

Konfigurieren der Cloud Security App für IBM QRadar

Inhalt

[Einleitung](#)

[Überblick](#)

[Anforderungen](#)

[Cisco Umbrella-Anforderungen](#)

[IBM Security QRadar SIEM-Anforderungen](#)

[Installation der Cisco Cloud Security App für IBM QRadar](#)

[Konfiguration der Cisco Cloud Security-App: Protokollquelle wird hinzugefügt](#)

[Authentifizierungstoken wird generiert](#)

[Konfigurieren der Cisco Cloud Security-App](#)

[Indizierung in QRadar](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Cisco Cloud Security-Anwendung mit IBM QRadar für die Protokollanalyse konfiguriert wird.

Überblick

QRadar von IBM ist ein beliebtes SIEM für die Protokollanalyse. Es bietet eine leistungsstarke Schnittstelle für die Analyse großer Datenmengen, wie z. B. die von Cisco Umbrella bereitgestellten Protokolle für den DNS-Datenverkehr Ihres Unternehmens. Die Cisco Cloud Security App für IBM QRadar bietet Einblicke in mehrere Sicherheitsprodukte (Investigate, Enforcement, and CloudLock) und integriert diese in QRadar. Darüber hinaus kann der Benutzer die Sicherheit automatisieren und Bedrohungen schneller und direkt von QRadar aus eindämmen.

Wenn Sie die Cisco Cloud Security-App für QRadar einrichten, werden alle Daten der Cisco Cloud Security-Plattform integriert, und Sie können die Daten in grafischer Form in der QRadar-Konsole anzeigen. Mithilfe der Anwendung können Analysten:

- Untersuchen von Domänen, IP-Adressen, E-Mail-Adressen
- Sperren und Aufheben der Blockierung von Domänen (Durchsetzung)
- Informationen zu allen Vorfällen im Netzwerk anzeigen.

In diesem Artikel wird erläutert, wie Sie QRadar einrichten und ausführen, damit Sie die Protokolle aus Ihrem S3-Eimer abrufen und verbrauchen können.

Anforderungen



Anmerkung: QRadar wird von IBM unterstützt, da Cisco keinen direkten Support für Hardware oder Software von Drittanbietern leistet. Bei Problemen, die Ihr Umbrella Dashboard mit Ihrem S3-Bucket verbinden, können wir Sie unterstützen. Viele der hier aufgeführten Informationen sind auch auf der IBM-Website zu finden:

https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umbrella.html

Cisco Umbrella-Anforderungen

In diesem Dokument wird davon ausgegangen, dass Ihr Amazon AWS S3-Bucket in Umbrella (Einstellungen > Protokollverwaltung) konfiguriert wurde und grün angezeigt wird, nachdem die letzten Protokolle hochgeladen wurden.

Weitere Informationen zum Konfigurieren dieser Funktion finden Sie hier: [Verwalten von Protokollen](#).

