WEBROOT®

BrightCloud Threat Intelligence for HPE ArcSight V1.0

User Guide — Linux

Table of Contents

Chapter 1: Solution Overview

1.1 Background

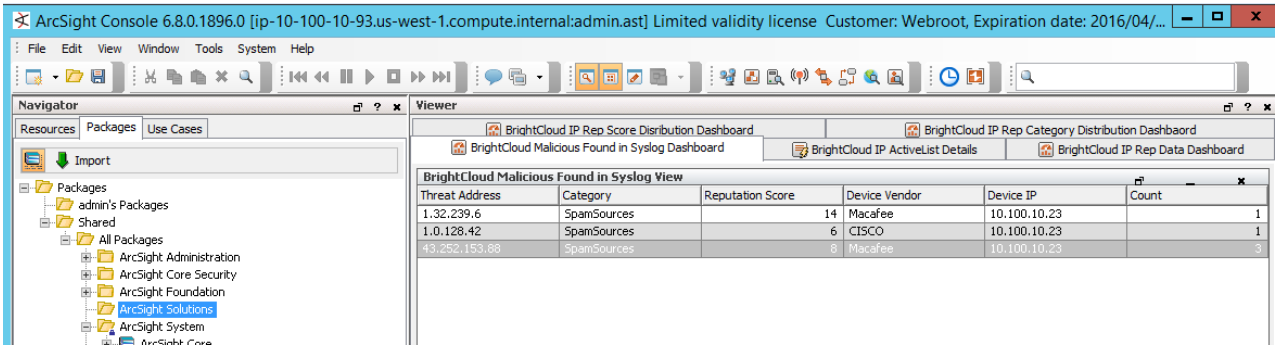
Webroot BrightCloud TI Use Case Summary

- **Problem —** Security team wants to focus on the most immediate and significant threats and is challenged with a high number of alerts to sift through. Team wants to enhance operational efficiency.
- **Benefits —** With prioritized alerts, the security team can react quickly to IP-related threats and investigate with rich contextual information about the threat to prevent costly breaches.
- **Solution —** Automatically correlate internal and external network events using prioritized real-time IP threat intelligence with contextual information to detect malicious IP threats for investigation.

1.2 How to Use BrightCloud Threat Intelligence With HPE ArcSight ESM

HPE ArcSight ESM uses the BrightCloud data to detect and alert you to situations where a malicious IP address has been seen within your network. Once you see an alert, you can learn more about the IP address through ESM and the BrightCloud Threat Investigator. The Threat Investigator is a companion product that is intended to be used along with TI for ArcSight from Webroot. ArcSight generates alerts, and Threat Investigator is used to understand why BrightCloud determined an IP is malicious.

Within ESM you will find alerts of malicious IPs seen within your network using the Matched IP Dashboard, click on the IP to see more detail.

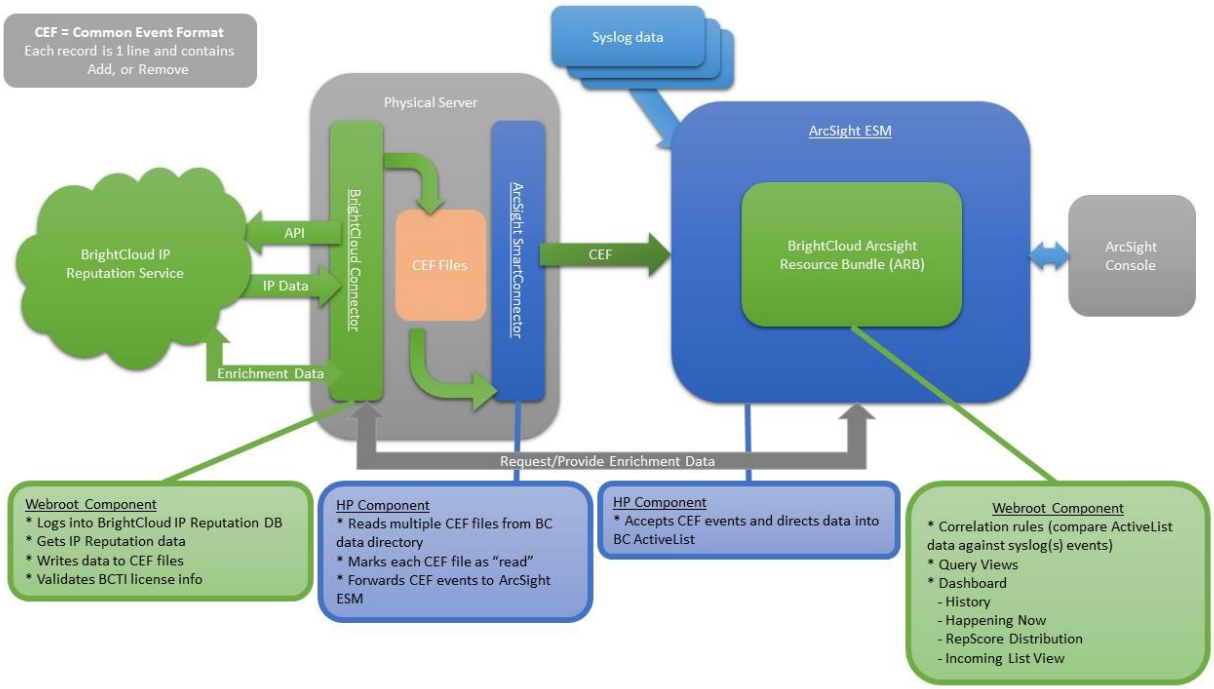


Then copy the IP address and paste it into the Threat Investigator to learn more about the IPs reputation score and threat history. This information will allow you to take the appropriate actions according to your operating procedures.

1.3 How the BrightCloud + ESM Solution Works

The Webroot BrightCloud threat intelligence data is downloaded through Webroot BrightCloud connector, and then converted into CEF records via HPE ArcSight SmartConnector (provided by HPE)

Those CEF records will be fed into **HPE ArcSight ESM** ActiveList for consumption by real time rules defined in HPEArcSight ESM. Webroot provides a default rule that looks for IP addresses in the syslog that are currently in the IP Reputation list from BrightCloud. HPEArcSight ESM rules in conjunction with Webroot BrightCloud Threat Intelligence data will be enable analysis to discover potential network threats. Webroot also provides queries and Dashboards to visualize the threat events that Webroot Threat Intelligence uncovers.



The diagram above illustrates the major components of the solution and data flows. We have 2 components in the product — the connector and the ARB package for ESM. The connector is installed on the same server as the HPE SmartConnector. The ARB installs the BrightCloud components within ESM.

Chapter 2: Preparing for Installation

We recommend that you read *HPE ArcSight ESM Install Guide* and *HPE ArcSight SmartConnector User Guide* available on HP's Protect724 before you begin the installation process.

2.2 System Requirements

For hardware requirement, please reference to *HPE ArcSight ESM Install Guide*. The following are the software requirements for Webroot BrightCloud Threat Intelligence integration:

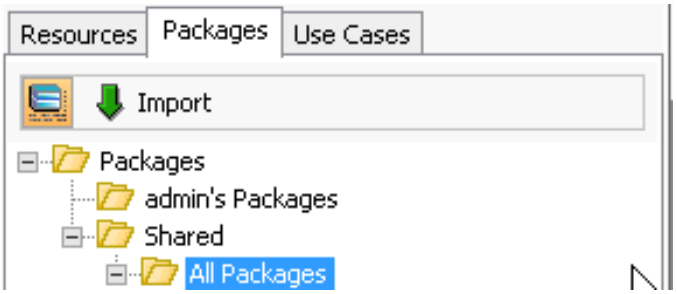
REQUIREMENTS	DESCRIPTION
Operating system (OS)	• Microsoft Windows Server • Edition — Enterprise • Version — 32/64 bit • Language — English
Java	• JDK 1.6 • Version — 32/64 bit
Software Components	• HPE ArcSight ESM 6.0 or above • HPE ArcSight ESM Console 6.0 or above • Webroot BrightCloud connector 1.0 • HPE ArcSight SmartConnector 32/64 Bit

2.3 Importing the Webroot BrightCloud ARB (ArcSight Resource Bundle) for ESM Console

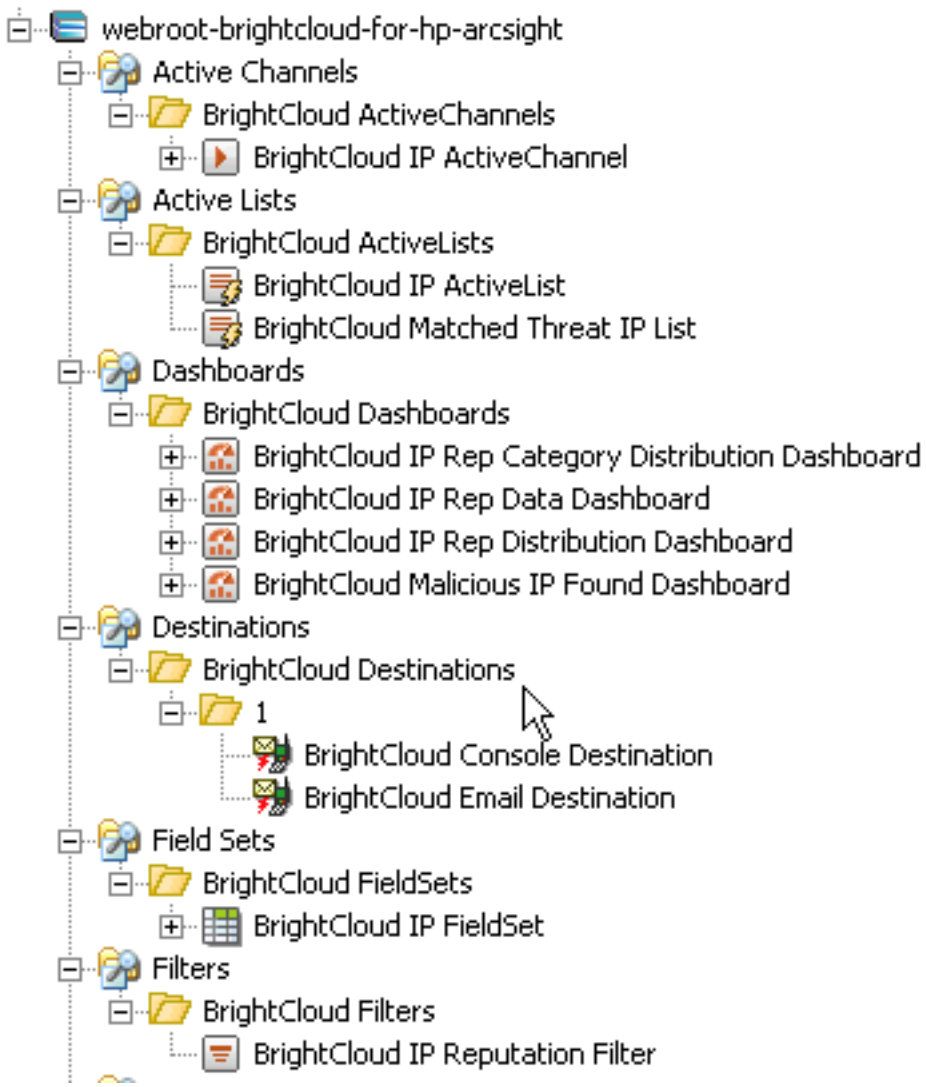
The **webroot-brightcloud-for-hp-arcsight.arb** contains all the default ESM console configurations needed to use the Webroot BrightCloud Threat Intelligence service. Although manual configuration is possible, please refer to the customization section, Chapter 6, we recommend an import of the ARB package for a quick start.

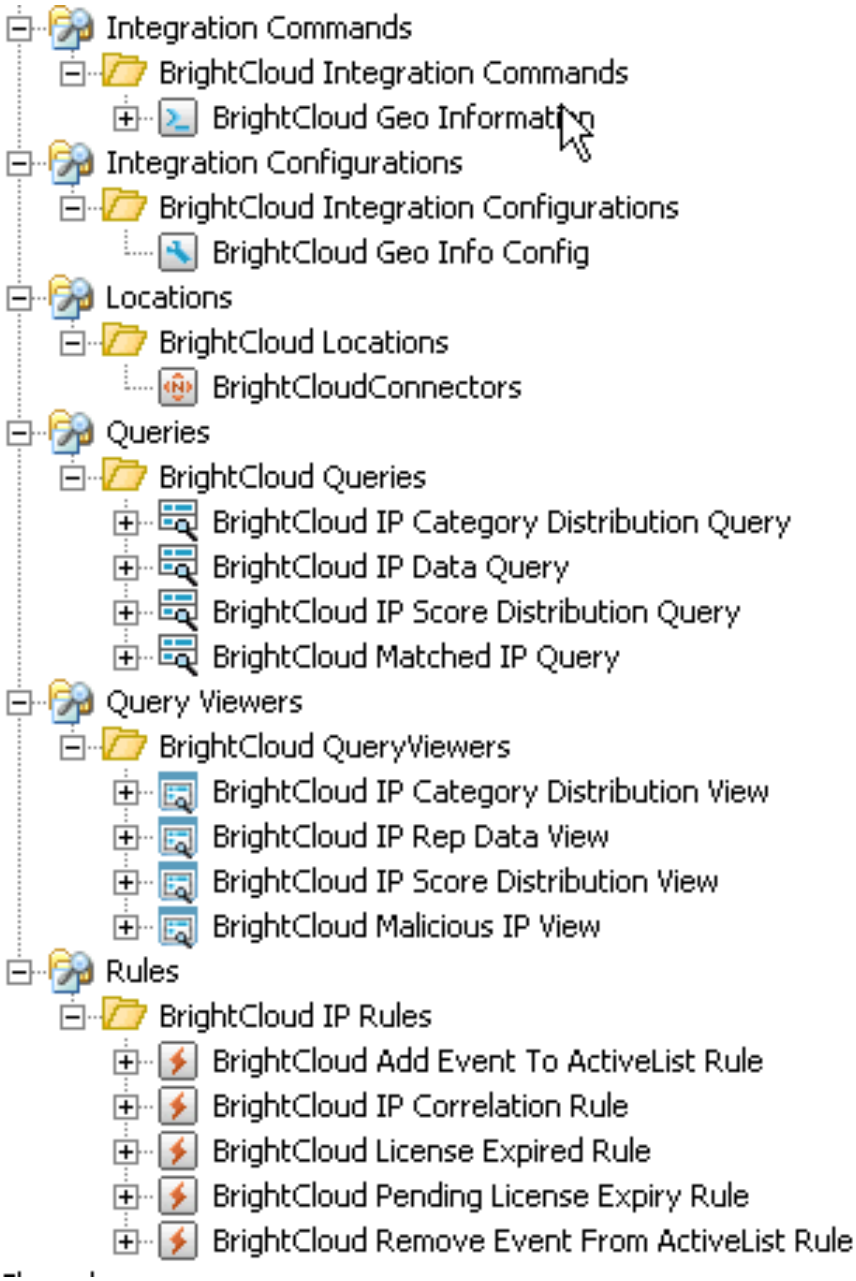
To import the Webroot BrightCloud ARB:

1. Log in to the ESM console
2. Import **webroot-brightcloud-for-hp-arcsight.arb** through **Package** tab in ESM console's **Navigator** panel.



The ARB package will be imported into /All Packages/Personal/admin's Packages/webroot-brightcloud-for-hp-arcsight.


webroot-brightcloud-for-hp-arcsight
Active Channels
BrightCloud ActiveChannels
BrightCloud IP ActiveChannel
Active Lists
BrightCloud ActiveLists
BrightCloud IP ActiveList
BrightCloud Matched Threat IP List
Dashboards
BrightCloud Dashboards
BrightCloud IP Rep Category Distribution Dashboard
BrightCloud IP Rep Data Dashboard
BrightCloud IP Rep Distribution Dashboard
BrightCloud Malicious IP Found Dashboard
Destinations
BrightCloud Destinations
1
BrightCloud Console Destination
BrightCloud Email Destination
Field Sets
BrightCloud FieldSets
BrightCloud IP FieldSet
Filters
BrightCloud Filters
BrightCloud IP Reputation Filter



Note: After importing the ARB package, please verify that all the above components are visible in the ESM console.

Chapter 3: Installing and Configuring the Webroot BrightCloud Connector

3.1 Fresh Install

Please note the following:

- Installation prompts are shown below in **bold**.
- Entry values are underlined.
- Values in [x] are defaults.

Java run time l.6 is a pre-requisite for the Webroot BrightCloud connector.

