# INTRODUCTION

Splunk is a generic data capture and reporting tool that can be used to analyze a variety of data, Blue Prism Version 6 has been specifically programmed an interface for Splunk such that it can be configured to consume Blue Prism’s session log data.

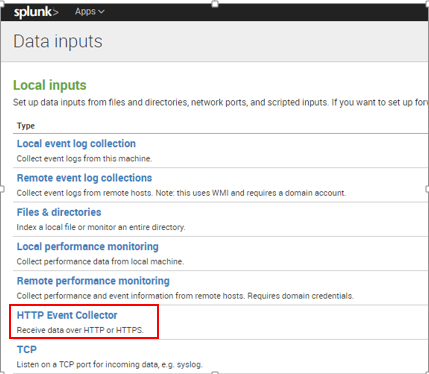
This document provides a walkthrough of the steps required to configure Splunk to consume Blue Prism’s session log information for reporting purposes.

# CONFIGURING SPLUNK

Start with installing splunk Enterprise, and login into splunk and configure the following settings to enable data capture for Blue Prism session log data.

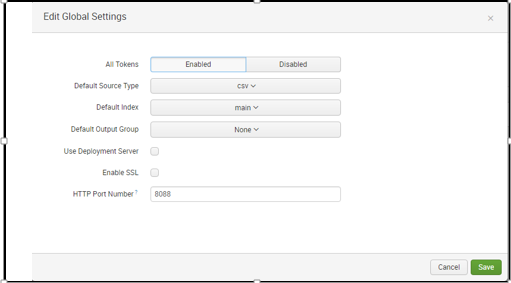
1. Navigate to HTTP Event Collector

* Go to Settings > Data Inputs
* Click HTTP Event Collector



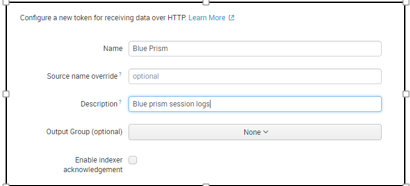
1. Enable HTTP Event Collection(HEC)

* Click on Global Settings, edit global settings and enable all the tokens.
* Save the changes.



1. Create a new token

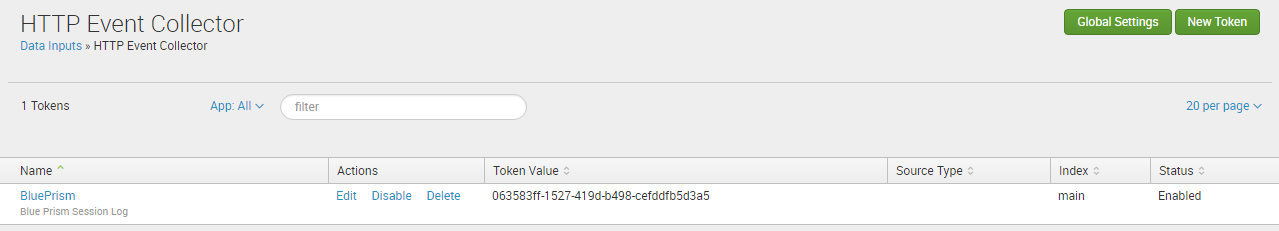
* Click New token.
* Complete the details as shown.
* Click Next at the top.





1. Generate a token value

* Record the Token Value string for use in the Blue Prism configuration file later in the process.



# CONFIGURING BLUE PRISM

For blue prism version 6.0, a configuration file called “splunk\_config.xml” is created in the %appdata% directory (e.g. C:\Users\<user>\AppData\Roaming).

The “splunk\_config.xml” configuration file is an XML file which has the following parameters in the format as shown-:



File Parameter Definitions

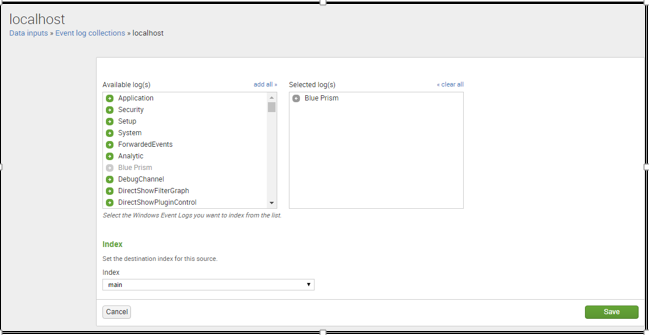
* + <host> : the machine where the data is being retrieved from (e.g. the machine hosting the Session Log data). This is usually the machine where the Blue Prism database resides.
  + <port> : the port number on the <host> machine. This is configured in Splunk and used to obtain the Blue Prism data.
  + <Secure> : the Enable SSL parameter in the Global Settings of Splunk.
  + <Token> : the Token Value of the HTTP Event Collector.
  + <Source> : the HTTP Event Collector Name.

Turn off the server service and restart the server service for the service to find and pick up the xml file.

