proofpoint

Proofpoint Threat Response™

Proofpoint SmartSearch Integration Guide

Proofpoint, Inc.

892 Ross Drive

Sunnyvale, CA 94089 United States

Tel +1 408 517 4710 | www.proofpoint.com

Printed in USA

Warranties and Disclaimers

Proofpoint, Inc. assumes no responsibility for errors or omissions in this publication or other documents which are referenced in or linked to this publication. This publication is provided "as is" without warranty of any kind and is subject to change without notice. Screen shot and illustrations may not represent the latest version of the software but are appropriate to explain the related text.

If you have any questions for our technical support staff, please contact us at either 877-64-POINT or at support.proofpoint.com.

Table of Contents

Chapter 1: Overview

Threat Response version 3.2 introduced the ability to ingest a CSV formatted report export from Proofpoint's Protection Server's Smart Search function. This report is ingested as an event source within the Threat Response platform and will create an individual event for each row that contains the proper data, recipient, messageID, etc. The process of uploading the report is currently manual however, as with all event sources within Threat Response, it is possible to create a Match Condition that can take automated actions.

This event source is available to Threat Response Auto Pull (TR-AP) licensed customers.

Chapter 2: Configuring the Smart Search Alert Source

This section will cover the steps for configuring a Smart Search alert source. It is important to note that only one instance of this alert source is able to be configured per Threat Response Instance.

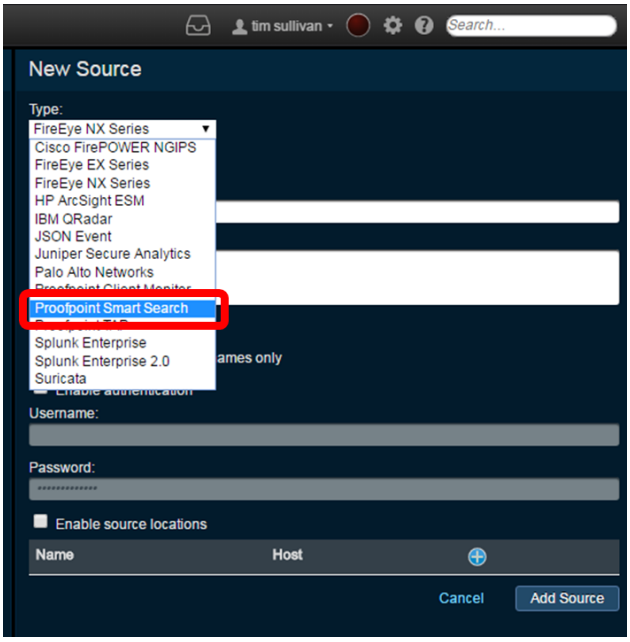
Navigate to the Alert Sources Configuration Page

1. Log into Threat Response with an administrator level account
2. Using the navigation drop down menu, navigate to the 'Sources' page

Create a New Smart Search Alert Source

1. Click the plus symbol to the right of Sources to add a new source:

2. In the right hand pane select "Proofpoint Smart Search" from the drop down menu under 'Type'



3. Within the 'New Source' window configure the following:

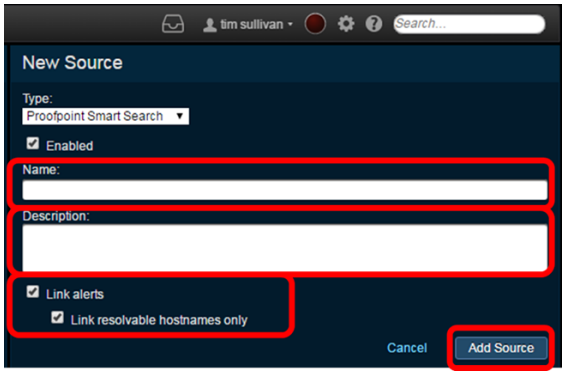
   'Enabled' checkbox: Clearing the checkbox will disable the event source while selecting the box will enable it.