Step 1: Run installer script with **sudo**, and choose **[1] Fresh Install**

sudo ./webroot-brightcloud-connector-for-hp-arcsight-installer-v1.run

---

The installer will guide you through the installation or configuration update of the BrightCloud connector for HPE ArcSight.

Installer Configuration

Please select installation option to proceed:

[1] Fresh Install: -Install BrightCloud connector for HPE ArcSight for the first time

[2] Update License: -Update your existing BrightCloud license-only available after first install

[3] Change Download Frequency: -Change the download frequency of BrightCloud IP Reputation Service data-only available after first install

Please choose an option [1] : 1

Step 2: Read the license agreement in a browser window with the given URL before selecting option 1 or 2

License Agreement

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

[1] I HAVE READ AND AGREE TO BE BOUND BY THE ENTERPRISE AGREEMENT - http://www.webroot.com/us/en/company/about/service-terms-and-conditions

[2] I DO NOT ACCEPT THE ENTERPRISE AGREEMENT - http://www.webroot.com/us/en/company/about/service-terms-and-conditions/

Please choose an option [2] : 1

Step 3: Customized the install location.

Installation location

BrightCloud connector for HPE ArcSight will be installed in this location:

Installation directory [/opt/Webroot/BrightCloudConnector]:

Step 4: Choose license types: If you have a license key, please select "**Enter a valid license**" option. New user can apply for a 30 days free trial.

Choose your license option

Please select one of the options below:

[1] Enter a valid license

[2] Request a trial license

Please choose an option [2] : 2

Step 5: Valid information is required for trial license application. Email is the primary identification for Webroot BrightCloud Threat Intelligence for HPE ArcSight license.

Request a trial license

Please complete the form below to request a trial license:

NOTE: All fields are mandatory.

First Name: []: John

Last Name: []: Millar

Company: []: XYZ Corp

Email: []: yourname@company.com

Phone: []: 123-456-7890

Country:

[1] Select

[2] United States

[3] Canada

…

[244] Zambia

[245] Zimbabwe

Please choose an option [1] : 2

Step 6: Trial license is auto populated upon successful application. If the "**Enter a valid license**" option was chosen, similar input form will be displayed.

Request a trial license

Your trial license:

[hparcsightes_ccacxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx]:

If you want to extend your trial license or need help with the license, please contact: **sales@webroot.com**

Would you like to continue the installation with this trial license?

3. Step 7: Configure the IP Reputation list update frequency and customize the CEF file location (BrightCloud's data). Please take note of the CEF location; it is needed to configure the HPE ArcSight SmartConnector.

BrightCloud IP Reputation Service Data Download Configuration

Configure the options for how to download BrightCloud IP Reputation Service data & integrate into HPE ArcSight:

Automatically download

[1] Every 30 min

[2] Every hour (default)

[3] Every 12 hours

[4] Every 24 hours

Please choose an option [2] : 2

Download immediately after installation [Y/N]: Y

Download directory for BrightCloud IP Reputation Service data where CEF events will be generated:

[/opt/Webroot/BrightCloudConnector/CEF]:

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Do you want to continue? [Y/N]: Y

Step 8: Webroot BrightCloud connector is installed, a readme file is available to review.

Please wait while Setup installs BrightCloud connector for HPE ArcSight on your computer:

Installing

0% _____ 50% _____ 100%

##

How to contact us:

- sales@webroot.com for questions on licensing & sales
- support@brightcloud.com for technical support

View Readme file? [Y/N]: Y

README

Readme for Webroot BrightCloud Threat Intelligence for HPE ArcSight

Introduction

The Webroot BrightCloud Threat Intelligence for HPE ArcSight enables detection, alert and investigation of malicious IP activities. It provides ArcSight customers with BrightCloud IP Reputation Service data to correlate with log files collected by ArcSight, detect malicious IP activities in incoming IP traffic, alert infosec teams, and provide them with detailed information on each malicious IP for incident response and investigation before those activities lead to security breaches.

Use Cases

- Detect & alert - Correlate with log data inside HPE ArcSight to detect & alert on malicious IP activities so the InfoSec team can perform incident response & investigation as early as possible before malicious activity leads to costly breaches
- Investigate - Provide detailed information on malicious IPs inside HPE ArcSight for InfoSec teams to perform incident response & investigation

Press [Enter] to continue:

Key Features

- Continuously downloads the most current 12M malicious IPs from BrightCloud IP Reputation Service to HPE ArcSight
- Provides out-of-the-box dashboards to correlate BrightCloud IP threat intelligence data with log files and detect malicious IP activities in real-time
- Provides detailed information on each malicious IP on demand for incident response & investigation

Prerequisites

Supports HPE ArcSight V6.0 & higher

Installation

Press [Enter] to continue:

It is a simple 3 step process:

1. Install Webroot BrightCloud connector for HPE ArcSight
2. Install a HPE SmartConnector in the same server and configure it to pull CEF events from the BrightCloud connector for HPE ArcSight
3. Install Webroot BrightCloud ARB package for HPE ArcSight for ArcSight ESM

For full installation & usage documentation, please refer to this URL

http://download.webroot.com/Webroot_BrightCloud_For_HPE_ArcSight.pdf

3.2 Update your existing BrightCloud license after first installation

You can upgrade your trial or expiring Webroot BrightCloud license via the Webroot BrightCloud connector after the initial installation.

Step 1: Choose "**Update License"** option after the welcome message.

sudo ./webroot-brightcloud-connector-for-hp-arcsight-installer-v1.run

---

Created with an evaluation version of BitRock InstallBuilder\

The installer will guide you through the installation or configuration update of the BrightCloud connector for HPE ArcSight.

Installer Configuration

Please select installation option to proceed:

[1] Fresh Install: -Install BrightCloud connector for HPE ArcSight for the first time

[2] Update License: -Update your existing BrightCloud license-only available after first install

[3] Change Download Frequency : -Change the download frequency of BrightCloud IP Reputation Service data-only available after first install

Please choose an option [3] : 2

Step 2: Input a new license key

Update License Key

Please enter your new license key to update, sample format shown below:

[]: hparcsightes_ccacxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ready to Update

Click Update to continue with the update configuration, or click Back if you want to review or change any settings.

Press [Enter] to continue:

Please wait while Setup installs BrightCloud connector for HPE ArcSight on your computer:

Installing

0% _____ 50% _____ 100%

##

How to contact us:

- sales@webroot.com for questions on licensing & sales
- support@brightcloud.com for technical support

View Readme file? [Y/N]: N

3.3 Update download frequency of BrightCloud Threat Intelligence data after first install

You can also use the connector to change the download frequency of an IP Reputation data after the initial installation.

Step 1: Choose "**Change Download Frequency"** option after the welcome messages.

sudo ./webroot-brightcloud-connector-for-hp-arcsight-installer-v1.run

---

Created with an evaluation version of BitRock InstallBuilder

The installer will guide you through the installation or configuration update of the BrightCloud connector for

HPE ArcSight.

Installer Configuration

Please select installation option to proceed:

[1] Fresh Install: -Install BrightCloud connector for HPE ArcSight for the first time

[2] Update License: -Update your existing BrightCloud license-only available after first install

[3] Change Download Frequency : -Change the download frequency of BrightCloud IP Reputation Service data-only available after first install

Please choose an option [3] : 3

Step 2: This is the same configuration screen as a 'Fresh Install". Again, it is important to keep track of the CEF stored location.

BrightCloud IP Reputation Service Data Download Configuration

Configure how you want to download BrightCloud IP Reputation Service data & integrate into HPE ArcSight:

Automatically download

[1] Every 30 min

[2] Every hour (default)

[3] Every 12 hours

[4] Every 24 hours

Please choose an option [2] : 1

Download immediately after installation [Y/N]: Y

Download directory for BrightCloud IP Reputation Service data where CEF events will be generated:

[/opt/Webroot/BrightCloudConnector/CEF

]: _____

Ready to Update

Click Update to continue with the update configuration, or click Back if you want to review or change any settings.

Press [Enter] to continue:

Please wait while Setup installs BrightCloud connector for HPE ArcSight on your computer:

Installing

0% _____ 50% _____ 100%

##

How to contact us:

- sales@webroot.com for questions on licensing & sales
- support@brightcloud.com for technical support

View Readme file? [Y/N]: N

3.4 Starting and stopping the connector

The Webroot BrightCloud Connector can be stopped via the command line at the installed directory:

sudo service BrightCloudConnector stop

Restarting without running installer by following command line at the installed directory:

sudo service BrightCloudConnector start

Chapter 4: Installing and Configuring HPE ArcSight SmartConnector

4.1 Fresh install

Please reference the official *HPE ArcSight SmartConnector User Guide* for up-to-date instructions. Please note the following:

- Installation prompts are shown below in **bold**.
- Entry values are <u>underlined</u>.

Pre-requisites: Java run time l.6 is required for the HPE ArcSight SmartConnector.

[root@localhost installers]# ./ArcSight-7.1.5.7538.0-Connector-Linux64.bin -i console

Preparing to install...

Extracting the JRE from the installer archive...

Unpacking the JRE...

Extracting the installation resources from the installer archive...

Configuring the installer for this system's environment...

Launching installer...

===

ArcSight SmartConnector (created with InstallAnywhere)

Preparing CONSOLE Mode Installation...

===

Platform Verification

You are installing this product on an unsupported platform. Please refer to the ArcSight SmartConnector Product and Platform Support Config document to find out about platforms supported for this release.

To cancel this installation, click [Cancel].

->1- OK

2- Cancel

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 1

==========

Introduction

The ArcSight Installer will guide you through the installation of the ArcSightSmartConnector. The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'. To cancel this installation at any time, type 'quit'.

PRESS <ENTER> TO CONTINUE:

==========

Choose Install Folder

Choose the folder where you would like to install an ArcSight SmartConnector. It is strongly recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. Ifyou are upgrading an ArcSight SmartConnector from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.

Where would you like to install?

Default Install Folder: /root/ArcSightSmartConnectors

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

: /root/ArcSightSmartConnectorsSilentInstallation

INSTALL FOLDER IS: /root/ArcSightSmartConnectorsSilentInstallation

IS THIS CORRECT? (Y/N): Y

==========

Choose Install Set

Please choose the Install Set to be installed by this installer.

->1- Typical

2- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

: 1

==========

Choose Link Location

Where would you like to create links?

->1- Default: /root

2- In your home folder

3- Choose another location...

4- Don't create links

ENTER THE NUMBER OF AN OPTION ABOVE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

: 1

==========

Pre-Installation Summary

Please Review the Following Information Before Continuing:

Product Name:

ArcSight SmartConnector

Install Folder:

/root/ArcSightSmartConnectorsSilentInstallation

Link Folder:

/root

Install Set:

Typical

PRESS <ENTER> TO CONTINUE:

==========

Installing...

[==========|==========|==========|==========]

[----------|----------|----------|----------]

==========

Installation Complete

The core components of the ArcSight SmartConnector have been successfully installed to:

/root/ArcSightSmartConnectorsSilentInstallation

To finish the configuration of the SmartAgent, please go to the folder:

/root/ArcSightSmartConnectorsSilentInstallation/current/bin/

and execute the script:

./runagentsetup.sh

PRESS <ENTER> TO EXIT THE INSTALLER:

[root@localhost installers]# cd /root/ArcSightSmartConnectorsSilentInstallation/current/bin/

[root@localhost bin]# ./runagentsetup.sh

Assuming ARCSIGHT_HOME: /root/ArcSightSmartConnectorsSilentInstallation/current

Assuming JAVA_HOME: /root/ArcSightSmartConnectorsSilentInstallation/current/jre

ArcSight Agent Setup starting...

Connector Setup Wizard starting in mode [CONSOLE]

[Fri Dec 04 03:16:42 PST 2015] [INFO] Checking for a running instance of connector...

[Fri Dec 04 03:16:42 PST 2015] [INFO] Starting up connector...

Connector Setup

What would you like to do?

0- Add a Connector

1- Enable FIPS mode

Please select an option: [Add a Connector] [0..1/cancel] :0

Select the connector to configure

Type:

0- ActivCard AAA Server Accounting Log DB (Legacy)

1- ActivCard AAA Server Authentication Log DB (Legacy)

2- Aladdin eSafe Gateway File

3- Amazon Web Services CloudTrail

4- Apache HTTP Server Access File

5- Apache HTTP Server Error File

6- Apache Tomcat File

7- ArcSight Asset Import File

8- ArcSight CEF Encrypted Syslog (UDP)

9- ArcSight Common Event Format File

10- ArcSight Common Event Format Hadoop

11- ArcSight Common Event Format Multiple File

12- ArcSight Common Event Format REST (Beta)

13- ArcSight FlexConnector CounterACT

14- ArcSight FlexConnector File

15- ArcSight FlexConnector ID-Based DB

16- ArcSight FlexConnector JSON Folder Follower

17- ArcSight FlexConnector Multiple DB

18- ArcSight FlexConnector Multiple Folder File

Note: CEF is the Recommended format

19- ArcSight FlexConnector Regex File

(N)ext - ---------- Next page ----------

Please select an option [0..19]: 11

Please verify the following parameters

Type: ArcSight Common Event Format Multiple File

Are the values correct [yes/no/back/cancel]? yes

Enter the device details

Row#|Folder|Wildcard|Log File Type

Please select an option: [A]dd [D]elete [I]mport [E]xport [F]inish =>A

Folder[]: /root/Desktop/webroot

Wildcard[*.cef]:

Log File Type:

0- cef

Please select an option [0..0][cef]: 0

Enter the device details

Row#|Folder |Wildcard|Log File Type

---

0 |/root/Desktop/webroot|*.cef |cef

Please select an option: [A]dd [D]elete [I]mport [E]xport [F]inish => F

Are the values correct [yes/no/back/cancel]? yes

| | 0%Verifying the parameters

|##| 100%

Enter the type of destination

0- ArcSight Manager (encrypted)

1- ArcSight Logger SmartMessage (encrypted)

2- ArcSight Logger SmartMessage Pool (encrypted)

3- NSP Device Poll Listener

4- CEF File

5- CEF Syslog

6- CEF Encrypted Syslog (UDP)

7- CSV File

8- Raw Syslog

Note: this is the default option

Please select an option: [ArcSight Manager (encrypted)] [0..8/back/cancel] :0

Enter the destination parameters

****

WARNING: Some of the required parameters will contain security

sensitive information. Do you want to hide the input for these
parameters from the screen? [yes/no]
(note: typically you would answer 'NO' only if you are using a slow
link (like a serial RS232 or a very slow network link) since
this may add additional delays to the connection. If you are
not sure, then select 'YES' or hit enter.
****

[yes]? yes

Input for private parameters will be hidden.

Manager Hostname: ip-10-100-0-24.us-west-1.compute.internal

Manager Port[8443]: _____

User: admin

Password: _____

AUP Master Destination:

0- true

1- false

Please select an option [0..1][false]: 1

Filter Out All Events:

0- true

1- false

Please select an option [0..1][false]: 1

Enable Demo CA:

0- true

1- false

Please select an option [0..1][false]: 0

Please verify the following parameters

Manager Hostname: ip-10-100-0-24.us-west-1.compute.internal

Manager Port: 8443

User: admin

Password: ********

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: true

Are the values correct [yes/no/back/cancel]? yes

Enter the connector details

Name[]: silentConnector

Location[]: WebrootConnectors

DeviceLocation[]: _____

Comment[]: _____

Please verify the following parameters

Name: silentConnector

Location: WebrootConnectors

DeviceLocation:

Comment:

Are the values correct [yes/no/back/cancel]? yes

Enabling demoCA Certs

|##| 100%

Registering destination

|##| 100%

Following certificate will be imported into connector trust store:

Host/port: ip-10-100-0-24.us-west-1.compute.internal_8443

Details: CN=ip-10-100-0-24.us-west-1.compute.internal, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

0- Import the certificate to connector from destination

1- Do not import the certificate to connector from destination

Please select an option: [Import the certificate to connector from destination] [0..1/back/cancel] :0

| | 0%Importing certificate, registering destination and restarting the container

|##| 100%

Add connector Summary

Following are the added connector details:

Connector Name [silentConnector], Connector Type [cef_multifolder_file]

Continue [yes] ? yes

The Smart Connector is currently installed as a standalone application

0- Install as a service

1- Leave as a standalone application

Please select an option: [Install as a service] [0..1/back/cancel] : 1

Would you like to continue or exit?

0- Continue

1- Exit

Please select an option: [Continue] [0..1/back/cancel] : 1

[Fri Dec 04 03:30:17 PST 2015] [INFO] Shutting Down Agent Framework Version [7.1.5.7538.0]

Shutting down Agent Modules now...

Shutting down Agent Setup Wizard...done.

