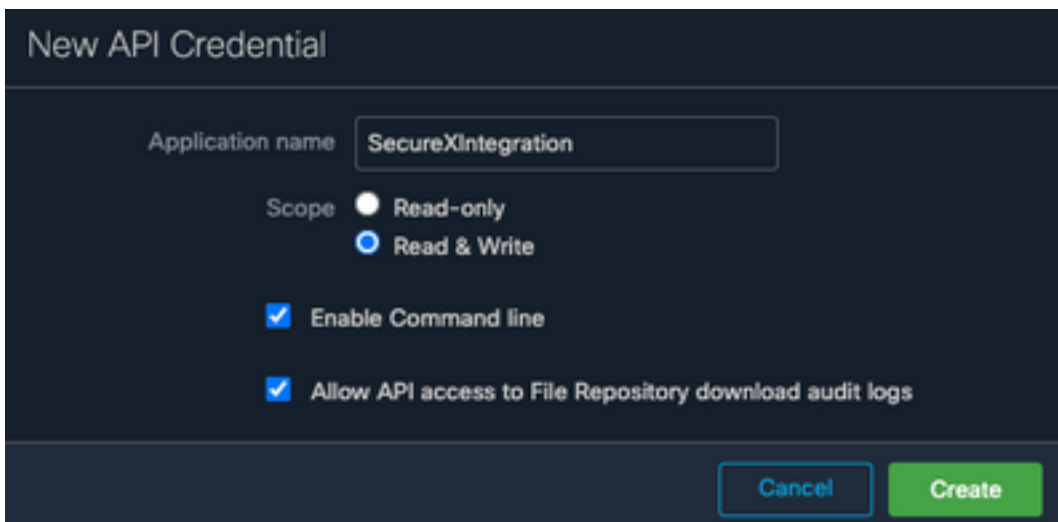
In de AMP-console worden nieuwe API-referenties gemaakt.

- Meld u aan bij de AMP-console met Administrator-rechten
- navigeer in de AMP-console naar **accounts > API-Credentials**
- Klik op **New API Credentials**



+ New API Credential

- Naam van de toepassing
- Selecteer **Lezen en schrijven**
- Controleer **Opdrachtlijn inschakelen** en **geef API toegang tot auditbestanden met bestandsindeling**.
- Klik op **Maken**



New API Credential

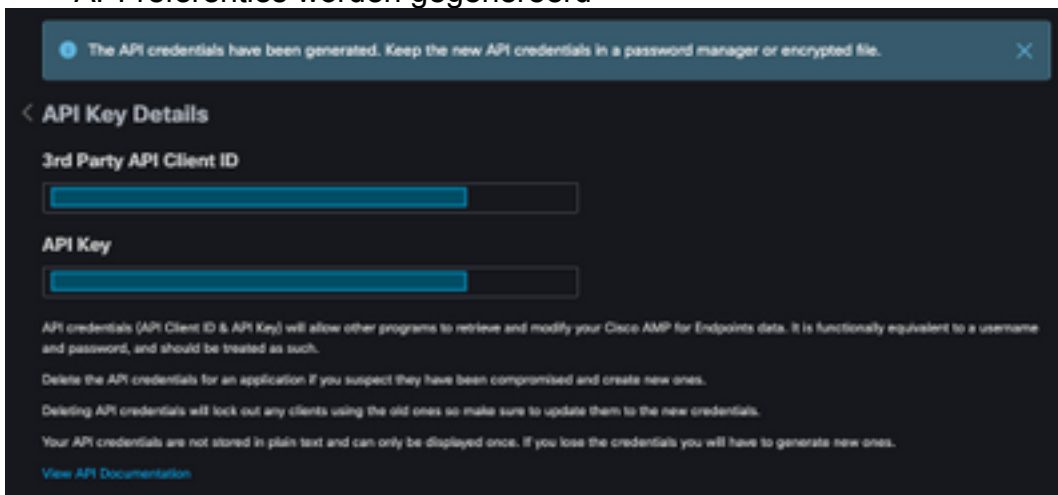
Application name

Scope  Read-only  Read & Write

Enable Command line

Allow API access to File Repository download audit logs

- API-referenties worden gegenereerd



The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

< API Key Details

3rd Party API Client ID

API Key

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

Opmerking: Deze informatie is alleen beschikbaar in dit venster, maar slaat uw aanmeldingsgegevens op in een reservekopiebestand.

