SentryWire
PACKET CAPTURE PLATFORM

FEDERATION MANAGER UI

USER GUIDE

Software Version: 7.3.0.309-408.14

Document version 1.7

12/10/2021

Document Revision History

Ver 1.0	Initial Release (#408.14)	05/31/2021
Ver 1.1	Added LDAP Map User details	06/05/2021
Ver 1.2	Merged Investigator View Guide with Administrator View Guide	06/19/2021
Ver 1.3	Removed static network access setup description.	07/17/2021
Ver 1.4	Updates to Expand IPv6, Map User, Search Library, BPF Help	09/10/2021
Ver 1.5	File Carving, System Health	10/20/2021
Ver 1.6	Support for multiple log receivers	11/10/2021
Ver 1.7	Added Appendix E, F, & G	12/10/2021

Contents

INTRODUCTION

Federation Manager (FM) allows seamless access to services from one domain to another irrespective to the physical location of the capture server. The Federation Manager (FM) allows the user to manage several groups having multiple Federated Nodes (also referred to in this guide as FNs or nodes), and actively monitor and perform packet analysis on each one of them, from a central interface. Each Federated Node is a capture and analytics server responsible for capturing, storing and indexing of all received traffic and analytics data.

The FN software captures all data/traffic traversing the network full duplex via Test Access Port (TAP) or SPAN ports and operates in passive mode. FN Software does concurrently capture inbound and outbound PCAP in standard libcap format for all traffic traversing the Internet Access Point (IAP), to include IPv6.Since each group in FM can have multiple Federated Nodes, any actions performed on a selected group applies to all nodes that are configured within the group.

Along with a central management, the administrators can actively monitor, execute, and view searches and track packet capture statistics across all connected Federated Nodes within the selected group. This provides increased scalability and allows the administrators to also detect and prioritize security threats, pinpoint performance issues and manage incident responses – all from a single control center.

The FM further allows the administrator to drill down into event details, perform root cause analysis and troubleshooting for all controlled federated nodes.

Before using this application, some basic initial configuration is required. Please refer to the Quick Start Guide for details.

1.1 SUPPORTED WEB BROWSERS

- Google Chrome 44.0.2403.157 or above. (Preferred browser)
- Mozilla Firefox version 45.0.1 - 47.0.1 (Refer to Firefox Certificate Exception in **Appendix E**)

1.2 SETTING UP YOUR NETWORK

To ensure this application is accessible via web, an IP address must be assigned to one of the Ethernet ports before installing this application. The install process will confirm if the Management IP address is accurate. Please refer to RHEL 7/CentOS 7 network setup process to ensure the IP Address is set correctly.

SSH Access: After setting up an IP address locally, you can perform future operating system administrative functions by remote login via an SSH client. Configure your SSH client to connect using port 22.

1.3 UI USERNAME/PASSWORD

- Username must be minimum of 8 characters and maximum of 32 characters.
- Password has the following restrictions:
  - Must be minimum of 8 characters and maximum of 32 characters.
  - Must have at least 1 uppercase character, 1 lowercase character, 1 special character
    - Allowed special characters for password:

      !@#&*$
  - Spaces, % ,^, Backslash “\” or Forward slash “/”is not allowed.

- $ is not allowed in the beginning.

