



Cisco Cloud Security App for Splunk

Version Number: 1.0.13

Date: May 26, 2021

Copyright © 2021 Cisco

Contents

Table of Contents

Contents.....	2
1. Introduction	3
1.1. Overview	3
1.2. About this Document.....	3
1.3. About the app	3
1.4. Prerequisites	3
2. General.....	3
2.1. Installation	3
2.2. Role Based Access Control	4
2.3. Configuration.....	5
3. Cisco Cloud Security App Usage.....	12
1.1. General	12
1.2. Time Range Selector.....	12
1.3. Investigate Tab	13
1.4. CASB Tab	13
1.5. Cloud Security Tab	15
1.6. Umbrella Tab.....	16
4. Configuring Custom Alerts in Splunk.....	22
Block Destinations.....	22
Investigate the Destinations	22
5. Cisco Cloud Security App and Add-on Distributed Deployment	23
6. Troubleshooting	24
· Cisco Umbrella DNS Logs.....	24
· Cisco Umbrella Proxy Logs.....	24
· Cisco Umbrella Firewall Logs.....	24

1. Introduction

1.1. Overview

The Cisco Cloud Security App for Splunk provides insights and capabilities from multiple Cisco Cloud Security products, (Umbrella, Investigate, and Cloudlock), and integrates them with Splunk. The Cisco Cloud Security platform helps the user automate security and contain threats directly from Splunk.

1.2. About this Document

This document explains how to deploy and use the Cisco Cloud Security App for Splunk.

1.3. About the app

Splunk provides a robust platform for Security Information and Event Management, (SIEM), anomaly detection, incident forensics, and vulnerability management.

When you set up the Cisco Cloud Security app for Splunk, you can get data from the Cisco Cloud Security platform, view it in graphic form and interact with it in the Splunk console. From the application, you can:

- Investigate destinations such as domains, URLs and IP addresses.
- Block and unblock destinations (Destination List).
- View detailed CASB incident information (Cisco Cloudlock).
- View graphical representations of Umbrella data.

1.4. Prerequisites

- Splunk version 8.0.1 and above.
- Access to Cisco Cloud security products.
- Splunk administration privileges.

2. General

2.1. Installation

- Navigate to Splunkbase <https://splunkbase.splunk.com/>
- Search for ‘Cisco Cloud Security’
- Download and install the Cisco Cloud Security App and Cisco Cloud Security Add-on.

- Restart your Splunk server when prompted to (a restart is required after each is installed).
 - NOTE: Install the Add-on to fetch Cisco Umbrella data from AWS S3 buckets. You can skip this installation if you do not use Cisco Umbrella.

2.2. Role Based Access Control

When the app is installed, 3 roles are created:

- cs_admin:
Can update and edit the settings page. In the CASB tab, this user can update an incident's status and severity.
- cs_supervisor:
Cannot view the application settings page. In the CASB tab, this user can update the incident status and severity.
- cs_user:
Can only view the dashboards. cs_user does not have access to the app settings page and cannot modify data, update data, or retrieve data, or perform any right-click actions such as enrich/block.

2.3. Configuration

2.3.1. Accept the terms and condition

1. Read and accept the terms and conditions.

The screenshot shows the Splunk interface with the title "Application Settings". Below the title is a detailed text of the Splunk End User License Agreement. At the bottom of the text is a checkbox labeled "I have read the terms and conditions of the Agreement and agree to be bound by them." To the right of the checkbox is a green "Submit" button.

2. Click Submit.

2.3.2. Configure the Umbrella Add-on Settings

The screenshot shows the Splunk interface with the title "Cisco Cloud Security Umbrella Addon". Under the "Inputs" tab, there is a table listing three inputs. The columns are "Name", "Interval", "Index", "Status", and "Actions". The inputs are: Aujas_Dns (Interval 60, Index umbrella, Enabled), Aujas_firewall (Interval 120, Index umbrella, Enabled), and Aujas_proxy (Interval 100, Index umbrella, Enabled). There is also a "Create New Input" button at the top right of the input list.

1. Click **Create New Input**.
2. In the dialog that opens, enter the AWS S3 settings:

The screenshot shows a modal dialog titled "Add Cisco Cloud Security Umbrella Addon". The form contains the following fields:

- Name*: A text input field with placeholder "Enter a unique name for the data input".
- Interval*: A text input field with placeholder "Time interval of input in seconds".
- Index*: A dropdown menu set to "default".
- AWS Region*: A dropdown menu with "AWS Region" selected.
- AWS Access Key Id*: A text input field with placeholder "AWS Access Key Id".
- AWS Secret Access Key*: A text input field with placeholder "AWS Secret Access Key".
- AWS S3 Bucket Name*: A text input field with placeholder "AWS S3 Bucket Name".
- AWS S3 Directory Prefix*: A text input field with placeholder "AWS S3 Directory Prefix".
- Default Start Date*: A text input field with placeholder "Default Start Date (YYYY-MM-DD)".
- Event Type*: A dropdown menu set to "dns".

At the bottom of the dialog are "Cancel" and "Add" buttons.

3. Enter a name (arbitrary) for this data input.
4. Provide an interval (in seconds) at which events should be fetched to the indexer. We recommend 600 seconds.
5. Choose the index to store the Umbrella logs.
6. Enter your AWS S3 region (for example, **us-west-1**).
7. Enter your AWS Access Key Id.
8. Enter your AWS Secret Access Key.
9. Enter your AWS S3 Bucket Name.
10. : Enter AWS S3 Directory Prefix and append it with “/”. For example, for logs from a Cisco Managed Bucket:

Log Type	Example
DNS logs	2506xxx_2db1xxxx1ddf7cxx18652xxxxfdab7xxxxd60xx/dnslogs/
Proxy logs	2506xxx_2db1xxxx1ddf7cxx18652xxxxfdab7xxxxd60xx/proxylogs/
Firewall logs	2506xxx_2db1xxxx1ddf7cxx18652xxxxfdab7xxxxd60xx/firewalllogs/

11. Enter the date from which you need data to be pulled into your Splunk app in the format YYYY-MM-DD. We highly recommend not requesting more than one week due to the backlog this may create.
12. Select the corresponding event type (for example, DNS, Proxy, or Firewall).