IBM Security QRadar SIEM-Anforderungen

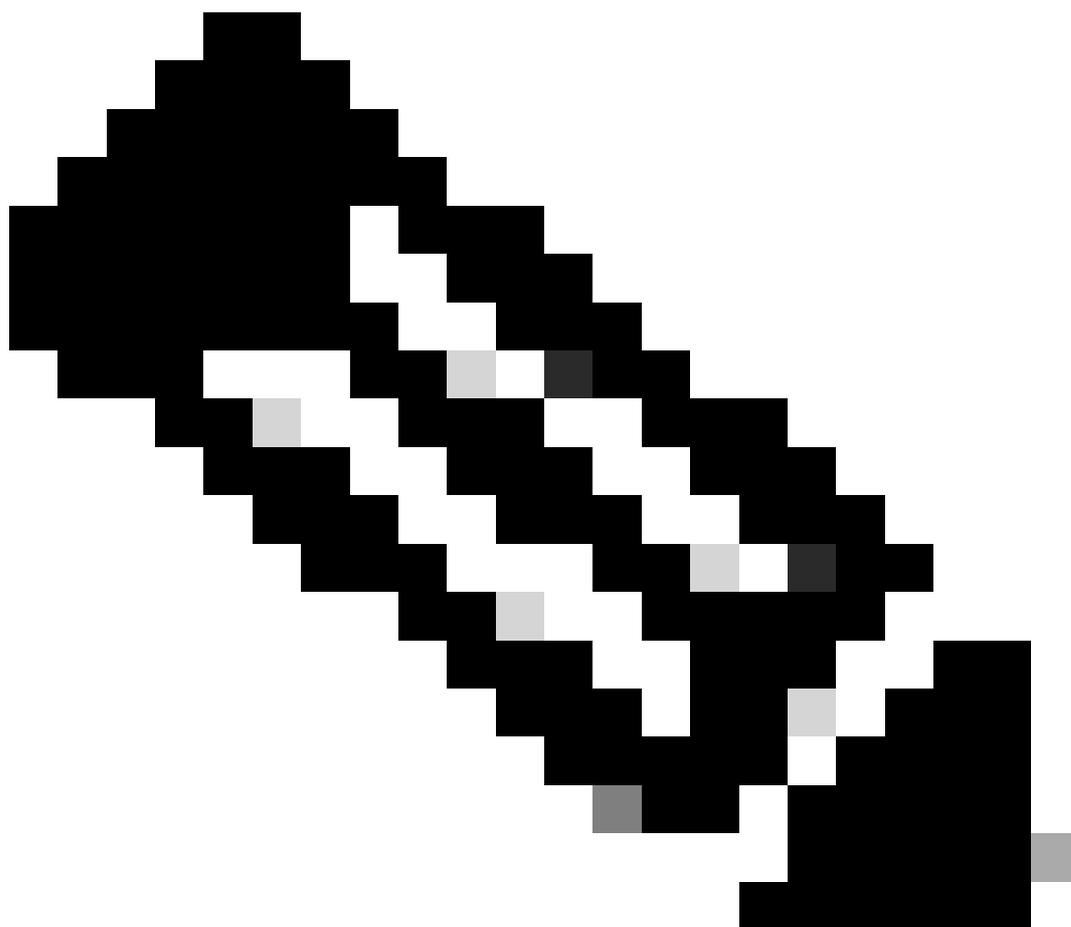
Der Administrator muss über Administratorrechte für die QRadar-Appliance(s), die Amazon S3-Konfiguration und das Umbrella Dashboard verfügen. Diese Anweisungen setzen voraus, dass der QRadar-Administrator mit der Erstellung von LSX-Dateien (Log Source Extension) vertraut ist.

Beachten Sie, dass die Cisco Cloud Security App v1.0.3 nur mit IBM QRadar 7.2.8 funktioniert. Die neue Version v1.0.6 arbeitet mit der aktuellen QRadar-Version ab 7.4.2.

Installation der Cisco Cloud Security App für IBM QRadar

1. Laden Sie die Cisco Cloud Security App für IBM QRadar herunter, und installieren Sie sie: [Cisco Cloud Security App v1.0.3](#) (für IBM QRadar v7.2.8) oder [Cisco Cloud Security App v1.0.6](#) (für IBM QRadar v7.4.8).
2. Nach der Installation können Sie Änderungen in QRadar bereitstellen.

Konfiguration der Cisco Cloud Security-App: Protokollquelle wird hinzugefügt



Anmerkung: Sie können andere Protokolle in S3 wie Audit und Firewall sehen, aber sie werden nicht unterstützt. Richten Sie nur die hier aufgeführten drei Geräte ein. Alle Versuche, diese anderen Protokolle zu konfigurieren, führen zu Fehlern.

