Configure the Cloud Security App for IBM QRadar

Contents

Introduction

This document describes how to configure the Cisco Cloud Security app with IBM QRadar for log analysis.

Overview

QRadar from IBM is a popular SIEM for log analysis. It provides a powerful interface for analyzing large chunks of data, such as the logs provided by Cisco Umbrella for your organization's DNS traffic. The Cisco Cloud Security App for IBM QRadar provide insight from multiple security products (Investigate, Enforcement, and CloudLock) and integrates them with QRadar. It also helps the user to automate security and contain threats faster and directly from QRadar.

When you set up Cisco Cloud Security app for QRadar, it integrates all the data from Cisco Cloud Security platform and allows you to view the data in graphical form in the QRadar console. From the application, analysts can:

- Investigate domains, ip addresses, email addresses
- Block and Unblock domains (enforcement)
- View the information of all the incidents of the network.

This article outlines the basic how-to of getting QRadar set up and running so that it is able to pull the logs from your S3 bucket and consume them.

Requirements

Note: Support for QRadar must come from IBM, as Cisco is unable to directly support third-party hardware or software. For any issues connecting your Umbrella dashboard to your S3 bucket, we can provide support. Much of the information found here can also be found on the IBM website: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umbrella_o

Cisco Umbrella requirements

This document assumes that your Amazon AWS S3 bucket has been configured in Umbrella (Settings > Log Management) and is showing green with recent logs having been uploaded.

For more information on how to configure this feature, read here: Manage Your Logs.

IBM Security QRadar SIEM requirements

The administrator is required to have administrative rights to the QRadar appliance(s), the Amazon S3 configuration and Umbrella dashboard, these instructions assume that the QRadar administrator is familiar with creating LSX (Log source Extension) files.

Please be aware that the Cisco Cloud Security App v1.0.3 only works up to IBM QRadar 7.2.8. The new version, v1.0.6, works with the current QRadar version from 7.4.2 and later.

Installing Cisco Cloud Security App for IBM QRadar

1. Download and install the Cisco Cloud Security App for IBM QRadar found here: Cisco Cloud Security App v1.0.3 (for IBM QRadar v7.2.8) or Cisco Cloud Security App v1.0.6 (for IBM QRadar v7.4.8).
2. After the installation, deploy changes in QRadar.

Cisco Cloud Security App Configuration: Adding Log Source

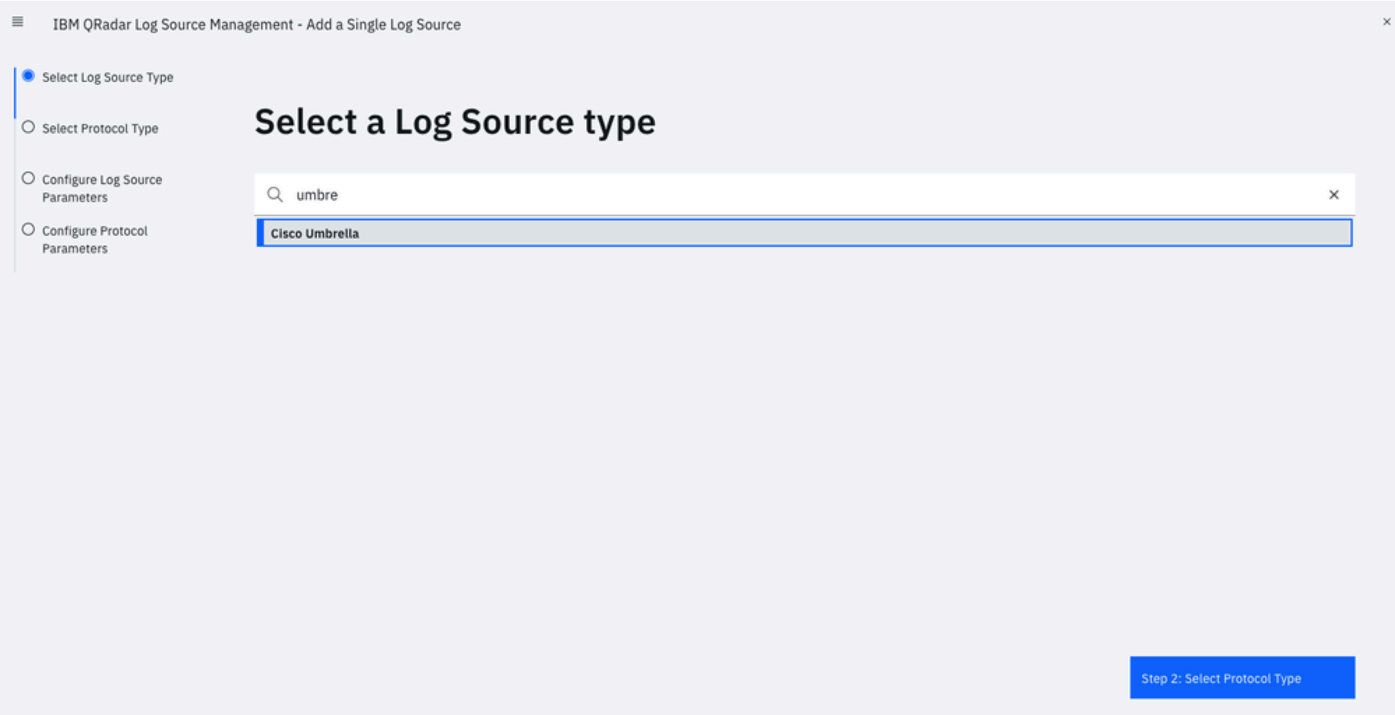
Note: You can see other logs in S3 such as Audit and Firewall, but they are not supported. Only set up the three listed here. Any attempts to configure those other logs results in failure.