2.3.3. Configuring the Cisco Cloud Security Application using the Application Settings page

In the Application Settings you can:

- Select which indexes your Umbrella logs are being sent to. This would have been defined when you configured the Add-on, (1.3.2). By matching up the index names, you will enable the Umbrella dashboards in the app.
- Configure Investigate, CASB and Destination List Settings.
- View the History of the configured settings.
- View the Health status of the APIs.

Application Settings

[View History](#) [Show Health Status](#)

Dashboard Settings

*Default Search Interval Panel Refresh Rate

Investigate Settings

*URL *Token *Investigate

CASB Settings

*Config Name *URL *Token

Retrieve event/entity raw data Yes No

Show Cisco CASB Incident UEBA panels Yes No

Start Date *Index

Destination List Settings

*URL *Token *Organization ID

Blocked Destination List (Admin and CS Admin)

Blocked Destination List (CS Supervisor)

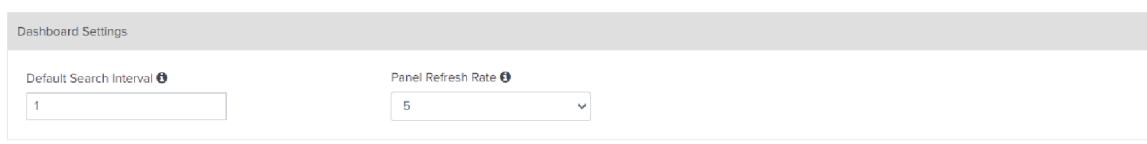
Umbrella Settings

DNS <input type="button" value="Select index for DNS"/>	PROXY <input type="button" value="Select index for Proxy"/>	IP <input type="button" value="Select index for IP"/>
FIREWALL <input type="button" value="Select index for Firewall"/>		

[Clear](#) [Save](#)

The Application Settings page enables you to configure the following settings:

A. Dashboard Settings

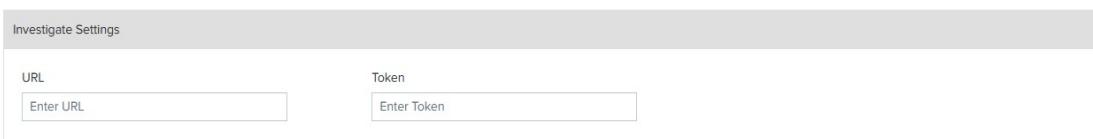


Dashboard Settings

Default Search Interval Panel Refresh Rate

- Select the default search interval and Panel refresh rate.

B. Investigate API settings:



Investigate Settings

URL Token

- Enter the following URL: <https://investigate.api.umbrella.com/>
- Enter an Investigate API Token generated from the [Umbrella dashboard](#).

C. CASB (Cloudlock) settings:



CASB Settings

Config Name URL Token

Retrieve event/entity raw data Yes No

Show Cisco CASB incident UEBA panels Yes No

Start Date

- Config Name is an arbitrary name you choose.
- Please obtain your URL from support@cloudlock.com. The format will be something like this:
<https://YourEnvironmentsAddress.cloudlock.com/api/v2> (for example
<https://api-app.cloudlock.com/api/v2>).
- You can generate you API Token from the [Cloudlock console](#).
- Choose **Retrieve event/entity raw data** to view raw event details for your incidents.
- Choose **Show Cisco CASB incident UEBA panels** to view the UEBA panels.
- When **Start Date** is blank, incidents are fetched from the previous 7 days. You can enter a preferred start date, but we highly recommend that this not be set to a date that is older than one month as this can involve bringing back large amounts of data.

D. Destination List settings

>, <,>>, <<)."/>

The screenshot shows the 'Destination List Settings' page. At the top, there are three input fields: 'URL' (containing 'example.com'), 'Token' (labeled 'Enter Token'), and 'Organization ID' (labeled 'Enter organization ID'). Below these fields is a blue button labeled 'Fetch'. Underneath the 'Fetch' button are two sections, each titled with its role: 'Blocked Destination List (Admin and CS Admin)' and 'Blocked Destination List (CS Supervisor)'. Each section contains a list view with four circular navigation buttons on the left: '>>', '>', '<', and '<<'.

- Enter the following URL:
<https://management.api.umbrella.com/v1/organizations>
- Enter a Management API Token generated from the Umbrella dashboard. The token is obtained by first generating the Management API key and secret in the Umbrella dashboard, and then running the following command:
`echo "key:secret" | openssl base64 -A`
The generated string should be entered in the Token field.
- Enter your [Organization ID](#).
- Click **Fetch**.
- The available Destination Lists are displayed. Select the Destination Lists to be available to your users based on their Splunk roles.

E. Umbrella Settings

Select the appropriate index for each Umbrella sourcetype (as defined when adding the Add-On inputs). This connects the inputs to the dashboards:

The screenshot shows the 'Umbrella Settings' page. It features four dropdown menus for selecting indices: 'DNS' (labeled 'Select index for DNS'), 'PROXY' (labeled 'Select index for Proxy'), 'IP' (labeled 'Select index for IP'), and 'FIREWALL' (labeled 'Select index for Firewall'). At the bottom right of the page are two buttons: 'Clear' and 'Save'.

Application Settings History

Click **View History** to see previously configured details:

The screenshot shows the 'Application Settings History' interface with three main sections:

- Investigate Settings:** Shows a table with columns: User Name, Created Date, URL, Token, Status, and Action. One entry is shown: admin, 2020/09/07 16:50:50, URL [REDACTED], Token [REDACTED], active, Deactivate.
- CASB Settings:** Shows a table with columns: User Name, Created Date, Config Name, URL, Token, Incident, UEBA, Status, and Action. One entry is shown: admin, 2020/09/07 16:50:50, casb, URL [REDACTED], Token [REDACTED], Yes, Yes, active, Deactivate.
- Destination Lists Settings:** Shows a table with columns: User Name, Created Date, URL, Token, Status, Organisation Id, and Action. Three entries are shown:
 - admin, 2020/09/08 12:57:03, URL [REDACTED], Token [REDACTED], inactive, 2387558, Activate
 - admin, 2020/09/08 12:58:11, URL [REDACTED], Token [REDACTED], active, 2387558, Deactivate
 - admin, 2020/09/07 16:50:36, URL [REDACTED], Token [REDACTED], inactive, 2387558, Activate

Pagination controls are at the bottom of each section.