## SecureX-lintje in AMP-console inschakelen

SecureX is zowel een gecentraliseerde console als een gedistribueerde reeks functies die zichtbaarheid verenigen, automatisering mogelijk maken, de respons op incidenten versnellen en de jacht op bedreigingen verbeteren. Deze gedistribueerde functies worden aangeboden in de vorm van toepassingen (apps) en tools in SecureX Ribbon. SecureX Ribbon kan worden geactiveerd in de AMP-console.

- Inloggen op SecureX
- Op de AMP-console
- Navigeren naar **accounts > Gebruikers > Klik op uw gebruiker**
- Klik in **het vakje Settings** op SecureX Ribbon **Authorized**

## Settings

Two-Factor Authentication [Manage](#)

Remote File Fetch **Enabled**

Command Line **Enabled**

Endpoint Isolation **Enabled**

Time Zone **UTC**

Appearance **Auto** Light Dark

SecureX Ribbon [Authorize](#)

Google Analytics [Opt Out](#)

- U wordt terugverwezen naar de SecureX Threat Response
- Klik op **AMP autoriseren voor endpoints**

## Grant Application Access

The application **AMP for Endpoints** ([console.amp.cisco.com](https://console.amp.cisco.com)) would like access to your Cisco Threat Response account.

Specifically, **AMP for Endpoints** is requesting the following:

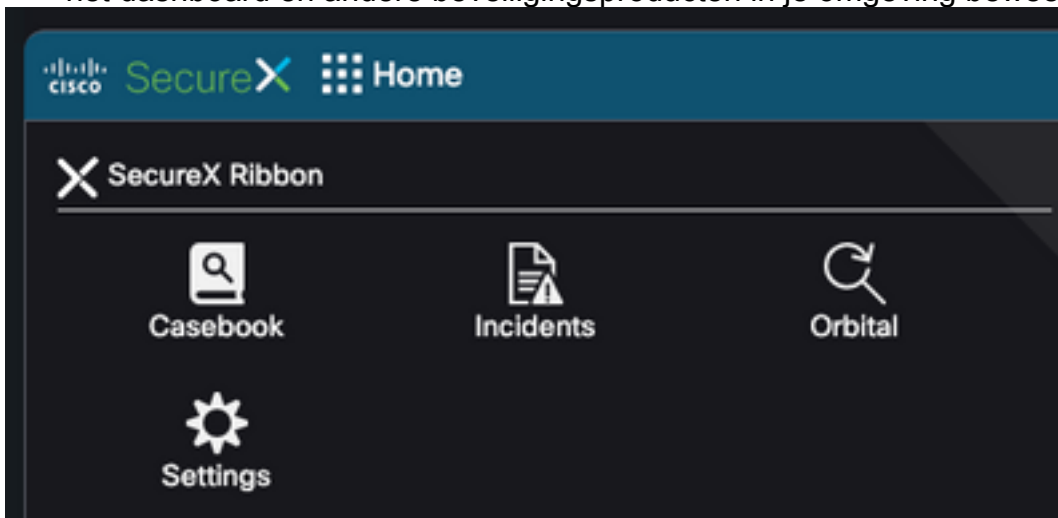
- **casebook**: access and modify your casebooks
- **enrich**: query your configured modules for threat intelligence (*enrich:read*)
- **global-intel**: query AMP Global Intelligence
- **inspect**: extract observables and data from text (*inspect:read*)
- **integration**: manage your integration modules configuration (*integration/module-instance:read, integration/module-type:read*)
- **orbital**
- **private-intel**: access Private Intelligence
- **profile**
- **registry** (*registry/user/ribbon*)
- **response**: list and execute response actions using configured modules
- **telemetry** (*telemetry:write*)
- **users**

[Authorize AMP for Endpoints](#)

Deny

- Het lintje bevindt zich in het onderste gedeelte van de pagina en blijft bestaan terwijl je tussen

het dashboard en andere beveiligingsproducten in je omgeving beweegt



## Opnemen van de Advanced Malware Protection voor endpoints in SecureX

Met de module Advanced Malware Protection voor endpoints kunt u meerdere bestanden met context van integraties tussen beveiligingsproducten onderzoeken en identificeren. Het verstrekt gedetailleerde informatie over beïnvloede endpoints en apparaten, waaronder IP adressen, OS, en AMP GUID.

