Umbrella Reporting API gebruiken via Postman

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Umbrella Reporting API in Postman kunt gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

Overzicht

De Umbrella API werd uitgebracht in september 2022 en biedt een gebruiksvriendelijk en veilig platform waarmee gebruikers kunnen bouwen op, uitbreiden en integreren met Umbrella.

De Umbrella API-eindpunten worden gehost op api.umbrella.com, met gegroepeerde paden per use case. API-sleutels kunnen zowel in het Umbrella-dashboard worden beheerd, onder Admin > API-sleutels, als programmatisch met de KeyAdmin API. Elke sleutel kan granulair worden geconfigureerd met meerdere scopes gegroepeerd onder vijf primaire use cases:

- Admin API-eindpunten stellen u in staat om Umbrella API-sleutels en -gebruikers te leveren en te beheren, rollen te bekijken en klanten voor providers en beheerde providers te beheren.
- Auth API-eindpunten stellen u in staat om de integraties van andere services met het Umbrella-platform te autoriseren.
- Met implementaties API-eindpunten kunt u netwerken en andere verschillende entiteiten aanbieden, bewaken en beheren en beveiligen door ze te configureren in uw bestaande overkoepelende beleidsregels.
- Met API-eindpunten voor beleidsregels kunt u bestemmingslijsten en de bestemmingen per lijst aanbieden en beheren.
- Met API-eindpunten voor rapporten kunt u realtime beveiligingsinformatie over uw implementaties lezen en controleren. De Umbrella App Discovery API biedt inzicht in uw cloudgebaseerde applicaties.

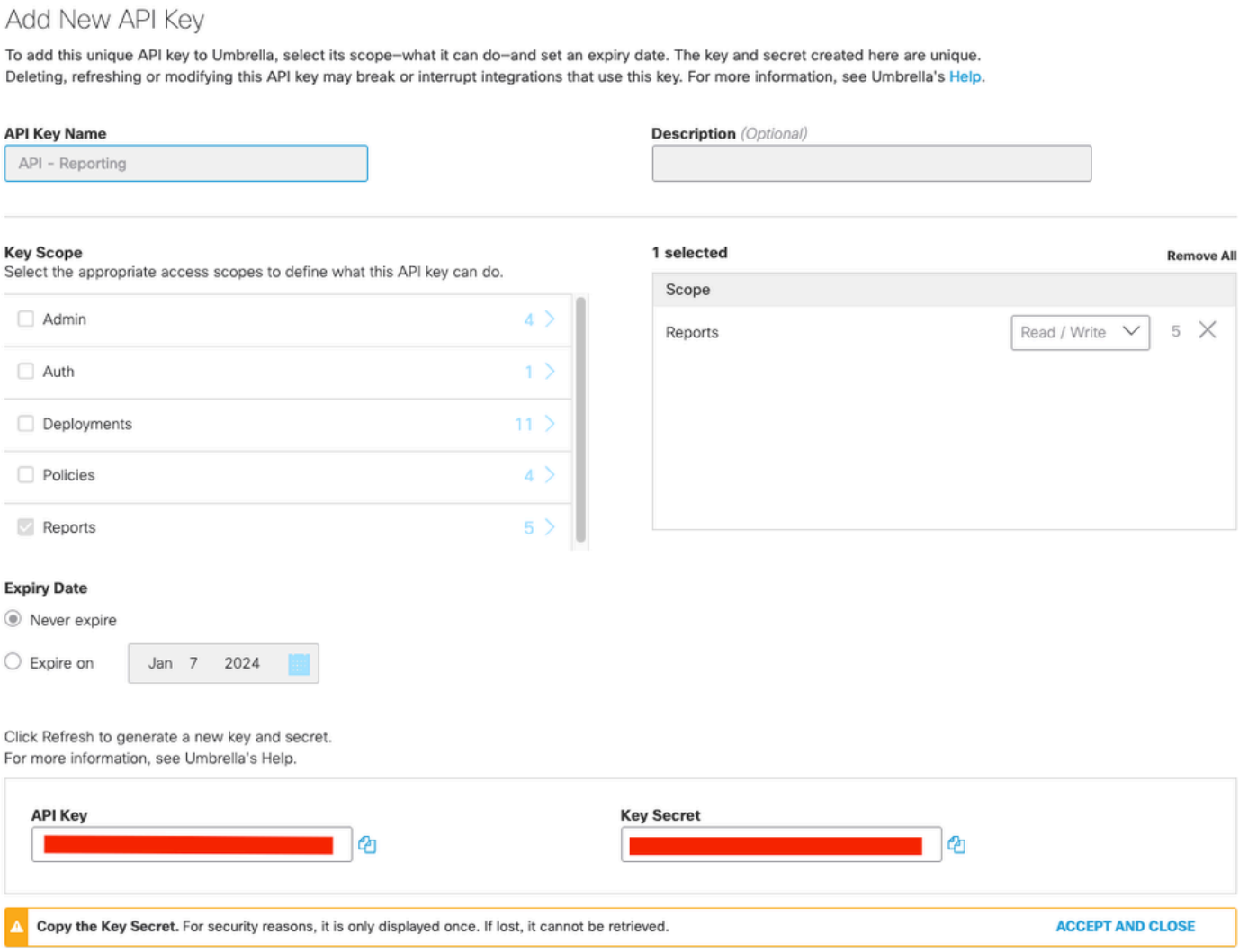
Dit artikel laat zien hoe je activiteitszoekrapporten kunt verzamelen via API.

