

IBM QRadar لةباحسلا نامأ قيبطت نيوكت

تايوتحمل

[قمدملا](#)

[ةماع قرظن](#)

[تابلطتملا](#)

[Cisco Umbrella تابلطتم](#)

[IBM Security QRadar SIEM تابلطتم](#)

[IBM QRadar لةباحسلا نامأ قيبطت تيبتت](#)

[لجس ردم ةفاض: Cisco نم ةباحسلا نامأ قيبطت نيوكت](#)

[زيمللا ةقداصلما زمر عاشنا](#)

[Cisco نم ةباحسلا نامأ قيبطت نيوكت](#)

[QRadar يف ةسرهفلا](#)

ةمدملا

IBM QRadar مادختساب Cisco نم ةباحسلا نامأ قيبطت نيوكت ةيفيك دنتسمللا اذه فصلي لجلسلا ليلحتل.

ةماع قرظن

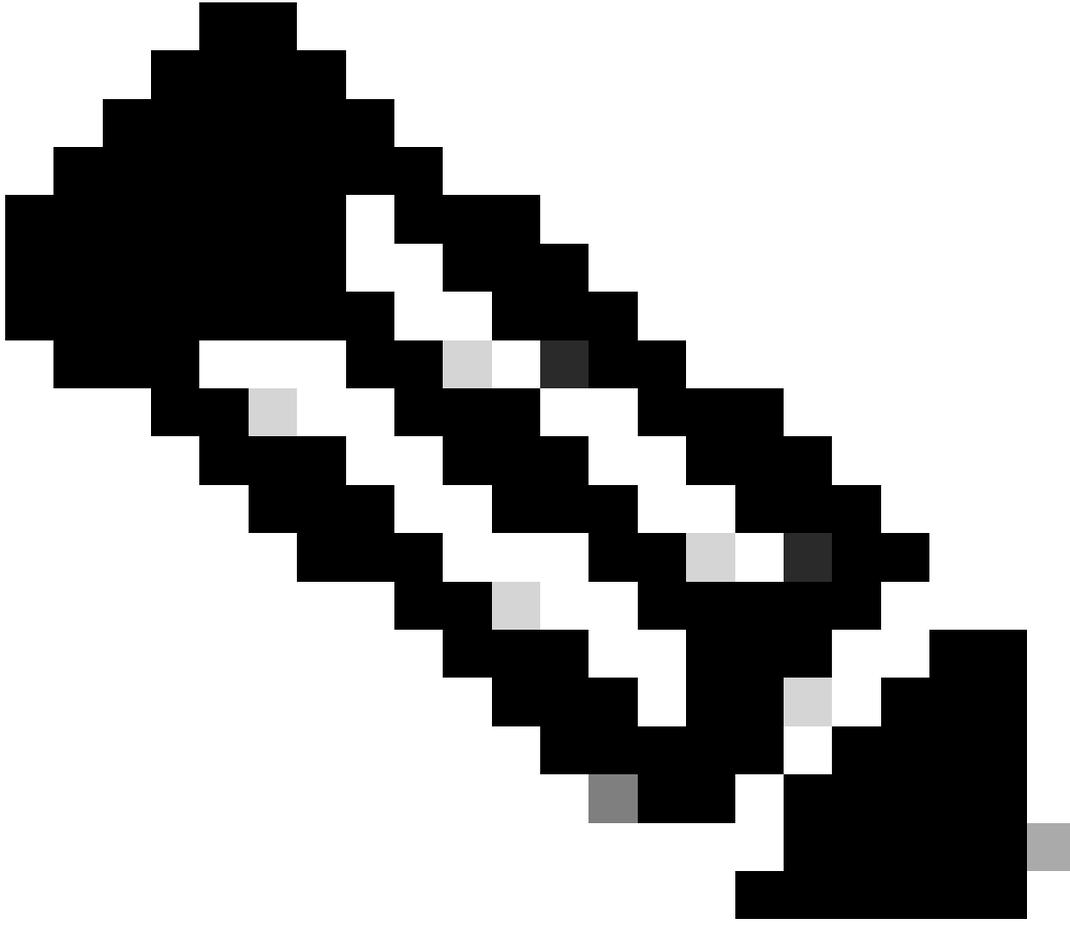
تاعومجم ليلحتل ةيوق ةهجاو رفوي وهو. لجلسلا ليلحتل ةئاش SIEM وه IBM نم QRadar يف DNS رورم ةكرحل Cisco Umbrella نم ةمدملا تالجلسلا لثم، تانايبلا نم ةريبك ةددتم نامأ تاجتنم نم ةيؤر IBM QRadar لةباحسلا نامأ قيبطت رفوي. كتسسؤم يلع مدختسمللا ةأدالا هذه دعاست امك. QRadar عم اهجمديو (CloudLock و ذافنإل او قيقتل) QRadar قيبطت لالخ نم رشابمو عرسأ لكشب تاديدهتلا ءاوتحاو نامألا ةتمتأ.

