

為IBM QRadar配置雲安全應用

目錄

[簡介](#)

[概觀](#)

[需求](#)

[Cisco Umbrella要求](#)

[IBM安全QRadar SIEM要求](#)

[安裝適用於IBM QRadar的思科雲安全應用](#)

[思科雲安全應用配置：新增日誌源](#)

[正在生成身份驗證令牌](#)

[配置思科雲安全應用](#)

[在QRadar中索引](#)

簡介

本文檔介紹如何使用IBM QRadar配置思科雲安全應用以進行日誌分析。

概觀

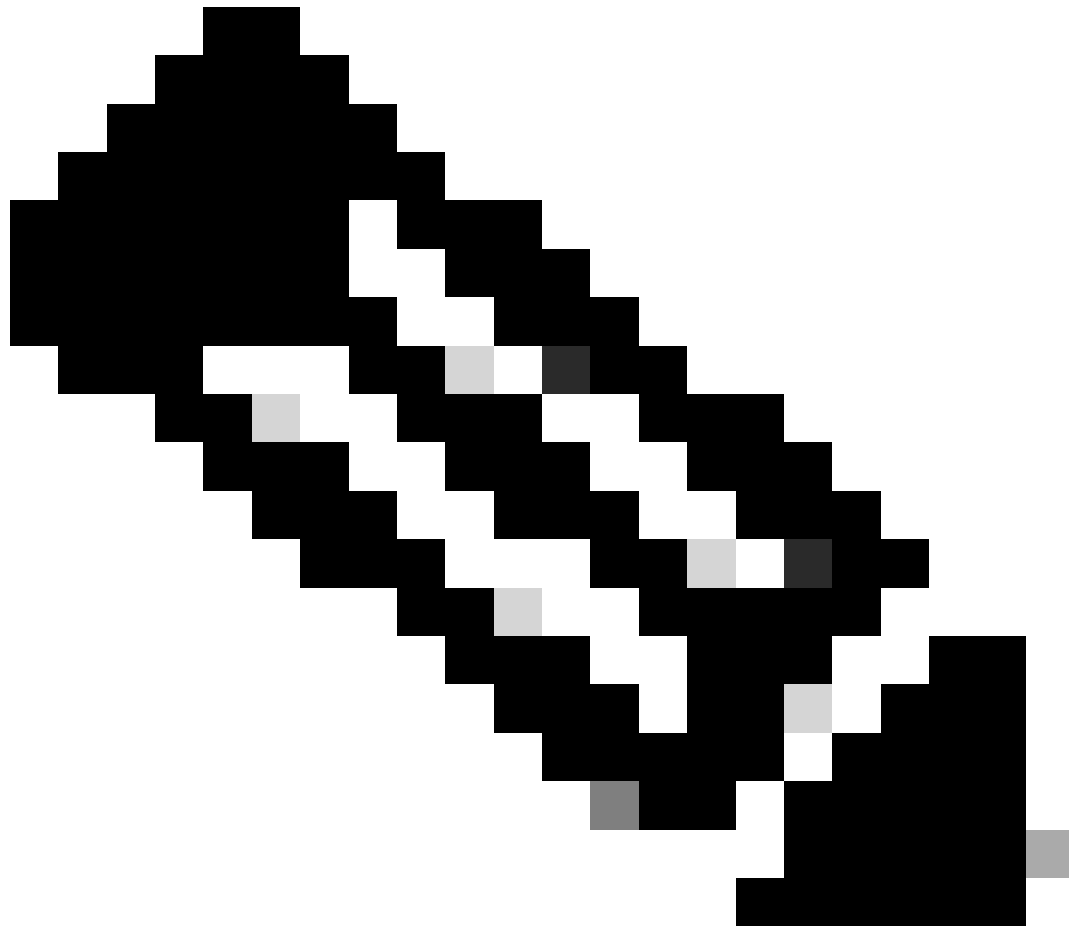
來自IBM的QRadar是日誌分析的常用的SIEM。它提供強大的介面來分析大量資料，例如Cisco Umbrella為您的組織的DNS流量提供的日誌。適用於IBM QRadar的Cisco Cloud Security App提供來自多種安全產品（調查、實施和CloudLock）的見解，並將它們與QRadar整合。它還可以幫助使用者自動執行安全操作，並從QRadar快速直接遏制威脅。

