# Blue Coat ProxySG App For Splunk

June 15, 2015

# Overview

Splunk Enterprise 6 makes machine data accessible, usable and valuable to everyone. It's the easy, fast and secure way to analyze the massive streams of machine data generated by your IT systems and technology infrastructure—physical, virtual and in the cloud. Thousands of organizations around the globe use Splunk Enterprise to monitor their end-to-end infrastructures, avoid service degradation or outages and to gain real-time visibility and critical insights into customer experience, transactions and other key business metrics.

ProxySG appliances provide complete control over all your web traffic, delivering world-class threat protection. Robust features include user authentication, web filtering, data loss prevention, inspection, and visibility of SSL-encrypted traffic (including the ability to stream decrypted content to an external server with an Encrypted Tap license), content caching, bandwidth management, stream-splitting and more.

The Blue Coat ProxySG App has several dashboards to visualize the data from the ProxySG logs. The app also includes a pivot Search into Blue Coats Security Analytics to allow for rapid response to events requiring more context.

# Prerequisite

### Splunk Versions

- 6.2 or greater

### ProxySG

- 6.5 or greater

# Installation

## Getting the App

1. Download the app from the Blue Touch Online
2. Click the ‘Install App From File’ button
3. Navigate to the Technical Add-On for ProxySG ( TA_BlueCoatProxySGAppForSplunk-4.0.tgz) and upload the file
4. Navigate to the ProxySG App file downloaded ( BlueCoatProxySGAppForSplunk-4.0.tgz) and upload the file

## After initial install, follow these steps

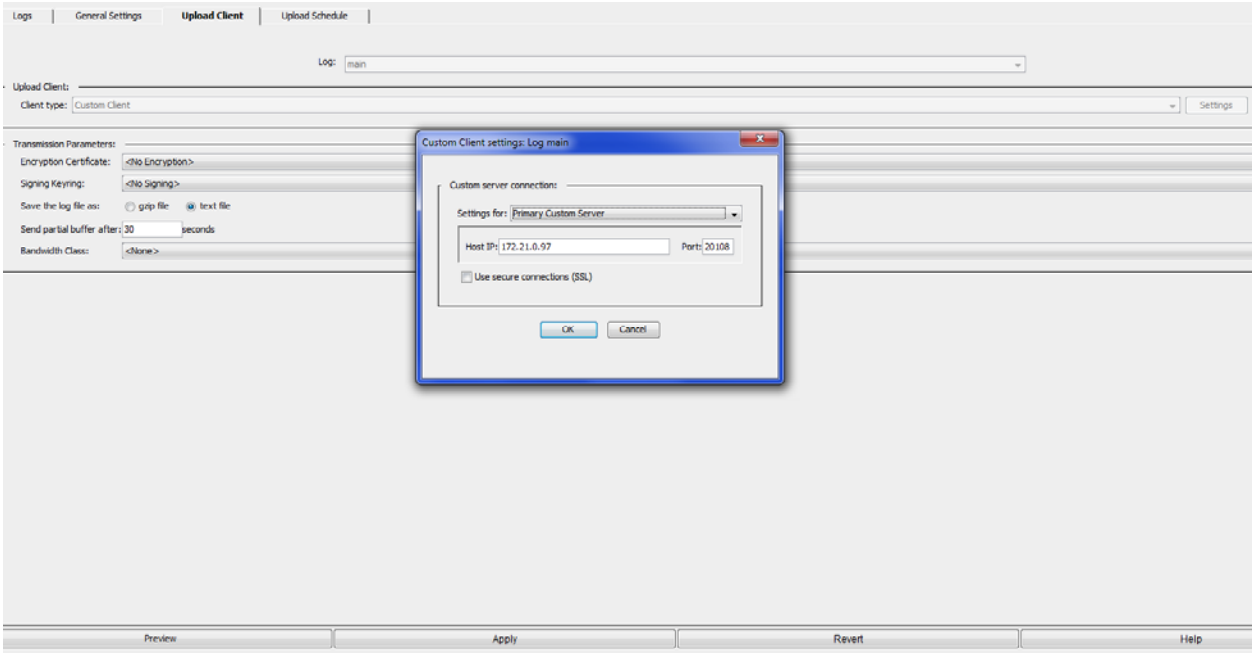
1. Restart Splunk
2. Log back in

## Setup

After initial installation the app is setup to receive input TCP events on port 20108. This port can be changed to another port of your choice and you would just need to use that same port when configuring the custom client logs from ProxySG.

