WEBROOT®

BrightCloud Threat Intelligence App for Splunk

User Guide v1.5

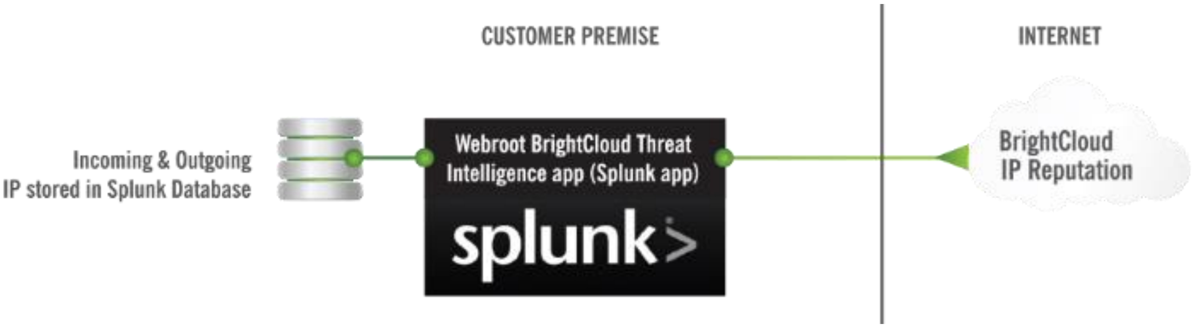
Table of Contents

Introduction

The Webroot BrightCloud Threat Intelligence App for Splunk is a predictive threat intelligence service that continuously monitors 4.3 billion IPs and identifies malicious IPs that enterprises should detect in their IP traffic and respond to quickly before those malicious IP activities lead to more costly security breaches.

The Webroot BrightCloud Threat Intelligence App for Splunk, hereafter known as the Splunk app, detects and alerts users of malicious IP activities in their infrastructure by doing the following:

- Regularly downloading the most up-to-date malicious IP database from BrightCloud.
- Comparing IP traffic logs stored inside Splunk against the malicious IP database downloaded from BrightCloud.
- Detecting and alerting users of malicious IP activities found in their IP traffic logs.


CUSTOMER PREMISE
INTERNET
Incoming & Outgoing
IP stored in Splunk Database
Webroot BrightCloud Threat
Intelligence app (Splunk app)
splunk>
BrightCloud
IP Reputation

Note: This document reflects information and images for Splunk Version 6.2.

Prerequisite

The Webroot BrightCloud Threat Intelligence app v1.5 supports Splunk Enterprise v6.0 and higher. The rest of the documentation assumes the user already has a Splunk Enterprise v6.0 or higher deployed and that the user has a valid userid to download apps from apps.splunk.com.

Installation and Configuration

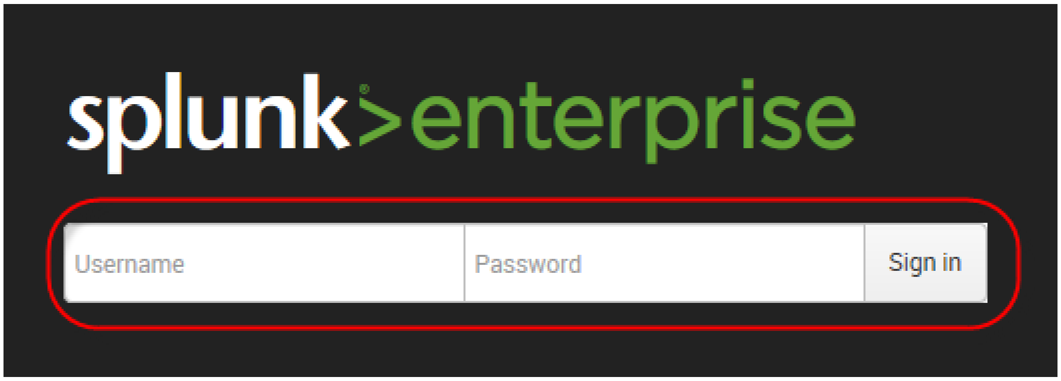
This document assumes that the user has already downloaded the Splunk app from apps.splunk.com. If not, please navigate your browser to apps.splunk.com, search for *Webroot BrightCloud Threat Intelligence* and download it to your local directory.

This section contains instructions on how to:

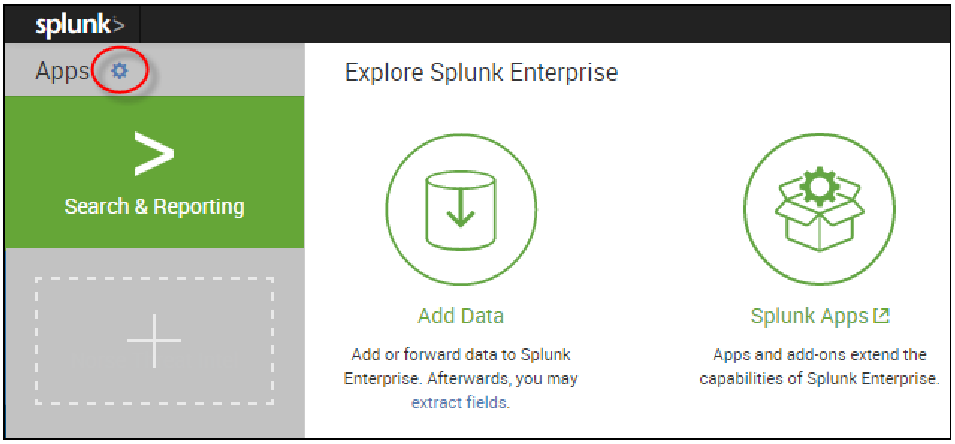
- Install and configure the Webroot BrightCloud Threat Intelligence app
- Uninstall the Webroot BrightCloud Threat Intelligence app

To install and configure the Webroot BrightCloud Threat Intelligence App for Splunk:

1. Log in to Splunk Web as administrator.



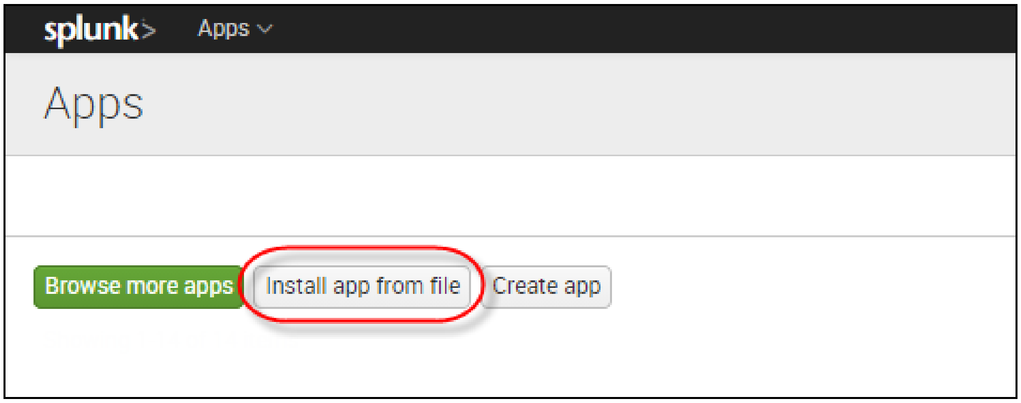
2. On the Home page, click the blue **Apps** icon.



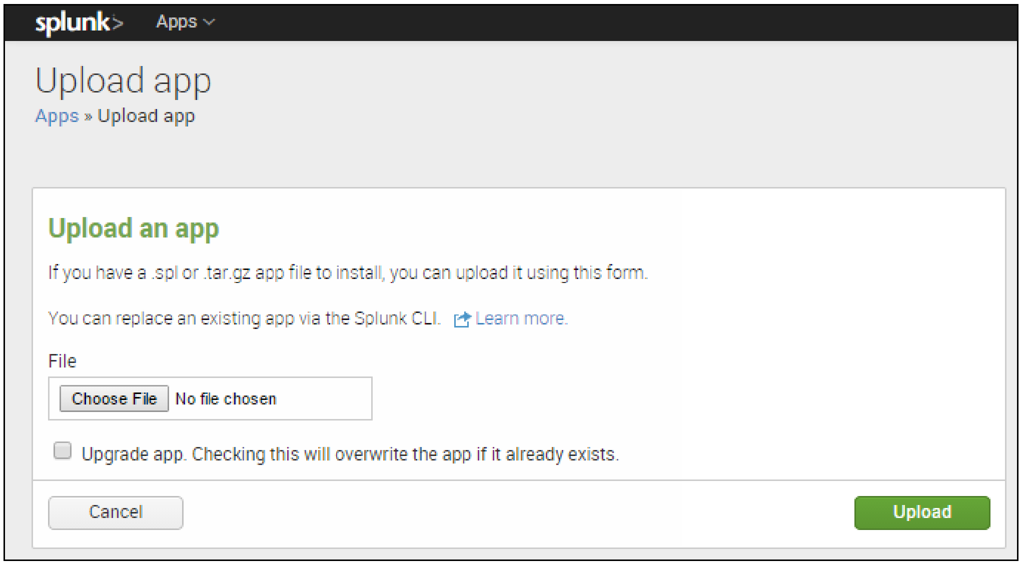
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

3. Click the **Install app from file** button.



The system displays the Upload app page.



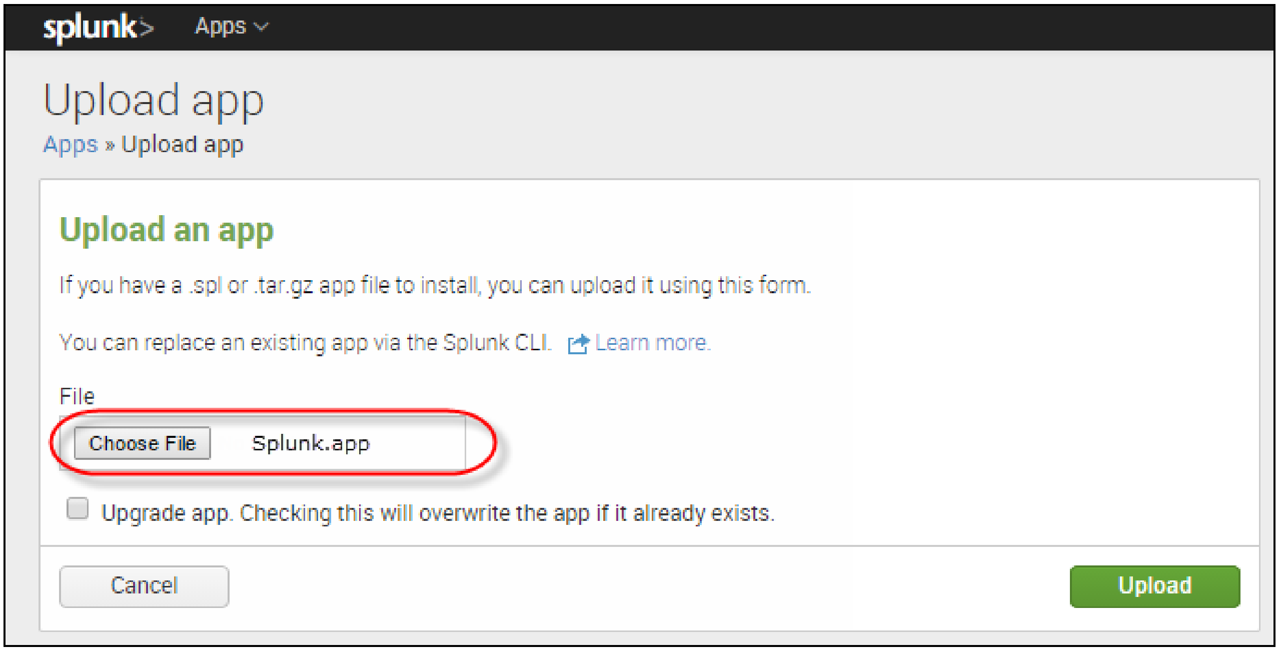
If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: No file chosen

□ Upgrade app. Checking this will overwrite the app if it already exists.

4. In the *File* field, click the **Choose File** button and browse to the file to select it.



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

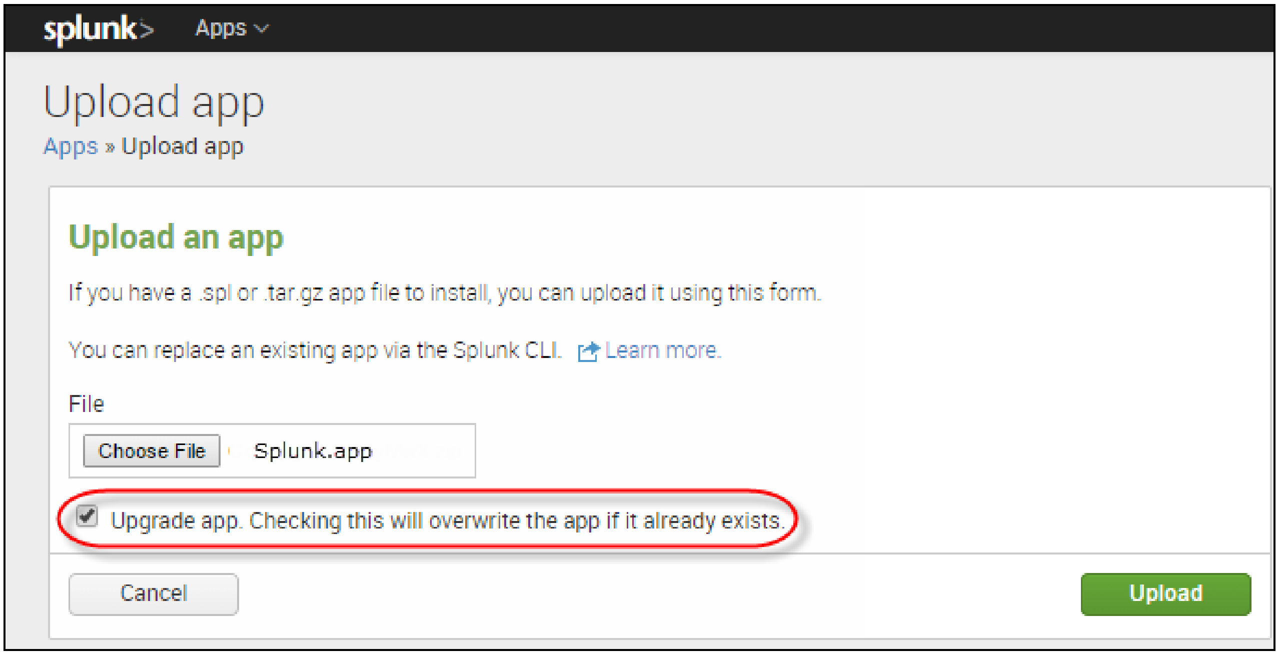
You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File Splunk.app

□ Upgrade app. Checking this will overwrite the app if it already exists.

5. Select the **Upgrade app** checkbox.



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

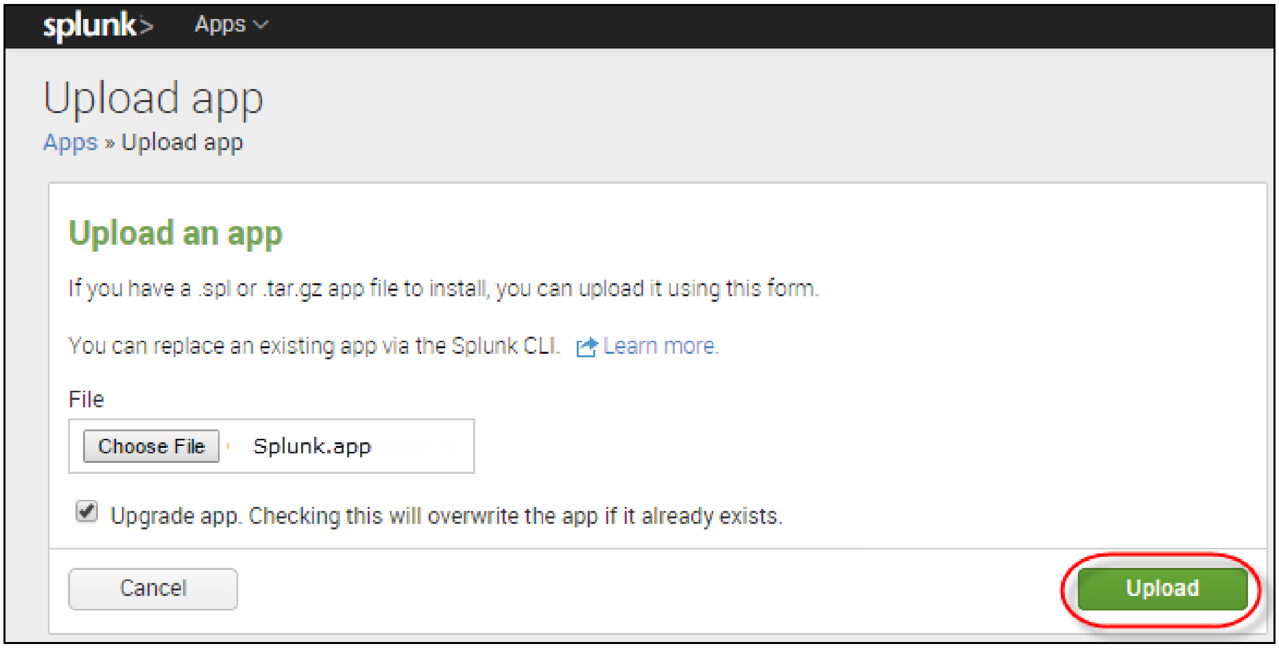
You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File Splunk.app

☑ Upgrade app. Checking this will overwrite the app if it already exists.