當您為QRadar設定思科雲安全應用時，它整合了思科雲安全平台的所有資料，並允許您在QRadar控制檯中以圖形形式檢視資料。從應用程式中，分析師可以：

- 調查域、IP地址、電子郵件地址
- 阻止和取消阻止域（實施）
- 檢視網路所有事件的資訊。

這篇文章概述了設定QRadar並運行的基本方法，以便它能夠從S3儲存桶提取日誌並使用這些日誌。

需求



附註：對QRadar的支援必須來自IBM，因為思科無法直接支援第三方硬體或軟體。對於將您的Umbrella控制面板連線到S3儲存桶的任何問題，我們可以提供支援。此處的大部分資訊也可在IBM網站上找到

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

Cisco Umbrella要求

本文檔假設您的Amazon AWS S3儲存桶已在Umbrella (設定>日誌管理) 中配置，並且顯示綠色且已上傳最近的日誌。

有關如何配置此功能的詳細資訊，請參閱此處：[管理日誌](#)。

IBM安全QRadar SIEM要求

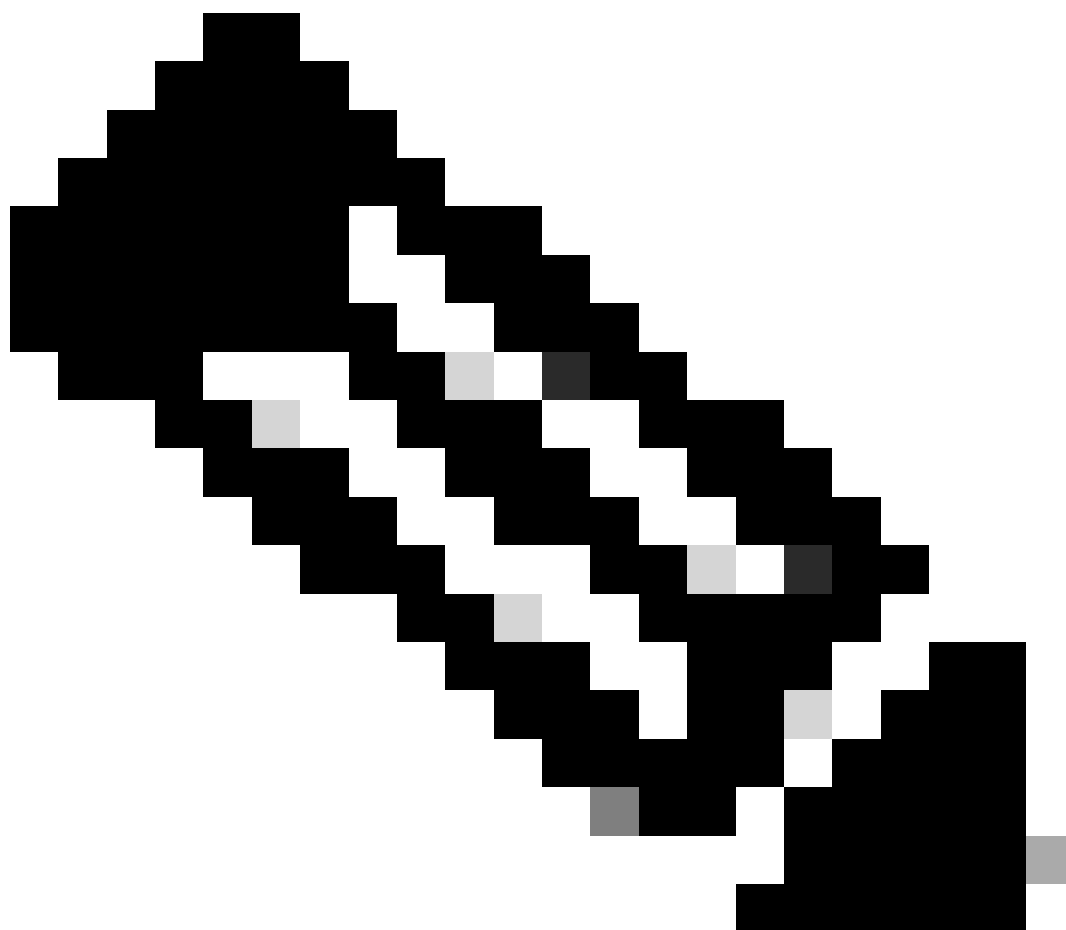
管理員需要擁有QRadar裝置、Amazon S3配置和Umbrella控制面板的管理許可權，這些說明假設QRadar管理員熟悉建立LSX (日誌源擴展) 檔案。

