De Cloud Security App configureren voor IBM QRadar

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Cloud Security-app kunt configureren met IBM QRadar voor logboekanalyse.

Overzicht

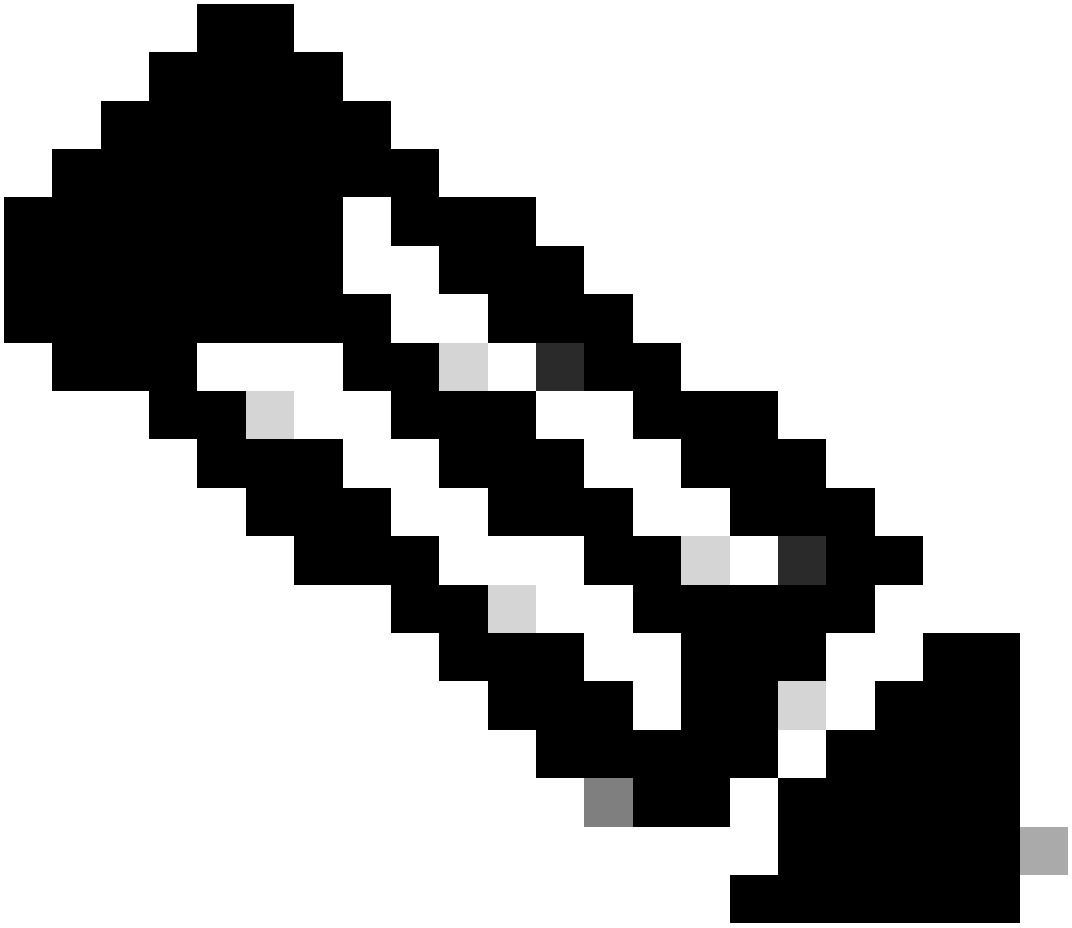
QRadar van IBM is een populaire SIEM voor log-analyse. Het biedt een krachtige interface voor het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor het DNS-verkeer van uw organisatie. De Cisco Cloud Security App voor IBM QRadar biedt inzicht in meerdere beveiligingsproducten (Investigate, Enforcement en CloudLock) en integreert deze met QRadar. Het helpt de gebruiker ook om de beveiliging te automatiseren en bedreigingen sneller en rechtstreeks vanuit QRadar te beheersen.

Wanneer u de Cisco Cloud Security-app voor QRadar instelt, worden alle gegevens van het Cisco Cloud Security-platform geïntegreerd en kunt u de gegevens in grafische vorm bekijken in de QRadar-console. Vanuit de applicatie kunnen analisten:

- Domeinen, IP-adressen, e-mailadressen onderzoeken
- Domeinen blokkeren en deblokkeren (handhaving)
- Bekijk de informatie over alle incidenten van het netwerk.

Dit artikel schetst de basis-how-to van het krijgen van QRadar ingesteld en uitgevoerd, zodat het in staat is om de logs te trekken uit uw S3 emmer en ze te consumeren.

Vereisten



Opmerking: ondersteuning voor QRadar moet afkomstig zijn van IBM, omdat Cisco niet in staat is om hardware of software van derden rechtstreeks te ondersteunen. Voor eventuele problemen die uw Umbrella-dashboard verbinden met uw S3-emmer, kunnen we ondersteuning bieden. Veel van de hier gevonden informatie is ook te vinden op de IBM-website: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Cisco Umbrella-vereisten

In dit document wordt ervan uitgegaan dat uw Amazon AWS S3-emmer is geconfigureerd in Umbrella (Instellingen > Logbeheer) en groen wordt weergegeven met recente logs die zijn geüpload.

Lees hier voor meer informatie over het configureren van deze functie: Uw logs beheren.

