

IBM QRadar向けクラウドセキュリティアプリの設定

内容

[はじめに](#)

[概要](#)

[要件](#)

[Cisco Umbrellaの要件](#)

[IBMセキュリティQRadar SIEM要件](#)

[IBM QRadar向けCisco Cloud Securityアプリのインストール](#)

[Cisco Cloud Securityアプリケーションの設定：ログソースの追加](#)

[認証トークンの生成](#)

[Cisco Cloud Securityアプリケーションの設定](#)

[QRadarでのインデックス作成](#)

はじめに

このドキュメントでは、ログ分析用にIBM QRadarを使用してCisco Cloud Securityアプリケーションを設定する方法について説明します。

概要

IBMのQRadarは、ログ分析用の一般的なSIEMです。Cisco Umbrellaが組織のDNSトラフィック用に提供するログなど、大量のデータを分析するための強力なインターフェイスを提供します。IBM QRadar向けCisco Cloud Security Appは、複数のセキュリティ製品 (Investigate、Enforcement、およびCloudLock) からの情報を提供し、それらをQRadarと統合します。また、セキュリティを自動化し、QRadarから脅威をすばやく直接封じ込めるのにも役立ちます。

QRadar用のCisco Cloud Securityアプリをセットアップすると、Cisco Cloud Securityプラットフォームからのすべてのデータが統合され、QRadarコンソールにグラフィカルな形式でデータを表示できるようになります。アナリストはアプリケーションから次の操作を実行できます。

- ドメイン、IPアドレス、電子メールアドレスの調査
- ドメインのブロックとブロック解除 (適用)
- ネットワークのすべてのインシデントに関する情報を表示します。

この記事では、S3バケットからログをプルして使用できるように、QRadarをセットアップして実行する基本的な方法について説明します。

要件



注:QRadarはIBMがサポートする必要があります。サードパーティ製のハードウェアまたはソフトウェアをシスコが直接サポートすることはできません。UmbrellaダッシュボードをS3バケットに接続する際に問題が発生した場合は、サポートを提供します。ここに記載されている情報の多くは、IBMのWebサイト (https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Um) も入手できます。

Cisco Umbrellaの要件

このドキュメントでは、Amazon AWS S3バケットがUmbrella(Settings > Log Management)で設定され、最新のログがアップロードされ、緑色で表示されていることを前提としています。

この機能の設定方法の詳細については、「[ログの管理](#)」を参照してください。

IBMセキュリティQRadar SIEM要件

管理者は、QRadarアプライアンス、Amazon S3構成、およびUmbrellaダッシュボードに対する

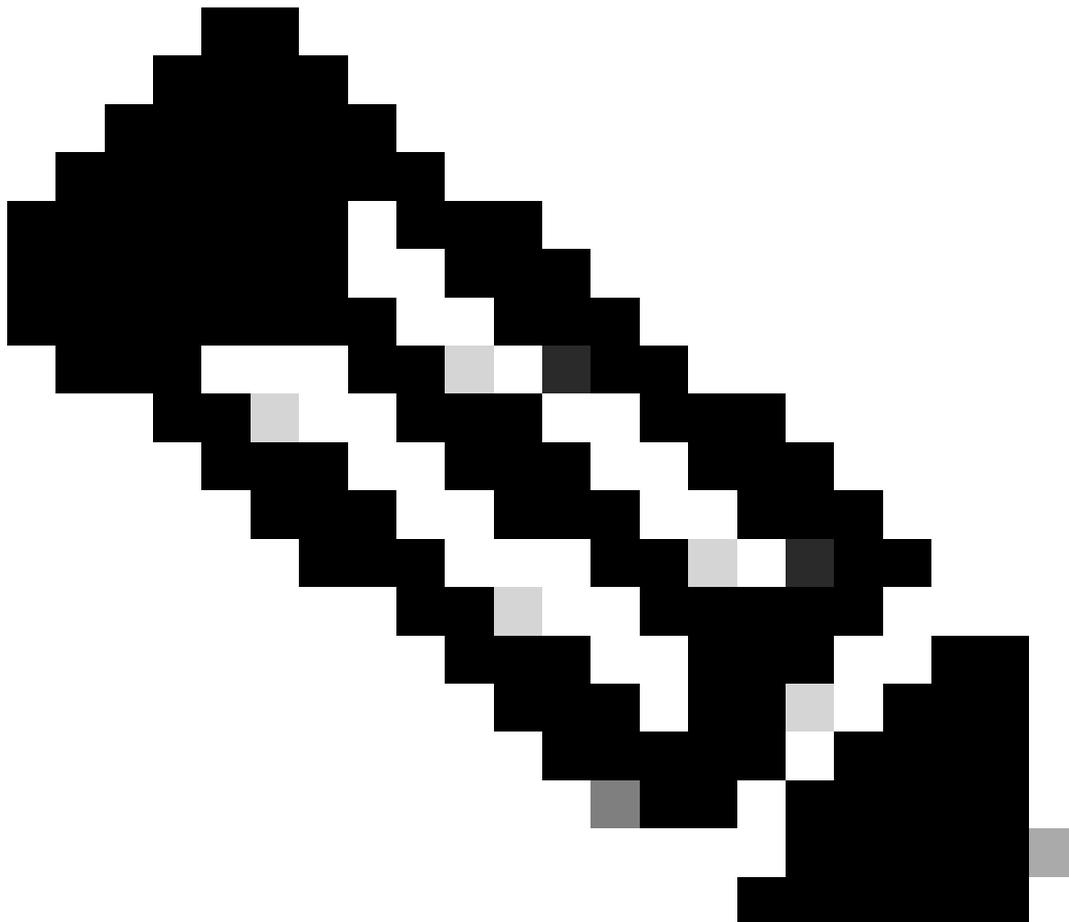
管理者権限を持っている必要があります。これらの手順は、QRadar管理者がLSX (Log source Extension)ファイルの作成に精通していることを前提としています。