To add a log source, click on the **Admin** tab on the QRadar navigation bar, scroll down and click on **QRadar Log Source Management**, then click the button **+New Log Source:**

- **Log Source Name *(entry names must match exactly as listed)*:**

    - Cisco DNS Logs: cisco_umbrella_dns_logs
    - Cisco Umbrella IP Logs: cisco_umbrella_ip_logs
    - Cisco Umbrella Proxy Logs: cisco_umbrella_proxy_logs
- **Event Format:** Cisco Umbrella CSV
- **Log Source Type:** Cisco Umbrella
- **Protocol Configuration:** Amazon AWS S3 REST API
- **File Pattern:** .*?\.csv\.gz
- **Log Source Extension:** CiscoUmbrella_ext **
- **Please select any groups you would like this log source to be a member of:** cisco_umbrella_logsource_group

Go through the Add a Single Log Source Wizard:

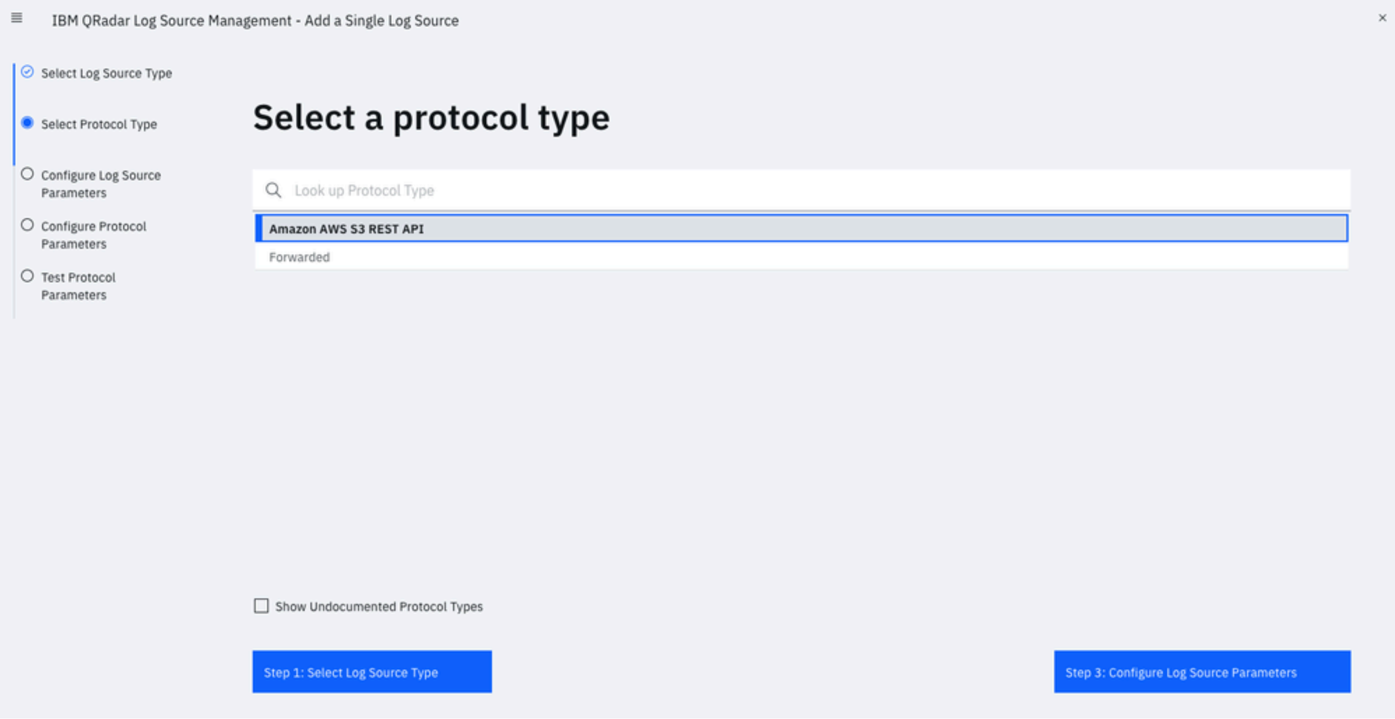

IBM QRadar Log Source Management - Add a Single Log Source
● Select Log Source Type
○ Select Protocol Type
○ Configure Log Source Parameters
○ Configure Protocol Parameters
Step 2: Select Protocol Type

Select a Log Source type

umbre

Cisco Umbrella

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
Step 1: Select Log Source Type
Step 3: Configure Log Source Parameters

