Cisco Cloud Security App for Splunk

Version Number: 1.0.15

Date: Aug 9, 2021

Contents

Table of Contents

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 the Add-On and App are 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

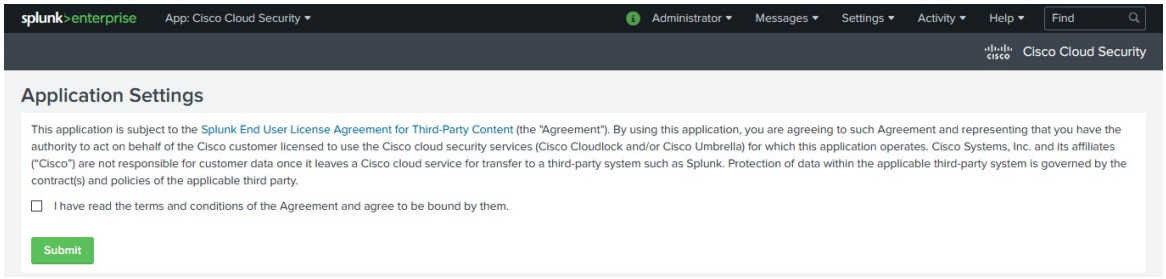
When the app is installed, 3 roles are created:

- 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

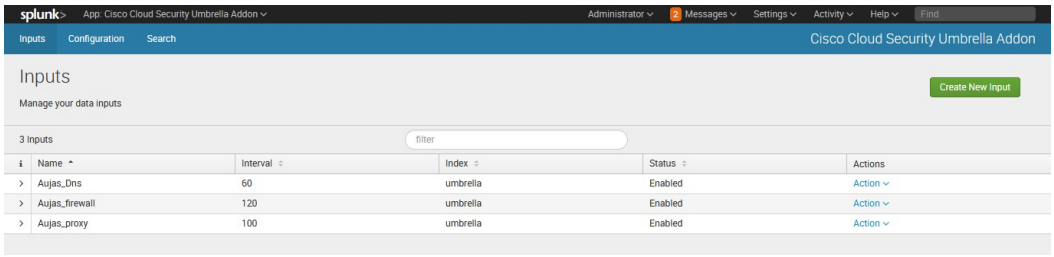
2.3.1. Accept the terms and condition

1. Read and accept the terms and conditions.

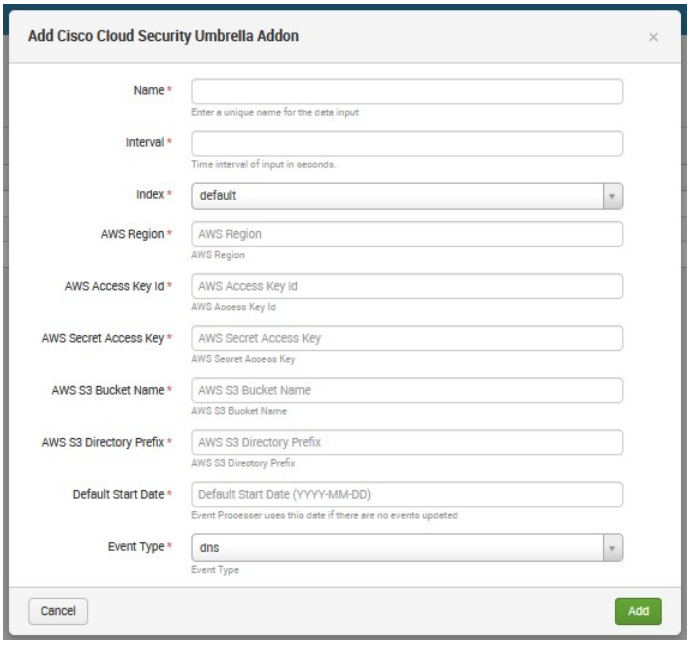


2. Click Submit.

2.3.2. Configure the Umbrella Add-on Settings



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



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:

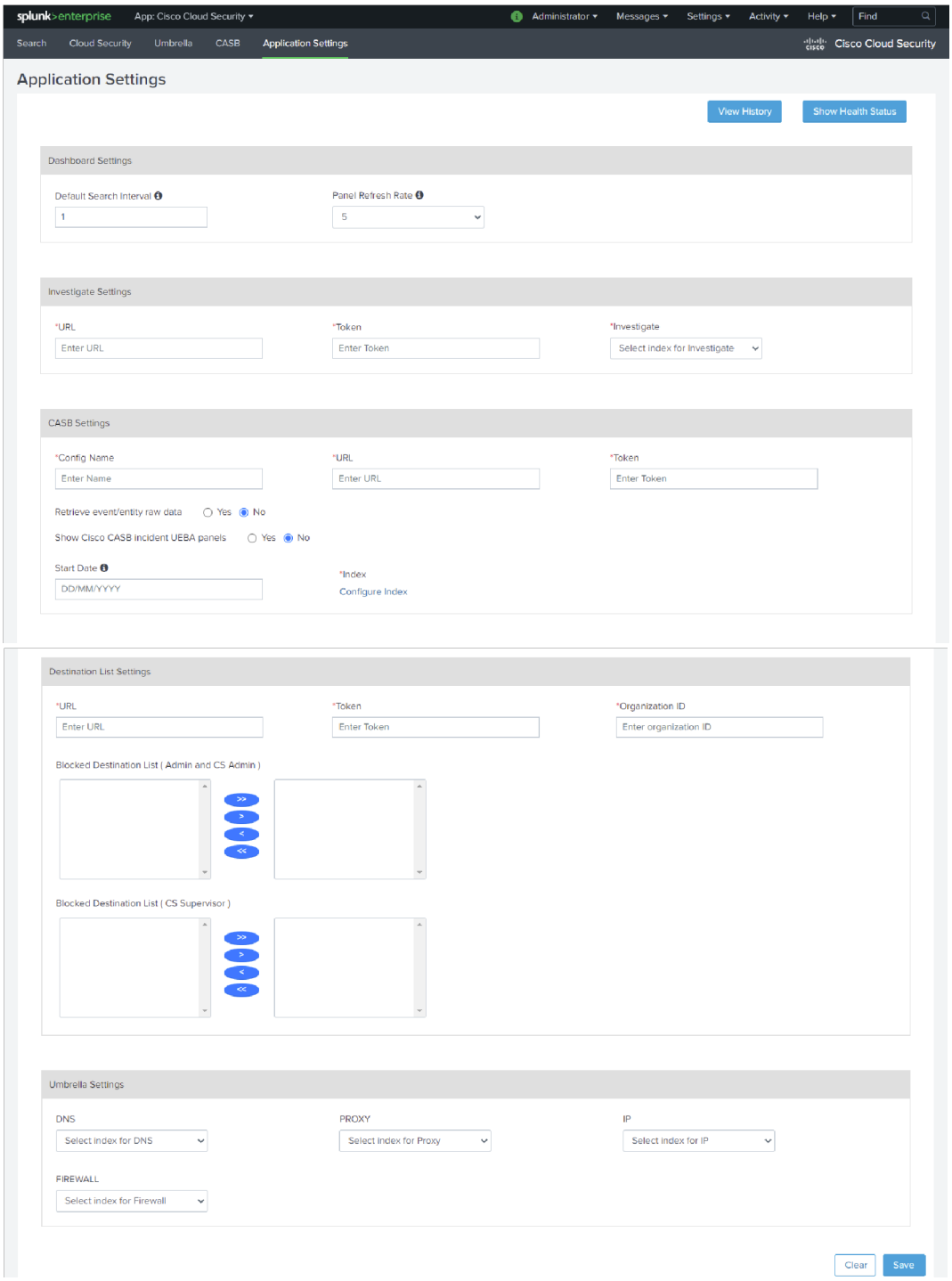
Log Type	Example
DNS logs	2506xxx_2db1xxxx1ddf7cxxx18652xxxxfdab7xxxxd60xx/dnslogs/
Proxy logs	2506xxx_2db1xxxx1ddf7cxxx18652xxxxfdab7xxxxd60xx/proxylogs/
Firewall logs	2506xxx_2db1xxxx1ddf7cxxx18652xxxxfdab7xxxxd60xx/firewalllogs/