نامأ ةصنم نم تانايبلا عيجم جمدي هناف، QRadar ل Cisco نم ةباحسلا نامأ قيبطت دادع دنع نم QRadar مكحت ةدحو يف يموسر لكش يف تانايبلا ضرعب لك حمسيو Cisco نم ةباحسلا نوللحمللا عيظتسي، قيبطتلا:

- ينورتكلال ديربلا نيوانعو IP نيوانعو تالاجملا يف قيقتل
- (ذافنإل) اهرظح ءاغلإو تالاجملا رظح
- ةكبشلا شداوح عيجم تامولعم ضرع.

بحس نم نكمتي يتح هليغشتو QRadar دادعإل ةيساسألا ةقيرطلا لاقملا اذه حضوي اهكالهتساو S3 ولد نم تالجلسلا.

تابلطتملا



وأهزجأل معد ىلع ةرداق ريغ Cisco نأل، IBM نم QRadar معد يتأي نأ بجي: ةظحالم ةحول ليصوتب قلعتت تالكشم ي أ ةلاح يف . ةرشابم ةيجراخ تاهج ةعبات لاجمارب لىلع روثعل انكمي امك . معدلاري فوت اننكمي ، S3 ةمزحب كب ةصاخلا Umbrella تامولعم ببولىلع IBM عقوم ىلع انه اهلىع روثعل مت يتلا تامولعمل نم ريثكلل

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

Cisco Umbrella تابلطتم

ةرادإ > تاداعلا) Umbrella يف Amazon AWS S3 ولد نيوكت مت دق هنأ دننسملا اذه ضررتفي ةثيدحلا تالجسلا ليمحت عم رضخألا نولل رهظي وهو (لجسلا

ةرادإ: انه ةءارقلا كنكمي ، ةزيملا هذه نيوكت ةيفيك لوح تامولعمل نم ديزم ىلع لوصحلل [كتالجس](#).

