

IPInfo App for Splunk

App Version: 5.6.3

Author: Neel Shah - Greenace Consultants

Description: Installation and Configuration Document for IPInfo App for Splunk

Latest Update Date: 25th March, 2022

Version Summary

Version	Change History
1.0.0	Initial Version
1.0.2	Added Screenshots and Web Installation Steps
1.0.3	Replace old dashboard screen with new
1.0.7	Bug Fixes, Color Issues
3.0.0	Support to Splunk 8.x and Python 3.x
	Internal Updates
3.4.9	New scripted lookup New ipinfobatch command
3.4.11	Bug Fixes and Compliance to Splunk App Inspect
3.5.3	Added Support for New Lookup Commands. - privacyinfolookup - domaininfolookup - rangesinfolookup
3.5.4	Bugfixes : Issues with ipinfolookup command
4.0.0	IPInfo not supported on Splunk 6.x and 7.x
4.0.9	Support for Proxy Settings
5.0.2	Support for Splunk Search Head Cluster
5.1.1	Merging ipinfolookup capability with original ipinfo command privacyinfolookup to now be privacyinfo domaininfolookup to now be domaininfo rangesinfolookup to now be rangesinfo
5.1.2	Updating `ipinfo` command to support ipinfo bulk api
5.2.8	Feature to Add custom rootCA certificate. Feature to Disable the SSL verification. Couple of other Bug fixes.
5.2.10	Updating Python Library to 1.6.15 Bug Fixes with Batch Command
5.3.1	Adding WorkFlow Action for IPInfo
5.4.0	Support batching in privacy command
5.4.1	Cleaning Up of Old Splunk Code and Minor Bug Fixes
5.4.2	Introducing lat/lon along with loc, for better support with maps
5.4.3	Adding prefix=true support with ipinfo command
5.5.0	Multi IP support with ipinfo command (eg ipinfo src_ip dest_ip)
5.5.1	Adding a privacy=true flag so that the results are returned as part of the ipinfo command and other Minor Bug Fixes

5.6.1	Adding a privacy=true flag so that the results are returned as part of the ipinfo command Support for multiple fields in one go , for example ipinfo prefix=true src_ip, dest_ip
5.6.2	Minor BugFixes with commands
5.6.3	Minor BugFixes with setup page

Supported OS

OS
Windows 10
Windows Server 2012
Windows Server 2016
RHEL 7
RHEL 8
UBUNTU 14
UBUNTU 16
UBUNTU 18
UBUNTU 20

Supported Splunk

Splunk
Splunk 8.X

IPInfo App for Splunk

IPInfo App for Splunk provides an Integration between IPInfo API and Splunk. This app adds *ipinfo* command to Splunk, which uses IPINFO API engine to lookup information for a given IP

Install the App

NOTE: There are multiple ways of deploying apps to Splunk environment, in this document we'll be referring installation via CLI (Command Line Interface)

CASE1: SINGLE STAND ALONE MACHINE (CLI)

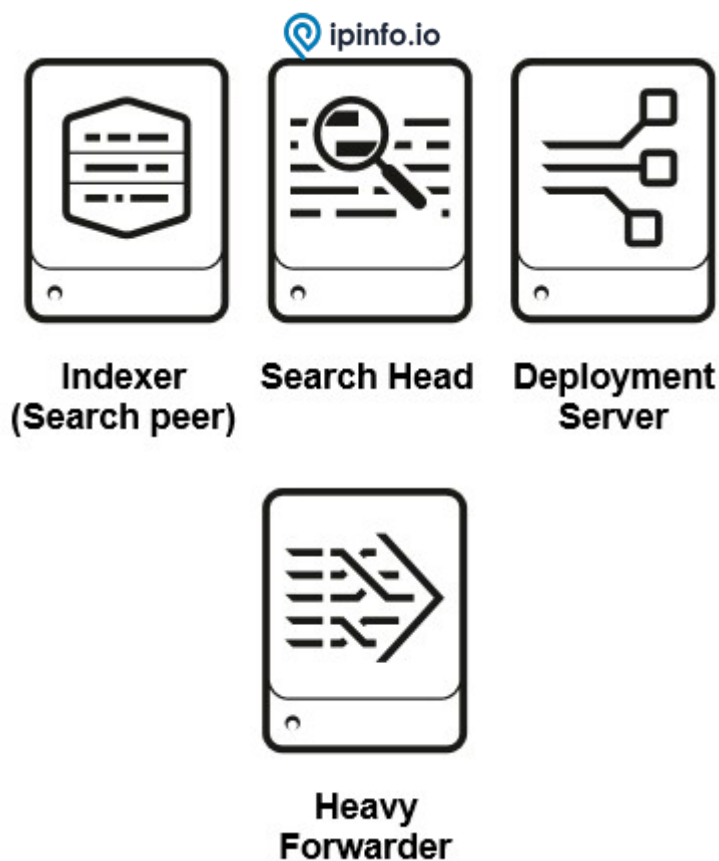
Single standalone Splunk Enterprise Installation on Windows/*NIX