請注意，Cisco Cloud Security App v1.0.3隻適用於IBM QRadar 7.2.8。新版本v1.0.6適用於當前7.4.2及更高版本的QRadar。

安裝適用於IBM QRadar的思科雲安全應用

1. 下載並安裝適用於IBM QRadar的Cisco Cloud Security App，網址為：[Cisco Cloud Security App v1.0.3](#)（適用於IBM QRadar v7.2.8）或[Cisco Cloud Security App v1.0.6](#)（適用於IBM QRadar v7.4.8）。
2. 安裝後，在QRadar中部署更改。

思科雲安全應用配置：新增日誌源



附註：您可以在S3中看到其他日誌，例如審計和防火牆，但不受支援。只設定此處列出的三項。任何配置其他日誌的嘗試都會導致失敗。

要新增日誌源，請按一下QRadar導航欄上的Admin頁籤，向下滾動並按一下QRadar Log Source

Management，然後按一下按鈕+New Log Source:

- 日誌源名稱 (條目名稱必須與所列條目名稱完全匹配) :
 - Cisco DNS日誌 : cisco_umbrella_dns_logs
 - Cisco Umbrella IP日誌 : cisco_umbrella_ip_logs
 - 思科Umbrella代理日誌 : cisco_umbrella_proxy_logs
- 事件格式 : Cisco Umbrella CSV
- 日誌源型別 : 思科資安防護傘
- 協定配置 : Amazon AWS S3 REST API
- 檔案模式 : .*?\.\csv\.\gz
- 日誌源擴展 : CiscoUmbrella_ext **
- 請選擇您希望此日誌源成為其成員的任何組 : cisco_umbrella_logsource_group

請通過「新增單個日誌源」嚮導：

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Select a Log Source type

Search: umbre

Cisco Umbrella

Step 2: Select Protocol Type

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

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](#)

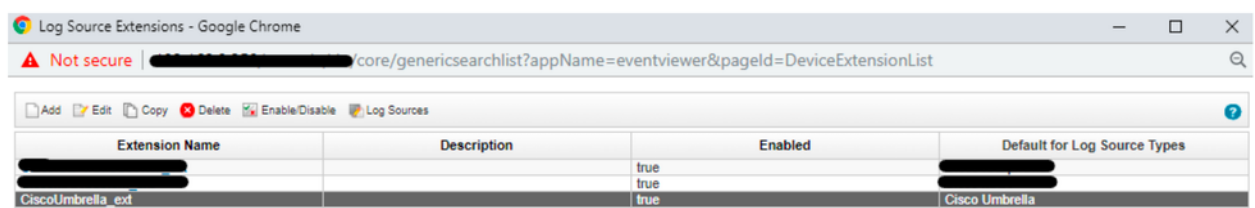
Results (4):