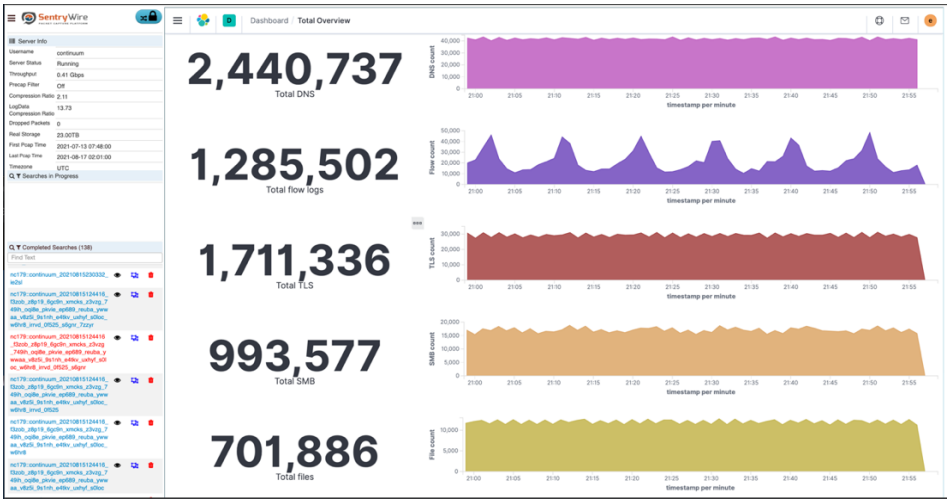
1.4 LOGGING IN TO THE APPLICATION

On any remote system connected to the network, open a supported web browser, and enter the IP address (not FM server's hostname) and port number 41395 over https. For Example: https://<IP Address>:41395
Login username and password will be provided directly to the customer.

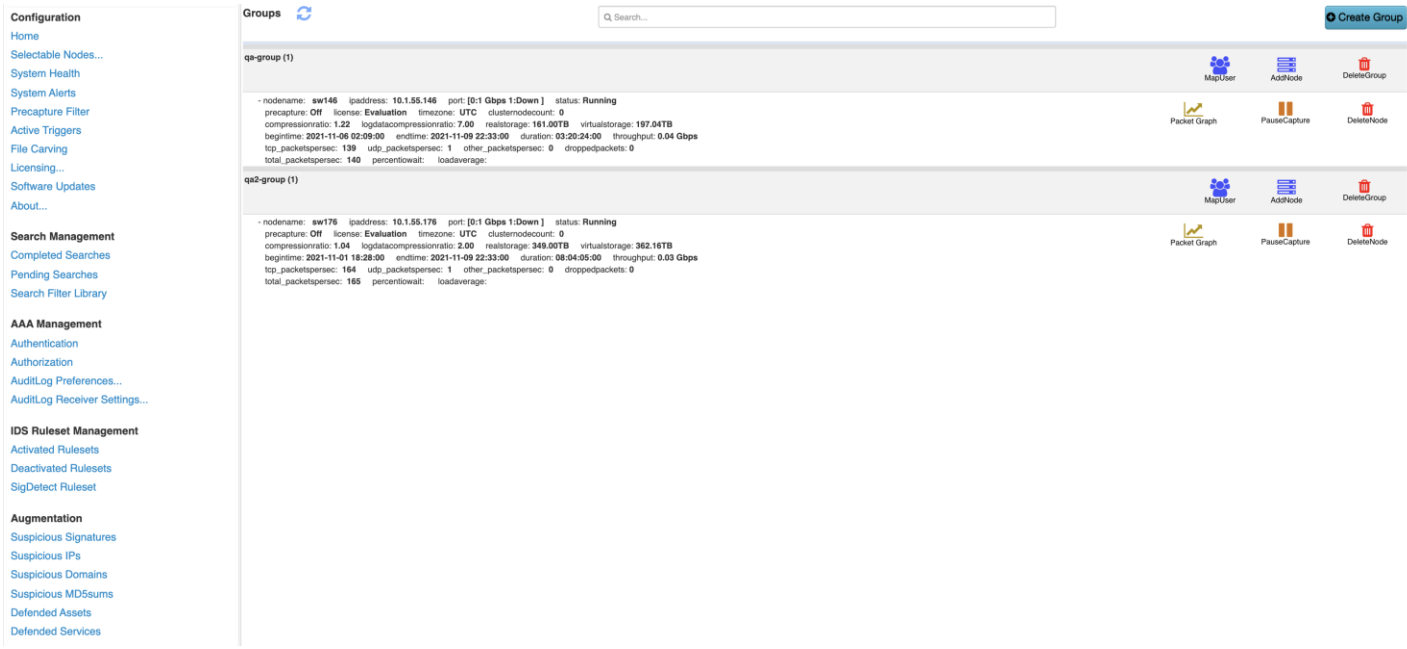
FEDERATION MANAGER UI

Federation Manager UI has two views – Users can switch between these two views by clicking on the button to the right of the company Logo:

1. Investigator View – primarily used by Analysts to view and analyze data via Kibana/Elastic, create searches and active triggers, IDS alerts, DPI events and PCAP data.



