

De Cloud Security App configureren voor IBM QRadar

Inhoud

[Inleiding](#)

[Overzicht](#)

[Vereisten](#)

[Cisco Umbrella-vereisten](#)

[IBM Security QRadar SIEM-vereisten](#)

[Cisco Cloud Security App installeren voor IBM QRadar](#)

[Configuratie Cisco Cloud Security-app: logboekbron toevoegen](#)

[Authenticatie-token genereren](#)

[De Cisco Cloud Security-app configureren](#)

[Indexering in QRadar](#)

Inleiding

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

Overzicht

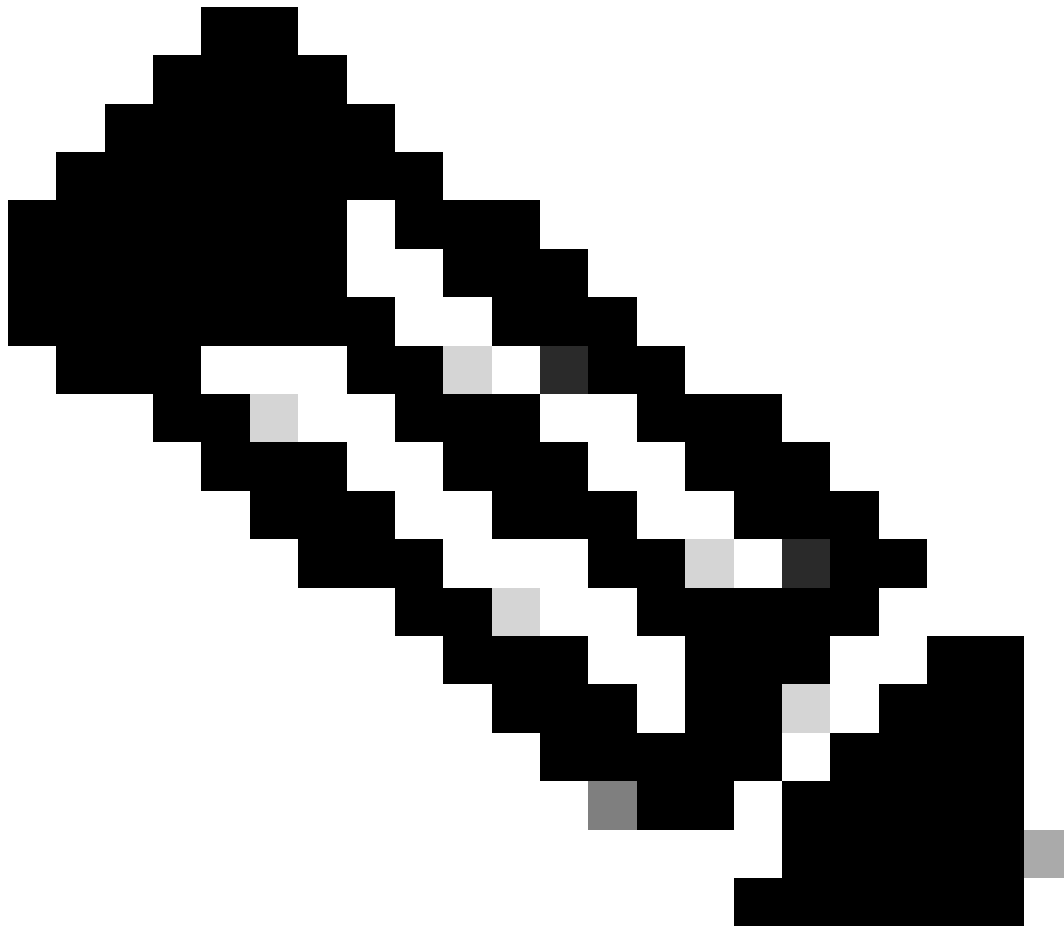
QRadar van IBM is een populaire SIEM voor log-analyse. Het biedt een krachtige interface voor het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor het DNS-verkeer van uw organisatie. De Cisco Cloud Security App voor IBM QRadar biedt inzicht in meerdere 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_Umbrella.html