   Name (Required Field): Provide a name for the event source. This is an internal name only and can be whatever is most helpful to the administrator or operators.

   Description (Optional Field): Provide any desired description of the event source

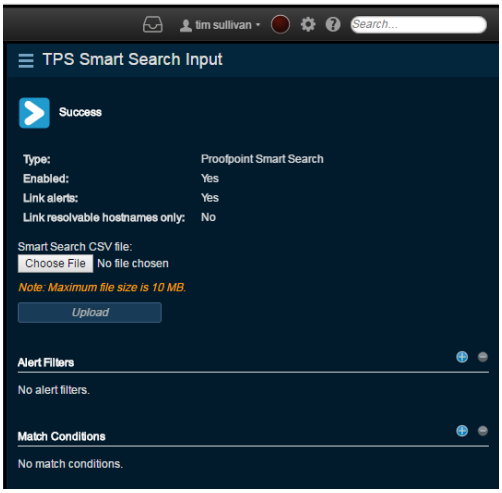
   'Link Alerts' checkbox: Clearing the checkbox will result in an individual incident being created per alert (1 to 1). Selecting the checkbox will leverage Threat Responses linking logic to group similar alerts into relatable incidents.

   'Link resolvable hostnames only' checkbox: Clearing this checkbox will group alerts into relatable incidents regardless of if the hostnames are able to be resolved. Selecting this checkbox will only associate alerts with resolvable hostnames with relatable incident, none resolvable hostname will result in a new incident being created.



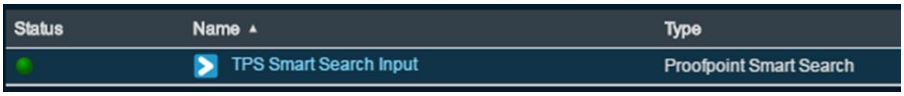
4. Once the proper information has been configured select 'Add Source' in the lower right corner.

5. Validate that the desired configuration has been saved to the new source

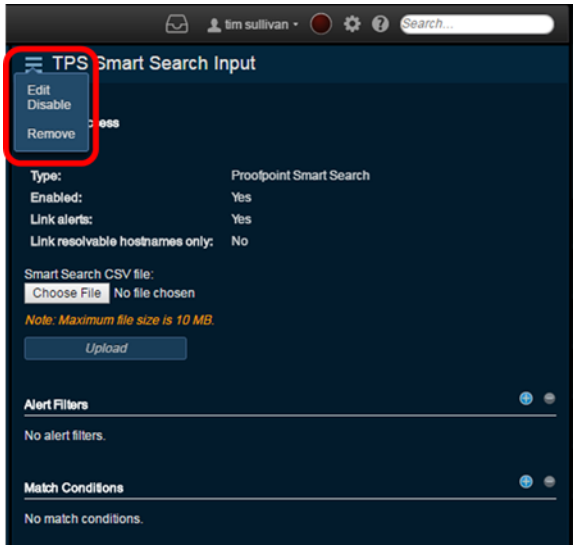


Edit/Disable/Remove the Smart Search Alert Source

1. From within the 'Sources' page select the Proofpoint Smart Search type alert source that needs to be edited/disabled/removed



2. In the right hand pane select the 3 horizontal lines next the alert source name.



Edit: Enables configuration changes within the current alert source

Disable/Enable: This selection will change depending on the current state of the alert source. If the source is currently enabled then 'Disable' will be shown and if the alert source is currently disabled then 'Enable' will be shown.