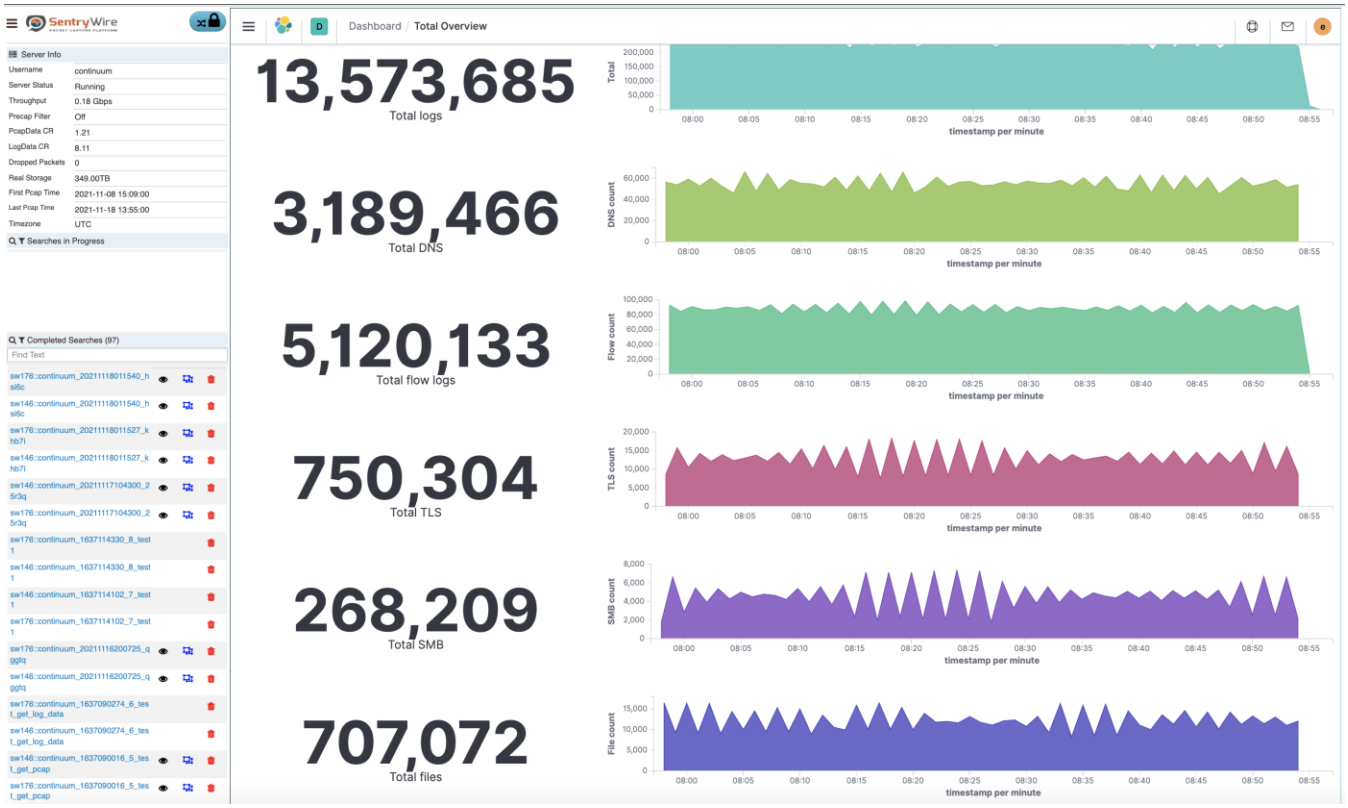
2. Administrator View - primarily used by UI administrators to setup, upload, or generally manage federation nodes.