1. **Unzip ipinfo_app.spl**
2. **Copy** the unzipped directory **ipinfo_app** to **\$SPLUNK_HOME/etc/apps/**
3. **Open CLI** and restart Splunk using **./splunk restart**

CASE2: DISTRIBUTED ARCHITECTURE

Single Indexer Single Search head and Single forwarder (Heavy or Universal) and Deployment server



1. **Unzip ipinfo_app.spl**
2. **Copy** the unzipped directory **ipinfo_app** to deployment server in the following location **\$SPLUNK_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< ipinfo_app > ]  
stateOnClient=enabled  
restartSplunkd=true
```

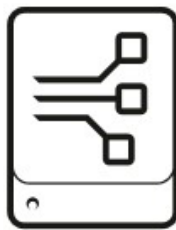
4. **Open CLI** deploy the apps using following command **./splunk reload deploy-server**

CASE3: DISTRIBUTED ARCHITECTURE

Multiple non-clustered Indexers, Multiple non-clustered SearchHeads, Forwarder(Heavy or Universal) and



Deployment server



**Deployment
Server**



**Heavy
Forwarder**

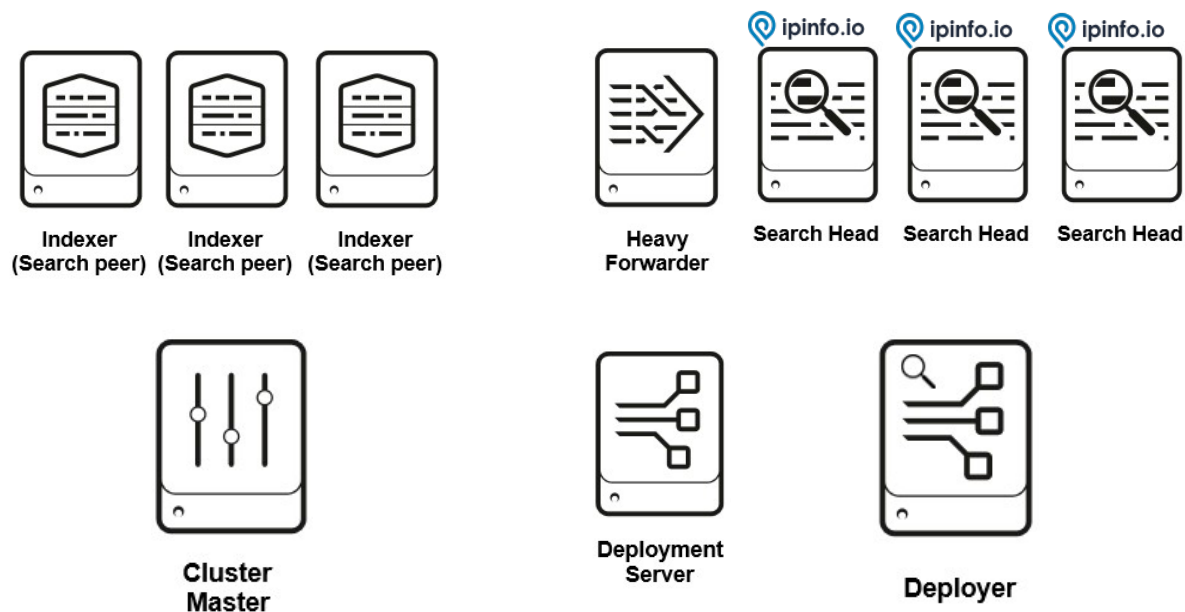
1. **Unzip ipinfo_app.spl**
2. **Copy** the unzipped directory **ipinfo_app** to deployment server in the following location
\$SPLUNK_HOME/etc/deployment-apps/
3. Add following to **serverclass.conf**

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< ipinfo_app >]
stateOnClient=enabled
restartSplunkd=true
```

4. **Open CLI** deploy the apps using following command **./splunk reload deploy-server**

