



Cisco Cloud Security App for Splunk

Version Number: 1.0.15

Date: Aug 9, 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	19
1.4. CASB Tab.....	20
1.5. Cloud Security Tab.....	13
1.6. Umbrella Tab	13
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 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.

This application is subject to the [Splunk End User License Agreement for Third-Party Content](#) (the "Agreement"). By using this application, you are agreeing to such Agreement and representing that you have the authority to act on behalf of the Cisco customer licensed to use the Cisco cloud security services (Cisco Cloudlock and/or Cisco Umbrella) for which this application operates. Cisco Systems, Inc. and its affiliates ("Cisco") are not responsible for customer data once it leaves a Cisco cloud service for transfer to a third-party system such as Splunk. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

I have read the terms and conditions of the Agreement and agree to be bound by them.

Submit

2. Click Submit.

2.3.2. Configure the Umbrella Add-on Settings

Name	Interval	Index	Status	Actions
Aujas_Dns	60	umbrella	Enabled	Action
Aujas_firewall	120	umbrella	Enabled	Action
Aujas_proxy	100	umbrella	Enabled	Action

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

Name *	<input type="text"/>
Interval *	<input type="text"/>
Index *	<input type="text"/>
AWS Region *	<input type="text"/>
AWS Access Key Id *	<input type="text"/>
AWS Secret Access Key *	<input type="text"/>
AWS S3 Bucket Name *	<input type="text"/>
AWS S3 Directory Prefix *	<input type="text"/>
Default Start Date *	<input type="text"/>
Event Type *	<input type="text"/>

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 PROXY IP

FIREWALL

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

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

A. Dashboard Settings

This screenshot shows the 'Dashboard Settings' section. It contains two input fields: 'Default Search Interval' with a value of '1' and 'Panel Refresh Rate' with a value of '5'.

- Select the default search interval and Panel refresh rate.

B. Investigate API settings:

This screenshot shows the 'Investigate Settings' section. It contains two input fields: 'URL' with placeholder 'Enter URL' and 'Token' with placeholder 'Enter Token'.

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

C. CASB (Cloudlock) settings:

This screenshot shows the 'CASB Settings' section. It includes fields for 'Config Name' (placeholder 'Enter Name'), 'URL' (placeholder 'Enter URL'), and 'Token' (placeholder 'Enter Token'). Below these are two radio button groups: 'Retrieve event/entity raw data' (radio buttons 'Yes' and 'No') and 'Show Cisco CASB incident UEBA panels' (radio buttons 'Yes' and 'No'). At the bottom is a date input field labeled 'Start Date' with placeholder 'DD/MM/YYYY'.

- 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 your 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

Destination List Settings

URL <input type="text" value="example.com"/>	Token <input type="text" value="Enter Token"/>	Organization ID <input type="text" value="Enter organization ID"/>
Fetch		
Blocked Destination List (Admin and CS Admin)		
Blocked Destination List (CS Supervisor)		

- 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:

Umbrella Settings

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

Application Settings History

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

Application Settings History								
Investigate Settings								
User Name	Created Date	URL	Token	Status	Action			
admin	2020/09/07 16:50:50	[REDACTED]	*****	active	Deactivate			
Showing 1 to 1 of 1 entries								
						Previous	1	Next
CASB Settings								
User Name	Created Date	Config Name	URL	Token	Incident	UEBA	Status	Action
admin	2020/09/07 16:50:50	casb	https://api.app.cloudlock.com/api/v2	*****	Yes	Yes	active	Deactivate
Showing 1 to 1 of 1 entries								
						Previous	1	Next
Destination Lists Settings								
User Name	Created Date	URL	Token	Status	Organisation Id			
admin	2020/09/08 12:57:03	[REDACTED]	*****	Inactive	2387558	Activate		
admin	2020/09/08 12:58:11	[REDACTED]	*****	active	2387558	Deactivate		
admin	2020/09/07 16:50:36	[REDACTED]	*****	Inactive	2387558	Activate		
Showing 1 to 3 of 3 entries								
						Previous	1	Next