6. Click the **Upload** button.



Upload app

Apps » Upload app

Upload an app

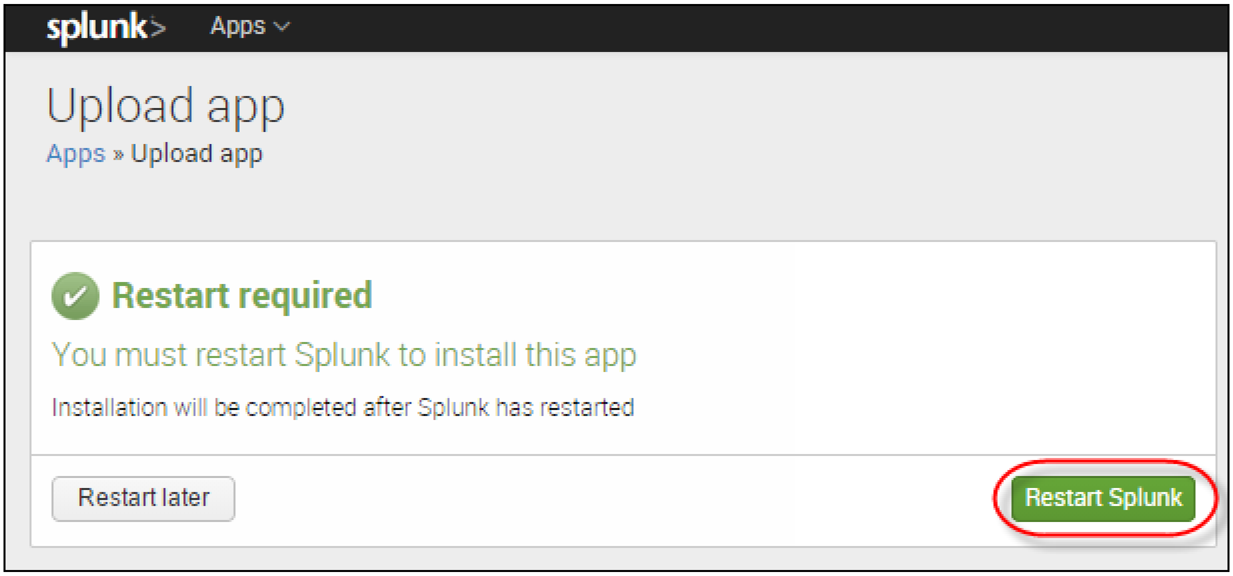
If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: Splunk.app

☑ Upgrade app. Checking this will overwrite the app if it already exists.

7. To complete the installation, click the **Restart Splunk** button.



Upload app

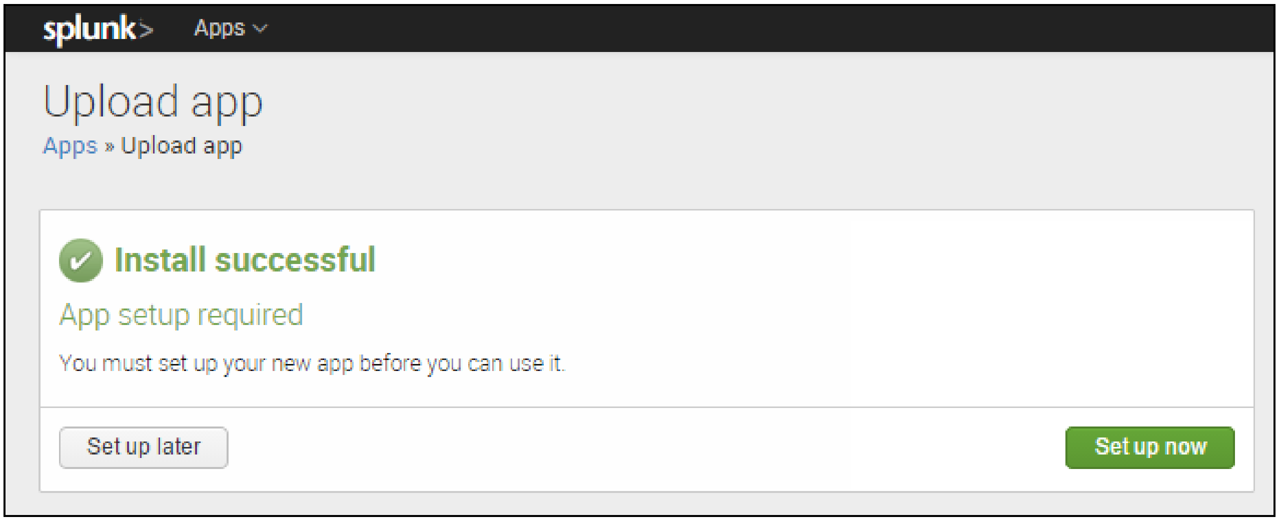
Apps » Upload app

Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted

The Install successful message displays.

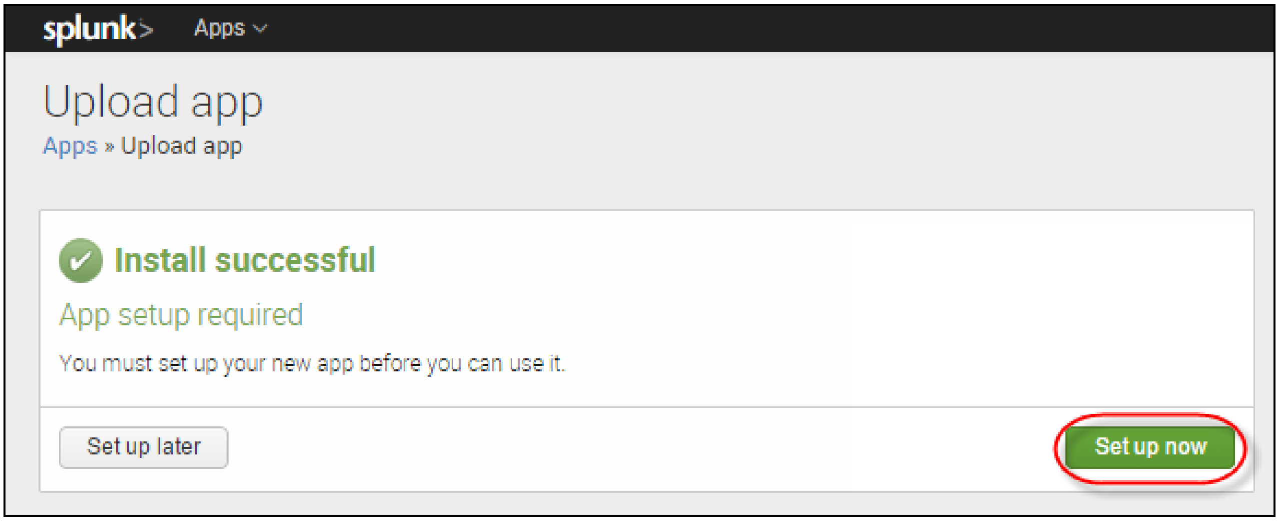


Install successful

App setup required

You must set up your new app before you can use it.

8. Click the **Set up now** button.

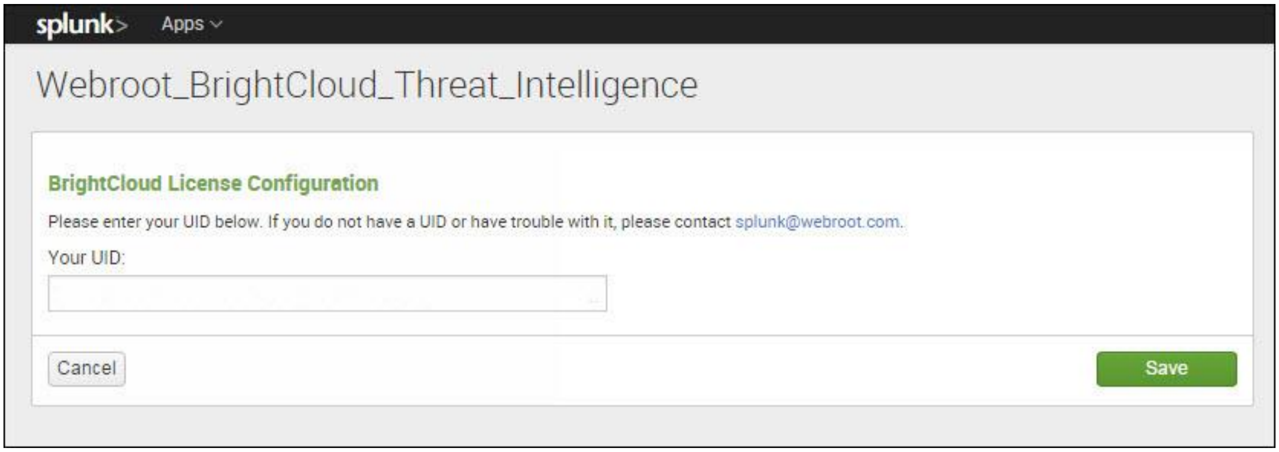


Install successful

App setup required

You must set up your new app before you can use it.

The system displays the Configuration window.



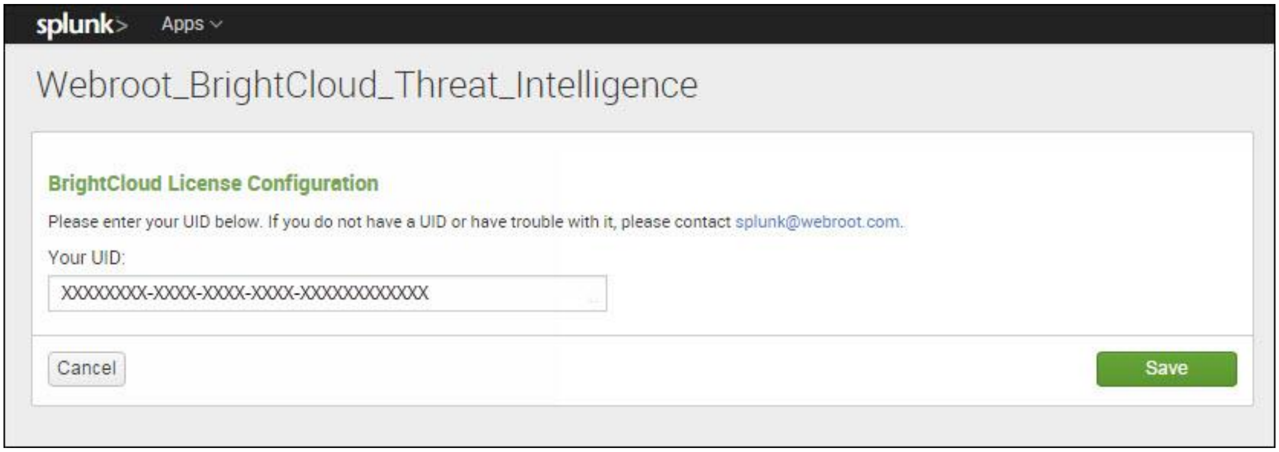
Webroot_BrightCloud_Threat_Intelligence

BrightCloud License Configuration

Please enter your UID below. If you do not have a UID or have trouble with it, please contact splunk@webroot.com.

Your UID:

9. In the field, enter your **UID**. This personal license key will be used during the update process.



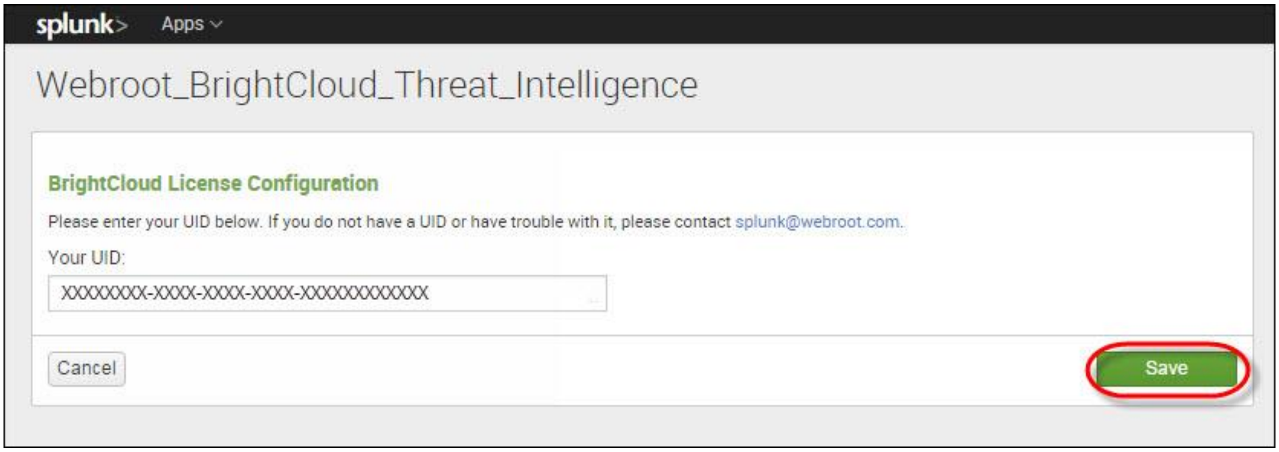
Webroot_BrightCloud_Threat_Intelligence

BrightCloud License Configuration

Please enter your UID below. If you do not have a UID or have trouble with it, please contact splunk@webroot.com.

Your UID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

10. Click the **Save** button.



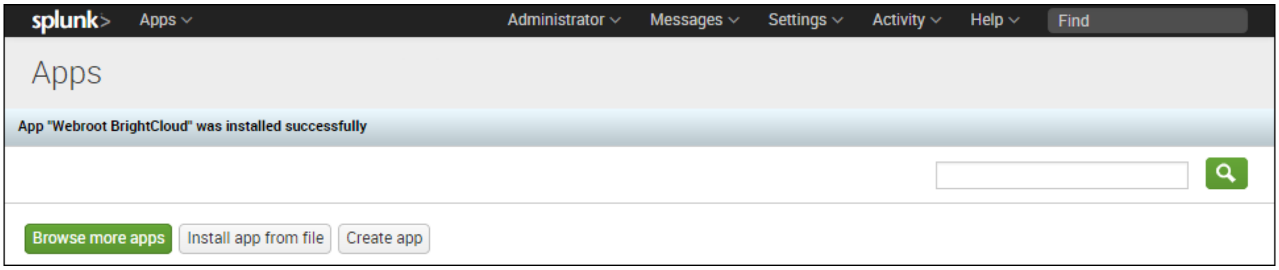
Webroot_BrightCloud_Threat_Intelligence

BrightCloud License Configuration

Please enter your UID below. If you do not have a UID or have trouble with it, please contact splunk@webroot.com.

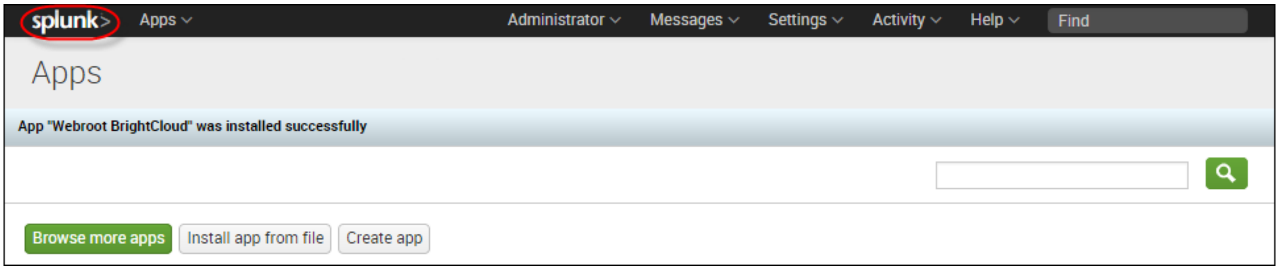
Your UID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

The system displays the Manage Apps window. The message in the upper left of the window indicates whether the app was successfully installed.