- ✓ 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"}

附註：如果日誌源擴展未對映到「CiscoUmbrella_ext」，請從清單中選擇日誌源名稱：



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

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

以下是思科託管儲存桶的示例：

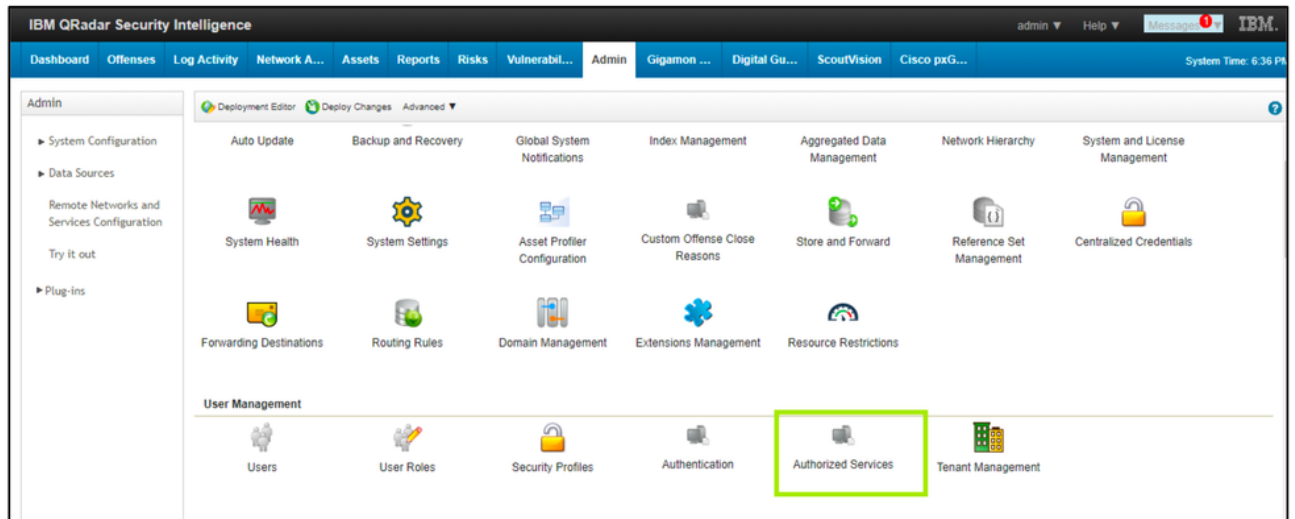
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

導覽回Cisco Cloud Security App Settings，並將Panel refresh rate（以小時為單位）設定為最小值「1」，以便圖形顯示資料。

正在生成身份驗證令牌

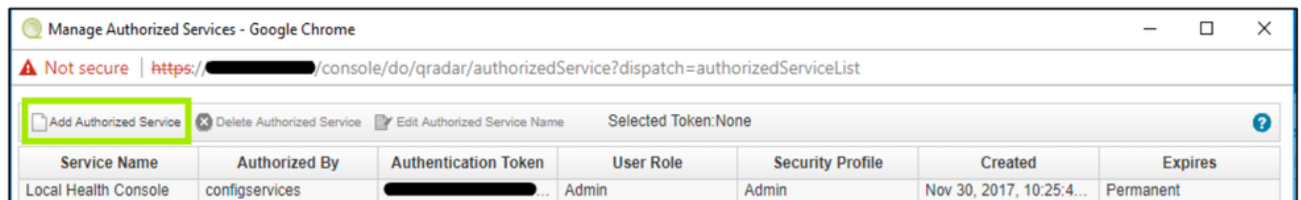
管理員需要生成服務令牌以新增到您的思科安全應用。最佳作法是每90天重新建立一次授權服務令牌：