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	

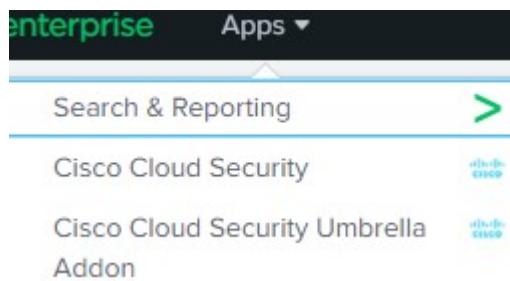
Showing 1 to 10 of 86 entries

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.

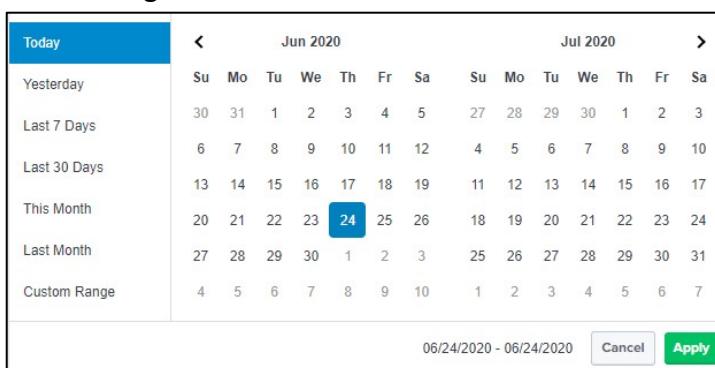


Open the Cisco Cloud Security App. You see the following tabs:

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.