IBM Security QRadar SIEM-vereisten

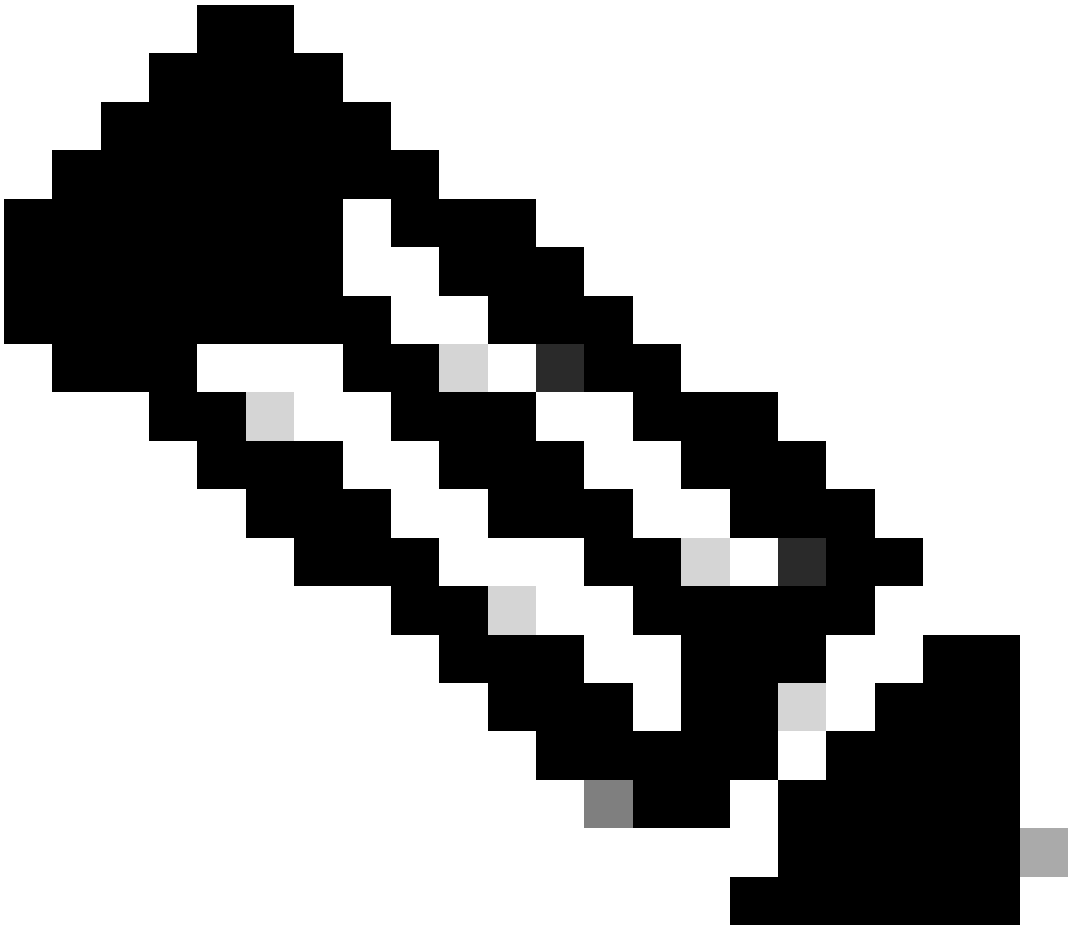
De beheerder moet beheerdersrechten hebben voor het QRadar-toestel(en), de Amazon S3-configuratie en het Umbrella-dashboard. In deze instructies wordt ervan uitgegaan dat de QRadar-beheerder bekend is met het maken van LSX-bestanden (Log Source Extension).

Houd er rekening mee dat de Cisco Cloud Security App v1.0.3 alleen werkt tot IBM QRadar 7.2.8. De nieuwe versie, v1.0.6, werkt met de huidige QRadar-versie van 7.4.2 en hoger.

Cisco Cloud Security App installeren voor IBM QRadar

1. Download en installeer de Cisco Cloud Security App voor IBM QRadar die u hier kunt vinden: Cisco Cloud Security App v1.0.3 (voor IBM QRadar v7.2.8) of Cisco Cloud Security App v1.0.6 (voor IBM QRadar v7.4.8).
2. Implementeer na de installatie wijzigingen in QRadar.

Configuratie Cisco Cloud Security-app: logboekbron toevoegen



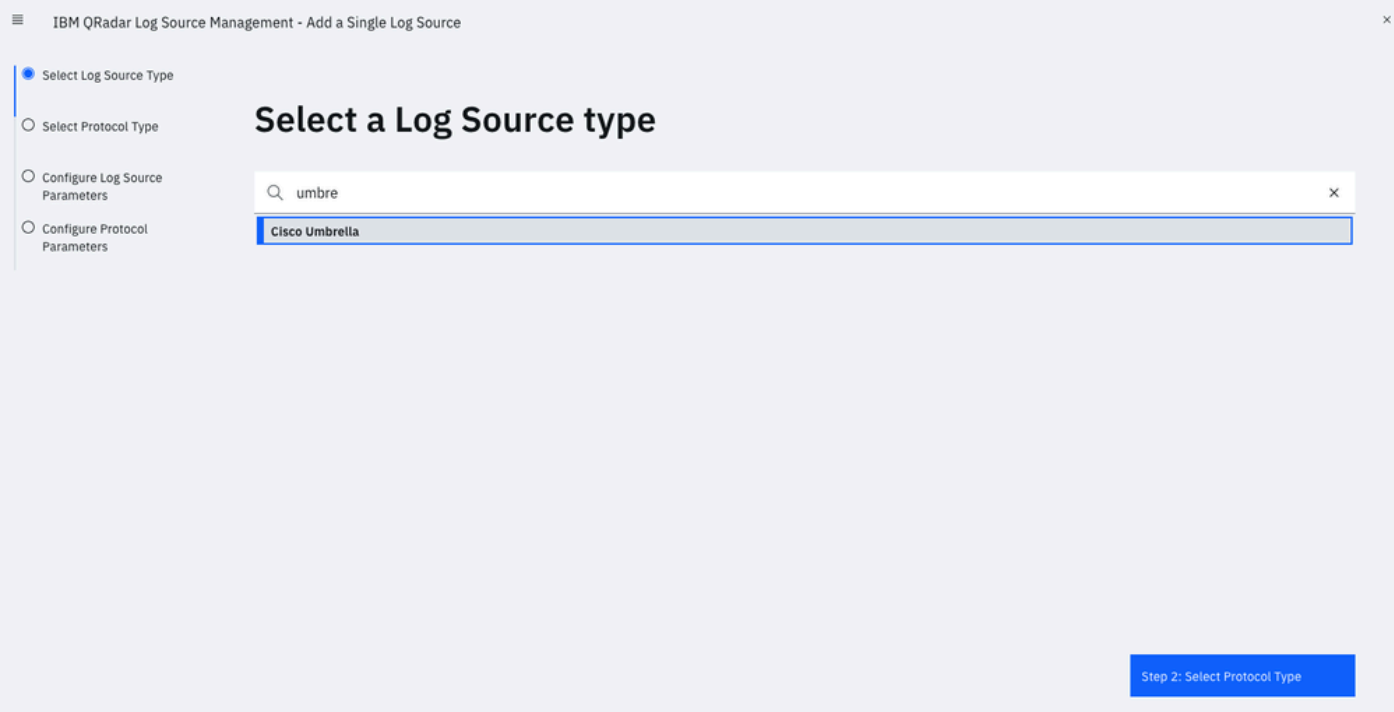
Opmerking: U kunt andere logs in S3 zien, zoals Audit en Firewall, maar deze worden niet