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

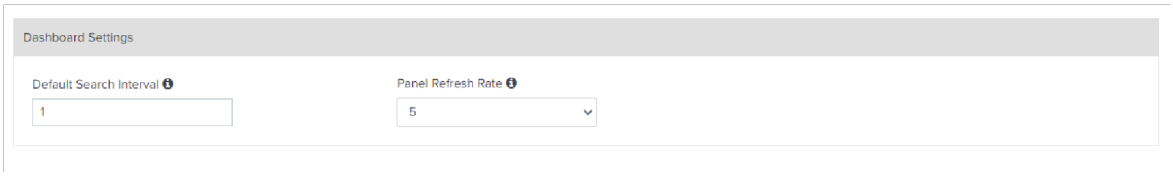
In the Application Settings you can:

- 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.


splunk>enterprise
App: Cisco Cloud Security
Administrator
Messages
Settings
Activity
Help
Find
Search
Cloud Security
Umbrella
CASB
Application Settings
Cisco Cloud Security
Application Settings
View History
Show Health Status
Dashboard Settings
Default Search Interval
1
Panel Refresh Rate
5
Investigate Settings
*URL
Enter URL
*Token
Enter Token
*Investigate
Select index for Investigate
CASB Settings
*Config Name
Enter Name
*URL
Enter URL
*Token
Enter Token
Retrieve event/entity raw data
Yes
No
Show Cisco CASB incident UEBA panels
Yes
No
Start Date
DD/MM/YYYY
*Index
Configure Index
Destination List Settings
*URL
Enter URL
*Token
Enter Token
*Organization ID
Enter organization ID
Blocked Destination List (Admin and CS Admin)
Blocked Destination List (CS Supervisor)
Umbrella Settings
DNS
Select index for DNS
PROXY
Select index for Proxy
IP
Select index for IP
FIREWALL
Select index for Firewall
Clear
Save

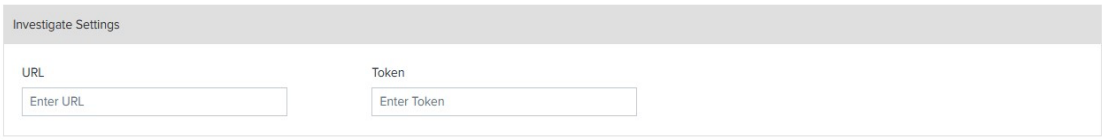
The Application Settings page enables you to configure the following settings:

A. Dashboard Settings



• Select the default search interval and Panel refresh rate.

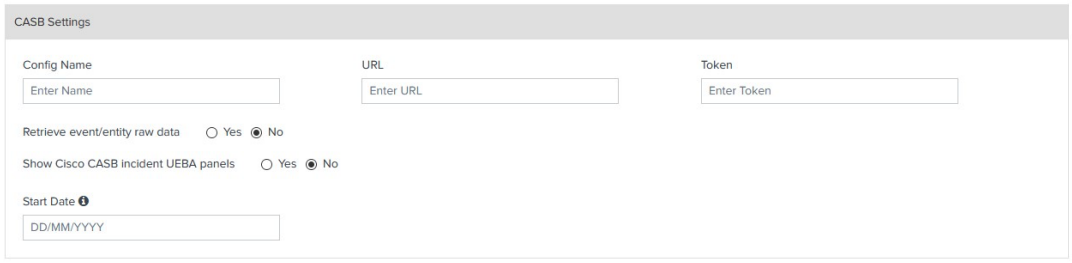
B. Investigate API settings:



• Enter the following URL: **https://investigate.api.umbrella.com/**

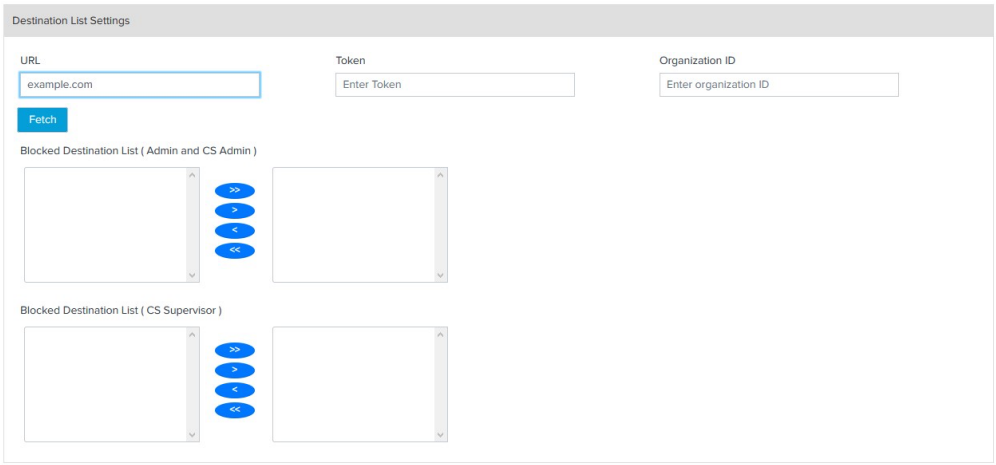
• Enter an Investigate API Token generated from the Umbrella dashboard.

C. CASB (Cloudlock) settings:



- 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.