Umbrella-verrichting

1. Navigeer vanuit het Umbrella-dashboard naar Beheer > API-sleutels.

2. Selecteer API-sleutels > Toevoegen.

3. Selecteer onder Belangrijkste bereik de optie Rapporten en vervolgens Sleutel maken.



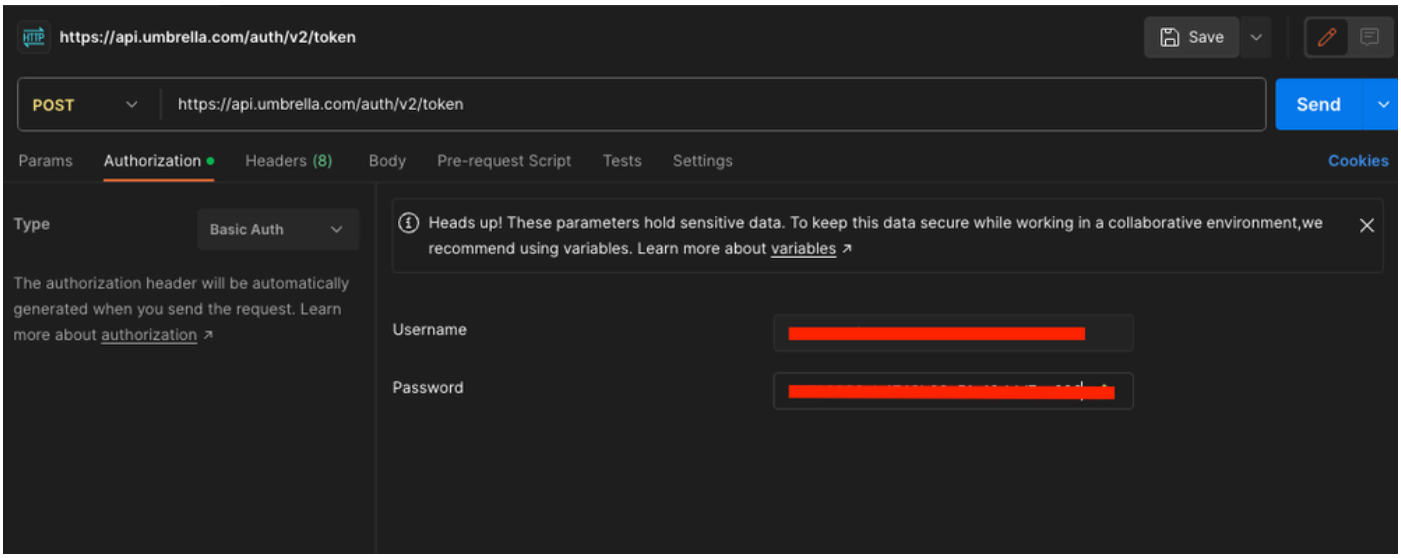
21495050167956

Beheerders kunnen het toegangsniveau per bereik tussen lezen / schrijven en alleen-lezen aanpassen, afhankelijk van het beoogde gebruik van elke API-sleutel, terwijl de API-sleutels kunnen worden geconfigureerd om op een vooraf gedefinieerde datum te verlopen. U bent verplicht om de API-sleutel / geheim in deze stap te verzamelen, omdat ze momenteel zichtbaar zijn en ze daarna niet kunnen worden weergegeven.

De API-referenties genereren API-toegangstokens die 60 minuten geldig zijn. Deze procedure ondersteunt de stroom OAuth 2.0-clientreferenties. In Umbrella multi-org- of serviceprovideromgevingen kunnen API-referenties van bovenliggende organisaties worden gebruikt om toegangstokens te genereren met dezelfde scopes voor een onderliggende organisatie die tijdens het autorisatieproces zijn opgegeven.