Cisco Cloud Security App v1.0.3は、IBM QRadar 7.2.8までしか使用できません。新しいバージョンv1.0.6は、7.4.2以降の現在のQRadarバージョンで動作します。

IBM QRadar向けCisco Cloud Securityアプリのインストール

1. IBM QRadar向けCisco Cloud Security Appのダウンロードとインストールについては、[Cisco Cloud Security App v1.0.3](#)(IBM QRadar v7.2.8)または[Cisco Cloud Security App v1.0.6](#)(IBM QRadar v7.4.8)を参照してください。
2. インストール後、QRadarで変更を展開します。

Cisco Cloud Securityアプリケーションの設定：ログソースの追加

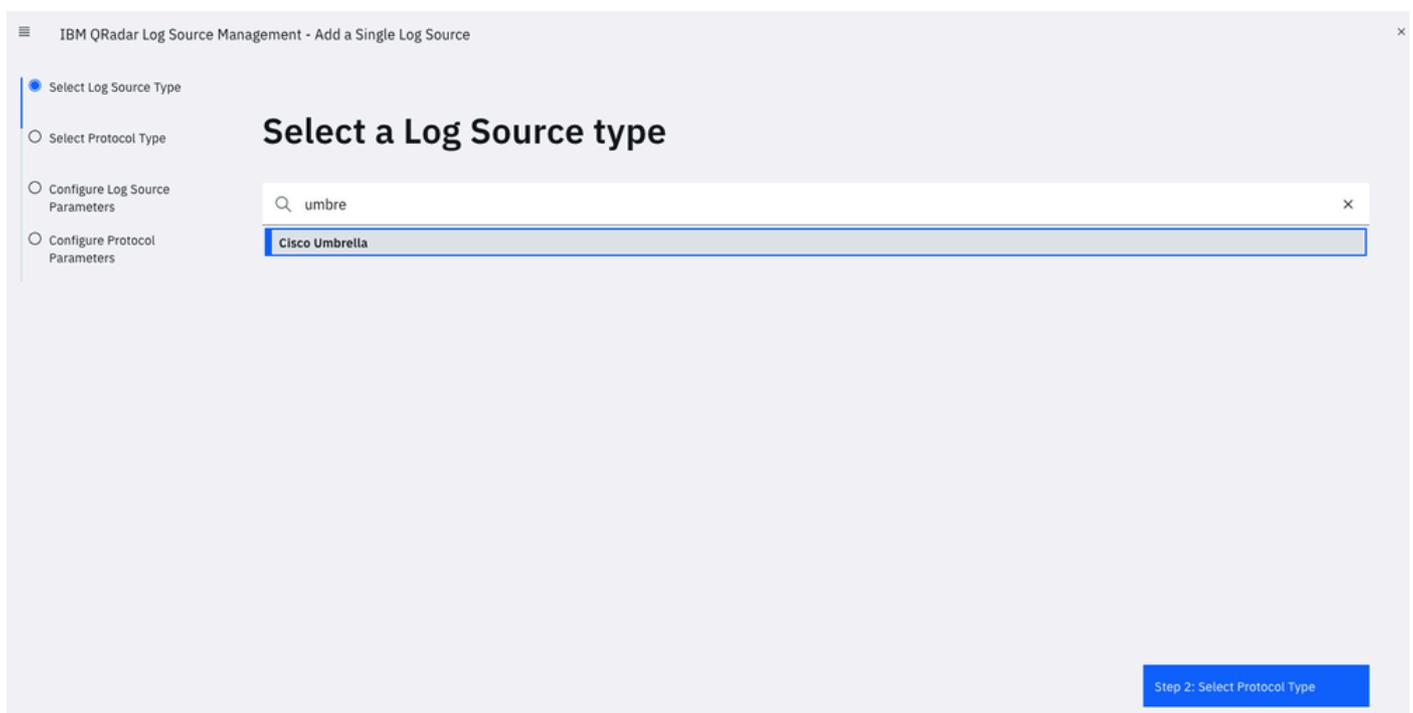


注:S3では監査やファイアウォールなどの他のログを確認できますが、サポートされていません。ここにリストされている3つだけを設定します。これらの他のログを設定しようとすると、エラーが発生します。

ログソースを追加するには、QRadarナビゲーションバーのAdminタブをクリックし、下にスクロールしてQRadar Log Source Managementをクリックし、+New Log Source:

- ログのソース名 (エントリ名はリストに示されている名前と正確に一致する必要があります):
 - Cisco DNSログ : cisco_umbrella_dns_logs
 - Cisco Umbrella IPログ : cisco_umbrella_ip_logs
 - Cisco Umbrellaプロキシログ : cisco_umbrella_proxy_logs