IBM Security QRadar SIEM تابلطتم

Amazon S3 يف نيوكتلاو QRadar (هزجأ) زاهج يف ةيرادا قوقح لوؤسملل نوكي نأ مزلي

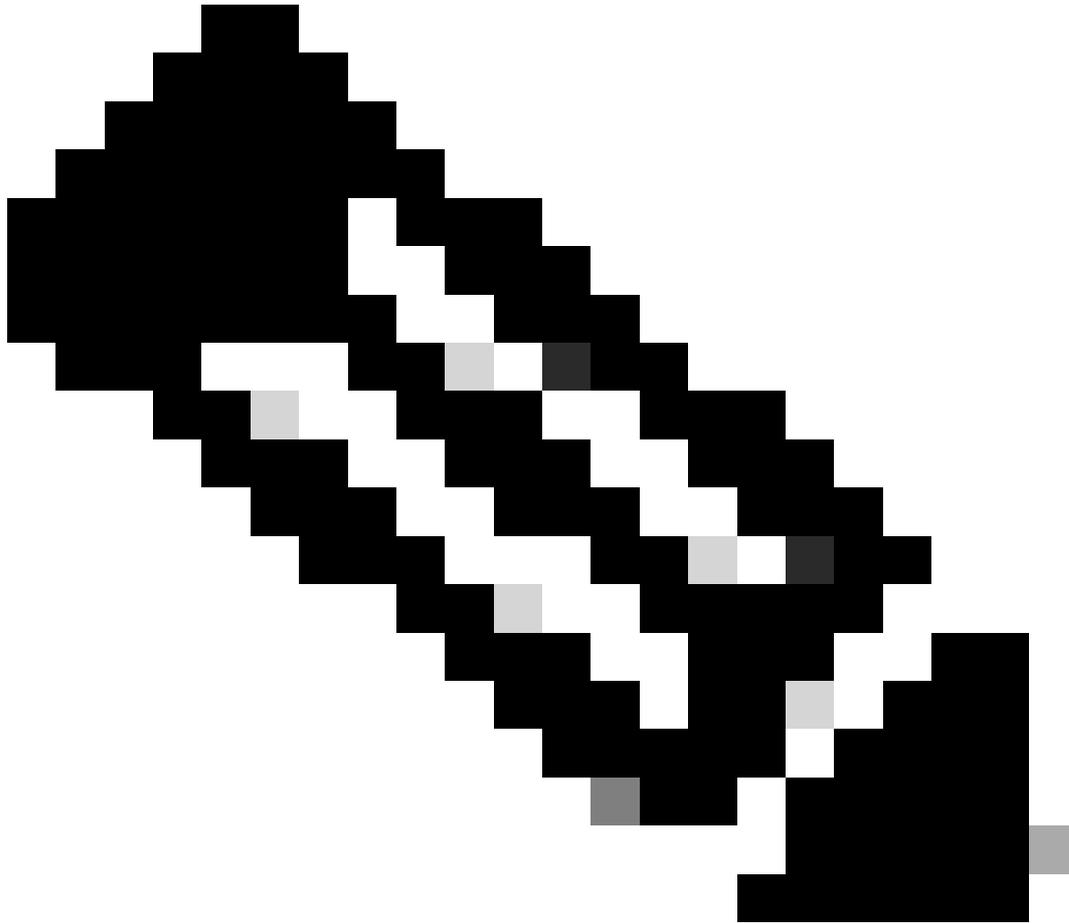
عاشنإب ةيارد ىلع QRadar لوؤسم نأ تامي لعلا هذه ضررتفتو، ةلظملا تامولعم ةحولو (لجسلا رصم قحلم) LSX تافلّم.

IBM QRadar 7.2.8 ىتح طقف لمعي Cisco v1.0.3 ةباحسلا نامأ قيبطت نام ملعلا عاجرلا .ثدحألا تارادصألاو 7.4.2 نم QRadar يلأحلا رادصألا عم ،v1.0.6، ديدجلا رادصألا لمعي

IBM QRadar ل ةباحسلا نامأ قيبطت تيبتت

1. انه دوجوملا IBM QRadar ل هتيبتتو Cisco نم ةباحسلا نامأ قيبطت لي زنت : [Cisco Cloud Security App v1.0.3](#) (ل IBM QRadar v7.2.8) وأ [Cisco Cloud Security App v1.0.6](#) (ل IBM QRadar v7.4.8).
2. QRadar في تاريخيغتلا رشنب مق ، تيبتتلا دعب .