[root@localhost bin]#

4.2 Start the ArcSight SmartConnector

ArcSight SmartConnector may not be automatically started after the installation.

To start SmartConnector:

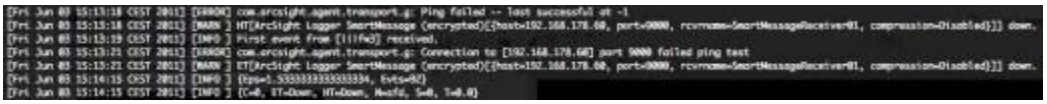
1. To start the SmartConnector, you need to go in the **$ARCSIGHT_HOME/current/bin** directory
2. Execute the **Arcsight script for Linux**, or **arcsight.bat** script under Linux terminal, with the following argument.

```
[root@fw3 bin]# ./arcsight -quiet agents
ArcSight Connectors starting...
```

3. Once started, to **confirm** that the SmartConnector is working properly, you will have to check these outputs.

```
[Fri Jun 03 12:58:04 CEST 2011] [INFO ] First event from [|||fw3] received.
[Fri Jun 03 12:58:56 CEST 2011] [INFO ] {Eps=0.9333333333333333, Evts=56}
[Fri Jun 03 12:58:56 CEST 2011] [INFO ] {C=0, ET=Up, HT=Up, N=sfd, S=56, T=0.9333333333333333}
```

4. Verify the following details:
   - **Eps** > EPS throughput
   - **Evts** > The total number of events have now been processed by the SmartConnector.
   - **ET and HT** > Should have twice the Up value in order to validate the SmartConnector connection with the ESM is working properly. If they are any communication troubles between the SmartConnector and the ESM, you will have these kind of outputs.



Checking Smart Connector Availability

To check SmartConnector availability:

1. To validate that the SmartConnector is **up** and **running**, use the following command.

```
[root@fw3 bin]# ./arcsight -quiet agentup
ArcSight Cluster Id (ARCSIGHT_CID): [null]. Agents are running. Returning [0]
```

2. If the SmartConnector is down, you will have this result.

```
[root@fw3 bin]# ./arcsight -quiet agentup
ArcSight Cluster Id (ARCSIGHT_CID): [null]. Agents are NOT running. Returning [1]
```

3. This command will not validate that the communication between the SmartConnector and the ESM is up and running.

Restarting the SmartConnector

To restart the SmartConnector:

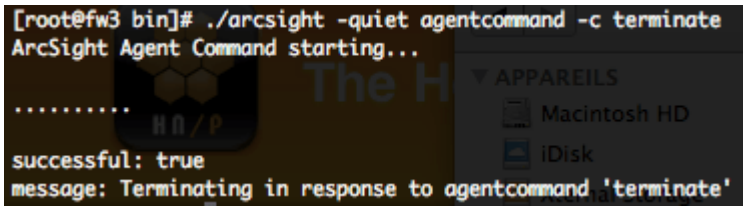
1. To restart the SmartConnector you will have to use the following command.

```
[root@fw3 bin]# ./arcsight -quiet agentcommand -c restart
ArcSight Agent Command starting...
.....
successful: true
message: Restarting in response to agentcommand 'restart'
```

Stopping the Smart Connector

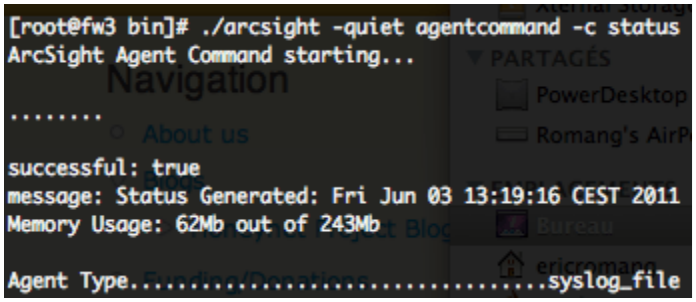
To stop the SmartConnector:

1. If you have to start the SmartConnector in the standalone mode, a simple CTRL+C will terminate the activities. But you can also stop the activities with the following command:



4.3 Verifying Connection

1. To check the complete SmartConnector **status,** use the following command.



4.4 Saving agent id for ESM Console Setup (optional)

1. Open the SmartConnector for Webroot log data command prompt and copy the text after agent id enclosed in square braces as selected in below screen.

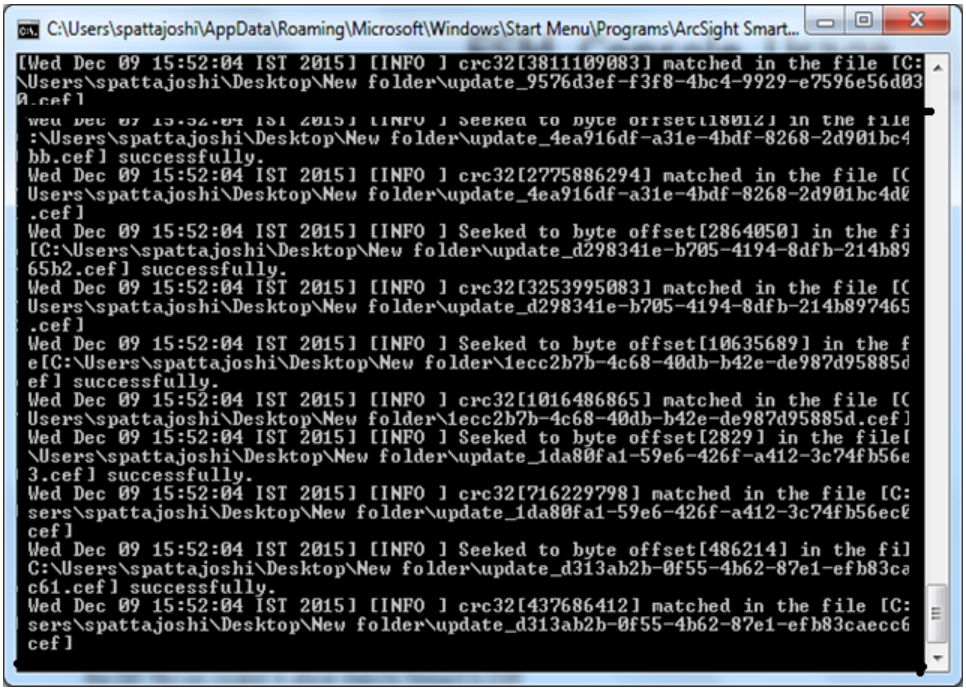
   Ex: - agent id [3VkpQQlEBABCDi2riUdhLrA==]

   Note: We can also filter bright cloud data using device vendor property as WEBROOT.

2. If you have chosen to run as a service, this step is not required. You can filter data using AgentID directly.

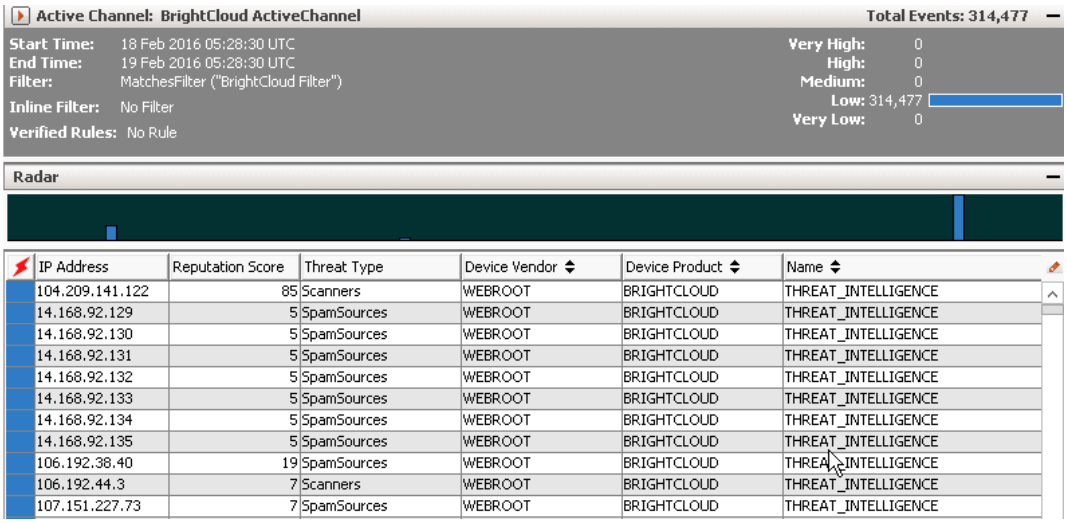
Chapter 5: Utilizing the BrightCloud data in ESM Console

Run **SmartConnector**, and view log at INFO level to verify that CEF events are being updated.



5.1 BrightCloud ActiveChannel in ESM Console

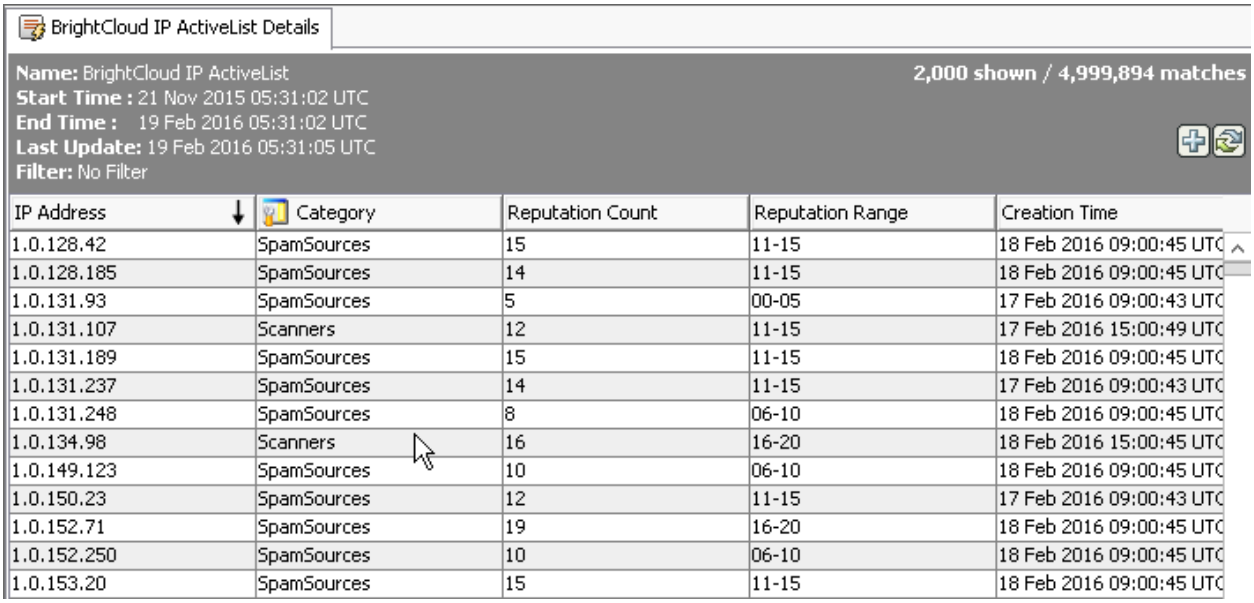
Active channels provide a streaming view of events coming into your system that can be viewed numerous ways using numerous types of filters and field sets.



IP Address	Reputation Score	Threat Type	Device Vendor	Device Product	Name
104.209.141.122	85	Scanners	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.129	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.130	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.131	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.132	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.133	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.134	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
14.168.92.135	5	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
106.192.38.40	19	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
106.192.44.3	7	Scanners	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
107.151.227.73	7	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE

5.2 BrightCloud IP data ActiveList

ActiveLists are usually defined in conjunction with rules specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules are empty or contain only manually added entries that have not timed out.

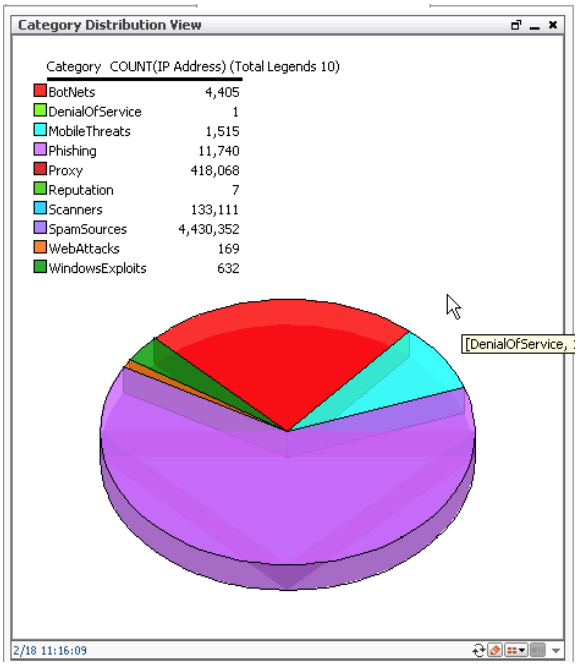


IP Address	Category	Reputation Count	Reputation Range	Creation Time
1.0.128.42	SpamSources	15	11-15	18 Feb 2016 09:00:45 UTC
1.0.128.185	SpamSources	14	11-15	18 Feb 2016 09:00:45 UTC
1.0.131.93	SpamSources	5	00-05	17 Feb 2016 09:00:43 UTC
1.0.131.107	Scanners	12	11-15	17 Feb 2016 15:00:49 UTC
1.0.131.189	SpamSources	15	11-15	18 Feb 2016 09:00:45 UTC
1.0.131.237	SpamSources	14	11-15	17 Feb 2016 09:00:43 UTC
1.0.131.248	SpamSources	8	06-10	18 Feb 2016 09:00:45 UTC
1.0.134.98	Scanners	16	16-20	18 Feb 2016 15:00:45 UTC
1.0.149.123	SpamSources	10	06-10	18 Feb 2016 09:00:45 UTC
1.0.150.23	SpamSources	12	11-15	17 Feb 2016 09:00:43 UTC
1.0.152.71	SpamSources	19	16-20	18 Feb 2016 09:00:45 UTC
1.0.152.250	SpamSources	10	06-10	18 Feb 2016 09:00:45 UTC
1.0.153.20	SpamSources	15	11-15	18 Feb 2016 09:00:45 UTC

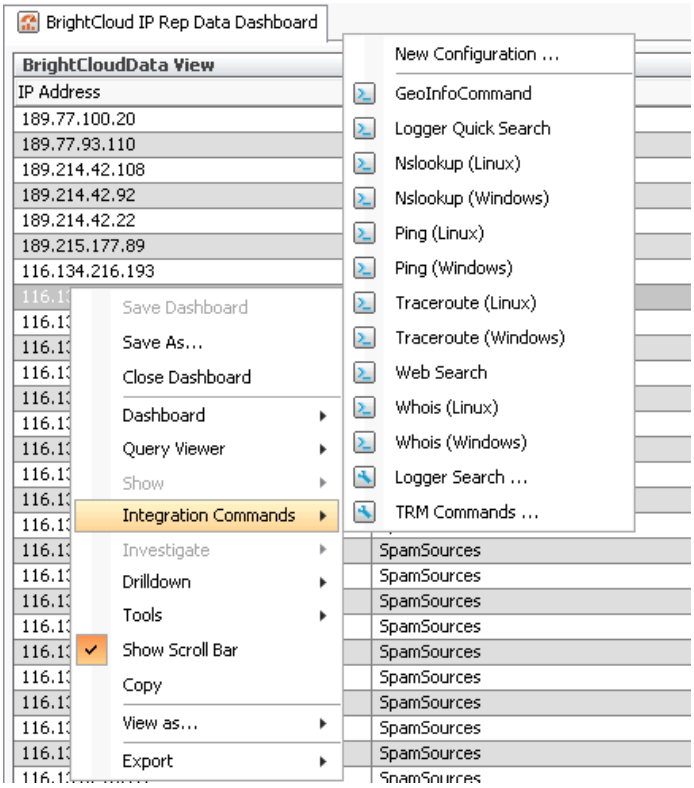
5.3 Dashboard displays categories as a pie chart

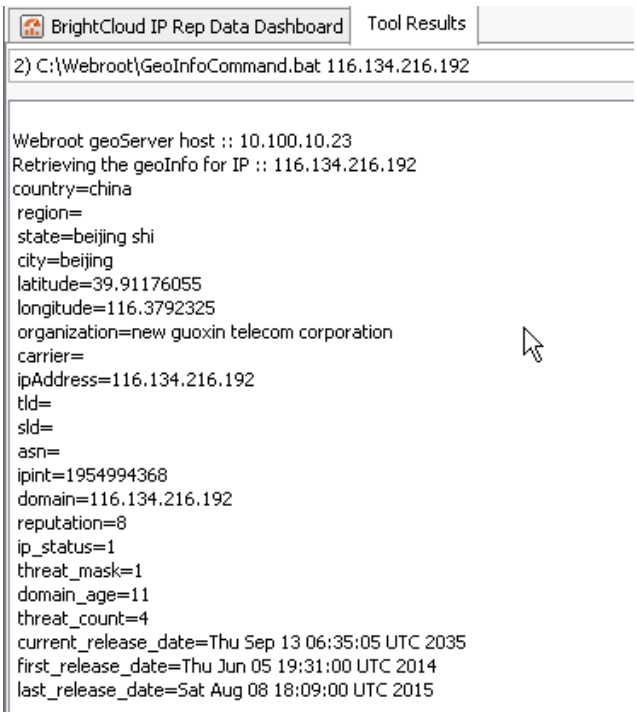
Dashboards can display data in a number of graphical formats, including the following:

- Pie charts
- Bar charts
- Tables
- Custom layouts



5.4. User can obtain additional geolocation information of the IP





Chapter 6: Customizing ESM Console Resources

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

The ESM Console serves as the control point for ArcSight Express and ESM administrators to configure content and resources. While Webroot has provided all the components necessary to begin using BrightCloud Threat Intelligence 'out of the box' (refer to Chapter 2.3 Importing the Webroot BrightCloud ARB for ESM console), additional configuration and tuning is possible through ESM. In this chapter we provide some information on additional configuration.