- イベント形式 : Cisco Umbrella CSV
- ログソースタイプ : Cisco Umbrella
- プロトコル構成 : Amazon AWS S3 REST API
- ファイルパターン : .*?\.csv\.gz
- ログソースの拡張子 : CiscoUmbrella_ext **
- このログソースをメンバーにするグループを選択してください :
cisco_umbrella_logsource_group

Add a Single Log Sourceウィザードを実行します。



4404306773524

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 X

Q + Add Group

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

CiscoUmbrella_ext X v

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):

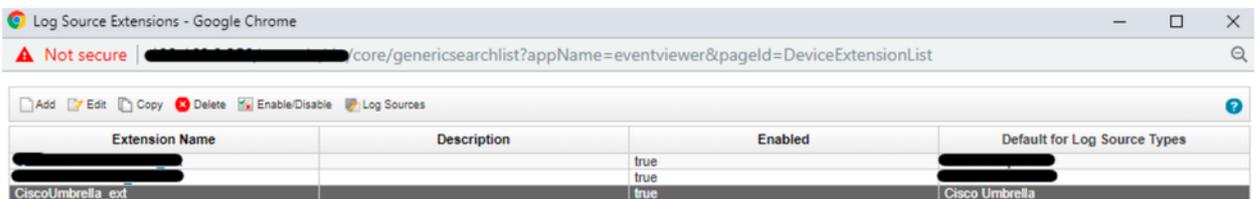
Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile": "[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile": "[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs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

[Step 4: Configure Protocol Parameters](#)

[Finish](#)