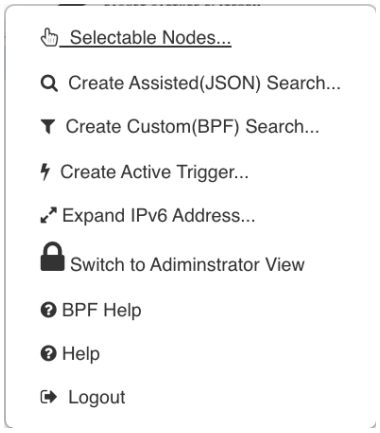
2 INVESTIGATOR VIEW

The capture and analytics platform has multiple ways for users to sync L7 metadata with its L4-L7 metadata, flexibility is at the core of the platform's capabilities. Additionally, the capture platform produces metadata in JSON format for L4 and L7 network flows with Community ID Flow Hashing allowing external monitoring systems to link L7 flow records with metadata more easily. Users are able to pivot with L7 metadata from other systems to FM and execute searches on the system using L4 or L7 metadata attributes on the local unit or via Federation Manager. **rsync** can be leveraged to pull data in from external systems and allow this metadata to be indexed via the capture software and searched against, the original timestamps are maintained during this process. REST API provides the ability to use an external tool's L7 data with timestamps to search against L4 metadata and packet attributes stored on the capture server.

Appendix D provides brief overview of the relevant portions of Kibana usage process.
The left panel shows drop-down menu to the left of the logo, and three different sections: Server Info, Searches in Progress, and Completed Searches. LogData CR, PcapData CR show logdata compression ratio and pcap data compression ratio respectively. The right panel shows Kibana UI.