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

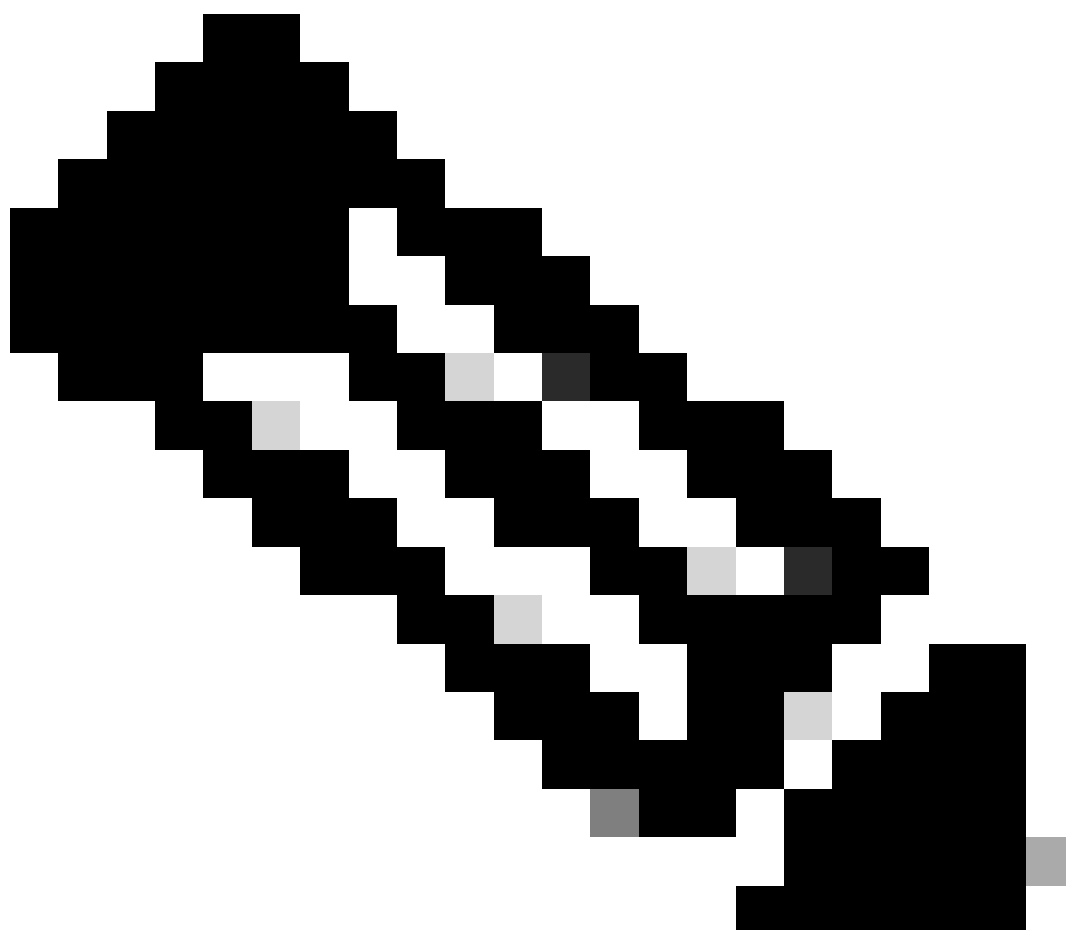
De beheerder moet beheerdersrechten hebben voor het QRadar-toestel(en), de Amazon S3-configuratie en het Umbrella-dashboard. In deze instructies wordt ervan uitgegaan dat de QRadar-beheerder bekend is met het maken van LSX-bestanden (Log Source Extension).

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:

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select a Log Source type

Search: umbre

Cisco Umbrella

Step 2: Select Protocol Type

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Select a protocol type

Look up Protocol Type

Amazon AWS S3 REST API

Forwarded

☐ Show Undocumented Protocol Types

Step 1: Select Log Source Type

Step 3: Configure Log Source Parameters

4404306773268

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the Log Source parameters

Name *
The name of the log source.

cisco_umbrella_dns_logs

Description
An optional description of the log source.

Enabled
Indicates whether the log source should be enabled.