Postmanprocedure

In het begin moet u een OAuth 2.0-toegangstoken maken. De Umbrella API-auteurspaden beginnen met https://api.umbrella.com/auth/v2. Na het indienen van een POST-query en gebruiker API-sleutel als gebruikersnaam en API-wachtwoord als wachtwoord, wordt een Access Token gegenereerd.

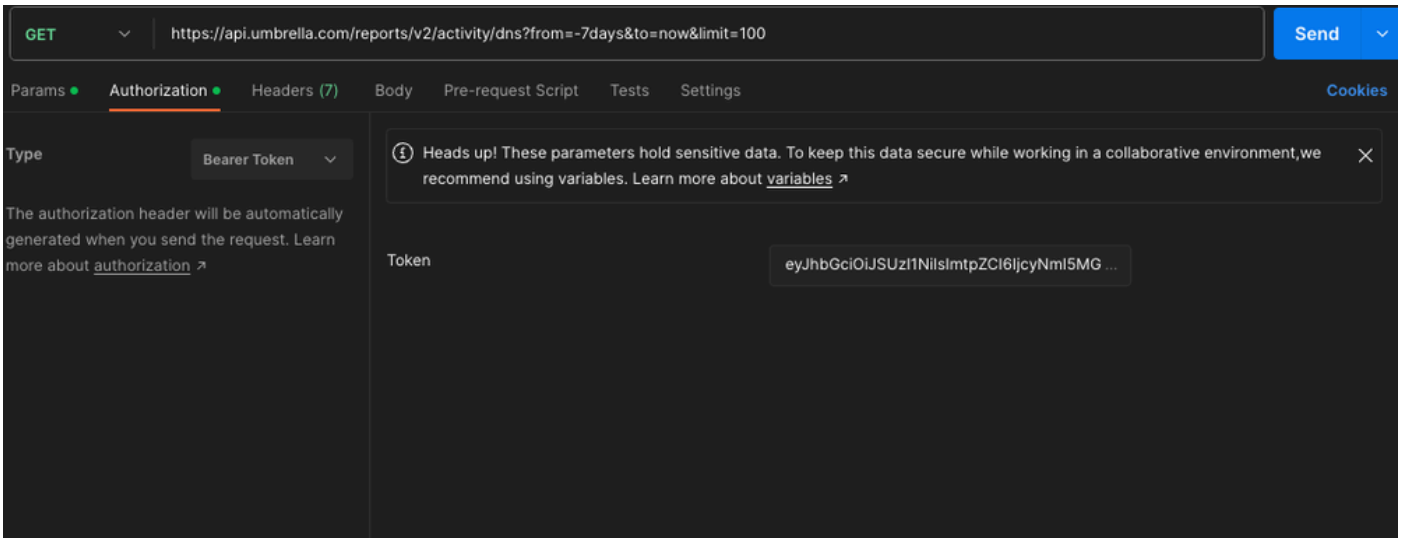


21606708808468

21607051456276

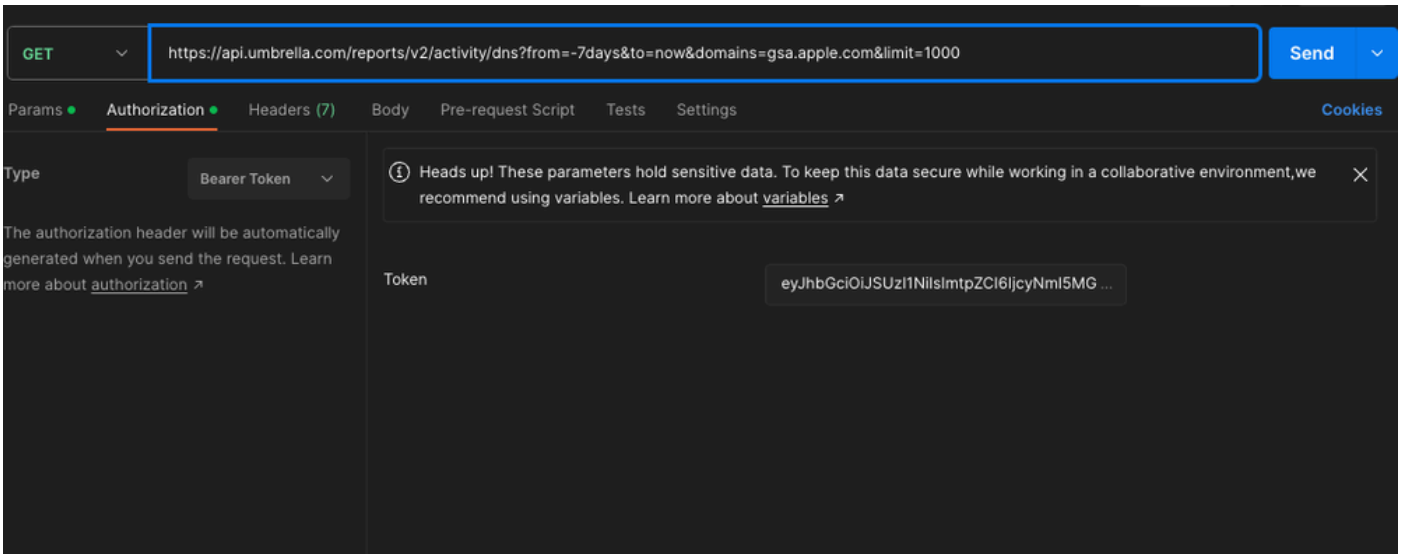
Bij deze stap moet u het toegangstoken verzamelen. Nu kunt u informatie ophalen met het toegangstoken.