1. 登入QRadar > Admin Tab > Authorized Services。



360071965571

2. 新增授權服務。

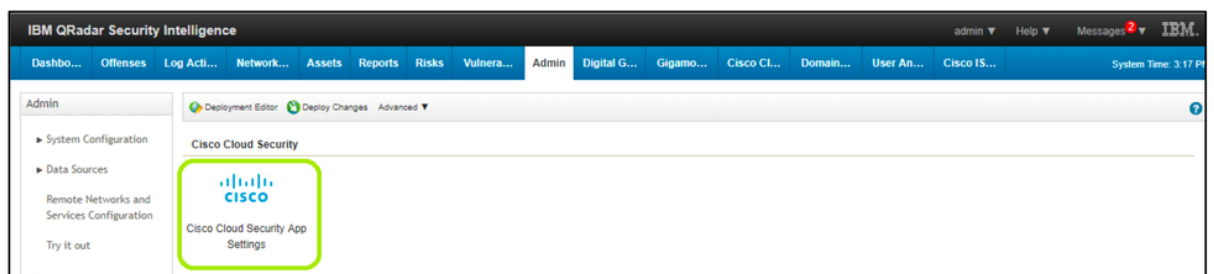


360071965551

3. 輸入詳細資訊並生成身份驗證令牌。
4. 生成令牌後，按一下「部署更改」。

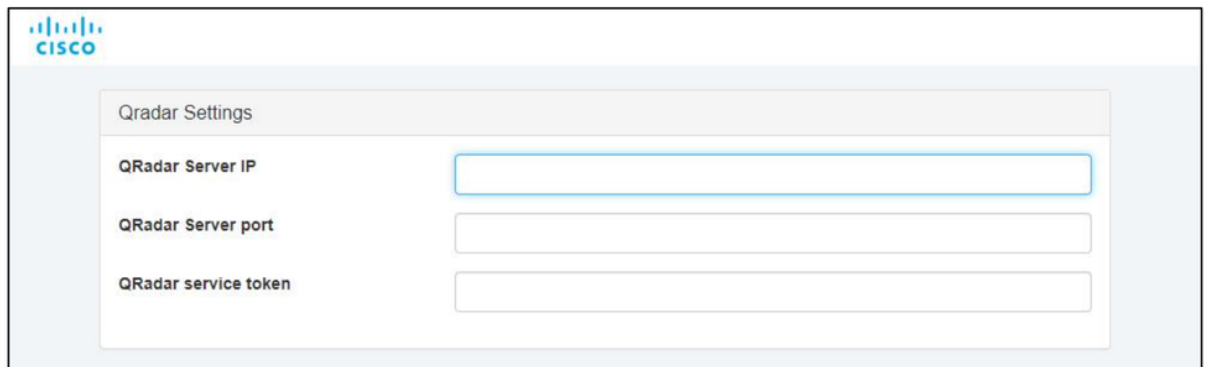
配置思科雲安全應用

1. 從QRadar導航欄上的Admin頁籤，向下滾動並開啟Cisco Cloud Security App Settings。



360071754732

2. 輸入在上一步中生成的身份驗證令牌。



Qradar Settings

QRadar Server IP

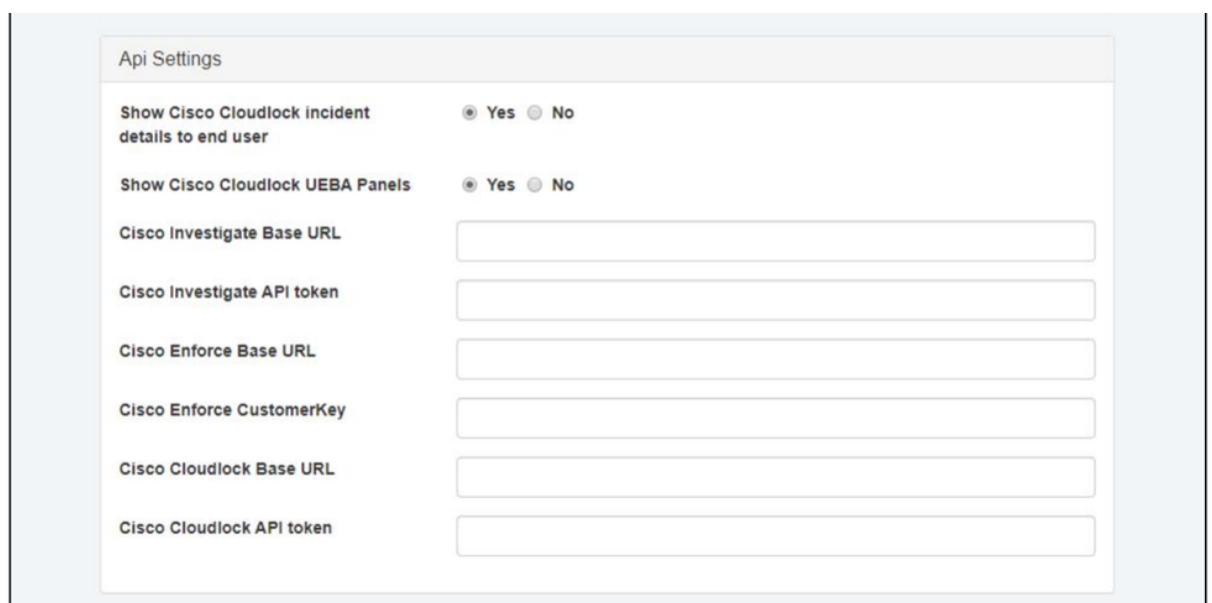
QRadar Server port

QRadar service token

360072462992

3. 按如下方式編輯Api設定：

- 思科調查基本URL:<https://investigate.api.umbrella.com/>
- 思科調查API令牌：通過Umbrella控制面板生成 — >調查 — > API金鑰 — >建立新令牌；有關詳細資訊，請參閱<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: 通過Umbrella控制面板 — > Policy Components -> Integrations -> Add;有關詳細資訊，請參閱<https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>