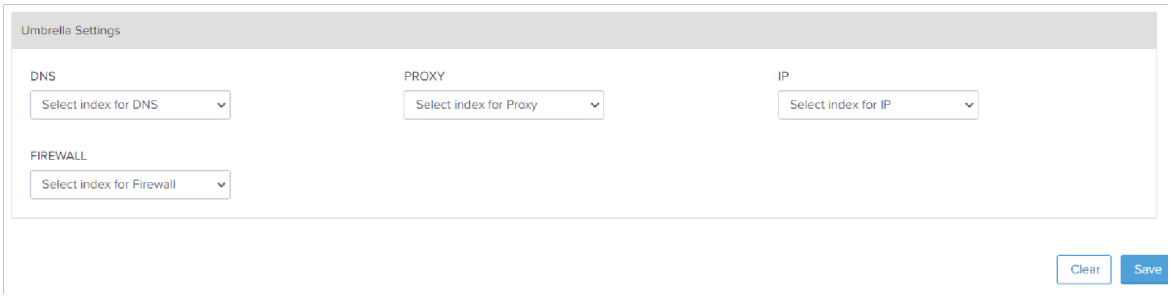
D. Destination List settings



- 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.

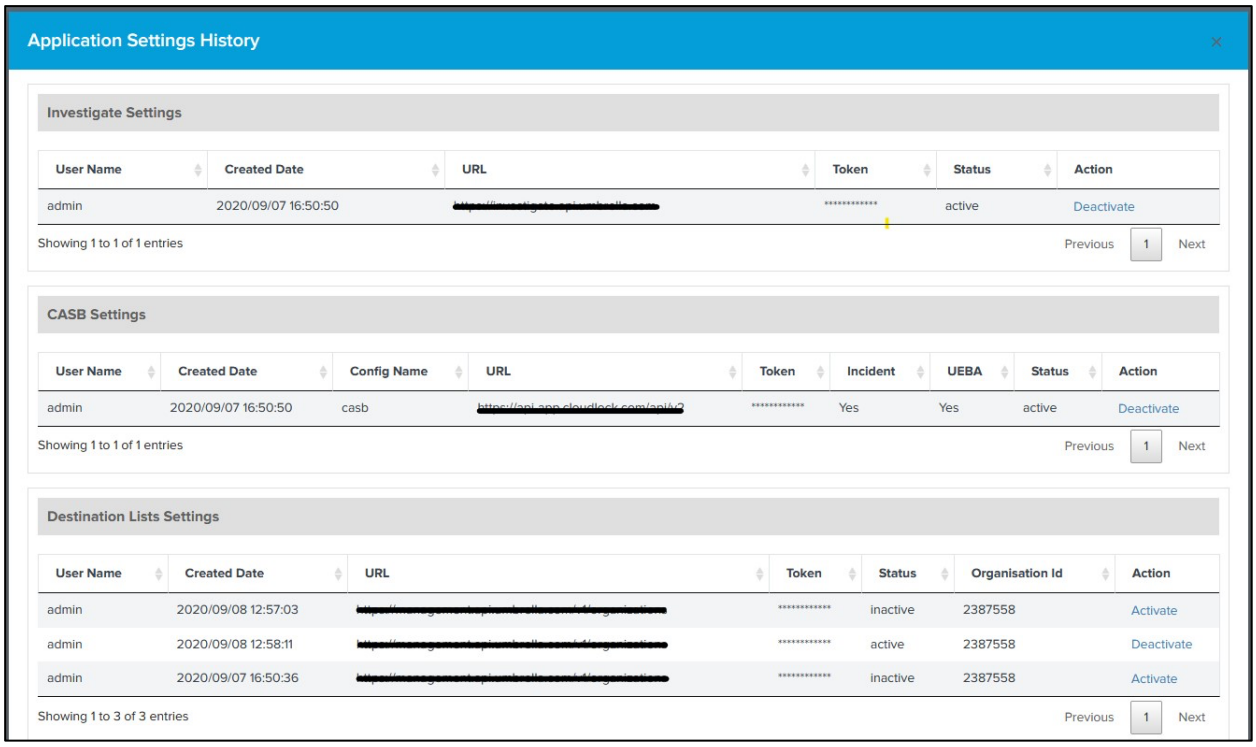
E. Umbrella Settings

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



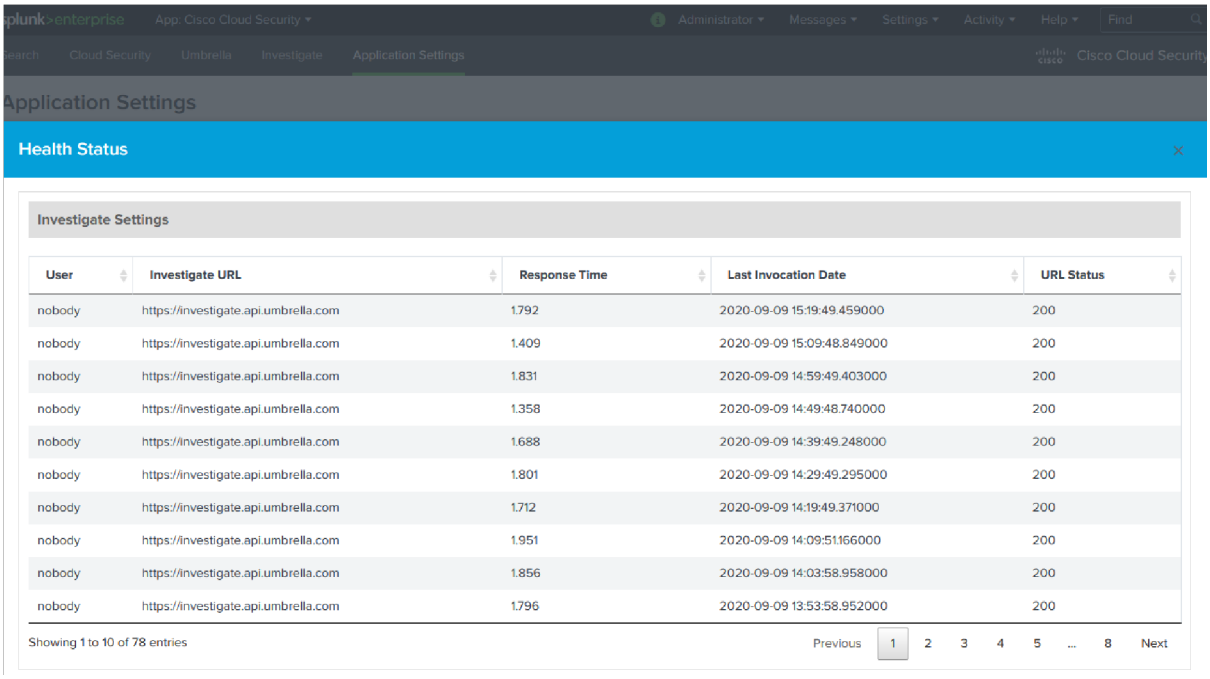
Application Settings History

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



Health Status

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



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

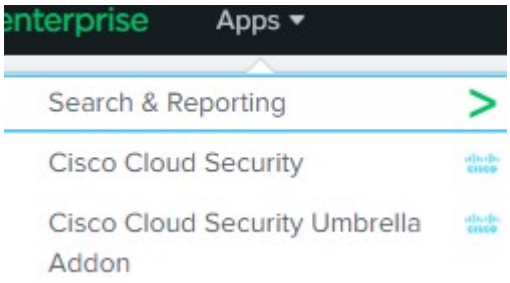
