Censys Splunk

Censys, Inc.

Mar 13, 2024

INTRODUCTION

The Censys for Splunk apps and add-ons allow Censys users to import ASM and Search data into Splunk.

CHAPTER

ONE

FEATURES

Censys Add-on for Splunk

- Import data from the Censys ASM Logbook API into Splunk
- Import data from the Censys ASM Risk Events API into Splunk

Censys ASM App for Splunk

- Dashboards for Censys ASM Logbook and Risk Events APIs
- Custom query-based alerts and reports

Censys Search App for Splunk

- Enrich logs with the most up-to-date information on public hosts and certificates

1.1 Frequently Asked Questions

1.1.1 Why do we have a Censys ASM for Splunk App and Censys Add-on for Splunk?

The Censys ASM for Splunk App is intended to be installed on the customer's search head. This is the visual layer for the data ingested. The app includes functionality such as dashboards, one-click pivot to Censys ASM, and pre-configured alerts. The Censys Add-on for Splunk is traditionally installed at the forwarder layer. The Add-on is what pulls the logs from Censys. We separated the functionality to align to Splunk best practices. Forwarders are the Splunk recommended way to ingest logs. To simplify deployment and support Splunk Cloud customers, we are required to provide 2 modes of deployment.

1.1.2 Does the app and add-on support Splunk Cloud deployments?

Splunk Cloud is the managed service offering of Splunk. Our application and add-on are both certified to be deployed in Splunk Cloud.

1.1.3 Does the add-on conform to the Common Information Model?

Yes. The add-on is compliant with the Common Information Model (CIM).

1.1.4 Does the add-on work with the Splunk Enterprise Security app?

Yes. If installed on a search head with Splunk Enterprise Security, the alerts and reports can be configured to generate notable events to enable a seamless workflow.

1.1.5 My question wasn't answered here

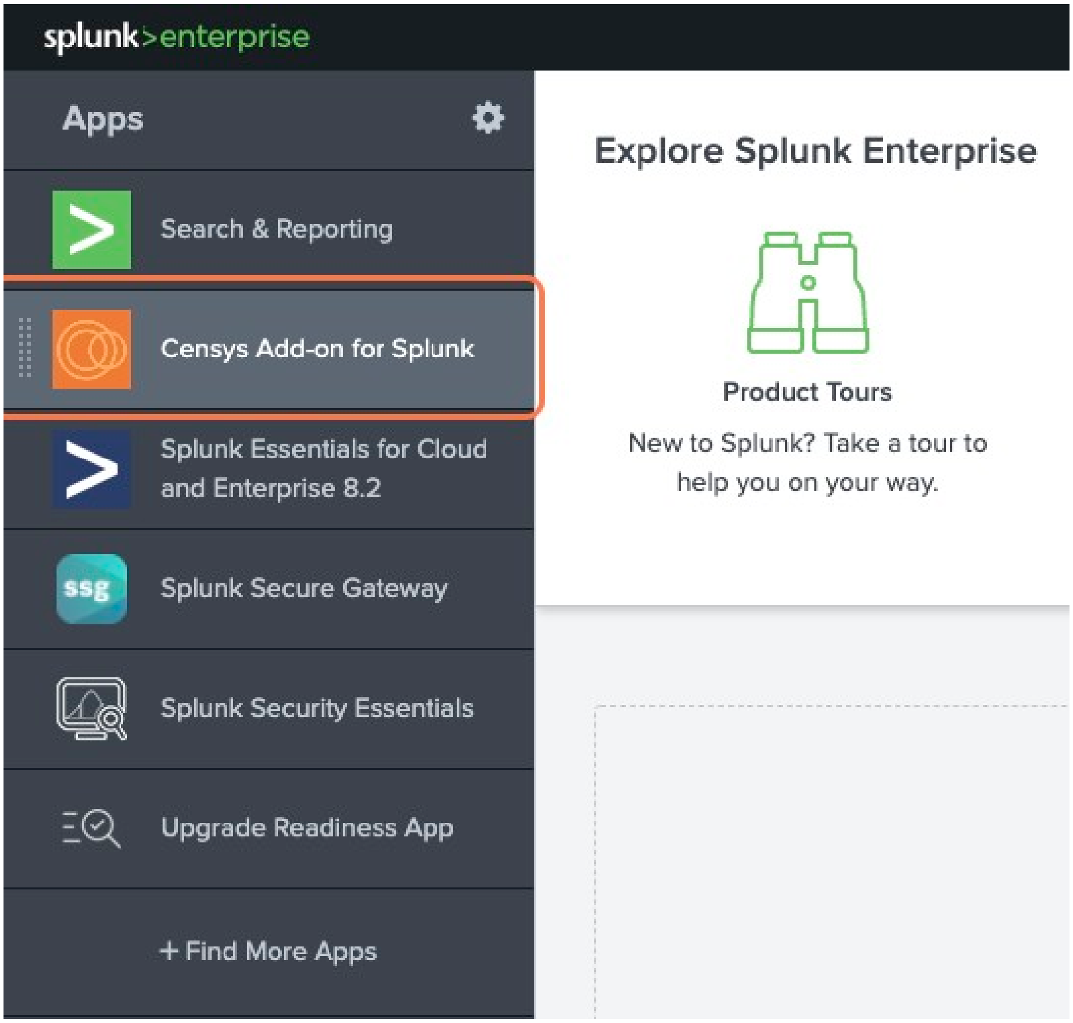
Ask a question on GitHub Discussions for direct communication with the developers and contributors.

1.2 Troubleshooting

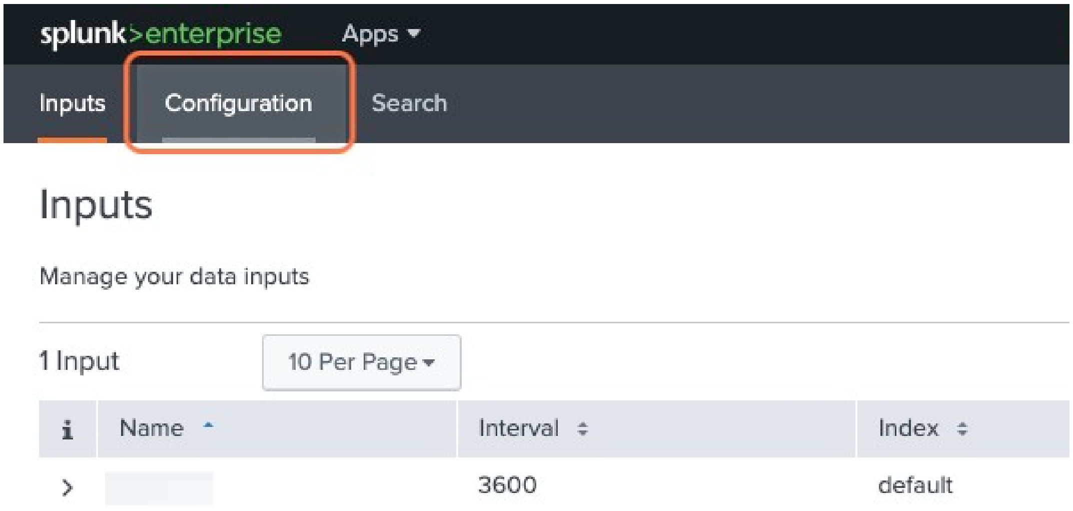
1.2.1 Troubleshooting Add-on

Enable Debug Logging

1. Navigate to the **Censys Add-on for Splunk**.


splunk>enterprise
Apps
Search & Reporting
Censys Add-on for Splunk
Splunk Essentials for Cloud and Enterprise 8.2
Splunk Secure Gateway
Splunk Security Essentials
Upgrade Readiness App
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.

2. Navigate to the **Configuration** tab.



Inputs

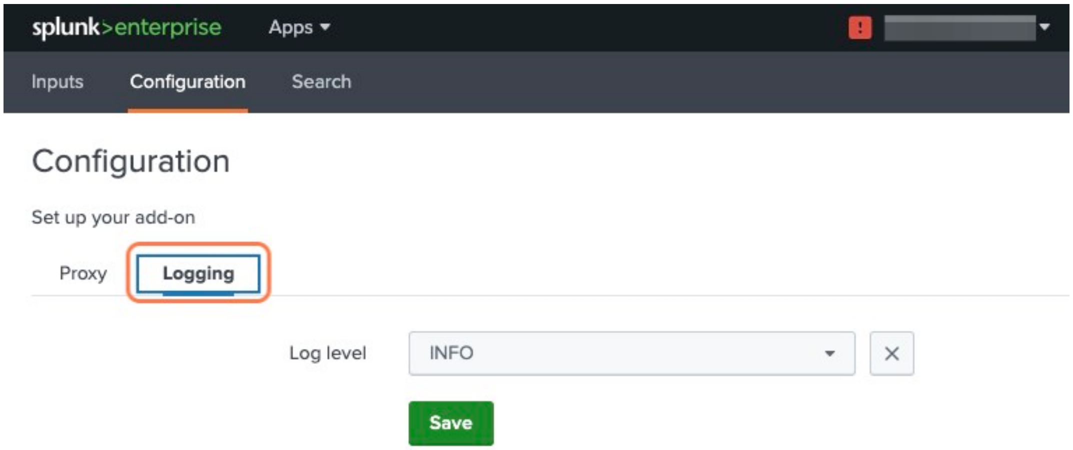
Manage your data inputs

1 Input

10 Per Page ▾

i	Name ▴	Interval ⇕	Index ⇕
>	[redacted]	3600	default

3. Navigate to the **Logging** section.

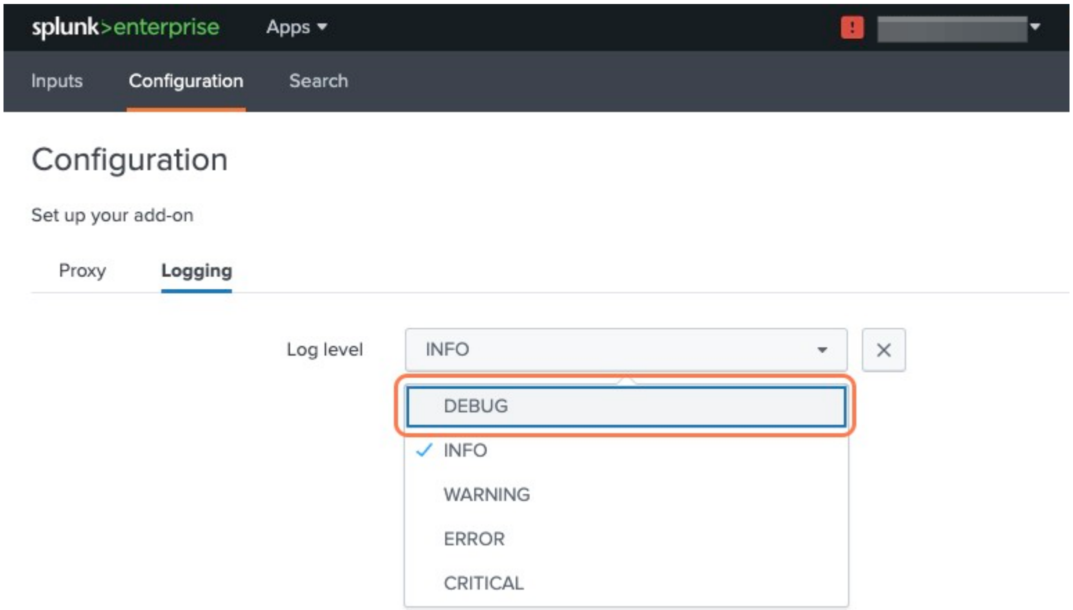


Configuration

Set up your add-on

Log level: INFO

4. Select the DEBUG option from the **Log level** dropdown menu.



Configuration

Set up your add-on

Log level: INFO

1.3 Support

1.3.1 Install and configuration

- **Add-on:** See *Add-on Installation* for more information.
- **ASM App:** See *ASM App Installation* for more information.

1.3.2 Troubleshooting an issue?

See *Troubleshooting* for more information.

1.3.3 Need more help?

GitHub Discussions: Ask a question on GitHub Discussions for direct communication with the developers and contributors.

1.3.4 Found a bug?

GitHub Issues: Report a bug on GitHub Issues.

1.4 Quick Start

1.4.1 Installation

Splunkbase Links

- Censys Add-on for Splunk
- Censys ASM App for Splunk
- Censys Search App for Splunk

The Censys Splunk Apps and Add-on are designed to work together, and with Splunk Enterprise Security if available. Both Apps require the Add-on to be installed. The Add-on can be used with or without either of the Apps.

What to install

Splunk Node	What to install
Search Head	Add-on and App(s)
Heavy Forwarder	Add-on only
Universal Forwarder	None

Install the App(s) and Add-on

- *Install the Censys Add-on for Splunk*
- *Install the Censys ASM App for Splunk*

1.5 Censys Add-on for Splunk

The Censys Add-on for Splunk allows Censys ASM users to import Logbook and Risks data into Splunk®, where changes in their attack surface can be easily directed to downstream security and analytics applications.