CASE4: DISTRIBUTED ARCHITECTURE

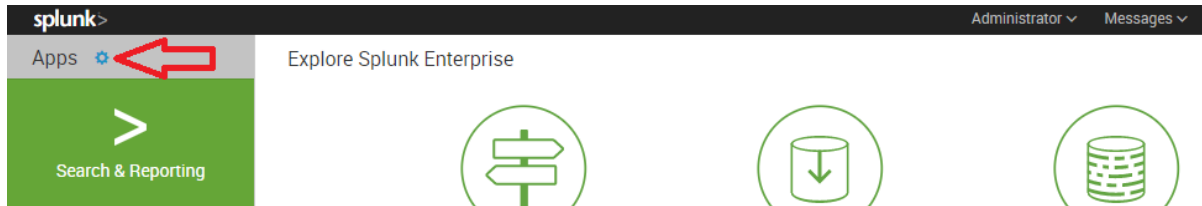
Single Site clustered Indexer, Clustered Search heads and Forwarder (Heavy or Universal).



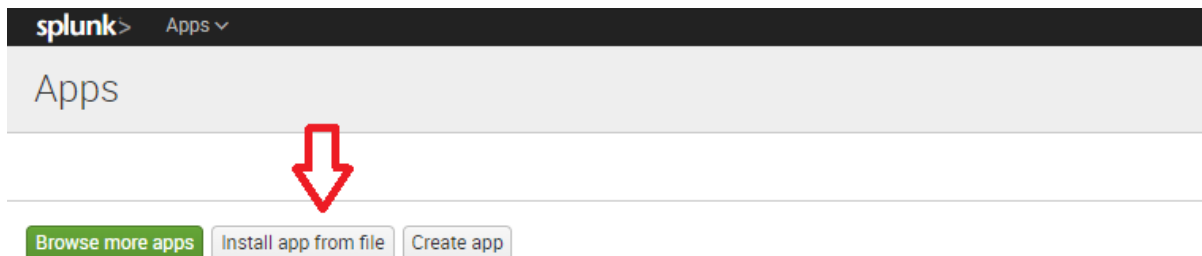
1. **Unzip ipinfo_app.spl**
2. **Copy ipinfo_app** to Deployer server in the following location `$SPLUNK_HOME/etc/shcluster/apps/`
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command
`./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>`

CASE5: STANDALONE INSTALLATION (WEB)

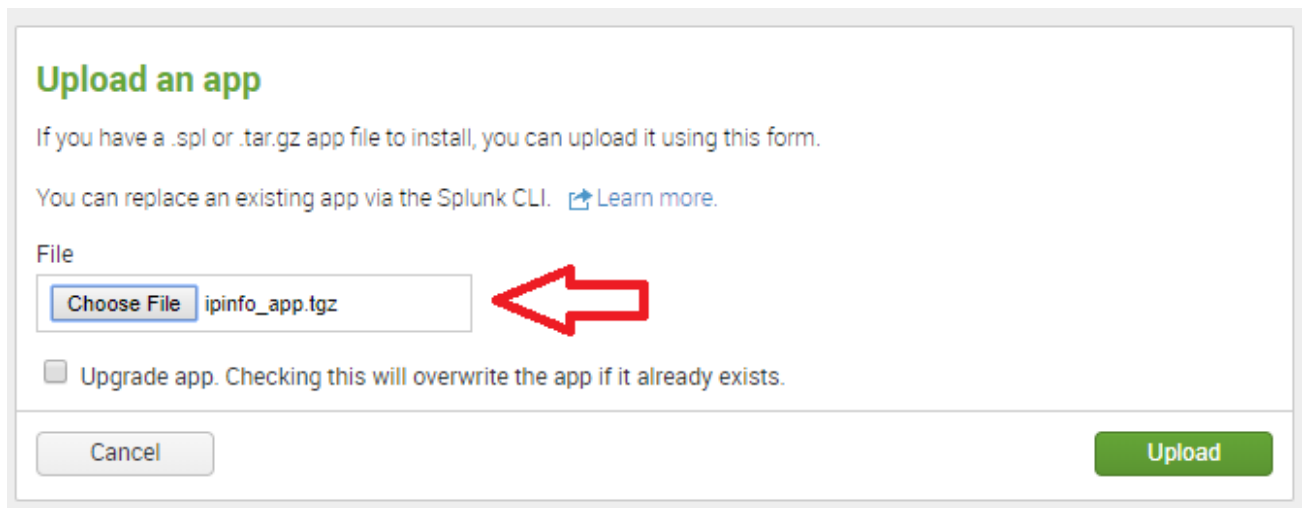
1. On the Splunk Home Page, Click on “Manage Apps”