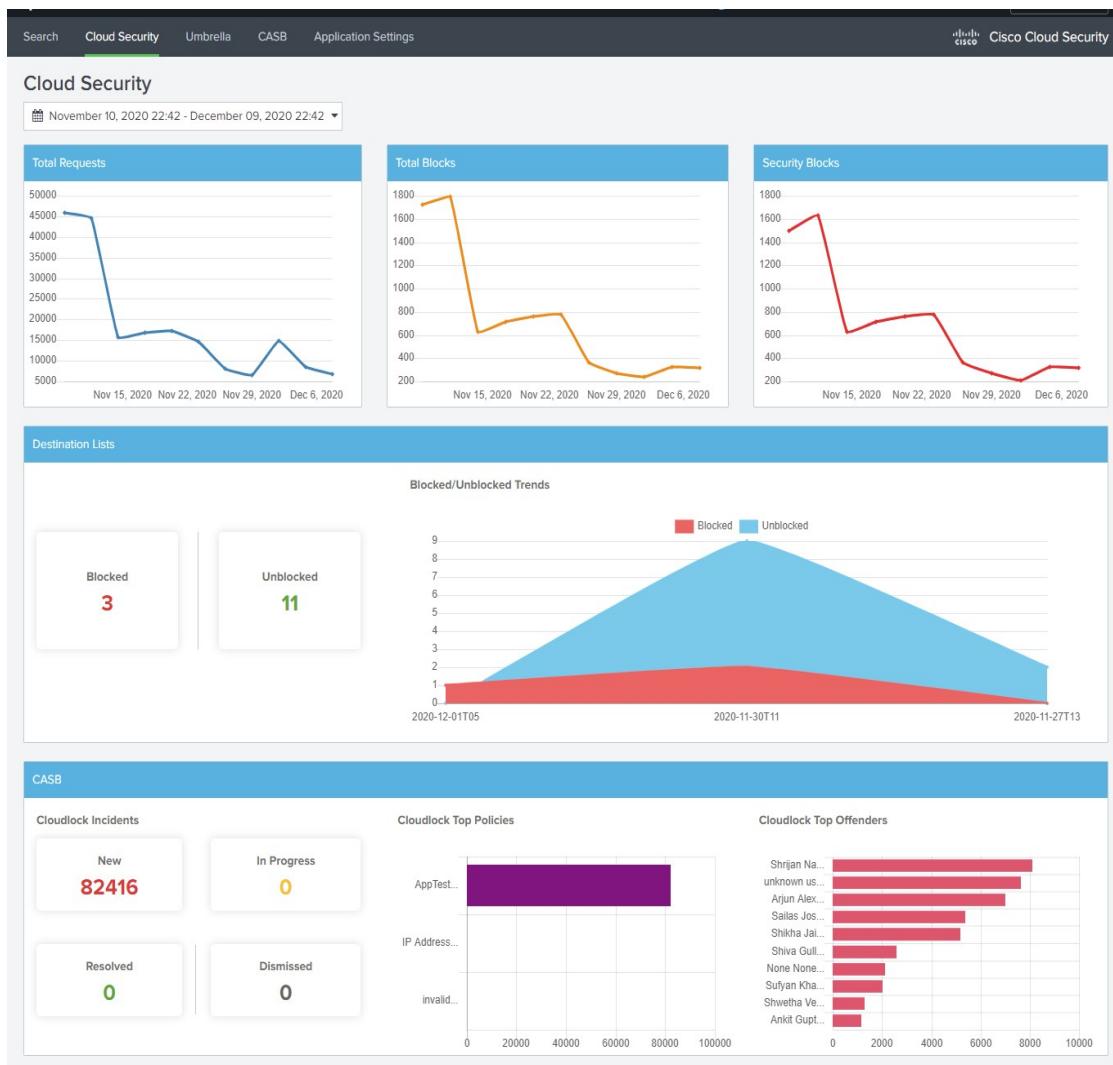


Note: The Time Range selector is available only in the dashboard.

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

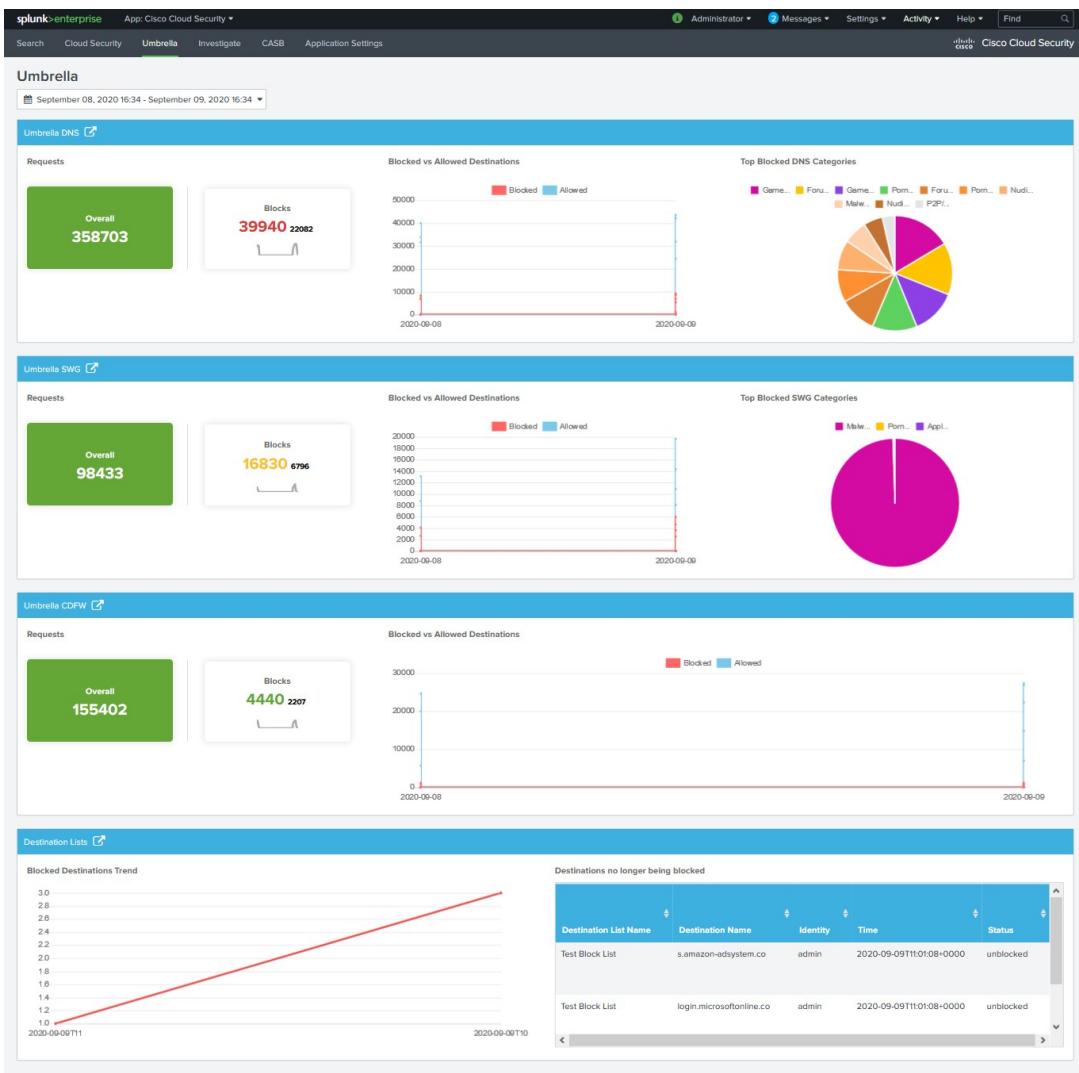
This section shows the Overall Request count, Blocked Requests for the selected time range and the equivalent previous time range, Block trend for the specified time, Blocked vs Allowed Destination, and Top Blocked SWG Categories.