Um eine Protokollquelle hinzuzufügen, klicken Sie auf die Registerkarte Admin in der QRadar-Navigationsleiste, scrollen Sie nach unten und klicken Sie auf QRadar Log Source Management, dann klicken Sie auf die Schaltfläche +Neue Protokollquelle:

- Name der Protokollquelle (die Eintragsnamen müssen genau den aufgeführten übereinstimmen):
 - Cisco DNS-Protokolle: cisco_umbrella_dns_logs
 - Cisco Umbrella IP-Protokolle: cisco_umbrella_ip_logs
 - Cisco Umbrella Proxy-Protokolle: Cisco Umbrella Proxy-Protokolle
- Veranstaltungsformat: Cisco Umbrella CSV
- Protokollquellentyp: Cisco Umbrella
- Protokollkonfiguration: Amazon AWS S3 REST-API
- Dateimuster: .*?.csv.gz
- Protokollquellenerweiterung: CiscoUmbrella_ext **
- Wählen Sie alle Gruppen aus, denen diese Protokollquelle angehören soll:
cisco_umbrella_logsource_group

Gehen Sie durch den Assistenten zum Hinzufügen einer einzelnen Protokollquelle:

The screenshot shows the 'IBM QRadar Log Source Management - Add a Single Log Source' window. On the left, a sidebar lists the steps: 'Select Log Source Type' (selected), 'Select Protocol Type', 'Configure Log Source Parameters', and 'Configure Protocol Parameters'. The main area is titled 'Select a Log Source type' and features a search bar with the text 'umbre'. Below the search bar, a single result 'Cisco Umbrella' is displayed and highlighted with a blue border. At the bottom right, there is a blue button labeled '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

+ Add Group

Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.

+ Show More

CiscoUmbrella_ext

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.

.....

^ [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]

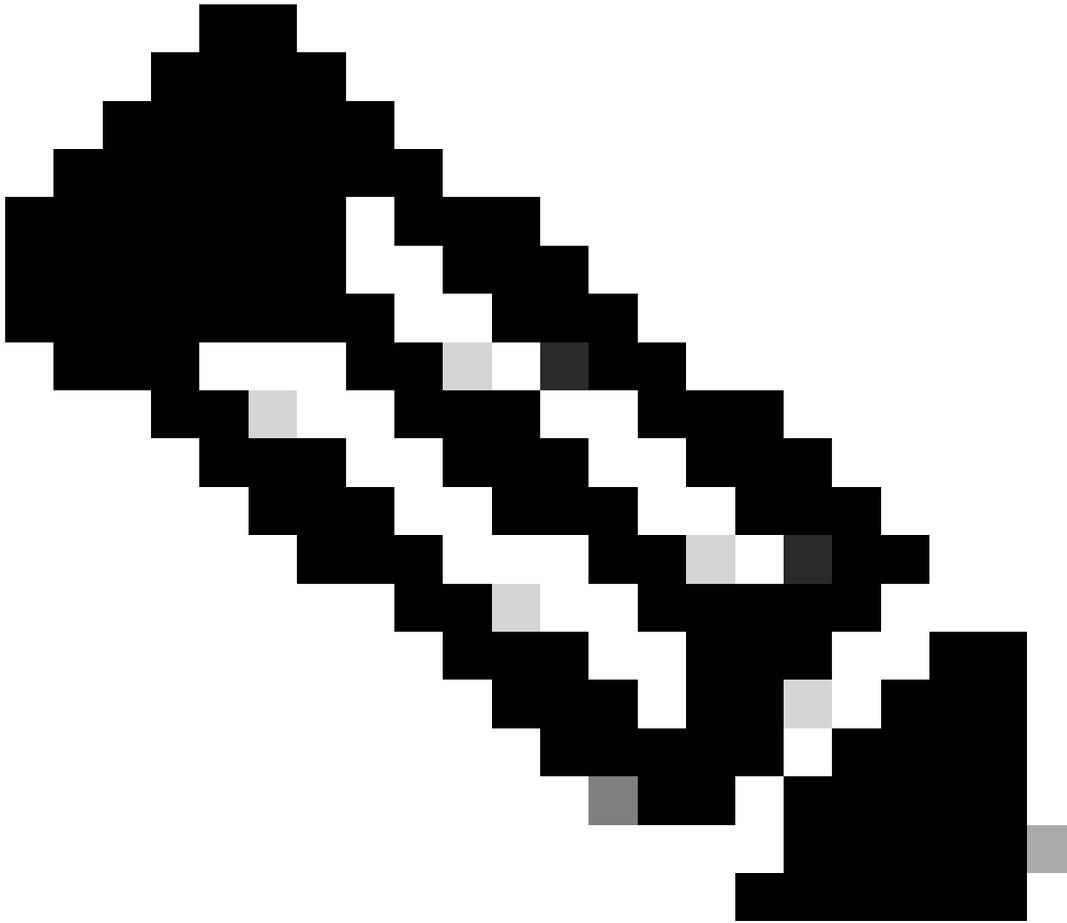
Events (5):