Remove: Removes the alert source
**Note removing an alert source does not remove the received alerts

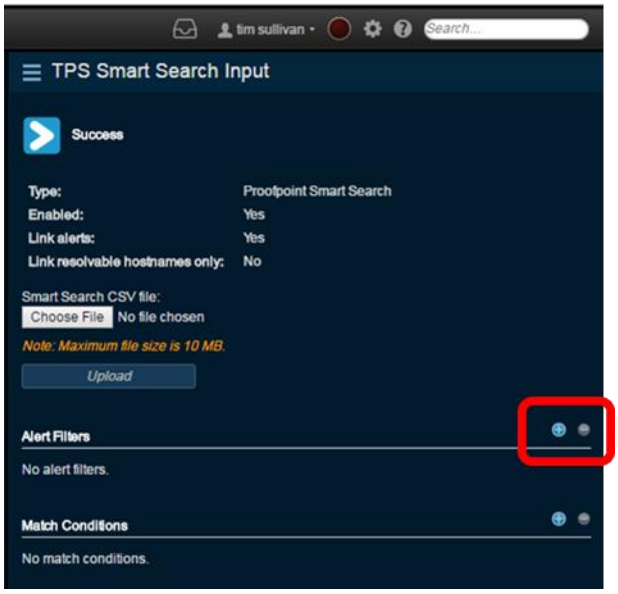
Chapter 3: Configuring Alert Filters and Match Conditions

This section will cover the steps for creating, modifying and removing Alert Filters and Match Conditions

Creating Alert Filters

An Alert Filter can be configured so that certain types of alerts will not be ingest by the associated alert source.

1. To create a new Alert Filter select the 'plus' symbol to the right of 'Alert Filters'



2. Within the 'New Alert Filter' configure the following:

   2.1. ***Name (Required Field):*** Provide a name for the event source. This is an internal name only and can be whatever is most helpful to the administrator or operators.

   2.2. ***Description (Optional Field):*** Provide any desired description of the event source

   2.3. ***For alerts of type:***

   Categories (Required Field): Enter the proper category.

   ****NOTE**** The Smart Search Alert source for Threat Response 3.2.x does not have any individual categories that are able to be matched. Therefore a wildcard asterisk '*' must be used. Ensure to add additional context as this setting by itself will filter **ALL** alerts.

   Threat Name (optional): The specific threat name to be filtered

Threat description (optional): The specific threat description to be filtered

Alert Result (optional): Not applicable in this alert source

If hosts with type (optional): Select the host type to be specified in the dropdown menu

Target: The host/IP address (es) that are indicated as the target of the attack

Attacker: The host/IP address(es) are indicated as the source of the attack

Callback: The host/IP address(es) that suspected malware is seen attempting to contact

Forensics: The host/IP address(es) that are seen within a sandbox detonation that do not fall into the previous categories.

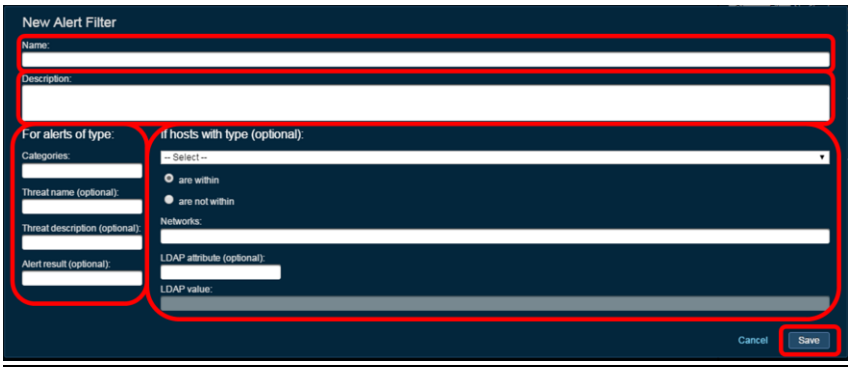
Are within | are not within: Radio button selections to specify if the hosts type selected is of is not within certain networks or IP ranges

Networks: Use to specify the network information for the previous step. It is required when 'If hosts with type' has been selected.

LDAP Attribute (optional): Provides a dropdown list/text box to enter in an LDAP attribute. In order for the alert to filter on an LDAP attribute Threat Response must be configured to retrieve that attribute. To configure this collection please refer to the admin guide. The dropdown list will only populate with attributes collected.