This guide will help you:

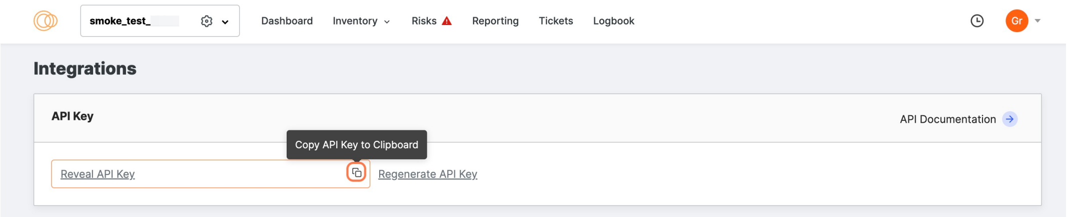
- Install the Censys Add-on in your Splunk environment
- Configure the Censys Add-on
- Use the Censys Add-on to monitor your attack surface

Splunkbase: Censys Add-on for Splunk

1.5.1 Add-on Prerequisites

1. Your Censys ASM API key

   Find your key on the Censys ASM integrations page.

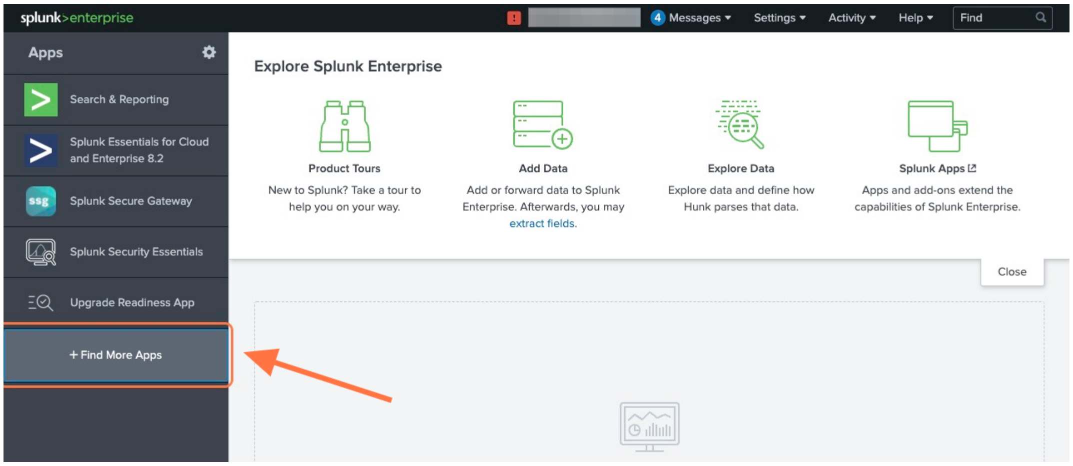


2. A Splunk account and installation.

1.5.2 Install the Censys Add-on for Splunk

Install from Splunkbase (Recommended)

1. From the Splunk main page, click the **+ Find More Apps** button in the sidebar.



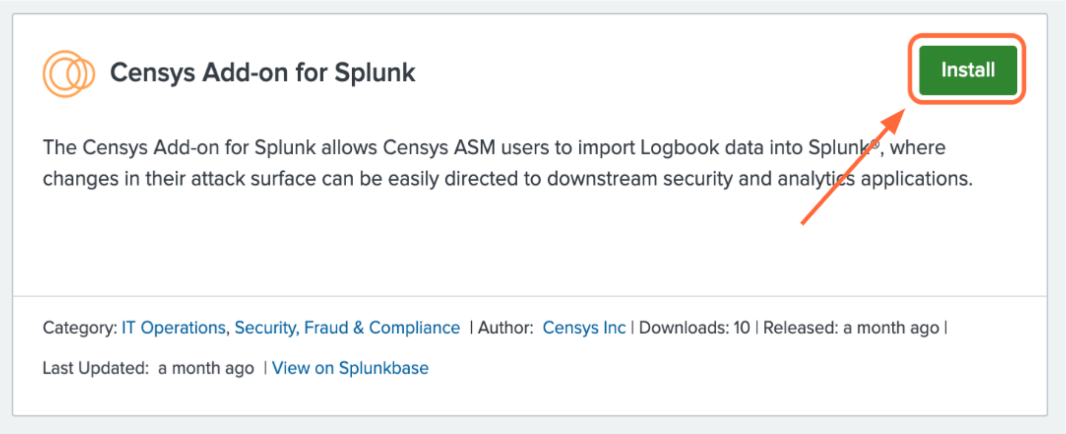
New to Splunk? Take a tour to help you on your way.

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

Explore data and define how Hunk parses that data.

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

2. Type “Censys” in the search bar.
3. On the results page, find the “Censys Add-on for Splunk” app card and click the green **Install** button.



Censys Add-on for Splunk

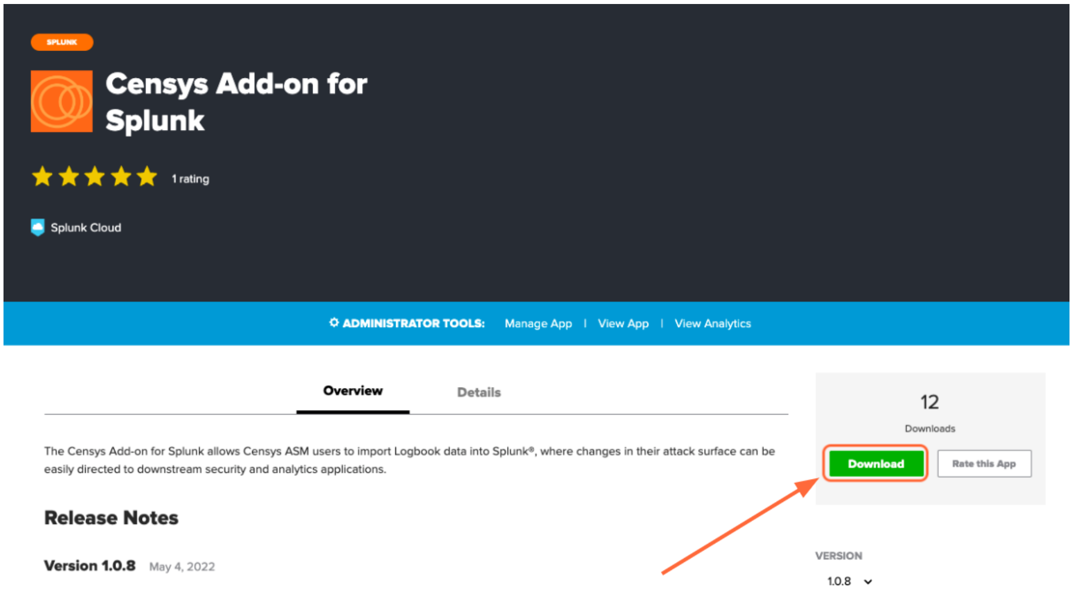
The Censys Add-on for Splunk allows Censys ASM users to import Logbook data into Splunk®, where changes in their attack surface can be easily directed to downstream security and analytics applications.

Category: IT Operations, Security, Fraud & Compliance | Author: Censys Inc | Downloads: 10 | Released: a month ago | Last Updated: a month ago | View on Splunkbase

4. Reenter login credentials to confirm your choice.

Install from File

1. Go to the Add-on’s page on Splunkbase and click the **Download** button.



Censys Add-on for Splunk

The Censys Add-on for Splunk allows Censys ASM users to import Logbook data into Splunk®, where changes in their attack surface can be easily directed to downstream security and analytics applications.

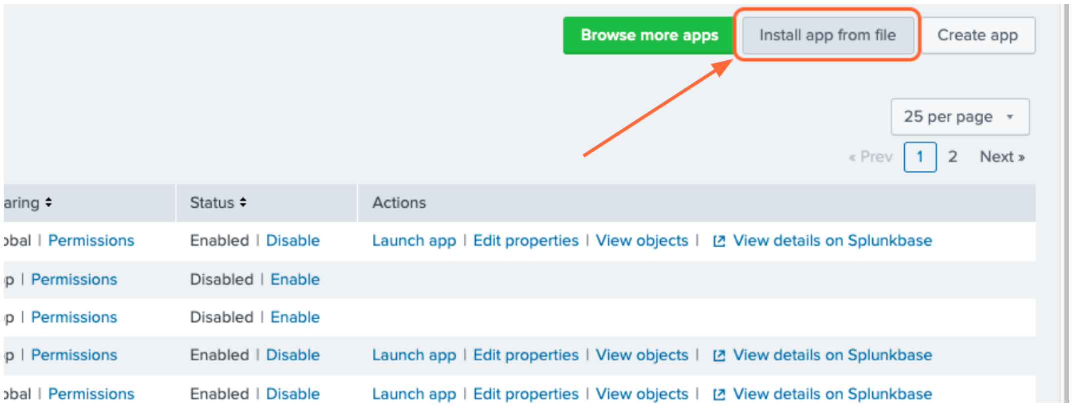
Release Notes

Version 1.0.8 May 4, 2022

12 Downloads

VERSION 1.0.8

2. From the Splunk Web main page, click the gear icon next to **Apps**, then click **Install app from file**.



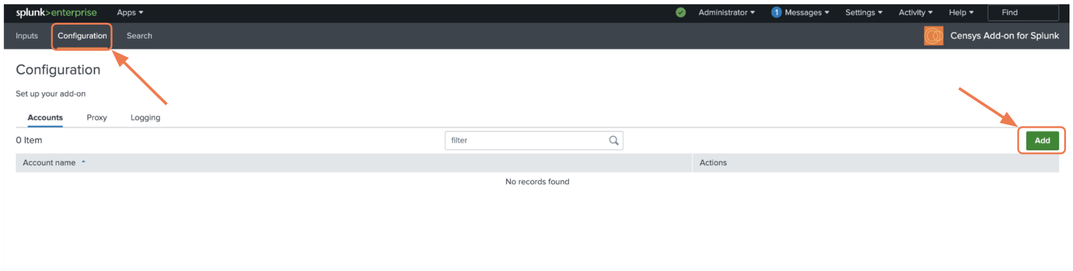
aring ≑	Status ≑	Actions
obal | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
p | Permissions	Disabled | Enable	
p | Permissions	Disabled | Enable	
p | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
obal | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase

1.5.3 Configure the Add-on

Global Settings

If you will be using the same Censys workspace for all Splunk work, you can enter your Censys ASM API key in one place, rather than for each input.

1. Click on the Configuration tab at the top of the page
2. Under the Accounts tab, you will see all of your configured accounts. Click "Add" to configure a new account.



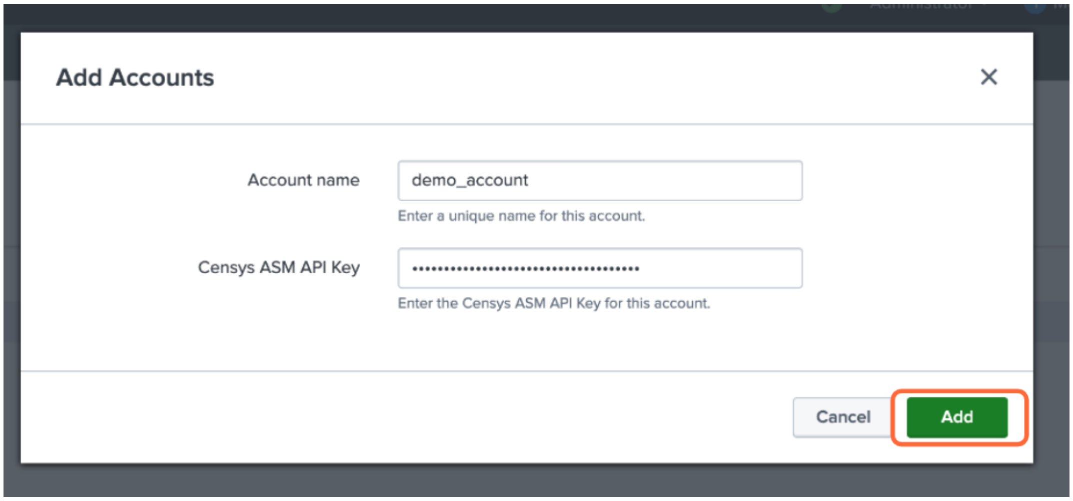
Configuration

Set up your add-on

0 Item

Account name ˄	Actions
No records found	

3. Enter a name for this account (the name of your ASM workspace is a good choice) and enter your Censys ASM API key (check out *Add-on Prerequisites* for help finding this)



Add Accounts

Account name: demo_account

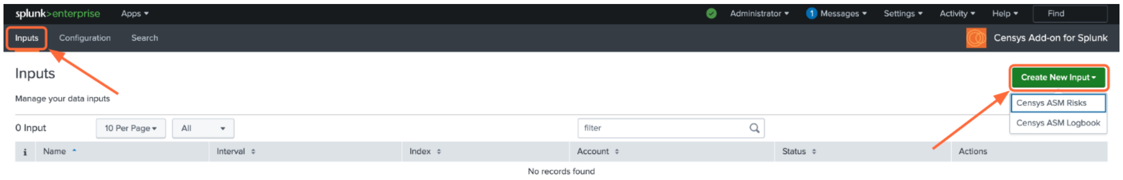
Enter a unique name for this account.

Censys ASM API Key: ••••••••••••••••••••••••••••••••••••

Enter the Censys ASM API Key for this account.