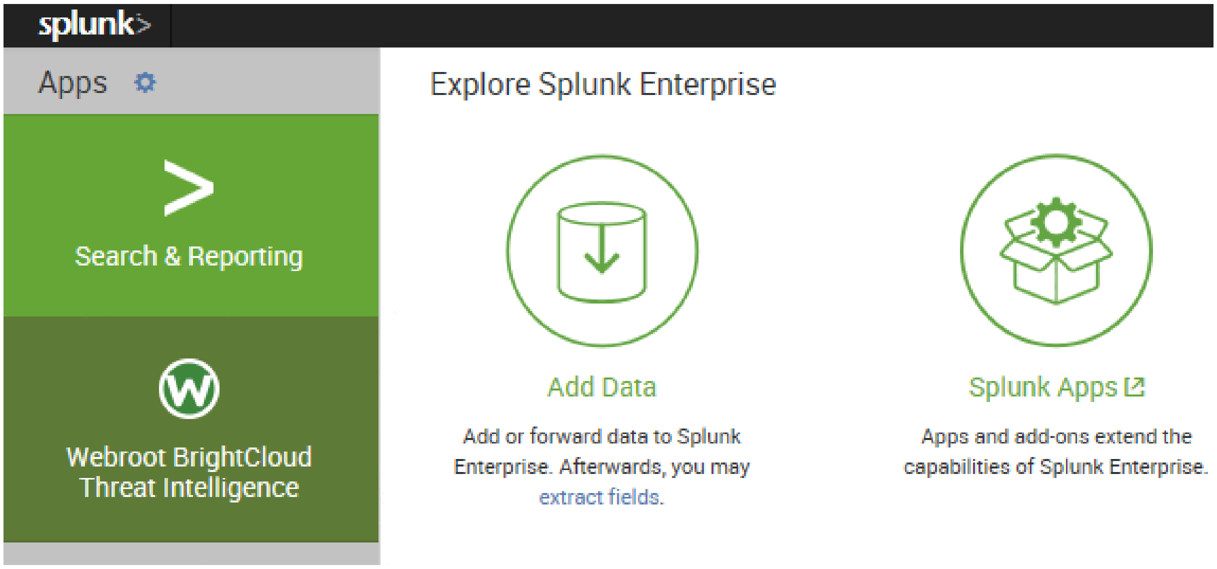
App "Webroot BrightCloud" was installed successfully

11.Click the **Splunk** link.



App "Webroot BrightCloud" was installed successfully

The system displays the Home page, with the icon for the Webroot BrightCloud app in the left column.

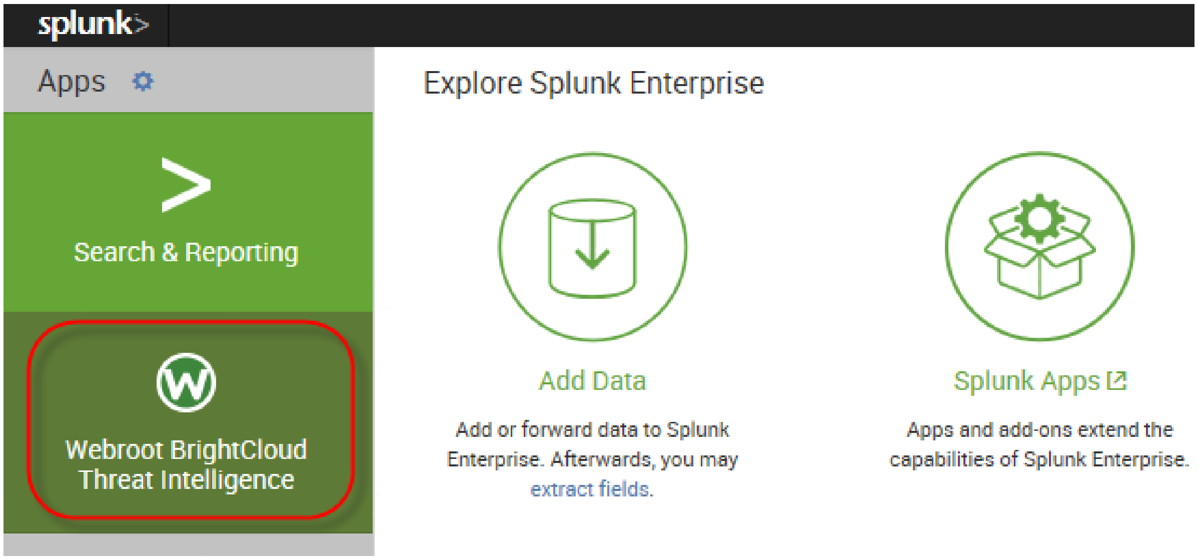


Explore Splunk Enterprise

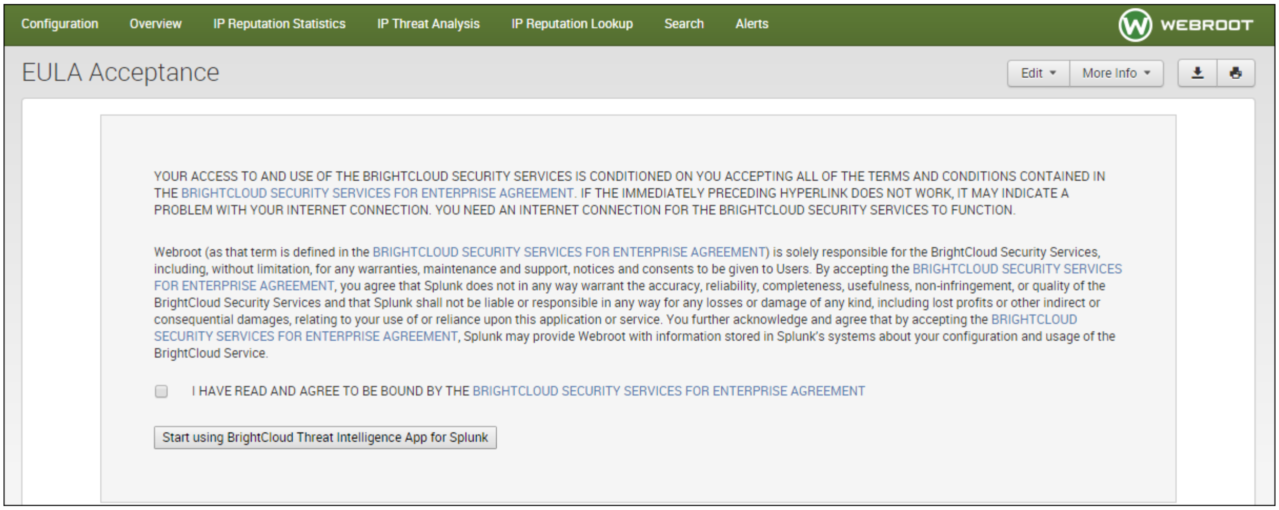
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

12. Click the **Webroot BrightCloud** icon.


splunk>
Apps
Explore Splunk Enterprise
Search & Reporting
Webroot BrightCloud Threat Intelligence
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

The first time you click the Webroot BrightCloud icon, the system displays the EULA Acceptance page.



EULA Acceptance

YOUR ACCESS TO AND USE OF THE BRIGHTCLOUD SECURITY SERVICES IS CONDITIONED ON YOU ACCEPTING ALL OF THE TERMS AND CONDITIONS CONTAINED IN THE BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT. IF THE IMMEDIATELY PRECEDING HYPERLINK DOES NOT WORK, IT MAY INDICATE A PROBLEM WITH YOUR INTERNET CONNECTION. YOU NEED AN INTERNET CONNECTION FOR THE BRIGHTCLOUD SECURITY SERVICES TO FUNCTION.

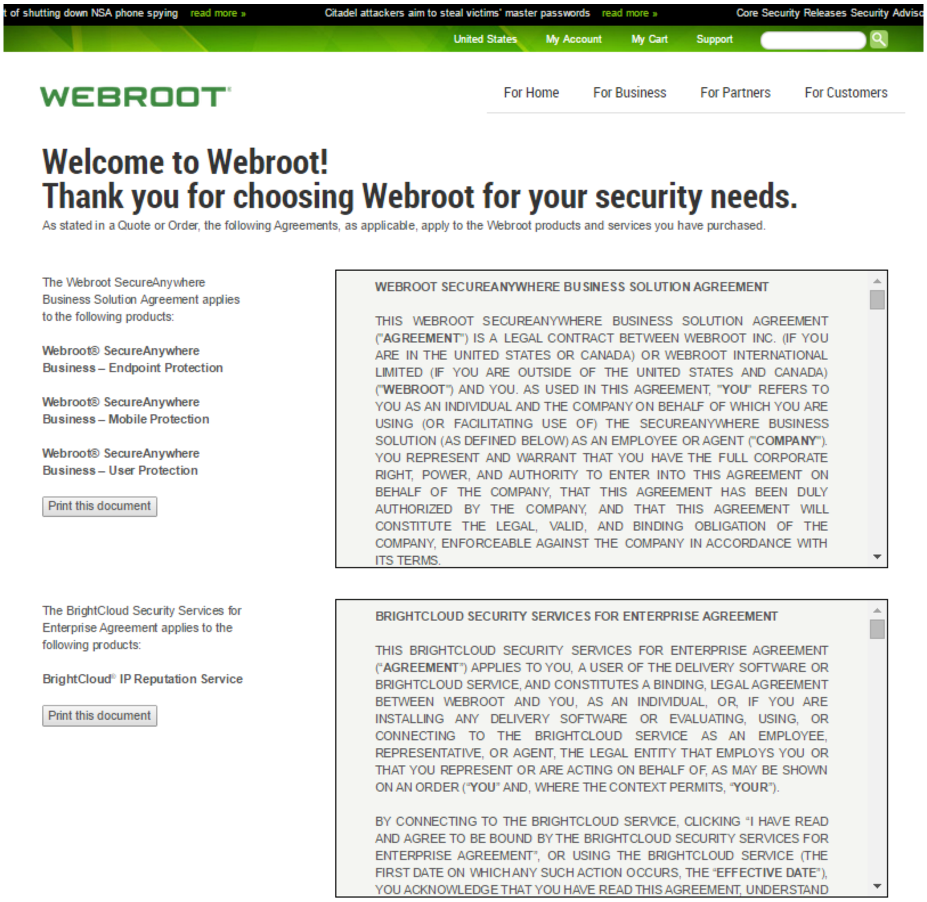
Webroot (as that term is defined in the BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT) is solely responsible for the BrightCloud Security Services, including, without limitation, for any warranties, maintenance and support, notices and consents to be given to Users. By accepting the BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT, you agree that Splunk does not in any way warrant the accuracy, reliability, completeness, usefulness, non-infringement, or quality of the BrightCloud Security Services and that Splunk shall not be liable or responsible in any way for any losses or damage of any kind, including lost profits or other indirect or consequential damages, relating to your use of or reliance upon this application or service. You further acknowledge and agree that by accepting the BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT, Splunk may provide Webroot with information stored in Splunk's systems about your configuration and usage of the BrightCloud Service.

☐ I HAVE READ AND AGREE TO BE BOUND BY THE BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT

Start using BrightCloud Threat Intelligence App for Splunk

13. Optionally, you can click the **BrightCloud Security Services for Enterprise Agreement** link and review the EULA Acceptance document.

    The system displays the Welcome to Webroot! Page, where you can review the EULA agreement.


t of shutting down NSA phone spying read more »
Citadel attackers aim to steal victims' master passwords read more »
Core Security Releases Security Adviso
United States
My Account
My Cart
Support
WEBROOT
For Home
For Business
For Partners
For Customers
Print this document
Print this document

Welcome to Webroot!
Thank you for choosing Webroot for your security needs.

As stated in a Quote or Order, the following Agreements, as applicable, apply to the Webroot products and services you have purchased.

The Webroot SecureAnywhere Business Solution Agreement applies to the following products:

Webroot® SecureAnywhere Business – Endpoint Protection

Webroot® SecureAnywhere Business – Mobile Protection

Webroot® SecureAnywhere Business – User Protection

WEBROOT SECUREANYWHERE BUSINESS SOLUTION AGREEMENT

THIS WEBROOT SECUREANYWHERE BUSINESS SOLUTION AGREEMENT ("**AGREEMENT**") IS A LEGAL CONTRACT BETWEEN WEBROOT INC. (IF YOU ARE IN THE UNITED STATES OR CANADA) OR WEBROOT INTERNATIONAL LIMITED (IF YOU ARE OUTSIDE OF THE UNITED STATES AND CANADA) ("**WEBROOT**") AND YOU. AS USED IN THIS AGREEMENT, "**YOU**" REFERS TO YOU AS AN INDIVIDUAL AND THE COMPANY ON BEHALF OF WHICH YOU ARE USING (OR FACILITATING USE OF) THE SECUREANYWHERE BUSINESS SOLUTION (AS DEFINED BELOW) AS AN EMPLOYEE OR AGENT ("**COMPANY**"). YOU REPRESENT AND WARRANT THAT YOU HAVE THE FULL CORPORATE RIGHT, POWER, AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THE COMPANY, THAT THIS AGREEMENT HAS BEEN DULY AUTHORIZED BY THE COMPANY, AND THAT THIS AGREEMENT WILL CONSTITUTE THE LEGAL, VALID, AND BINDING OBLIGATION OF THE COMPANY, ENFORCEABLE AGAINST THE COMPANY IN ACCORDANCE WITH ITS TERMS.

The BrightCloud Security Services for Enterprise Agreement applies to the following products:

BrightCloud® IP Reputation Service

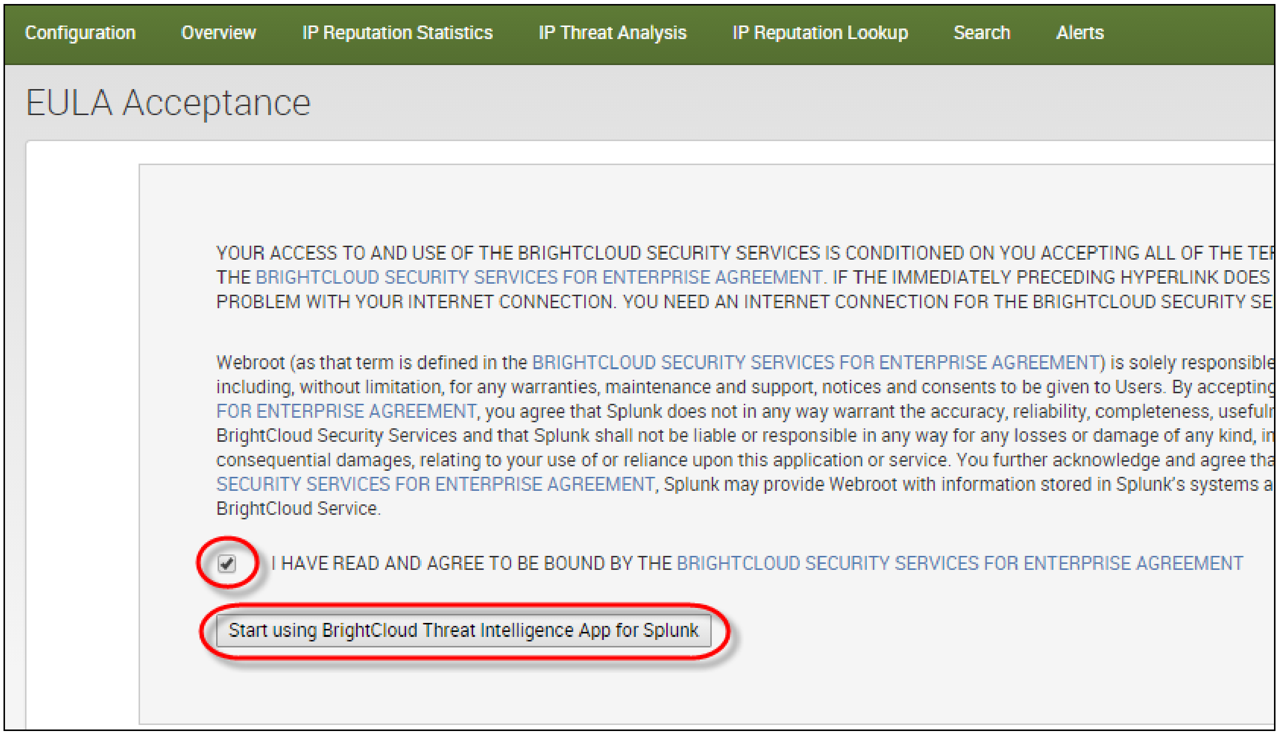
BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT

THIS BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT ("**AGREEMENT**") APPLIES TO YOU, A USER OF THE DELIVERY SOFTWARE OR BRIGHTCLOUD SERVICE, AND CONSTITUTES A BINDING, LEGAL AGREEMENT BETWEEN WEBROOT AND YOU, AS AN INDIVIDUAL, OR, IF YOU ARE INSTALLING ANY DELIVERY SOFTWARE OR EVALUATING, USING, OR CONNECTING TO THE BRIGHTCLOUD SERVICE AS AN EMPLOYEE, REPRESENTATIVE, OR AGENT, THE LEGAL ENTITY THAT EMPLOYS YOU OR THAT YOU REPRESENT OR ARE ACTING ON BEHALF OF, AS MAY BE SHOWN ON AN ORDER ("**YOU**" AND, WHERE THE CONTEXT PERMITS, "**YOUR**").

BY CONNECTING TO THE BRIGHTCLOUD SERVICE, CLICKING "I HAVE READ AND AGREE TO BE BOUND BY THE BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT", OR USING THE BRIGHTCLOUD SERVICE (THE FIRST DATE ON WHICH ANY SUCH ACTION OCCURS, THE "**EFFECTIVE DATE**"), YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND

Note: If you do click the link, click the **Splunk** tab in your browser to return to the EULA Acceptance page.