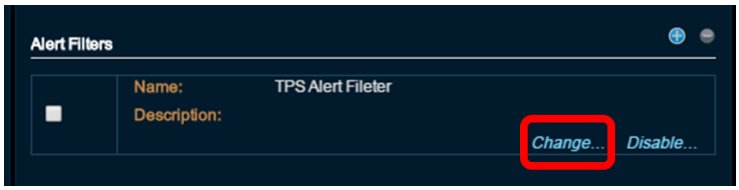
LDAP value: This test field is grey out unless the LDAP attribute field is configured. It is required to be populated when active.

Save: review the settings and select save to apply filter.



Changing Alert Filters

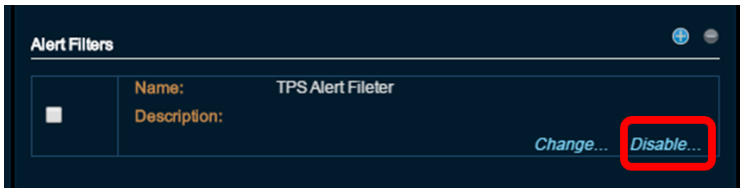
1. Select the appropriate Alert Source
2. In the right hand pane identify the Alert Filter to change
3. Click 'Change' in the bottom right corner of the Alert Filter



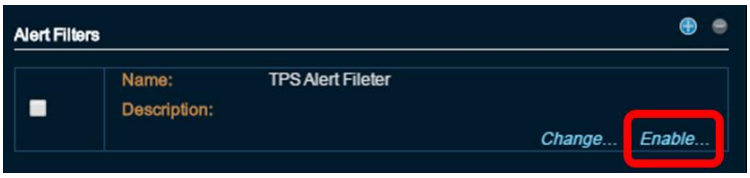
4. Make appropriate adjustments and save the Alert Filter. Reference "Creating Alert Filters" in this document for specifics about each configurable setting.

Disabling Alert Filters

1. Select the appropriate Alert Source
2. In the right hand pane identify the Alert Filter to disable
3. Click 'Disable…' in the bottom right corner of the Alert Filter

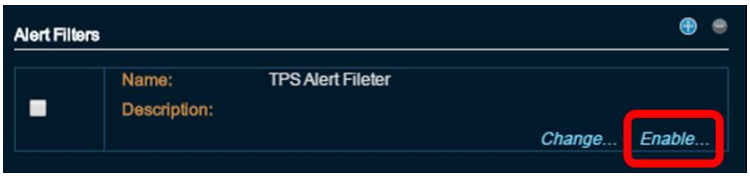


4. The selection in the bottom right corner should change to ‘Enable’

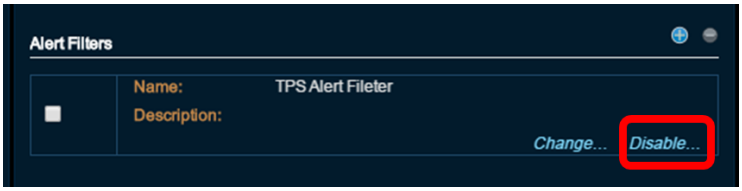


Enabling Alert Filters

1. Select the appropriate Alert Source
2. In the right hand pane identify the Alert Filter to enable
3. Click ‘Enable…’ in the bottom right corner of the Alert Filter