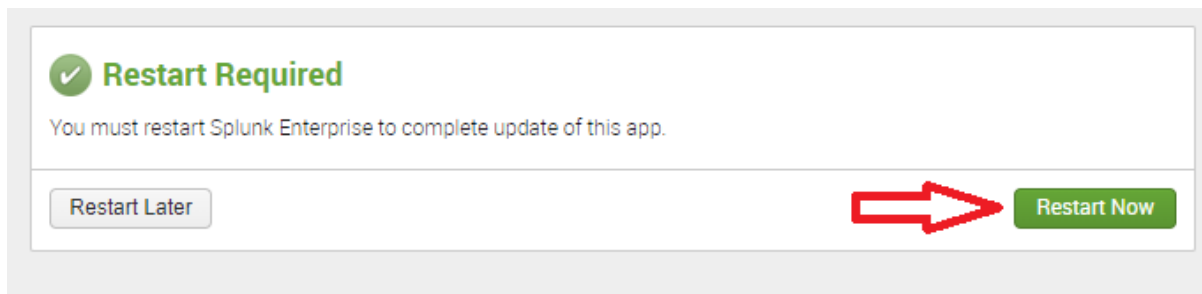
2. On the Manage Apps page, Click on “Install app from file”



3. Select path for IPINFO Splunk app and Click “Upload”

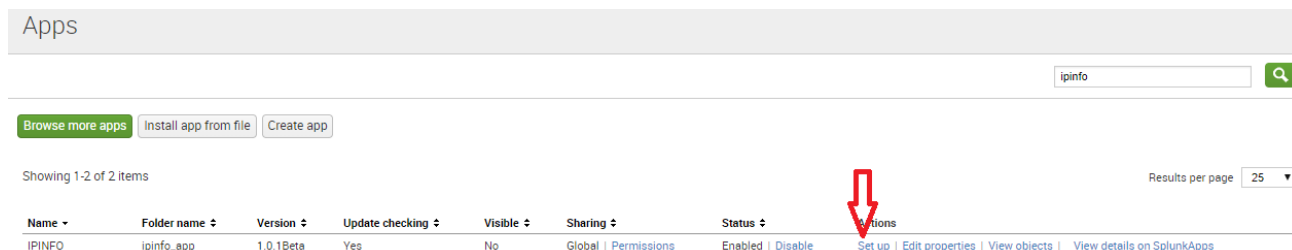


4. Splunk will prompt you to restart the machine, please restart



Configuration

1. After Installation and restart, login to the Splunk web and go to 'Manage Apps'
2. It will list out all the installed application and their configuration option.
3. Look for 'IPINFO' and click on the 'Set-Up' link to configure the add on.
- 4.