4404306881812

注：ログソースの拡張子が「CiscoUmbrella_ext」にマッピングされていない場合は、リストからログソース名を選択してください。



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

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

Cisco Managed Bucketの例を示します。

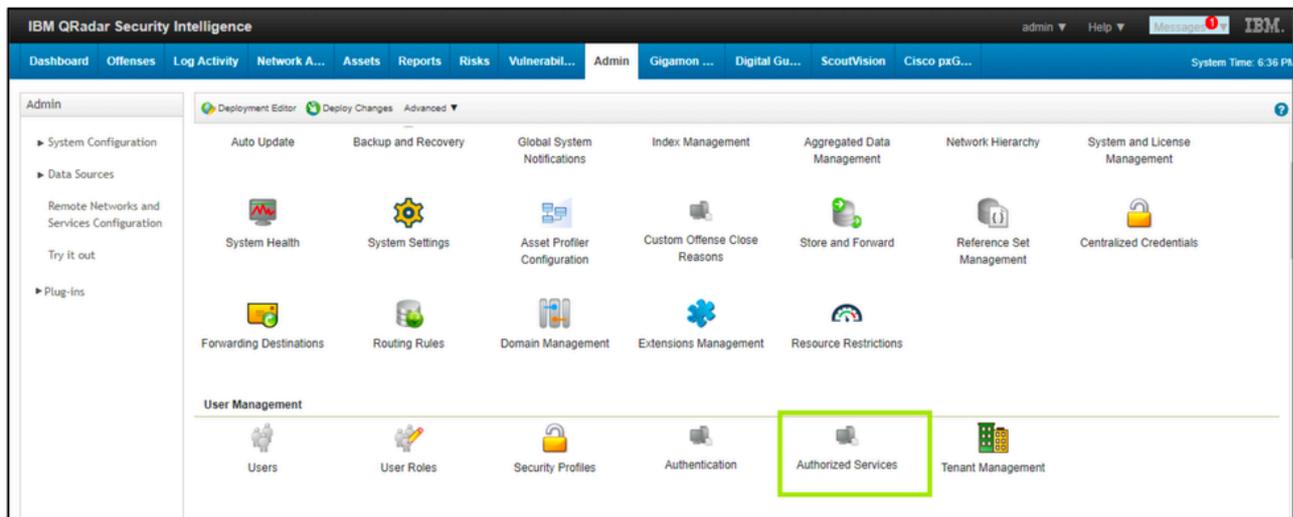
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

Cisco Cloud Security App Settingsに戻り、グラフにデータを表示するために、Panel refresh rate in hoursを最小値の「1」に設定します。

認証トークンの生成

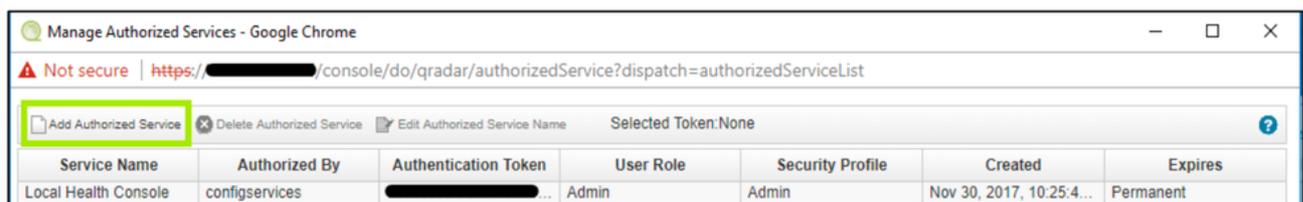
管理者は、Cisco Security Appに追加するサービストークンを生成する必要があります。ベストプラクティスとして、Authorized Service Tokenを90日ごとに再作成しました。