Note: The following instructions are based on ESM Console version 6.8.0. For up-to-date ESM information, please check HPE ArcSight's product documentation.

6.1 Location

ESM provides a location database that maps an IP address to the owning body for the block of IP addresses to which it belongs. Your organization may have finer-grained detail, such as the physical location of all of your networks or networks outside your control, or corrections to the database that ESM supplies. The Location resource is the way you can override the ESM default location mappings with location information relevant to your network.

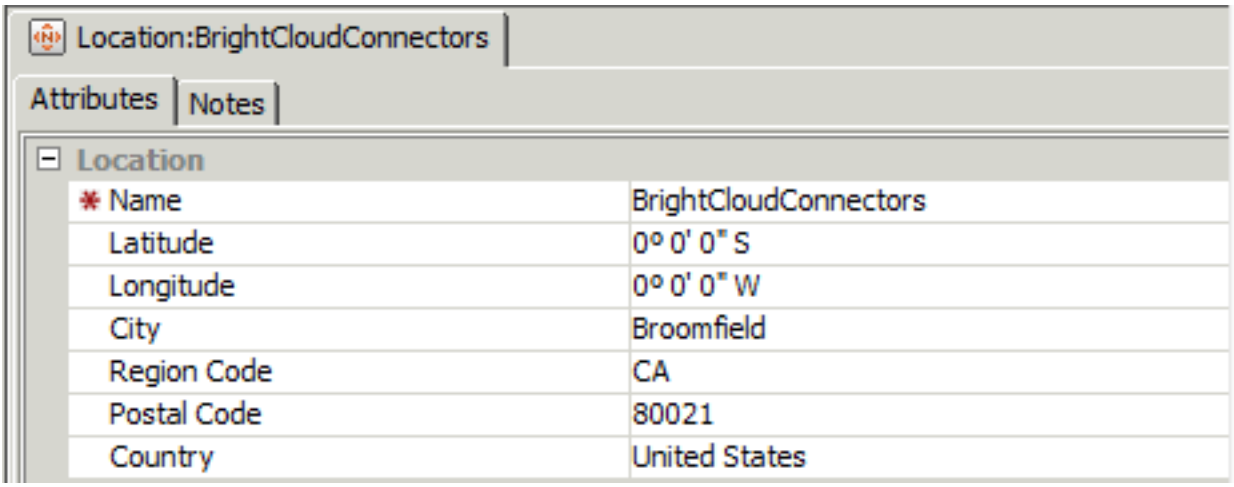
Location is an attribute you can set if the asset you are modeling resides in a geographic location that differs from the location set by the mapping database that associates IP addresses with location information.

To create a location:

1. Check the **Navigator** panel on top left of ESM console and click the **Resources** tab.
2. Click the drop-down and select **Assets** as in below screen.
3. Click the **Locations** sub-tab for **Assets** resource.

4. Right-click **public group** and select **New Location** to create new Location as in below screen.
5. Check **Inspect/Edit** panel on top right of ESM console and provide below details to create a new location in **Attributes** tab.

   Name :- BrightCloudConnectors
6. Leave other fields default and click **Apply** button as in below screen to save the attribute values.
7. Check Navigator panel, the created Location BrightCloudConnectors will be added into Public group as in below screenshot.



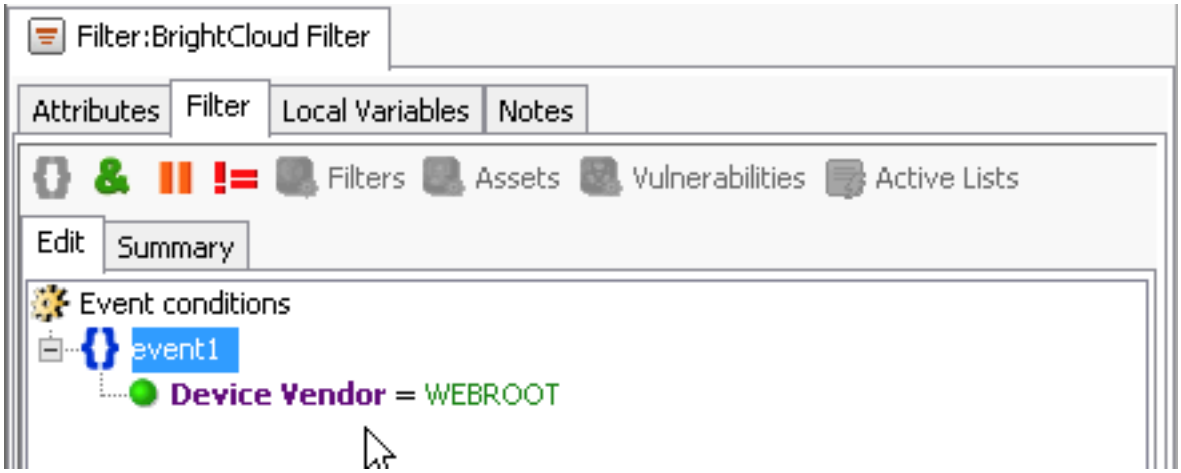
6.2 Filter

Filters are used to specify criteria that narrow the scope of monitored data and reduce the number, or constrain the nature, of the Events displayed through the Console.

Filtering criteria are based on the Console's event Data Fields, used in various combinations and with various conditions placed on their content. As you apply more restrictive filter parameters, the number of events reaching the Console may decrease, but the likelihood increases that the events are significant.

To create a filter:

1. Login to the ESM Console and go to **Filters** section.
2. Select **Filters** from the Resources drop-down as below screenshot.
3. Right-click on admin's **Filters** and select **New Group** to create new group.
4. Provide name as **BrightCloudFilters** for the group as below screenshots.
5. Right-click on **BrightCloudFilters** group and select **New Filter** to create new filter as below screen.
6. In **Inspect/Edit** panel provide details in tabs as below screenshot.
7. In Filter tab, right-click on **Events** and select **New Condition -> Device->Device Vendor**.
8. Paste the **agent id** we copied on above steps from Webroot SmartConnector command prompt (WEBROOT) in the text field after the equals' operator.
9. Click **OK** and **Apply** button.



6.3 Field Sets

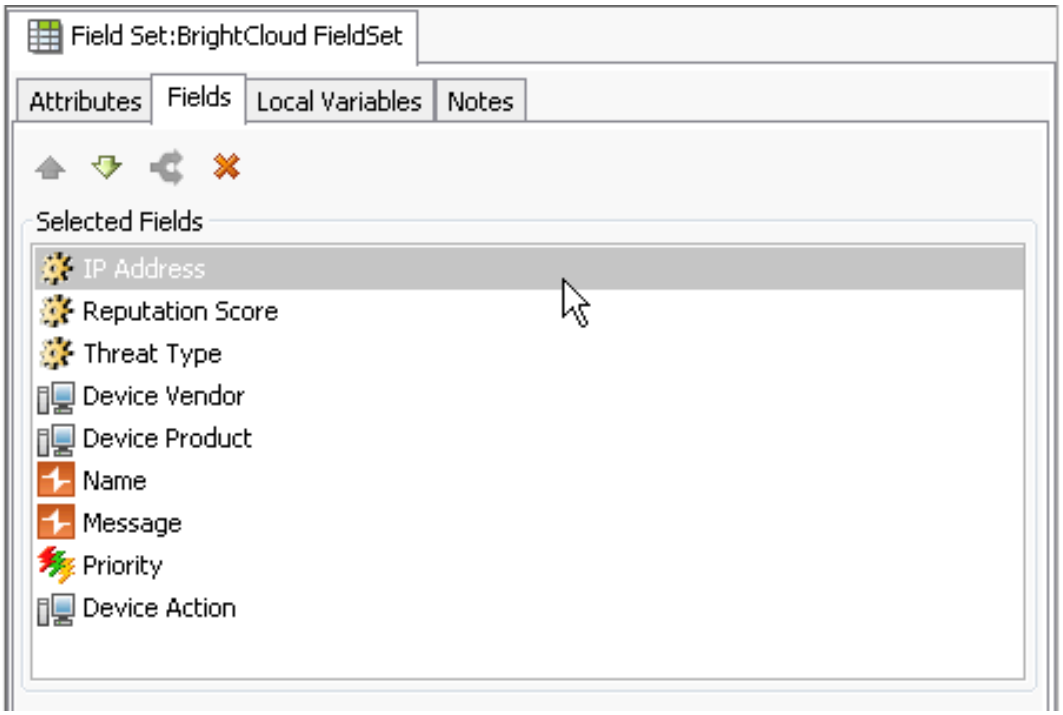
Field sets are named subsets chosen from the available Data Fields. Field sets can help you quickly focus a grid view, Event Inspector, or other field array on a particular context such as customer accounts or vulnerability.

Field sets are a shareable resource that you can manage and apply through the Field Sets resource tree in the Active Channels section of the Navigator panel.

In the Navigator, select **Active Channels**, and click the **Field Sets** tab. These field sets also support the Variables data fields. Field sets supersede and include the previous concept of column sets.

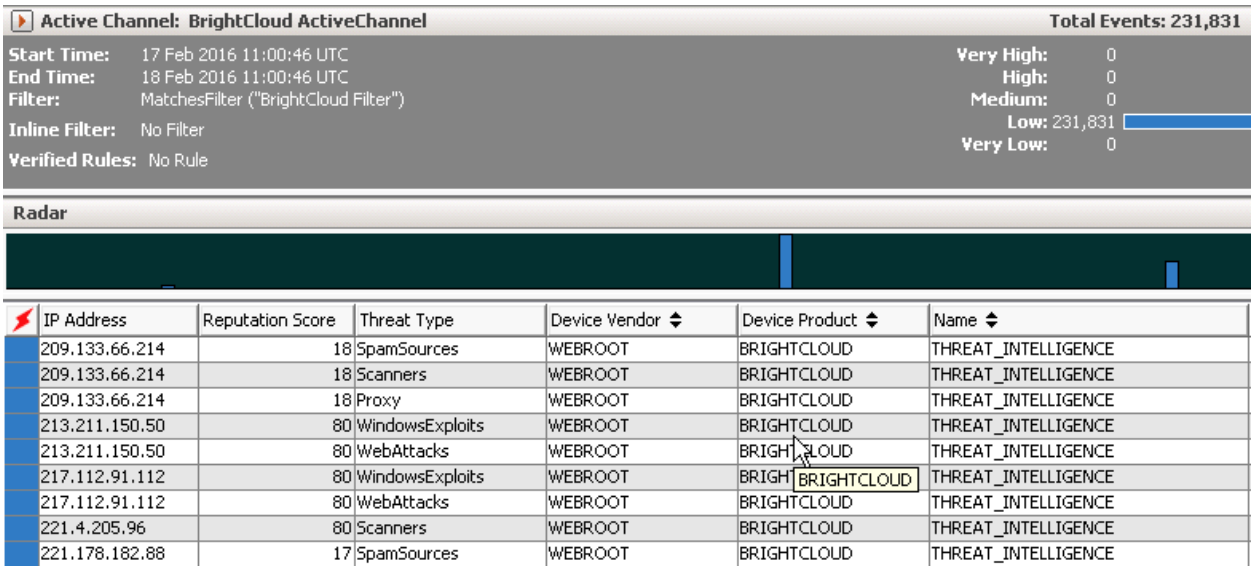
To create a field set:

1. Choose **Field Sets** from Resources drop-down in Navigator panel as below screenshot.
2. Right-click on admin's **Field Sets** and choose **New group** to create a new group under which we will create Field Set.
3. Type the name as **BrightCloud FieldSets** and press **Enter**.
4. Right-click on group **BrightCloudFieldSets** and choose **New Field Sets**. In Inspect/Edit panel, provide details in different tab as below screenshot.



6.4 ActiveChannels

Almost all event-related views are **ActiveChannels**. ActiveChannels are definitions for collections of events; definitions that are always freshly re-evaluated so the resulting sets are as valid as the data received up to that moment.



IP Address	Reputation Score	Threat Type	Device Vendor	Device Product	Name
209.133.66.214	18	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
209.133.66.214	18	Scanners	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
209.133.66.214	18	Proxy	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
213.211.150.50	80	WindowsExploits	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
213.211.150.50	80	WebAttacks	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
217.112.91.112	80	WindowsExploits	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
217.112.91.112	80	WebAttacks	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
221.4.205.96	80	Scanners	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE
221.178.182.88	17	SpamSources	WEBROOT	BRIGHTCLOUD	THREAT_INTELLIGENCE

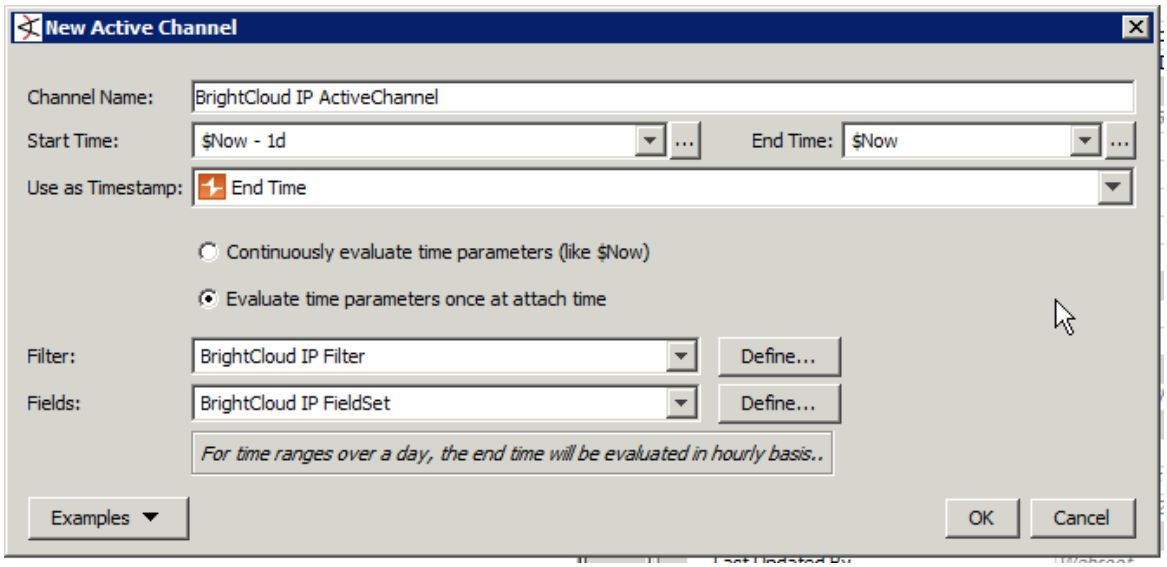
To create an ActiveChannel:

1. Choose **Active Channel** from the Resources drop-down in Navigator panel.
2. Right click on **admin's Active channels** and choose **New Group** to create new group under which we will create Active channel.
3. Type the name *BrightCloudActiveChannels* and press **Enter**.
4. Right click on **BrightCloudActiveChannels** group and select **New Active Channel**.
5. Provide below details for creating Active channel for reading **BrightCloud Malicious IP Data:**

   - **Channel Name —** BrightCloud ActiveChannel
   - **Start Time —** $Now - 2h
   - **End Time —** $Now
   - **Use as Timestamp —** Manager Receipt Time
   - Select the **Continuously evaluate time parameters (like $Now)** radio button.