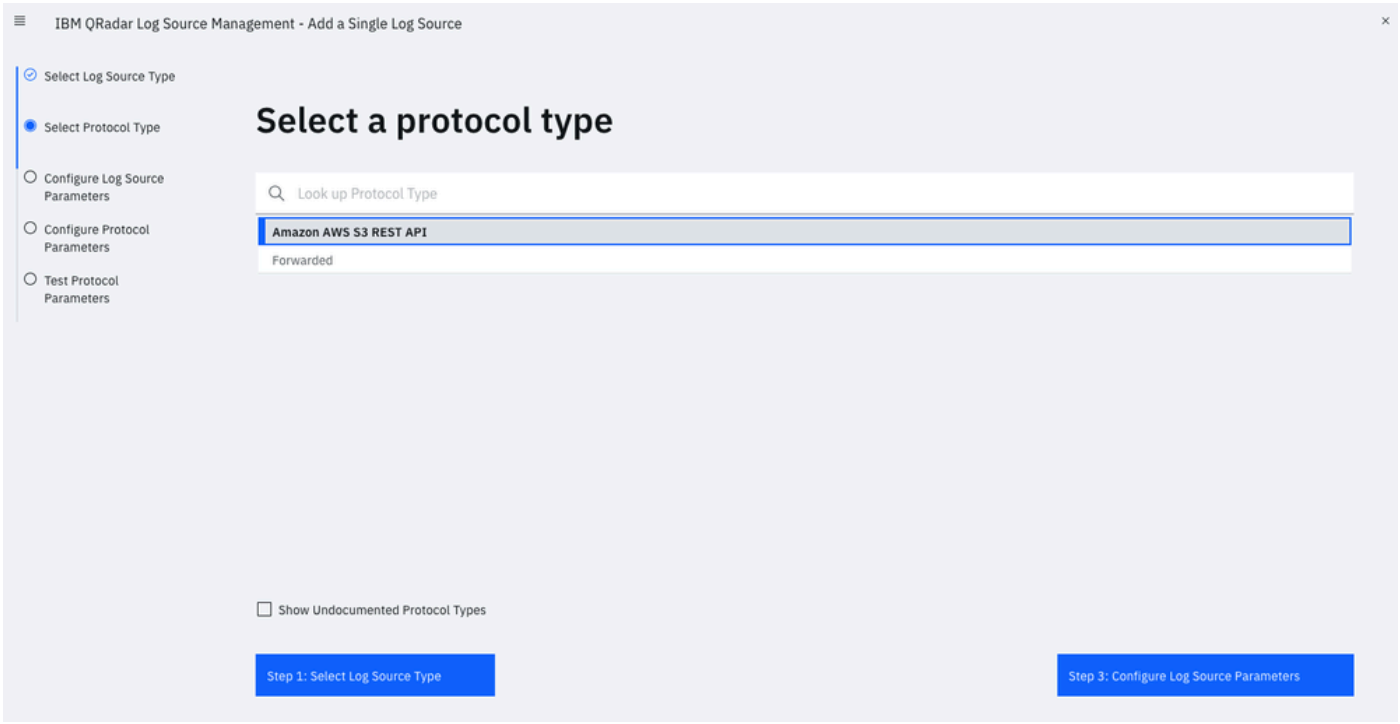
ondersteund. Stel alleen de drie hier genoemde op. Pogingen om die andere logs te configureren, leiden tot fouten.

Als u een logboekbron wilt toevoegen, klikt u op het tabblad Beheer op de navigatiebalk van QRadar, bladert u omlaag en klikt u op QRadar-logboekbronbeheer, en klikt u op de knop +Nieuwe logboekbron:

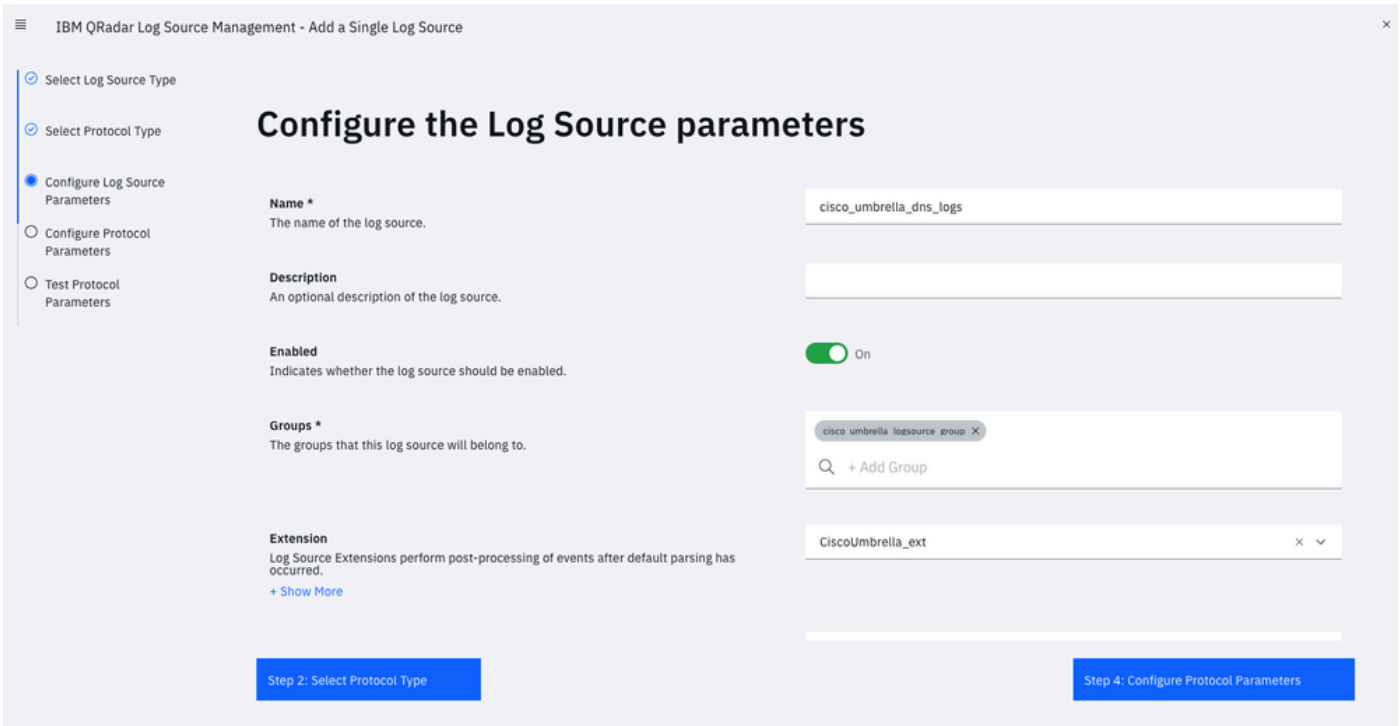
- Naam logbron (de namen van de items moeten exact overeenkomen zoals vermeld):
  - Cisco DNS-logs: cisco_umbrella_dns_logs
  - Cisco Umbrella IP-logs: cisco_umbrella_ip_logs
  - Cisco Umbrella Proxy-logs: cisco_umbrella_proxy_logs
- Indeling gebeurtenis: Cisco Umbrella CSV
- Logbrontype: Cisco Umbrella
- Protocolconfiguratie: Amazon AWS S3 REST API
- Bestandspatroon: .*?\\.csv\.gz
- Logbronextensie: CiscoUmbrella_ext **
- Selecteer de groepen waarvan u wilt dat deze logboekbron lid wordt: cisco_umbrella_logsource_group