4. The selection in the bottom right corner should change to ‘Disable’



Removing Alert Filters

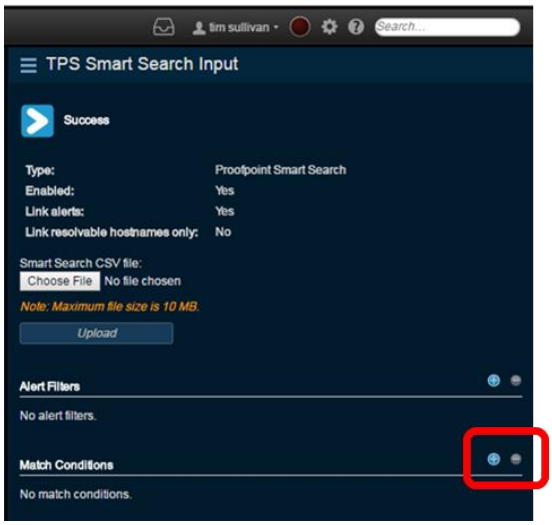
1. Select the appropriate Alert Source
2. In the right hand pane identify the Alert Filter to remove
3. Click checkbox to the left of the Alert Filter to remove
4. Click the red circle indicator that become active opposite the ‘Alert Filters’ heading

NOTE: There is no warning given to verify and there is no way to undo this action.

Creating Match Conditions

A Match Condition is a configuration that allows Threat Response to take automated action based on certain criteria found in the reviewed alert.

1. To create a new Match Condition select the 'plus' symbol to the right of 'Match Condition'



2. Within the 'New Match Condition' configure the following:

   Name (Required Field): Provide a name for the event source. This is an internal name only and can be whatever is most helpful to the administrator or operators.

   Description (Optional Field): Provide any desired description of the event source

   For alerts of type: (Not Used) Used to specify the type of alert to match. Not used for this alert source type

   Categories (Required Field): Enter the proper category.

      ****NOTE**** The asterisk '*' is a wildcard and matches everything. If more granularity is desired include additional selections.

   Threat Name (optional): The specific threat name to be matched

   Threat description (optional): The specific threat description to be matched

   Alert Result (optional): Not applicable in this alert source

If hosts with type (optional): Select the host type to be specified in the dropdown menu

Target: The host/IP address(es) that are indicated as the target of the attack

Attacker: The host/IP address(es) are indicated as the source of the attack

Callback: The host/IP address(es) that suspected malware is seen attempting to contact

Forensics: The host/IP address(es) that are seen within a sandbox detonation that do not fall into the previous categories.

Are within | are not within: Radio button selections to specify if the hosts type select in step 2.4 are or are not within certain networks or ranges to be specified in 2.13

Networks: Indicate the network information for use with step 2.5. It is required when 'If hosts with type' has been selected.

LDAP Attribute (optional): Provides a dropdown list/text box to enter in an LDAP attribute. In order for the alert to match on an LDAP attribute Threat Response must be configured to retrieve that attribute. To configure this collection please refer to the admin guide. The dropdown list will only populate with attributes collected.

LDAP value: This test field is grey out unless the LDAP attribute field is configured. It is required to be populated when active.

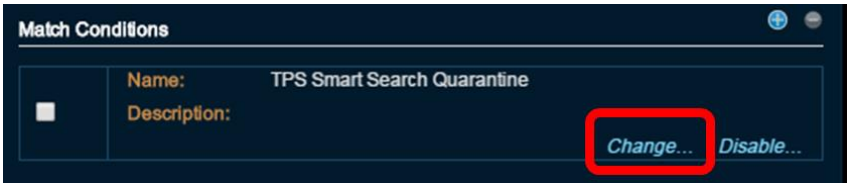
Suppress incident creation: A checkbox that can be select so that the match condition will take the appropriate action but **will not** create an incident for the alerts that have been matched nor retain the alert information.

Responses (Required Field): The response action to take when the match condition criteria is met. The available responses are dynamic and will only appear if certain configurations have been made. For example if no lists have been configured then the options 'Add to host list', 'Add to URL list', 'Add to file list' and 'Add to user list' will not be available.

Save: After reviewing the settings, select save to save and apply the filter.