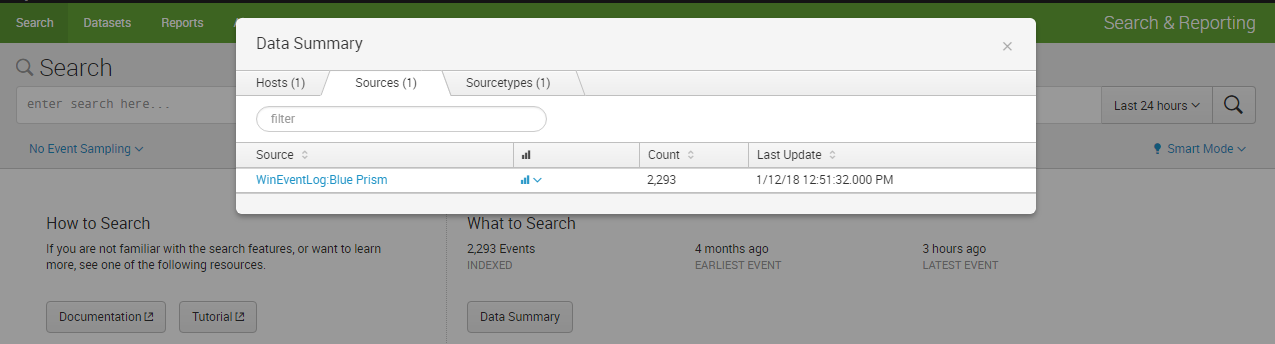
# EVENT LOG DATA

To add the Blue Prism Event Log for the monitoring of events logged by Blue Prism activities, we need to configure splunk for event log analysis.

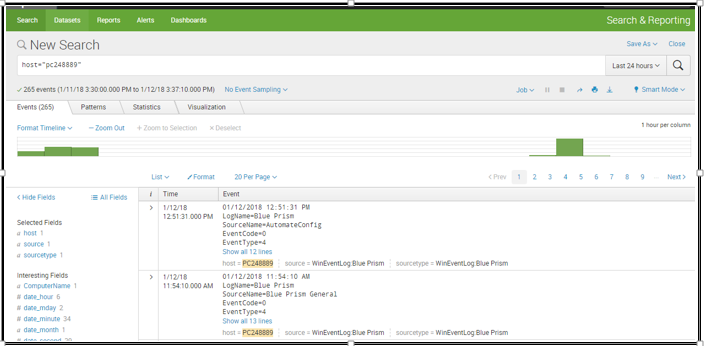
* Go to Setting > Data Inputs > Local event log collection.
* Brows Blue Prism event log, drag it to selected log.
* Save the configuration.



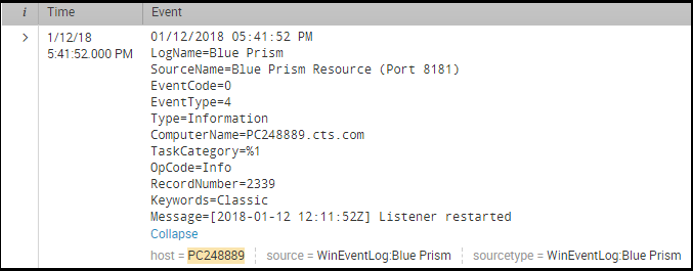
* In search and reporting section, choose WinEventLog:Blue Prism source.



* Report of Blue Prism event log appears like as shown.

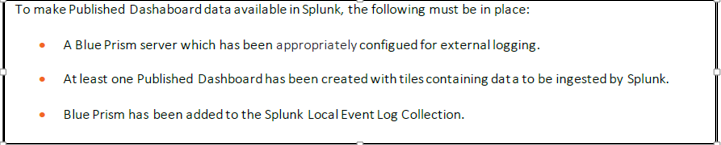


In the event logs generated in Splunk for blue prism processes, Stage level parameters information is not given.

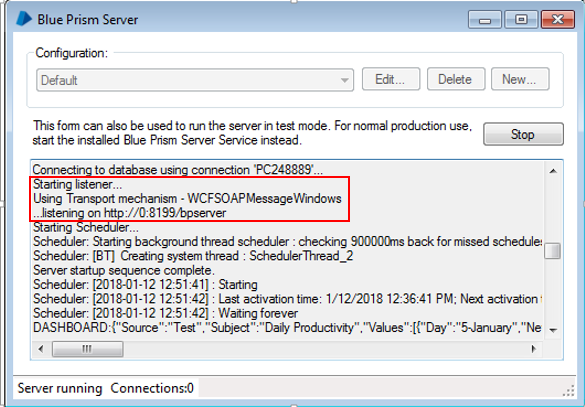


# PUBLISHED DASHBOARD

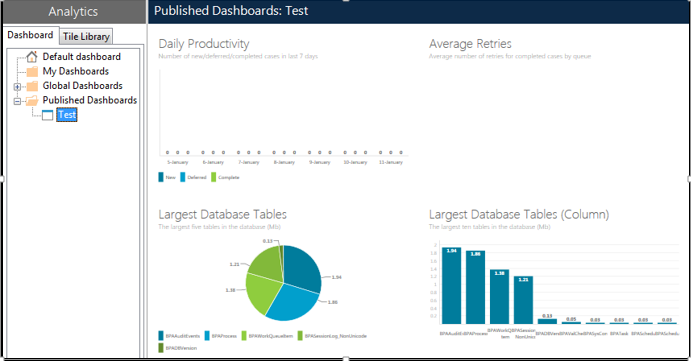
As mentioned in the BP 6.0 documentation reports-:



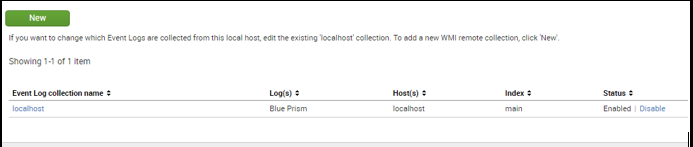
* Blue prism server is configured for external logging



* A published dashboard is created in Blue Prism.



* Blue Prism is added to local event log collection in splunk.



After configuring splunk for capturing the published dashboards, these dashboards cannot appear in Splunk dashboard section.