14. Select the checkbox, then click the **Start using Webroot BrightCloud Threat Intelligence App for Splunk** button.



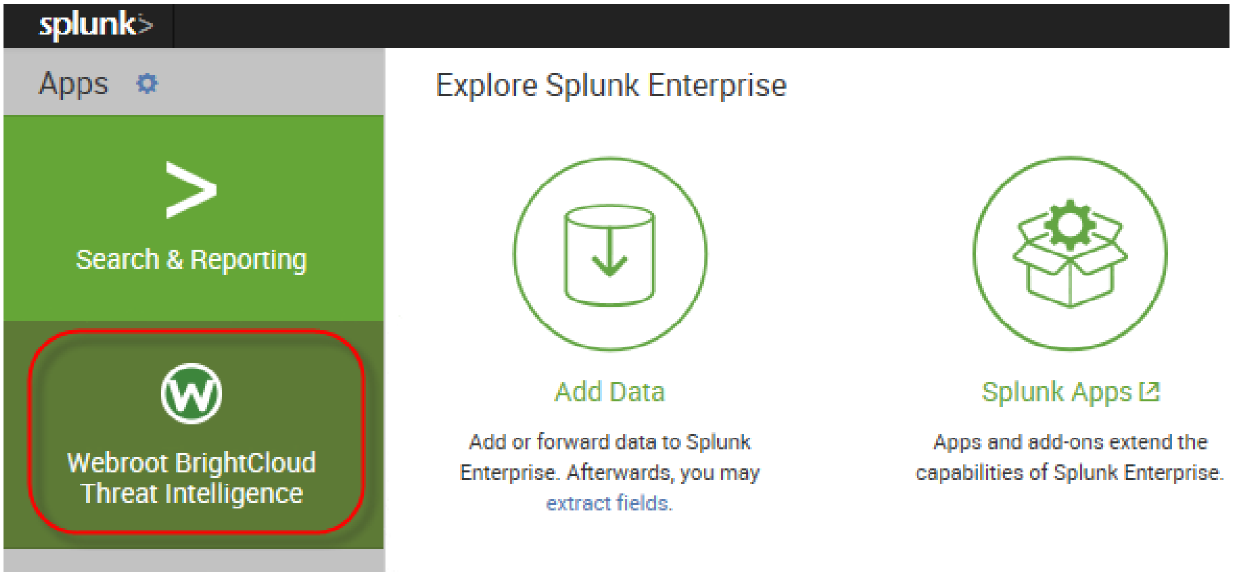
EULA Acceptance

YOUR ACCESS TO AND USE OF THE BRIGHTCLOUD SECURITY SERVICES IS CONDITIONED ON YOU ACCEPTING ALL OF THE TEI
THE BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT. IF THE IMMEDIATELY PRECEDING HYPERLINK DOES
PROBLEM WITH YOUR INTERNET CONNECTION. YOU NEED AN INTERNET CONNECTION FOR THE BRIGHTCLOUD SECURITY SE

Webroot (as that term is defined in the BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT) is solely responsible
including, without limitation, for any warranties, maintenance and support, notices and consents to be given to Users. By accepting
FOR ENTERPRISE AGREEMENT, you agree that Splunk does not in any way warrant the accuracy, reliability, completeness, usefulr
BrightCloud Security Services and that Splunk shall not be liable or responsible in any way for any losses or damage of any kind, ir
consequential damages, relating to your use of or reliance upon this application or service. You further acknowledge and agree tha
SECURITY SERVICES FOR ENTERPRISE AGREEMENT, Splunk may provide Webroot with information stored in Splunk's systems a
BrightCloud Service.

☑ I HAVE READ AND AGREE TO BE BOUND BY THE BRIGHTCLOUD SECURITY SERVICES FOR ENTERPRISE AGREEMENT

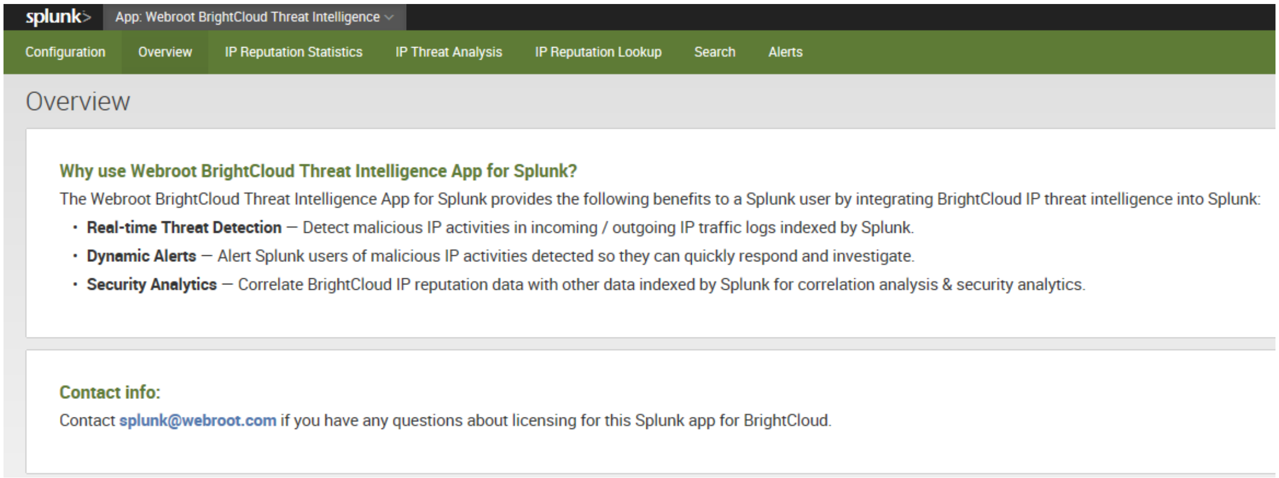
15. When you are ready, return to the Splunk page, and click the Webroot BrightCloud icon.


splunk>
Apps
Explore Splunk Enterprise
Search & Reporting
Webroot BrightCloud Threat Intelligence
Add Data
Splunk Apps

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

The system displays the Overview page, where you can access additional functionality.



Overview

Why use Webroot BrightCloud Threat Intelligence App for Splunk?

The Webroot BrightCloud Threat Intelligence App for Splunk provides the following benefits to a Splunk user by integrating BrightCloud IP threat intelligence into Splunk:

- **Real-time Threat Detection** – Detect malicious IP activities in incoming / outgoing IP traffic logs indexed by Splunk.
- **Dynamic Alerts** – Alert Splunk users of malicious IP activities detected so they can quickly respond and investigate.
- **Security Analytics** – Correlate BrightCloud IP reputation data with other data indexed by Splunk for correlation analysis & security analytics.

Contact info:

Contact splunk@webroot.com if you have any questions about licensing for this Splunk app for BrightCloud.

To uninstall the Webroot BrightCloud Threat Intelligence App for Splunk:

1. Remove the app or add-on's indexed data.

   Typically, Splunk does not access indexed data from a deleted app or add-on. However, you can use Splunk's CLI clean command to remove indexed data from an app before deleting the app. For more information, see Remove data from indexes with the CLI command.

   Note: This is an optional step.

2. Delete the app and its directory. This should be located here:

   ```
   $SPLUNK_HOME/etc/apps/<appname>
   ```

   You can run the following command in the CLI:

   ```
   /splunk remove app [appname] -auth <username>:<password>
   ```

3. You may need to remove user-specific directories created for your app or add-on by deleting the files, if any, found here:

   ```
   $SPLUNK_HOME/splunk/etc/users/*/<appname>
   ```

4. Restart Splunk.

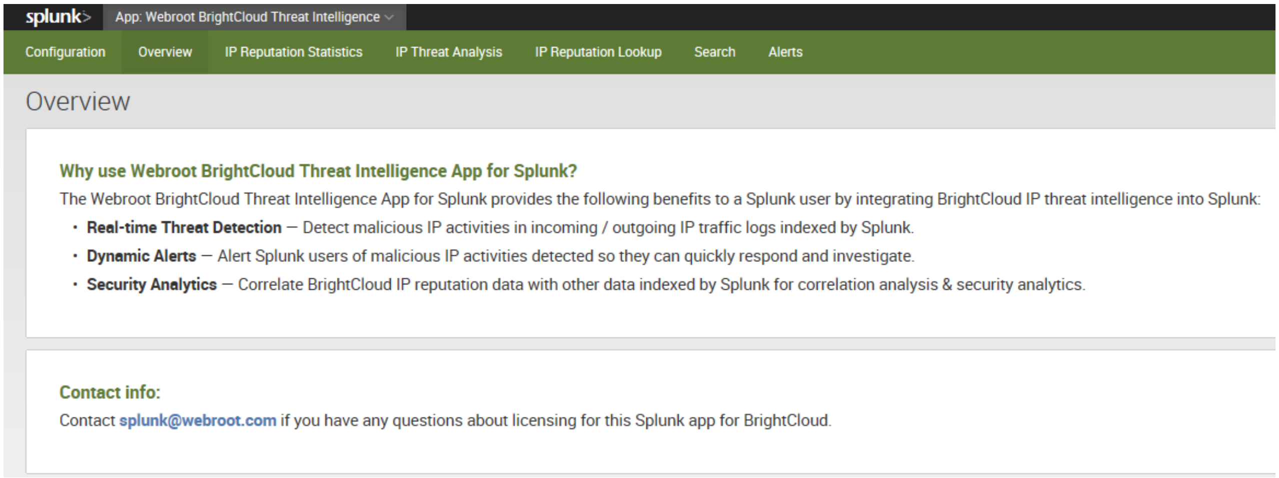
How To Use

The app consists of several dashboards, which are described in this section.

Overview

The Overview tab displays the following information:

- The email address where you can contact Webroot to upgrade your license.
- A description of the Splunk app.



Overview

Why use Webroot BrightCloud Threat Intelligence App for Splunk?

The Webroot BrightCloud Threat Intelligence App for Splunk provides the following benefits to a Splunk user by integrating BrightCloud IP threat intelligence into Splunk:

- **Real-time Threat Detection** — Detect malicious IP activities in incoming / outgoing IP traffic logs indexed by Splunk.
- **Dynamic Alerts** — Alert Splunk users of malicious IP activities detected so they can quickly respond and investigate.
- **Security Analytics** — Correlate BrightCloud IP reputation data with other data indexed by Splunk for correlation analysis & security analytics.

Contact info:

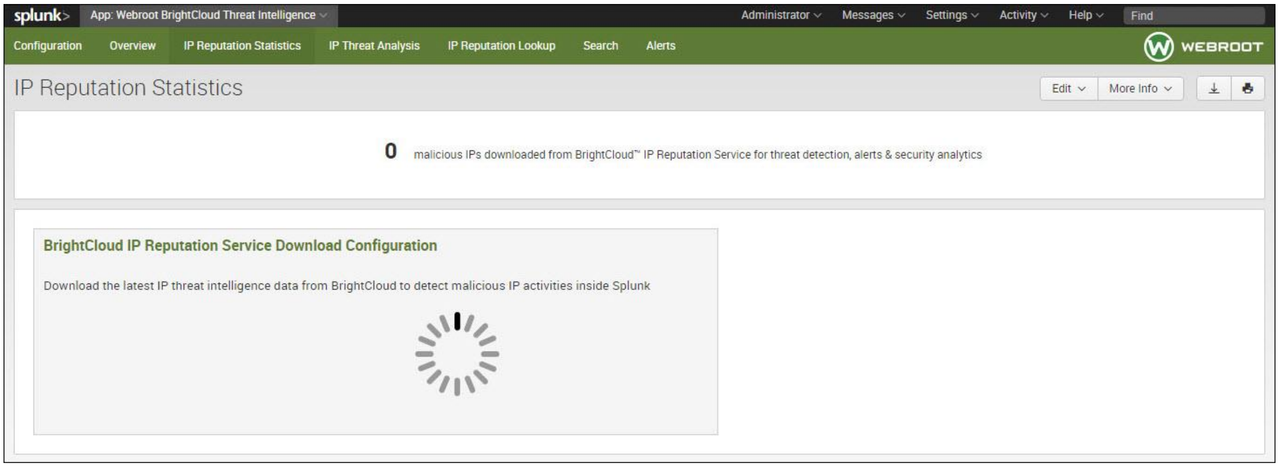
Contact splunk@webroot.com if you have any questions about licensing for this Splunk app for BrightCloud.

IP Reputation Statistics

The Splunk app needs to first download the list of millions of malicious IPs from the BrightCloud IP Reputation Service to a local IP reputation database. It will then regularly update the local IP reputation database with updates from BrightCloud. The local IP reputation database is used to correlate against log files indexed by Splunk and detect malicious IP activities.

The IP Reputation Statistics tab displays information about the local IP reputation database:

- The number of IP addresses contained in the database that have been downloaded from BrightCloud Threat Intelligence Service.
- The version number and the build date.



IP Reputation Statistics

0 malicious IPs downloaded from BrightCloud™ IP Reputation Service for threat detection, alerts & security analytics

BrightCloud IP Reputation Service Download Configuration

Download the latest IP threat intelligence data from BrightCloud to detect malicious IP activities inside Splunk

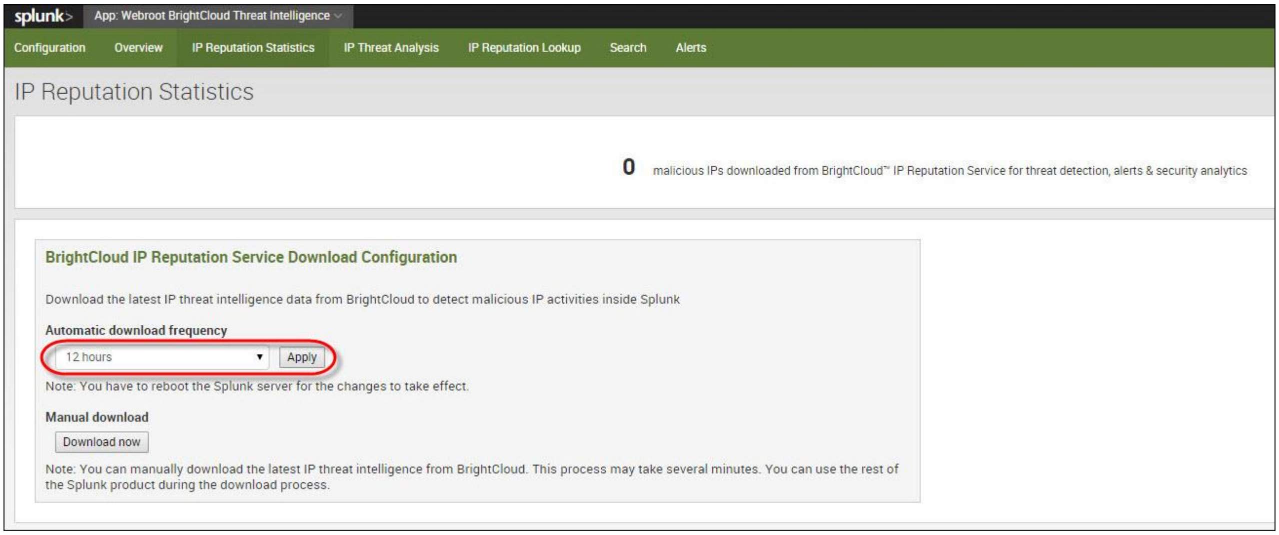
To download the first version of the IP reputation database:

1. Do either of the following:

   - From the *Automatic download frequency* drop-down menu, select a frequency and then click the **Apply** button. This will trigger the initial download and creation of the local IP reputation database as well as subsequent regular updates to it. After installation, you can define the update frequency of the TI db by setting the frequency from the *Automatic download frequency* drop-down menu.

     The first and initial download starts after the defined period of time of the download frequency; for example, if you select the 12 hour period, the download will run at 12 am and 12 pm every day.

     If you don't want to wait for the scheduled download, we recommend that you manually download the TI db, and you will be able to start working with our app immediately.



IP Reputation Statistics

0 malicious IPs downloaded from BrightCloud™ IP Reputation Service for threat detection, alerts & security analytics

BrightCloud IP Reputation Service Download Configuration

Download the latest IP threat intelligence data from BrightCloud to detect malicious IP activities inside Splunk

Automatic download frequency

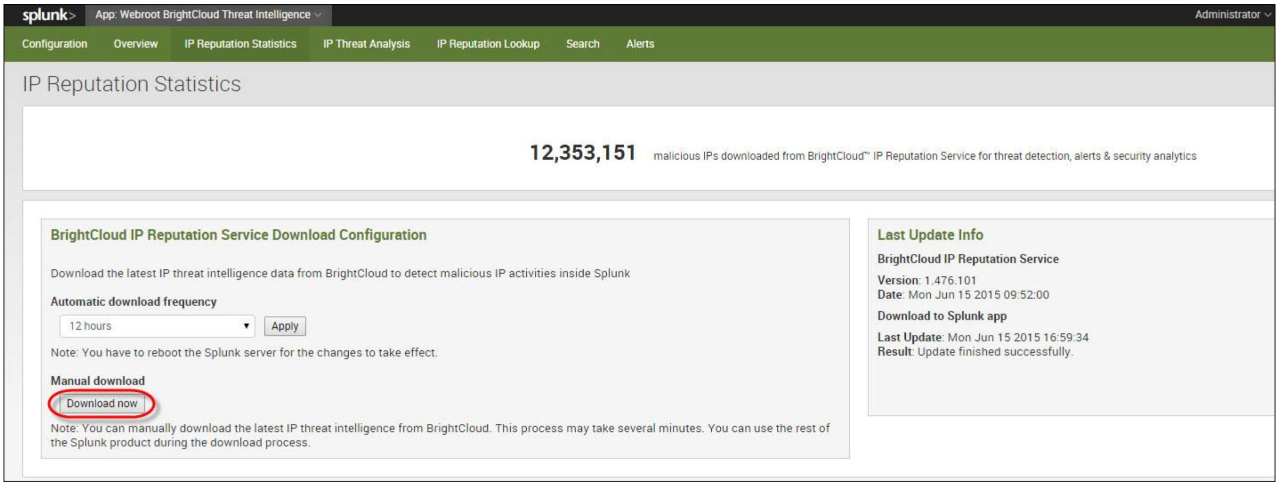
12 hours

Note: You have to reboot the Splunk server for the changes to take effect.