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](#)

4404306881812



Anmerkung: Wenn die Protokollquellenerweiterung nicht "CiscoUmbrella_ext" zugeordnet ist, wählen Sie den Protokollquellennamen aus der Liste aus:

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

360071157752

?

Edit a Log Source Extension

Name

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

Ambiron TrustWave ipAngel Intrusion Prevention Sy:

Apache HTTP Server

Application Security DbProtect

↔

↔

Set to default for

Cisco Umbrella

Upload Extension: No file chosen

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>

```

360071326791

Das nachfolgende Beispiel zeigt das Aussehen eines Cisco Managed Buckets:

```

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

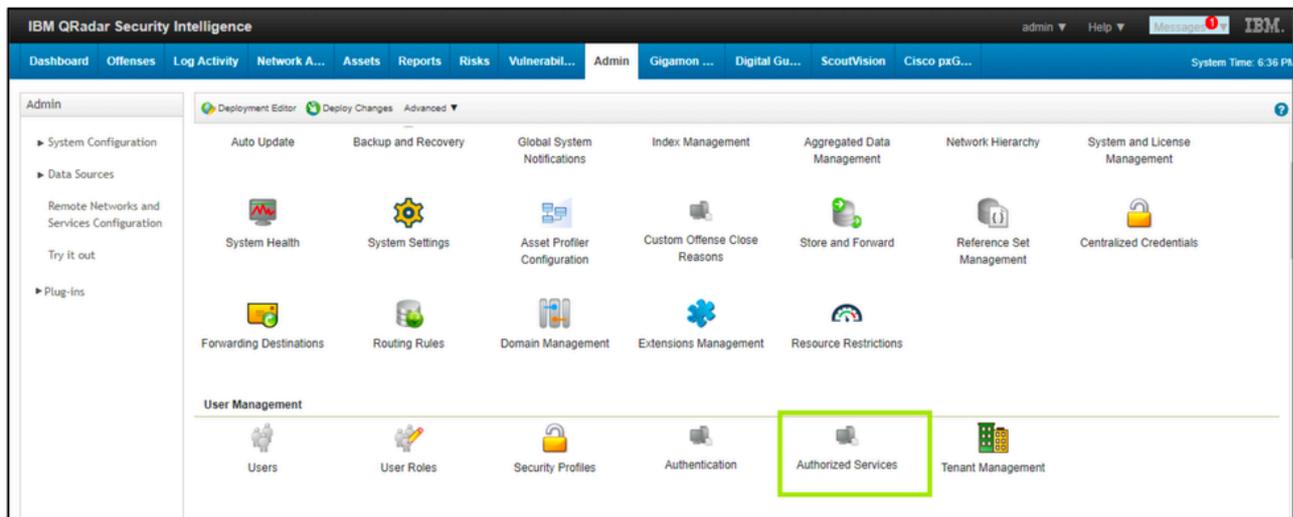
```

Navigieren Sie zurück zu den Cisco Cloud Security-App-Einstellungen, und stellen Sie die Aktualisierungsrate des Bereichs in Stunden auf den Mindestwert "1" ein, damit die Diagramme Daten anzeigen.

Authentifizierungstoken wird generiert

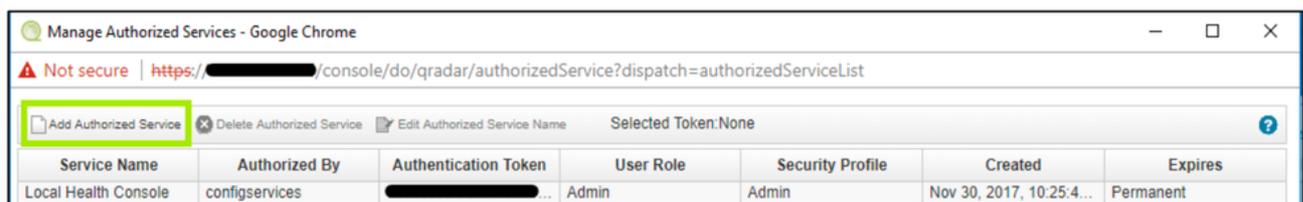
Der Administrator muss ein Service-Token generieren, um es Ihrer Cisco Security-App hinzuzufügen. Als Best Practice wurde das Authorized Service Token alle 90 Tage neu erstellt:

1. Melden Sie sich bei QRadar > Registerkarte Admin > Authorized Services an.



360071965571

2. Autorisierte Services hinzufügen