Select a protocol type

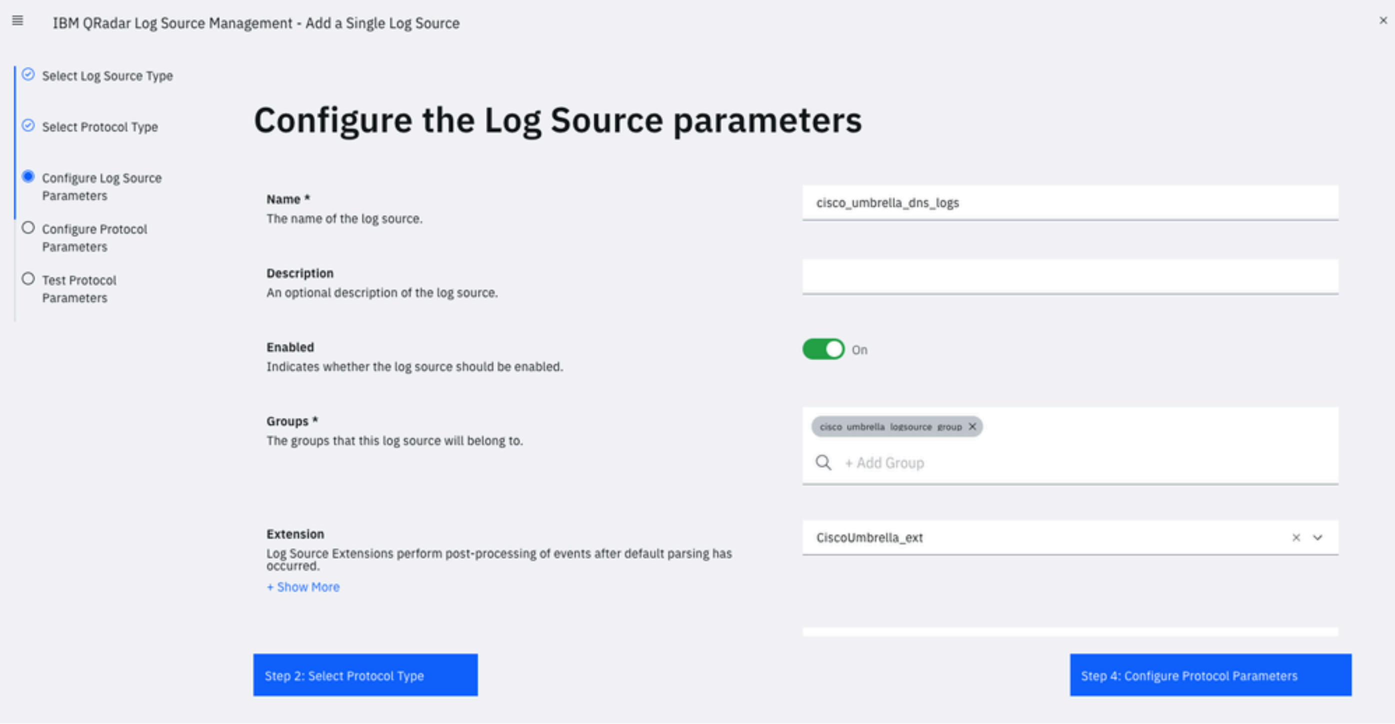
Look up Protocol Type

Amazon AWS S3 REST API

Forwarded

□ Show Undocumented Protocol Types

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
+ Show More
Step 2: Select Protocol Type
Step 4: Configure Protocol Parameters

Configure the Log Source parameters

Name *
The name of the log source.
cisco_umbrella_dns_logs

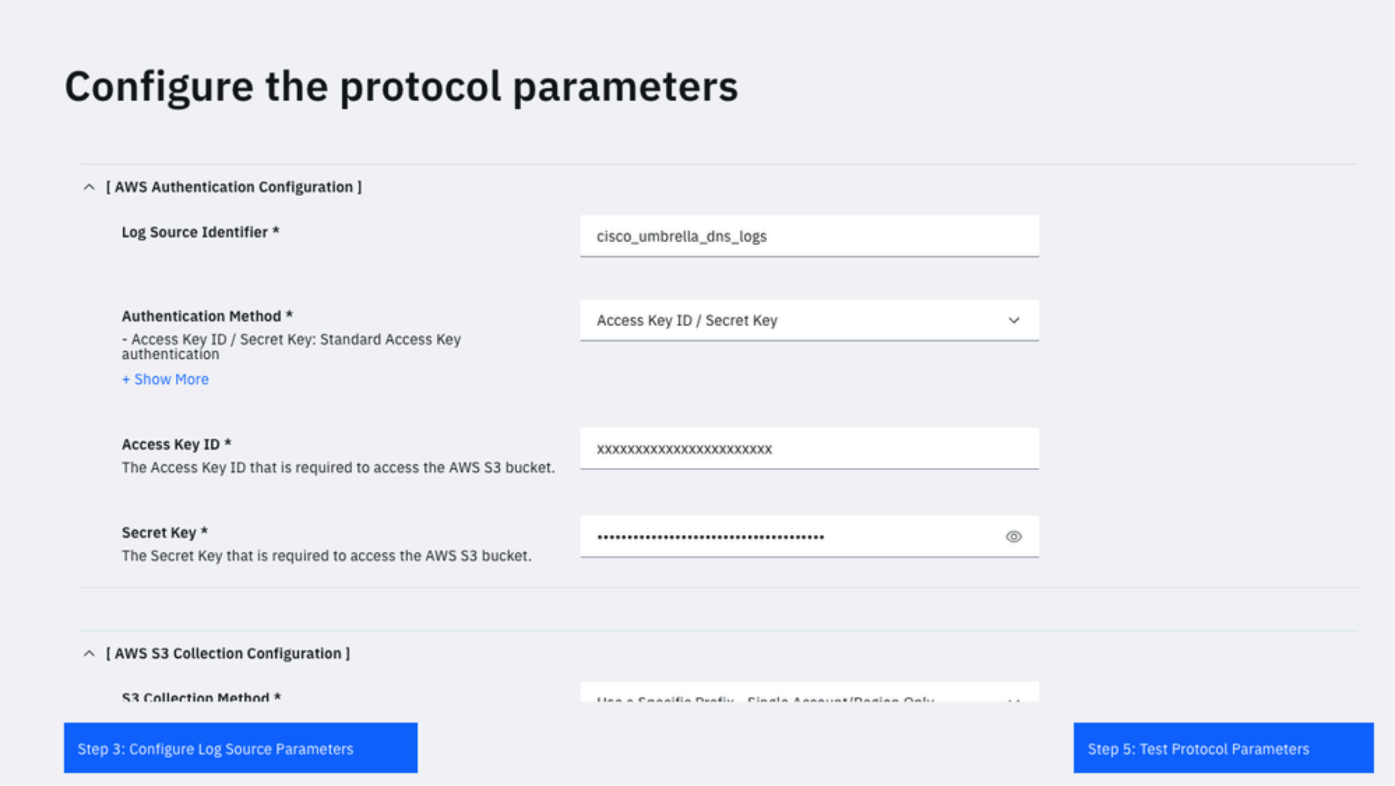
Description
An optional description of the log source.