لجس رصم ةفاضأ : Cisco نم ةباحسلا نامأ قيبطت نيوكت



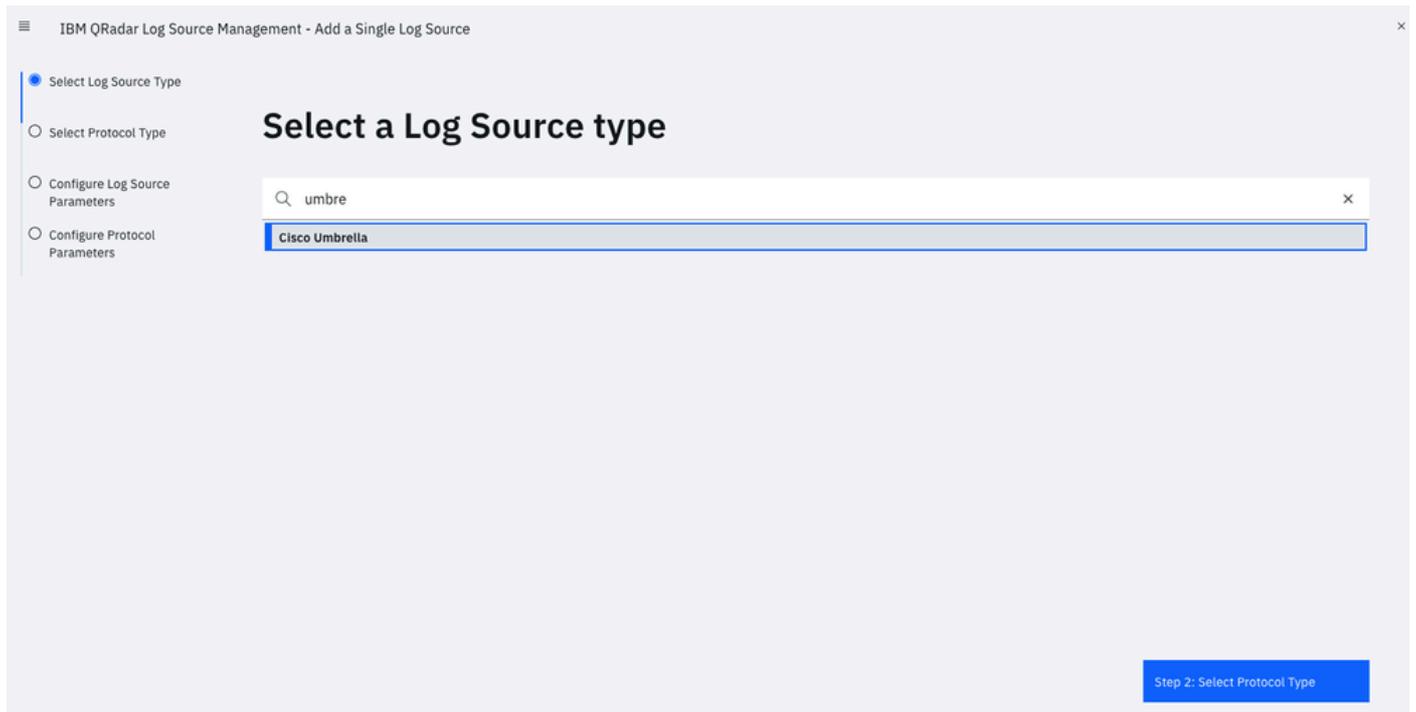
ال مه نأ ريغ ، ةيامح رادجو قيقدت لثم S3 في لجس رخآ تيأرعيطتسي تنأ : ةظحالم هذه نيوكتل تالواحم يأ نع جتنى . انه ةروكذملا ةثالثلا دادعأب طقف مق . دناسي

لش ف ىرأل تاللسل

لقتناو QRadar لقتنل لطيرش في Admin بيوبتل عمال ع قوف رقنا ،لجس رصم ةفاضل
ديج لجس رصم + رزلا قوف رقنا مث ، QRadar لجس رصم ةراد قوف رقناو لفسأل

- (جردم وه امك امامت لاخدإل عامسأ قباطت نأ بجي) رصم لاسا لجس:
 - Cisco: cisco_umbrella_dns_log نم تاللس DNS
 - Cisco Umbrella IP: cisco_umbrella_ip_log تاللس
 - Cisco Umbrella: cisco_umbrella_proxy_log لىكوت تاللس
- تاللس قيسنت: Cisco Umbrella CSV
- لجس لاسا رصم عون: Cisco Umbrella
- لوكوت ووربل نىوكت: Amazon AWS S3 REST API
- فللمال جذومن: .*?\.csv\.gz
- دادت مال رصم لجس: Cisco Umbrella_ext **
- اهيف اوضع اذه لجس لاسا رصم نوكي نأ ديرت تاعومجم ي اديحت ااجرلا:
cisco_umbrella_logsource_group

دحاو لجس رصم ةفاضل لاسا لقتنا



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):