Changing Match Conditions

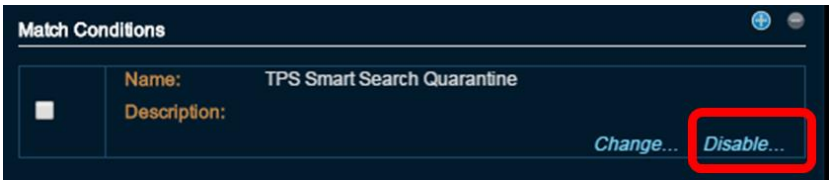
1. Select the appropriate Alert Source
2. In the right hand pane identify the Match Condition to change
3. Click 'Change' in the bottom right corner of the Match Condition



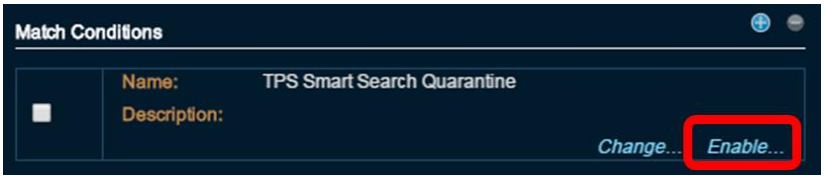
4. Make appropriate adjustments and save the Match Condition. Reference "Creating Match Conditions" in this document for specifics about each configurable setting.

Disabling Match Conditions

1. Select the appropriate Alert Source
2. In the right hand pane identify the Match Condition to disable
3. Click 'Disable' in the bottom right corner of the Match Condition

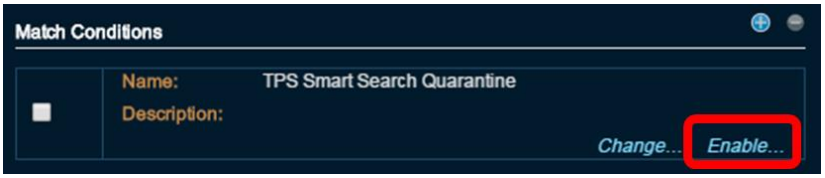


4. The selection in the bottom right corner should change to 'Enable'

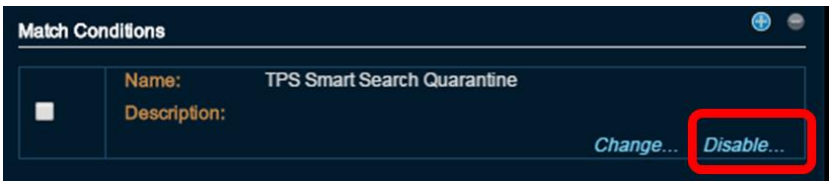


Enable Match Conditions

1. Select the appropriate Alert Source
2. In the right hand pane identify the Match Condition to enable
3. Click 'Enable' in the bottom right corner of the Match Condition

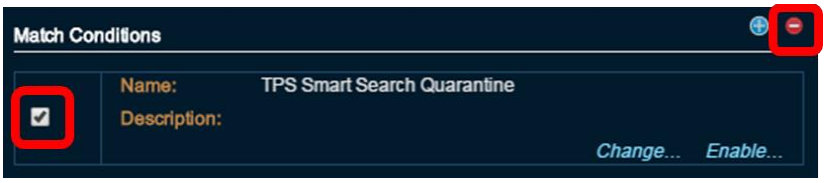


4. The selection in the bottom right corner should change to 'Disable'



Remove Match Conditions

1. Select the appropriate Alert Source
2. In the right hand pane identify the Match Condition to remove
3. Click checkbox to the left of the Match Condition to remove
4. Click the red circle indicator that becomes active opposite the 'Match Condition' heading