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.
CiscoUmbrella_ext

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.

xxxxxxxxxxxxxxxxxxxxxxx

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

•••••••••••••••••••••••••••••••••••••

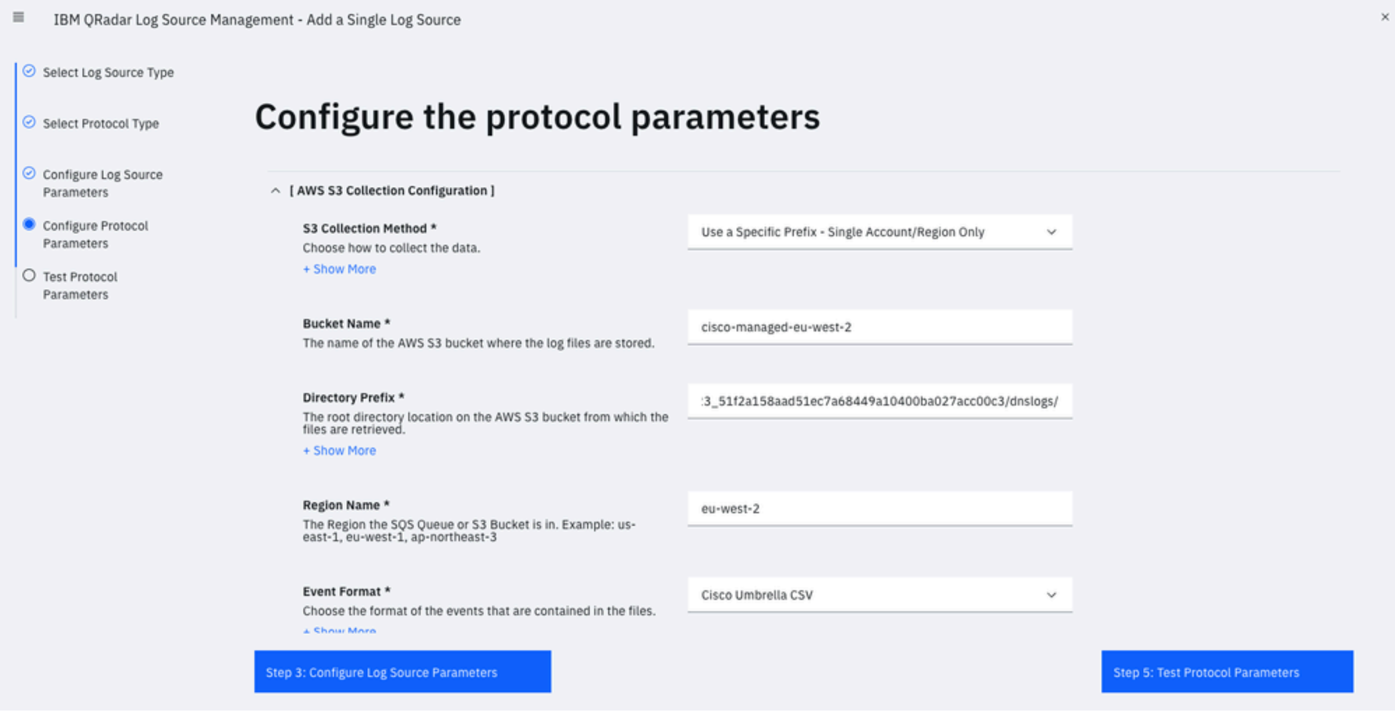
^ [AWS S3 Collection Configuration]