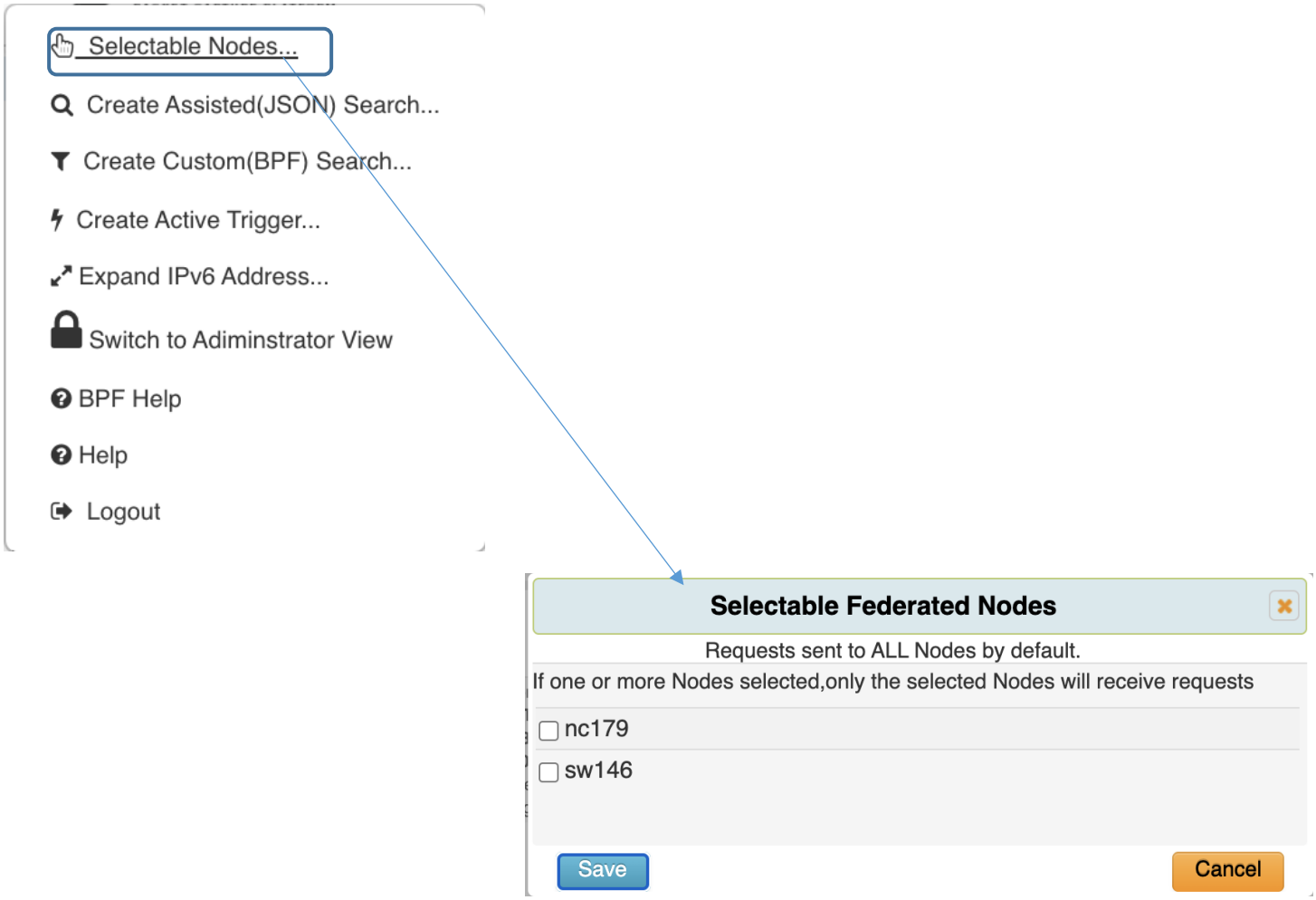


The Investigator drop down menu (☰) to the left the product logo is shown below:



2.1.1 Selectable Nodes

Each FM UI request goes to all connected federation nodes by default. This menu option allows users to restrict which federation nodes receive requests.

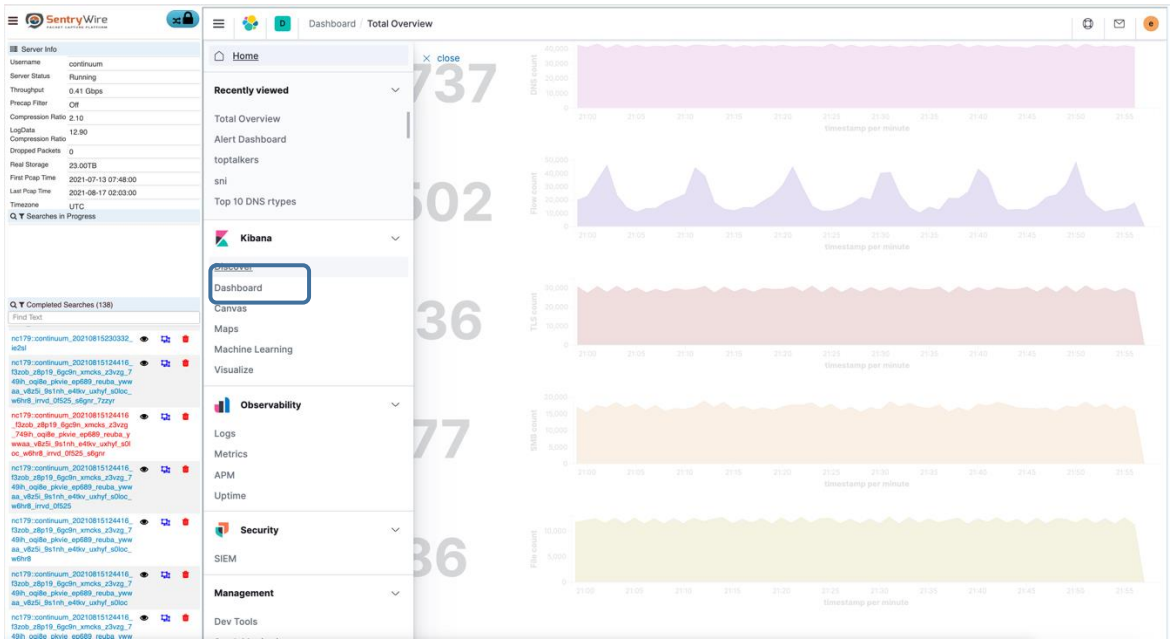


Users with Supervisor role are shown names of all the federated nodes. Other users are shown only the federated nodes from the groups they are allowed to view. The selected node list is effective until a new selection is made.