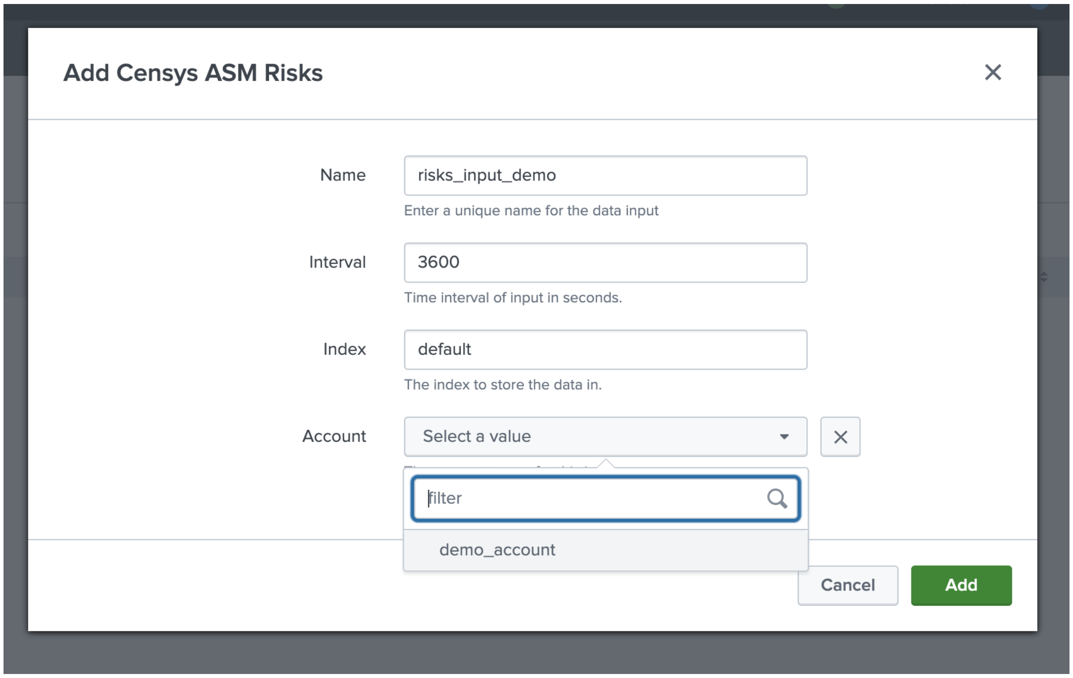
Inputs

From the Inputs page, select Create New Input. Select the API you would like to pull from.



Fill out the following fields:

- Input Name (required): A name for the input
- Interval (in seconds): How often the input should run (default is 3600 seconds, or 1 hour)
- Index: The index where the data will be stored
- Account: The Censys account to use (if you have multiple accounts)



Add Censys ASM Risks

Name: risks_input_demo
Enter a unique name for the data input

Interval: 3600
Time interval of input in seconds.

Index: default
The index to store the data in.

Account: Select a value

See also:

For more information on logbook events, visit our Logbook Event Catalog.

1.5.4 Use the Add-on

Download our *Censys ASM App for Splunk*!

Under the Search tab, you can enter queries on your data inputs. If you are not familiar with Splunk search syntax, Splunk has the following helpful resources:

- Splunk Search Documentation
- Splunk Search Tutorial

1.5.5 FAQs

What if I'm seeing no events in my index?

1. Confirm your *Censys ASM API key* is up to date
2. Confirm your index is accessible

1.6 Censys ASM App for Splunk

The Censys ASM App for Splunk allows ASM users to visualized Logbook API data with a pre-built dashboard that can be customized with additional views.

> **Note**: This app is dependent on Censys Add-on for Splunk.

This guide will help you:

- Set up the Censys Add-on for Splunk (if you haven't already)
- View our Attack Surface Management dashboard and create your own dashboards
- Set up reports and alerting
- Move seamlessly between Splunk and Censys ASM

Splunkbase: Censys ASM App for Splunk

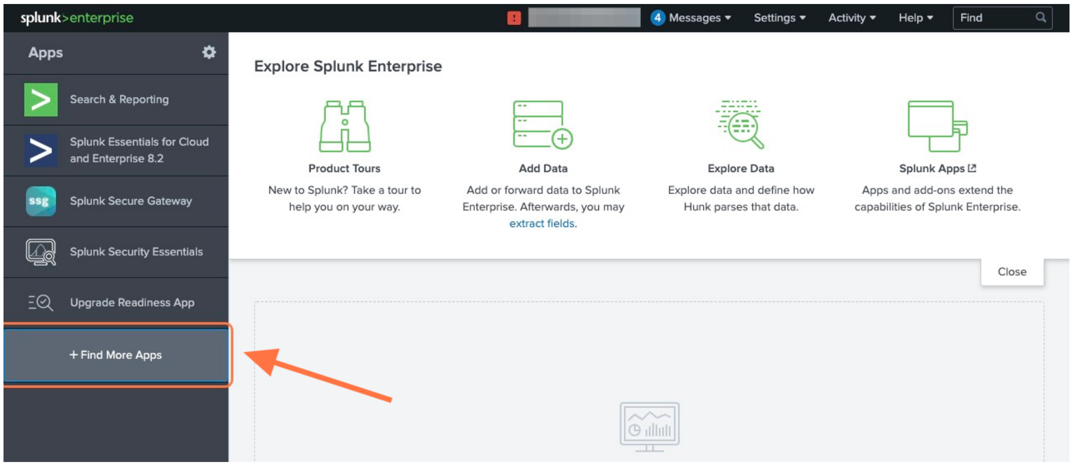
1.6.1 ASM App Prerequisites

1. A Splunk account and installation.
2. *Censys Add-on for Splunk* installed and configured with your Censys API key.

1.6.2 Install the Censys ASM App for Splunk

Install from Splunkbase (Recommended)

1. From the Splunk Web main page, click the **+ Find More Apps** button in the sidebar.



Product Tours: New to Splunk? Take a tour to help you on your way.

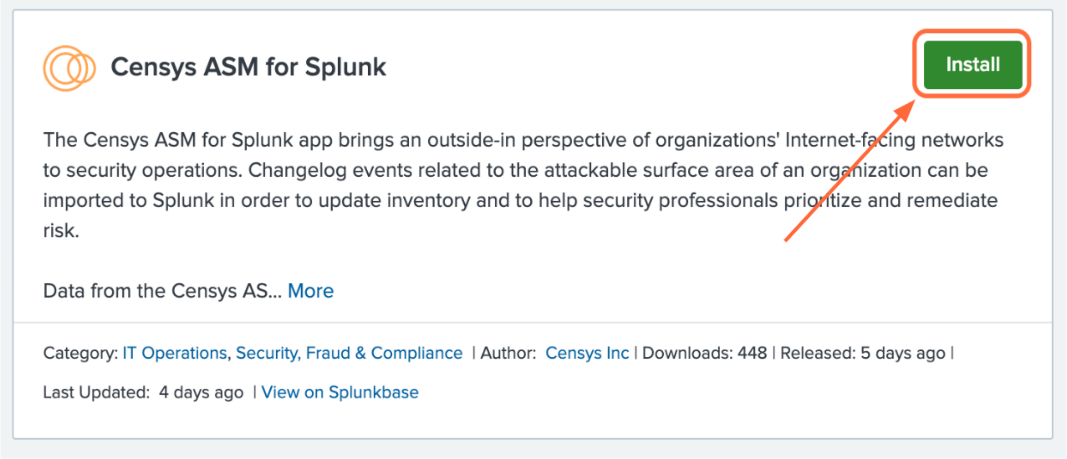
Add Data: Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore Data: Explore data and define how Hunk parses that data.

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

2. Type "**Censys**" in the search bar and press **Enter**.

3. On the results page, find the "Censys ASM App for Splunk" app card and click the green **Install** button.



Censys ASM for Splunk

The Censys ASM for Splunk app brings an outside-in perspective of organizations' Internet-facing networks to security operations. Changelog events related to the attackable surface area of an organization can be imported to Splunk in order to update inventory and to help security professionals prioritize and remediate risk.

Data from the Censys AS... More

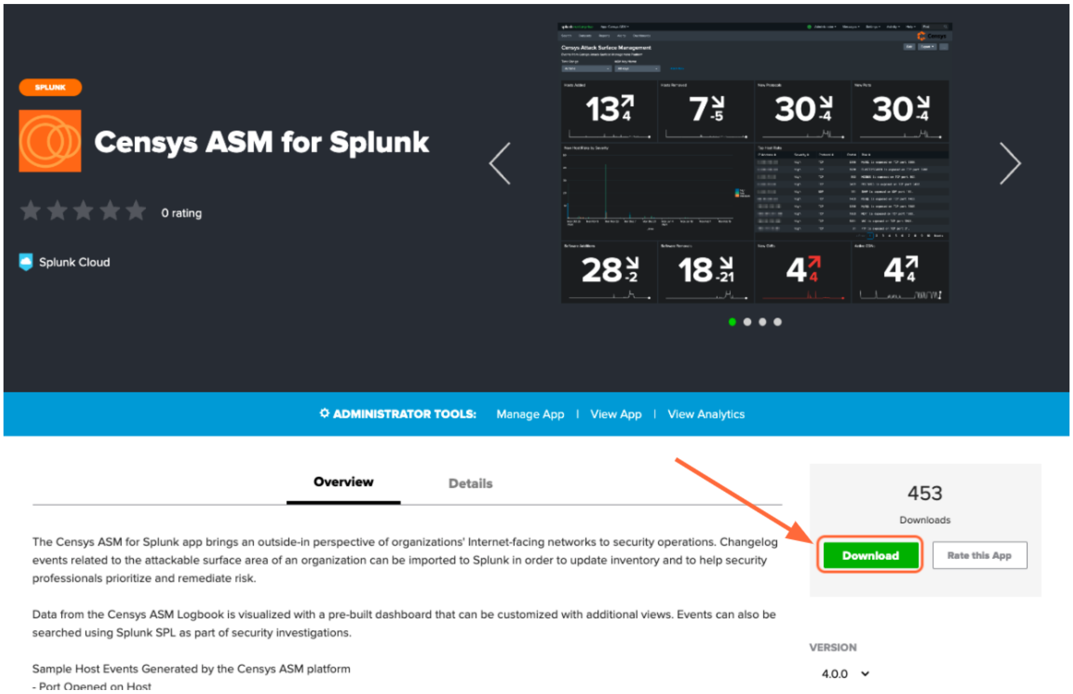
Category: IT Operations, Security, Fraud & Compliance | Author: Censys Inc | Downloads: 448 | Released: 5 days ago |

Last Updated: 4 days ago | View on Splunkbase

4. Reenter login credentials to confirm your choice.

Install from File

1. Go to the Add-on's page on Splunkbase and click the **Download** button.

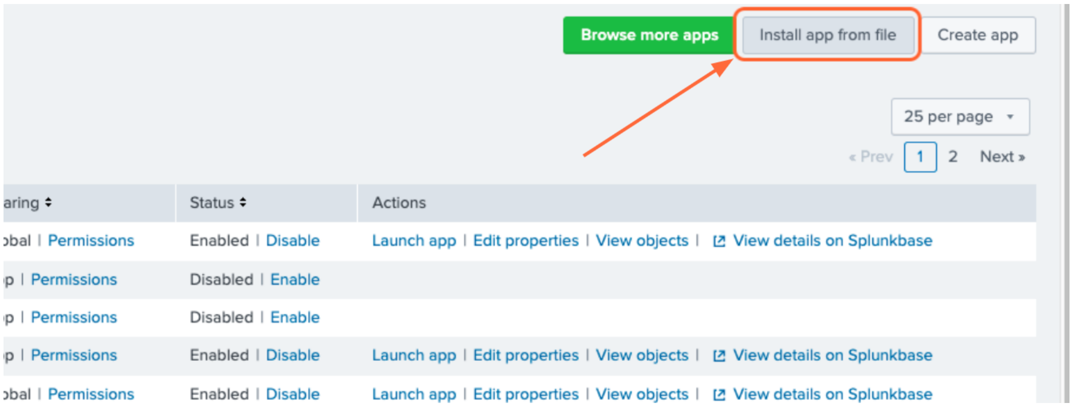


The Censys ASM for Splunk app brings an outside-in perspective of organizations' Internet-facing networks to security operations. Changelog events related to the attackable surface area of an organization can be imported to Splunk in order to update inventory and to help security professionals prioritize and remediate risk.

Data from the Censys ASM Logbook is visualized with a pre-built dashboard that can be customized with additional views. Events can also be searched using Splunk SPL as part of security investigations.