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

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

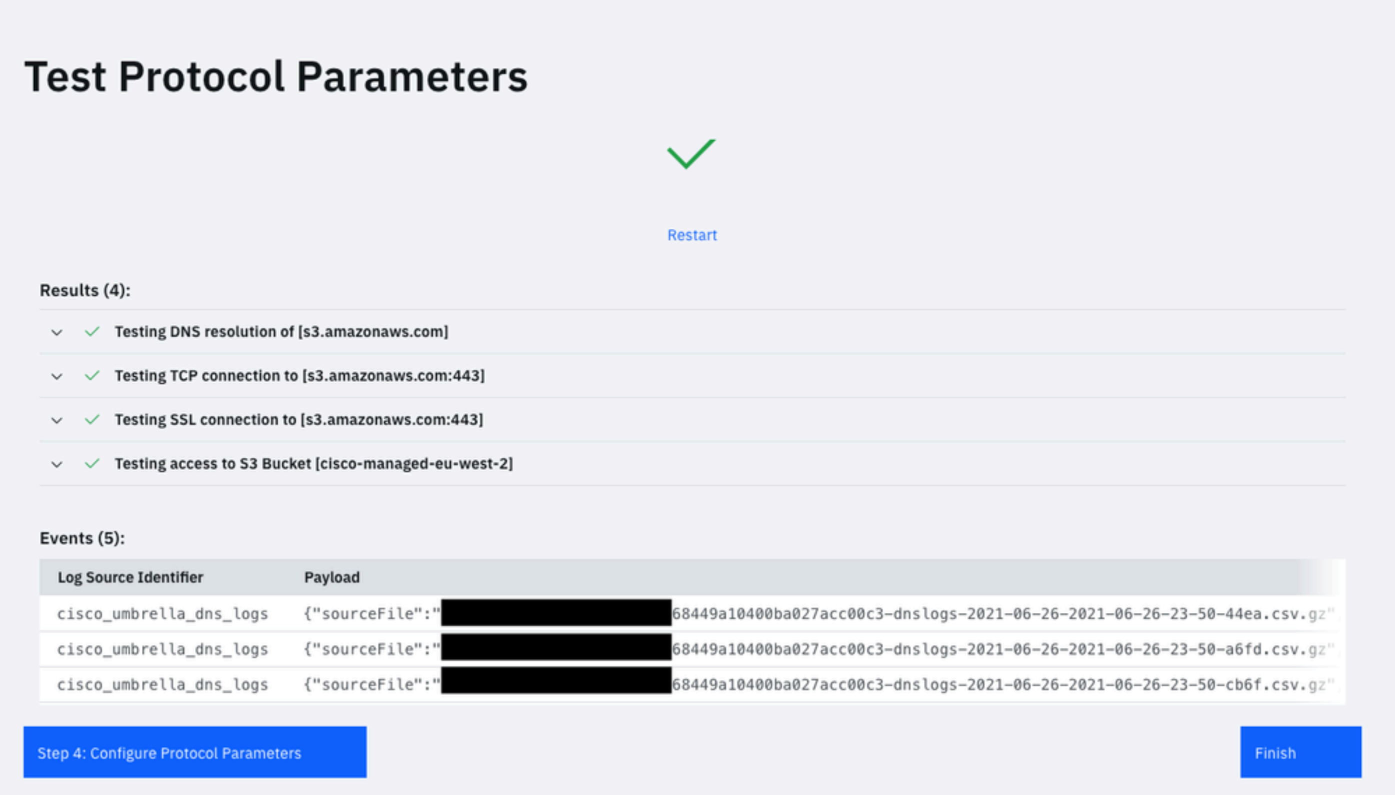
eu-west-2

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

Results (4):

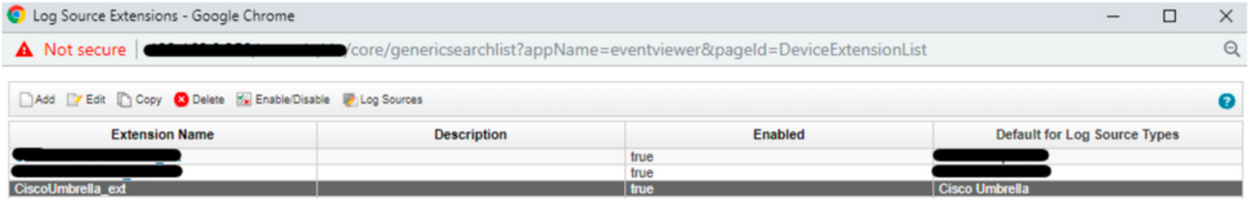
- ✓ Testing DNS resolution of [s3.amazonaws.com]
- ✓ Testing TCP connection to [s3.amazonaws.com:443]
- ✓ Testing SSL connection to [s3.amazonaws.com:443]
- ✓ Testing access to S3 Bucket [cisco-managed-eu-west-2]

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"

4404306881812

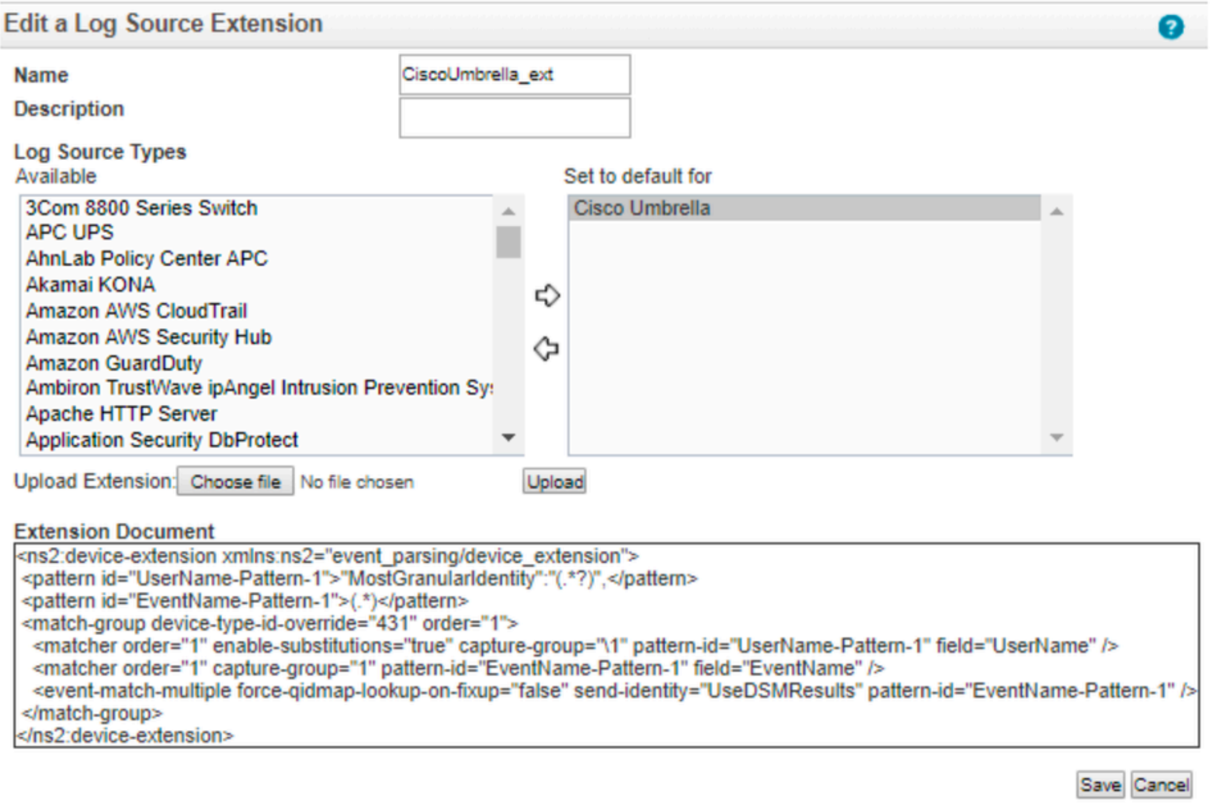
Note: If the Log Source Extension is not mapped to "CiscoUmbrella_ext", please choose the Log Source Name from the list:



[redacted]/core/genericsearchlist?appName=eventviewer&pageId=DeviceExtensionList

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

360071157752



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
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

Here is an example of what a Cisco Managed Bucket looks like:

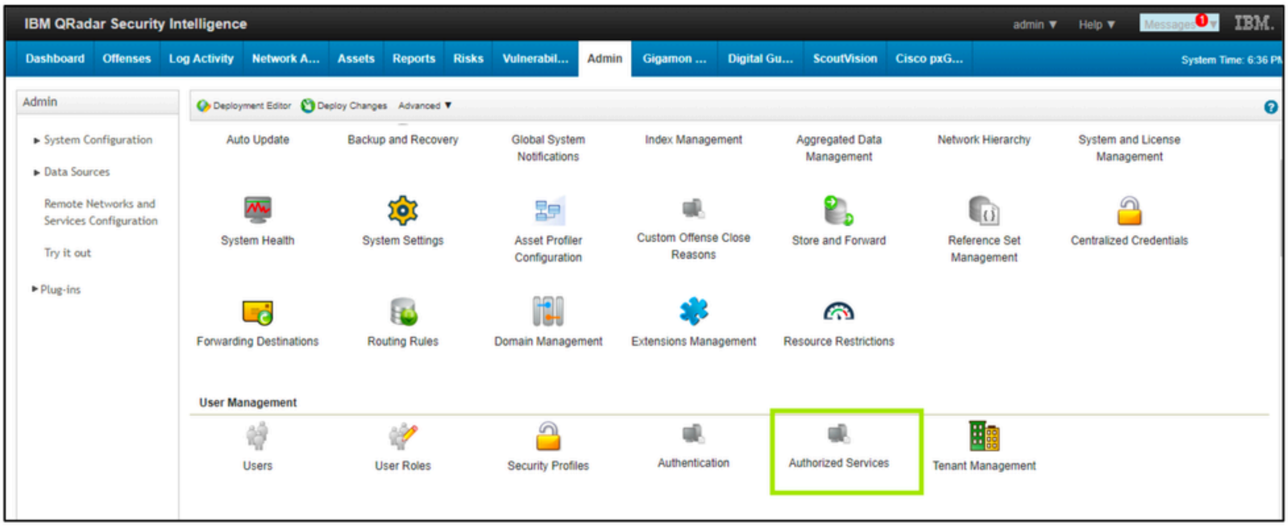
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs
```

Navigate back to **Cisco Cloud Security App Settings** and set the **Panel refresh rate in hours** to a minimum value of "1" in order for the graphs to display data.

Generating Authentication Token

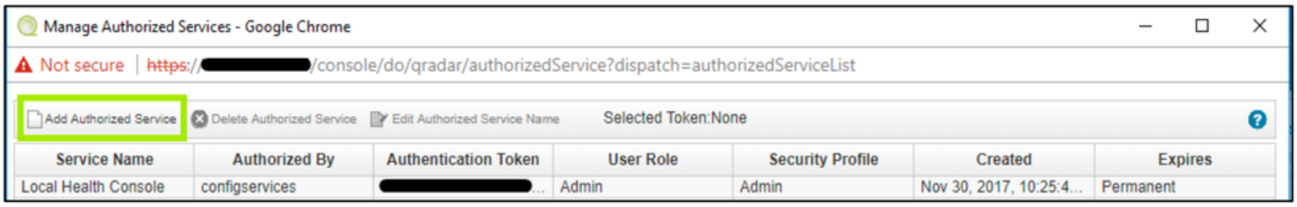
The administrator needs to generate a service token to add to your Cisco Security App. As best practice, recreated the Authorized Service Token every 90 days:

1. Login to **QRadar** > **Admin Tab** > **Authorized Services**.



360071965571

2. Add Authorized Services.


Manage Authorized Services - Google Chrome
Not secure
Add Authorized Service
Delete Authorized Service
Edit Authorized Service Name

https://[redacted]/console/do/qradar/authorizedService?dispatch=authorizedServiceList

Selected Token:None

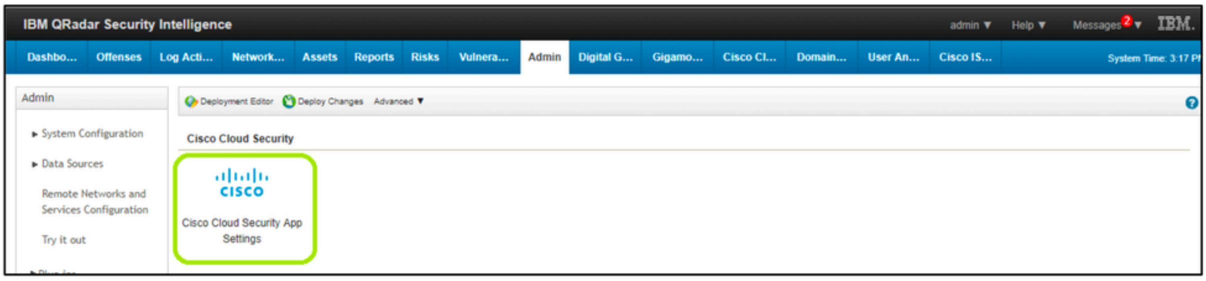
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
Local Health Console	configservices	[redacted]...	Admin	Admin	Nov 30, 2017, 10:25:4...	Permanent