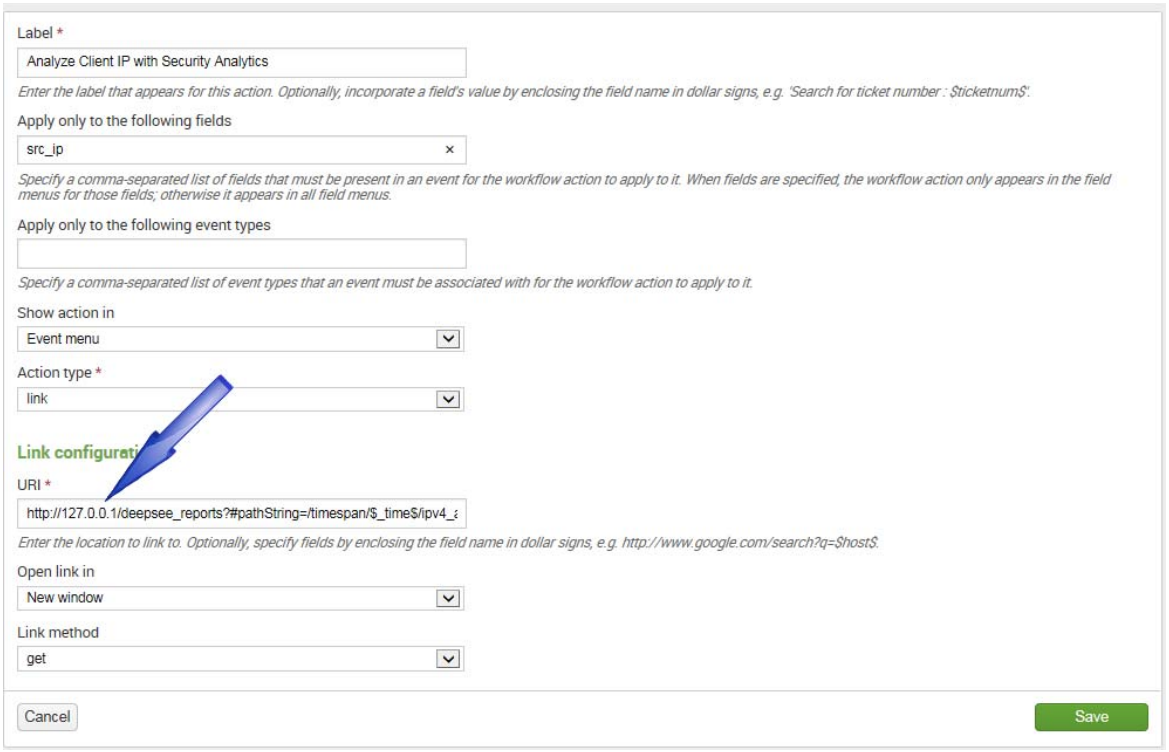
**[ProxySG]**

1. Log into the ProxySG UI
2. Navigate to Configuration->Access Logging
3. Select ‘Upload Client’
4. Choose ‘Custom Client’ from Client type
5. Click the setting button
6. Enter the IP Address for your Splunk system (the default port can be changed here if you changed it in Splunk as well)
7. Click OK to close the dialog box
8. Click Apply on the bottom for these setting to take affect