Health Status

Click **Health Status** to see your configurable API health check results:

The screenshot shows the 'Health Status' interface under the 'Application Settings' tab, specifically the 'Investigate Settings' section. The table has the following columns: User, Investigate URL, Response Time, Last Invocation Date, and URL Status.

User	Investigate URL	Response Time	Last Invocation Date	URL Status
nobody	https://investigate.api.umbrella.com	1.792	2020-09-09 15:19:49.459000	200
nobody	https://investigate.api.umbrella.com	1.409	2020-09-09 15:09:48.849000	200
nobody	https://investigate.api.umbrella.com	1.831	2020-09-09 14:59:49.403000	200
nobody	https://investigate.api.umbrella.com	1.358	2020-09-09 14:49:48.740000	200
nobody	https://investigate.api.umbrella.com	1.688	2020-09-09 14:39:49.248000	200
nobody	https://investigate.api.umbrella.com	1.801	2020-09-09 14:29:49.295000	200
nobody	https://investigate.api.umbrella.com	1.712	2020-09-09 14:19:49.371000	200
nobody	https://investigate.api.umbrella.com	1.951	2020-09-09 14:09:51.166000	200
nobody	https://investigate.api.umbrella.com	1.856	2020-09-09 14:03:58.958000	200
nobody	https://investigate.api.umbrella.com	1.796	2020-09-09 13:53:58.952000	200

Pagination controls are at the bottom of the table.

CASB Settings					
User	CASB URL	Response Time	Last Invocation Date	URL Status	
nobody	https://api-app.cloudlock.com/api/v2	3.151	2020-09-09 15:19:49.629000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.796	2020-09-09 15:09:48.193000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.288	2020-09-09 14:59:47.981000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.379	2020-09-09 14:49:47.790000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.261	2020-09-09 14:39:47.608000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.369	2020-09-09 14:29:47.728000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.255	2020-09-09 14:19:47.786000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.575	2020-09-09 14:09:49.291000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.301	2020-09-09 14:03:57.672000	403	
nobody	https://api-app.cloudlock.com/api/v2	1.534	2020-09-09 13:53:57.929000	403	

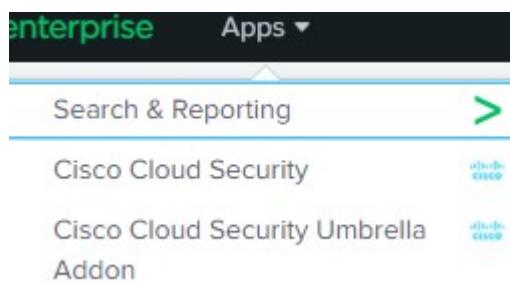
Showing 1 to 10 of 86 entries

Previous 1 2 3 4 5 ... 9 Next

Destination Lists Settings					
User	Destination List URL	Response Time	Last Invocation Date	URL Status	
nobody	https://management.api.umbrella.com/v1/organizations	2.303	2020-09-09 15:19:49.290000	200	
nobody	https://management.api.umbrella.com/v1/organizations	2.206	2020-09-09 15:09:49.131000	200	
nobody	https://management.api.umbrella.com/v1/organizations	2.22	2020-09-09 14:59:49.461000	200	
nobody	https://management.api.umbrella.com/v1/organizations	2.226	2020-09-09 14:49:49.198000	200	

3. Cisco Cloud Security App Usage

1.1. General



When the Cisco Cloud Security App and Cisco Cloud Security Add-on are successful installed, you can list the App and Add-on under the installed App menu.

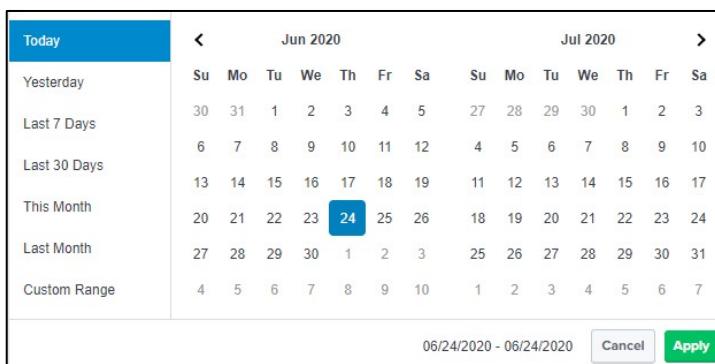


Open the Cisco Cloud Security App. You see the following tabs:

1. Search
2. Cloud Security
3. Umbrella
4. Investigate
5. CASB
6. Application Settings

1.2. Time Range Selector

1. You use the time range selector tool to display information for a given interval. By default, the application shows the data of the Last 1 Hour. You can configure this in **App Settings**.
2. You can select the predefined date ranges or click **Custom** to select Custom Date Ranges.

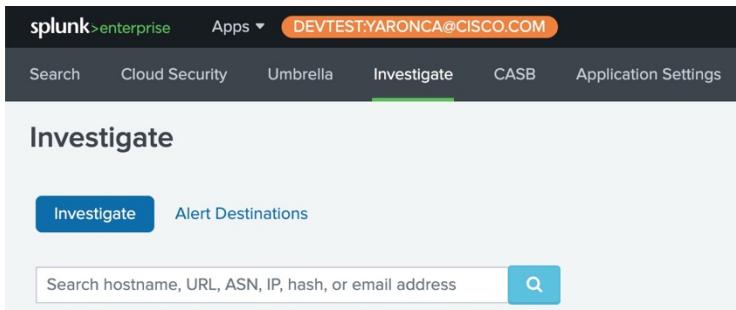


Note: The Time Range selector is available only in the dashboard.