Manual download

Note: You can manually download the latest IP threat intelligence from BrightCloud. This process may take several minutes. You can use the rest of the Splunk product during the download process.

- To manually trigger the download of the latest data from BrightCloud IP Reputation Service to the local IP reputation database, click the **Download now** button. Please note that this is a one-time operation. To set up regular update of the local IP reputation database, select a frequency from the *Automatic download frequency* drop-down menu.



IP Reputation Statistics

12,353,151 malicious IPs downloaded from BrightCloud™ IP Reputation Service for threat detection, alerts & security analytics

BrightCloud IP Reputation Service Download Configuration

Download the latest IP threat intelligence data from BrightCloud to detect malicious IP activities inside Splunk

Automatic download frequency

12 hours

Note: You have to reboot the Splunk server for the changes to take effect.

Manual download

Note: You can manually download the latest IP threat intelligence from BrightCloud. This process may take several minutes. You can use the rest of the Splunk product during the download process.

Last Update Info

BrightCloud IP Reputation Service

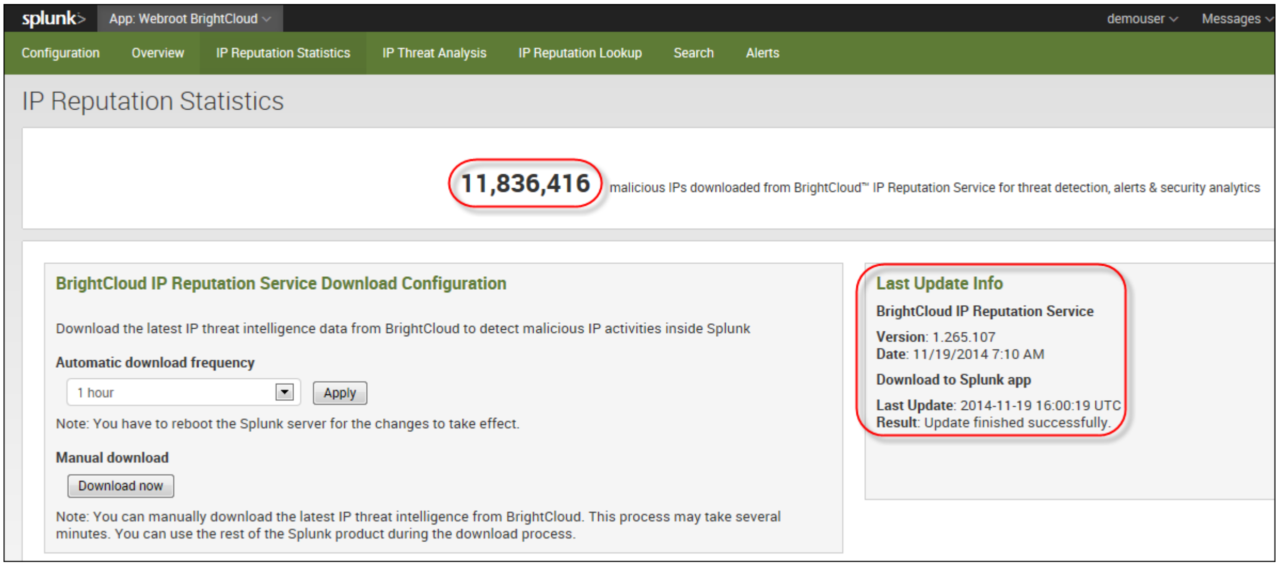
Version: 1.476.101
Date: Mon Jun 15 2015 09:52:00

Download to Splunk app

Last Update: Mon Jun 15 2015 16:59:34
Result: Update finished successfully.

The system displays the following information:

- The number of IP addresses contained in the database that have been downloaded from BrightCloud IP Reputation Service.
- The version number and the build date.



IP Reputation Statistics

11,836,416 malicious IPs downloaded from BrightCloud™ IP Reputation Service for threat detection, alerts & security analytics

BrightCloud IP Reputation Service Download Configuration

Download the latest IP threat intelligence data from BrightCloud to detect malicious IP activities inside Splunk

Automatic download frequency

1 hour

Note: You have to reboot the Splunk server for the changes to take effect.

Manual download

Note: You can manually download the latest IP threat intelligence from BrightCloud. This process may take several minutes. You can use the rest of the Splunk product during the download process.

Last Update Info

BrightCloud IP Reputation Service

Version: 1.265.107
Date: 11/19/2014 7:10 AM

Download to Splunk app

Last Update: 2014-11-19 16:00:19 UTC
Result: Update finished successfully.

Keep in mind the following:

- It takes a couple of minutes for the update to take place as it downloads the changes since the last update and merges those into the local database file.
- Additionally, you can set the frequency of the update to either 15 minutes, 1 hour, 12 hours, or 24 hours. If you change the frequency, you must reboot the Splunk server for the change to take effect.

IP Threat Analysis

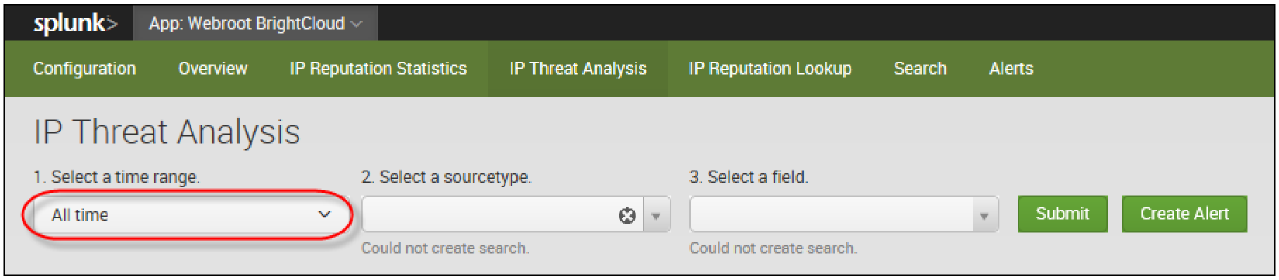
The IP Threat Analysis tab lets you examine threats using time ranges, source types, and other data points.

You can look for malicious IP activities in specific log files indexed by Splunk and alert the info security team so that they can quickly respond and investigate these activities. Use the IP Threat Analysis tab to accomplish this by:

- Selecting specific time frame when user wants to search for malicious IP activities
- Selecting specific log files for searching
- Selecting specific IP fields in those log files

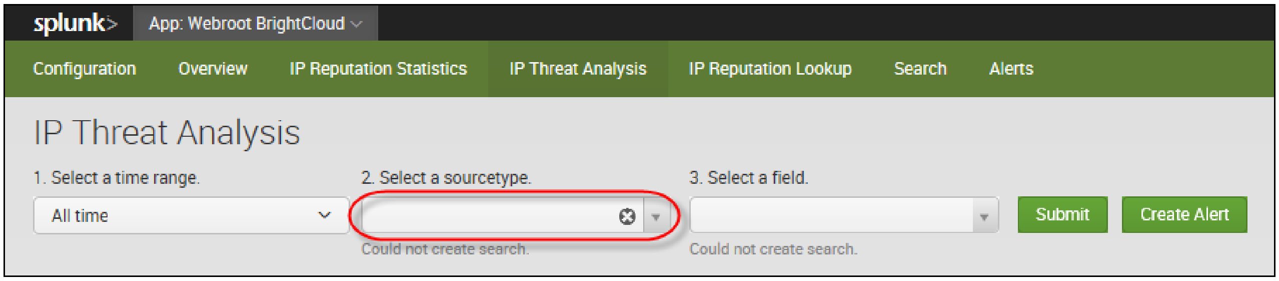
To run a threat analysis:

1. From the *Select a time range* drop-down menu, select a time range.



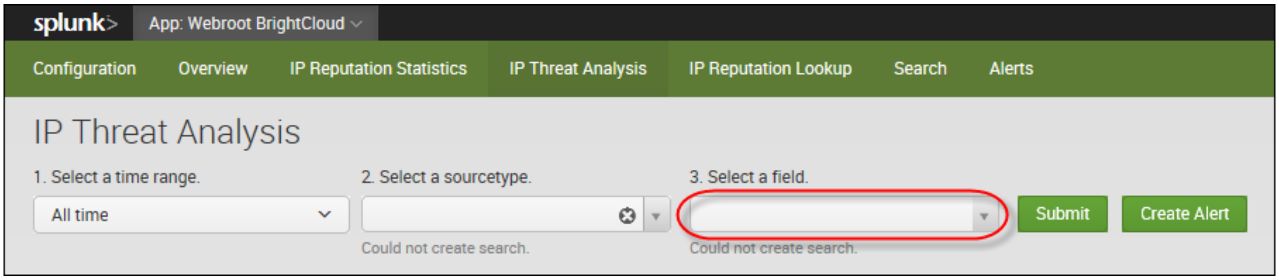
2. From the *Select a sourcetype* drop-down menu, select a sourcetype.

   A sourcetype is a log file that will be analyzed against the IP reputation database. The user can select **All** to include all sourcetypes, or the user can select a specific sourcetype.



3. From the *Select a field* drop-down menu, select a data field in the log file specified in the sourcetype selection.

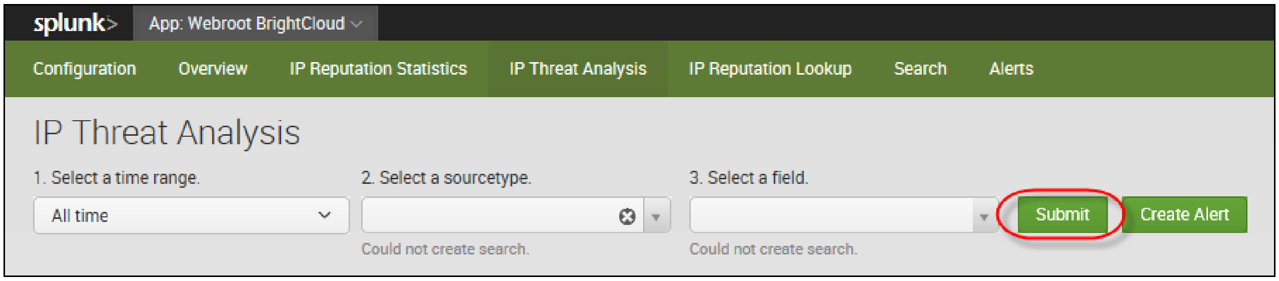
   A data field is the specific IP field inside of the log files that will be compared against the IP reputation database.



IP Threat Analysis

1. Select a time range. All time
2. Select a sourcetype. Could not create search.
3. Select a field. Could not create search.

4. Click the **Submit** button.



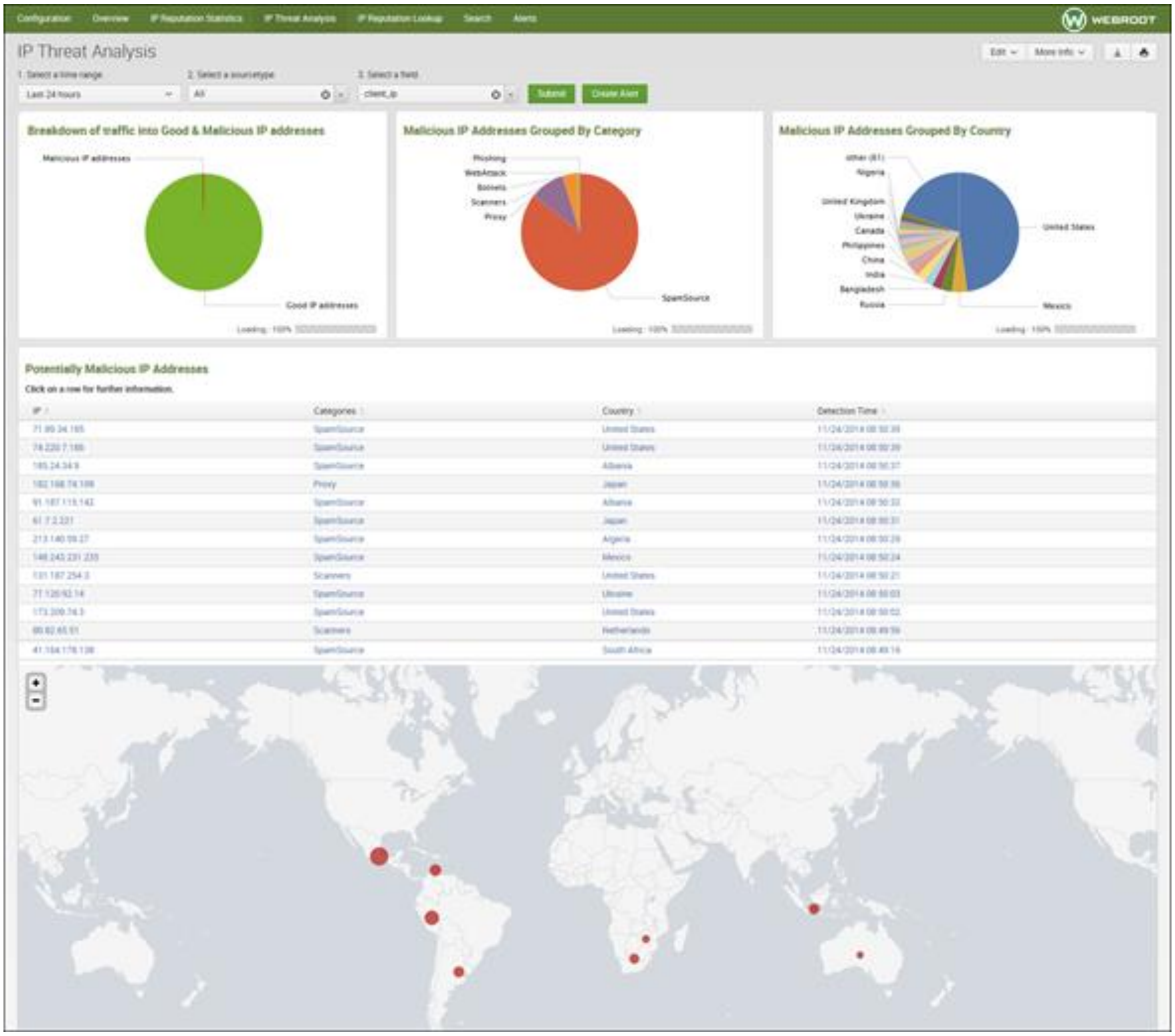
IP Threat Analysis

1. Select a time range. All time
2. Select a sourcetype. Could not create search.
3. Select a field. Could not create search.

Note: To correlate IP rep against multiple sourcetypes or fields, please create merged sourcetypes and fields by combining multiple sourcetypes or fields into singles in Splunk, and then come back to this Splunk app to use those merged sourcetypes or fields.

The dashboard displays a table with the following information:

- The proportion between good and bad IP addresses
- Malicious IPs grouped by category and country.
- Potentially malicious IP addresses.
- A map with the threats' geo-distribution.



IP Threat Analysis

1. Select a time range: Last 24 hours

2. Select a sourcetype: All

3. Select a field: client_ip

Breakdown of traffic into Good & Malicious IP addresses

Malicious IP Addresses Grouped By Category

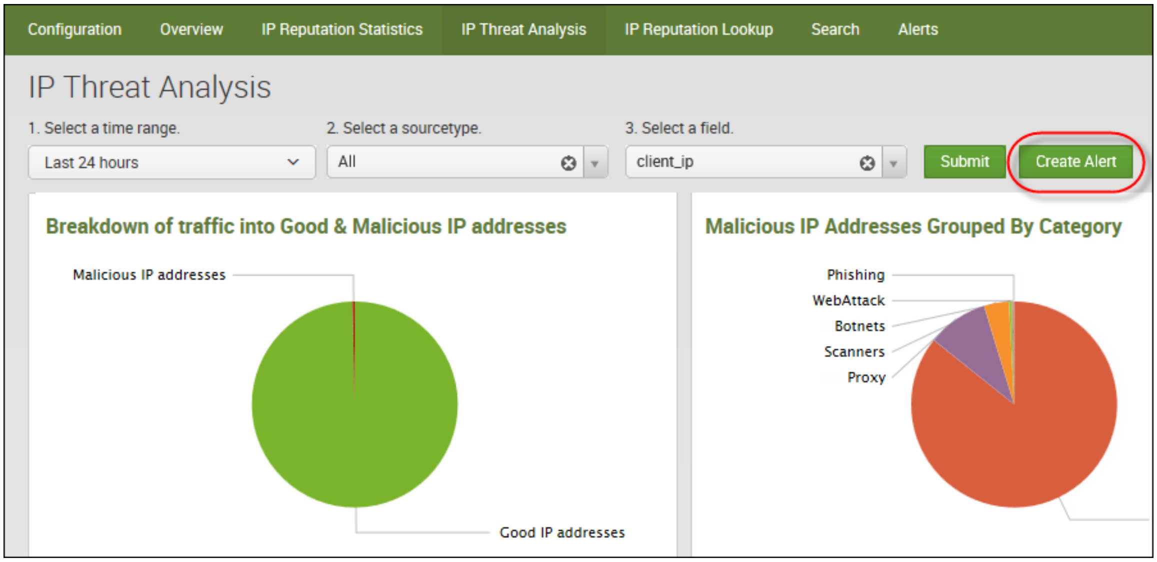
Malicious IP Addresses Grouped By Country

Potentially Malicious IP Addresses

Click on a row for further information.