Sample Host Events Generated by the Censys ASM platform
- Port Opened on Host

2. From the Splunk Web main page, click the gear icon next to **Apps**, then click **Install app from file**.



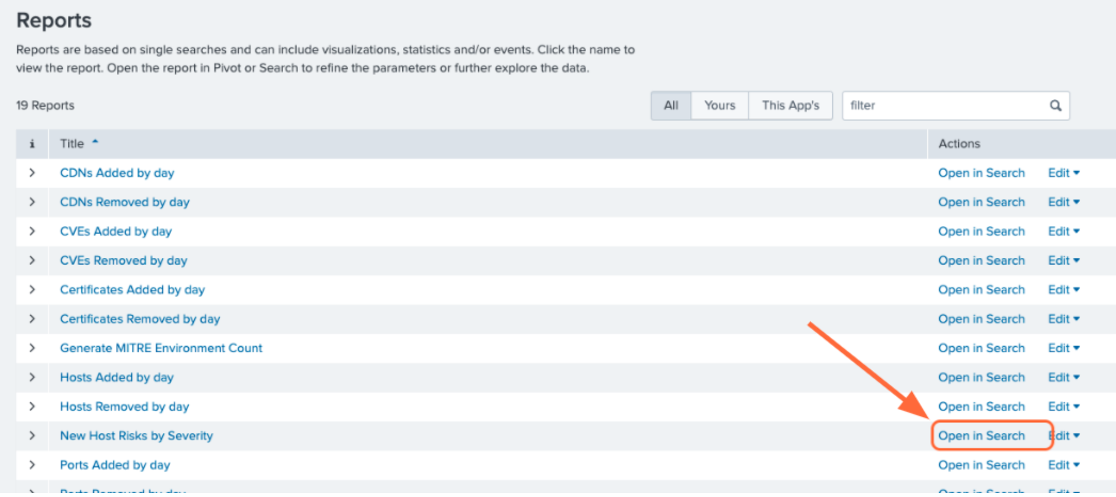
aring	Status	Actions
obal | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
p | Permissions	Disabled | Enable	
p | Permissions	Disabled | Enable	
p | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
obal | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase

1.6.3 Use the App

Censys has provided several reports based on ASM data for users to start with. These reports can be used for alerting and creating dashboards. Workflow actions provide a seamless transition between Splunk Search and Censys ASM.

Create Alerts from Reports

To view the pre-configured reports, click the **Reports** tab at the top of the page. To create an alert based on a report, click **Open in Search** next to the report you want to use.



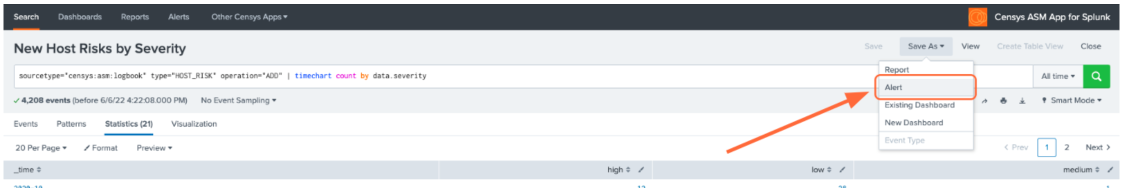
Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

19 Reports

i	Title ^	Actions	
>	CDNs Added by day	Open in Search	Edit ▾
>	CDNs Removed by day	Open in Search	Edit ▾
>	CVEs Added by day	Open in Search	Edit ▾
>	CVEs Removed by day	Open in Search	Edit ▾
>	Certificates Added by day	Open in Search	Edit ▾
>	Certificates Removed by day	Open in Search	Edit ▾
>	Generate MITRE Environment Count	Open in Search	Edit ▾
>	Hosts Added by day	Open in Search	Edit ▾
>	Hosts Removed by day	Open in Search	Edit ▾
>	New Host Risks by Severity	Open in Search	Edit ▾
>	Ports Added by day	Open in Search	Edit ▾
>	Ports Removed by day	Open in Search	Edit ▾

Modify the query to your liking or leave as is, then click **Save As Alert**.



New Host Risks by Severity

```
sourcetype="censys:asm:logbook" type="HOST_RISK" operation="ADD" | timechart count by data.severity
```

✓ 4,208 events (before 6/6/22 4:22:08.000 PM) No Event Sampling ▾

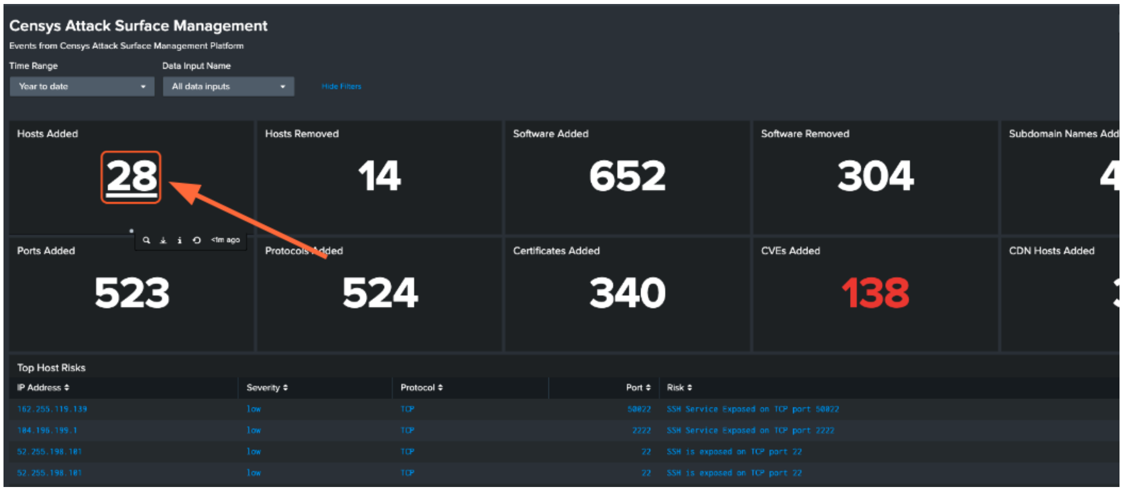
_time	high	low	medium

Give your alert a title, set the alert to be scheduled or real-time, and configure the alert's trigger settings and trigger actions.

Interact with Dashboards

To view the pre-configured dashboards, click the **Dashboards** tab at the top of the page.

The **Censys ASM Logbook** dashboard gives you a broad overview of your attack surface. To view a query in Splunk Search, click on panel.



Censys Attack Surface Management

Events from Censys Attack Surface Management Platform

Time Range: Year to date

Data Input Name: All data inputs

Hosts Added	Hosts Removed	Software Added	Software Removed	Subdomain Names Add
28	14	652	304	4

Ports Added	Protocols Added	Certificates Added	CVEs Added	CDN Hosts Added
523	524	340	138	3

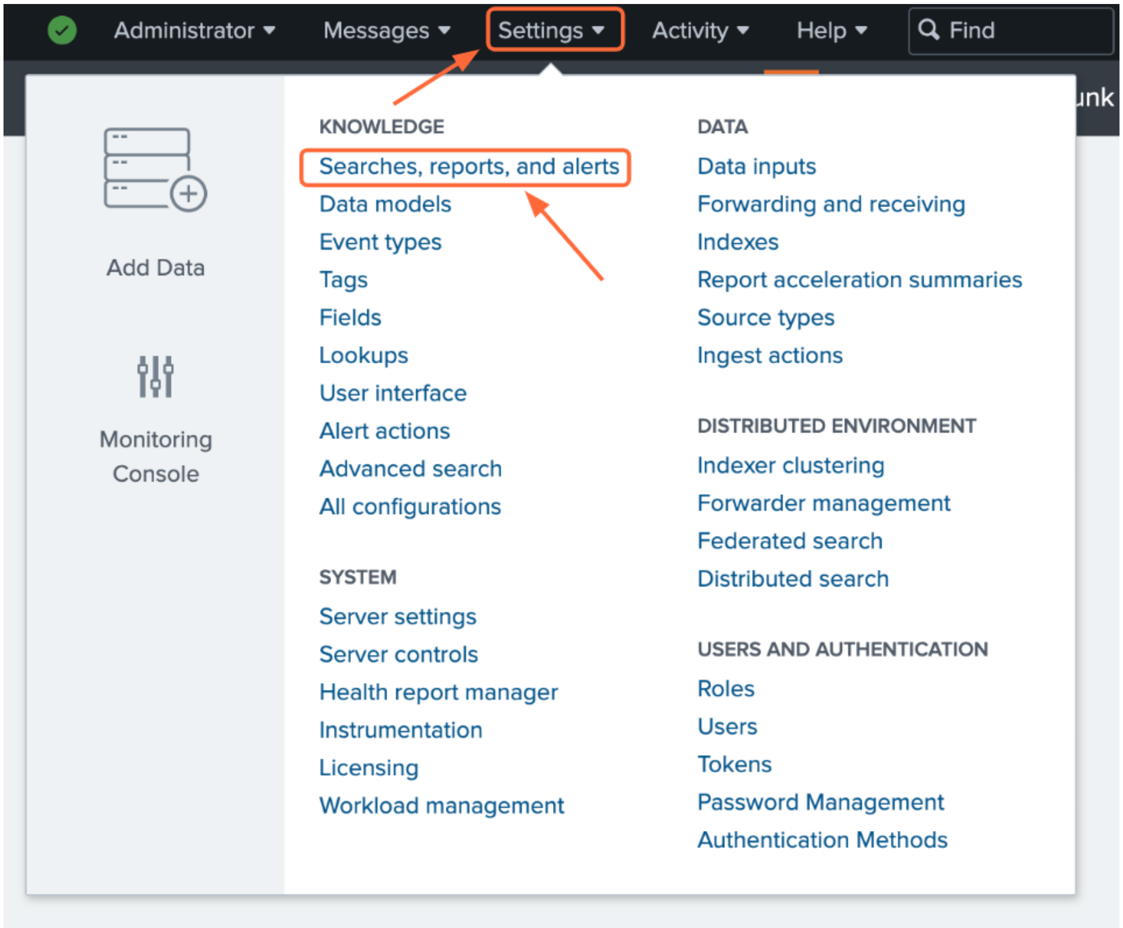
Top Host Risks

IP Address	Severity	Protocol	Port	Risk
162.255.119.139	low	TCP	50022	SSH Service Exposed on TCP port 50022
184.196.199.1	low	TCP	2222	SSH Service Exposed on TCP port 2222
52.255.198.101	low	TCP	22	SSH is exposed on TCP port 22
52.255.198.101	low	TCP	22	SSH is exposed on TCP port 22

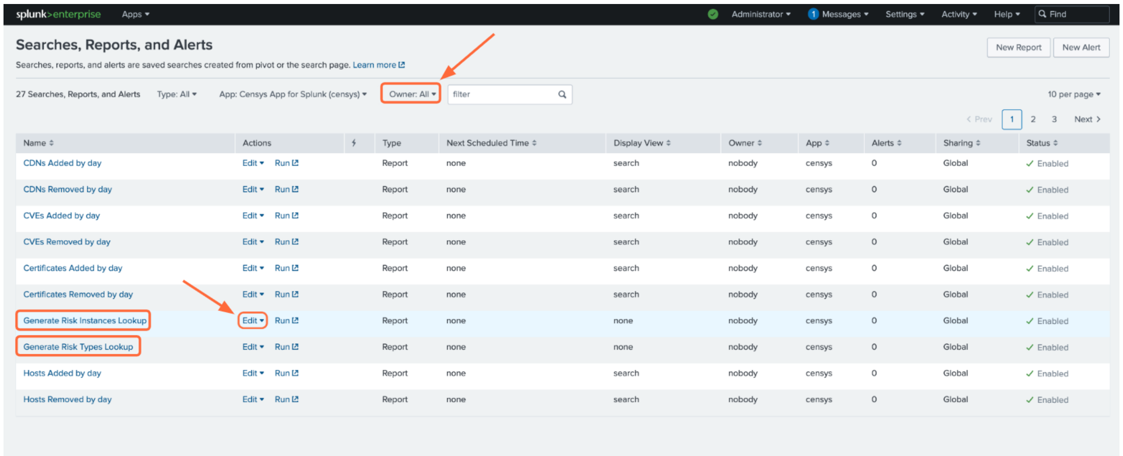
A few more steps are required to enable the pre-configured **Censys ASM Risks** dashboard. In order to keep the dashboard up to date, we recommend that you enable scheduled runs of the following five saved searches:

- Generate Risk Instances Lookup
- Generate Risk Types Lookup
- Hosts with most risks lookup
- Hosts with most risks with severities
- Hosts with most risks with types

To enable scheduled runs, click the **Settings** tab at the top of the page, then click **Searches, reports, and alerts**.



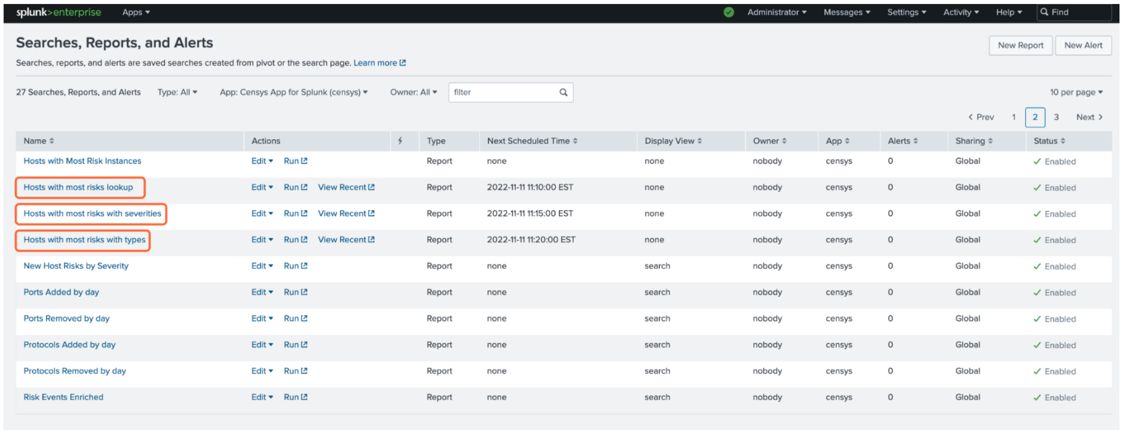
Make sure that the **Owner** filter at the top of the page is set to **All**. For the five saved searches listed above, click **Edit -> Edit Schedule**.



Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

Name	Actions	⚡	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
CDNs Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
CDNs Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
CVEs Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
CVEs Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Certificates Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Certificates Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Generate Risk Instances Lookup	Edit Run		Report	none	none	nobody	censys	0	Global	✓ Enabled
Generate Risk Types Lookup	Edit Run		Report	none	none	nobody	censys	0	Global	✓ Enabled
Hosts Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Hosts Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled

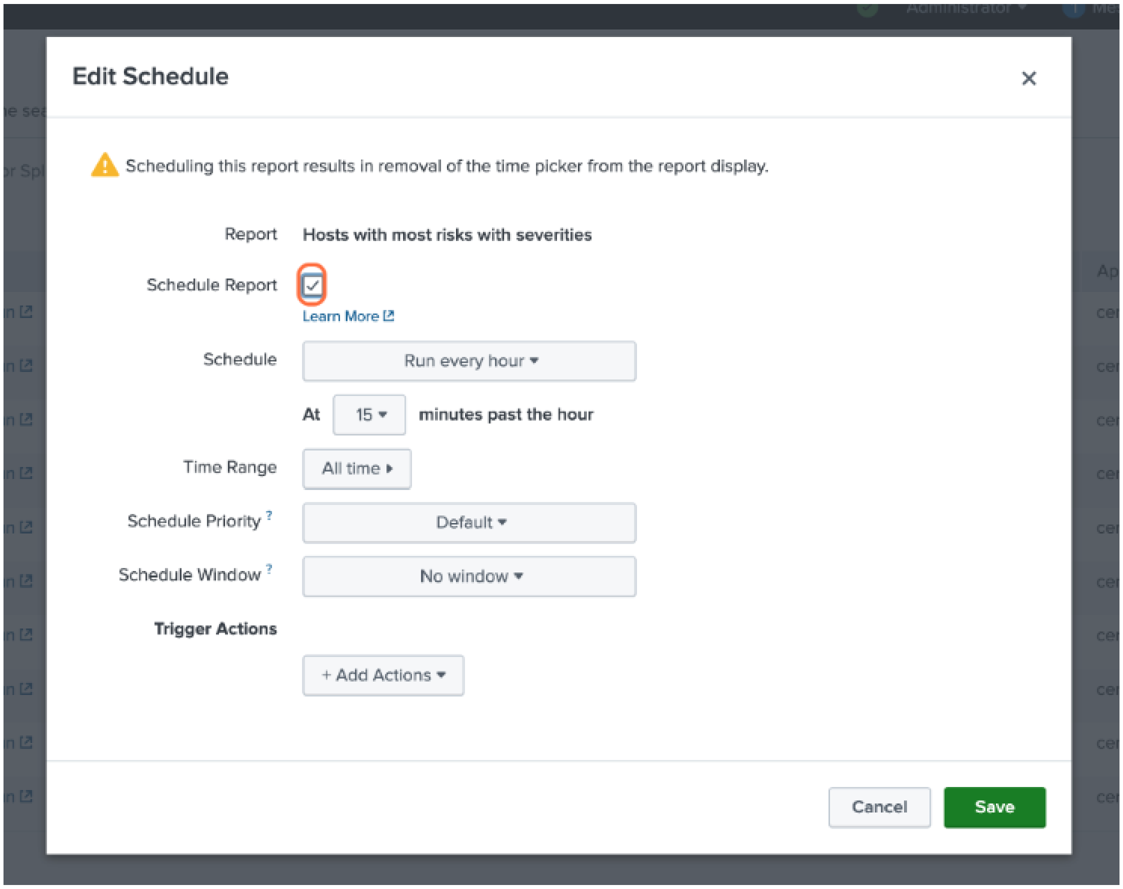


Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

Name	Actions	⚡	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
Hosts with Most Risk Instances	Edit Run		Report	none	none	nobody	censys	0	Global	✓ Enabled
Hosts with most risks lookup	Edit Run View Recent		Report	2022-11-11 11:10:00 EST	none	nobody	censys	0	Global	✓ Enabled
Hosts with most risks with severities	Edit Run View Recent		Report	2022-11-11 11:15:00 EST	none	nobody	censys	0	Global	✓ Enabled
Hosts with most risks with types	Edit Run View Recent		Report	2022-11-11 11:20:00 EST	none	nobody	censys	0	Global	✓ Enabled
New Host Risks by Severity	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Ports Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Ports Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Protocols Added by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Protocols Removed by day	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled
Risk Events Enriched	Edit Run		Report	none	search	nobody	censys	0	Global	✓ Enabled

Click the checkbox next to **Schedule Report**. By default, the report will run every hour. You can change this frequency in this window.



Edit Schedule

Scheduling this report results in removal of the time picker from the report display.

Report: Hosts with most risks with severities

Schedule Report: ☑

Learn More

Schedule: Run every hour

At 15 minutes past the hour

Time Range: All time

Schedule Priority: Default

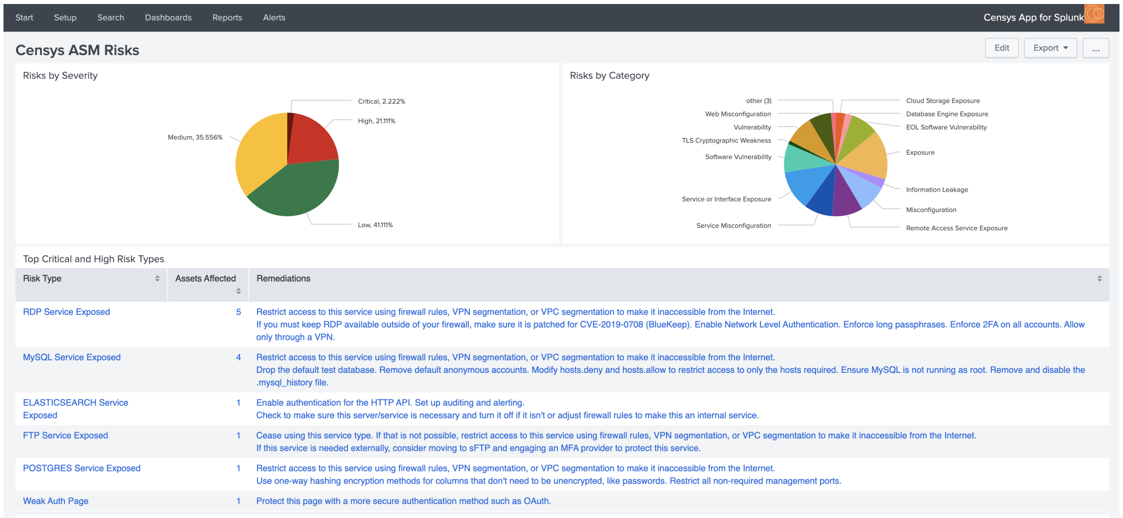
Schedule Window: No window

Trigger Actions

If you'd like to check out the **Censys ASM Risks** dashboard right away, you'll need to manually run each of these five searches by clicking the **Run** button. Otherwise, the lookup tables will populate according to the schedule you have set.

> If you do not wish to enable scheduled runs, you can still use the **Censys ASM Risks** dashboard, but you will need to manually run each of the five saved searches to pull in current data.

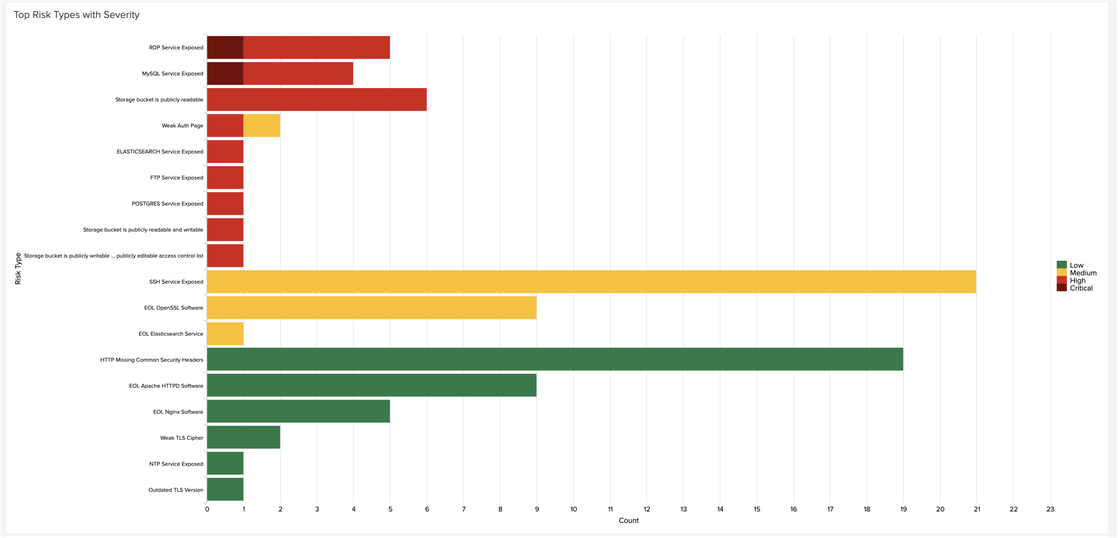
Below are just a few insights you can gain about your attack surface with the **Censys ASM Risks** dashboard:



Censys ASM Risks

Top Critical and High Risk Types

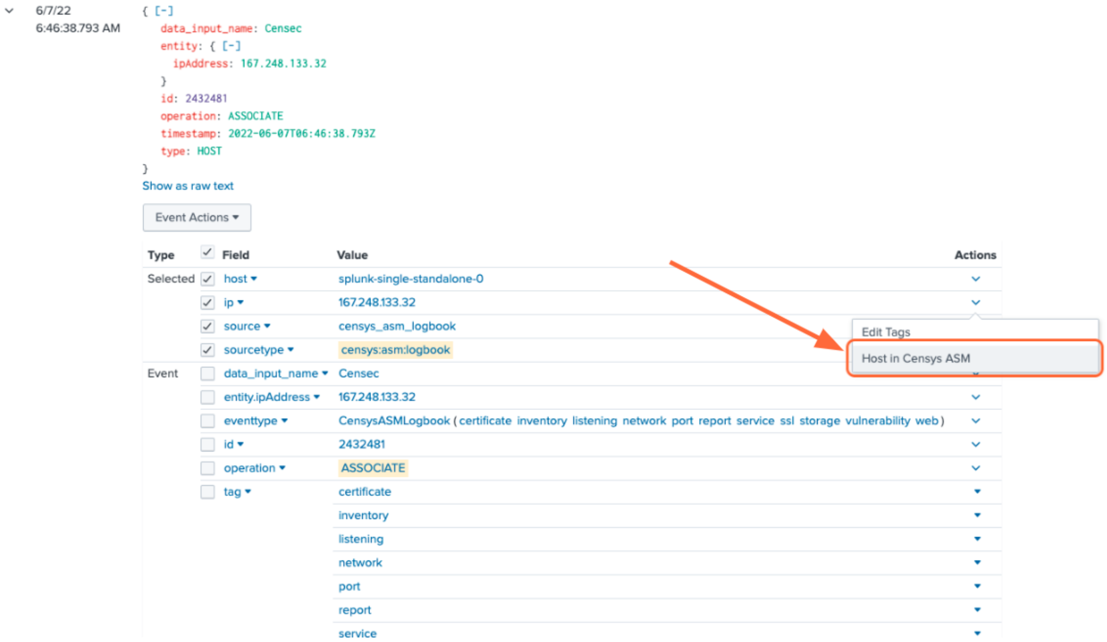
Risk Type	Assets Affected	Remediations
RDP Service Exposed	5	Restrict access to this service using firewall rules, VPN segmentation, or VPC segmentation to make it inaccessible from the Internet. If you must keep RDP available outside of your firewall, make sure it is patched for CVE-2019-0708 (BlueKeep). Enable Network Level Authentication. Enforce long passphrases. Enforce 2FA on all accounts. Allow only through a VPN.
MySQL Service Exposed	4	Restrict access to this service using firewall rules, VPN segmentation, or VPC segmentation to make it inaccessible from the Internet. Drop the default test database. Remove default anonymous accounts. Modify hosts.deny and hosts.allow to restrict access to only the hosts required. Ensure MySQL is not running as root. Remove and disable the .mysql_history file.
ELASTICSEARCH Service Exposed	1	Enable authentication for the HTTP API. Set up auditing and alerting. Check to make sure this server/service is necessary and turn it off if it isn't or adjust firewall rules to make this an internal service.
FTP Service Exposed	1	Cease using this service type. If that is not possible, restrict access to this service using firewall rules, VPN segmentation, or VPC segmentation to make it inaccessible from the Internet. If this service is needed externally, consider moving to sFTP and engaging an MFA provider to protect this service.
POSTGRES Service Exposed	1	Restrict access to this service using firewall rules, VPN segmentation, or VPC segmentation to make it inaccessible from the Internet. Use one-way hashing encryption methods for columns that don't need to be unencrypted, like passwords. Restrict all non-required management ports.
Weak Auth Page	1	Protect this page with a more secure authentication method such as OAuth.



You can click on any piece of data to view more details in Censys ASM.

Workflow Actions

From the events page, click the dropdown to the left of the event's timestamp. This will show all the fields for the event.