**[Splunk Pivot Search Setup]**

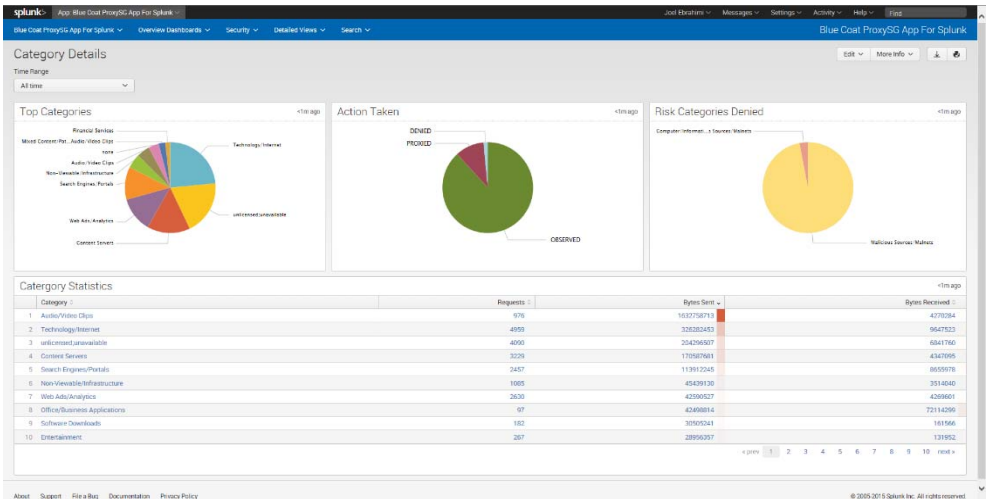
1. Log into the Splunk UI
2. Navigate to Fields->Workflow Action
3. Select App Context:Blue Coat Proxy SG App For Splunk
4. Click on SecurityAnalyticsInvestigate
5. Change the loopback IP address to the IP address or hostname of your ProxySG Appliance and click save



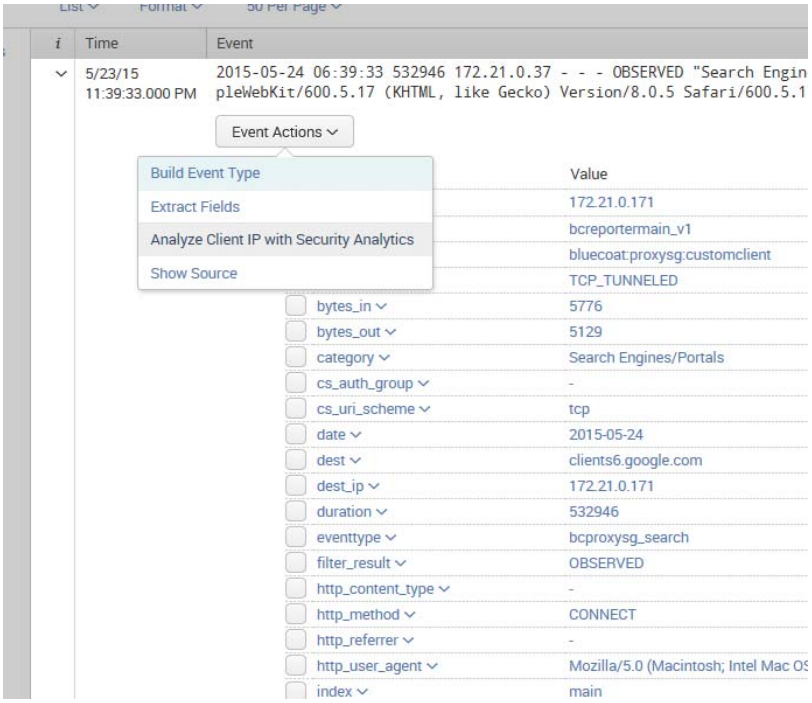
# Usage

### [Dashboards]

The ProxySG App for Splunk contains several dashboards preconfigured to display the data from Blue Coats ProxySG Appliance. The dashboards are left in edit mode to allow users to expand and create new panels to the existing dashboards. The dashboard show the data in views such as General Overviews, Bandwidth Statistics and Security Overviews.




### [Pivot Link on Search]




The app also includes a Search page. The Search page is similar to the standard Splunk search page but it adds the additional functionality of being able to extract samples of task values in the data entries. By click on Event Actions on a particular event from ProxySG you can launch directly into the specific task or sample to get more details around the event contained within Splunk.