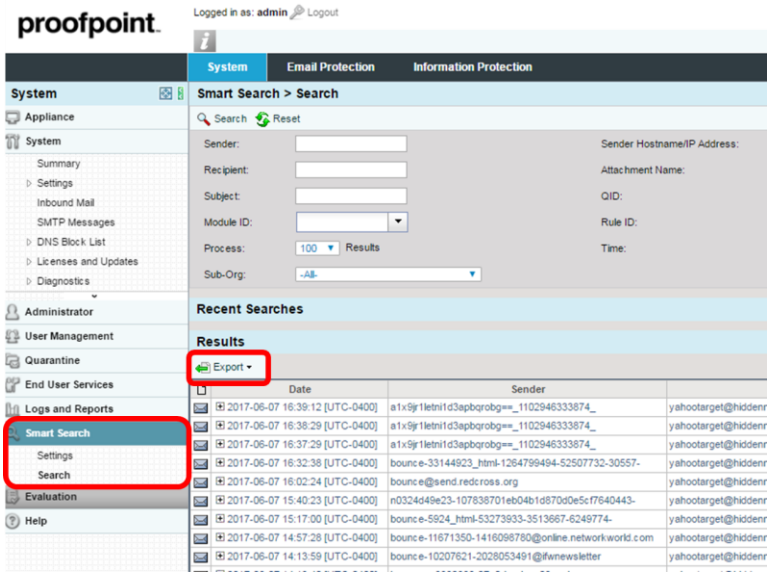
NOTE: There is no warning given to verify and there is no way to undo this action.

Chapter 4: Retrieving and Uploading a Smart Search Report

This section will cover the steps for retrieving a Smart Search CSV from a PPS server and uploading it.

Retrieving the Smart Search PPS report

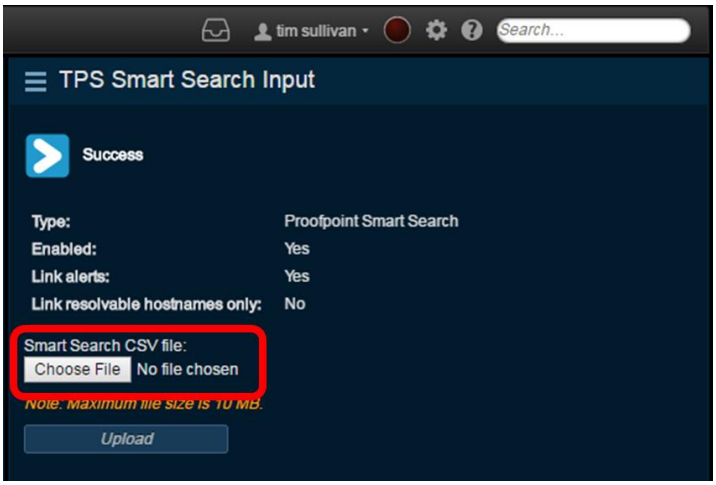
1. Access the Proofpoint Protection Server and run the appropriate Smart Search
2. Once the appropriate search results are retrieved select 'Export' for download the CSV file. Ensure to note the download location of the file.



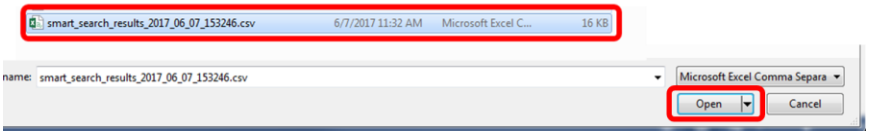
Uploading the Smart Search Report to Threat Response

1. Navigate to the 'Sources' page
2. Select the appropriate 'Smart Search' alert source
3. Ensure that the alert source is enabled
   Optional: Ensure that any match conditions are properly configured and enabled prior to continuing to take automated action.