Apps

ipinfo

Browse more apps | Install app from file | Create app

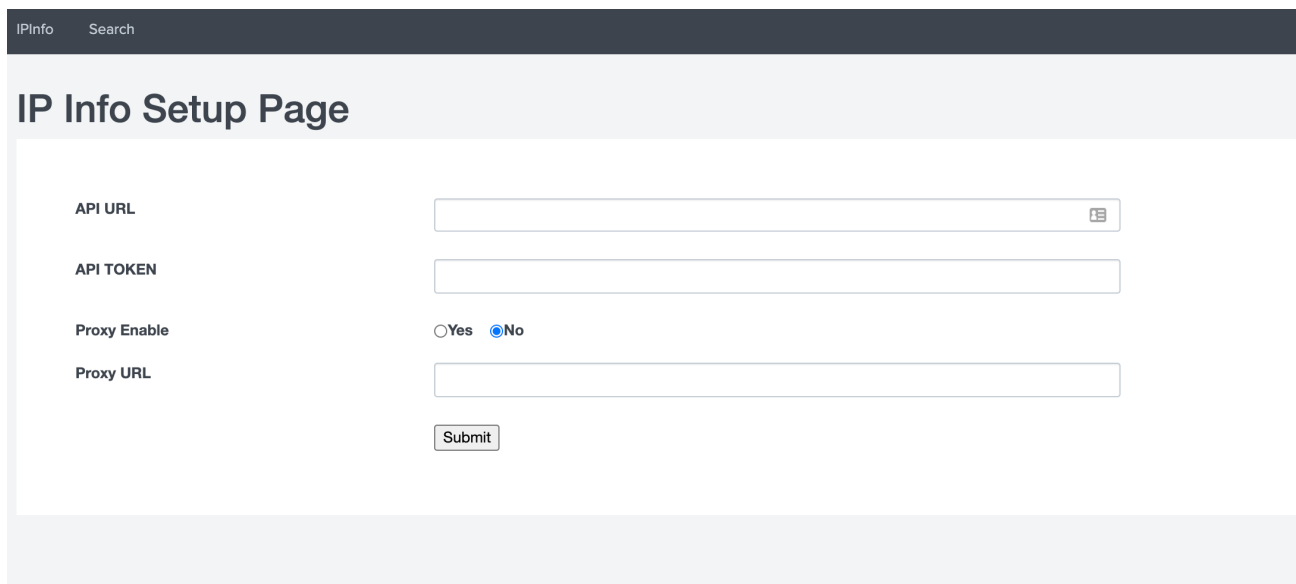
Showing 1-2 of 2 items

Results per page 25

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
IPINFO	ipinfo_app	1.0.1Beta	Yes	No	Global Permissions	Enabled Disable	Set up Edit properties View objects View details on SplunkApps

API Configuration

Just Enter your personalized authorization token, there is also link to purchase the token



IPInfo Search

IP Info Setup Page

API URL

API TOKEN

Proxy Enable ☐ Yes ☒ No

Proxy URL

Submit

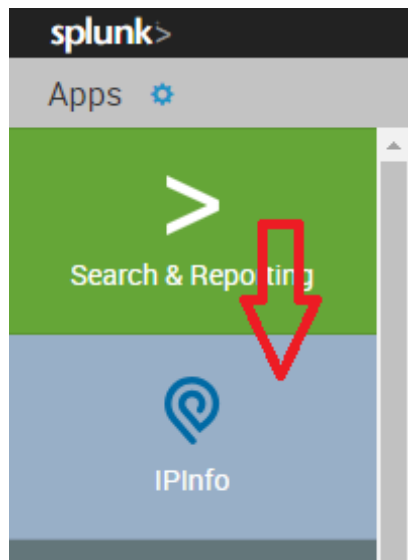
CLI Configuration

Just update ip_info_setup.conf in \$SPLUNK_HOME/etc/apps/ip_info/local/

```
[ip_info_configuration]
api_url = https://ipinfo.io/
api_token = <your token here>
```

and restart Splunk

ACCESSING THE APP



TEST COMMAND

-----IPInfo -----

```
| makeresults 1 | eval IP1=random()%192, IP2=random()%210, IP3=random()%230,
IP4=random()%192, IP='IP1'.'.'IP2'.'.'IP3'.'.'IP4'| table _time IP | ipinfo IP
```

Availability of Fields

- **Basic Subscription** - ip, city, region, country, loc, org, postal, hostname
- **Standard Subscription** - ip, city, region, country, loc, postal, hostname, asn_asn, asn_name, asn_domain, asn_route, asn_type
- **Pro Subscription** - ip, city, region, country, loc, postal, hostname, asn_asn, asn_name, asn_domain, asn_route, asn_type, company_name, company_domain, company_type, carrier_name, carrier_mcc, carrier_mnc

----- IPInfo -----

```
| makesresults count=2000
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
IP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| table _time IP
| ipinfo IP
```

----- IPInfo ----- (Multi)

```
| makesresults count=100
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
SRCIP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
DESTIP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| table _time SRCIP DESTIP
| ipinfo SRCIP DESTIP
```

----- IPInfo ----- (prefix)

```
| makesresults count=100
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
SRCIP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| table _time SRCIP
| ipinfo prefix=true SRCIP
```

----- IPInfo ----- (privacy)

```
| makesresults count=2000
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
SRCIP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| eval IP1=random()%192, IP2=random()%210, IP3=random()%230, IP4=random()%192,
DESTIP='IP1'.'.'.'IP2'.'.'.'IP3'.'.'.'IP4'
| table _time SRCIP DESTIP
| ipinfo prefix=true privacy=true SRCIP, DESTIP
```

----- IPInfo Batch -----

```
| ipinfobatch ip="197.94.71.228,197.94.71.227,197.94.71.221 , 197.94.71.226,197.94.71.225
,197.94.71.22"
```

----- privacyinfo -----

```
| makesresults | eval IP="23.24.240.0" | privacyinfo IP
```

----- rangesinfo -----

```
| makesresults | eval domain="comcast.net" | rangeinfo domain
```

----- domaininfo-----

```
| makesresults | eval IP="1.1.1.1" | domaininfo IP
```


IPINFO BASIC

splunk> App: IPInfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export ...