Ga door de wizard Eén logboekbron toevoegen:

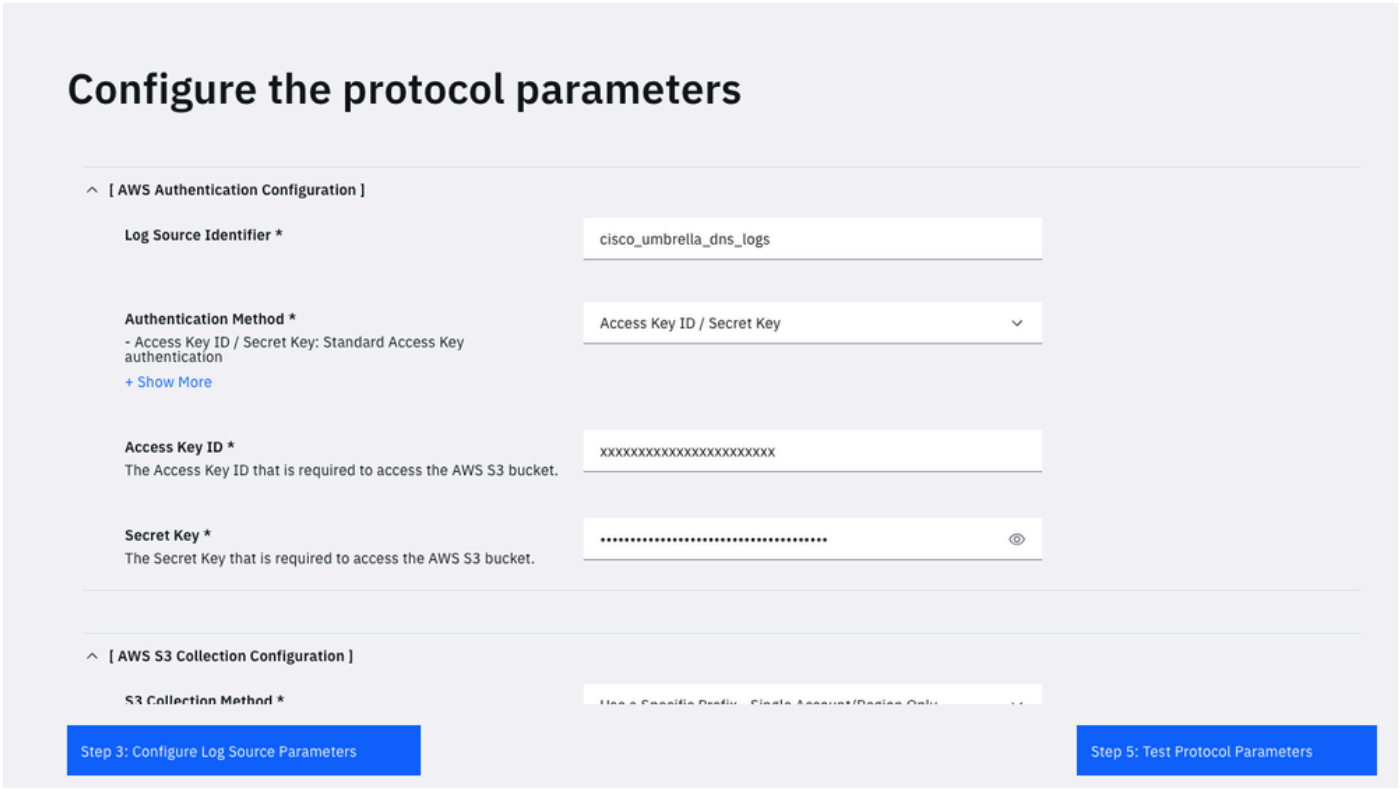




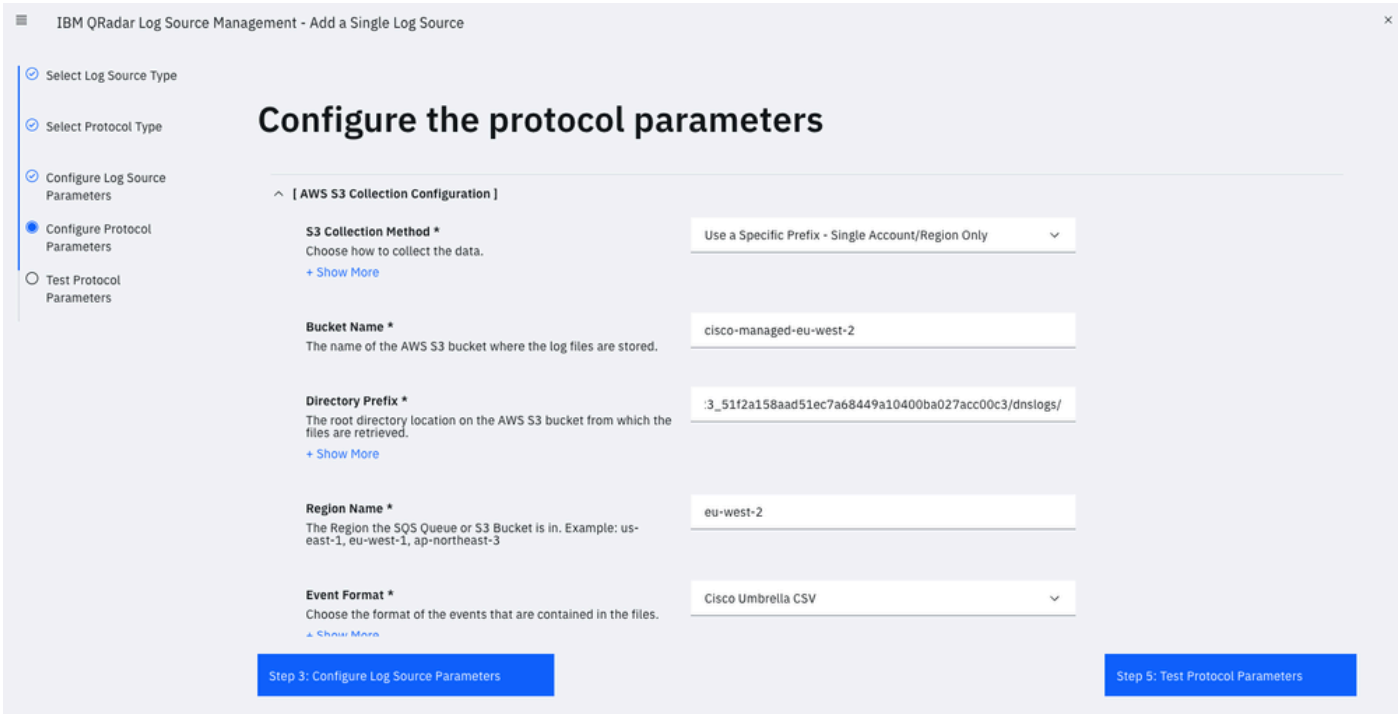
4404306773268



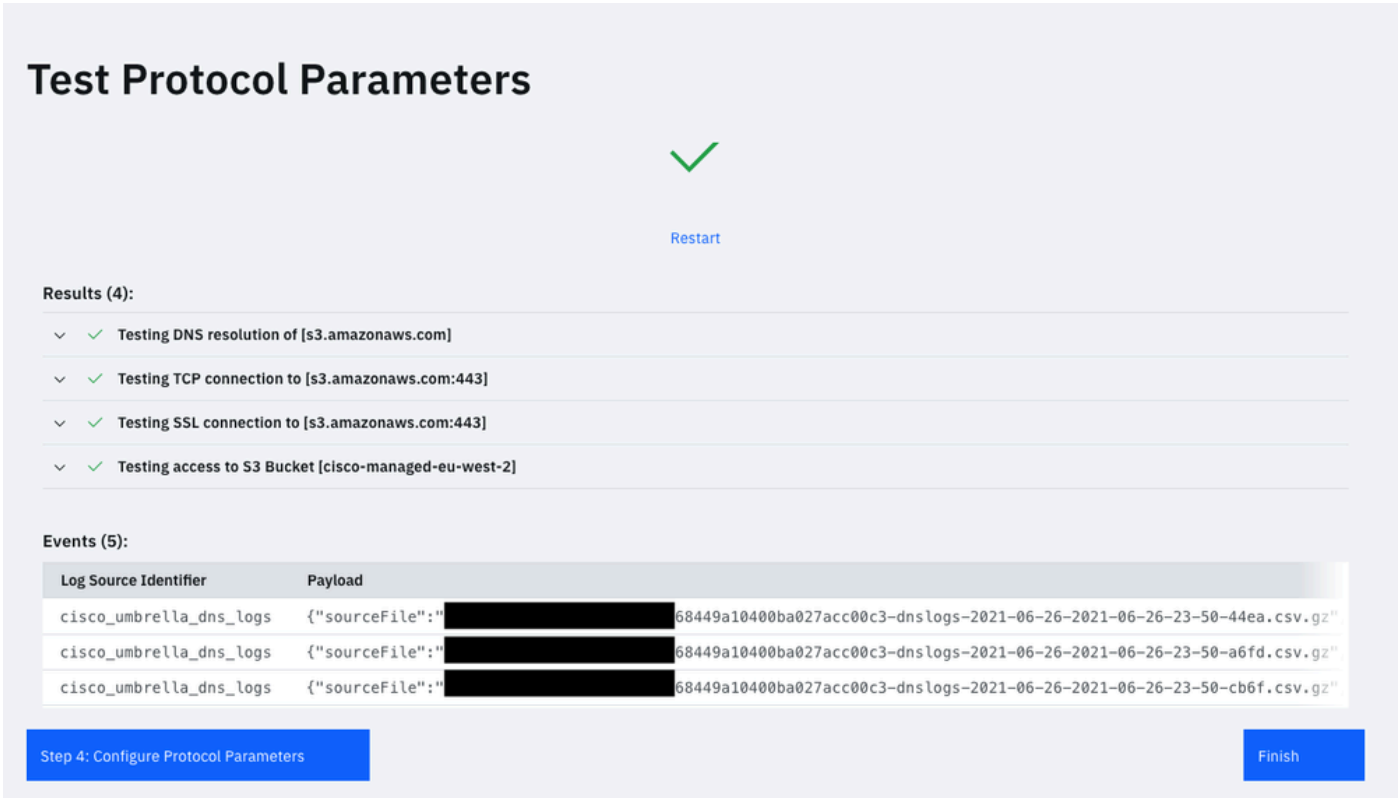
4404313505300