- Op SecureX-console navigeren naar **integraties > Klik op Add New Module**
- Selecteer de **Advanced Malware Protection voor endpoints** en klik op **Nieuwe module toevoegen**
- Naam van de module
- Selecteer de **Advanced Malware Protection Cloud**
- De eerder verzamelde API-crediteuren worden ingevoerd onder **client-ID van derden** en **API-toets**


## Add New AMP for Endpoints Module

Module Name\*

URL\*

3rd Party API Client ID\*

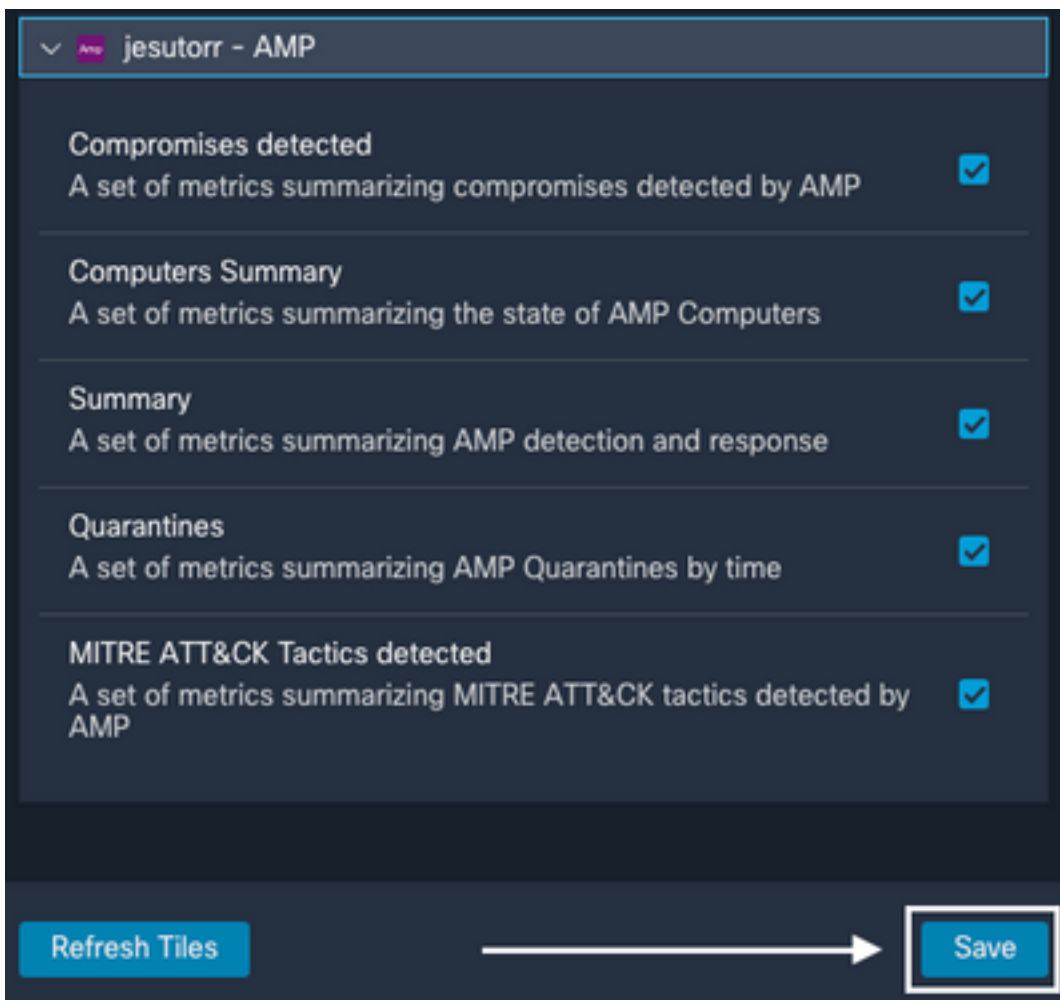
API Key\*

Act in the name of Active User 

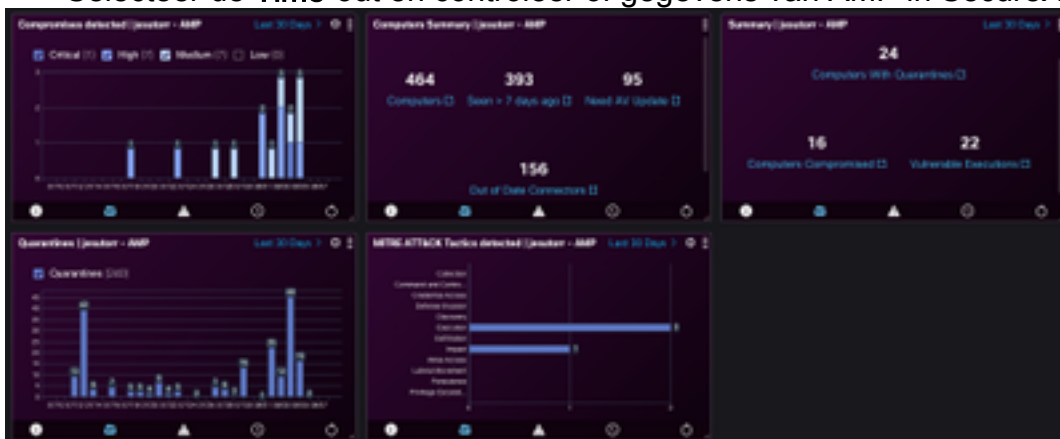
## Verifiëren

Bevestig dat de informatie uit de AMP-console in het SecureX-dashboard wordt weergegeven.

- Op SecureX navigeren naar **Dashboard**
- Klik op **Nieuw Dashboard** en noem het op
- Selecteer de eerder gegenereerde AMP-module