139.130.188.239 Hide Filters

139.130.188.239 IP Address		zet1364080.lnk.telstra.net Hostname	
Clarkson City	Western Australia Region	AU Country	6030 Postal



ASN

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

COMPANY

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

CARRIER

Full company details are displayed here when you're subscribed to the pro plan.

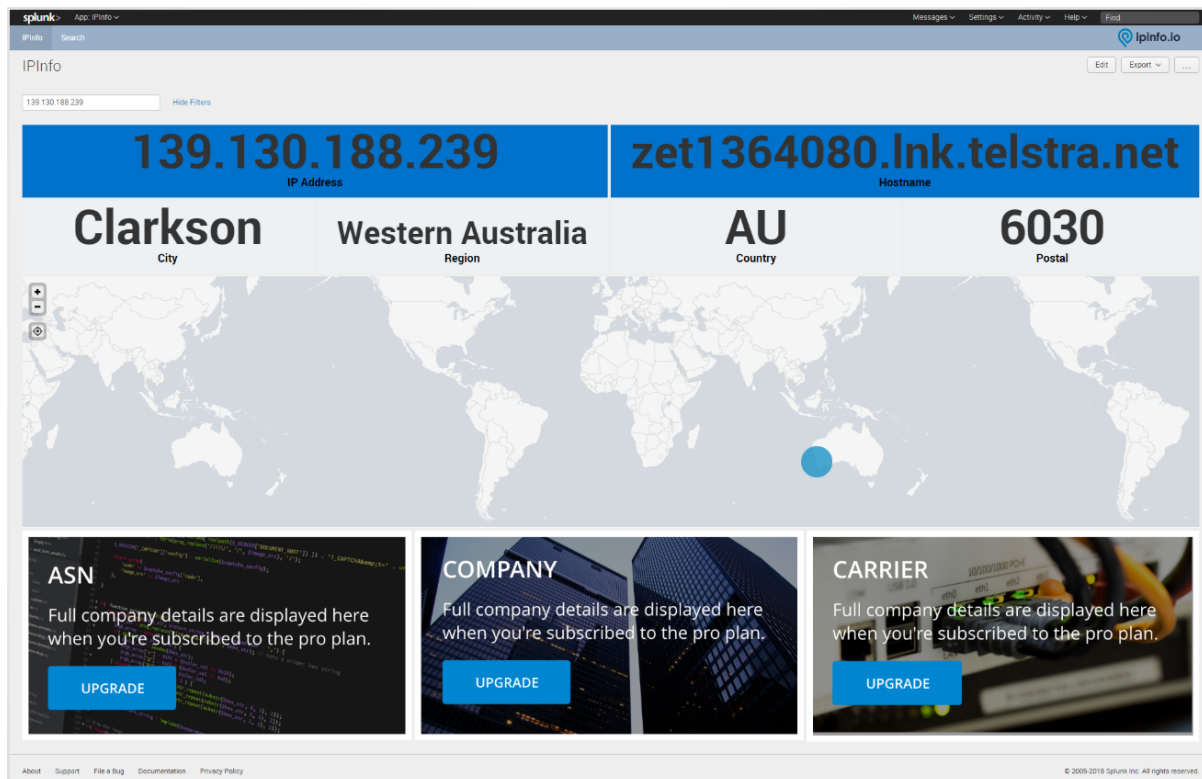
UPGRADE

splunk> App: IPInfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export ...

139.130.188.239 Hide Filters

139.130.188.239 IP Address		zet1364080.lnk.telstra.net Hostname	
Clarkson City	Western Australia Region	AU Country	6030 Postal



ASN

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

COMPANY

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

CARRIER

Full company details are displayed here when you're subscribed to the pro plan.

UPGRADE

About Support File a Bug Documentation Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.

IPINFO PRO (NO CARRIER)

splunk App: ipinfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export

139.130.188.239 Hide Filters

139.130.188.239
IP Address


zet1364080.lnk.telstra.net
Hostname

Clarkson
City

Western Australia
Region

AU
Country

6030
Postal



ASN		COMPANY		CARRIER	
Key	Value	Key	Value	Key	Value
ASN	AS1221	NAME	Telstra Internet	NAME	N/A
NAME	Telstra Pty Ltd	DOMAIN	telstra.com.au	MCC	N/A
DOMAIN	telstra.net	TYPE	isp	MNC	N/A
ROUTE	139.130.0.0/16				
TYPE	isp				

About Support File a Bug Documentation Privacy Policy © 2005-2018 Splunk Inc. All rights reserved.