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

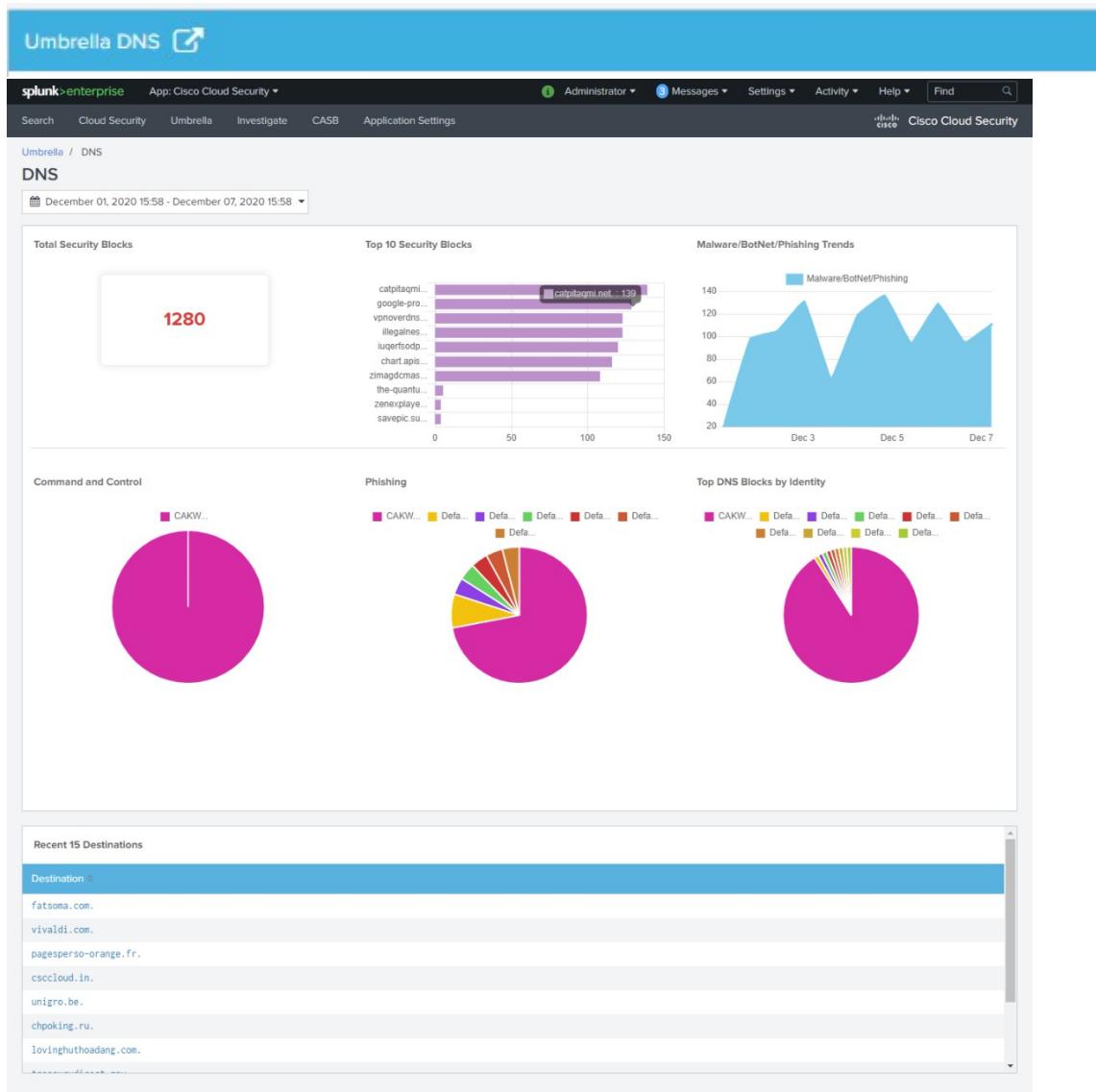
This section shows the Blocked Destination trend and Destinations no longer being blocked.