U moet de methode GET selecteren en zowel uw API-pad (inclusief de vereiste parameter) als toegangstoken invoeren. In dit voorbeeld kunt u 100 rapporten ophalen van de activiteit zoeken exclusief voor DNS-verkeer voor de laatste 7 dagen.



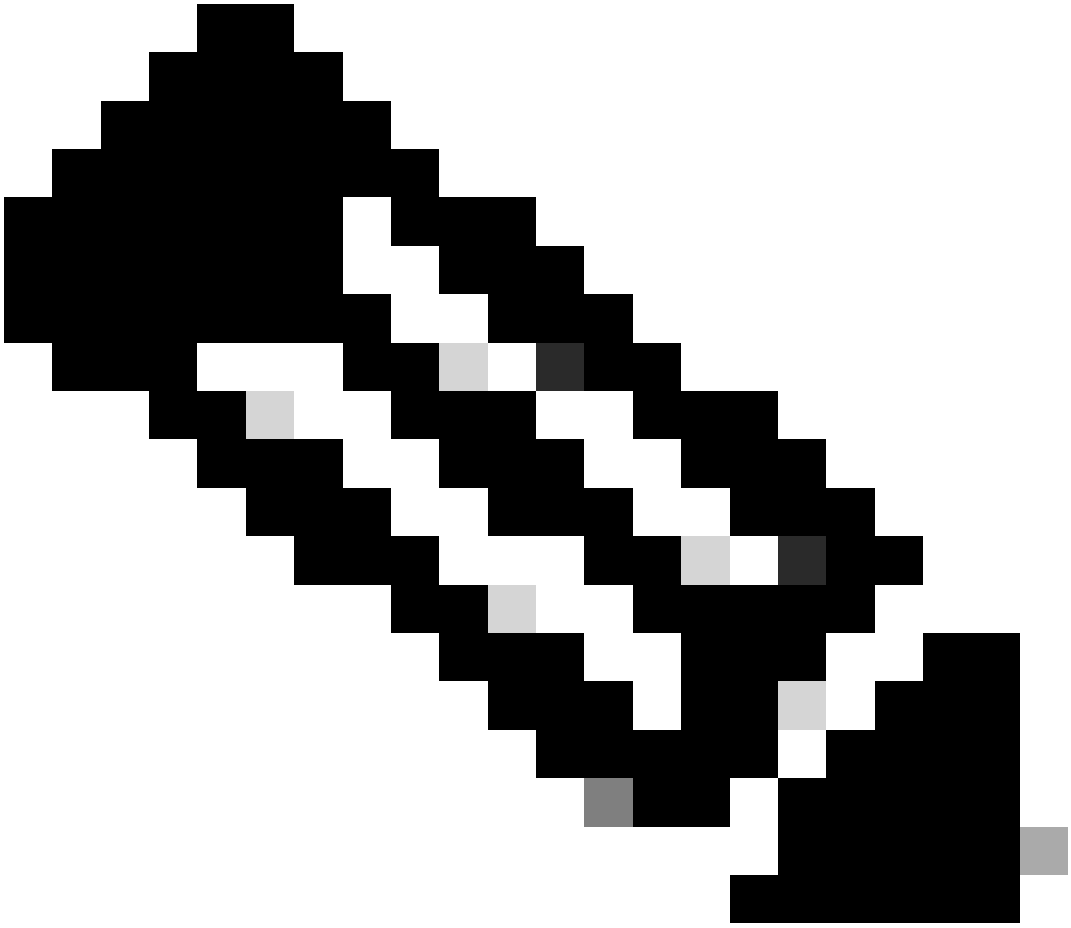
21607952074772

In een ander voorbeeld kunt u proberen om 1000 rapporten te extraheren uit de activiteit zoeken, exclusief voor DNS-verkeer voor de laatste 7 dagen, specifiek voor het domein "gsa.apple.com".