splunk App: ipinfo Messages Settings Activity Help Find

IPInfo Search ipinfo.io Edit Export

139.130.188.239 Hide Filters

139.130.188.239
IP Address


zet1364080.lnk.telstra.net
Hostname

Clarkson
City

Western Australia
Region

AU
Country

6030
Postal



ASN		COMPANY		CARRIER	
Key	Value	Key	Value	Key	Value
ASN	AS1221	NAME	Telstra Internet	NAME	N/A
NAME	Telstra Pty Ltd	DOMAIN	telstra.com.au	MCC	N/A
DOMAIN	telstra.net	TYPE	isp	MNC	N/A
ROUTE	139.130.0.0/16				
TYPE	isp				

About Support File a Bug Documentation Privacy Policy © 2005-2018 Splunk Inc. All rights reserved.



IPINFO PRO (WITH CARRIER)

splunk

App IPInfo

Messages

Settings

Activity

Help

Find

IPInfo

Search

IPInfo

105.4.5.193

Hide Filters

105.4.5.193

IP Address

N/A

Hostname

Germiston

City

Gauteng

Region

ZA

Country

1401

Postal

+

-

+

-

ASN	COMPANY	CARRIER
<div>Key</div> <div>Value</div>	<div>Key</div> <div>Value</div>	<div>Key</div> <div>Value</div>
ASN: AS37158	NAME: NEOTEL GGSNZ	NAME: Cell C
NAME: Cell C (Pty) Ltd	DOMAIN: neotel.co.za	MCC: 655
DOMAIN: cellc.co.za	TYPE: isp	MNC: 7
ROUTE: 105.4.0.0/14		
TYPE: isp		

About

Support

File a Bug

Documentation


Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.

splunk>
App: IPInfo
Messages
Settings
Activity
Help
Find

IPInfo

105.4.5.193 IP Address		N/A Hostname	
Germiston City	Gauteng Region	ZA Country	1401 Postal



ASN		COMPANY		CARRIER	
Key	Value	Key	Value	Key	Value
ASN	AS37168	NAME	NEOTEL GCSN2	NAME	Cell C
NAME	Cell C (Pty) Ltd	DOMAIN	neotel.co.za	MCC	655
DOMAIN	celic.co.za	TYPE	isp	MNC	7
ROUTE	105.4.0.0/14				
TYPE	isp				

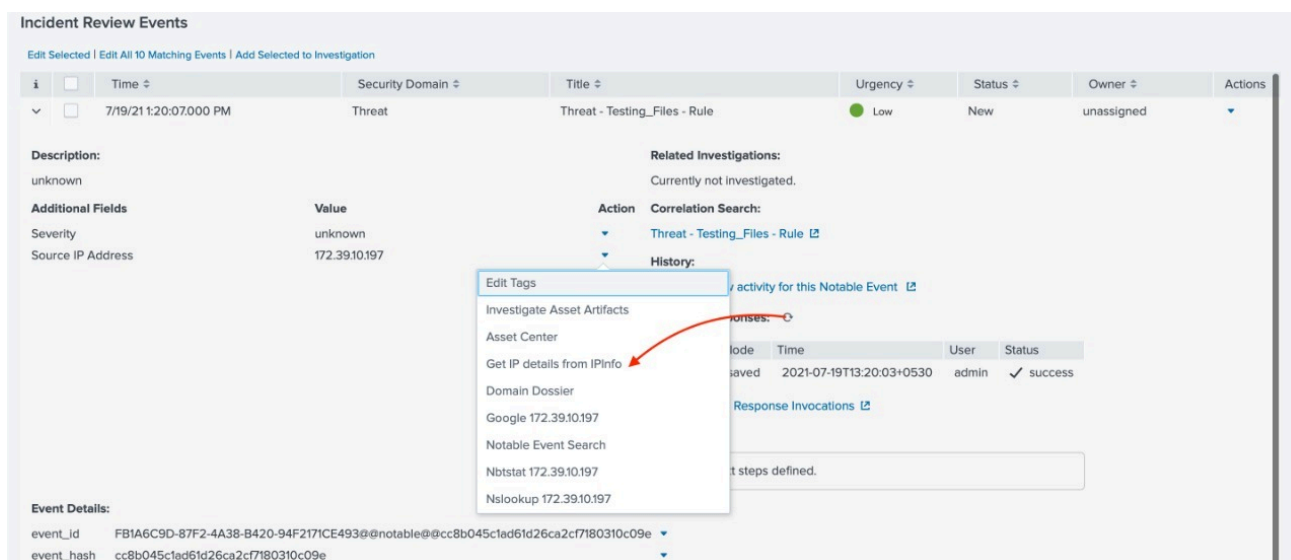
[About](#)
[Support](#)
[File a Bug](#)
[Documentation](#)
[Privacy Policy](#)

© 2005-2016 Splunk Inc. All rights reserved.