Previous 1 2 3 4 5 ... 9 Next

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



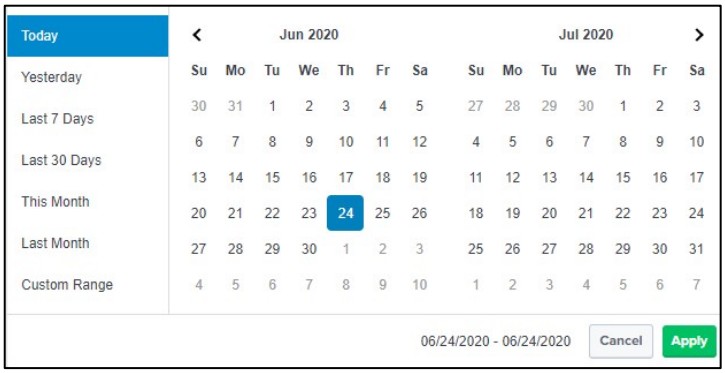
When the Cisco Cloud Security App and Cisco Cloud Security Add-on are successful installed, you can list the App and Add-on under the installed App menu.

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.

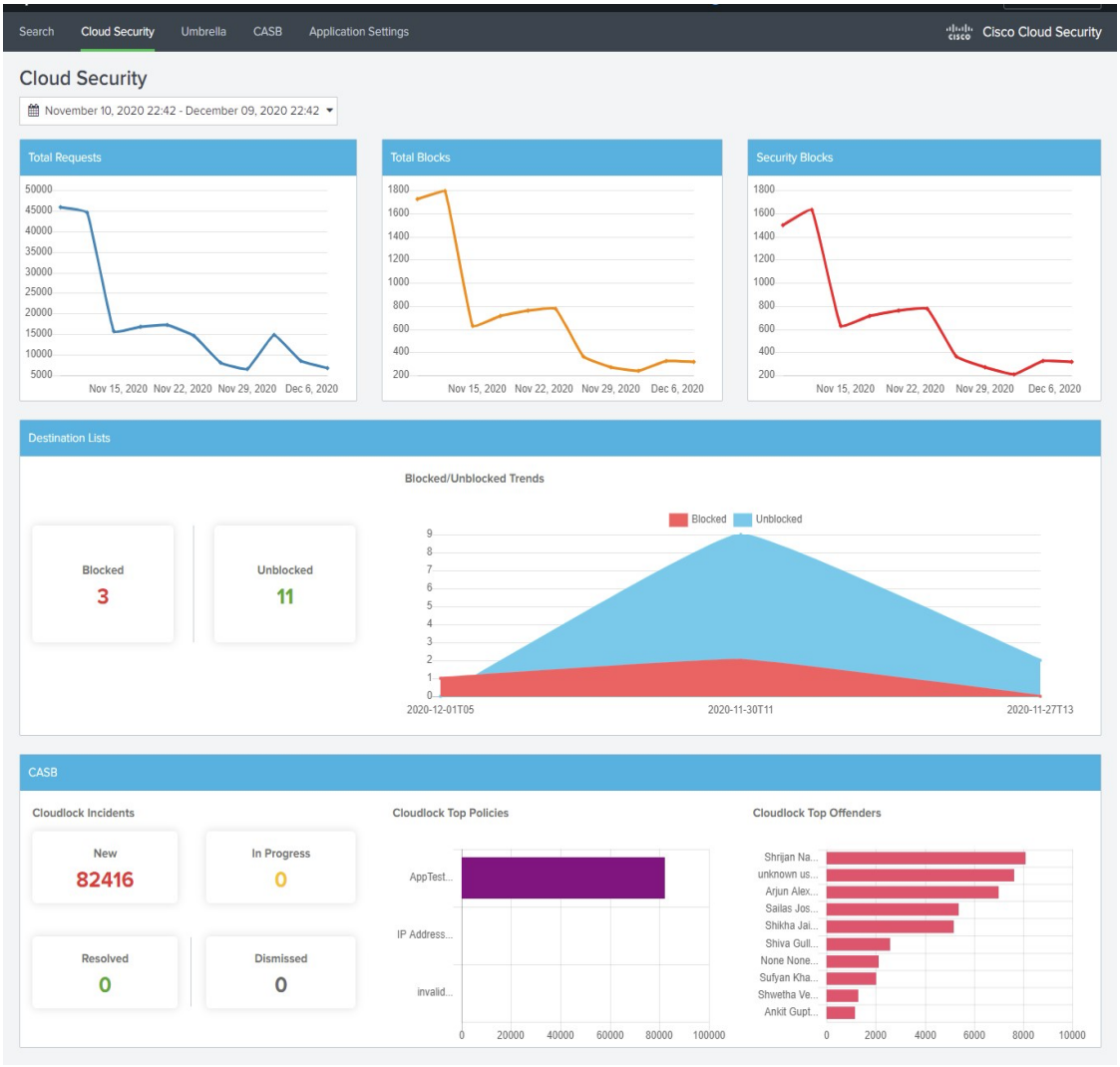


Note: The Time Range selector is available only in the dashboard.

1.3. 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:



1.4. 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

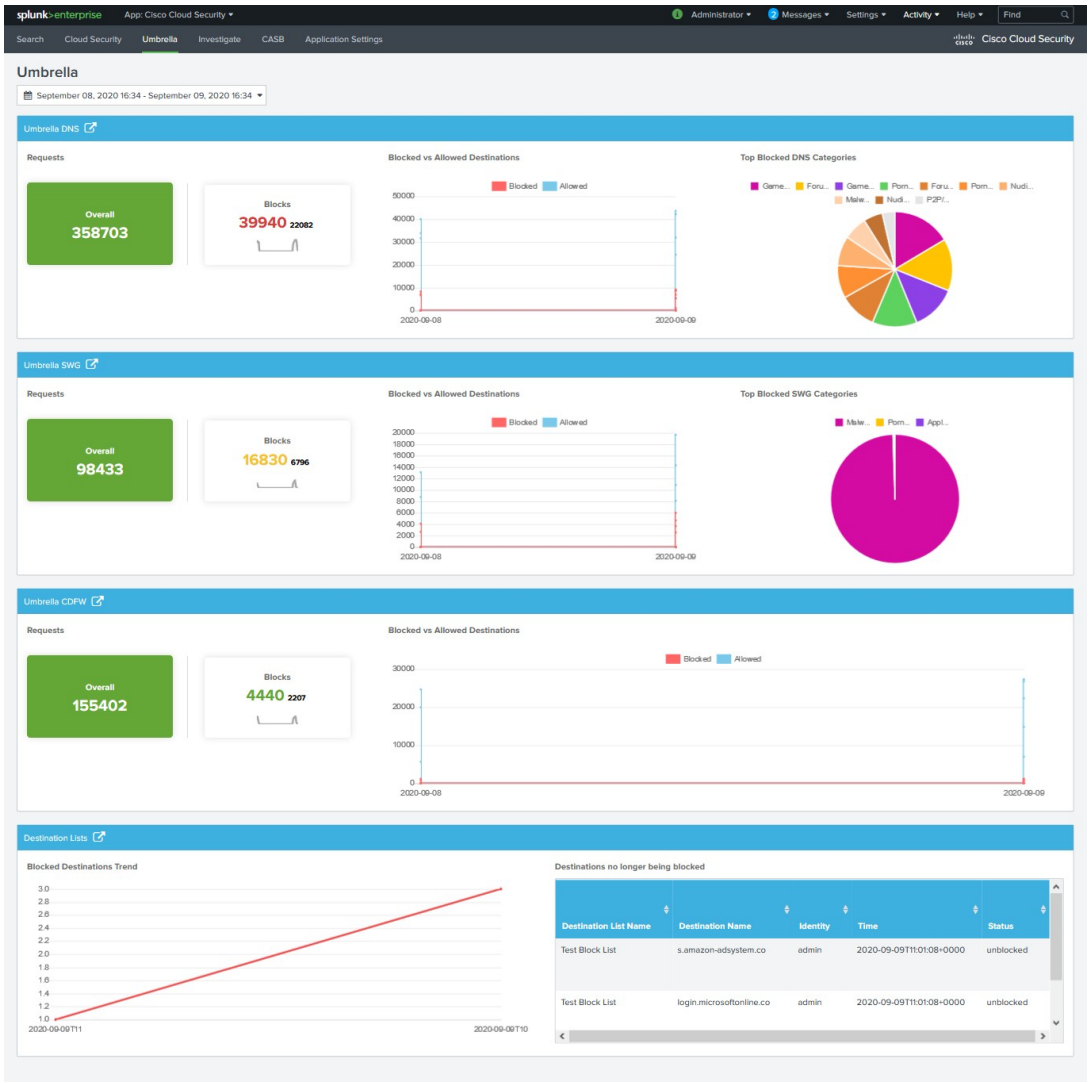
   This section shows the Overall Request count, Blocked Requests for the selected time range and the equivalent previous time range, Block trend for the specified time, Blocked vs Allowed Destination, and Top Blocked SWG Categories.

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

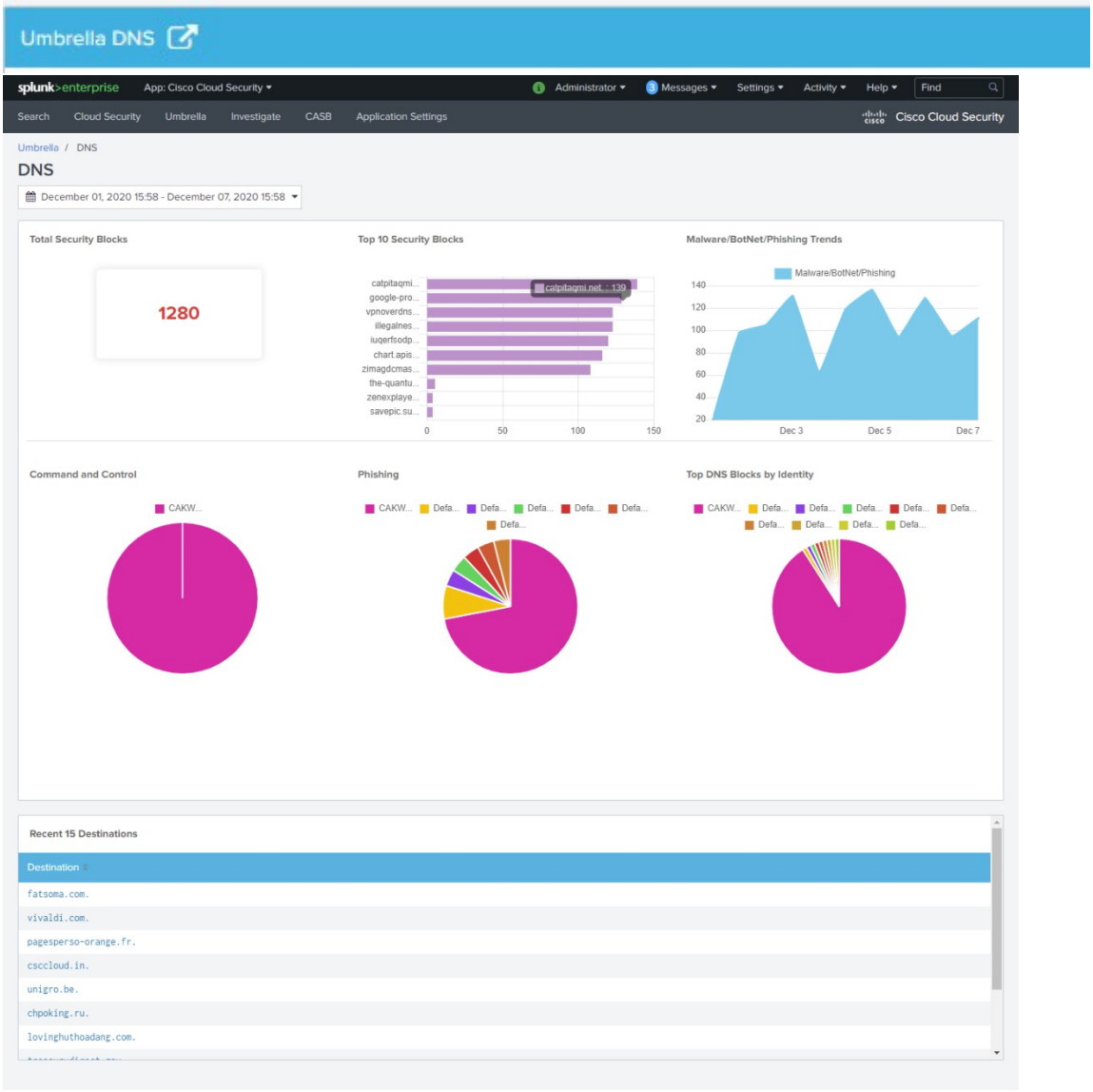
   This section shows the Blocked Destination trend and Destinations no longer being blocked.