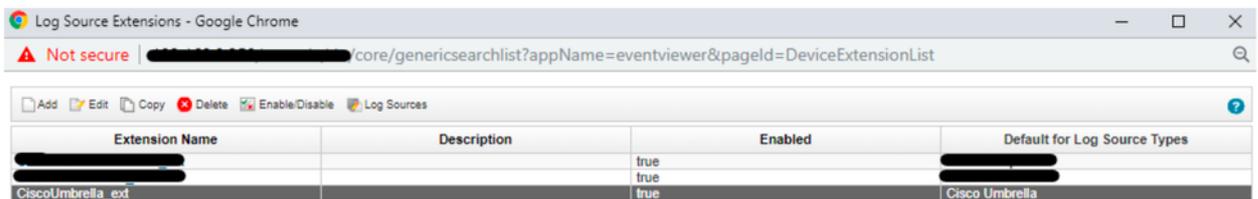
Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06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

[Step 4: Configure Protocol Parameters](#)

[Finish](#)

4404306881812

ءاچرلا ، "CiscoUmbrella_ext" ىلع "لجسلا ردصم قحلم" نبيعت متي مل اذ: ةظحالم
ةمئاقلا نم لجسلا ردصم مسا رايخ:



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: نم رادم ولد هيلع ودي ام يلع لاثم انه

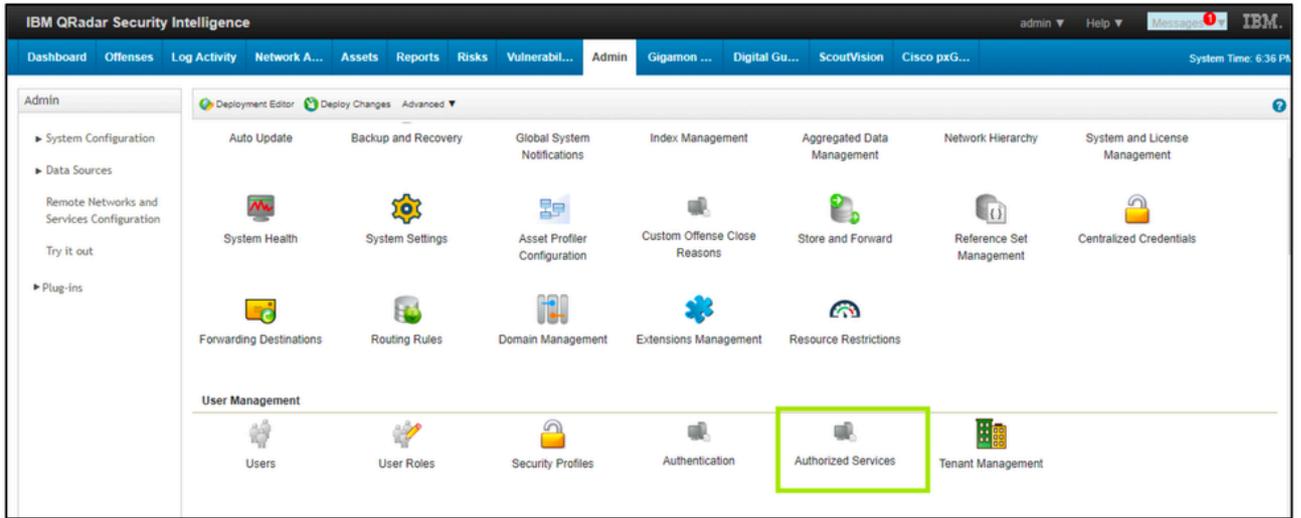
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

قحولل شي دحت لدعم نيي عتب مقو Cisco نم ةباحسل ناما قيبطت تادادع| يلإ ىرخأ ةرم لقتنا
ةينايلال تاموسرللا في تانايلال ضرعل "1" اهرادقم ىندا ةميقي يلإ تاعاسلاب