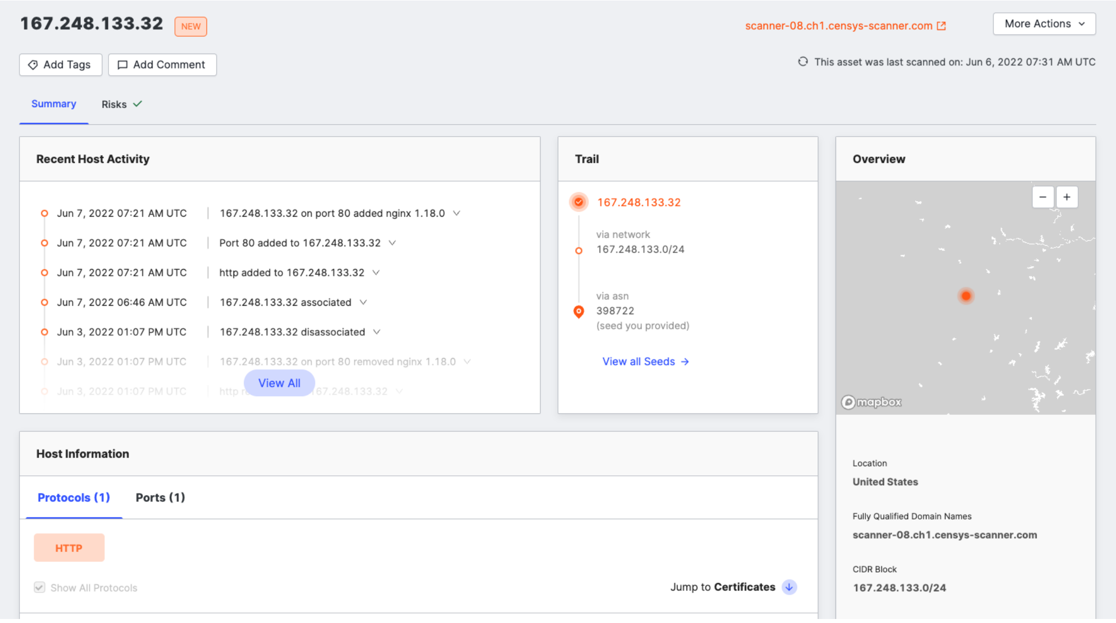


6/7/22
6:46:38.793 AM

```
{ [-]
   data_input_name: Censec
   entity: { [-]
     ipAddress: 167.248.133.32
   }
   id: 2432481
   operation: ASSOCIATE
   timestamp: 2022-06-07T06:46:38.793Z
   type: HOST
}
```

Type	☑	Field	Value	Actions
Selected	☑	host ▾	splunk-single-standalone-0	⌄
	☑	ip ▾	167.248.133.32	⌄
	☑	source ▾	censys_asm_logbook	
	☑	sourcetype ▾	censys:asm:logbook	
Event	□	data_input_name ▾	Censec	
	□	entity.ipAddress ▾	167.248.133.32	⌄
	□	eventtype ▾	CensysASMLogbook (certificate inventory listening network port report service ssl storage vulnerability web)	⌄
	□	id ▾	2432481	⌄
	□	operation ▾	ASSOCIATE	⌄
	□	tag ▾	certificate	▾
			inventory	▾
			listening	▾
			network	▾
			port	▾
			report	▾
			service	▾

To view more information about an event, click the **Actions** dropdown next to the asset you'd like to view, then **[Domain|Host|Storage Asset|Certificate] in Censys ASM/Search**.



This asset was last scanned on: Jun 6, 2022 07:31 AM UTC

Recent Host Activity

Jun 7, 2022 07:21 AM UTC	167.248.133.32 on port 80 added nginx 1.18.0
Jun 7, 2022 07:21 AM UTC	Port 80 added to 167.248.133.32
Jun 7, 2022 07:21 AM UTC	http added to 167.248.133.32
Jun 7, 2022 06:46 AM UTC	167.248.133.32 associated
Jun 3, 2022 01:07 PM UTC	167.248.133.32 disassociated
Jun 3, 2022 01:07 PM UTC	167.248.133.32 on port 80 removed nginx 1.18.0
Jun 3, 2022 01:07 PM UTC	http r 167.248.133.32

Trail

167.248.133.32

via network
167.248.133.0/24

via asn
398722
(seed you provided)

Overview

Location
United States

Fully Qualified Domain Names
scanner-08.ch1.censys-scanner.com

CIDR Block
167.248.133.0/24

Host Information

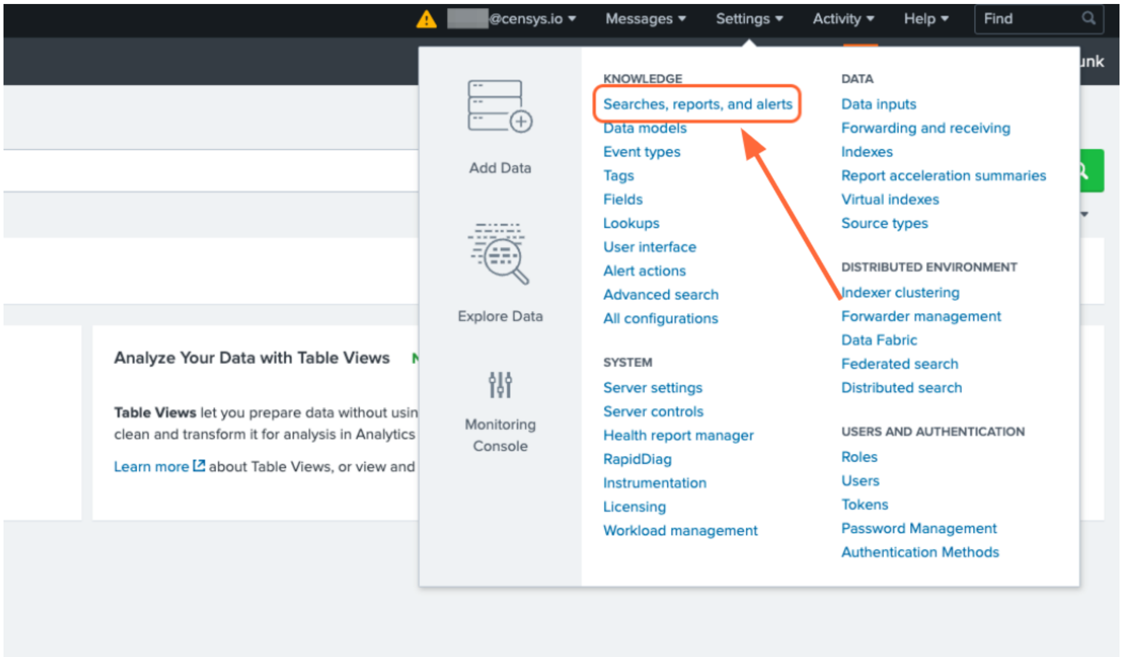
Protocols (1) Ports (1)

Turn Queries into Reports, Alerts, and Dashboards

From Splunk Search, any query can be used to create custom reports, alerts, and dashboards by clicking the **Save As** button in the top right corner. A query can be added as a new panel to an existing dashboard or a new dashboard can be created.

Create Reports and Alerts from Scratch

One more way to create reports and alerts is by going to **Settings -> Searches, reports, and alerts**.



Analyze Your Data with Table Views

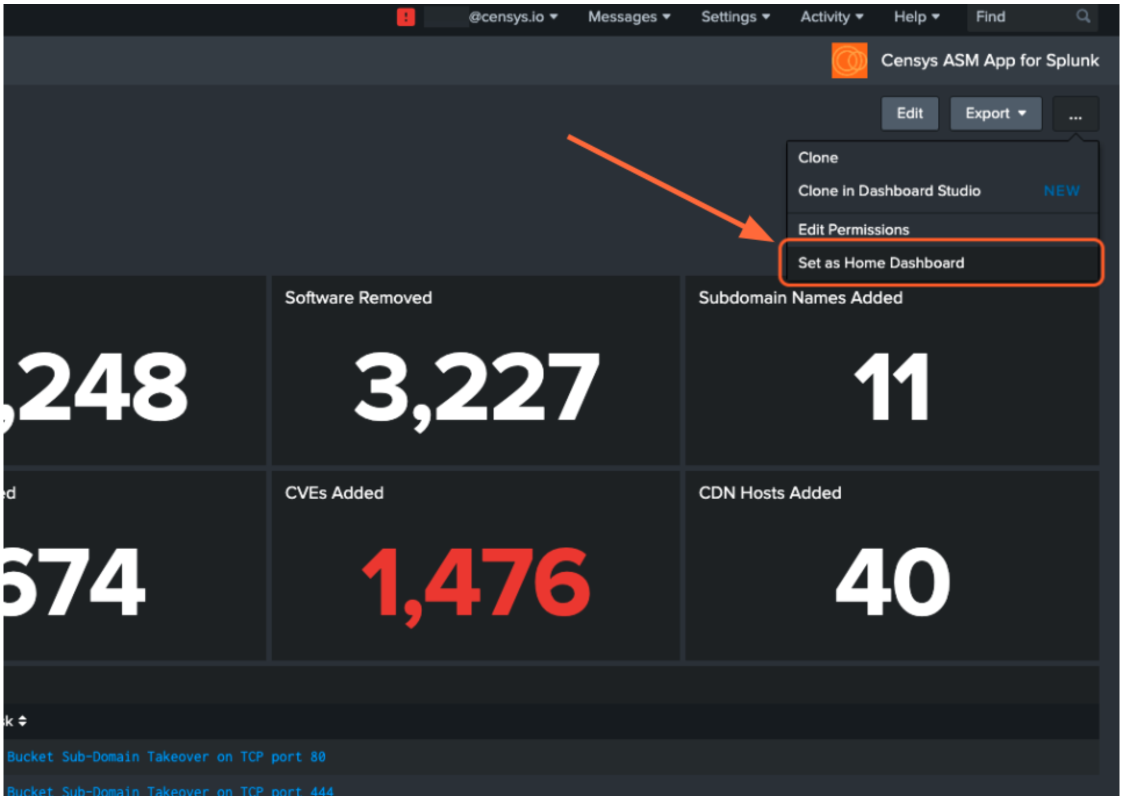
Table Views let you prepare data without usin clean and transform it for analysis in Analytics

Learn more about Table Views, or view and

From there, you can manage current reports and alerts, create new reports and alerts from custom queries.

Set a Home Dashboard

Easily check out the Censys ASM dashboard or your own custom dashboard by setting it as your home dashboard.



Bucket Sub-Domain Takeover on TCP port 80
Bucket Sub-Domain Takeover on TCP port 444

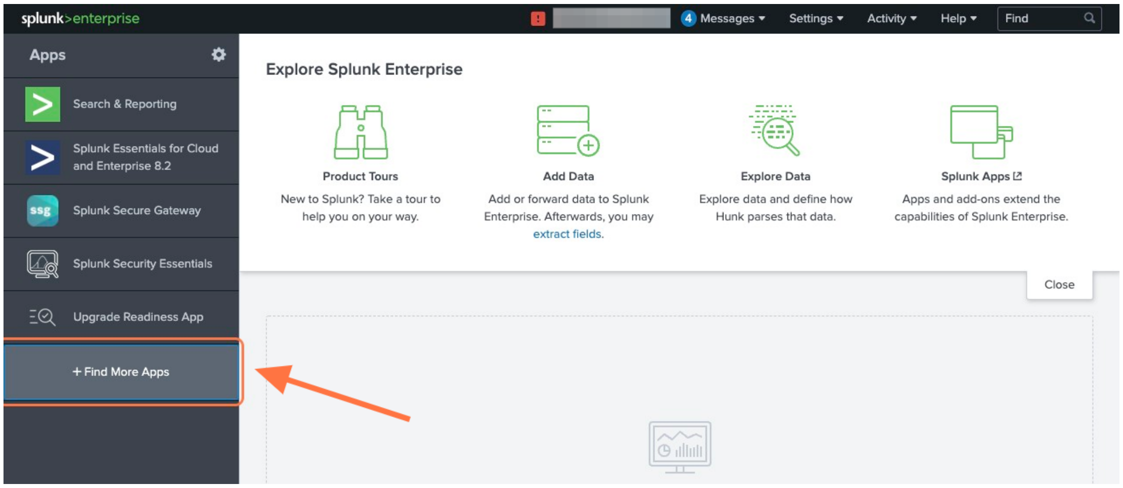
Now, when you open your Splunk Web main page, you'll easily see changes in your attack surface.

Set Up Splunk Event Generator (Eventgen)

Splunk Event Generator is a useful tool for generating configurable events to simulate real-time data. We have provided a sample `eventgen.conf` file along with sample events to get you started.

1. Install and enable the Splunk Eventgen app

From the Splunk Web main page, click the **+ Find More Apps** button in the sidebar.



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

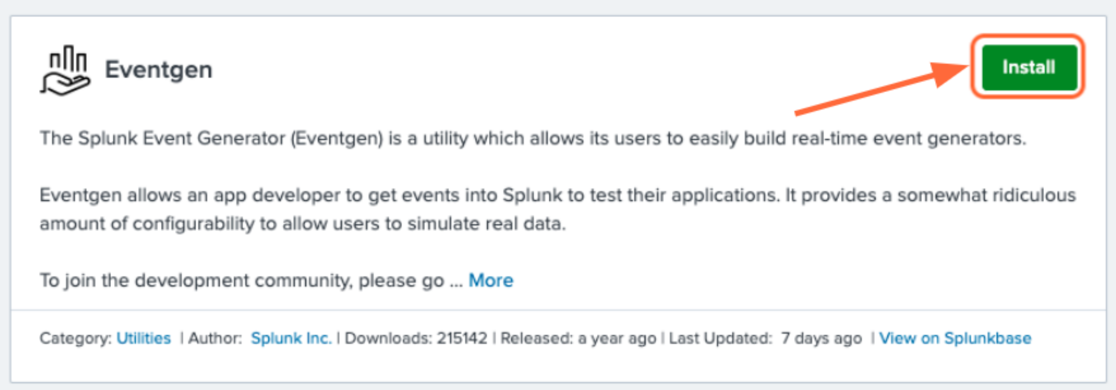
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore Data
Explore data and define how Hunk parses that data.