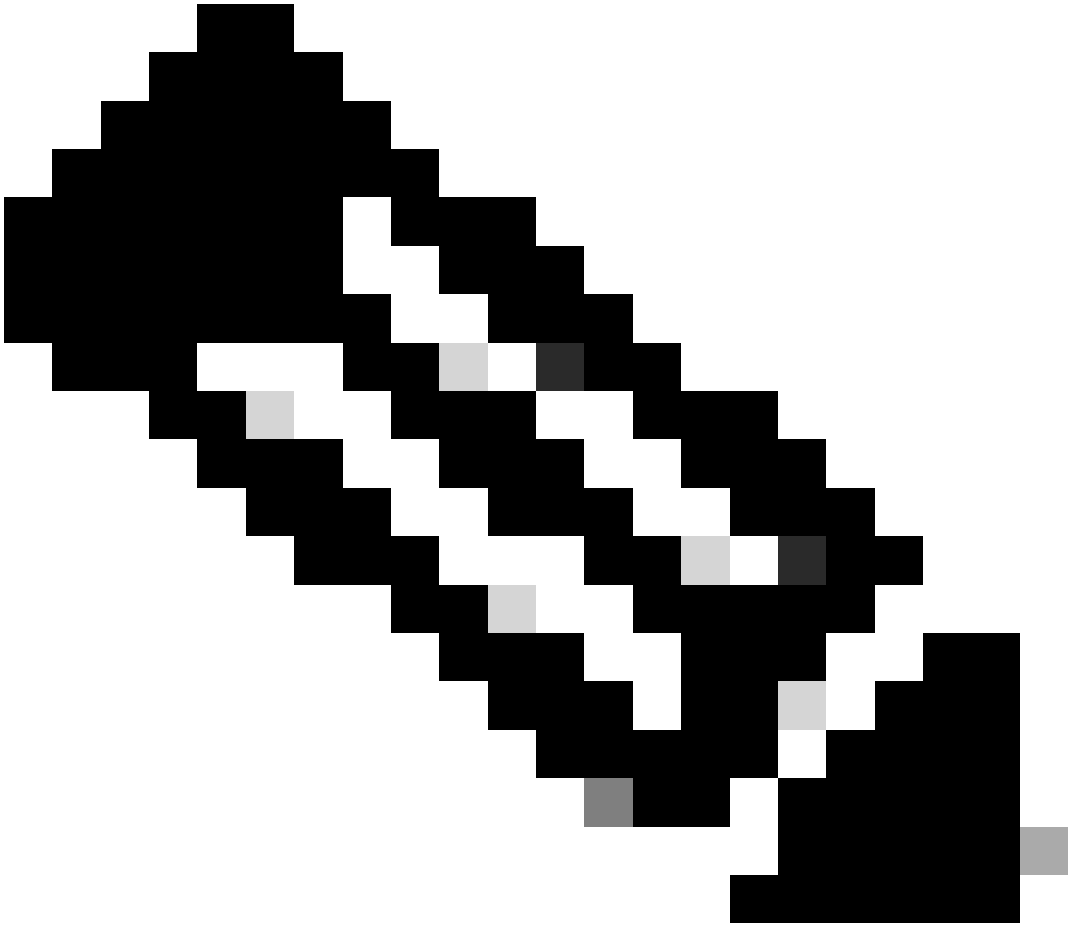
4404306774164



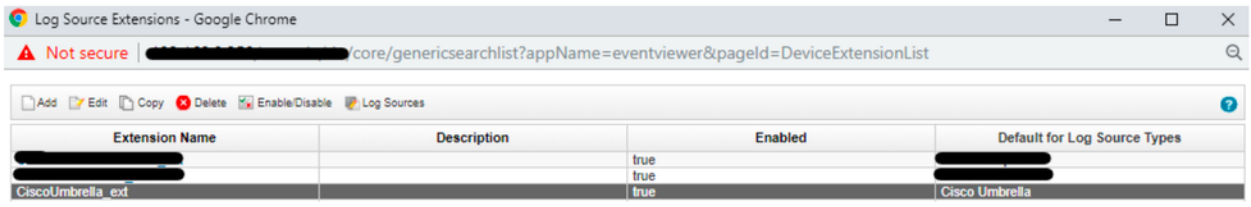
4404306897556



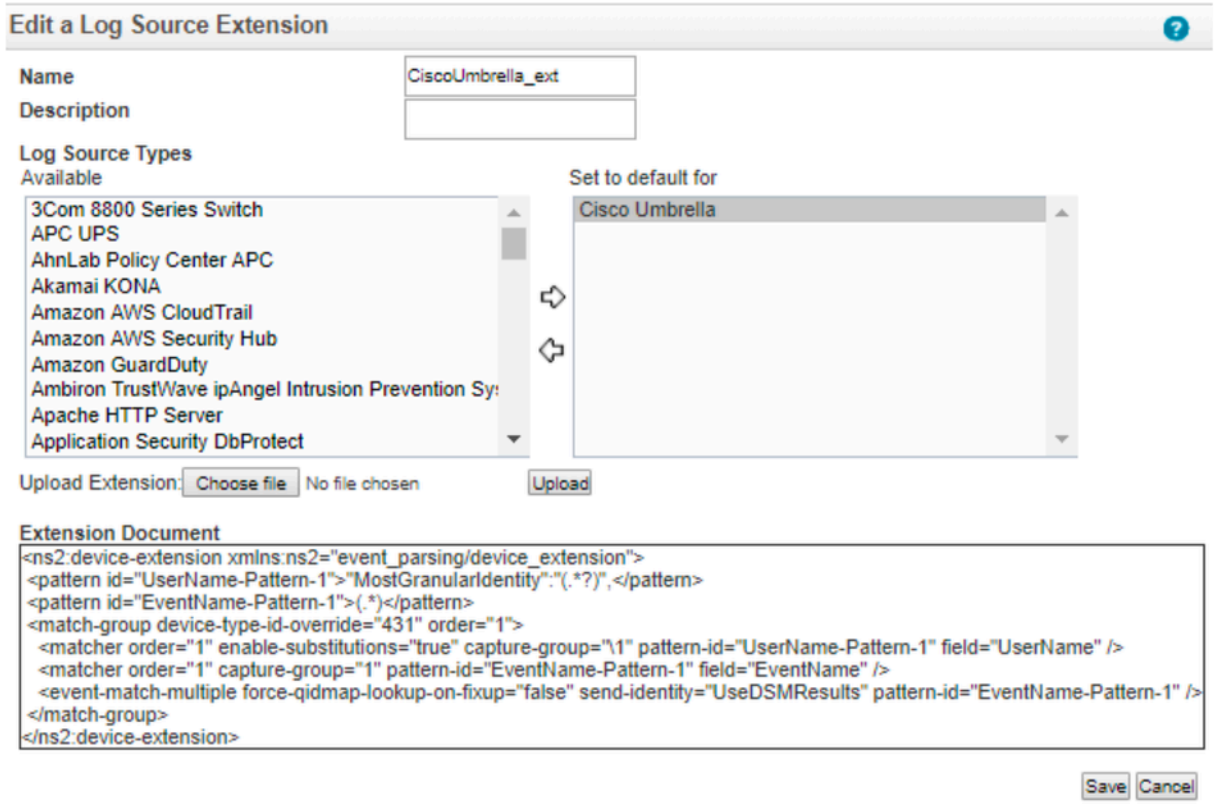
4404306881812



Opmerking: Als de Logbronextensie niet is toegewezen aan "CiscoUmbrella_ext", kiest u de Logbronnaam in de lijst:



360071157752



360071326791

Hier is een voorbeeld van hoe een Cisco Managed Bucket eruit ziet:

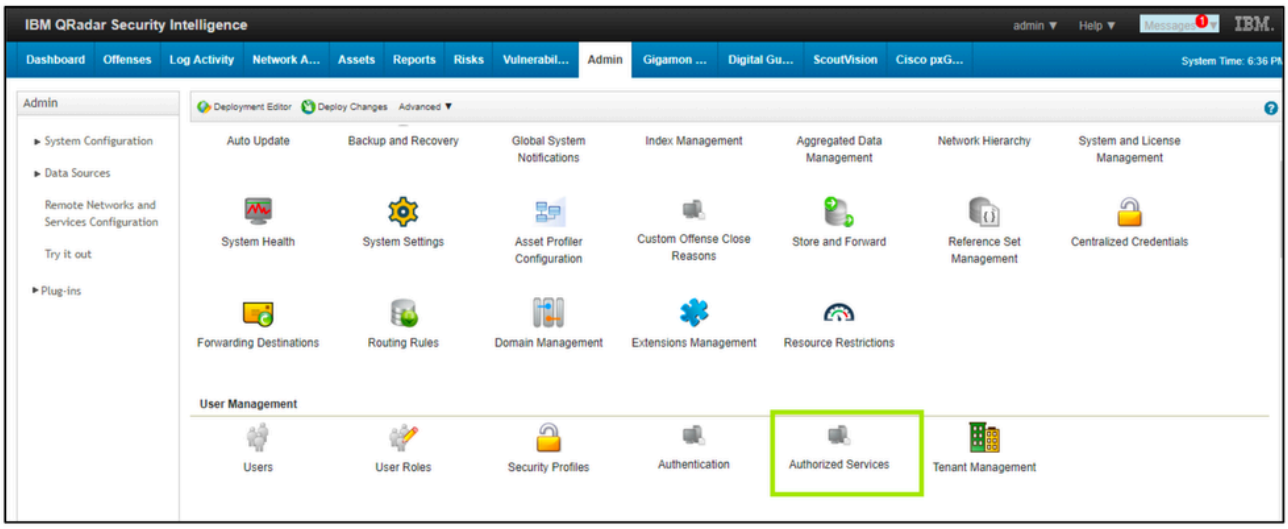
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs
```

Navigeer terug naar Cisco Cloud Security App Settings en stel de verversingssnelheid van het paneel in uren in op een minimumwaarde van "1" zodat de grafieken gegevens kunnen weergeven.

Authenticatie-token genereren

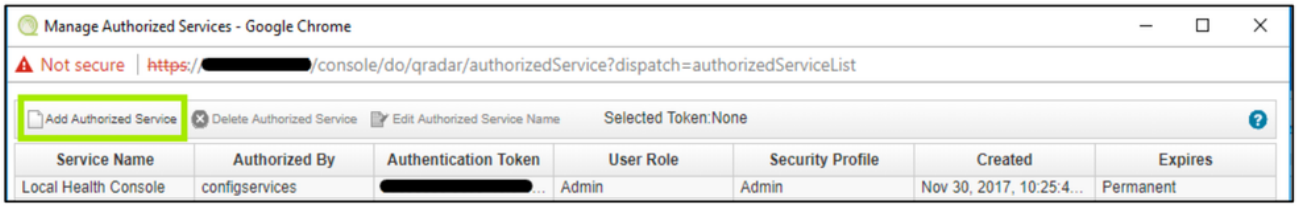
De beheerder moet een service-token genereren om toe te voegen aan uw Cisco Security App. Als beste praktijk wordt het geautoriseerde servicetoken elke 90 dagen opnieuw gemaakt:

1. Meld u aan bij QRadar > tabblad Beheer > Geautoriseerde services.



360071965571

2. Geautoriseerde services toevoegen.

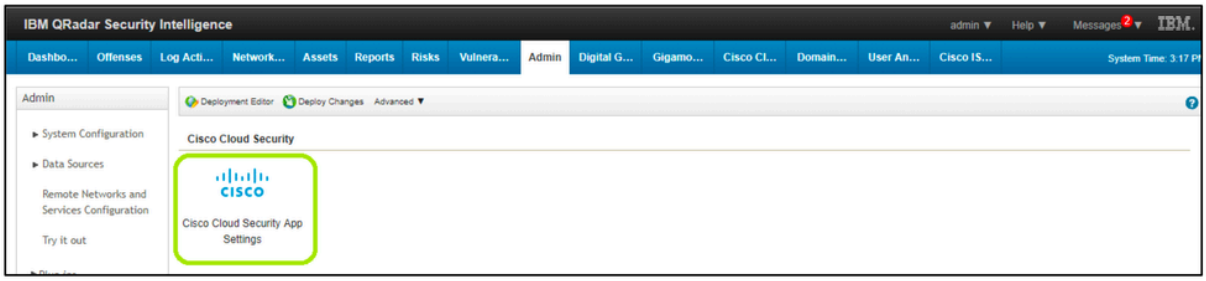


360071965551

3. Voer de gegevens in en genereer een verificatietoken.
4. Klik na het genereren van de token op "Wijzigingen implementeren".

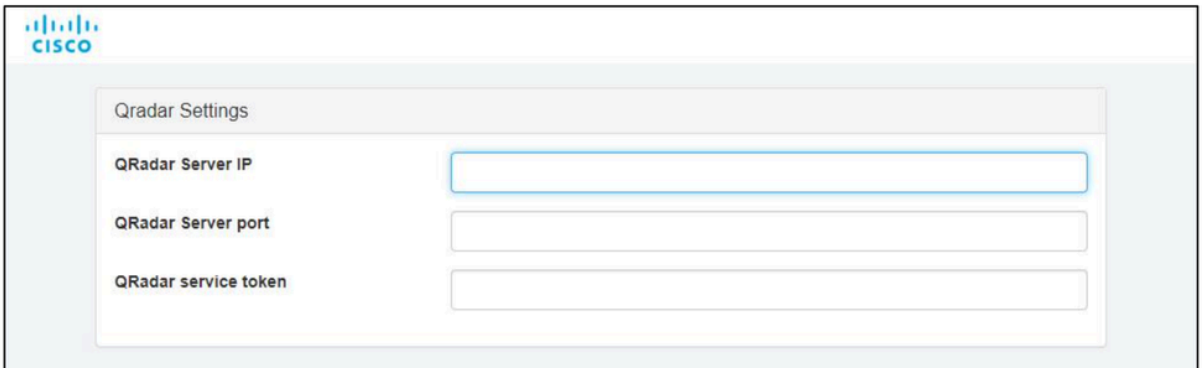
De Cisco Cloud Security-app configureren

1. Blader omlaag op het tabblad Beheer op de navigatiebalk van de QRadar en open Cisco Cloud Security App Settings.



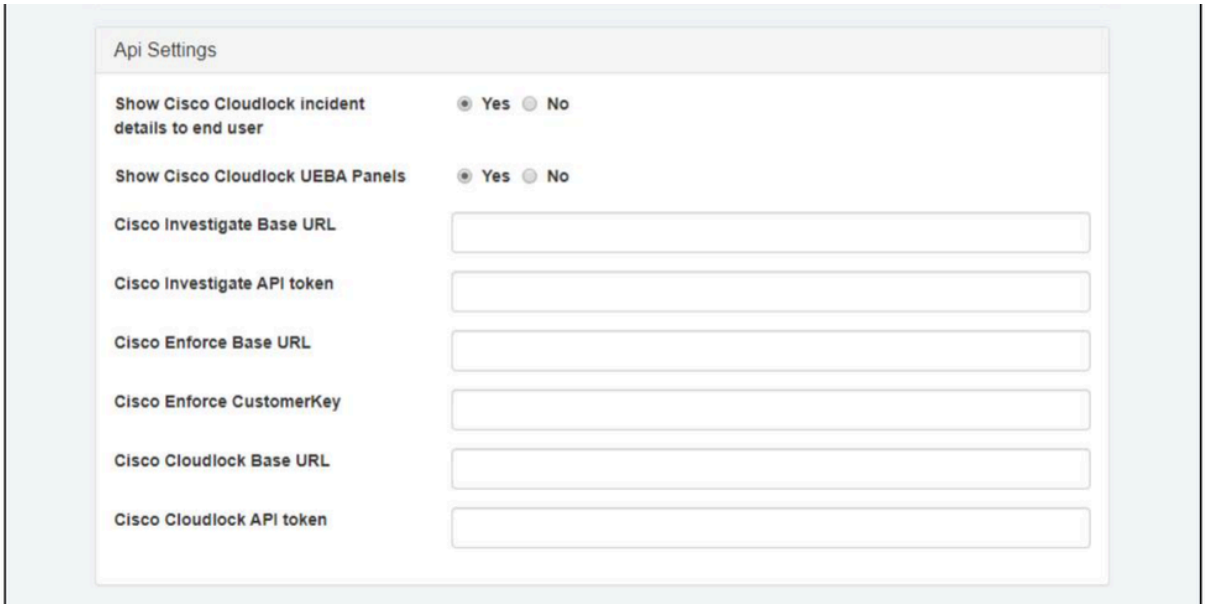
360071754732

2. Voer de verificatietoken in die in de vorige stap is gegenereerd.



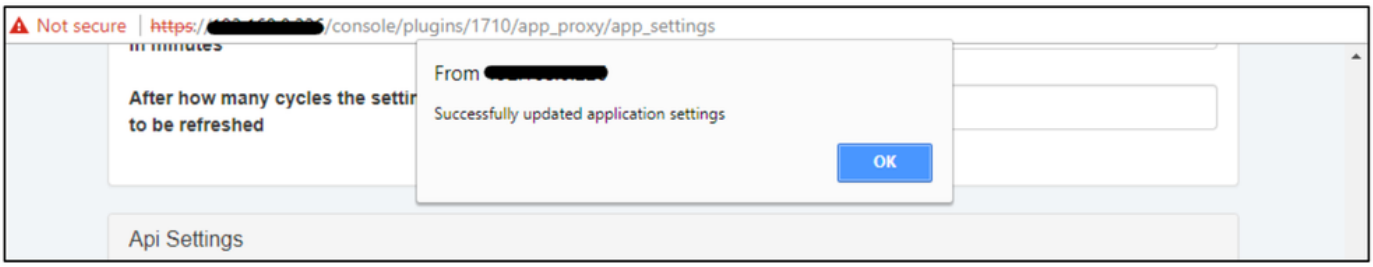
360072462992

3. Bewerk de API-instellingen als volgt:
    - Cisco Investigate Base-URL: https://investigate.api.umbrella.com/
    - Cisco Investigate API token: genereren via het Umbrella dashboard -> Investigate -> API Keys -> Create New Token; voor meer informatie, zie https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