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

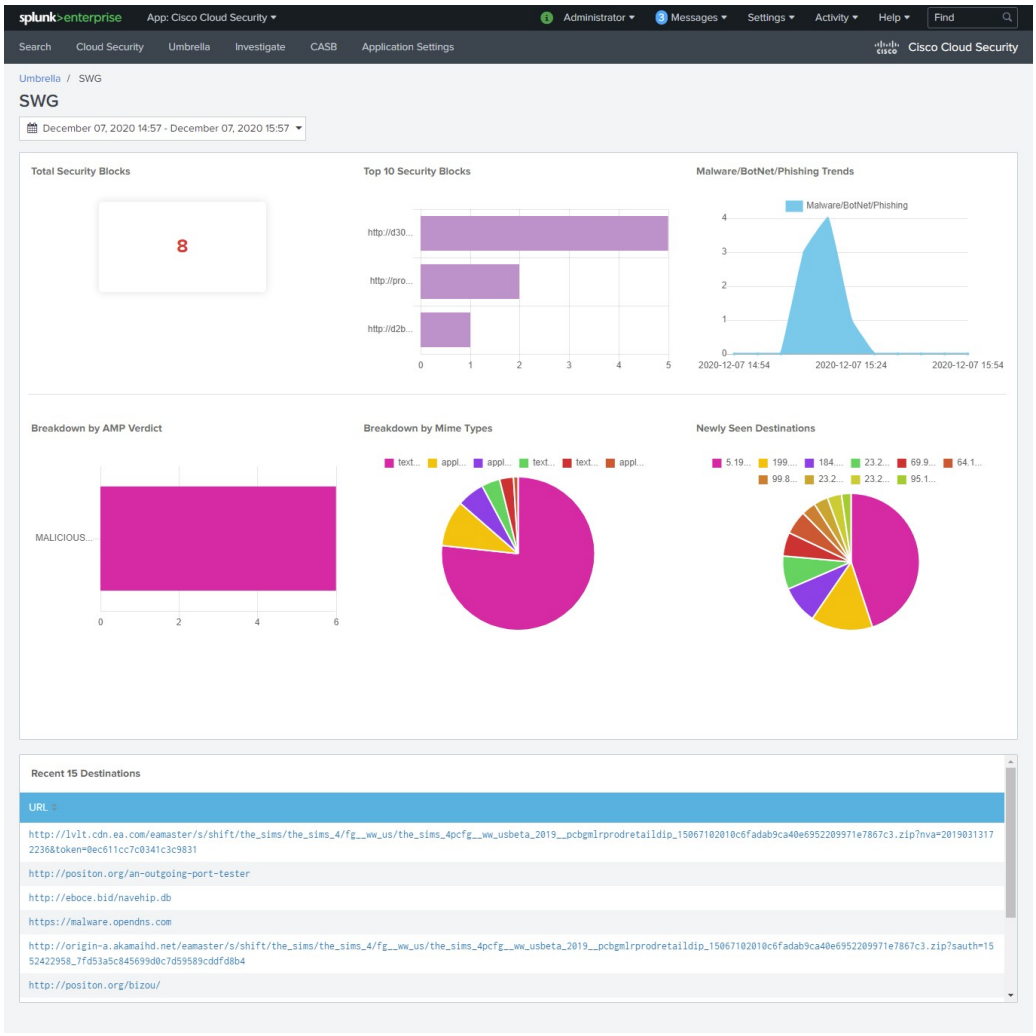
1.4.1. Cisco Umbrella DNS

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



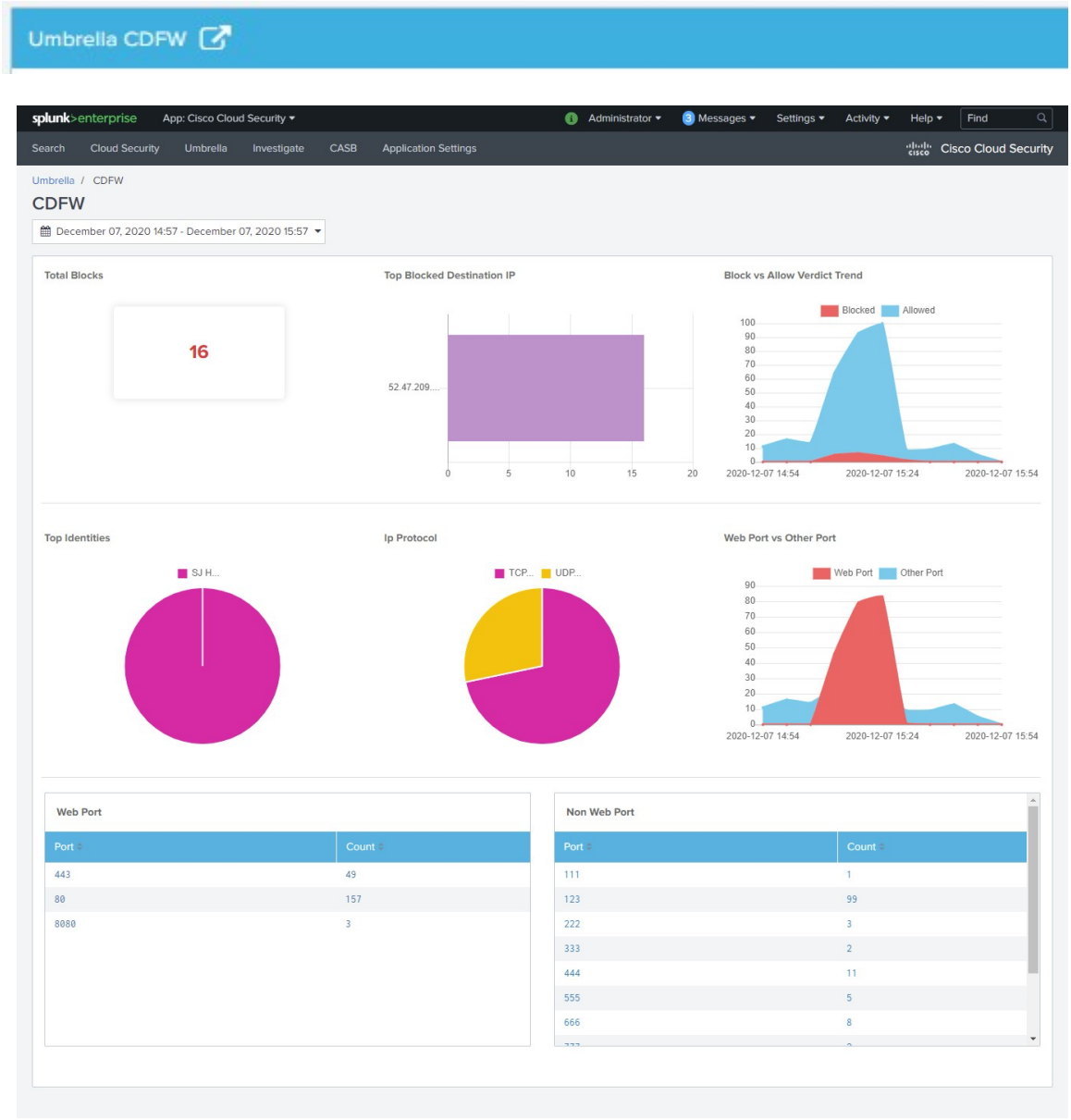
1.4.2. Cisco Umbrella SWG

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



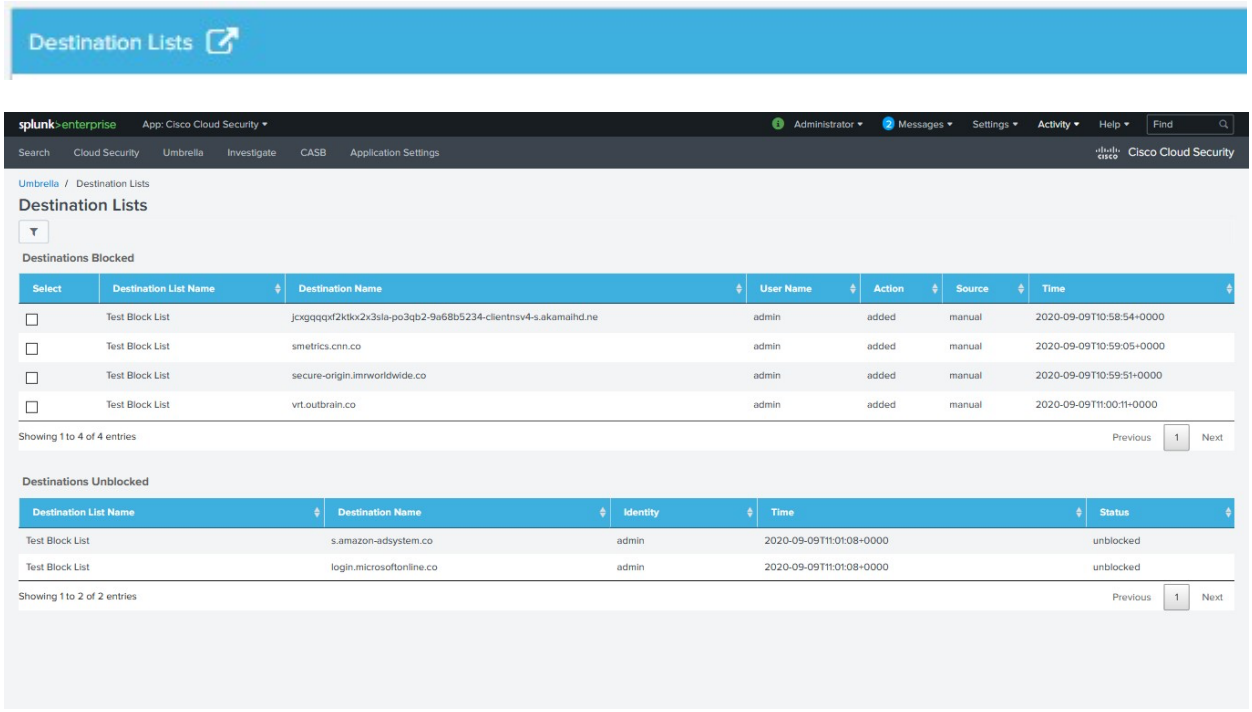
1.4.3. Cisco Umbrella CDFW

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

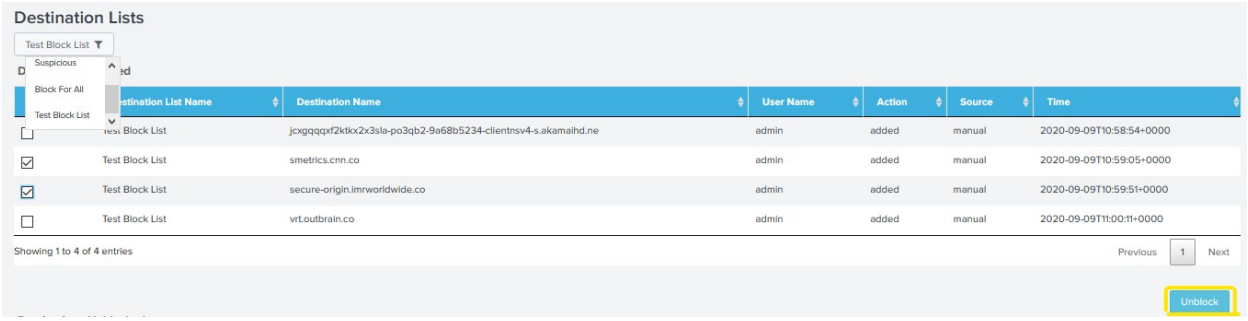