☒ On

Groups *
The groups that this log source will belong to.

cisco_umbrella_logsource_group

Q

+ Add Group

Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.
[+ Show More](#)

CiscoUmbrella_ext

X

▼

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

4404313505300

Configure the protocol parameters

^ [AWS Authentication Configuration]

Log Source Identifier *

cisco_umbrella_dns_logs

Authentication Method *

- Access Key ID / Secret Key: Standard Access Key authentication

[+ Show More](#)

Access Key ID / Secret Key

Access Key ID *

The Access Key ID that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXX

Secret Key *

The Secret Key that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXX

^ [AWS S3 Collection Configuration]

S3 Collection Method *

Use a Specific Prefix - Single Account/Region Only

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306774164

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the protocol parameters

^ [AWS S3 Collection Configuration]

S3 Collection Method *

Choose how to collect the data.

[+ Show More](#)

Use a Specific Prefix - Single Account/Region Only

Bucket Name *

The name of the AWS S3 bucket where the log files are stored.

cisco-managed-eu-west-2

Directory Prefix *

The root directory location on the AWS S3 bucket from which the files are retrieved.

[+ Show More](#)

:3_51f2a158aad51ec7a68449a10400ba027acc00c3/dnslogs/

Region Name *

The Region the SQS Queue or S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3

eu-west-2

Event Format *

Choose the format of the events that are contained in the files.

[+ Show More](#)

Cisco Umbrella CSV

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306897556

Test Protocol Parameters



[Restart](#)

Results (4):

- ✓ Testing DNS resolution of [s3.amazonaws.com]
- ✓ Testing TCP connection to [s3.amazonaws.com:443]
- ✓ Testing SSL connection to [s3.amazonaws.com:443]
- ✓ Testing access to S3 Bucket [cisco-managed-eu-west-2]

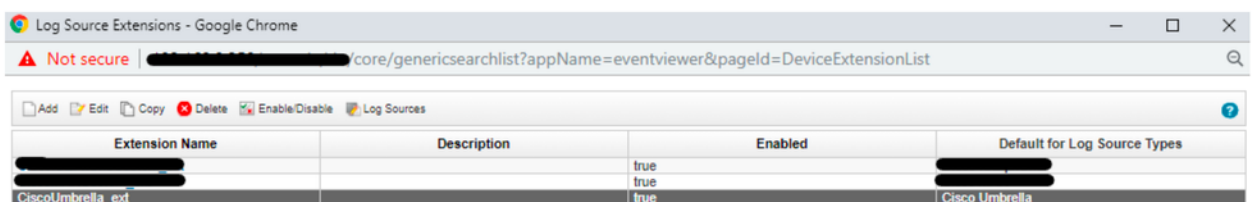
Events (5):

Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-cb6f.csv.gz"}

Step 4: Configure Protocol Parameters

Finish

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



Extension Name	Description	Enabled	Default for Log Source Types
[Redacted]	[Redacted]	true	[Redacted]
[Redacted]	[Redacted]	true	[Redacted]
CiscoUmbrella_ext	[Redacted]	true	Cisco Umbrella

360071157752

Edit a Log Source Extension

Name
CiscoUmbrella_ext

Description

Log Source Types

Available

3Com 8800 Series Switch
APC UPS
AhnLab Policy Center APC
Akamai KONA
Amazon AWS CloudTrail
Amazon AWS Security Hub
Amazon GuardDuty
Ambion TrustWave ipAngel Intrusion Prevention Sy
Apache HTTP Server
Application Security DbProtect

Set to default for

Cisco Umbrella

Upload Extension: Choose file No file chosen Upload

Extension Document

<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
<pattern id="UserName-Pattern-1">"MostGranularIdentity": "(.*)", </pattern>
<pattern id="EventName-Pattern-1">(.*)</pattern>
<match-group device-type-id-override="431" order="1">
<matcher order="1" enable-substitutions="true" capture-group="1" pattern-id="UserName-Pattern-1" field="UserName" />
<matcher order="1" capture-group="1" pattern-id="EventName-Pattern-1" field="EventName" />
<event-match-multiple force-qidmap-lookup-on-fixup="false" send-identity="UseDSMResults" pattern-id="EventName-Pattern-1" />
</match-group>
</ns2:device-extension>