- **Filter —** Choose **BrightCloud IP Filter**; created above.
- **Fields —** Choose **BrightCloud IP FieldSet**; created in above steps.

6. Click the **OK** button.



6.5 Active Lists

Active lists are used to create a configurable data store that can hold information derived from events, or other sources.

Active lists can monitor activity based on any rule-driven combination of event attributes or set of custom fields. For example, active lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised.

Active lists function differently than active channels. Active lists are not continuously re-evaluated and are not time-window constrained. Active lists draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them

To create an ActiveList:

1. From the Resources drop-down in the Navigator panel, select **Lists**.
2. Click the **Active Lists** tab.
3. Right-click on admin's **Active Lists** group and choose **New group** to create new group.
4. Type the name *BrightCloud ActiveLists* and press **Enter**.
5. Right-click on the group **BrightCloud ActiveLists** and choose **New Active List** to create list.
6. On Inspect/Edit panel give below details as below screenshot.
7. ActiveList Capacity is determined by the **activelist.max_capacity** property in ESM manager configuration.

   You need to refer to ArcSight User's guide version 6.8, List Authoring chapter on page 511 to learn about how to set this property.
8. You will also need to change the memory settings as shown below, in order for the

   In *server.config* file Add the property

   ➔ activelist.max_capacity=20000000

In *server.wrapper.config* Add the two properties

➔ **wrapper.java.initmemory=32768**

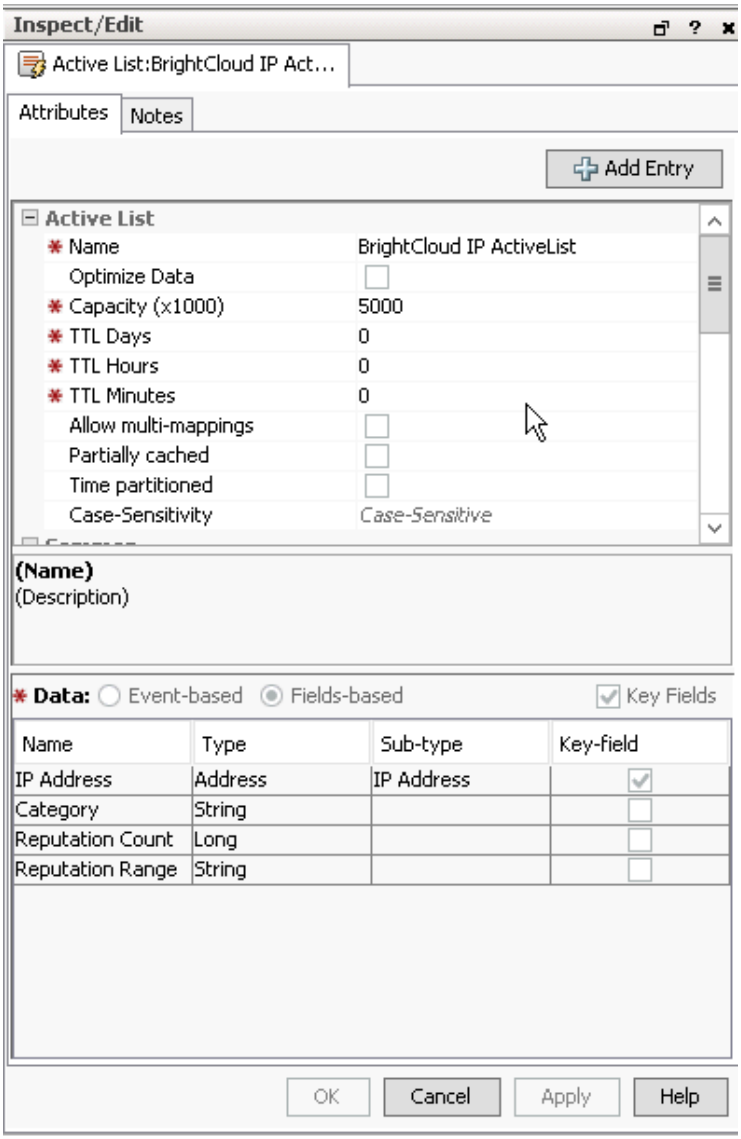
➔ **wrapper.java.maxmemory=32768**

Note: Depending on the size of the memory available in your environment, you can increase the java memory values.

9. The number of records in the ActiveList should be set using Capacity property in order to match the max capacity.

10. Set TTL Days=0 so that the ActiveList data never expires.

11. Click the **Apply** button to save the changes.



6.6 Query

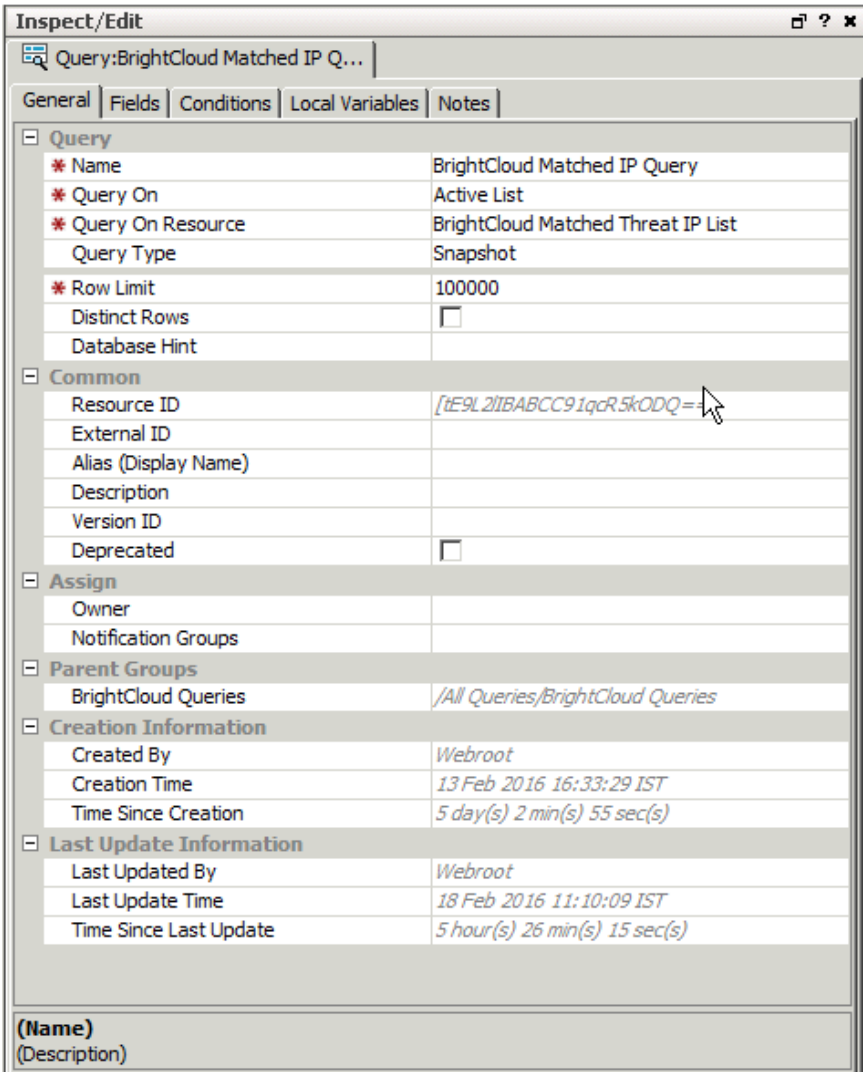
A query is an ArcSight resource that defines the parameters of the data you want to report on derived from an ArcSight data source. The result of the query then becomes the basis for one or more ArcSight report. The Query Editor is a component of ArcSight Reporting resource tools.

In a query, you select the data fields you want to report on, specify any additional functions you want run on them (such as sum, average, and so on), and any sort or group-by conditions you want to add, such as grouping results by source address, zone, or priority.

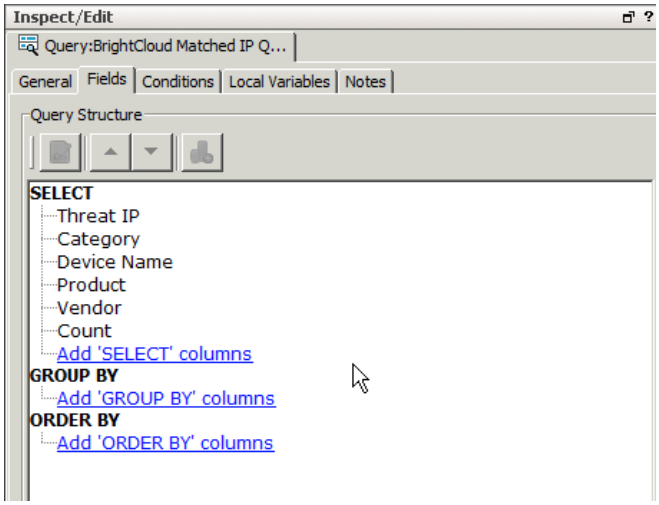
To build a query:

1. Select **Reports** from the Resources drop-down in Navigator panel.
2. Click the **Query** tab.
3. Right-click on admin's query and select **New group** to create new group under which we will be creating query.
4. Type the name *BrightCloud Queries* and press **Enter**.
5. Right-click on the group **BrightCloud Queries** and select **New Query**.

6. In Inspect/Edit panel provide details in Attributes tabs below screenshot.



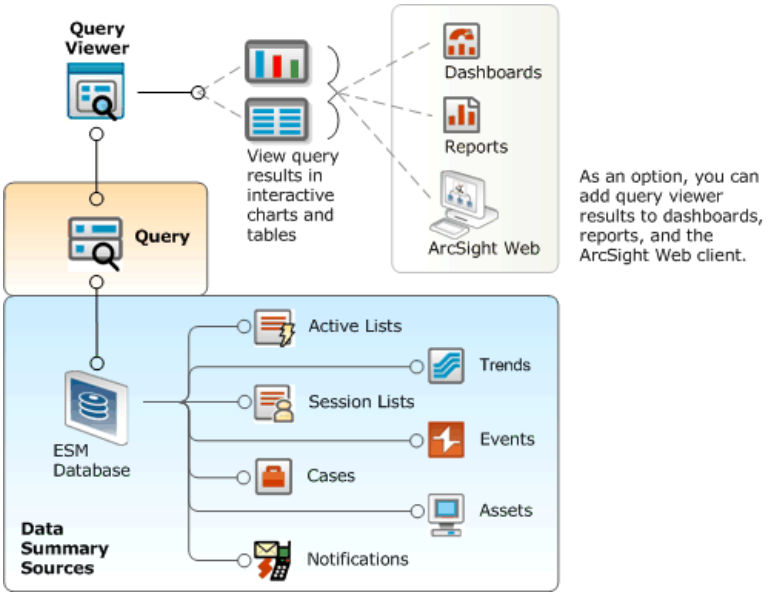
7. Provide details in Fields and Conditions tab as below screenshot.



6.7 Query Viewers

Query viewer is a type of resource for defining and running SQL queries on other ESM resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results. The query viewer you create displays all the fields and domain fields specified in the query you select (or create) for the query viewer.

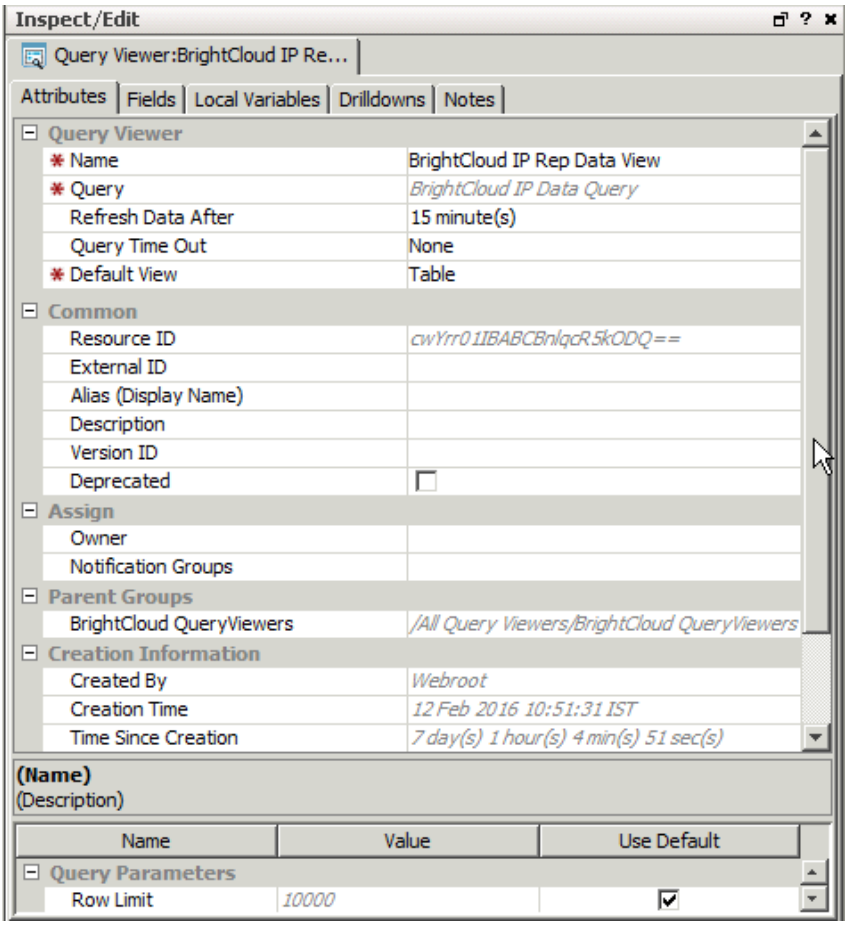
Query viewers provide high-level summaries to monitor system health, reveal trends, and allow for drill-down investigation of all types of resources.



To create a query viewer:

1. In the Navigator panel, choose the **Query Viewers** resource.
2. Right-click on admin's **Query viewers group** and choose **New group**.
3. Give name as BrightCloudQueryViewers and press **Enter**.
4. Right click on **BrightCloudQueryViewers** and choose **New Query Viewer**.
5. On Inspect/Edit panel provide details in attributes tab as below screenshot.

6. Leave other fields default in Attributes and other tabs and click **Apply** button.



6.8 Dashboard

Dashboards are a graphical display of data gathered from one or more Query viewers. Dashboards can display data in a number of graphical formats, including pie and bar charts, tables, and custom layouts.

In the Navigator panel's Dashboards resource tree, right-click a dashboard and choose **Show Dashboard**.

To create a dashboard:

1. Choose **Dashboard** from the Resources drop-down in Navigator panel.
2. Click **Dashboards** tab.
3. Right-click on admin's **Dashboards** and choose **New group** to create new group
4. Give name as BrightCloud Dashboards and press **Enter**.
5. Right click on **BrightCloud Dashboards** group and select **New Dashboard**.
6. Right-click on **Untitled - Dashboard** in the Viewer panel and choose **Save Dashboard as**.
7. Provide Name as **BrightCloudThreatIPDashboard** and select **BrightCloudDashboards** group.
8. Click **OK** button.
9. Go to QueryViewers resource by choosing **QueryViewers** under Resource drop down in Navigator panel.
10. Select the query viewer **BrightCloudThreatIPQueryViewer** we created before and right-click and select **BrightCloudThreatIPQueryViewer -> Add to Dashboard as -> Table**.

    We will be seeing the data populating in dashboard.

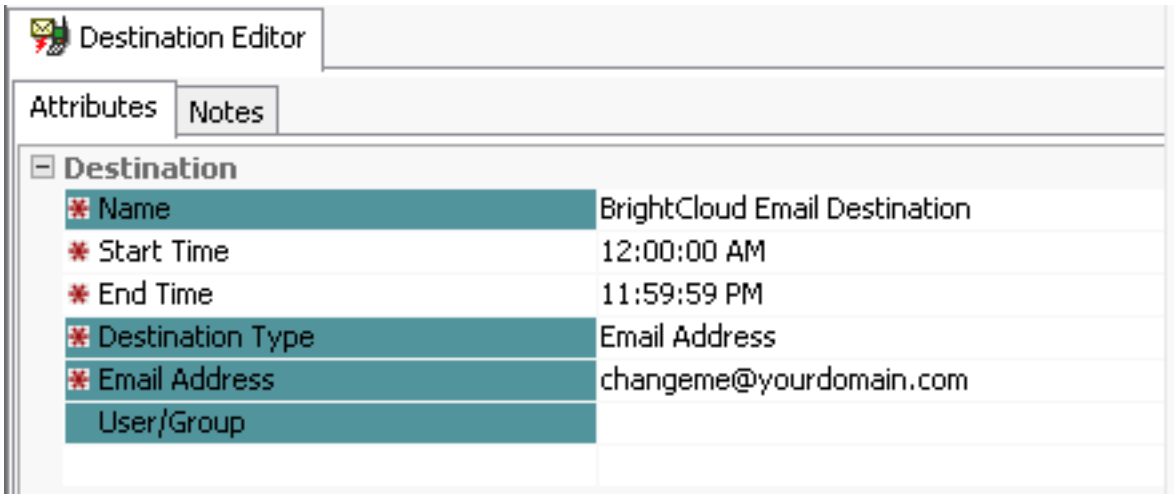
6.9 Notification

To be informed when certain defined events or circumstances occur. You might receive notifications by pager, or e-mail or similar means, but you can be sure to see an indicator in the Notifications button in the toolbar line of the Console.