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

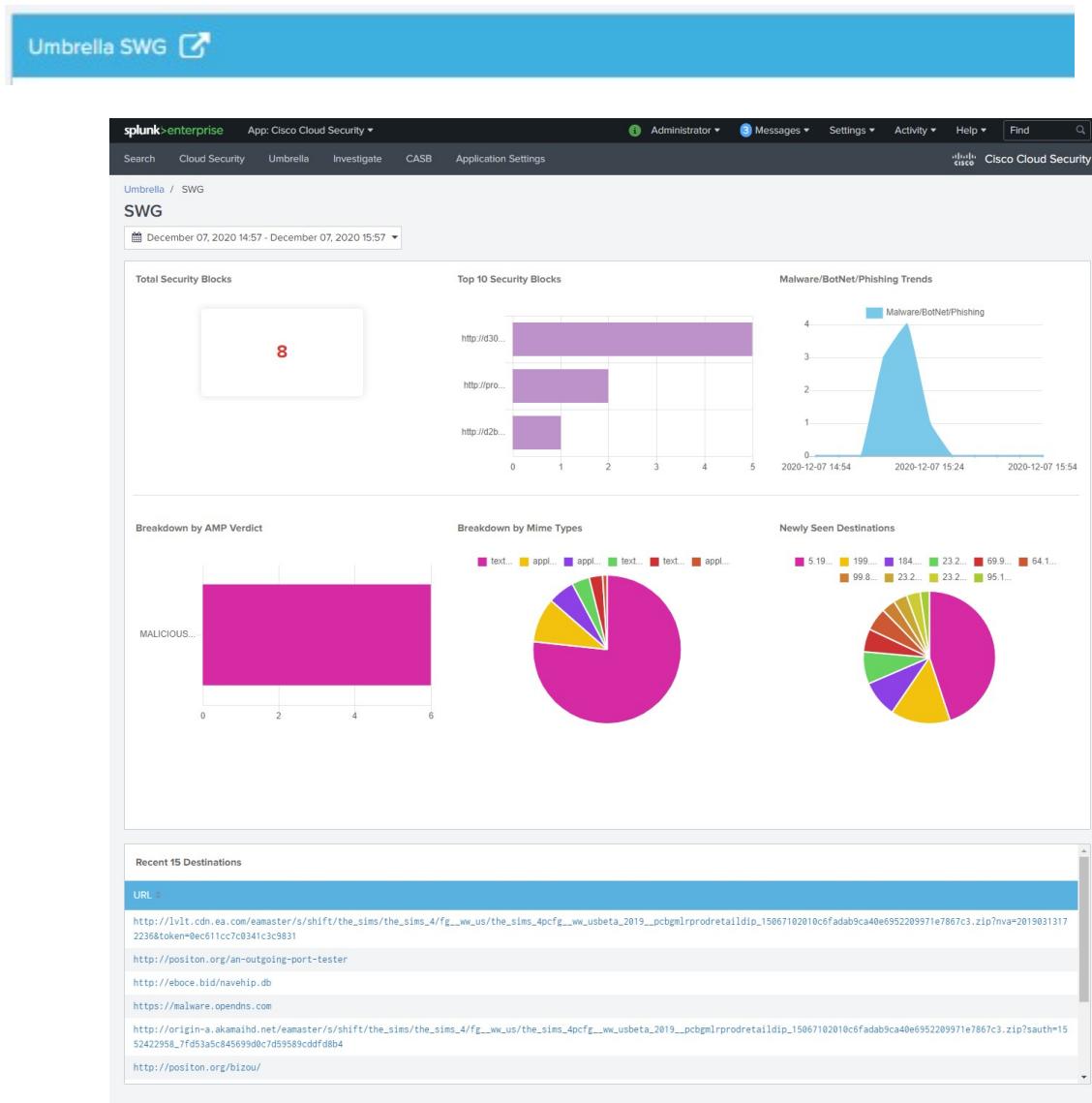
1.4.1. Cisco Umbrella DNS

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



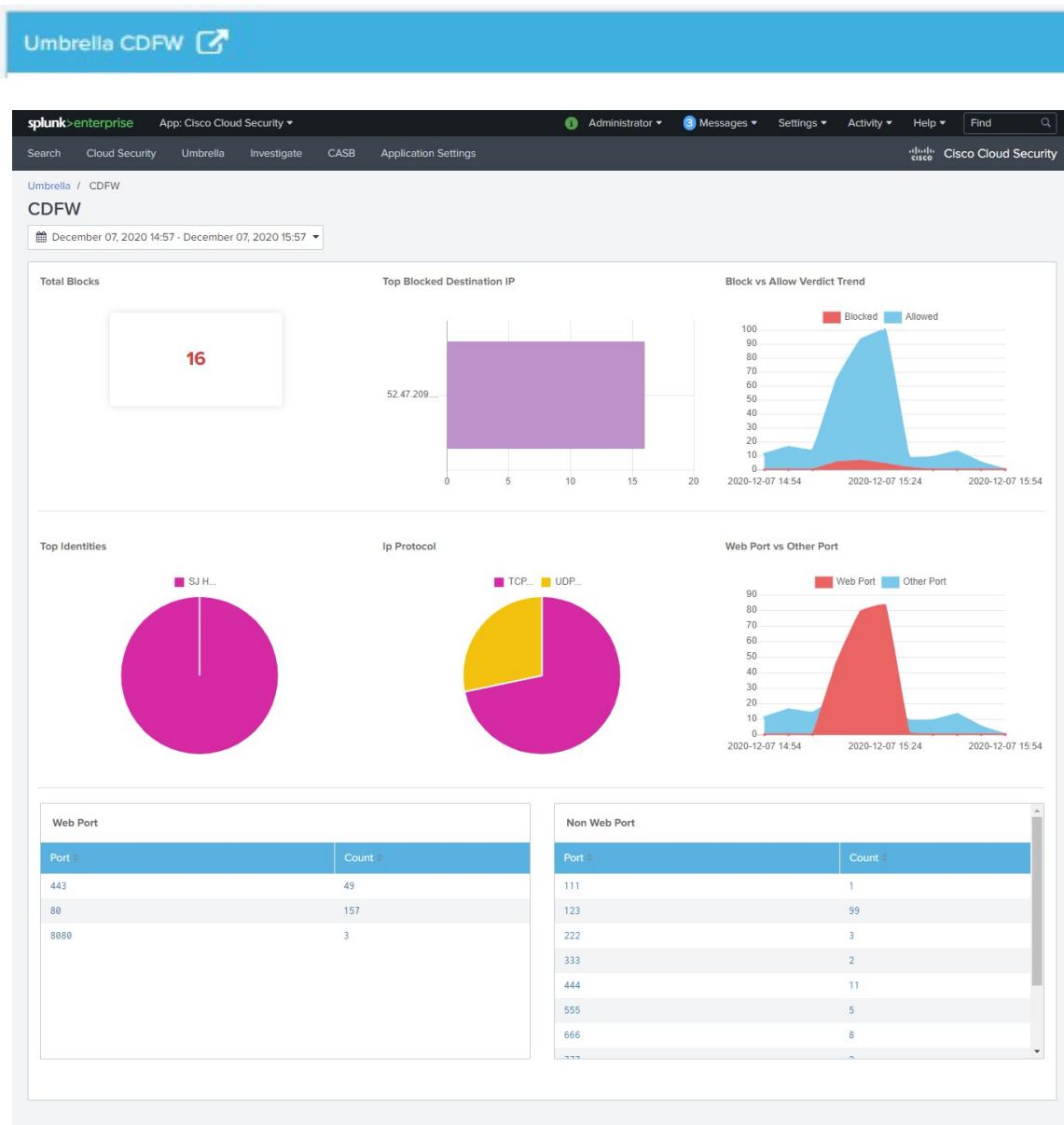
1.4.2. Cisco Umbrella SWG

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:

The screenshot shows the Splunk Enterprise interface with the "Destination Lists" dashboard. The top navigation bar includes "splunk>enterprise" and "App: Cisco Cloud Security". Below the navigation are links for "Search", "Cloud Security", "Umbrella", "Investigate", "CASB", and "Application Settings". The top right features "Administrator", "Messages", "Settings", "Activity", "Help", and a search bar. The main content area is titled "Destination Lists" with a blue header bar containing a red "X" icon. Below the header, the page title is "Umbrella / Destination Lists". The dashboard displays two sections: "Destinations Blocked" and "Destinations Unblocked".

Destinations Blocked

Select	Destination List Name	Destination Name	User Name	Action	Source	Time
<input type="checkbox"/>	Test Block List	jcxgqqqxf2ktkx2x3sla-po3qb2-9e68b5234-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.mnworldwide.co	admin	added	manual	2020-09-09T10:59:51+0000
<input type="checkbox"/>	Test Block List	vr.outbrain.co	admin	added	manual	2020-09-09T11:00:11+0000

Showing 1 to 4 of 4 entries

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

Showing 1 to 2 of 2 entries

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 a filter icon applied to the "Test Block List" entry. The table below shows the blocked destinations.