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

Type “**Eventgen**” in the search bar and press **Enter**.

On the results page, find the **Eventgen** app card and click the green **Install** button.



Eventgen

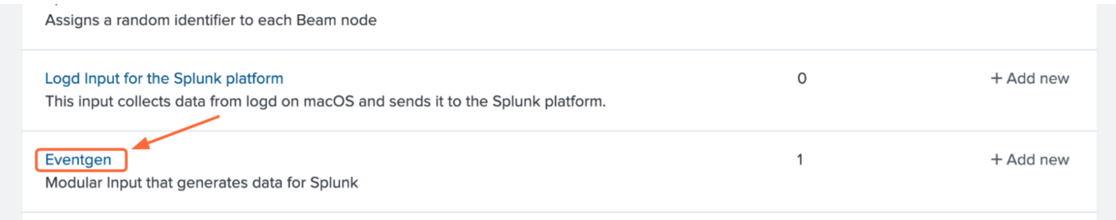
The Splunk Event Generator (Eventgen) is a utility which allows its users to easily build real-time event generators.

Eventgen allows an app developer to get events into Splunk to test their applications. It provides a somewhat ridiculous amount of configurability to allow users to simulate real data.

To join the development community, please go ... More

Category: Utilities | Author: Splunk Inc. | Downloads: 215142 | Released: a year ago | Last Updated: 7 days ago | View on Splunkbase

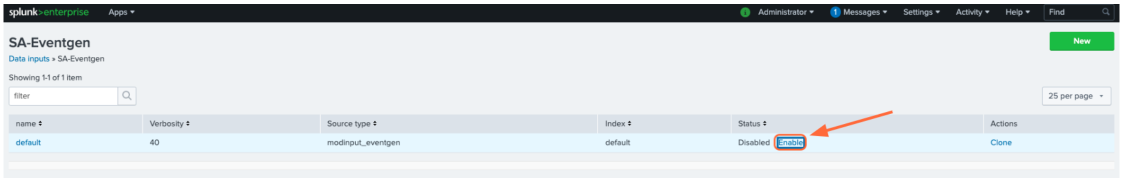
Go to **Settings > Data inputs** and click **Eventgen**.



Assigns a random identifier to each Beam node

Logd Input for the Splunk platform This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
Eventgen Modular Input that generates data for Splunk	1	+ Add new

Click **Enable** in the **modinput_eventgen** row.



SA-Eventgen

Data inputs » SA-Eventgen

Showing 1-1 of 1 item

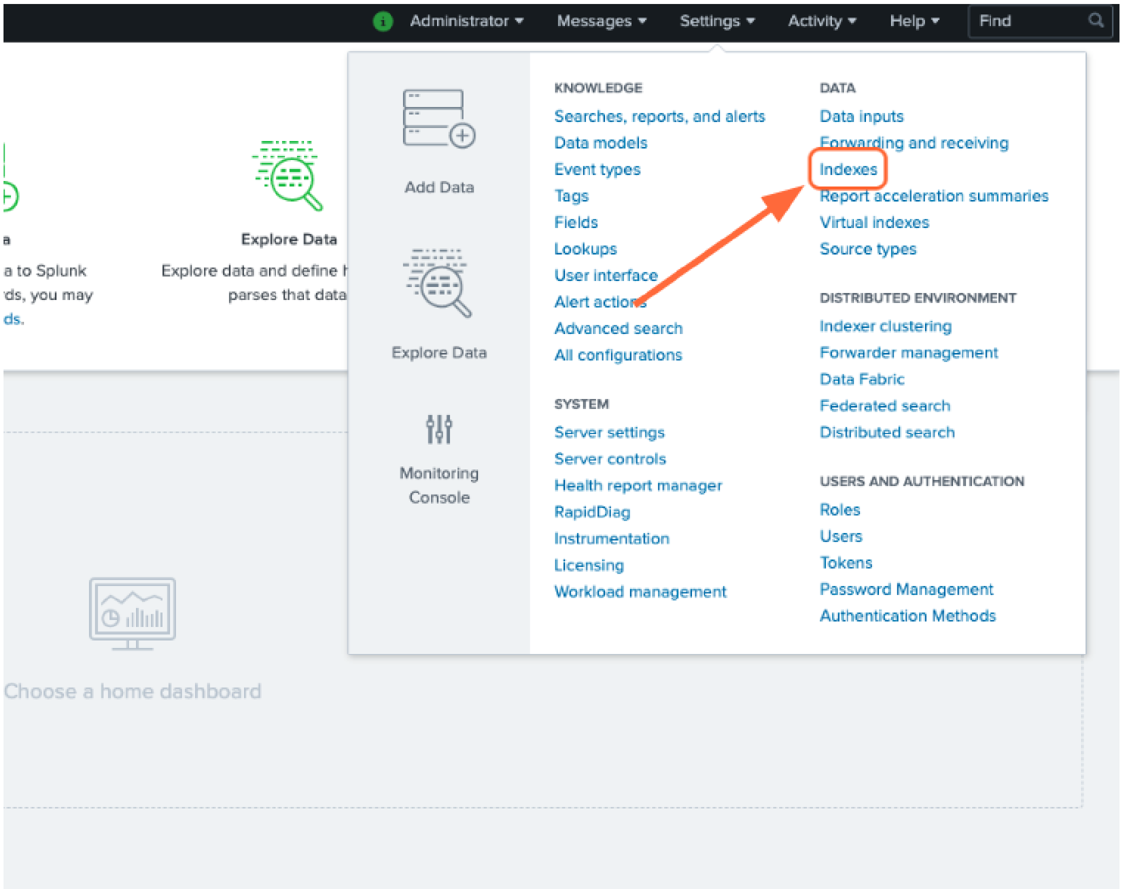
name ⇕	Verbosity ⇕	Source type ⇕	Index ⇕	Status ⇕	Actions
default	40	modinput_eventgen	default	Disabled Enable	Clone

2. Create an Index

A new index for your sample events can be created through the Splunk Web UI or the Splunk Enterprise CLI. Instructions for each option are detailed below.

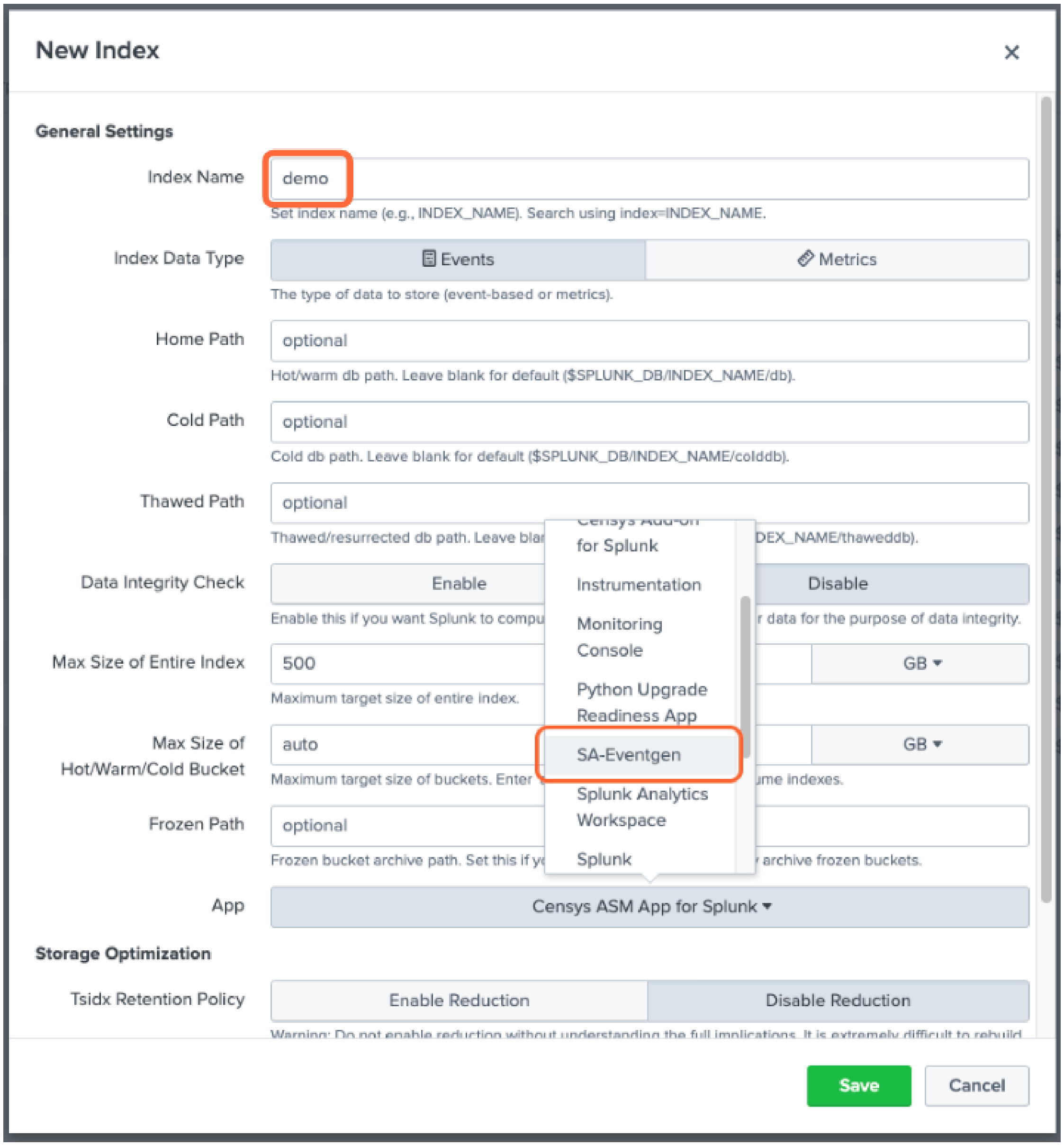
Option #1: Splunk Web UI

Go to **Settings > Indexes**.



On the Indexes page, click **New Index**.

Enter “**demo**” in the **Index Name** field and select **SA-Eventgen** in the **App** field.



New Index

General Settings

Index Name: demo

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Home Path: optional

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional

Thawed/resurrected db path. Leave blar DEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable

Enable this if you want Splunk to compu r data for the purpose of data integrity.

Max Size of Entire Index: 500 GB

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB

Maximum target size of buckets. Enter ıme indexes.

Frozen Path: optional

Frozen bucket archive path. Set this if y archive frozen buckets.

App: Censys ASM App for Splunk ▾

Storage Optimization

Tsidx Retention Policy: Enable Reduction | Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild

Click **Save**.

Option #2: Splunk Enterprise CLI

From the terminal (Mac or Linux), navigate to `$SPLUNK_HOME/bin` and enter the following command:

```
./splunk add index demo
```

You will likely need to enter your Splunk username and password.

> **Note:** If you would like to name your index something other than **demo**, you will need to edit the `eventgen.conf` file.

3. View your Sample Events

In the Censys ASM App, click the **Search** tab at the top of the page.

Enter the search query `index=demo` to see all sample events.

Additional Resources

- Splunk Eventgen Documentation
- Splunk Dev Eventgen Setup Tutorial

Additional information can be found in Splunk documentation:

- Splunk Alerting Manual
- Splunk Reporting Manual
- Splunk Search Manual

1.7 Censys Search App for Splunk

The Censys Search App for Splunk enables rapid enrichment of logs with the most up-to-date information on public hosts and certificates.