ESM Console helps you stay informed about developing situations involving events, and critical system status.

To create a notification:

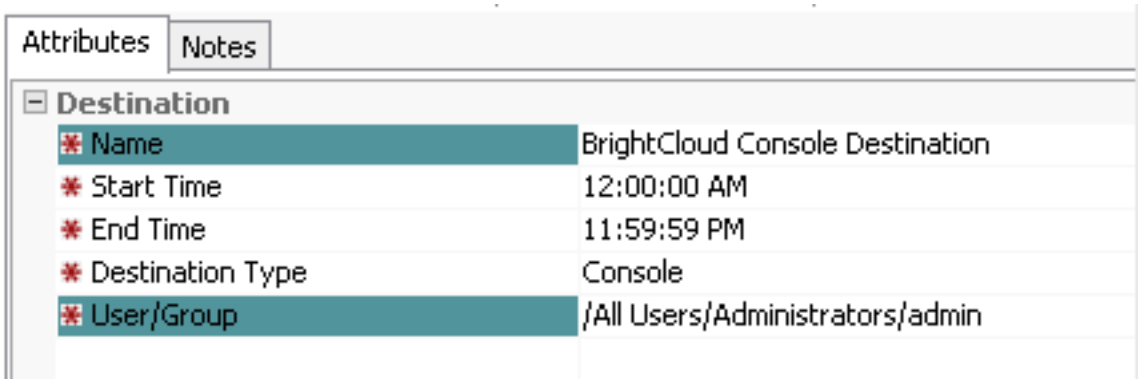
1. Choose **Notifications** from Resources drop-down in Navigator panel.
2. Create new destination at **SOC Operators -> Level 1 -> New Destination**.



3. Provide below details on Inspect/Edit panel:
   - **Destination Type —** Email Address
   - **Email —** [changeme@yourdomain.com] # Email to which notification will be sent
   - **User group —** [user group]
   - **Name —** EmailNotification
4. Click the **Apply** button.
5. Configure **One more Destination** for sending Notification in Console.
6. Right click **Level1 -> New Destination**.

7. Provide below details on right side Inspect/Edit panel:

   - **Destination Type —** Console
   - **User group —** [user group]
   - **Name —** BrightCloud Console Destination



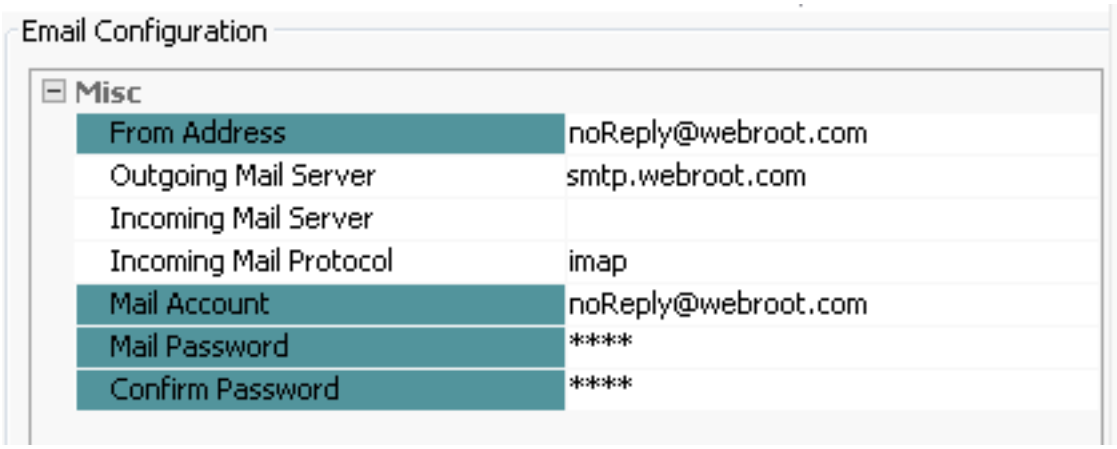
8. Click the **Apply** button.

   You have successfully configured Notification for Email and Console.

6.10 Changing Email Settings for Notification

To change email settings:

1. In the Notification resource tree, right-click **SOC Operators group** and choose **Settings**, then **Edit E-mail Settings**.



2. In the Notification Editor, type in the following text fields:

   - **From Address —** [E-mail address]
   - **Outgoing Mail Server —** [mail server]
   - **Incoming Mail Server —** [incoming mail server]
   - **Incoming Map Protocol —** [imap/pop3] #Change as per above server

3. Type the **E-mail Account password** in the Password text field and confirm it in the Confirm Password text field.

4. Click the **Apply** button.

6.11 Rules

An ArcSight rule is a programmed procedure that attempts to correlate incoming network Events and generates new events that report on correlation when it occurs, as determined by security policy. Rules also apply Conditions and perform Rule Actions.

A rule has three parts: a condition, threshold and time window aggregation, and an action. The condition states if exists and satisfies expressions and the action states do expressions. A rule states if [one or more conditions] exist and satisfy the rule, then do [action expressions].

A rule can have one or more rule conditions. If there is one condition, the rule acts as a filtering tool. If there is more than one condition, the rule acts as a correlation tool. A rule can be created for any incoming event from one or more event generators, with various conditions, logic statements, and threshold and time window qualification of events.

6.11.1 Create Rule

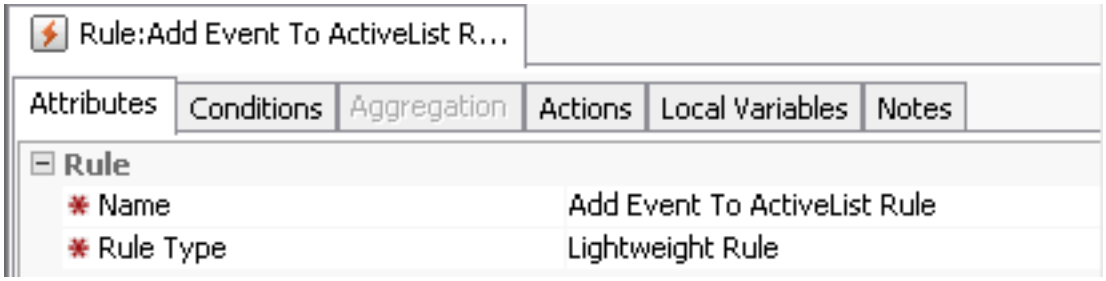
To create a rule:

1. From the Resources drop-down in the Navigator panel, select **Rules**.

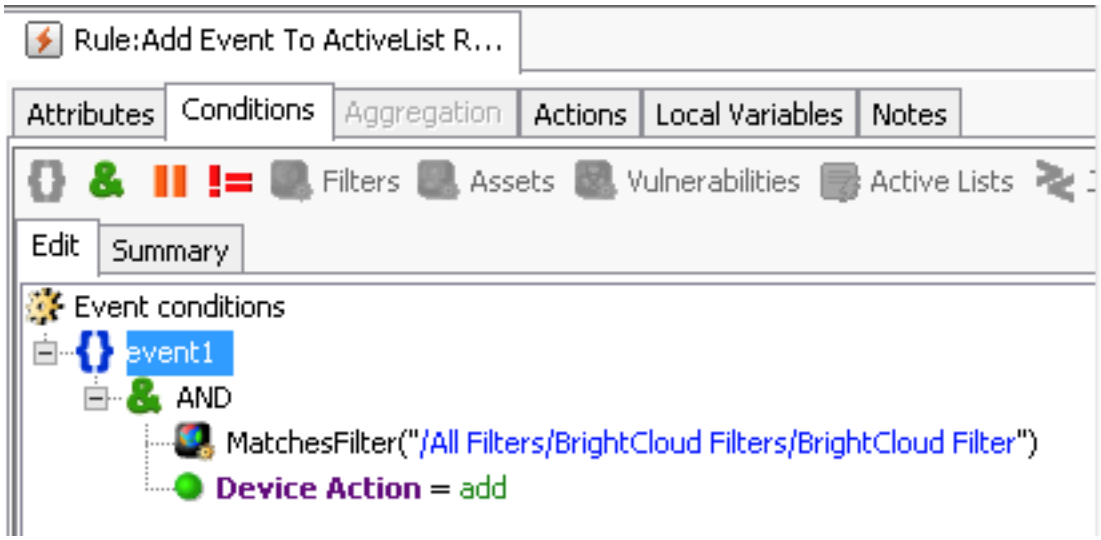
2. Right-click on **Real Time Rules** and select **New Group**.

3. Type the name *BrightCloudRules* and press **Enter**.

4. Right-click **BrightCloudRules** group and select **New Rule -> Lightweight Rule**.

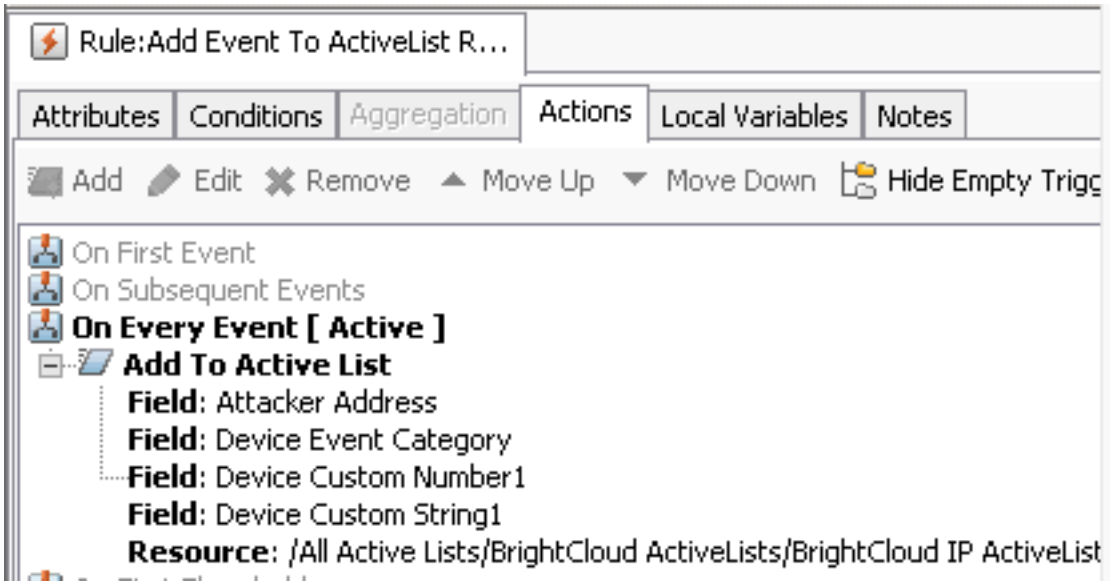


5. On Inspect/Edit panel provide below details for Attributes and Conditions tab.



6. Click the **Actions** tab and right-click on **On Every Event** and select **Active Trigger**.

7. Right-click on **On Every Event** and select **Add -> Active List -> Add to Active List**.

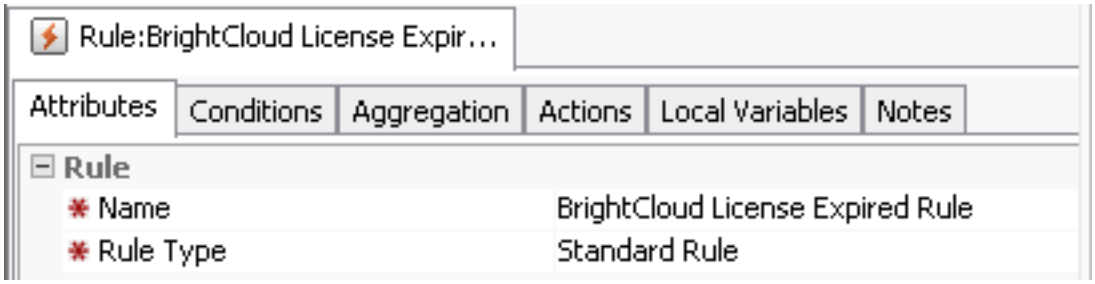


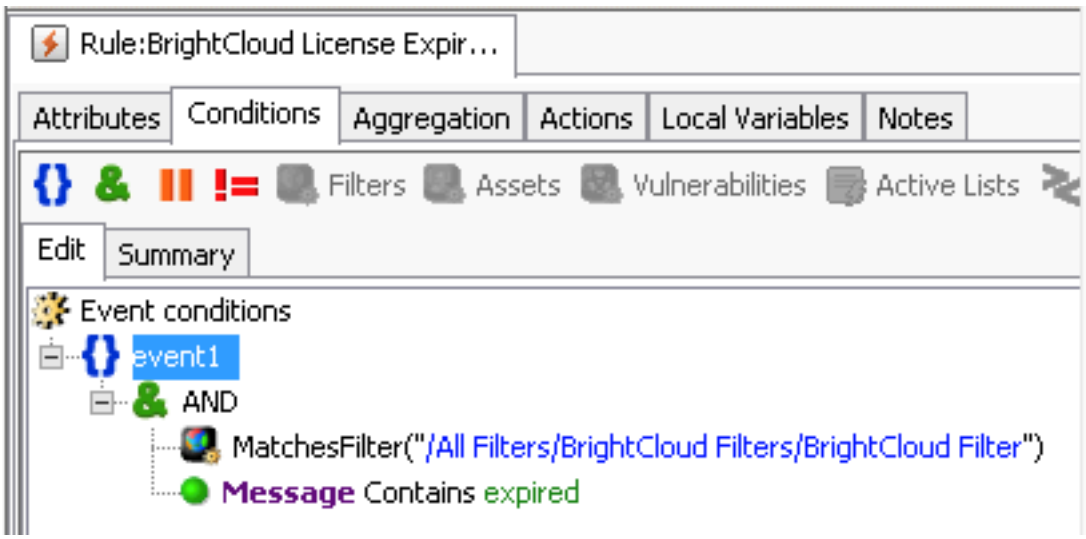
8. Choose **BrightCloudDataActiveList** from the drop-down and click **OK** button.
9. Choose below fields for each fields in Active List for mapping from real time event values to Active list field.
   - **Webroot IPAddress —** Attacker Address
   - **Category —** Device Event Category
   - **Action —** Device Action
   - **Reputation Score —** Device Severity
   - **Message —** Message
10. Click the **OK** button.
11. Click the **Apply** button and click the **Yes** button.

6.11.2 Configure Rule for License Expiry Notification for BrightcloudConnector

To configure rule for license expiry notification:

1. Create rule and provide details in Attributes and Conditions tab as below screenshot.





2. Click the **Actions** tab.

3. Right-click **On Every Event** and select:

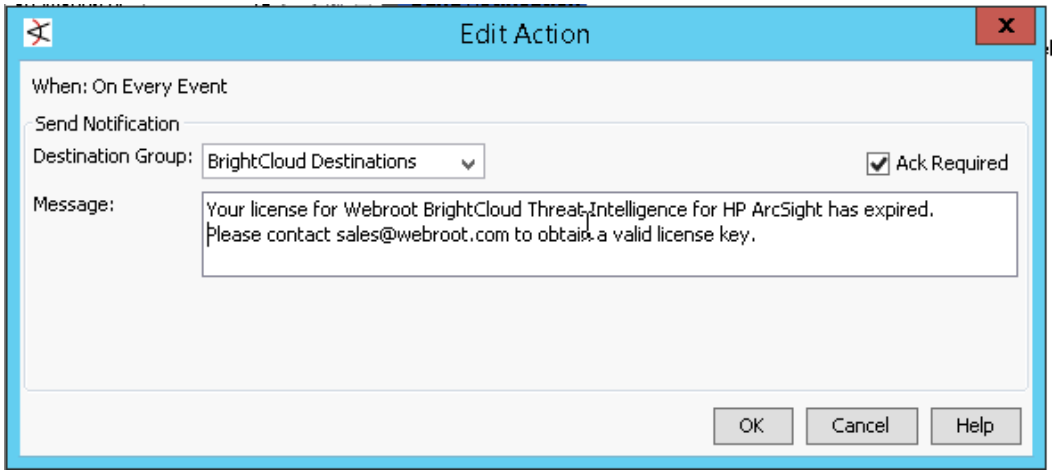
   - **On Every Event -> Active Trigger**
   - **On Every Event -> Add -> Send Notifications**

4. Provide below details

   - **Destination Group —** SOC Operators
   - **Message —** Your License has already Expired. Please check # Subject line in mail notification.