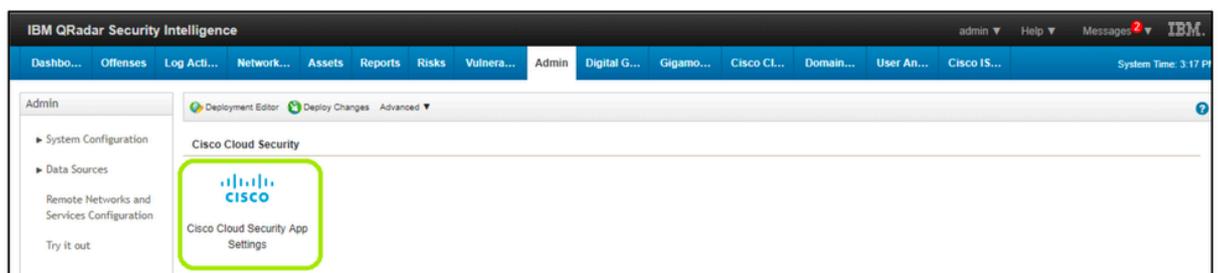


360071965551

3. Geben Sie die Details ein, und generieren Sie ein Authentifizierungstoken.
4. Nachdem Sie das Token generiert haben, klicken Sie auf "Deploy Changes".

Konfigurieren der Cisco Cloud Security-App

1. Scrollen Sie von der Registerkarte Admin in der QRadar-Navigationsleiste nach unten, und öffnen Sie die Einstellungen der Cisco Cloud Security-App.



360071754732

2. Geben Sie das im vorherigen Schritt generierte Authentifizierungstoken ein.

QRadar Settings

QRadar Server IP

QRadar Server port

QRadar service token

360072462992

3. Bearbeiten Sie die API-Einstellungen wie folgt:

- URL der Cisco Investigate Base: <https://investigate.api.umbrella.com/>
- Cisco Investigate API-Token: Generieren über das Umbrella Dashboard -> Investigate -> API Keys -> Create New Token; Weitere Informationen finden Sie unter <https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>
- Basis-URL für Cisco Enforce: <https://s-platform.api.opendns.com/1.0/>
- Cisco Kundenschlüssel durchsetzen: Generierung über das Umbrella Dashboard -> Richtlinienkomponenten -> Integrationen -> Hinzufügen; Weitere Informationen finden Sie unter <https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>
- Cisco Cloudlock Base-URL: `https://{YourCloudlockAPIServer}/api/v2/` (z. B. <https://api-demo.cloudlock.com/api/v2/>). Bitte bestätigen Sie Ihre Cloudlock Base-URL, auch Cloudlock Enterprise API-URL genannt, per E-Mail an support@cloudlock.com.)