1.3. Investigate Tab

If the Investigate module cannot connect to the API, this page might not be available. You can see its status in **Application Settings > Health**.

1. The Investigate Tab enables you to search for detailed information about a destination by entering a domain name, IP or URL.



The screenshot shows the Splunk Enterprise web interface. At the top, there is a dark header bar with the text "splunk>enterprise" on the left, "Apps" with a dropdown arrow in the middle, and a user email "DEVTEST.YARONCA@CISCO.COM" on the right. Below the header is a navigation bar with several tabs: "Search", "Cloud Security", "Umbrella", "Investigate" (which is highlighted in green), "CASB", and "Application Settings". The main content area has a light gray background and is titled "Investigate". Inside this area, there are two buttons: "Investigate" (which is blue and outlined) and "Alert Destinations". Below these buttons is a search bar containing the placeholder text "Search hostname, URL, ASN, IP, hash, or email address" and a magnifying glass icon. The overall layout is clean and modern, typical of enterprise software interfaces.

1.4. CASB Tab

If the Cloudlock module cannot connect to the API, this page might not be available. You can see its status in **Application Settings > Health**.

1. The Cloudlock Tab displays information related to Cloudlock incidents:

The screenshot shows the Splunk Enterprise interface with the CASB tab selected. At the top, there are navigation links: Search, Cloud Security, Umbrella, Investigate, CASB (highlighted in green), and Application Settings. The main content area is divided into several sections:

- Incidents:** A table listing three incidents. Each row includes columns for ID, Platform, Matches, Policy, CreatedAt, UpdatedAt, Source, Owner, Severity, Status, and Actions.
- When ?**: A line chart showing the count of events over time, with the x-axis labeled "updated_at".
- Event Types:** A table listing various event types and their counts.
- Where ?**: A world map showing the geographical distribution of incidents.

2. You can click on an ID to view the details about an incident:

The screenshot shows the "Incident Details" modal window. It contains the following sections:

- Incident Details:** A summary table with the following data:

Objective Type	UBEA
Name	Pankaj Tanwar
Platform	office365
Owner	[REDACTED]
Policy	AppTest
Time	2020-09-03T00:50:55.925470+00:00
Status	NEW
Severity	CRITICAL
- Detected:** A table showing a single event entry:

Detected	Match Type	Match
09M 03, 2020	null	null
- Raw Details:** A code block displaying raw JSON data from the event:

```
{"event_type": "UBEA", "incident_status": "NEW", "ubea_data_set": [{"item": [{"raw": {"UserType": 0, "HighPriorityMediaProcessing": false, "UserId": "[REDACTED]", "ClientIp": "[REDACTED]", "Id": "0217476a-51e0-468d-83a1-144902", "CorrelationId": "d237709f-0086-0000-383f-7a9d8dd76bb9", "Version": 1, "ItemType": "File", "CreationTime": "2020-09-03T00:14:12", "OrganizationId": "[REDACTED]6e8b1faf2", "SourceRelativeUrl": "Shared Documents/Incident Management"}]}]}
```

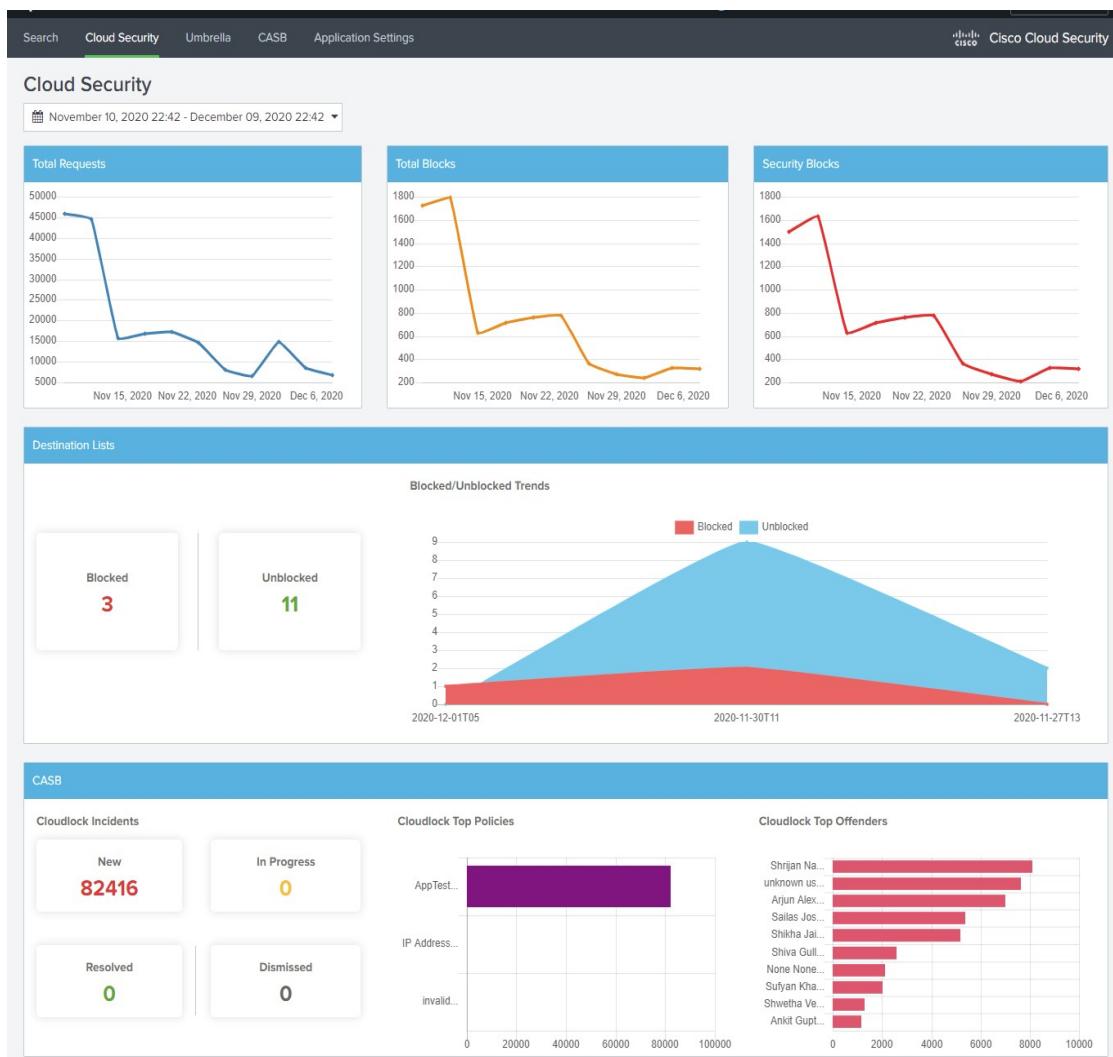
3. You can also update the severity and/or status of an incident by selecting the values from the drop-down list and clicking **Update**:

Incidents											Incident ID	<input type="text"/>
Id	Platform	Matches	Policy	CreatedAt	UpdatedAt	Source	Owner	Severity	Status	Actions		
317630935	office365	1	AppTest	06-04-2020 08:57:04	06-04-2020 08:57:04	OneDrive Folder Created	Koppisetti Krishna	ALERT	<input type="button" value="DISMISS"/>	<input type="button" value="Update"/>		
317630934	office365	1	AppTest	06-04-2020 08:57:04	06-04-2020 08:57:04	OneDrive File Sync Uploaded Full	Prathamesh Mhatre	ALERT	<input type="button" value="DISMISSED"/> IN PROGRESS NEW RESOLVED	<input type="button" value="Update"/>		

1.5. Cloud Security Tab

If the Destination List or Cloudlock module cannot connect to their APIs, this page might not be available. You can see its status in **Application Settings > Health**.

The Cloud Security Tab displays information about Umbrella requests, Destination List activity and Cloudlock Incidents at a high level:



1.6. Umbrella Tab

This tab is available only when the Cisco Cloud Security Add-on is installed and configured successfully. Be sure to select the indexes under the Umbrella section in the Application Settings page.

The Umbrella Tab comprises 4 parts:

1. Umbrella DNS

This section shows the Overall Request count, Blocked Requests for the selected time range and the equivalent previous time range, Block trend for the specified time, Blocked vs Allowed Destinations, and Top Blocked DNS Categories.

2. Umbrella SWG

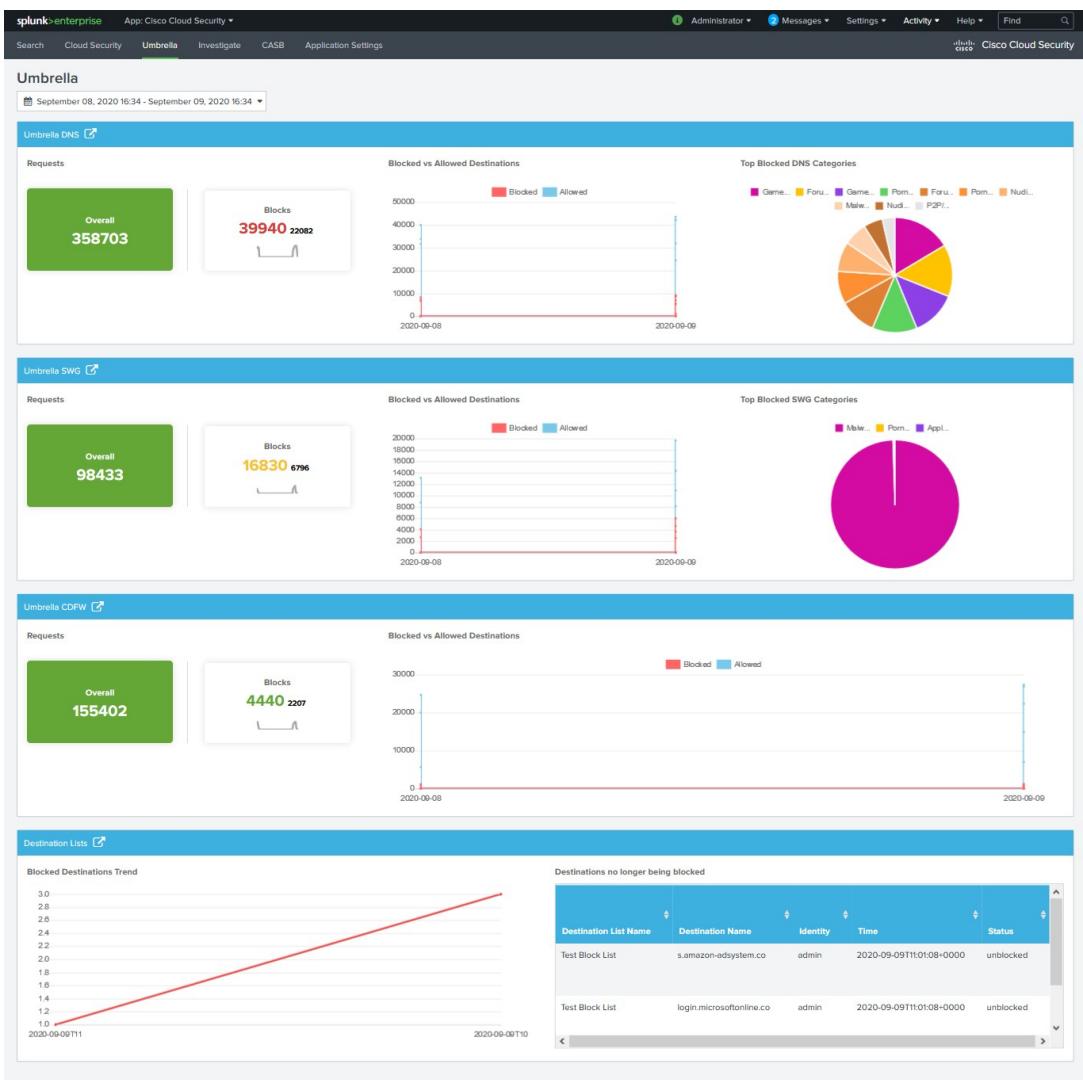
This section shows the Overall Request count, Blocked Requests for the selected time range and the equivalent previous time range, Block trend for the specified time, Blocked vs Allowed Destination, and Top Blocked SWG Categories.