Save Cancel

360071326791

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

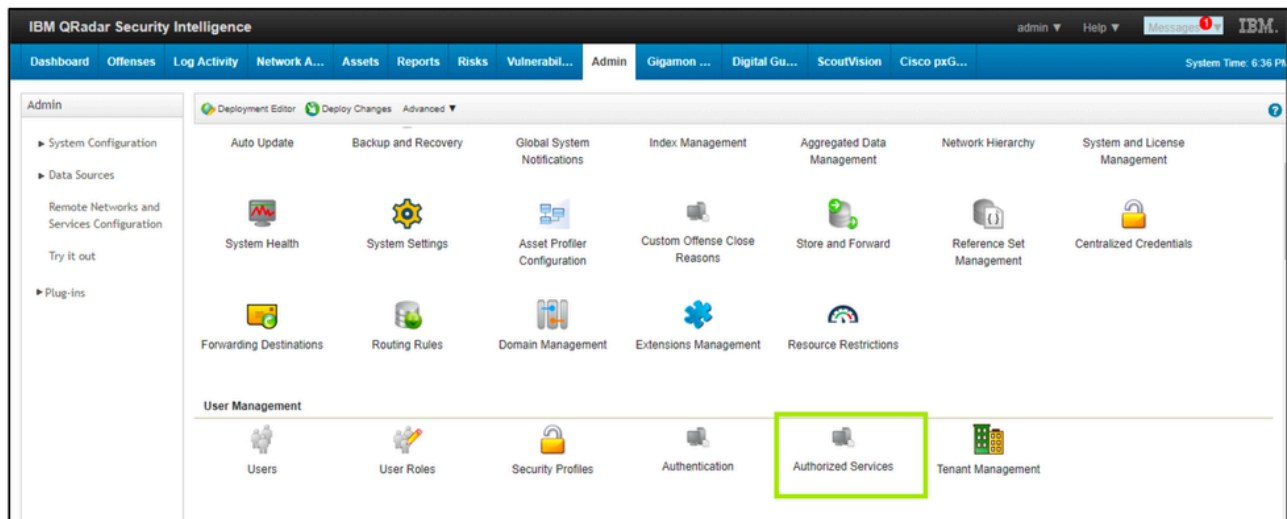
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

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

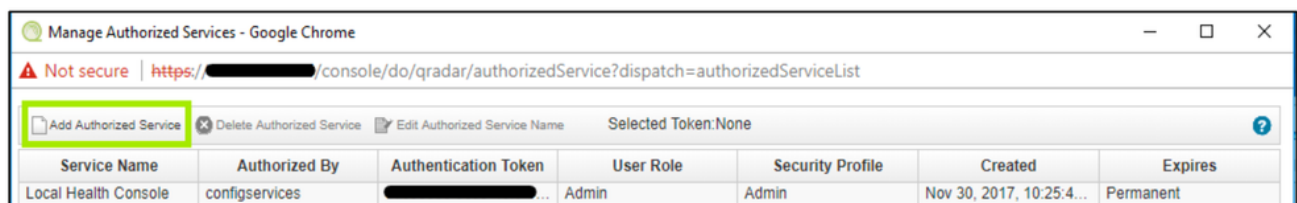
De beheerder moet een service-token genereren om toe te voegen aan uw Cisco Security App. Als beste praktijk wordt het geautoriseerde servicetoken elke 90 dagen opnieuw gemaakt:

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



360071965571

2. Geautoriseerde services toevoegen.



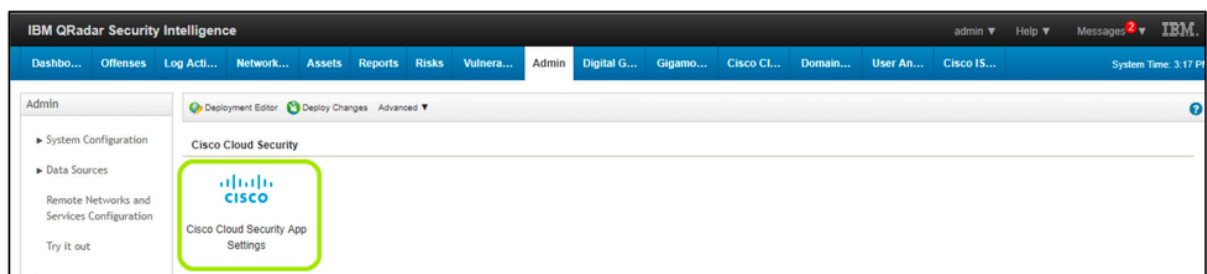
360071965551

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.