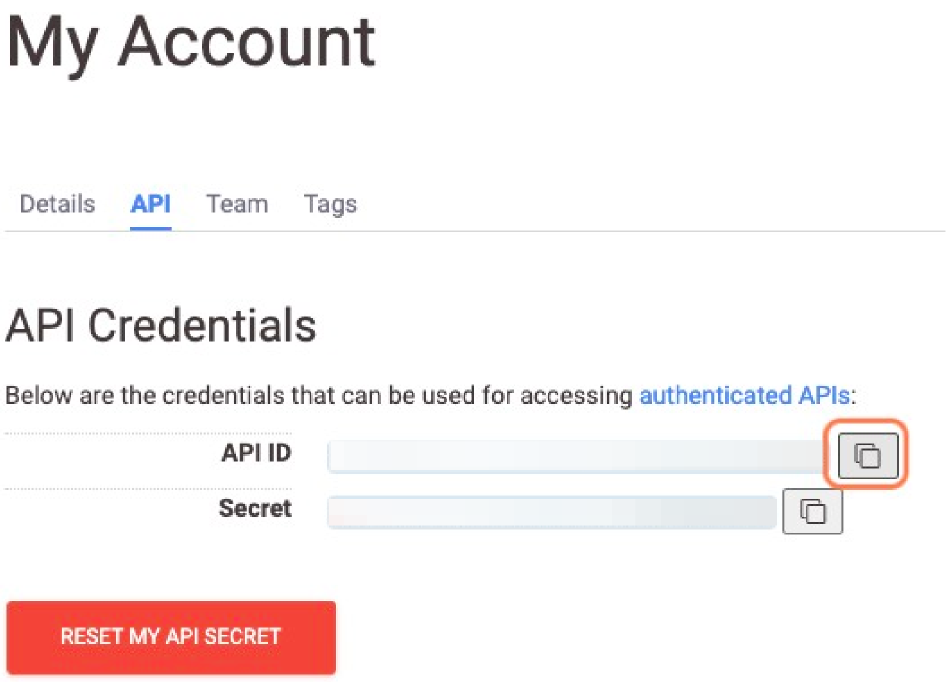
This guide will help you:

- Install the Censys Search App in your Splunk environment
- Configure the Censys Search app
- Use the Censys Search command to enrich Splunk logs by IP address

Splunkbase: Censys Search App for Splunk

1.7.1 Search App Prerequisites

1. Your Censys Search API key and secret.



My Account

API Credentials

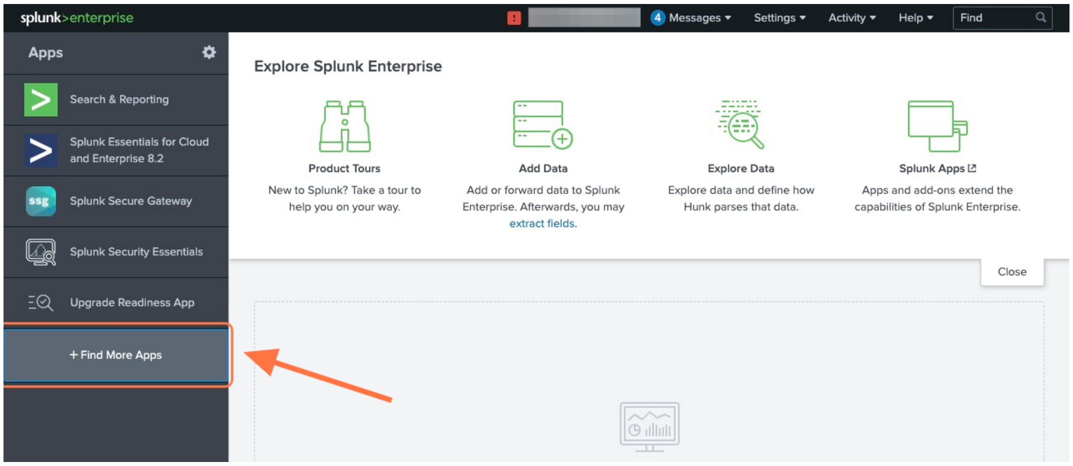
Below are the credentials that can be used for accessing authenticated APIs:

2. A Splunk account and installation.

1.7.2 Install the Censys Search App for Splunk

Install from Splunkbase

1. From the Splunk main page, click the **+ Find More Apps** button in the sidebar.



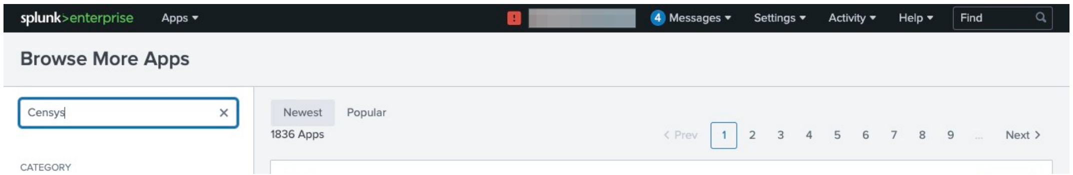
New to Splunk? Take a tour to help you on your way.

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

Explore data and define how Hunk parses that data.

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

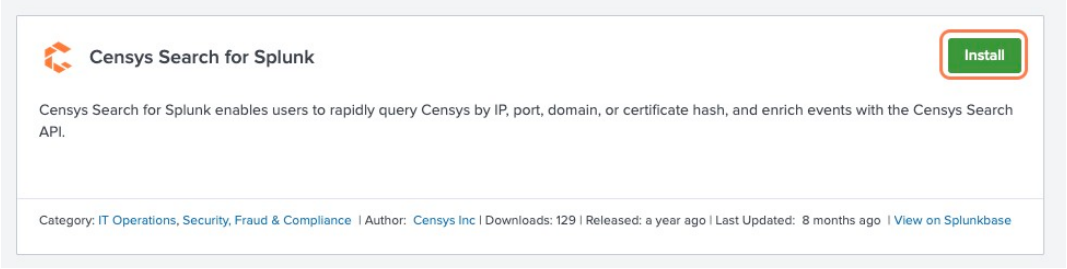
2. Type “Censys” in the search bar.



Censys

1836 Apps

3. On the results page, find the “Censys Search for Splunk” app card and click the green **Install** button.



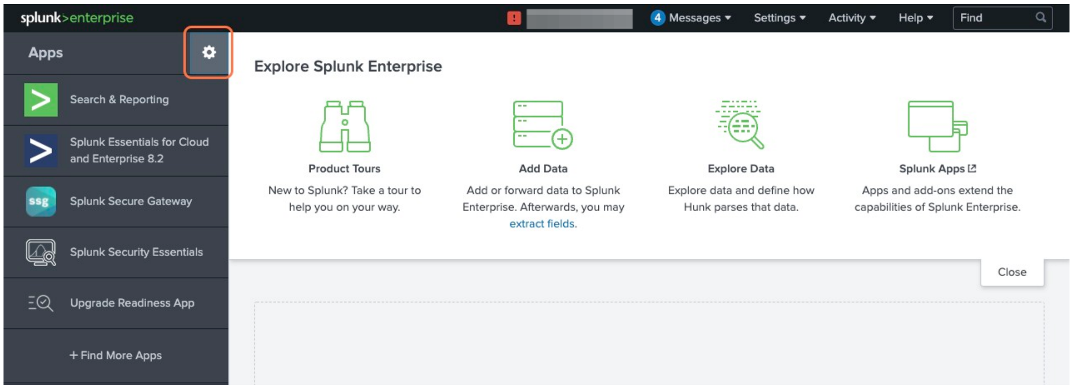
Censys Search for Splunk enables users to rapidly query Censys by IP, port, domain, or certificate hash, and enrich events with the Censys Search API.

Category: IT Operations, Security, Fraud & Compliance | Author: Censys Inc | Downloads: 129 | Released: a year ago | Last Updated: 8 months ago | View on Splunkbase

4. Enter your Splunkbase credentials and click the **Login and Install** button.

1.7.3 Configure the Censys Search App

1. From the Splunk main page, click the **Manage Apps** gear in the top left corner of the page.



Explore Splunk Enterprise

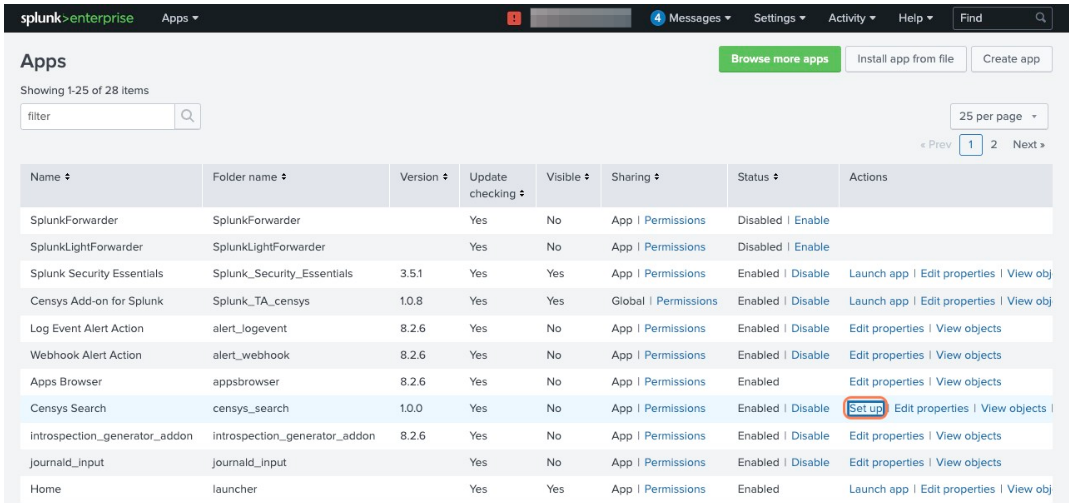
Product Tours
New to Splunk? Take a tour to help you on your way.

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

Explore Data
Explore data and define how Hunk parses that data.

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

2. Find "Censys Search" in the list of installed apps.
3. Click the **Set up** button to open the Censys Search app.

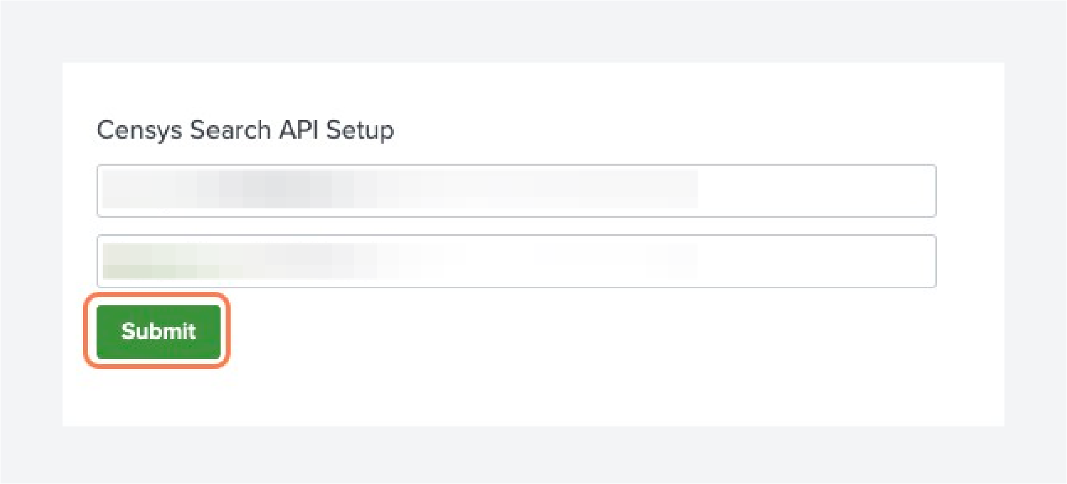


Apps

Showing 1-25 of 28 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Splunk Security Essentials	Splunk_Security_Essentials	3.5.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View obj
Censys Add-on for Splunk	Splunk_TA_censys	1.0.8	Yes	Yes	Global | Permissions	Enabled | Disable	Launch app | Edit properties | View obj
Log Event Alert Action	alert_logevent	8.2.6	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	8.2.6	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	8.2.6	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Censys Search	censys_search	1.0.0	Yes	No	App | Permissions	Enabled | Disable	Set up | Edit properties | View objects |
introspection_generator_addon	introspection_generator_addon	8.2.6	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
journald_input	journald_input		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View obj

4. Enter your Censys Search API key and secret in the fields provided.



Censys Search API Setup

[redacted]

[redacted]

1.7.4 Use the Censys Search command

censyssearch

The censyssearch command enables the enrichment of events by IP address. This command takes the events from a search as input and adds context to the events by querying the Censys API.

Syntax

```
censyssearch <ip_address_field> <summary|verbose>
```

Parameter	Usage
ip_address_field	The name of the field containing the IP address to search.
verbosity	The level of detail to return. Either summary or verbose.

Note: For each enrichment command executed, responses will be cached for previously seen IPs, so the number of API credits consumed will equal the number of unique IPs enriched.

Examples

```
sourcetype="access_combined" | dedupe clientIP | censyssearch clientIP verbose
```

```
sourcetype="censys:asm:logbook" | dedupe ip | censyssearch ip summary
```

See also:

For more information on how Censys collects and models host data, visit our help center.

1.8 Common Information Model Mapping

1.9 censys:asm:logbook

Logbook API docs

Table 1: CIM Models

Tag	CIM Model
certificate	Certificates
inventory	ComputeInventory
listening	Endpoint
network	NetworkResolutionDNS
port	NetworkTraffic
report	Endpoint
service	Endpoint
ssl	Certificates
storage	ComputeInventory
vulnerability	Vulnerabilities
web	Web

Table 2: Field Aliases

Field	CIM Alias
data.cve	cve
data.cvss	cvss
data.mailExchange	dest_name
data.port	dest_port
data.port	src_port
data.severity	severity
data.sha256	ssl_hash
data.softwareName	app
data.softwareName	service_name
data.softwareProduct	service
data.softwareSource	src
data.softwareUri	service_id
data.softwareVendor	vendor_product
data.subdomain	dest_name
data.title	signature
data.transportProtocol	transport
entity.domain	dns
entity.domain	src_name
entity.hostname	dns
entity.hostname	site
entity.hostname	src_host
entity.hostname	ssl_subject_common_name
entity.ipAddress	ip
entity.ipAddress	src_ip
entity.objectStorageName	storage_name
entity.objectStorageName	url
entity.sha256	ssl_hash
timestamp	creation_time

1.10 censys:asm:risks

Risks API docs

Table 3: CIM Models

Tag	CIM Model
report	Endpoint
vulnerability	Vulnerabilities

Table 4: Field Aliases

Field	CIM Alias
riskName	signature
riskType	signature_id
ts	creation_time