- Cisco Cloudlock API-Token: via Cloudlock generieren -> Einstellungen -> Authentifizierung & API -> Generieren; Weitere Informationen finden Sie unter <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

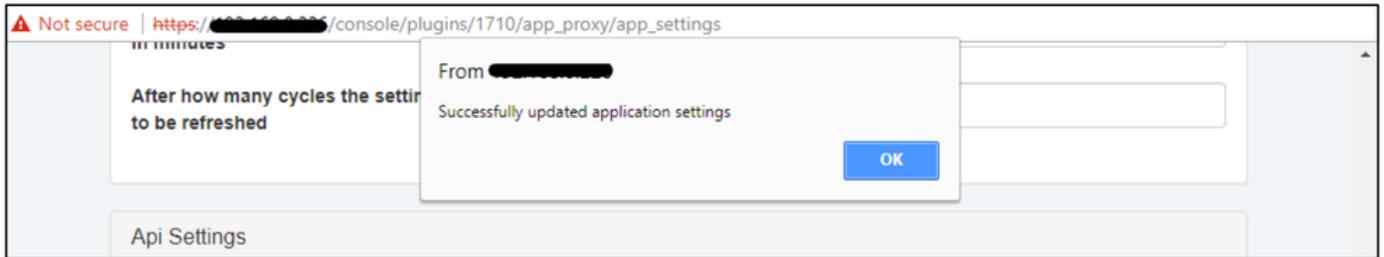
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

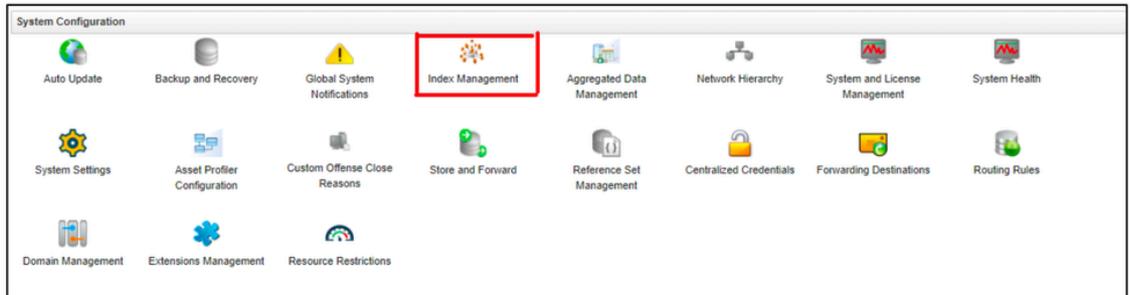
Ein Popup zeigt an, dass die Anwendungseinstellungen erfolgreich aktualisiert wurden.



360071986151

Indizierung in QRadar

1. Navigieren Sie zur Registerkarte Admin, und klicken Sie dann auf Indexverwaltung.



360071780112

2. Indizieren Sie die mit der App verpackten CEPs.

Index Management - Google Chrome
console/do/qradar/indexManagementConsole?appName=QRadar&pageId=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	81.49%	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

Die folgenden CEPs werden für die Indizierung empfohlen:

1. Protokollquelle
2. DNS-Kategorie
3. Ereignistyp
4. Domänen-URL
5. Identitäten
6. Detaillierter Benutzer
7. Benutzername
8. Standort-Ursprungs-ID
9. Ereigniskategorie
10. Richtlinie
11. Ressource

Jetzt können Sie mit QRadar die Überwachung von Details zu Cisco Umbrella, Investigate und CloudLock starten. Weitere Anweisungen zur Navigation in QRadar finden Sie hier: [Navigation in der Cisco Cloud Security App](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.