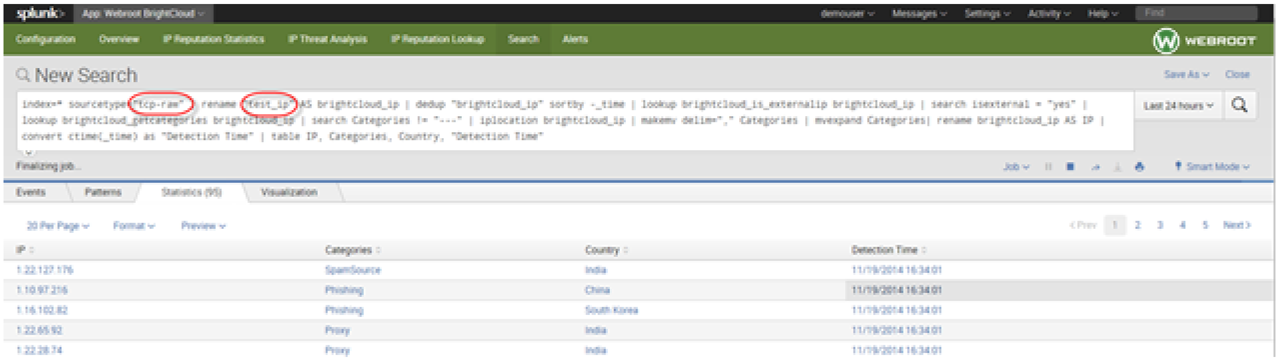
IP	Categories	Country	Detection Time
71.89.34.165	SpamSource	United States	11/24/2014 08:50:39
74.220.7.180	SpamSource	United States	11/24/2014 08:50:39
185.24.34.9	SpamSource	Albania	11/24/2014 08:50:37
182.168.74.199	Proxy	Japan	11/24/2014 08:50:36
91.187.115.142	SpamSource	Albania	11/24/2014 08:50:33
61.7.2.221	SpamSource	Japan	11/24/2014 08:50:31
213.140.59.27	SpamSource	Algeria	11/24/2014 08:50:28
148.243.231.235	SpamSource	Mexico	11/24/2014 08:50:24
131.187.254.3	Scanners	United States	11/24/2014 08:50:21
77.120.92.14	SpamSource	Ukraine	11/24/2014 08:50:03
173.209.74.3	SpamSource	United States	11/24/2014 08:50:02
80.82.65.51	Scanners	Netherlands	11/24/2014 08:49:56
41.164.178.138	SpamSource	South Africa	11/24/2014 08:49:16

5. To create an alert, click the **Create Alert** button at the top of the page.



1. Select a time range. Last 24 hours
2. Select a sourcetype. All
3. Select a field. client_ip

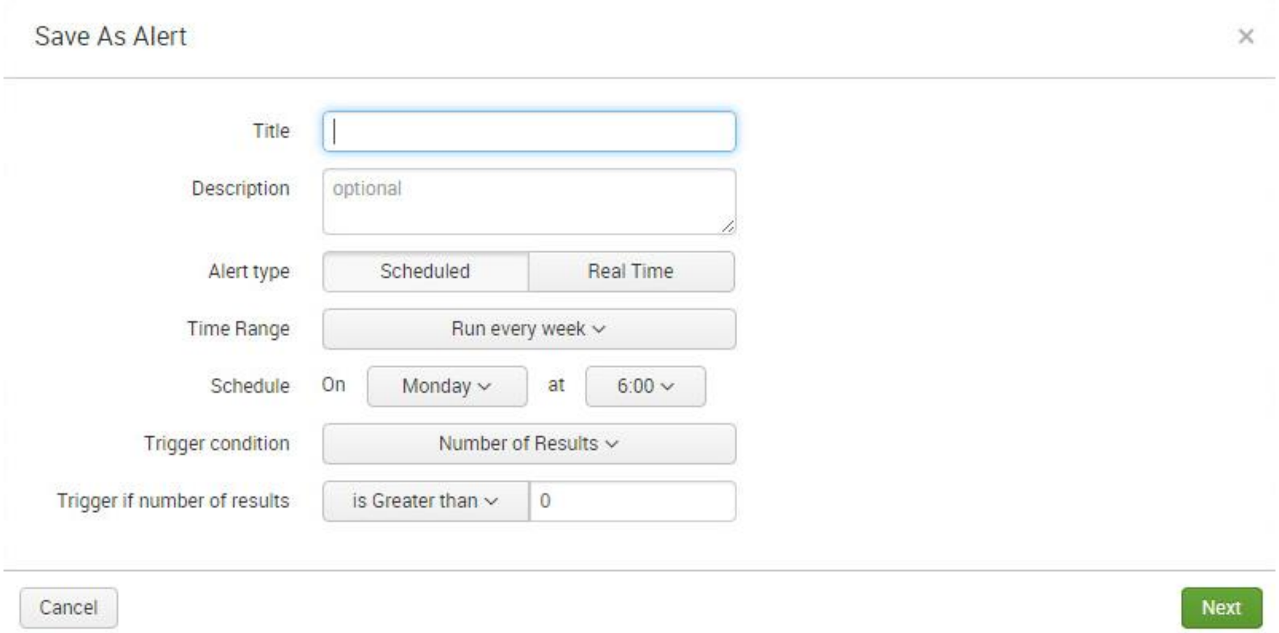
When you create an alert, you will be notified of malicious IP activities detected with BrightCloud Reputation.



```
index=* sourcetype="tcp-raw" | rename "test_ip" AS brightcloud_ip | dedup "brightcloud_ip" sortby -_time | lookup brightcloud_is_externalip brightcloud_ip | search isexternal = "yes" |
lookup brightcloud_getcategories brightcloud_ip | search Categories != "---" | iplocation brightcloud_ip | makemv delim="," Categories | mvexpand Categories| rename brightcloud_ip AS IP |
convert ctime(_time) as "Detection Time" | table IP, Categories, Country, "Detection Time"
```

IP	Categories	Country	Detection Time
1.22.127.176	SpamSource	India	11/19/2014 16:34:01
1.10.97.216	Phishing	China	11/19/2014 16:34:01
1.16.102.82	Phishing	South Korea	11/19/2014 16:34:01
1.22.65.92	Proxy	India	11/19/2014 16:34:01
1.22.28.74	Proxy	India	11/19/2014 16:34:01

6. From here you can create a personalized alert.



Save As Alert

Title

Description: optional

Alert type: Scheduled | Real Time

Time Range: Run every week

Schedule: On Monday at 6:00

Trigger condition: Number of Results

Trigger if number of results: is Greater than 0

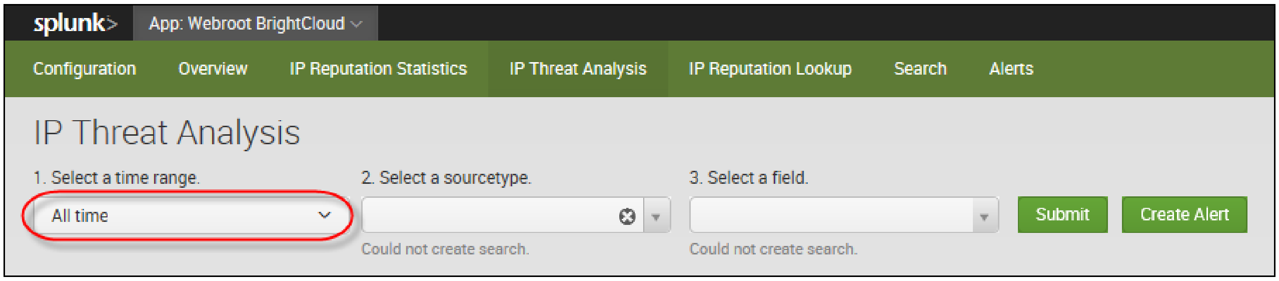
For more information on how to create a personalized alert, see the Splunk Alerting Manual.

One-Click Lookup of Malicious IPs From IP Threat Analysis

In addition to creating an alert from the IP Threat Analysis tab, you can also click on any malicious IP detected and look up additional info on that IP for investigation and analysis.

To look up malicious IPs:

1. From the *Select a time range* drop-down menu, select a time range.



IP Threat Analysis

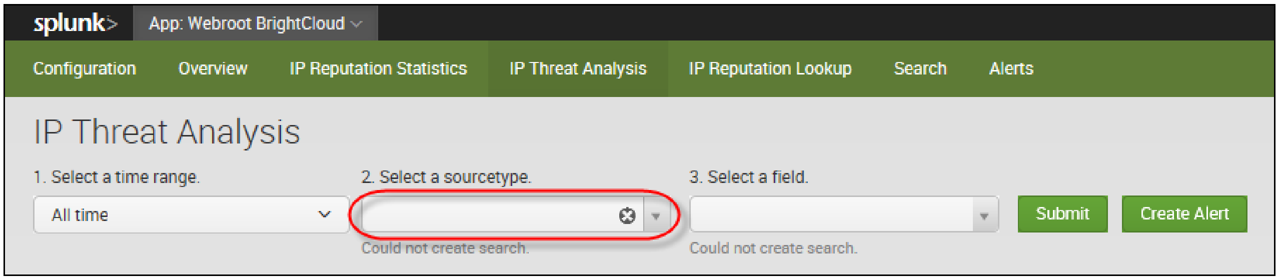
1. Select a time range. All time

2. Select a sourcetype. Could not create search.

3. Select a field. Could not create search.

2. From the *Select a sourcetype* drop-down menu, select a sourcetype.

   A sourcetype is a log file that will be analyzed against our IP reputation database.



IP Threat Analysis

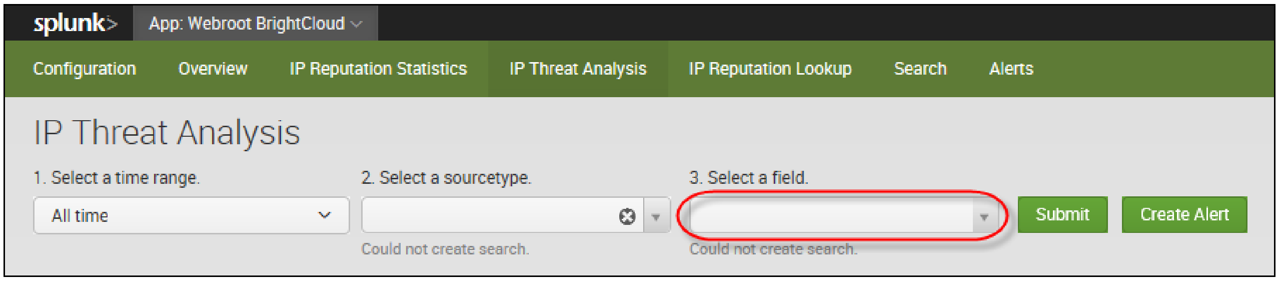
1. Select a time range. All time

2. Select a sourcetype. Could not create search.

3. Select a field. Could not create search.

3. From the *Select a field* drop-down menu, select a data field in the log file specified in the sourcetype selection.

   A data field is the specific IP field inside of the log files that will be compared against our malicious IP list.



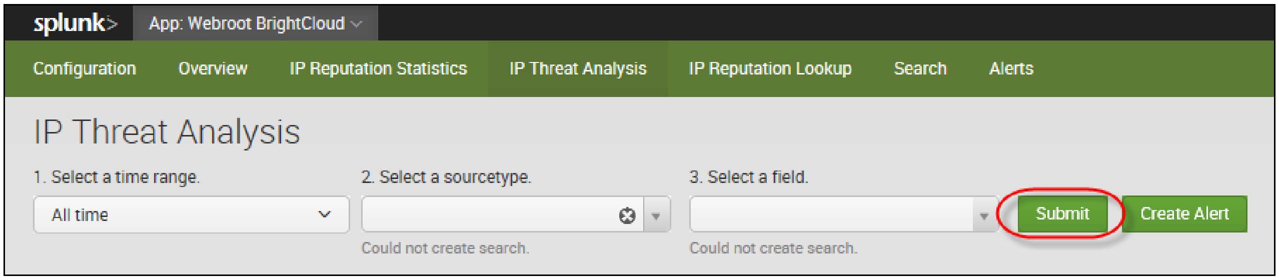
IP Threat Analysis

1. Select a time range. All time

2. Select a sourcetype. Could not create search.

3. Select a field. Could not create search.

4. Click the **Submit** button.



IP Threat Analysis

1. Select a time range.: All time

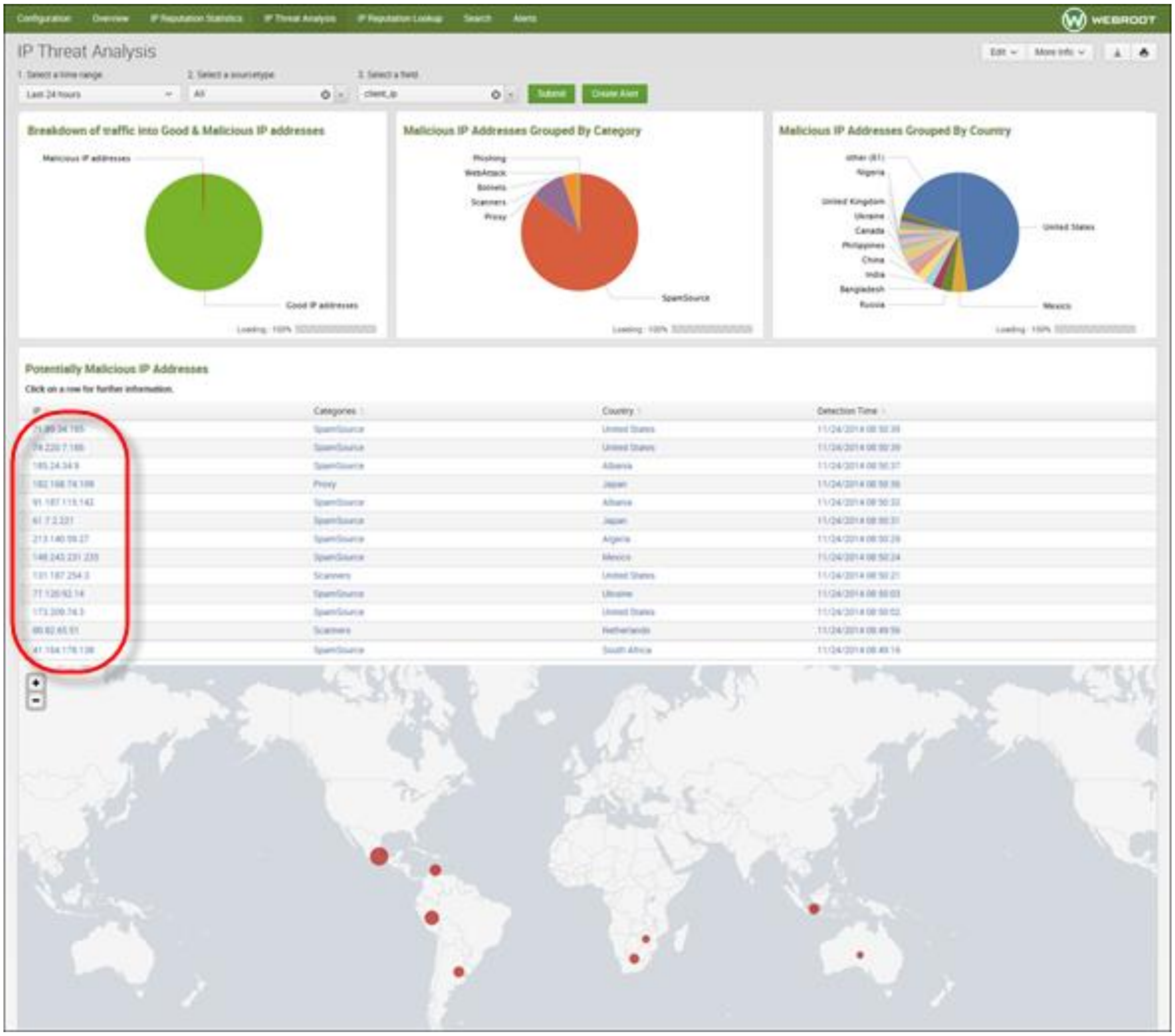
2. Select a sourcetype.: Could not create search.

3. Select a field.: Could not create search.

Note: To correlate IP rep against multiple sourcetypes or fields, please create merged sourcetypes and fields first, for example, combine multiple sourcetypes or fields into singles, in Splunk and then come back to this Splunk app.