1.4.4. Cisco Destination List

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



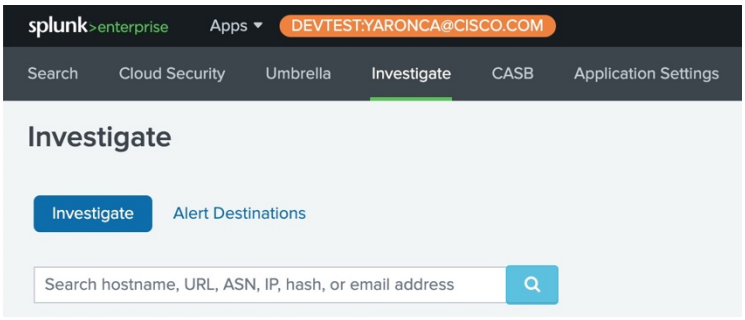
You can use the filter icon to choose a destination list from the list and block those destinations.



1.5. 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**.

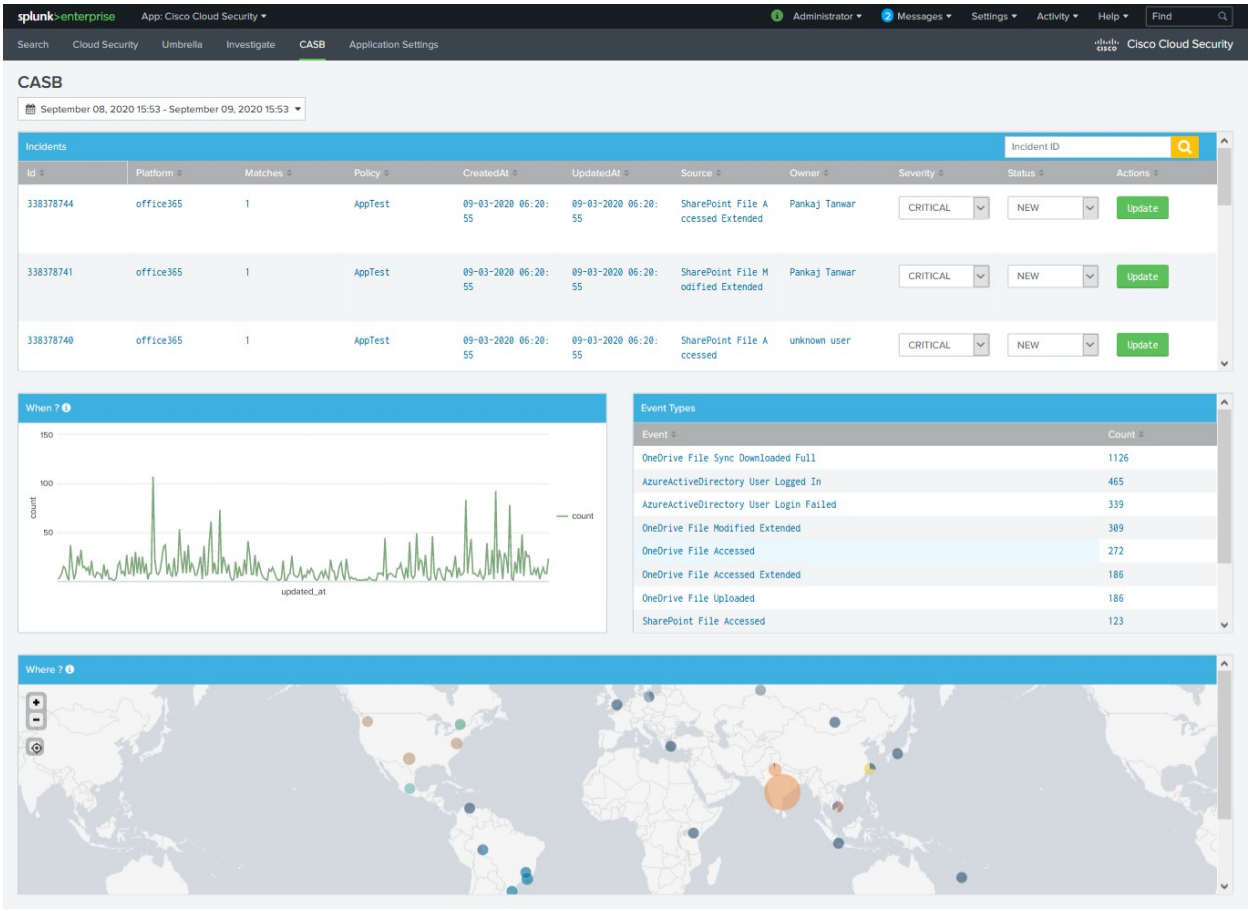
1. The Investigate Tab enables you to search for detailed information about a destination by entering a domain name, IP or URL.