21607927544468

U kunt verzoekqueryparameters raadplegen om aanvullende parameters te vinden die u in uw API-query kunt gebruiken.



Opmerking: Als een HTTP-clientverzoek niet afkomstig is van hetzelfde continent als de locatie van het datawarehouse van Umbrella, reageert de Umbrella-server met 302 Gevonden. Als u HTTP-verzoeken automatisch wilt omleiden en de header HTTP-autorisatie wilt behouden, kunt u extra markeringen instellen of een omleidingsinstelling inschakelen.

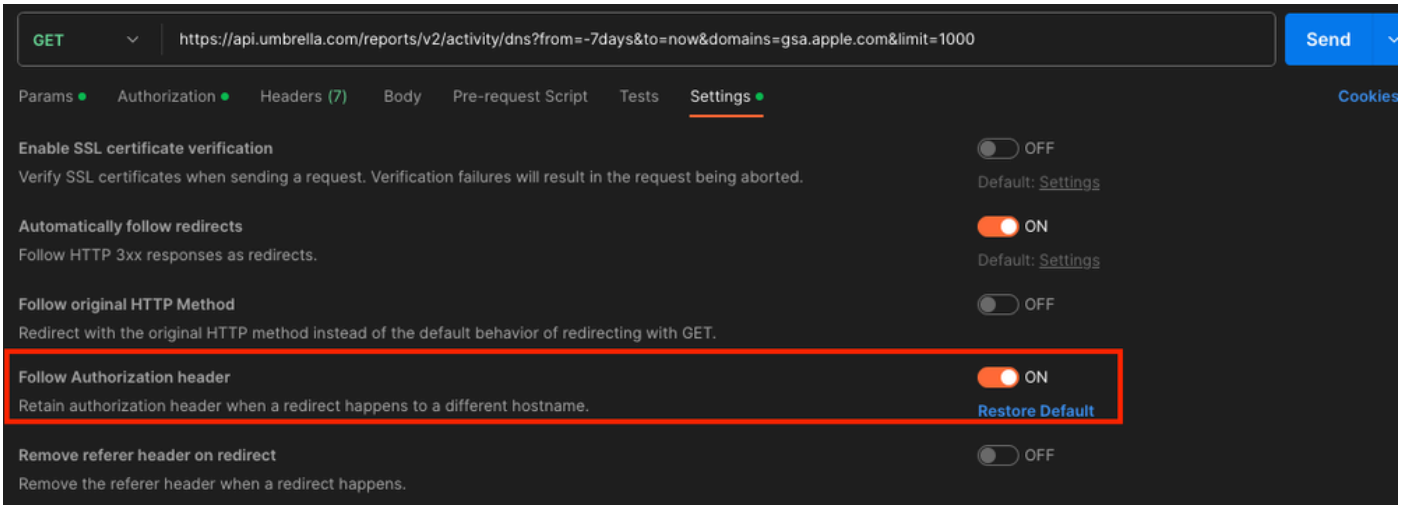
---

curl: U moet de -L of -locatie en -locatie-vertrouwde vlaggen doorgeven om de curl HTTP-aanvraag om te leiden en de koptekst voor autorisatie te behouden.

```
cURL
1 curl --location--trusted 'https://api.
      umbrella.com/reports/v2/activity/dns?
      from=-7days&to=now&domains=gsa.apple.
      com&limit=1000' \
```

21608126036628

Postman: Navigeer binnen de Postman-omgeving naar een API en selecteer een GET-methode. Navigeer naar Instellingen > De koptekst Volgen inschakelen om de koptekst Autorisatie te behouden voor omleidingsverzoeken.



21608126042388

Reacties

Na het verzenden van GET-actie naar de URL kunt u verschillende statuscodes ontvangen:

- Status:200: De aanvraag heeft de door u gevraagde informatie overgenomen.
- Status: 400: Ongeldige aanvraag. Het kan gerelateerd zijn aan de URL die u naar de query hebt verzonden. Een of meerdere parameters zijn niet correct.
- Status: 401: Niet geautoriseerd. De autorisatieheader ontbreekt of het token is niet geautoriseerd.
- 403: Verboden. Het token is ongeldig.

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.