- Selecteer de tegels. Voor deze geleider worden deze allemaal toegevoegd
- Klik op **Opslaan**



- Selecteer de **Time-out** en controleer of gegevens van AMP in SecureX worden weergegeven



## Problemen oplossen

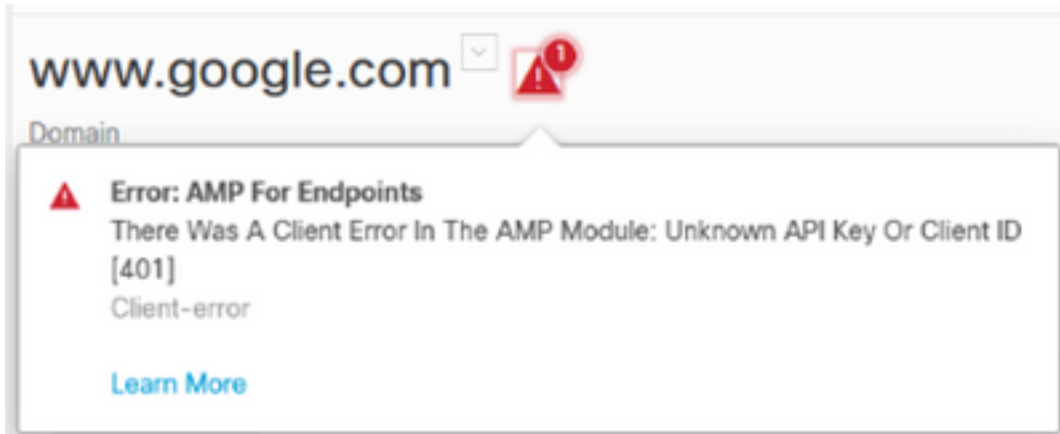
### API-client heeft geen schrijftoegang [403]

Voor SecureX - AMP voor endpoints Integration is OCR-oplossing **nodig** voor endpoints en API's. Indien niet, wordt er een foutmelding weergegeven zoals in de afbeelding.



## Fout: Onbekende API-toets of client-ID [401]

Als de API's niet geldig zijn als een onderzoek wordt uitgevoerd in SecureX Threat Response zoals in de afbeelding getoond.



Controleer of de API-referenties geldig zijn of bestaan in de AMP-console, als dat niet het geval is, probeer dan nieuwe.

Als u de bovenstaande informatie hebt bekeken, neemt u contact op met Support.

## Video-handleiding