The dashboard displays a table with the following information:

- The relationship between good and bad IP addresses
- Malicious IPs grouped by category and country.
- Potentially malicious IP addresses.
- A map with the threats’ geo-distribution.



IP Threat Analysis

1. Select a time range: Last 24 hours

2. Select a sourcetype: All

3. Select a field: client_ip

Breakdown of traffic into Good & Malicious IP addresses

Malicious IP Addresses Grouped By Category

Malicious IP Addresses Grouped By Country

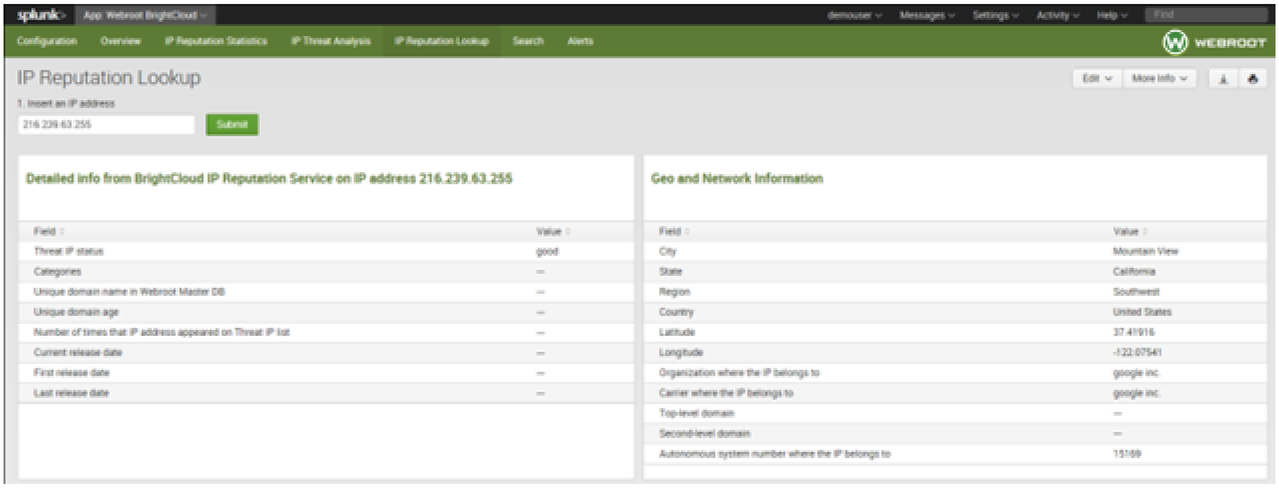
Potentially Malicious IP Addresses

Click on a row for further information.

IP	Categories	Country	Detection Time
71.89.34.195	SpamSource	United States	11/24/2014 08:50:39
74.220.7.186	SpamSource	United States	11/24/2014 08:50:39
185.24.34.9	SpamSource	Albania	11/24/2014 08:50:37
182.168.74.109	Proxy	Japan	11/24/2014 08:50:36
91.187.115.142	SpamSource	Albania	11/24/2014 08:50:33
61.7.2.231	SpamSource	Japan	11/24/2014 08:50:31
213.140.59.27	SpamSource	Algeria	11/24/2014 08:50:26
148.243.231.235	SpamSource	Mexico	11/24/2014 08:50:24
131.187.254.3	Scanners	United States	11/24/2014 08:50:21
77.120.92.14	SpamSource	Ukraine	11/24/2014 08:50:03
173.209.74.3	SpamSource	United States	11/24/2014 08:50:02
80.82.65.51	Scanners	Netherlands	11/24/2014 08:49:56
41.164.178.138	SpamSource	South Africa	11/24/2014 08:49:16

5. To view information on the IP Lookup page, click on a specific IP in the dashboard.

   The dashboard displays additional information about malicious IPs, which you can use for investigation or incident response.



Detailed info from BrightCloud IP Reputation Service on IP address 216.239.63.255

Field	Value
Threat IP status	good
Categories	—
Unique domain name in Webroot Master DB	—
Unique domain age	—
Number of times that IP address appeared on Threat IP list	—
Current release date	—
First release date	—
Last release date	—

Geo and Network Information

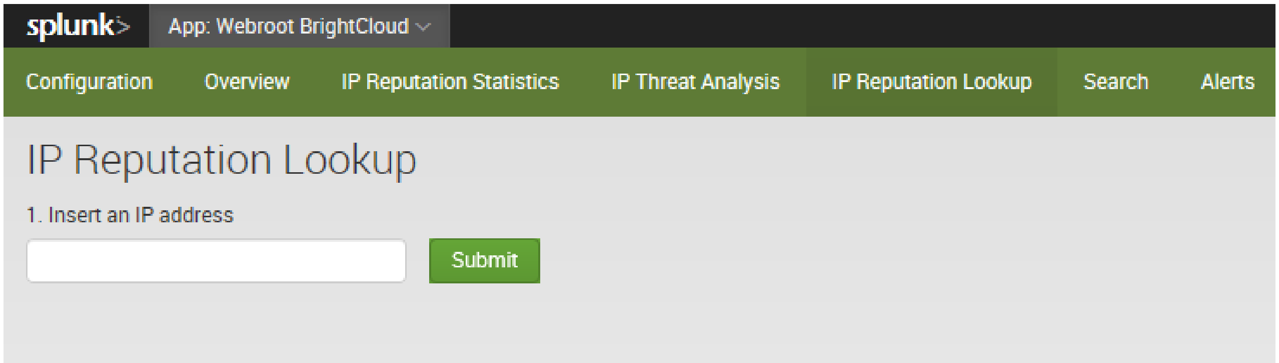
Field	Value
City	Mountain View
State	California
Region	Southwest
Country	United States
Latitude	37.41916
Longitude	-122.07541
Organization where the IP belongs to	google inc.
Carrier where the IP belongs to	google inc.
Top-level domain	—
Second-level domain	—
Autonomous system number where the IP belongs to	15169

IP Reputation Lookup

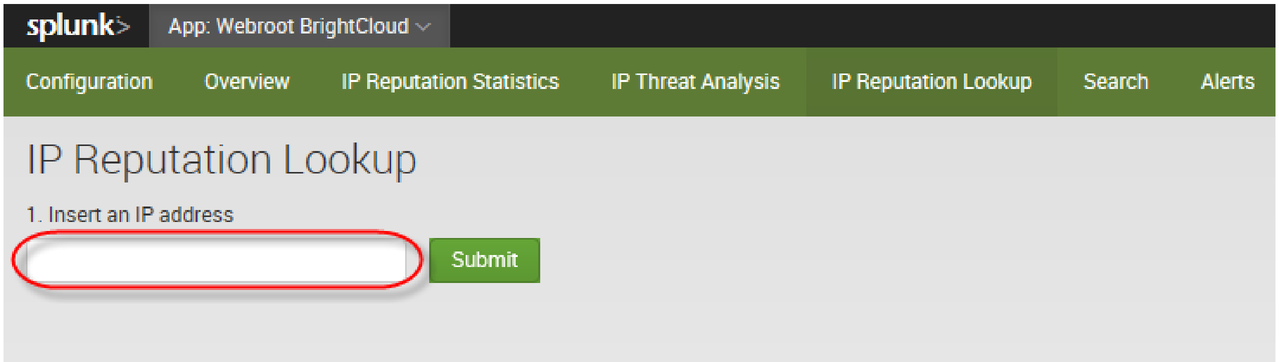
Use the IP Reputation Lookup tab to check whether an IP is malicious or not. You can enter an IP address, and get information about the IP address. If it's malicious, you will see additional information about the IP, for example, where the IP is located, what kind of threat the IP presents, etc.

To look up an IP's reputation:

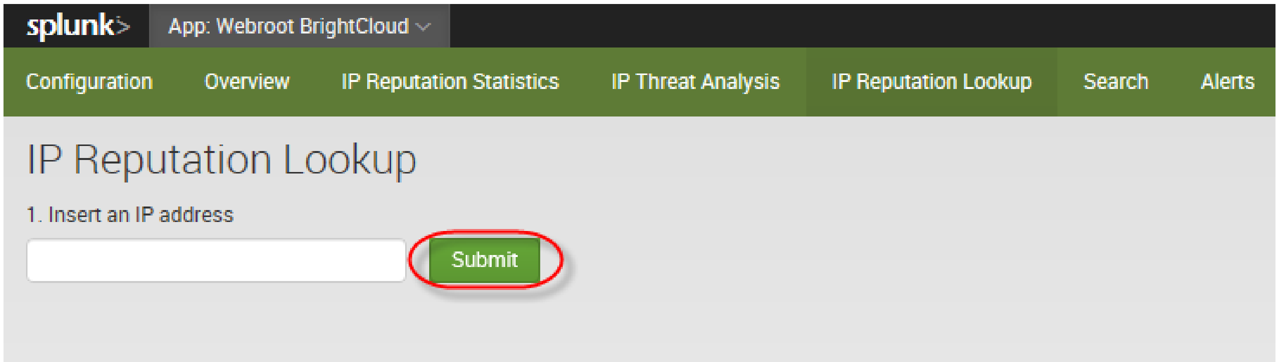
1. Within Splunk, click the **IP Reputation Lookup** tab.



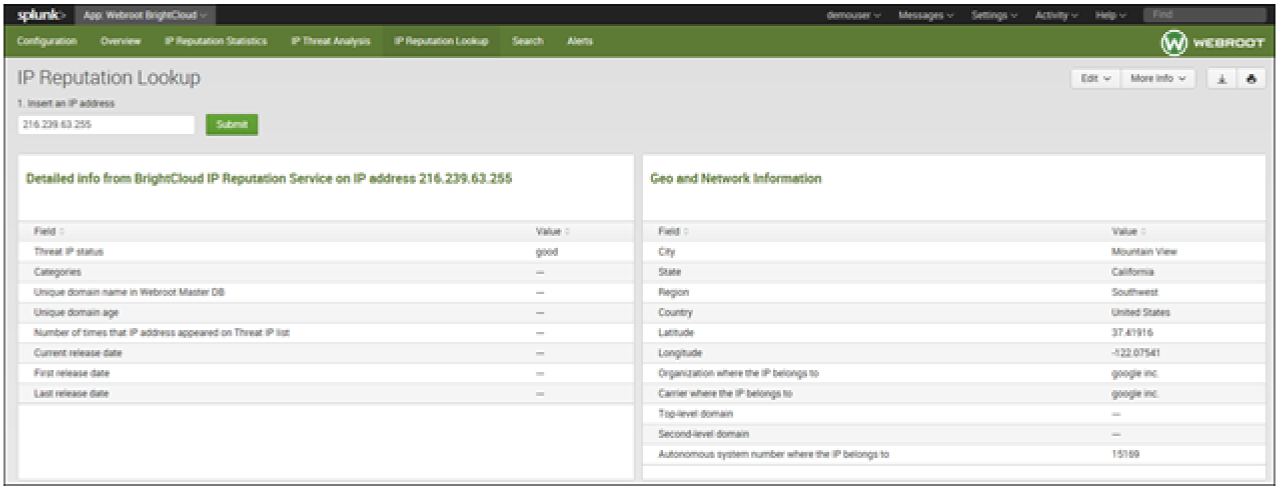
2. In the *Insert an IP address* field, enter a site's IP address.



3. Click the **Submit** button.



The system displays information about the IP's reputation, including their status and geographical information.



1. Insert an IP address: 216.239.63.255

Detailed info from BrightCloud IP Reputation Service on IP address 216.239.63.255

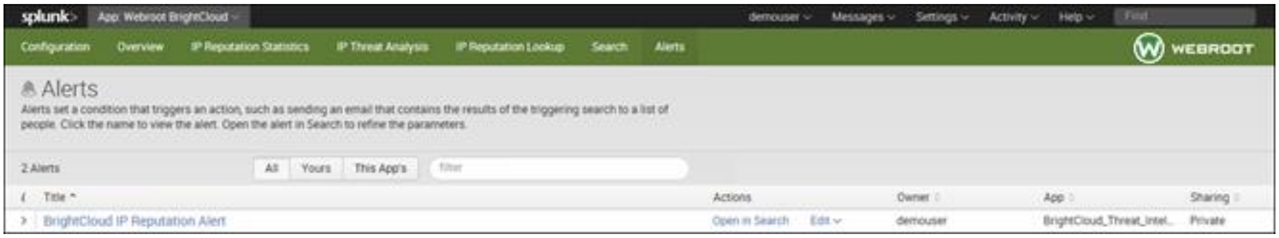
Field	Value
Threat IP status	good
Categories	—
Unique domain name in Webroot Master DB	—
Unique domain age	—
Number of times that IP address appeared on Threat IP list	—
Current release date	—
First release date	—
Last release date	—

Geo and Network Information

Field	Value
City	Mountain View
State	California
Region	Southwest
Country	United States
Latitude	37.41916
Longitude	-122.07541
Organization where the IP belongs to	google inc.
Carrier where the IP belongs to	google inc.
Top-level domain	—
Second-level domain	—
Autonomous system number where the IP belongs to	15169

Alerts

From the Alerts tab, you can manage all the alerts you created.



Alerts

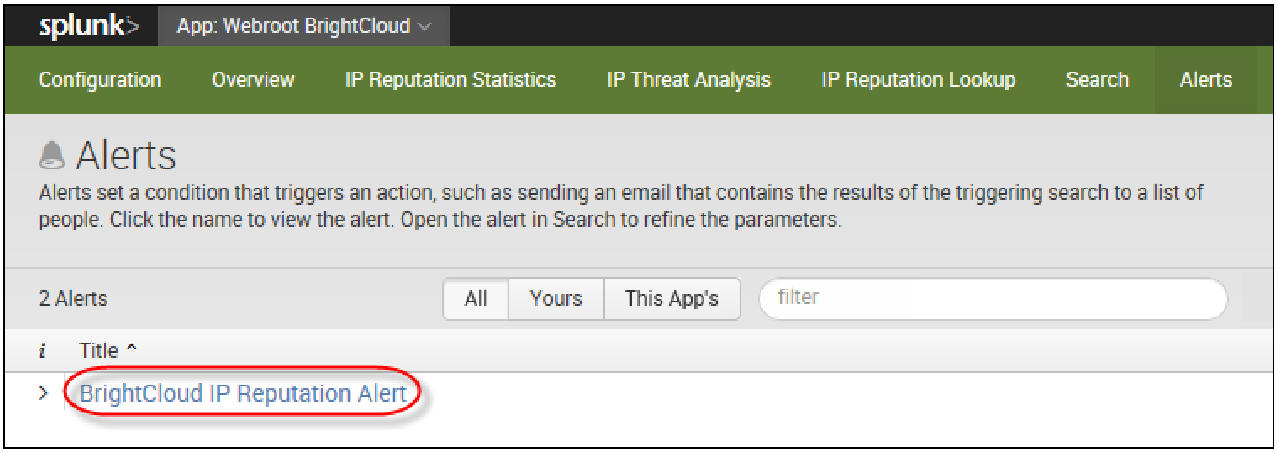
Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts

i	Title ^	Actions		Owner	App	Sharing
>	BrightCloud IP Reputation Alert	Open in Search	Edit	demouser	BrightCloud_Threat_Intel...	Private

To manage an alert:

1. Click on an alert to view the trigger history.



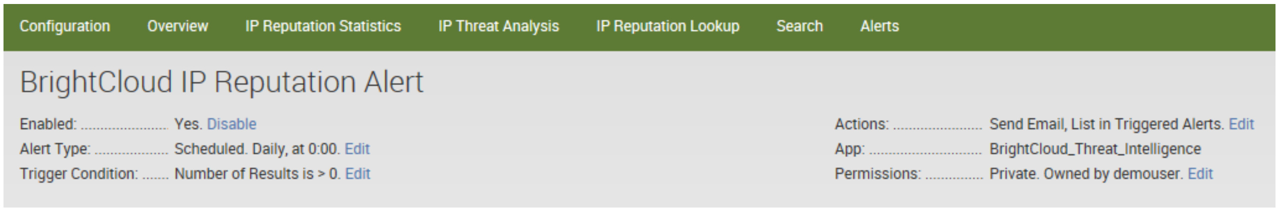
Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts

i	Title ^
>	BrightCloud IP Reputation Alert

The system displays information about the alert.