3. Umbrella CDFW trend

This section shows the Overall Request count, Blocked Requests for the selected time range and the equivalent previous time range, Block trend for the specified time and Blocked vs Allowed Destination trend.

4. Destination List

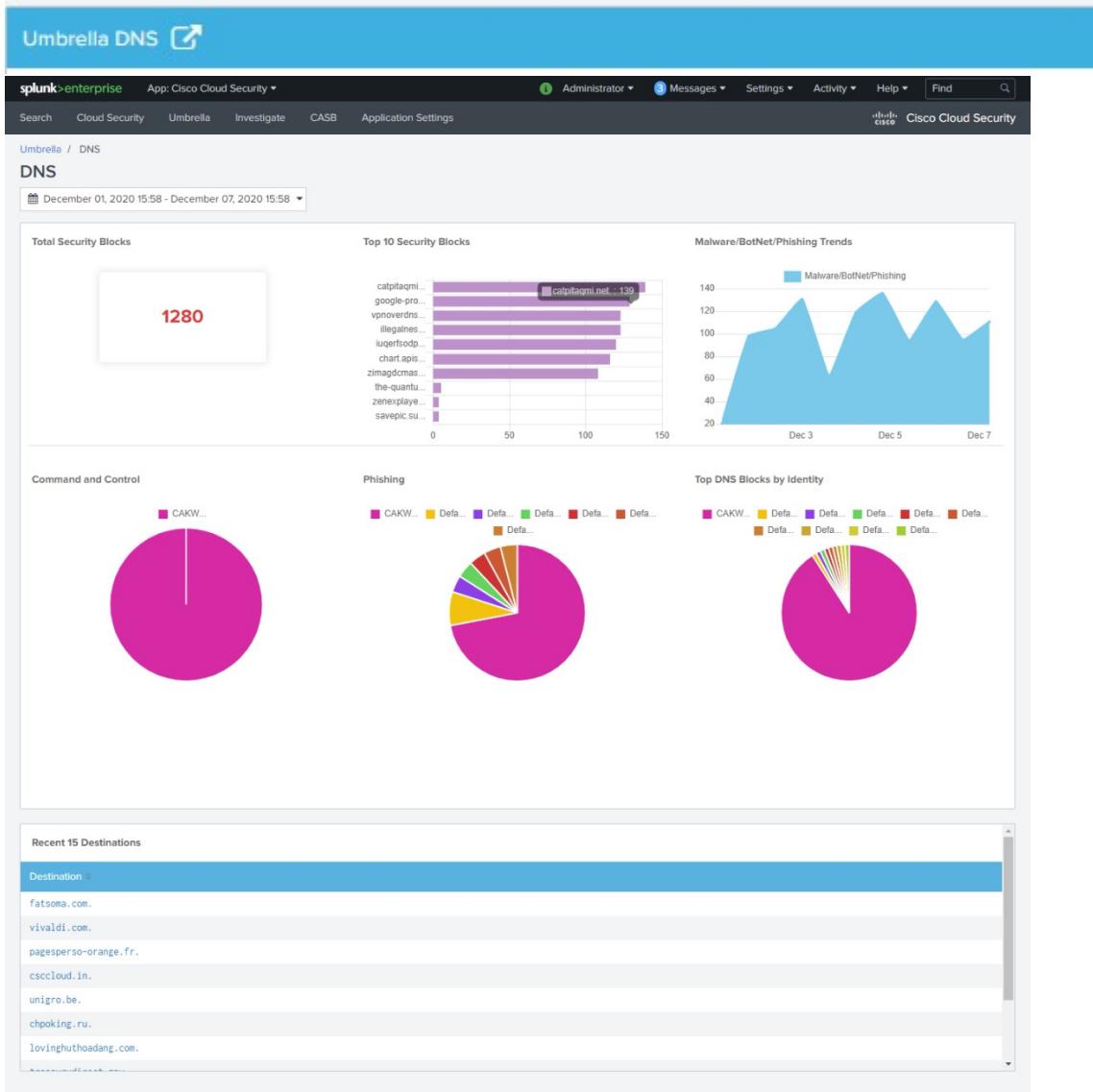
This section shows the Blocked Destination trend and Destinations no longer being blocked.



Click the redirection/popup icon: to see a detailed view of these sections.

1.6.1. Cisco Umbrella DNS

To open the DNS dashboard, click the redirection icon next to the Umbrella DNS title in the Umbrella dashboard panel tab:



1.6.2. Cisco Umbrella SWG

To open the SWG dashboard, click the redirection icon next to the Umbrella SWG title in the Umbrella dashboard panel tab:

The screenshot shows the Cisco Umbrella SWG dashboard with the following sections:

- Total Security Blocks:** A summary card showing the number 8.
- Top 10 Security Blocks:** A bar chart showing the top 10 security blocks. The data is as follows:

Block	Count
http://d30...	5
http://pro...	2
http://d2b...	1
- Malware/BotNet/Phishing Trends:** A line chart showing trends over time. The data is as follows:

Time	Value
2020-12-07 14:54	0
2020-12-07 15:24	4
2020-12-07 15:54	0
- Breakdown by AMP Verdict:** A bar chart showing the breakdown of AMP verdicts. The data is as follows:

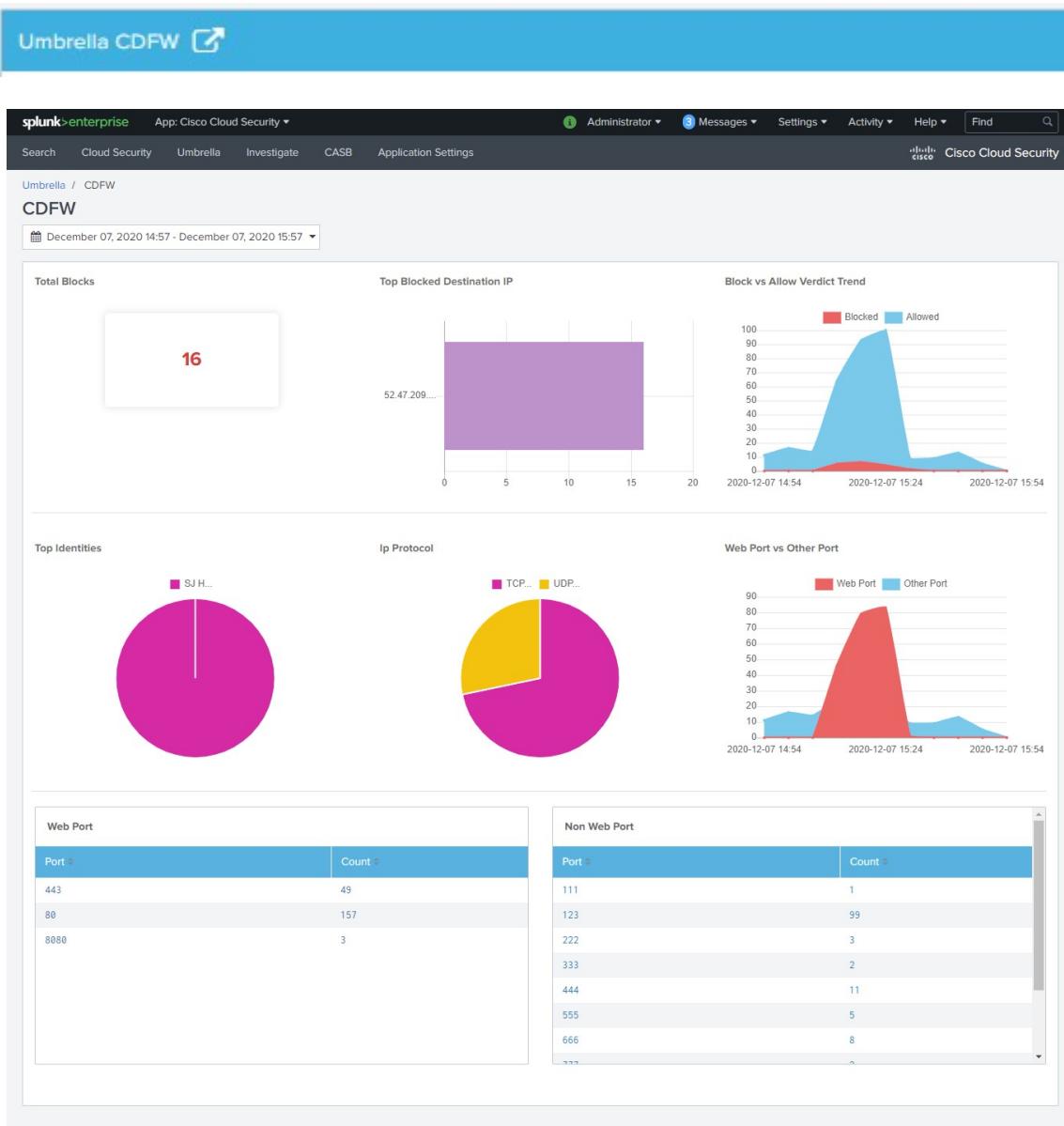
Verdict	Count
MALICIOUS...	6
- Breakdown by Mime Types:** A pie chart showing the breakdown of mime types. The data is as follows:

Mime Type	Percentage
text...	~95%
appl...	~3%
appl...	~1%
text...	~1%
- Newly Seen Destinations:** A pie chart showing newly seen destinations. The data is as follows:

Destination	Percentage
5.19...	~35%
199...	~15%
184...	~10%
23.2...	~10%
69.9...	~5%
64.1...	~5%
99.8...	~5%
23.2...	~5%
95.1...	~5%
- Recent 15 Destinations:** A list of URLs:
 - http://l1vit.cdn.ea.com/eamaster/s/shift/the_sims/the_sims_4/fg_ww_us/the_sims_4pcfg_ww_usbeta_2019_pcbsmlrprodretailidip_15067102010c6fadab9ca40e6952209971e7867c3.zip?nva=20190313172236&token=0ec611cc7c0341c3c9831
 - http://positon.org/an-outgoing-port-tester
 - http://eboce.bid/navehip.db
 - https://malware.opendns.com
 - http://origin-a.akamaihd.net/eamaster/s/shift/the_sims/the_sims_4/fg_ww_us/the_sims_4pcfg_ww_usbeta_2019_pcbsmlrprodretailidip_15067102010c6fadab9ca40e6952209971e7867c3.zip?sauth=152422958_7fd53ac5c845699d0c7d59589cdffdb4
 - http://positon.org/bizou/

1.6.3. Cisco Umbrella CDFW

To open the CDFW dashboard, click the redirection icon next to the Umbrella CDFW title in the Umbrella dashboard panel tab:



1.6.4. Cisco Destination List

To open the Destination Lists dashboard, click the redirection icon next to the Umbrella Destination Lists title in the Umbrella dashboard panel tab:

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise App: Cisco Cloud Security
- Top Bar:** Administrator, Messages, Settings, Activity, Help, Find, Cisco Cloud Security logo
- Breadcrumbs:** Umbrella / Destination Lists
- Section:** Destination Lists
- Filter:** A dropdown menu is open, showing options: Test Block List, Suspicious, Block For All, and Test Block List again.
- Table 1: Destinations Blocked**