360071965551

3. Enter the details and generate authentication token.
4. After generating the token, click "Deploy Changes".

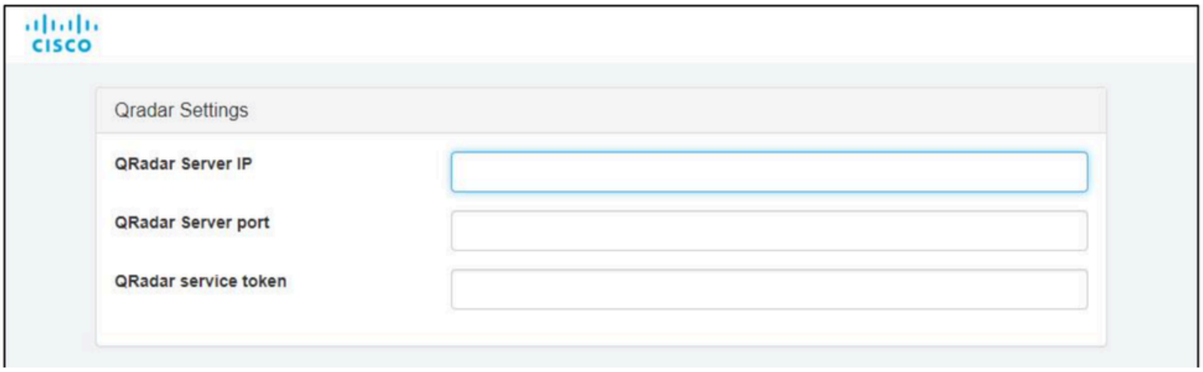
Configuring the Cisco Cloud Security App

1. From the **Admin** tab on the QRadar navigation bar, scroll down and open **Cisco Cloud Security App Settings**.



360071754732

2. Enter the Authentication Token generated in previous step.

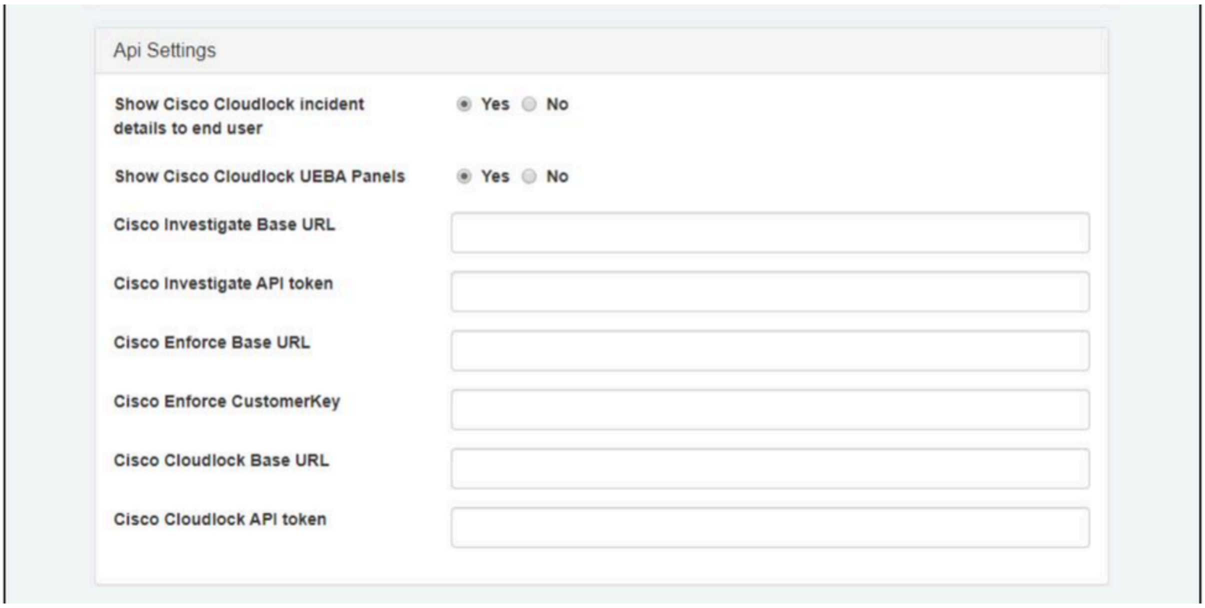


Qradar Settings

QRadar Server IP	
QRadar Server port	
QRadar service token	

360072462992

3. Edit the **Api Settings** as follows:
   - Cisco Investigate Base URL: https://investigate.api.umbrella.com/
   - Cisco Investigate API token: generate via the Umbrella dashboard -> Investigate -> API Keys -> Create New Token; for more information see 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: generate via the Umbrella dashboard -> Policy Components -> Integrations -> Add; for more information see https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
   - Cisco Cloudlock Base URL: https://{YourCloudlockAPIServer}/api/v2 (for example, https://api-demo.cloudlock.com/api/v2/. **Please confirm your Cloudlock Base URL aka Cloudlock Enterprise API URL by sending an email to support@cloudlock.com**.)
   - Cisco Cloudlock API token: generate via Cloudlock -> Settings -> Authentication & API -> Generate; for more information see https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication

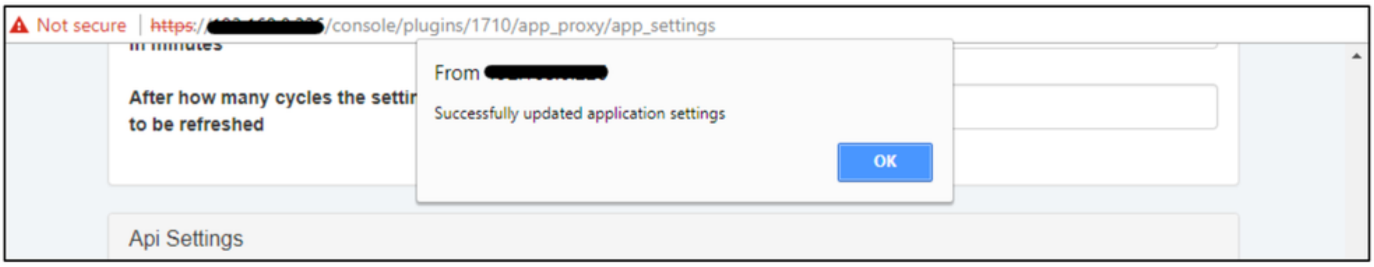


Api Settings

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

A popup indicates that the application settings have been successfully updated.



Not secure | https://[redacted]/console/plugins/1710/app_proxy/app_settings

in minutes

After how many cycles the settir
to be refreshed

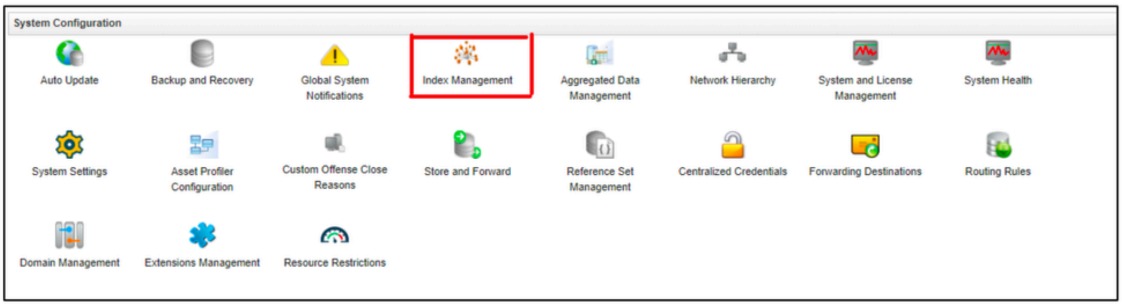
From [redacted]

Successfully updated application settings

360071986151

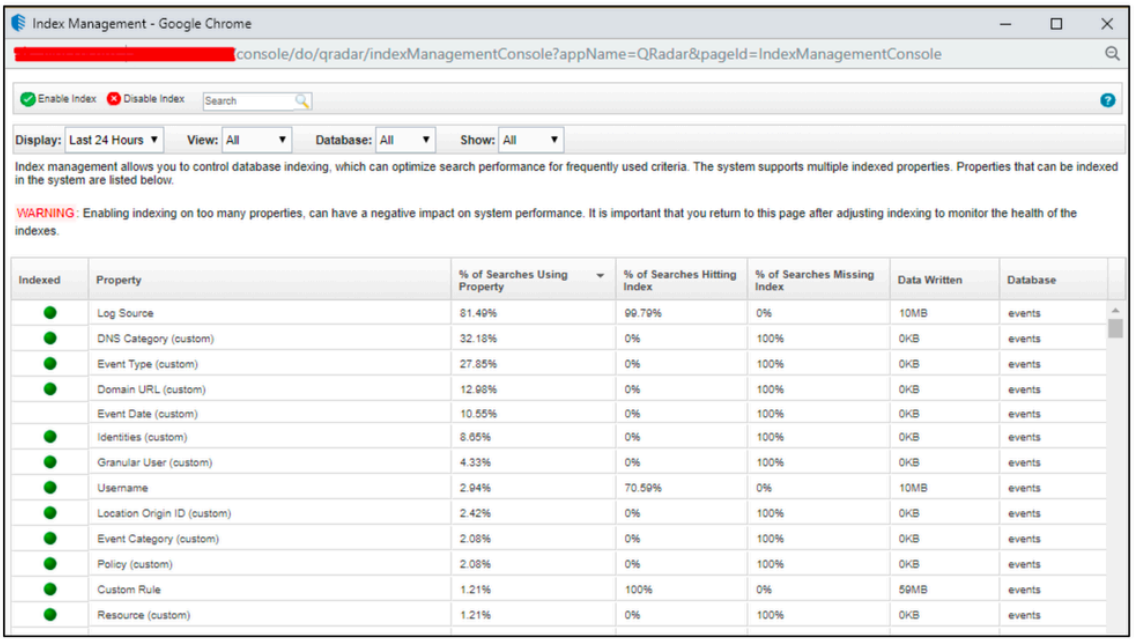
Indexing in QRadar

1. Navigate to the **Admin** tab, then click on **Index Management**.



360071780112

2. Index the CEPs Packaged with the app.



[redacted]console/do/qradar/indexManagementConsole?appName=QRadar&pageId=IndexManagementConsole

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)	8.65%	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

These are the recommended CEPs to be indexed:

1. Log Source
2. DNS Category
3. Event Type
4. Domain URL

5. Identities
6. Granular User
7. Username
8. Location Origin ID
9. Event Category
10. Policy
11. Resource

Now you are ready to use QRadar to start monitoring activities for Cisco Umbrella, Investigate, and CloudLock details. More instructions on how to navigate QRadar can be found here: Navigating the Cisco Cloud Security App.