Qradar Settings

QRadar Server IP	
QRadar Server port	
QRadar service token	

360072462992

3. Bewerk de API-instellingen als volgt:

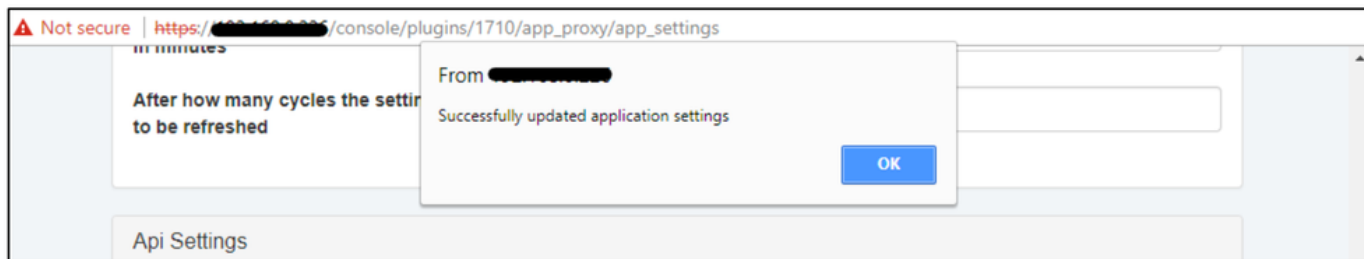
- Cisco Investigate Base-URL: <https://investigate.api.umbrella.com/>
- Cisco Investigate API token: genereren via het Umbrella dashboard -> Investigate -> API Keys -> Create New Token; voor meer informatie, zie <https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>
- Cisco Enforce 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>

Api Settings

Show Cisco Cloudlock incident details to end user	☒ Yes ☐ No
Show Cisco Cloudlock UEBA Panels	☒ Yes ☐ No
Cisco Investigate Base URL	
Cisco Investigate API token	
Cisco Enforce Base URL	
Cisco Enforce CustomerKey	
Cisco Cloudlock Base URL	
Cisco Cloudlock API token	

360072703611

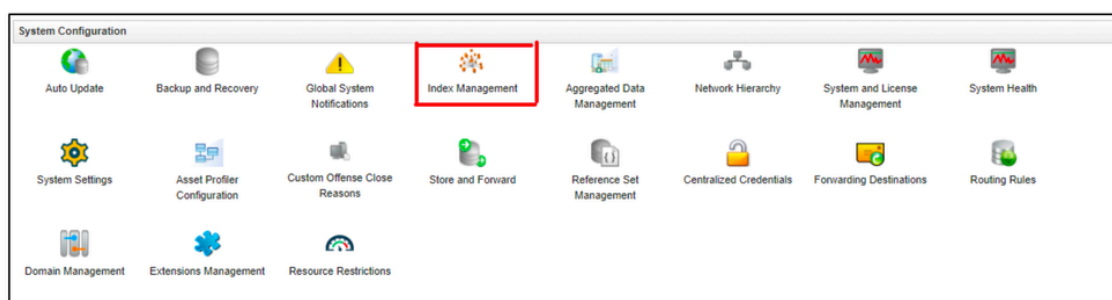
Een pop-upvenster geeft aan dat de toepassingsinstellingen zijn bijgewerkt.



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.

Index Management - Google Chrome

console/do/qradar/indexManagementConsole?appName=QRadar&pagId=IndexManagementConsole

Enable Index Disable Index Search

Display: Last 24 Hours View: All Database: All Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Log Source	81.40%	99.79%	0%	10MB	events
●	DNS Category (custom)	32.18%	0%	100%	0KB	events
●	Event Type (custom)	27.85%	0%	100%	0KB	events
●	Domain URL (custom)	12.98%	0%	100%	0KB	events
●	Event Date (custom)	10.55%	0%	100%	0KB	events
●	Identities (custom)	8.85%	0%	100%	0KB	events
●	Granular User (custom)	4.33%	0%	100%	0KB	events
●	Username	2.94%	70.59%	0%	10MB	events
●	Location Origin ID (custom)	2.42%	0%	100%	0KB	events
●	Event Category (custom)	2.08%	0%	100%	0KB	events
●	Policy (custom)	2.08%	0%	100%	0KB	events
●	Custom Rule	1.21%	100%	0%	59MB	events
●	Resource (custom)	1.21%	0%	100%	0KB	events

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.