5. Click the **OK** button.

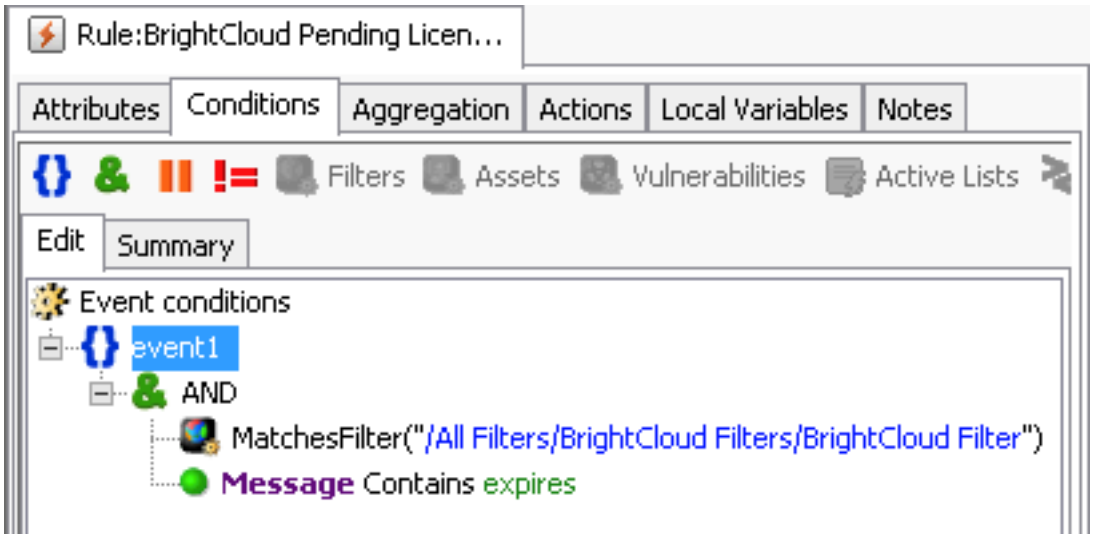
6. Click the **Apply** button.



6.11.3 Configure Rule for Pending License Expiry Notification

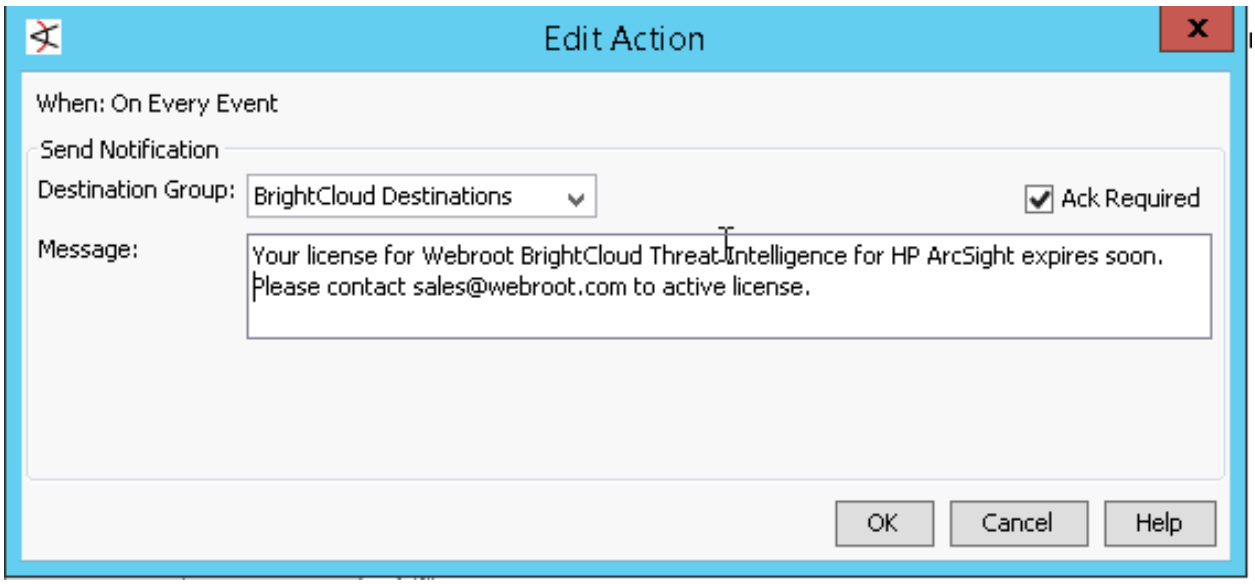
To create a configure rule for pending license expiry notification:

1. Create rule and provide details in Attributes and Conditions tab as below screenshot.



2. Click **Actions** tab.
3. Right-click the following:
   - **On Every Event -> Activate Trigger**
   - **On Every Event -> Add -> Send Notifications**
4. Select Destination Group as **SOC Operators**.
5. Add text as shown below image.

6. Click the **OK** button and then click the **Apply** button.



6.12 Integration Command

Integration commands provide a lightweight way to link to information and run commands from ESM Console in other views and applications. You can build and launch commands locally and on remote servers or appliances, using field values in ESM events as command parameters. You can configure the commands as context-aware, right-click options on different views, resources, and editors on the ESM Console

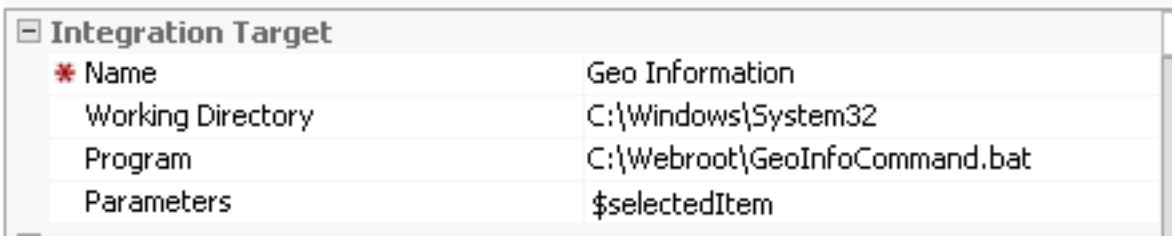
To create an integration command:

1. From the Resources drop-down in the Navigator panel, select **Integration Commands**.
2. Click **Commands** tab.
3. Right-click on **admin's Integration commands** and choose **New group** to create new group.
4. Type the name as BrightCloudIntegrationCommands and press **Enter**.
5. Right-click on **BrightCloudIntegrationCommands** group and choose **New Command**.
6. On Inspect/Edit panel choose **Type = Script**.

7. Provide below details in the Attributes tab.

   - **Name —** GeoInfoCommand
   - **Working Directory —** C:\Windows\System32
   - **Program —** [Path to batch script]
   - **Parameters** - $selectedItem

8. Click the **Apply** button.



6.13 Integration Configuration

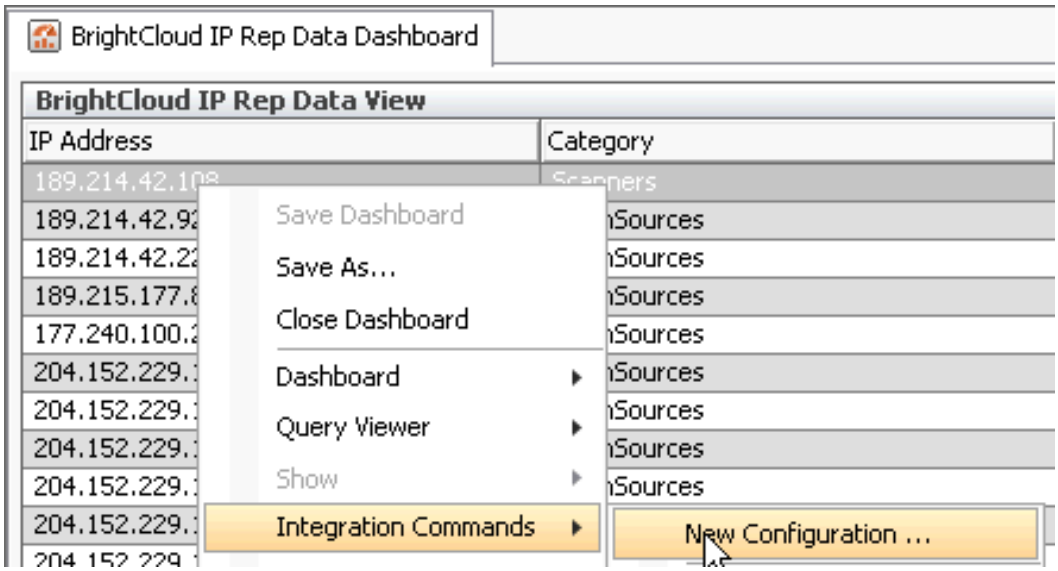
An integration configuration resource represents a family of commands of the same type. Commands in a configuration share the same context, rendering method, and targets.

Configurations provide a way of grouping similar commands and specifying common options for where on the Console UI the commands will be available (contexts), how command results will be displayed (renderer), and where commands will run (scripts run locally; others, like Connector commands, can have one or more remote targets).

To create integration configuration:

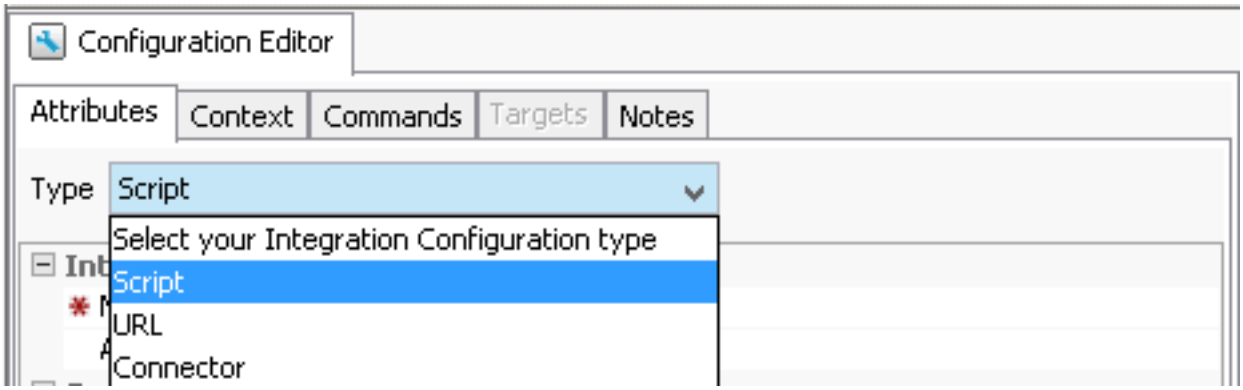
1. From the Resources drop-down in the Navigator panel, select **Integration Command**.
2. Click the **Integration Configuration** tab.
3. Right-click on **admin's Integration Configurations** and select **New group**.
4. Type the name *BrightCloudIntegrationConfigurations* and press **Enter**.
5. Show Dashboard we created in above steps in Viewer panel as below screenshot.

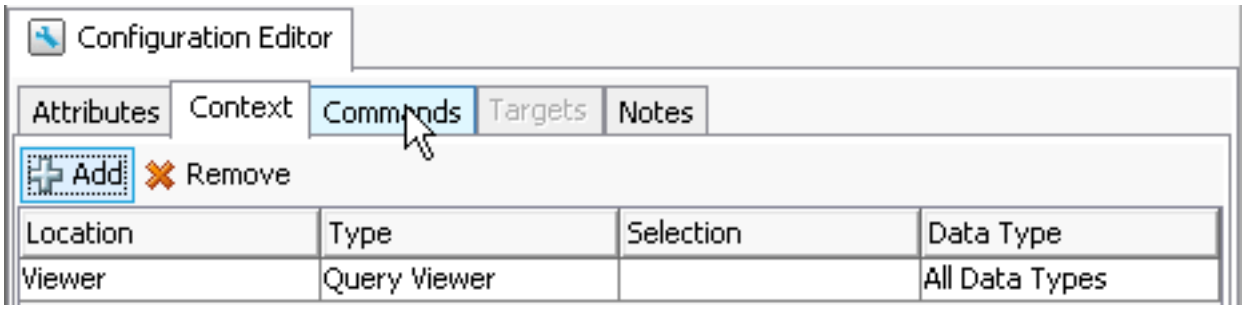
6. Right-click on any IP address column in the Dashboard and select **Integration Commands -> New Configuration**.



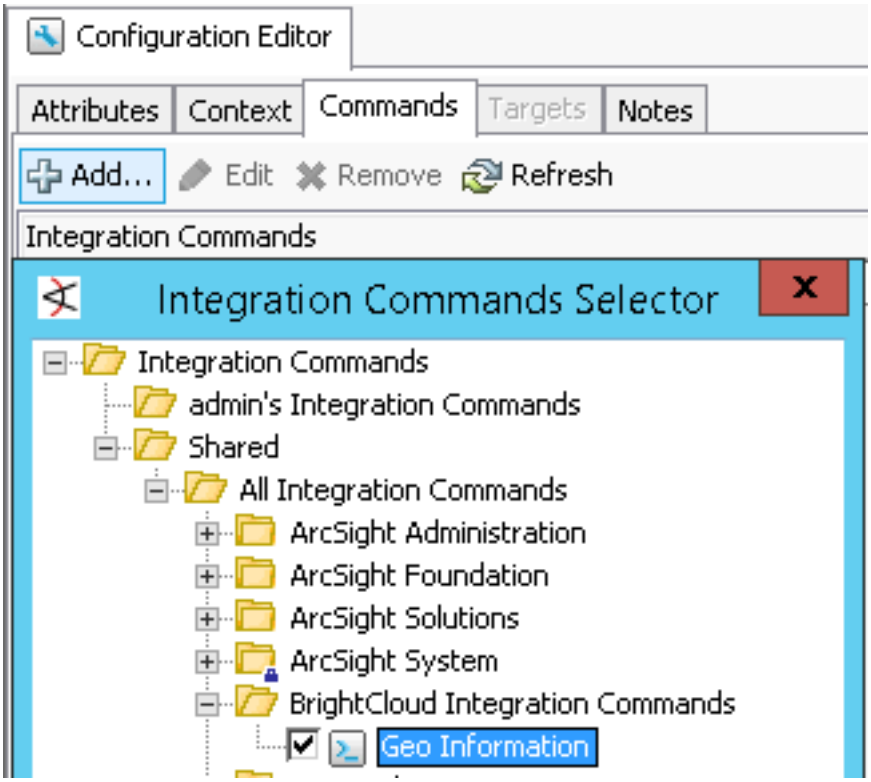
7. On the Inspect/Edit panel, select **Type = Script**.
8. Provide below details in Attributes tab:
   - **Name —** GeoInfoConfiguration
9. Click the **Commands** tab, the click the **Add** button, and select **GeoInfoCommand** we created before.
10. Press the **OK** button.
11. Press the **Apply** button.