1. QRadar > Admin Tab > Authorized Servicesにログインします。



360071965571

2. Authorized Servicesを追加します。

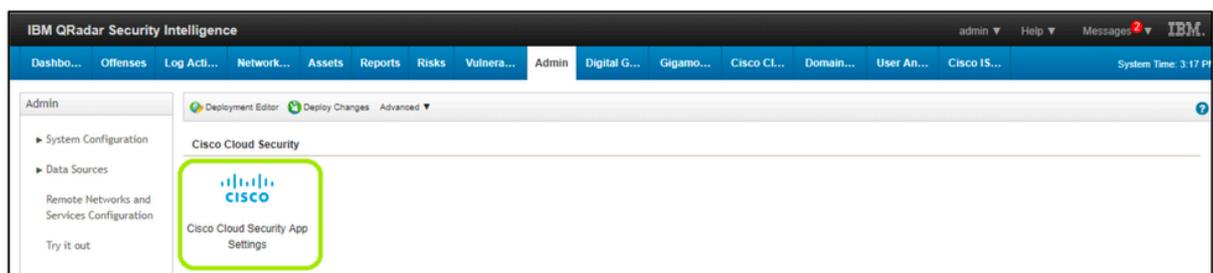


360071965551

3. 詳細を入力し、認証トークンを生成します。
4. トークンを生成したら、「Deploy Changes」をクリックします。

Cisco Cloud Securityアプリケーションの設定

1. QRadarナビゲーションバーのAdminタブで、スクロールダウンしてCisco Cloud Security App Settingsを開きます。



360071754732

2. 前のステップで生成した認証トークンを入力します。

Qradar Settings

QRadar Server IP

QRadar Server port

QRadar service token

360072462992

3. Api Settingsを次のように編集します。

- Cisco InvestigateのベースURL:<https://investigate.api.umbrella.com/>
- Cisco Investigate APIトークン : Umbrellaダッシュボードから生成 -> Investigate -> API Keys -> Create New Token。詳細については、<https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>を参照してください。
- Cisco EnforceベースURL:<https://s-platform.api.opendns.com/1.0/>
- Cisco Enforce CustomerKey: Umbrellaダッシュボード -> ポリシーコンポーネント -> 統合 -> 追加で生成。詳細については、<https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>を参照してください。
- Cisco CloudlockベースURL: <https://{YourCloudlockAPIServer}/api/v2/>(例 : <https://api-demo.cloudlock.com/api/v2/>) CloudlockベースURL (別名 CloudlockエンタープライズAPI URL) を support@cloudlock.com に電子メールを送信して確認してください)。
- Cisco Cloudlock APIトークン : Cloudlockによる生成 -> 設定 -> 認証& API -> 生成。詳細については、<https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication>を参照してください。

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

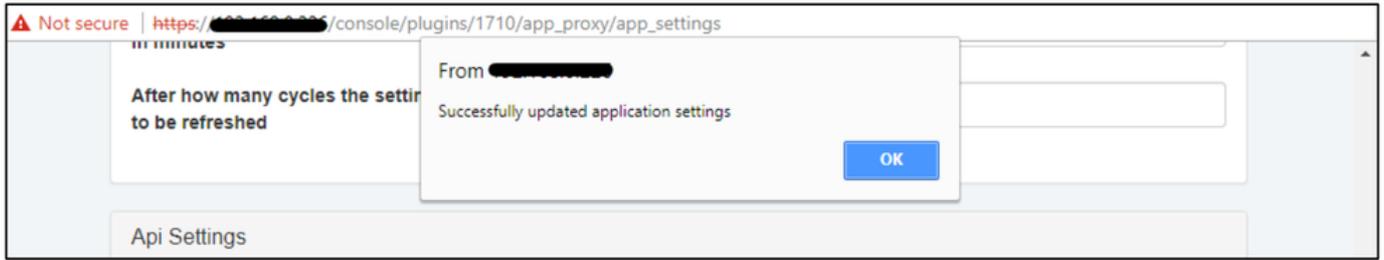
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

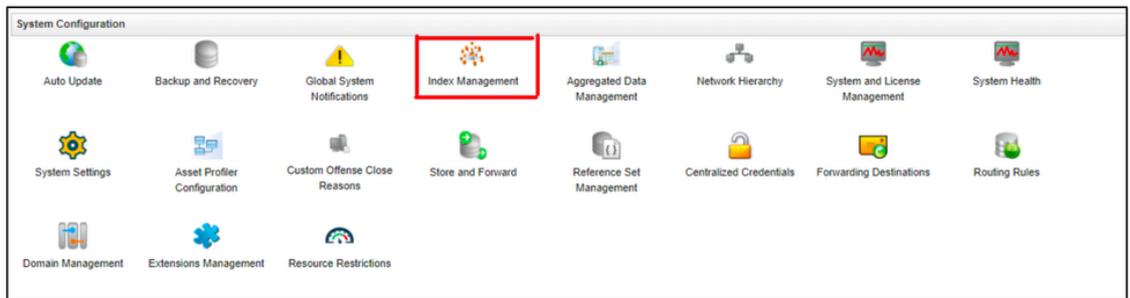
ポップアップが表示され、アプリケーション設定が正常に更新されたことが示されます。



360071986151

QRadarでのインデックス作成

1. Adminタブに移動し、Index Managementをクリックします。



360071780112

2. アプリにパッケージされているCEPをインデックス化します。

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)	12.68%	0%	100%	0KB	events
●	Event Date (custom)	10.55%	0%	100%	0KB	events
●	Identities (custom)	8.65%	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

インデックスを作成する推奨CEPは次のとおりです。

1. ログソース
2. DNSカテゴリ
3. イベント タイプ
4. ドメインURL
5. ID
6. 詳細なユーザ
7. ユーザ名
8. 場所の原点ID
9. イベントカテゴリ
10. ポリシー
11. リソース

これで、QRadarを使用して、Cisco Umbrella、Investigate、およびCloudLockの詳細のアクティビティの監視を開始する準備が整いました。QRadarのナビゲーション方法の詳細については、Cisco Cloud Securityアプリのナビゲーションをご覧ください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。