Select	Destination List Name	Destination Name	User Name	Action	Source	Time
<input type="checkbox"/>	Test Block List	jcxgqqqxf2ktkx2x3sla-po3qb2-9e68b5234-clientnsrv4-s.akamaihd.ne	admin	added	manual	2020-09-09T10:58:54+0000
<input checked="" type="checkbox"/>	Test Block List	smetrics.cnn.co	admin	added	manual	2020-09-09T10:59:05+0000
<input checked="" type="checkbox"/>	Test Block List	secure-origin.mnworldwide.co	admin	added	manual	2020-09-09T10:59:51+0000
<input type="checkbox"/>	Test Block List	vr.outbrain.co	admin	added	manual	2020-09-09T11:00:11+0000

Showing 1 to 4 of 4 entries

Unblock

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.

The screenshot shows the Splunk Enterprise web interface. At the top, there is a navigation bar with the following items: 'splunk>enterprise' (highlighted in green), 'Apps ▾' (highlighted in orange), and 'DEVTTEST:YARONCA@CISCO.COM'. Below the navigation bar, there is a horizontal menu with the following items: 'Search', 'Cloud Security', 'Umbrella', 'Investigate' (which is underlined in green, indicating it is the active tab), 'CASB', and 'Application Settings'. The main content area has a title 'Investigate' and two buttons: 'Investigate' (highlighted in blue) and 'Alert Destinations'. Below these buttons is a search bar with the placeholder text 'Search hostname, URL, ASN, IP, hash, or email address' and a magnifying glass icon.

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:

Id	Platform	Matches	Policy	CreatedAt	UpdatedAt	Source	Owner	Severity	Status	Actions
338378744	office365	1	AppTest	09-03-2020 06:20:55	09-03-2020 06:20:55	SharePoint File Accessed Extended	Pankaj Tanwar	CRITICAL	NEW	<button>Update</button>
338378741	office365	1	AppTest	09-03-2020 06:20:55	09-03-2020 06:20:55	SharePoint File Modified Extended	Pankaj Tanwar	CRITICAL	NEW	<button>Update</button>
338378740	office365	1	AppTest	09-03-2020 06:20:55	09-03-2020 06:20:55	SharePoint File Accessed	unknown user	CRITICAL	NEW	<button>Update</button>

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

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	Match Type	Match
09M 03, 2020	null	null

Raw Details

```
{"event_type": "UBEAA", "incident_status": "NEW", "ubeaa_data_set": [{"item": [{"raw": {"UserType": 0, "HighPriorityMediaProcessing": false, "UserId": "0217476a-51e0-44c1-863d-144902", "CorrelationId": "d237769f-0086-0000-383f-7a9d8dd70bb9", "Version": 1, "ItemType": "File", "CreationTime": "2020-09-03T00:14:12", "OrganizationId": "0217476e-8b1faf2", "SourceRelativeUrl": "Shared Documents/Incident Management"}}, "source": "SharePoint File Accessed", "owner": "Pankaj Tanwar", "severity": "CRITICAL", "status": "NEW"}]}
```

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	Search
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	Koppisetty Krishna	ALERT	DISMISS DISMISSED	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	IN PROGRESS NEW RESOLVED	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.

The screenshot shows the 'Create Alert' dialog box. At the top, there are trigger options: 'Once' and 'For each result'. Below that is a 'Throttle' checkbox. The main area is titled 'Trigger Actions' with a '+ Add Actions' button. Under 'When triggered', there is a section for 'Block The Destinations'. It includes a 'Field Name' input field with placeholder 'Enter Domain/URL/IP.' and a 'Destination List' dropdown menu. At the bottom right are 'Cancel' and 'Save' buttons.

Investigate the Destinations

To investigate the destination by type and field name:

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

The screenshot shows the 'Create Alert' dialog box. It has a 'Throttle' checkbox. The 'Trigger Actions' section has a '+ Add Actions' button. Under 'When triggered', there is a section for 'Investigate The Destinations'. It includes a 'Field Name' input field and a 'Type' dropdown menu. A sub-menu is open, showing 'Select' (which is checked) and three other options: 'Domain', 'Url', and 'IP'. At the bottom right are 'Cancel' and 'Save' buttons.

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.