زي ممل ةقداصملا زمر عاشنإ

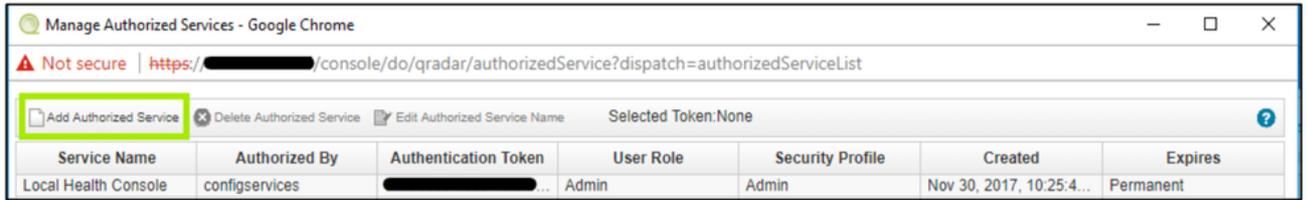
كب صاخلا Cisco ناما قيبطت يلإ هتفاضل ةمدخلل زيمم زمر عاشنإ يلإ لوؤسمللا جاتحي
اموي 90 لك دمتمملا زيمملا ةمدخلل زمر عاشنإ ةداعإ تم، ةسرامم لضفأك

1. ةدمتمملا تامدخل > "لوؤسمللا" بيوبتللا ةمالع > QRadar يلإ لوخدلا ليجست.



360071965571

2. قدمت عمل تامدخل اة فاضا .

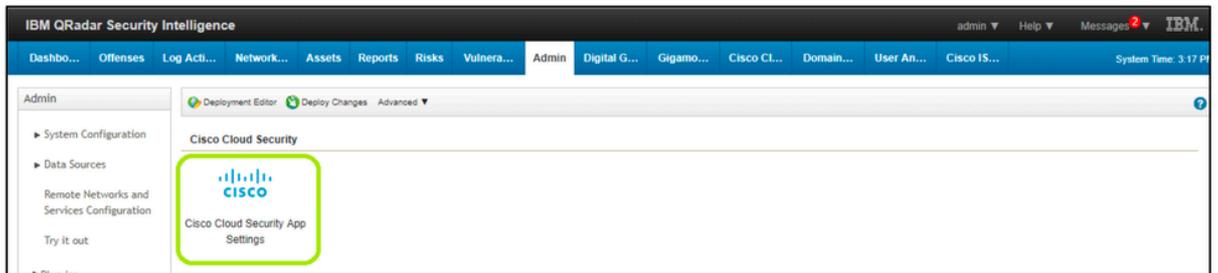


360071965551

3. زيمم اة قداصم زمر عاشن اب مقو لي صافات لا لخدأ .
4. "تاريغ تال رشن" قوف رقنا ، زيمم ل زمر ل عاشن ا دع ب .

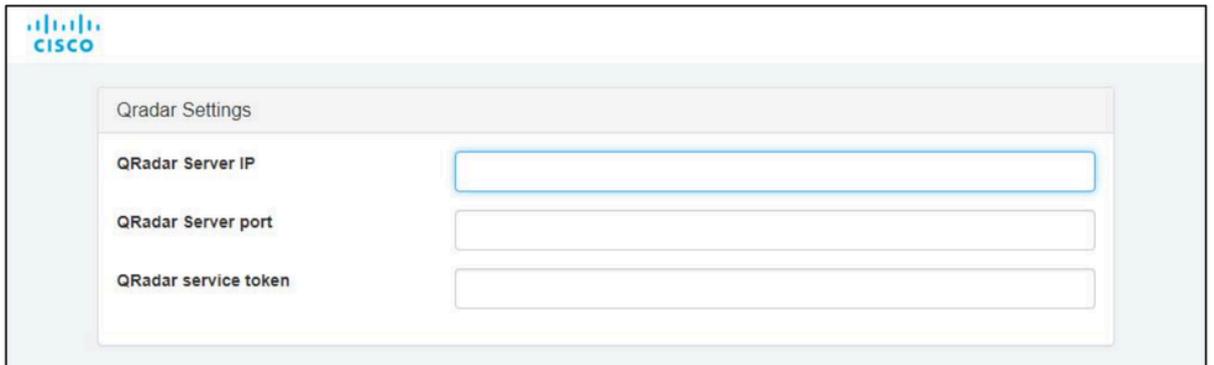
Cisco نم اة باحس ل نام ا ق ي ب ط ت ني و ك ت

1. لفس ا ل ا ريرم ت ل اب مق ، QRadar ل قنن ت ل ا طيرش ي ف Admin بي و ب ت ل ا ا م ال ع نم .
Cisco اة باحس نام ا ق ي ب ط ت ا ا د ا ع ا ح ت ف و .