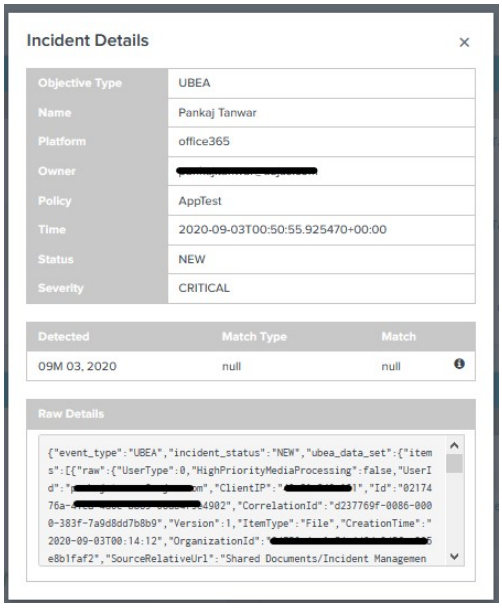
1.6. CASB Tab

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

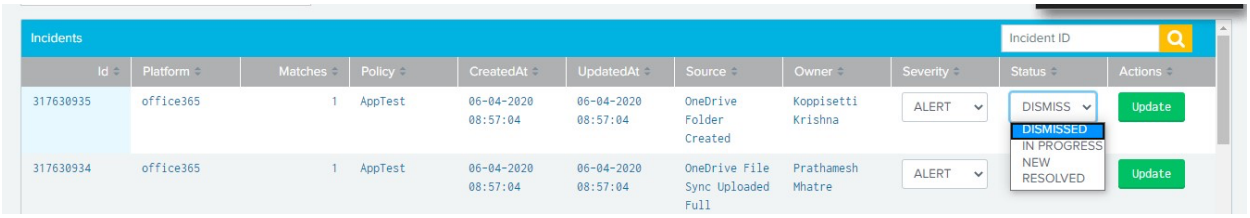
1. The CASB Tab displays information related to Cloudlock incidents:



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



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**:



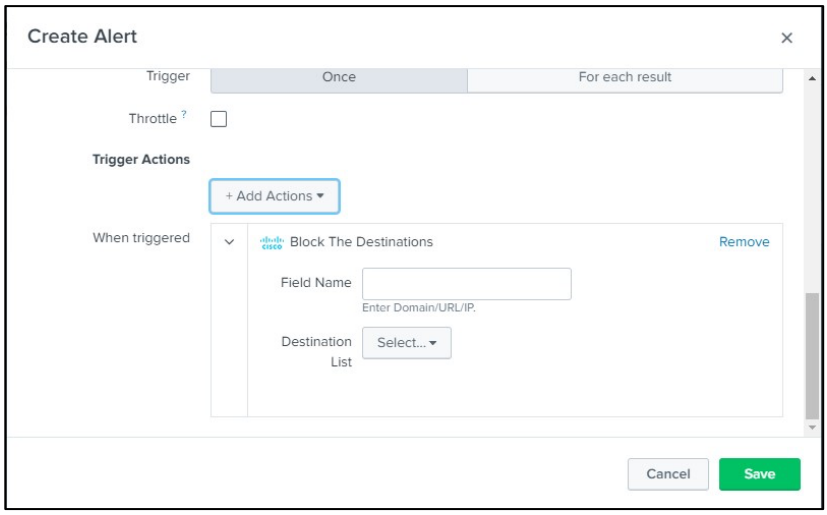
4. Configuring Custom Alerts in Splunk

The Cisco Cloud Security Splunk App provides 2 Alert Actions:

1. Block Destinations
2. Investigate Destinations

Block Destinations

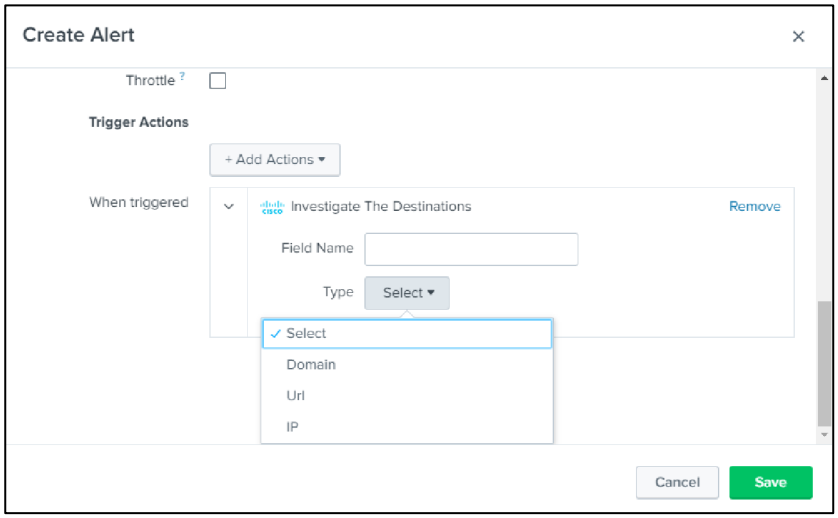
This Alert Action enables you to Block a Domain, URL, or IP by providing the field name and selecting the Destination List name.



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.