BrightCloud IP Reputation Alert

Enabled: .... Yes. Disable
Alert Type: .... Scheduled. Daily, at 0:00. Edit
Trigger Condition: .... Number of Results is > 0. Edit

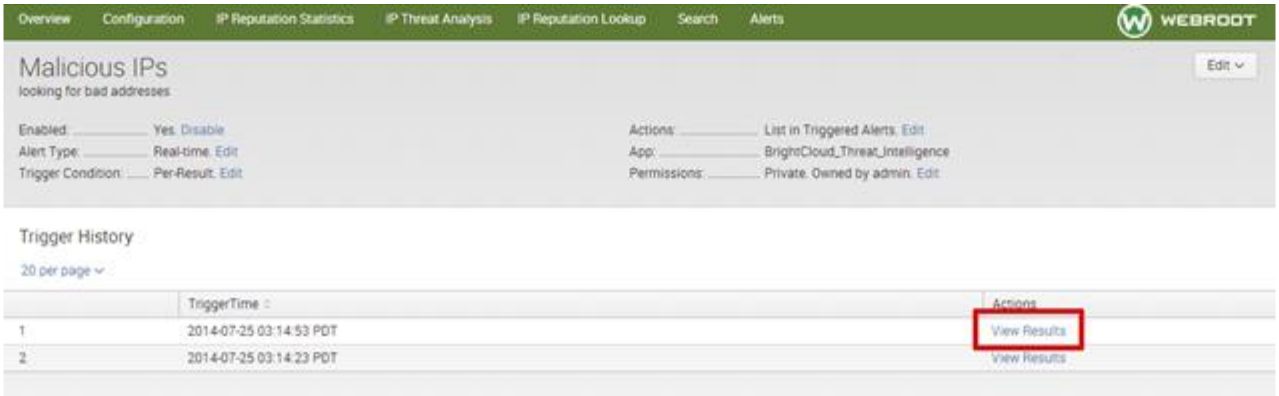
Actions: .... Send Email, List in Triggered Alerts. Edit
App: .... BrightCloud_Threat_Intelligence
Permissions: .... Private. Owned by demouser. Edit

2. From here you can do either of the following:

   - Click **Disable** to disable the alert.
   - Click **Edit** next to any setting for the alert.

     The system displays a window where you can edit the settings.

3. In the Actions column, click the **View results** button.



Malicious IPs
looking for bad addresses

Enabled: Yes. Disable
Alert Type: Real-time. Edit
Trigger Condition: Per-Result. Edit

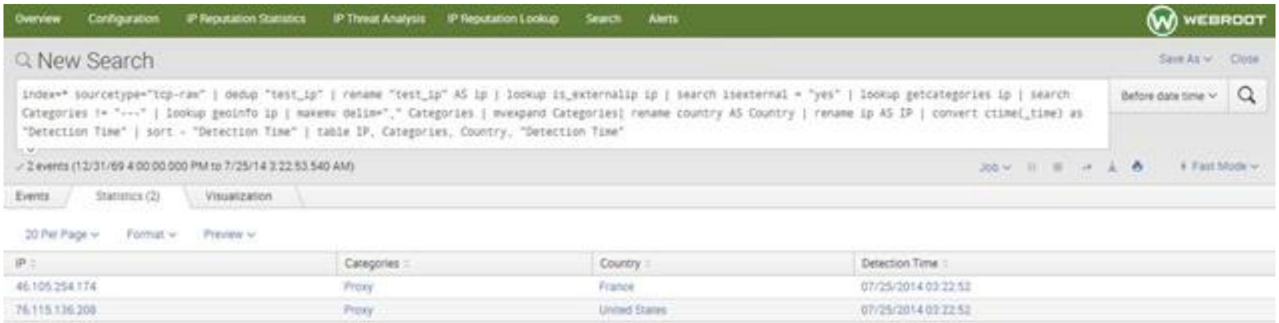
Actions: List in Triggered Alerts. Edit
App: BrightCloud_Threat_Intelligence
Permissions: Private. Owned by admin. Edit

Trigger History

20 per page

	TriggerTime	Actions
1	2014-07-25 03:14:53 PDT	View Results
2	2014-07-25 03:14:23 PDT	View Results

The system displays the Statistics tab.



New Search

```
index=* sourcetype="tcp-raw" | dedup "test_ip" | rename "test_ip" AS ip | lookup is_externalip ip | search isexternal = "yes" | lookup getcategories ip | search
Categories != "---" | lookup geoinfo ip | makemv delim="," Categories | mvexpand Categories| rename country AS Country | rename ip AS IP | convert ctime(_time) as
"Detection Time" | sort - "Detection Time" | table IP, Categories, Country, "Detection Time"
```

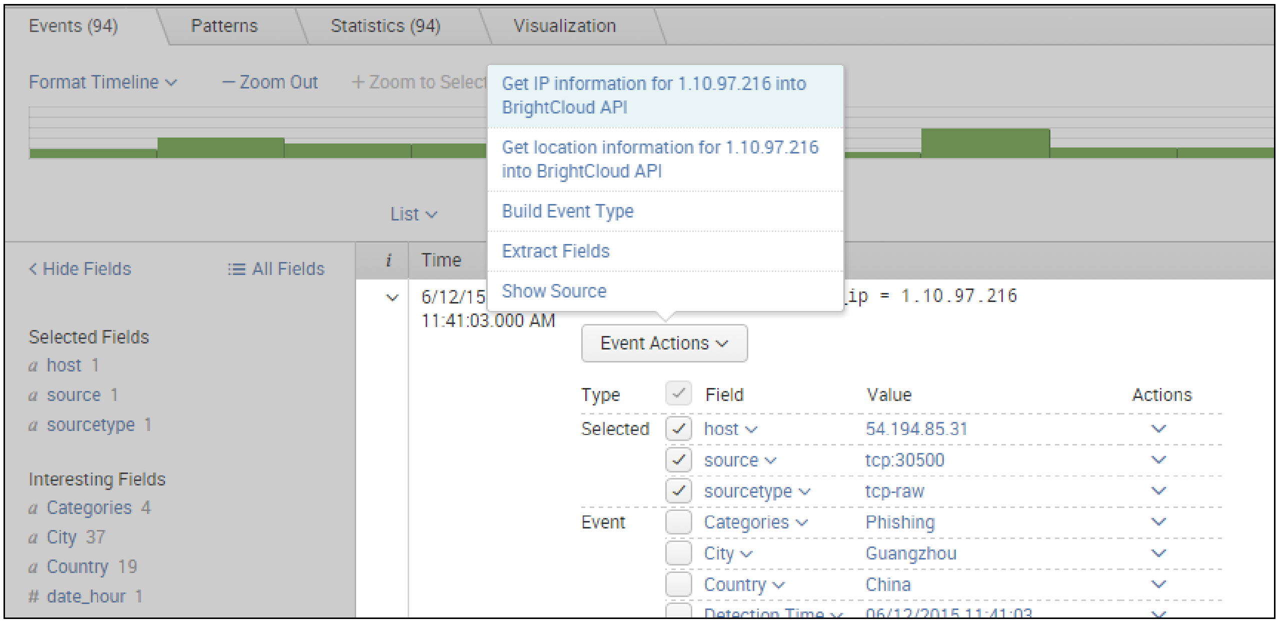
✓ 2 events (12/31/69 4:00:00.000 PM to 7/25/14 3:22:53.540 AM)

IP	Categories	Country	Detection Time
46.105.254.174	Proxy	France	07/25/2014 03:22:52
76.115.136.208	Proxy	United States	07/25/2014 03:22:52

Additionally, you can click any of the following tabs:

- Events
- Patterns
- Visualization

The following image reflects the fact that when executing a search within the app, all retrieved raw events provide the option for a BrightCloud IP lookup from the Events Action menu. This includes searches when originally coming from Alerts > Open in Search.



Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
a Categories 4
a City 37
a Country 19
# date_hour 1

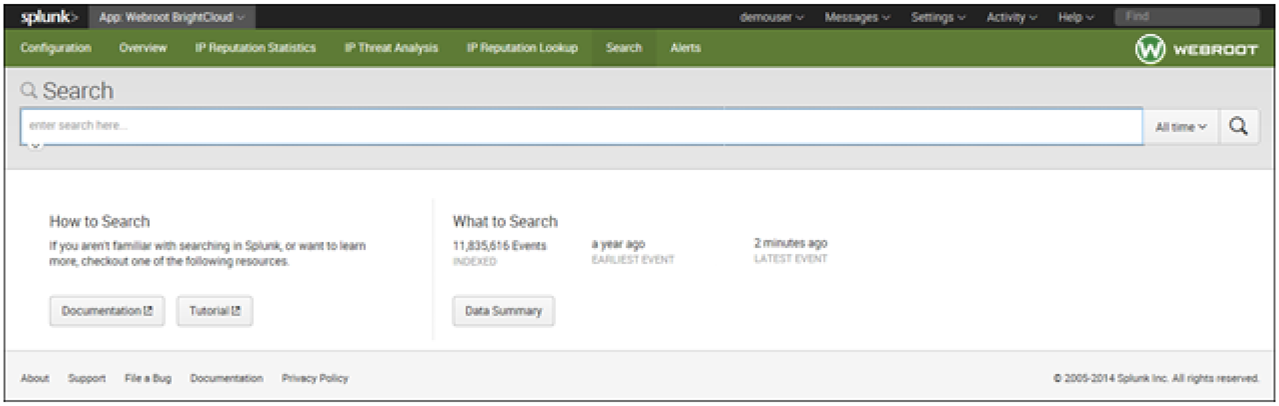
6/12/15 11:41:03.000 AM ip = 1.10.97.216

Type	✓	Field	Value	Actions
Selected	✓	host ⌄	54.194.85.31	⌄
	✓	source ⌄	tcp:30500	⌄
	✓	sourcetype ⌄	tcp-raw	⌄
Event	□	Categories ⌄	Phishing	⌄
	□	City ⌄	Guangzhou	⌄
	□	Country ⌄	China	⌄
	□	Detection Time ⌄	06/12/2015 11:41:03	⌄

Using BrightCloud Data in Splunk Queries

BrightCloud IP Reputation data can be used both inside and outside of the Splunk app in Splunk queries.

Go to the Search tab either inside or outside the Splunk app to access the Search panel.



If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

11,835,616 Events INDEXED

a year ago EARLIEST EVENT

2 minutes ago LATEST EVENT

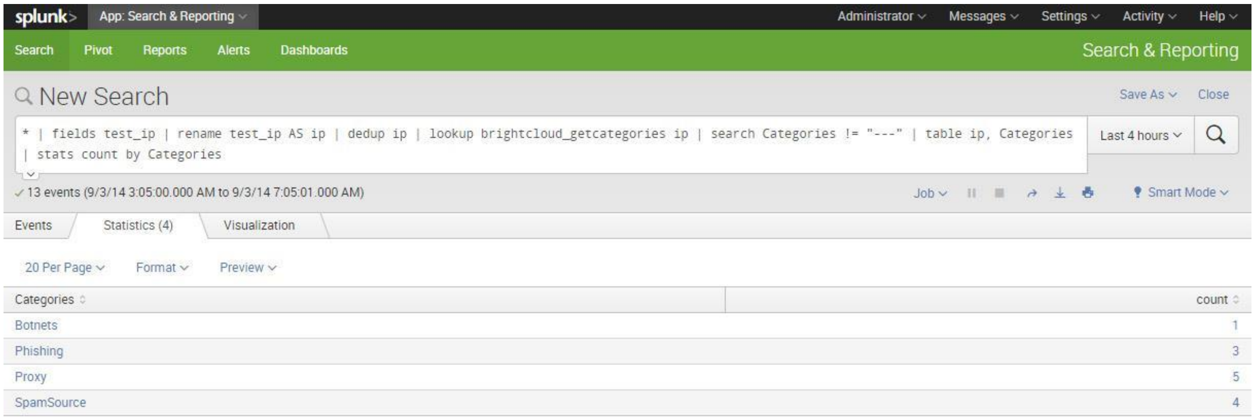
© 2005-2014 Splunk Inc. All rights reserved.

Use the following commands in Splunk queries to correlate BrightCloud IP reputation data with other data in Splunk. For more information, see Splunk Documentation.

- brightcloud_getcategories
- brightcloud_bcss_info

brightcloud_getcategories

This command takes as input one field, named *ip,* and returns the category that the IP address matches or a list of categories if the IP address matches more than one category.



```
* | fields test_ip | rename test_ip AS ip | dedup ip | lookup brightcloud_getcategories ip | search Categories != "---" | table ip, Categories
| stats count by Categories
```

✓ 13 events (9/3/14 3:05:00.000 AM to 9/3/14 7:05:01.000 AM)

Categories	count
Botnets	1
Phishing	3
Proxy	5
SpamSource	4

Threat Categories

BrightCloud tracks IP threats across these categories:

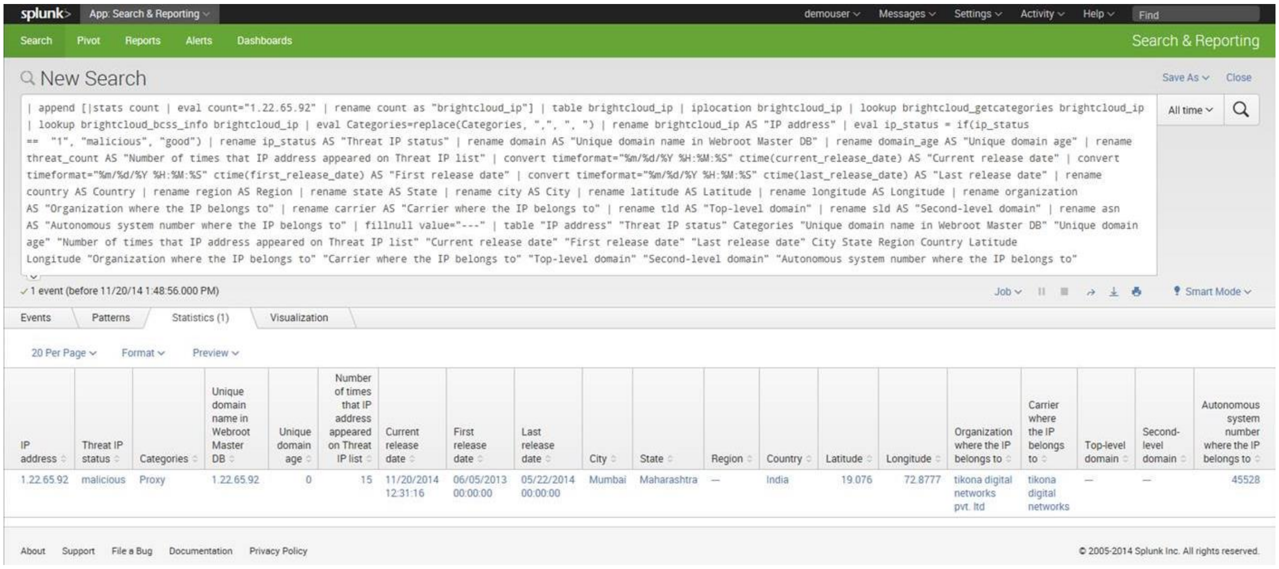
- SpamSources
- WindowsExploits
- WebAttacks
- BotNets
- Scanners
- DenialofService
- Reputation
- Phishing
- Proxy
- Network
- CloudProviders
- MobileThreats

You can use these categories directly inside a Splunk search query:
Search Categories =”Proxy”

brightcloud_bcss_info

This command is used to get more contextual information about the IP, for example, where it came from, what type of IP threat it is, etc. Query results are large because the system renames and reformats to make the information more readable.

Note: Because this lookup performs a cloud lookup it should not executed against large lists of IP addresses, due to latency of online lookup.



```
| append [|stats count | eval count="1.22.65.92" | rename count as "brightcloud_ip"] | table brightcloud_ip | iplocation brightcloud_ip | lookup brightcloud_getcategories brightcloud_ip
| lookup brightcloud_bcss_info brightcloud_ip | eval Categories=replace(Categories, ",", ", ") | rename brightcloud_ip AS "IP address" | eval ip_status = if(ip_status
==  "1", "malicious", "good") | rename ip_status AS "Threat IP status" | rename domain AS "Unique domain name in Webroot Master DB" | rename domain_age AS "Unique domain age" | rename
threat_count AS "Number of times that IP address appeared on Threat IP list" | convert timeformat="%m/%d/%Y %H:%M:%S" ctime(current_release_date) AS "Current release date" | convert
timeformat="%m/%d/%Y %H:%M:%S" ctime(first_release_date) AS "First release date" | convert timeformat="%m/%d/%Y %H:%M:%S" ctime(last_release_date) AS "Last release date" | rename
country AS Country | rename region AS Region | rename state AS State | rename city AS City | rename latitude AS Latitude | rename longitude AS Longitude | rename organization
AS "Organization where the IP belongs to" | rename carrier AS "Carrier where the IP belongs to" | rename tld AS "Top-level domain" | rename sld AS "Second-level domain" | rename asn
AS "Autonomous system number where the IP belongs to" | fillnull value="---" | table "IP address" "Threat IP status" Categories "Unique domain name in Webroot Master DB" "Unique domain
age" "Number of times that IP address appeared on Threat IP list" "Current release date" "First release date" "Last release date" City State Region Country Latitude
Longitude "Organization where the IP belongs to" "Carrier where the IP belongs to" "Top-level domain" "Second-level domain" "Autonomous system number where the IP belongs to"
```

✓ 1 event (before 11/20/14 1:48:56.000 PM)

IP address	Threat IP status	Categories	Unique domain name in Webroot Master DB	Unique domain age	Number of times that IP address appeared on Threat IP list	Current release date	First release date	Last release date	City	State	Region	Country	Latitude	Longitude	Organization where the IP belongs to	Carrier where the IP belongs to	Top-level domain	Second-level domain	Autonomous system number where the IP belongs to
1.22.65.92	malicious	Proxy	1.22.65.92	0	15	11/20/2014 12:31:16	06/05/2013 00:00:00	05/22/2014 00:00:00	Mumbai	Maharashtra	—	India	19.076	72.8777	tikona digital networks pvt. ltd	tikona digital networks	—	—	45528

Legal Notice

netaddr

COPYRIGHT AND LICENSE