    - Cisco Enforce Base-URL: https://s-platform.api.opendns.com/1.0/
    - Cisco Enforce CustomerKey: genereren via het Umbrella-dashboard -> Beleidscomponenten -> Integraties -> Toevoegen; voor meer informatie, zie https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
    - Cisco Cloudlock Base-URL: https://{YourCloudlockAPIServer}/api/v2 (bijvoorbeeld https://api-demo.cloudlock.com/api/v2/. Bevestig uw Cloudlock Base-URL, ook bekend als Cloudlock Enterprise API-URL, door een e-mail te sturen naar support@cloudlock.com.)
    - Cisco Cloudlock API-token: genereren via Cloudlock -> Instellingen -> Authenticatie en API -> Genereren; voor meer informatie, zie https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

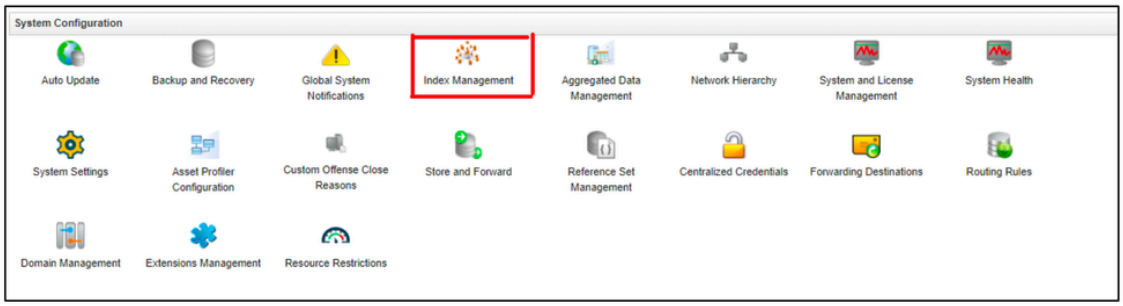
Een pop-upvenster geeft aan dat de toepassingsinstellingen zijn bijgewerkt.



360071986151

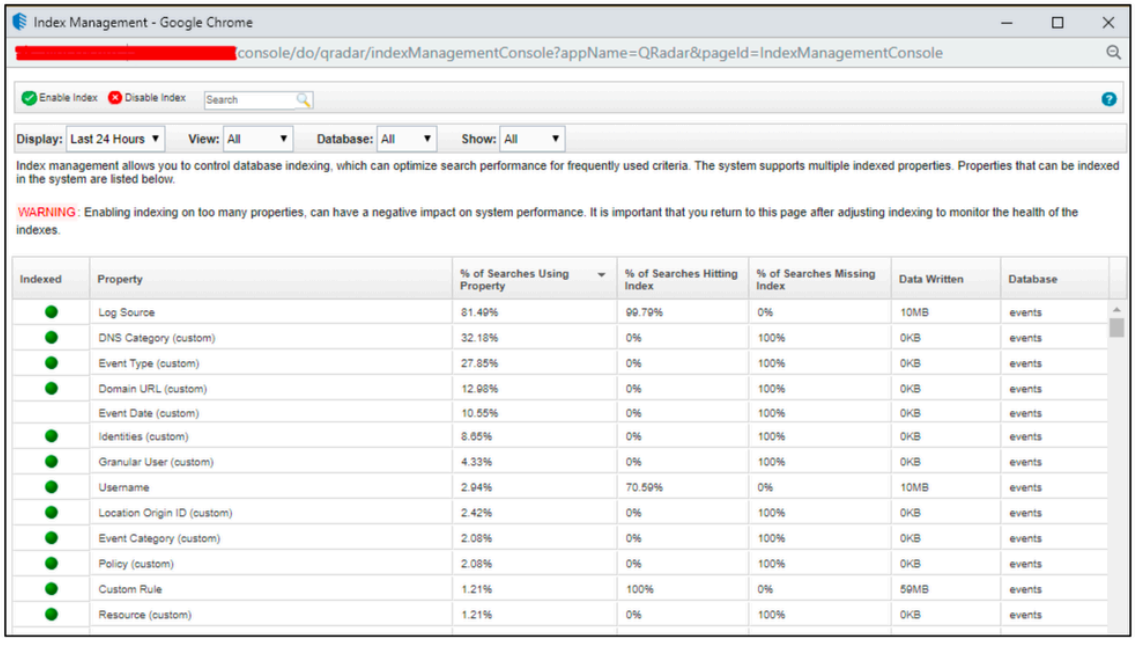
Indexering in QRadar

1. Navigeer naar het tabblad Beheer en klik vervolgens op Indexbeheer.



360071780112

2. Index de CEP's die zijn verpakt met de app.



360071988811

Dit zijn de aanbevolen te indexeren CEP's:

1. logboekbron
2. DNS-categorie

3. Type gebeurtenis
4. Domein-URL
5. Identiteiten
6. korrelgebruiker
7. Username
8. Locatie-oorsprong-ID
9. gebeurteniscategorie
10. Beleid
11. Bron

Nu kunt u QRadar gebruiken om activiteiten voor Cisco Umbrella-, Investigate- en CloudLock-gegevens te controleren. Meer instructies over het navigeren door QRadar vindt u hier: Navigeren door de Cisco Cloud Security App.

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.