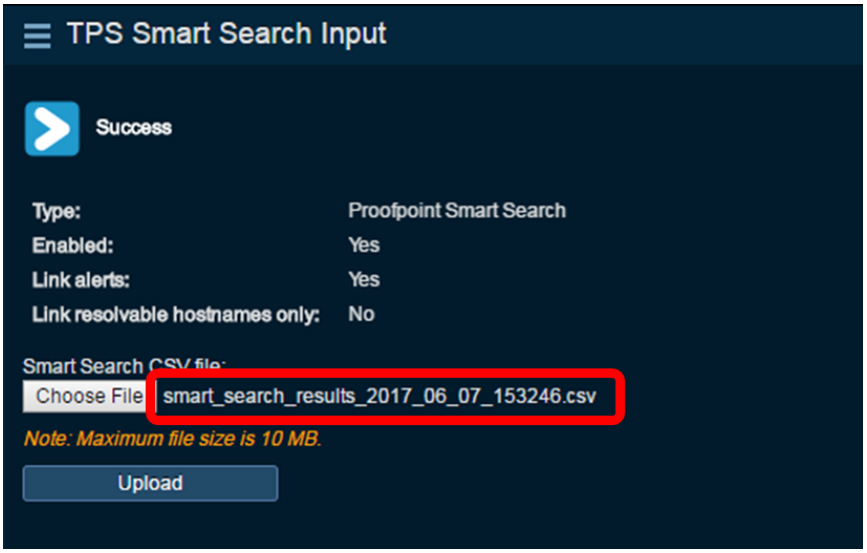
4. Under ‘Smart Search CSV File’ click ‘Choose File’ to locate the CSV export



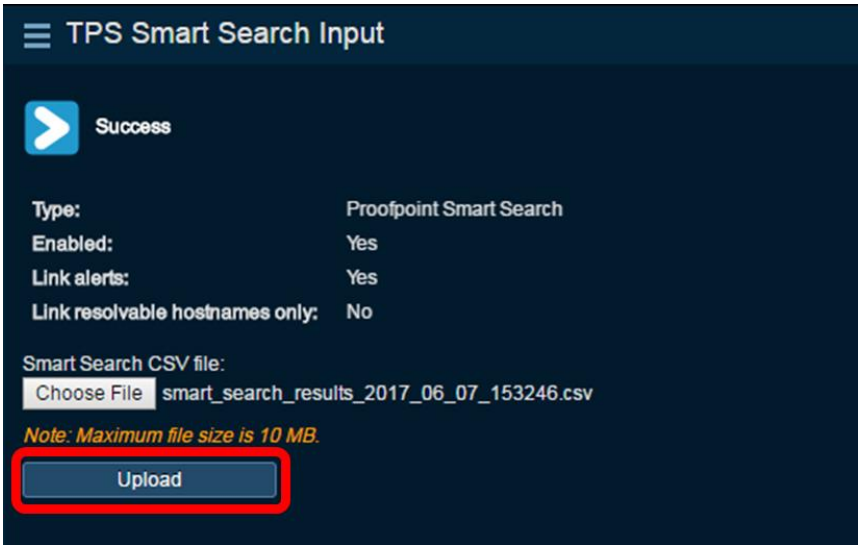
5. Select the appropriate file and click ‘Open’



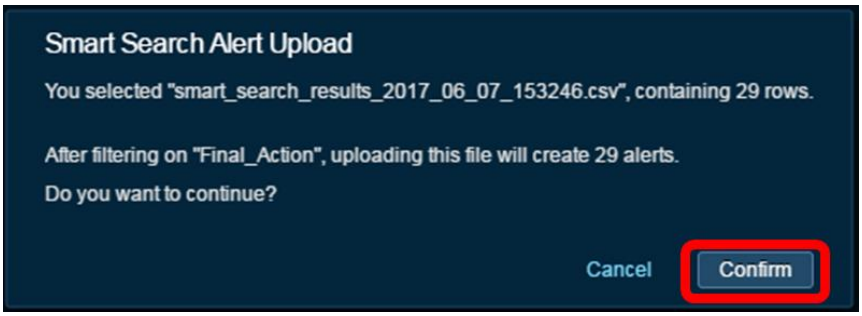
6. Ensure that the correct file name is displayed next to the ‘Choose File’ button



7. Select 'Upload' to upload the alerts into Threat Response



8. A popup window will appear detailing the number of rows that the report contains as well as the number of alerts that will be created after filtering on "Final_Action". Validate the information and click Confirm.



9. The report will now be converted to alerts within Threat Response.