Select	Destination List Name	Destination Name	User Name	Action	Source	Time
<input type="checkbox"/>	Test Block List	jcxgqqqxf2kdkx2x3sla-po3qb2-9a68b5234-clientnsrv4-s.akamaihd.ne	admin	added	manual	2020-09-09T10:58:54+0000
<input type="checkbox"/>	Test Block List	smetrics.cnn.co	admin	added	manual	2020-09-09T10:59:05+0000
<input type="checkbox"/>	Test Block List	secure-origin.lmworldwide.co	admin	added	manual	2020-09-09T10:59:51+0000
<input type="checkbox"/>	Test Block List	virt.outbrain.co	admin	added	manual	2020-09-09T11:00:11+0000
- Text:** Showing 1 to 4 of 4 entries
- Buttons:** Previous, Next
- Table 2: Destinations Unblocked**

Destination List Name	Destination Name	Identity	Time	Status
Test Block List	s.amazon-adsystem.co	admin	2020-09-09T11:01:08+0000	unblocked
Test Block List	login.microsoftonline.co	admin	2020-09-09T11:01:08+0000	unblocked
- Text:** Showing 1 to 2 of 2 entries
- Buttons:** Previous, Next

You can use the filter icon to choose a destination list from the list and block those destinations.

The screenshot shows the Destination Lists dashboard with the following changes:

- Filter:** The "Test Block List" checkbox is checked.
- Table:** The same data as the first screenshot is present, but the "Test Block List" row is highlighted in blue.
- Buttons:** A yellow box highlights the "Unblock" button at the bottom right.

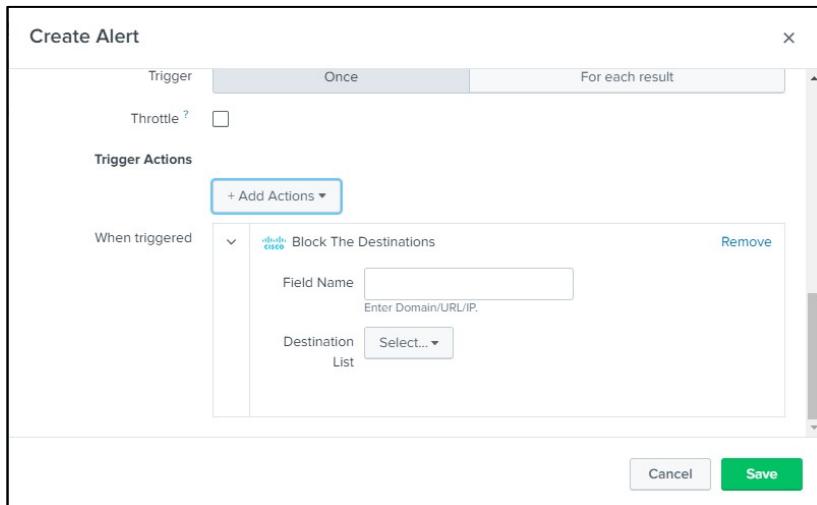
4. Configuring Custom Alerts in Splunk

The Cisco Cloud Security Splunk App provides 2 Alert Actions:

1. Block Destinations
2. Investigate Destinations

Block Destinations

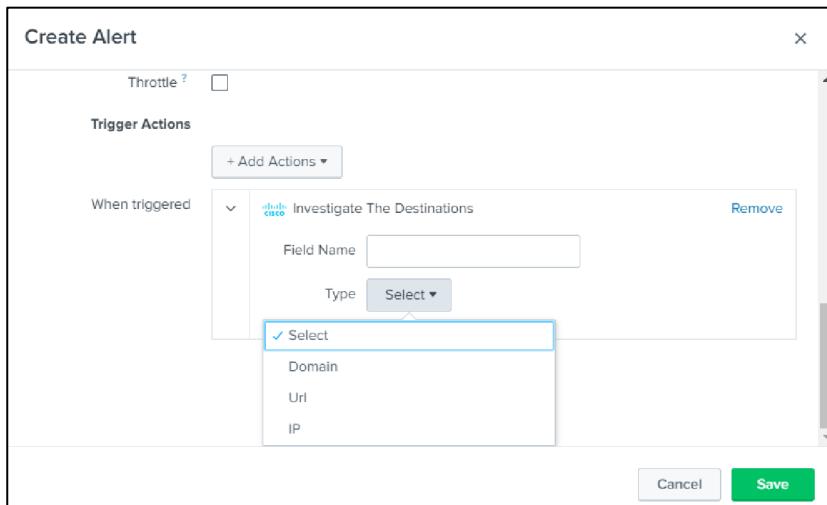
This Alert Action enables you to Block a Domain, URL, or IP by providing the field name and selecting the Destination List name.



Investigate the Destinations

To investigate the destination by type and field name:

- enter the field name
- select the type (URL, IP, or Domain):



5. Cisco Cloud Security App and Add-on Distributed Deployment

The following tables describe where and how to install the Cloud Security app and add-on in a distributed deployment of Splunk Enterprise, or any deployment for which you are using forwarders to retrieve your data. Depending on your environment and preferences, and the requirements of the app and add-on, you may need to install the app or add-on in multiple places.

Where to install this app?

This table provides a reference for installing this specific app on a distributed deployment of Splunk.

Where to install the app?

Splunk platform component	Support
Search Heads	Install and configure the Destination Lists and S3 indexes only
Indexers	Install and configure the Investigate and Cloudlock APIs and indexes only

Where to install the add-on?

While it's possible to install add-ons on all tiers of a distributed Splunk platform deployment, we recommend the following:

Splunk platform component	Support
Heavy Forwarder	Best Practice
Indexer/s	Only if there are no Heavy Forwarders

6. Troubleshooting

Validating events are being indexed:

1. Umbrella Logs being indexed:

- Cisco Umbrella DNS Logs**

In the Search tab enter “sourcetype = cisco:umbrella:dns” to view Umbrella DNS events.

- Cisco Umbrella Proxy Logs**

In the Search tab enter “sourcetype = cisco:umbrella:proxy” to view Umbrella proxy events.

- Cisco Umbrella Firewall Logs**

In the Search tab enter “sourcetype = cisco:umbrella:firewall” to view Umbrella firewall events.

2. To support Spunk running on servers that also have python2 installed:

```
python.version=python3
```

The configuration mentioned above should be removed from restmap.conf and inputs.conf.spec.