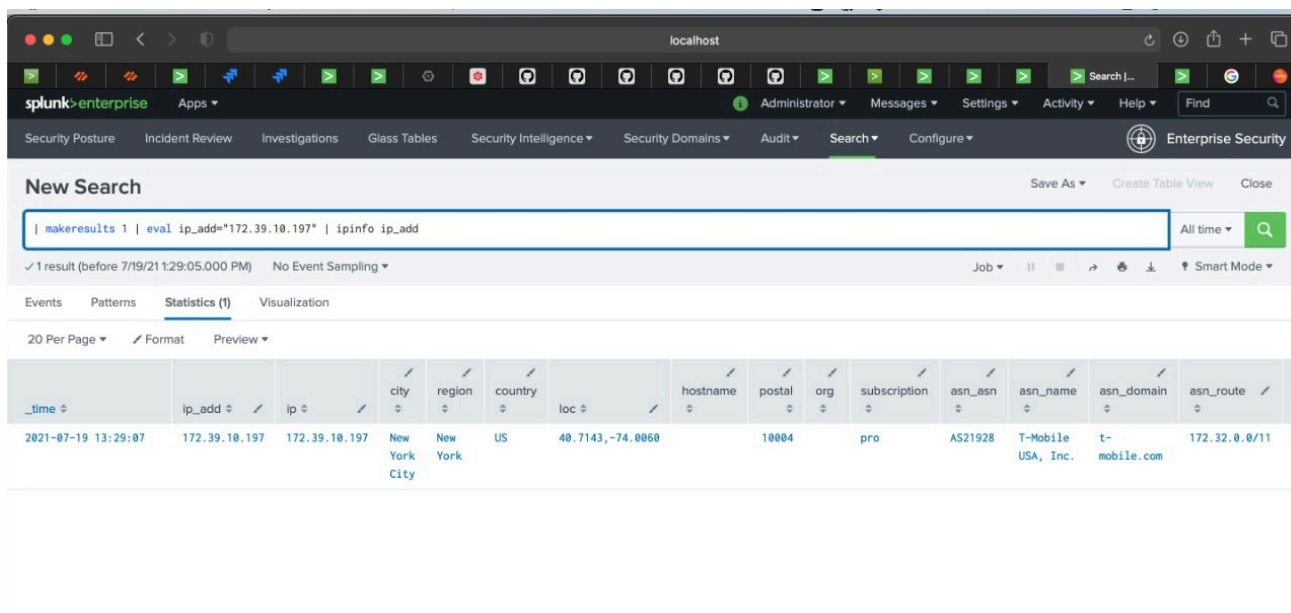
Workflow Action:

From V5.3.1, we have added a new workflow actions in Splunk which will give you option to fetch details of IP from IPInfo by single click. It will work when fieldname is **ip** OR ***_ip** like **ip,dest_ip,src_ip** etc.

For Example:



The screenshot shows the 'Incident Review Events' interface in Splunk. A table lists events, with one event selected. The 'Description' field is 'unknown'. The 'Additional Fields' section shows 'Severity' as 'unknown' and 'Source IP Address' as '172.39.10.197'. A context menu is open over the 'Source IP Address' field, showing options like 'Investigate Asset Artifacts', 'Asset Center', 'Get IP details from IPInfo', 'Domain Dossier', 'Google 172.39.10.197', 'Notable Event Search', 'Nbtstat 172.39.10.197', and 'Nslookup 172.39.10.197'. A red arrow points to the 'Get IP details from IPInfo' option.



The screenshot shows the 'New Search' interface in Splunk. The search bar contains the query: `| makeresults 1 | eval ip_add="172.39.10.197" | ipinfo ip_add`. The search results show a single result for the IP address 172.39.10.197. The results table includes fields for location, organization, and other details.

_time	ip_add	ip	city	region	country	loc	hostname	postal	org	subscription	asn_asn	asn_name	asn_domain	asn_route
2021-07-19 13:29:07	172.39.10.197	172.39.10.197	New York City	New York	US	40.7143,-74.0060		10004	pro		AS21928	T-Mobile USA, Inc.	t-mobile.com	172.32.0.0/11

THANK YOU