360071754732

2. اة ق باس ل ا ا و ط خ ل ا ف ه و ا ش ن ا م ت ي ذ ل ا ز ي م م ل ا ا ق د ا ص م ل ا ز م ر ل خ د ا .



Qradar Settings

QRadar Server IP

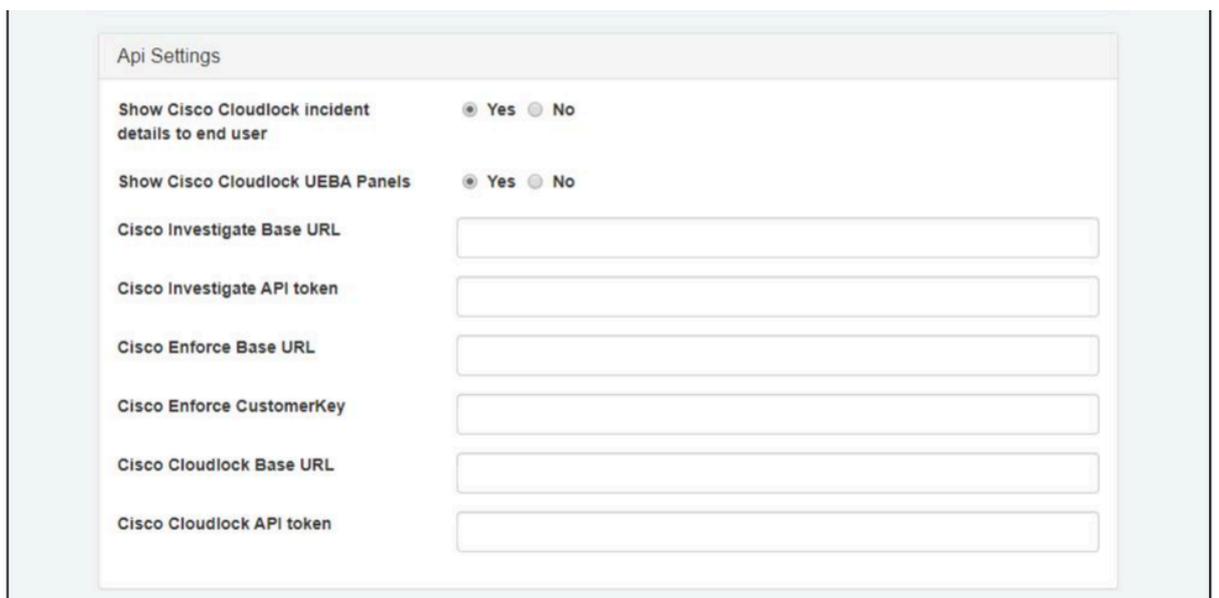
QRadar Server port

QRadar service token

360072462992

3. يلي امك API تادادع| رح :

- Cisco: <https://investigate.api.umbrella.com/> نم يساسأل URL ناو نع نم ققحت
- Umbrella تامولعمل ةحول لالخ نم عاشن| :زيمملا API زمر نم Cisco ققحت -> عجار ،تامولعمل نم ديزمل ؛ديج زيمم زمر عاشن| -> API حيتافم -> قيقحتلا <https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>
- Cisco: <https://s-platform.api.opendns.com/1.0/> نم يساسأل URL ناو نع صرف
- Umbrella تامولعمل ةحول لالخ نم عاشن| : Cisco نم ليمعلا حاتفم صرف -> عجار ،تامولعمل نم ديزمل ؛ةفاض| -> لمكتلا تايلمع -> جهنلا تانوكم <https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>
- Cisco: CloudLock ةدعاق ل URL ناو نع :
<https://api-demo.cloudlock.com/api/v2/> ،لاثملا ليبس يلع) <https://api-demo.cloudlock.com/api/v2/>. Cloudlock ةدعاق صاخلا URL ناو نع ديكأت عاجرلا .
ينورتكلل ديرب لاسرا قيرط نع URL API Enterprise Cloudlock مساب فورعمللا support@cloudlock.com لى
- Cisco Cloudlock: عاشن| : Cisco Cloudlock تاقيبطتلا ةجمرب ةهجاو زيمملا زمرلا نم ديزمل ؛عاشن| -> تاقيبطتلا ةجمرب ةهجاو ةقداصملا -> تادادع| -> عجار ،تامولعمل <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