12. Show Dashboard we created in above steps in Viewer panel as below screenshot.

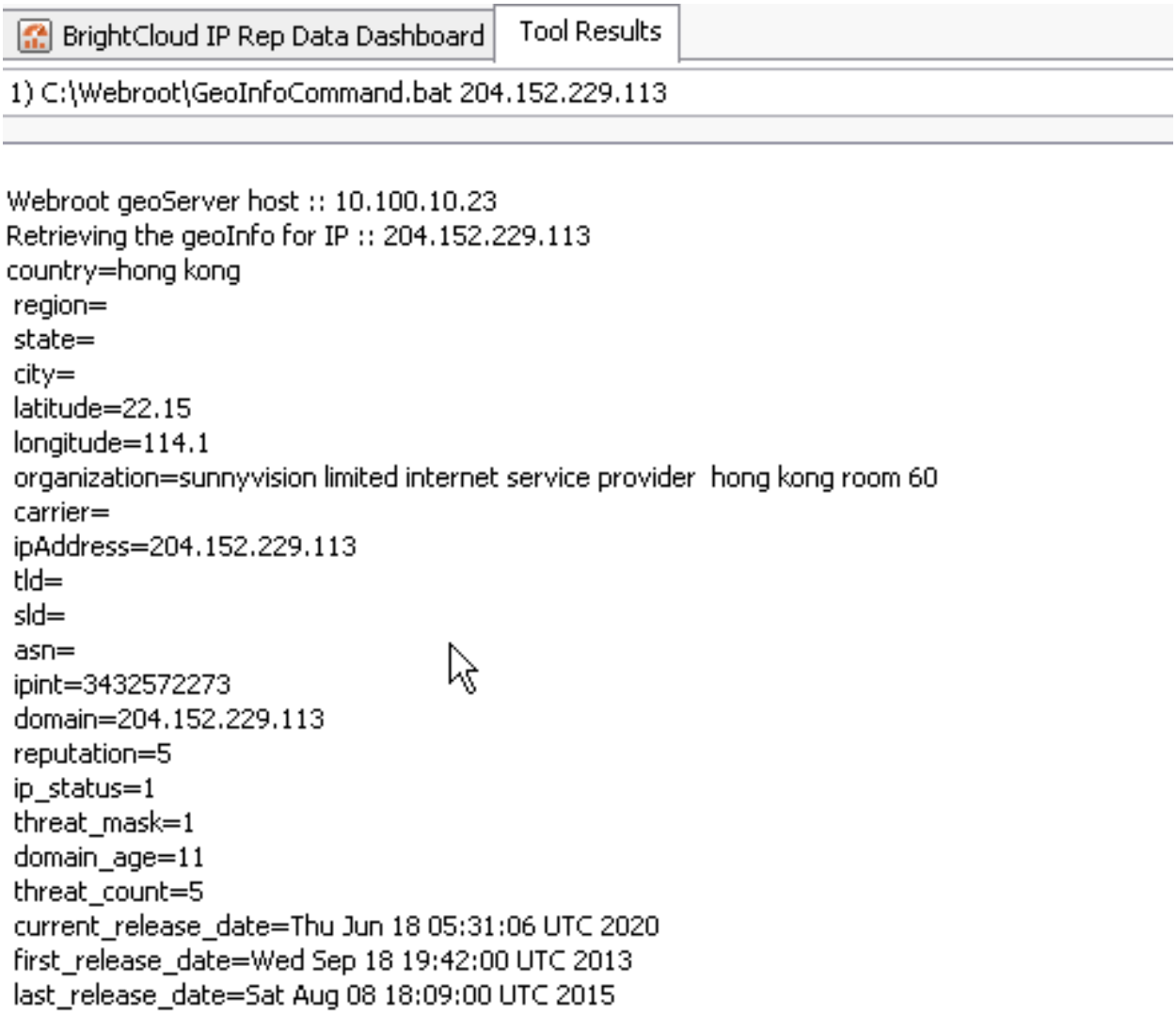




13. Right click on any IP address column in Dashboard and select **Integration Commands -> GeoInfoCommand**.



You will get the GeoInfo details in a separate tab in the Viewer panel as below screenshot.

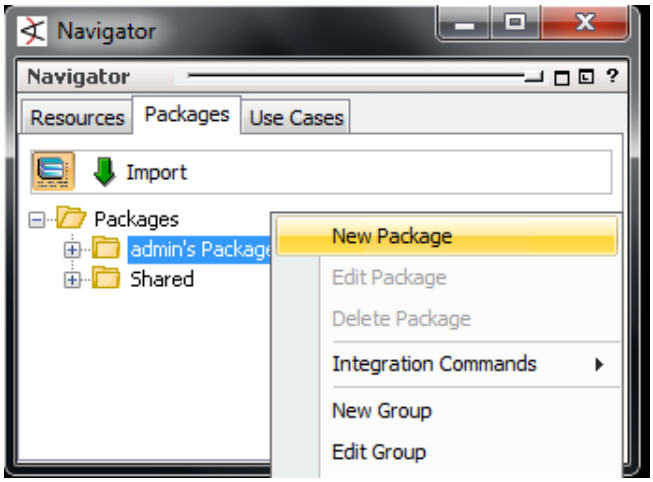


6.14 Package

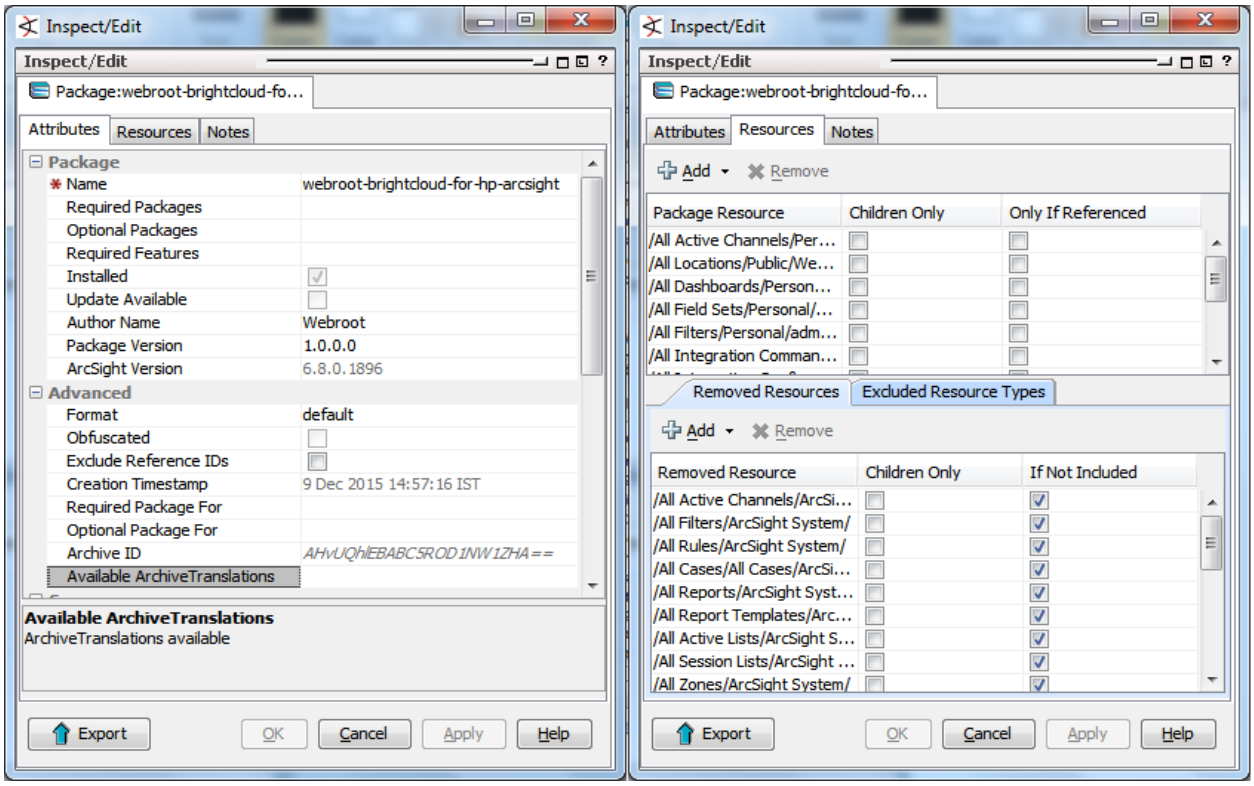
Packages are collections of resources that can be installed into the system resource tree.

To create a package:

1. From the Navigator panel, select **Packages**.
2. Right-click on **admin's Packages** and select **New Package**.



3. On the Inspect/Edit panel, provide below details in Attributes and Resources tabs below screenshots.



4. Click the **Resources** tab and below resources and choose below resources:

   - **Active channel**
   - **Assets -> Location**
   - **Dashboard -> Dashboard**
   - **Field Sets**
   - **Filters**
   - **Integration Commands -> Integration Commands**
   - **Integration Commands -> Integration Configurations**
   - **Lists -> Active Lists**
   - **Notifications**
   - **Query Viewer**
   - **Report -> Query**
   - **Rule**

5. After adding all the resources click the **Apply** button to save the details.

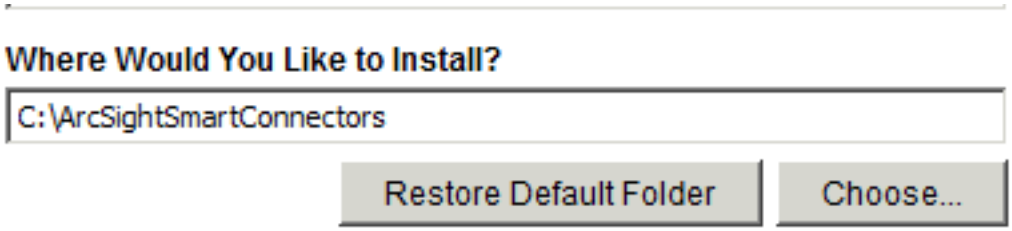
6. Right-click on the **package brightcloud-for-hp-arcsight** and select **Export Package to Bundle**.

7. Select the directory you want to save the package and click the **OK** button and then click the **Next** button to export the packages below screenshot.
8. Click the **OK** button to save export the package and verify the exported package in the selected directory as an **.arb** file.

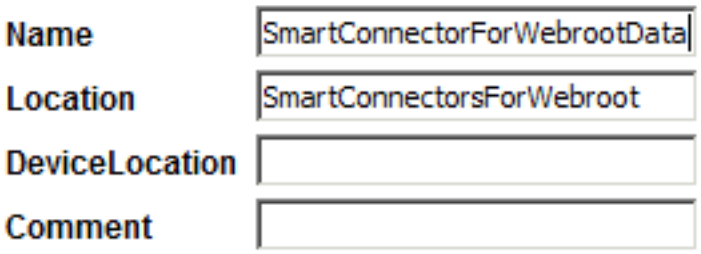
FAQs

Can we install the BrightCloud connector in the default location?

No. Change the location of connector as mentioned below. It shouldn't have space between folders, as shown.



Also, provide name and location fields left other fields empty, as shown.

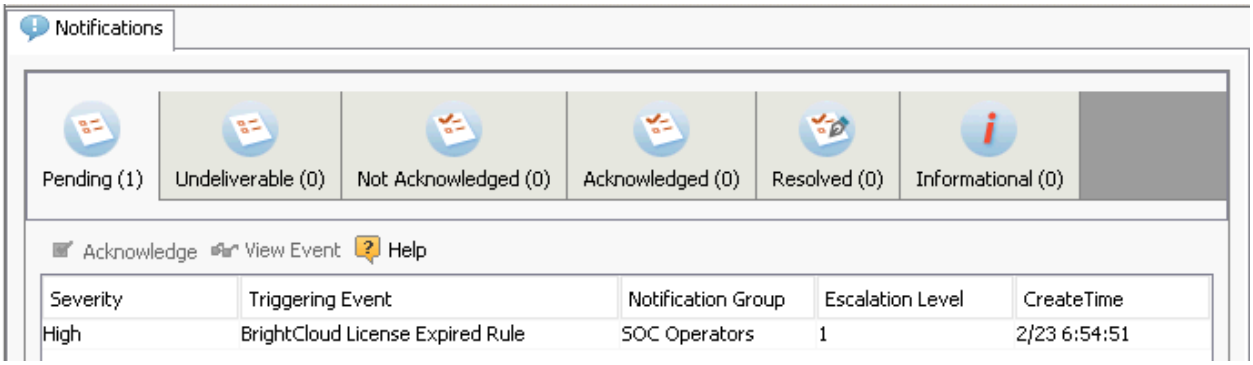


How do I process a License Expiry notification for BrightCloud connector?

Prepare the CEF as below for License Expiry for which you will Notification alert in Console as well as mail.

CEF:0|WEBROOT|BRIGHTCLOUD|1.0|wbr_bcti_licenseWarning|THREAT_INTELLIGENCE_LICENSE_WARNING|5|msg=Your license for Webroot BrightCloud Threat Intelligence for HPE ArcSight expires in 7 days. Please contact sales@webroot.com to obtain a valid license key.

CEF:0|WEBROOT|BRIGHTCLOUD|1.0|wbr_bcti_licenseExpired|THREAT_INTELLIGENCE_LICENSE_EXPIRED|8|msg=Your license for Webroot BrightCloud Threat Intelligence for HPE ArcSight has expired. Please contact sales@webroot.com to obtain a valid license key.



You will receive email with below subject line:

Your license for Webroot BrightCloud Threat Intelligence for HPE ArcSight expires soon. Please contact sales@webroot.com to active license.

What are the pre-requisites to install the BrightCloud connector in Windows/Linux OS?

Before installing the product check the java version installed is jre 1.6 and user should have the admin/root privileges. Check the proxy/internet connection is stable, as BrightCloud connector interacts with Webroot rest service to fetch the malicious IP data at regular intervals.

What are the pre-requisites to install the connector in Windows/Linux OS?

Before installing the smart connector check the java version installed is jre 1.6. Please have below details readily available

- Location name created in ESM console.
- ESM Manager host name
- Path to pick the data
- Type of malicious data file.
- ESM manager credentials

What are the pre-requisites to install the ESM console in Windows/Linux OS?

Before installing the ESM console check the java version installed is jre 1.6. Please have below details readily available

- ESM manager host name.
- ESM login credentials

What to do when data is not being populated in the active list?

Verify the Filters properly configured and make sure BrightCloud connector is running and generating the CEF events and Smart connector is running and listening the same location where CEF are generated.

What to do when the integration command does not fetch the geo info for an IP?

Check the internet connectivity, verify the java version installed with respect to the ESM console also verify whether the IP you are trying is a valid IP.

Troubleshooting

HPE ArcSight SmartConnector issues (Windows/linux):

Before installing the smart connector check the java version installed is jre 1.6. Please have the following details readily available:

- Location name created in ESM console
- ESM Manager host name
- Path to pick the data
- Type of malicious data file
- ESM manager credentials

I have installed HPE ArcSight SmartConnector successfully, but it is not starting

Check the following:

- Make sure there is no space used in the HPE ArcSight SmartConnector installation directory. For example, the default location *c:/Program Files/* has a space in the folder name, the SmartConnector won't run after the installation. Hence, use C:/Webroot/SmartConnector or any other drive with similar folder pattern.
- Run HPE ArcSight SmartConnector as standalone application instead of service. Copy the AgentID from log and input into ESM console's filter. Refer to 3.5 Saving agent id for ESM Console Setup.
- Select the same CEF generation path, which is given at the time of BrightCloud connector installation.

HPE ESM Console issues (Windows/Linux):

Before installing the ESM console check the java version installed is jre 1.6. Please have below details readily available:

- ESM manager host name

- ESM login credentials

ARB package is imported and SmartConnector is processing CEF, but nothing is displaying on the ESM console

Check the following:

- This may due to the AgentID mismatch. After installation of SmartConnector, copy its AgentID from the log and update the ESM console's BrightCloudConnector's filter as above. Once AgentID is updated, verify with GeoLocation integration command.
- Wrong batch file path. Change integration command batch (.bat) file location. Please refer to section 5.12 Integration Command.
- Host name should be where the ESM server is running.

Integration command does not fetch the geo info for an IP

Do the following:

- Check the Internet connectivity
- Verify the java version installed with respect to the ESM console
- Verify whether the IP you are trying is a valid IP

Not getting notification email

Change the email address under the SOC operators so that you will receive notifications through mail. Please refer to section 5.9 Notification.

BrightCloud connector issues (Windows/Linux):

Before installing the product check the java version installed is jre 1.6 or higher. All installations need the admin/root privileges. The proxy/internet connection is stable, as BrightCloud connector interacts with Webroot rest service to fetch the malicious IP data at regular intervals.

BrightCloud connector installation failed or not generating CEF files

Try the following:

- You don't have admin rights. Please run the installer as administrator in Windows; in Linux, use sudo. Same admin right is required for stop and start.
- Start/stop BrightCloud connector

  In Linux, BrightCloud connector is registered as service that can be started and stopped:

  $/>sudo service BrightCloudConnector stop

  $/>sudo service BrightCloudConnector start

In Windows, BrightCloud connector is registered as service that can be started and stopped:

You have run start/stop shortcuts on the start menu. Or in the installation location you can find service.bat to start, shutdown.bat to stop the services. You must run these as an administrator as well.

- Port is blocked.

  Port 7777 is needed for BrightCloud connector. Please make sure it is free.

Change the log level of the BrightCloud connector

Locate log4j2.xml in BrightCloud connector's installed directory, and change the log level. Restart (stop and start) the connector to reflect the changes.

Copyright Information

Contact Information

Phone	A list of phone numbers for Webroot BrightCloud Technical Support is available on the Webroot BrightCloud contacts page: www.brightcloud.com/about/contactus.php
Support Website	To request investigation into an IP Address reputation please visit: www.brightcloud.com/tools/change-request-ip-reputation.php