- Cisco Cloudlock基本URL:<https://{YourCloudlockAPIServer}/api/v2/>(例如，<https://api-demo.cloudlock.com/api/v2/>。請通過向support@cloudlock.com傳送電子郵件來確認您的Cloudlock基本URL，又稱Cloudlock企業API URL。)
- Cisco Cloudlock API令牌：通過Cloudlock -> Settings -> Authentication & API -> Generate;有關詳細資訊，請參閱<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

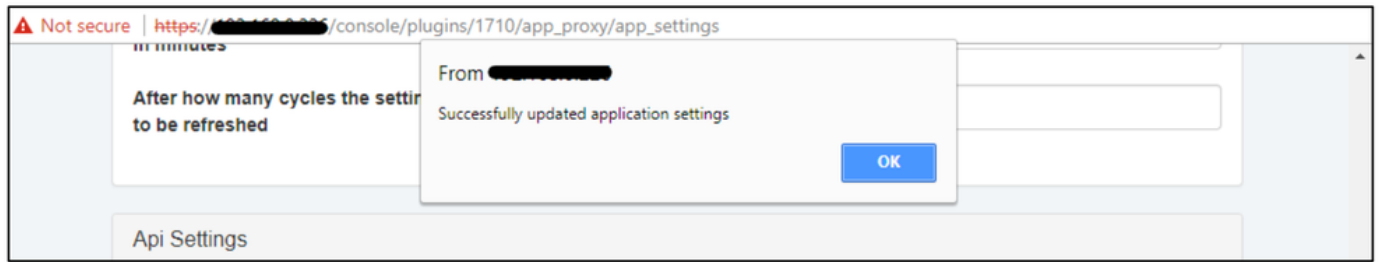
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

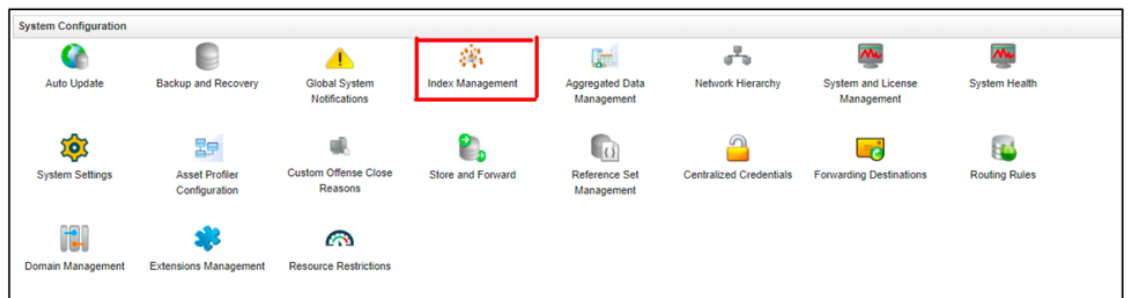
彈出視窗表示已成功更新應用程式設定。



360071986151

在QRadar中索引

1. 導航到Admin頁籤，然後按一下Index Management。



360071780112

2. 為應用程式打包的CEP編制索引。

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

以下是建議編制索引的CEP:

1. 日誌源
2. DNS類別

3. 事件型別
4. 域URL
5. 身份
6. 精確定位使用者
7. 使用者名稱
8. 位置來源ID
9. 事件類別
10. 政策
11. 資源

現在，您已準備好使用QRadar開始監控Cisco Umbrella、Investigate和CloudLock詳細資訊中的活動。有關如何瀏覽QRadar的更多說明可在此處找到：[導航思科雲安全應用](#)。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。