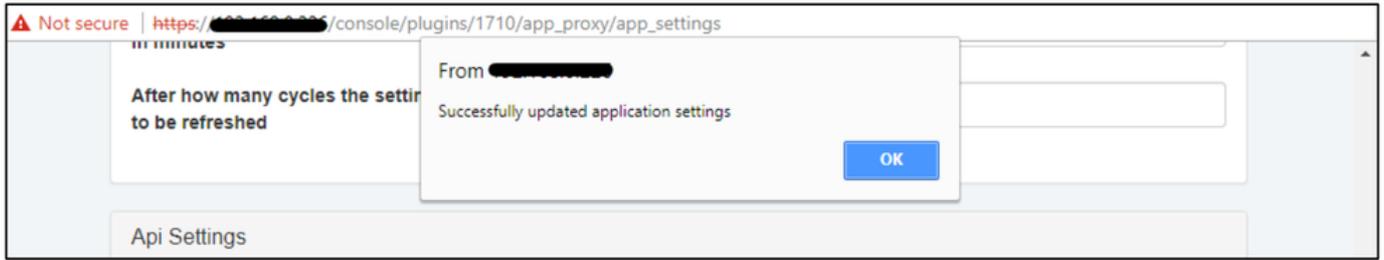
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

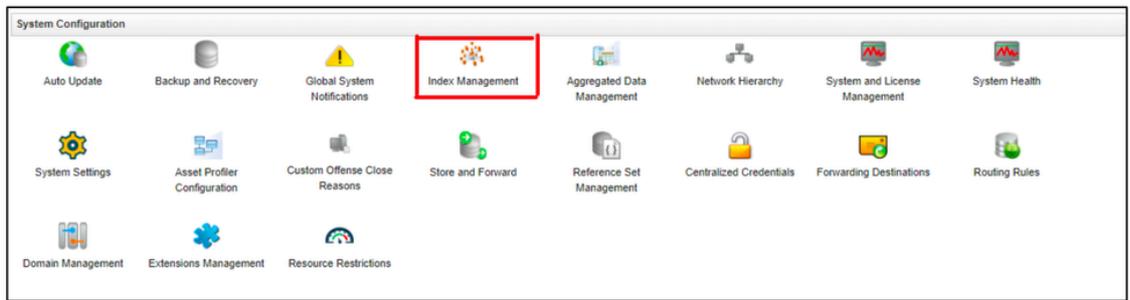
حاجن ب قيبطتال تاداعل شيحت مت هنا إلى عقث بنم الم عمئاق ل ريشت



360071986151

QRadar في سرهف ل

1. سرهف ل ةراد إ قوف رقنا م، Admin بيوبتال عمال ع إلى لقتنا 1.



360071780112

2. قيبطتال عم CEPs Packaged سرهف 2.

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)	12.68%	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

اهت سرهف بجي يتل اهب ي صوم ل CEP تادحو يه هذه

1. لجسلا ردصم
2. DNS ةئف
3. ثدحلا عون
4. لاجملا ل URL ناونع
5. تايوهلا
6. تايوتسملا ددعت ممدختسم
7. Username
8. عقوملا لصأ فرعم
9. ثدحلا ةئف
10. ةسايسلا
11. دروم

Cisco Umbrella، و Investigate، لېصافت ةبقارم ةطشنأ ءدبل QRadar مادختسال زهاج تنأ نآلا
ان: QRadar ربع لقننتلا ةيفيك لوح تاداشرالا نم ديزم ىلع روثعل كنكمي. CloudLock و
Cisco. نم ةباحسلا نامأ قيبطت ربع لقننتلا