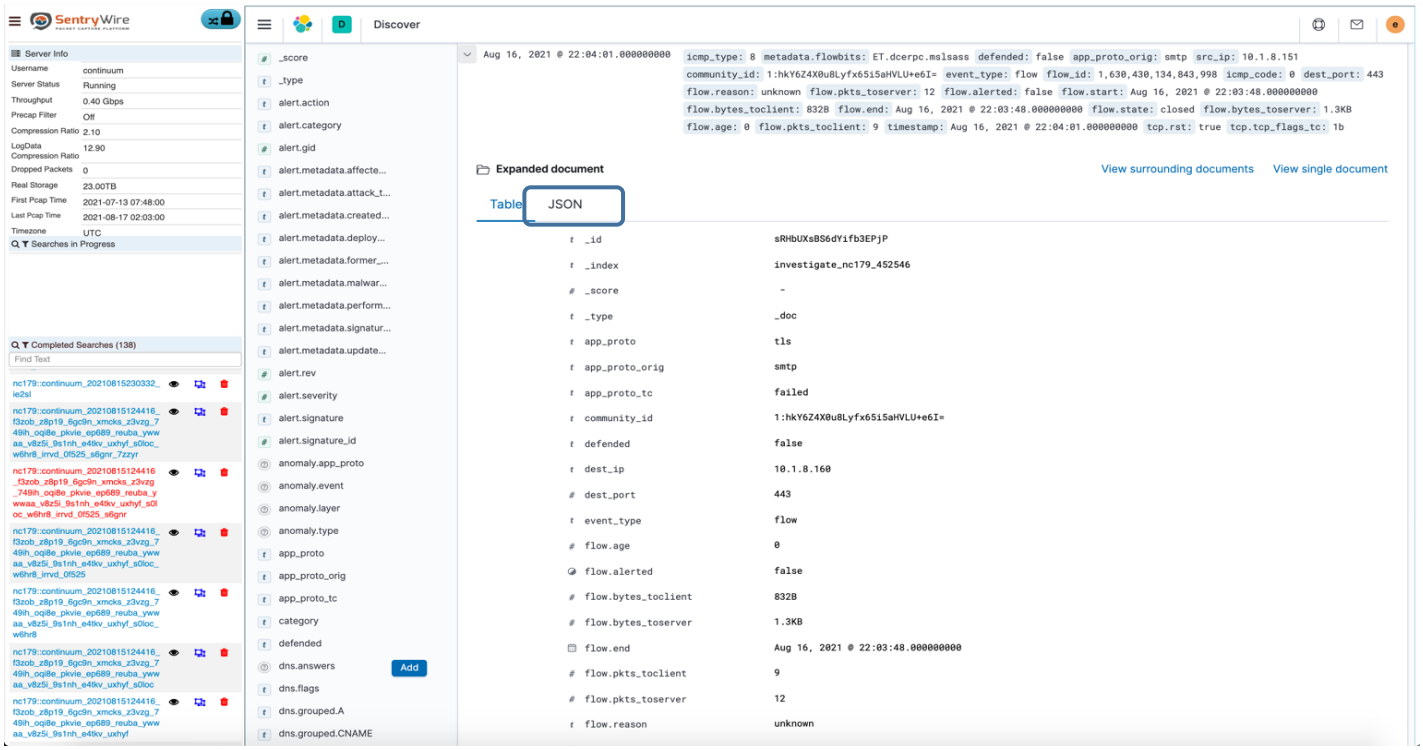
2.1.2 ASSISTED (JSON) Search

Following sections describe how to create a search, an active trigger.

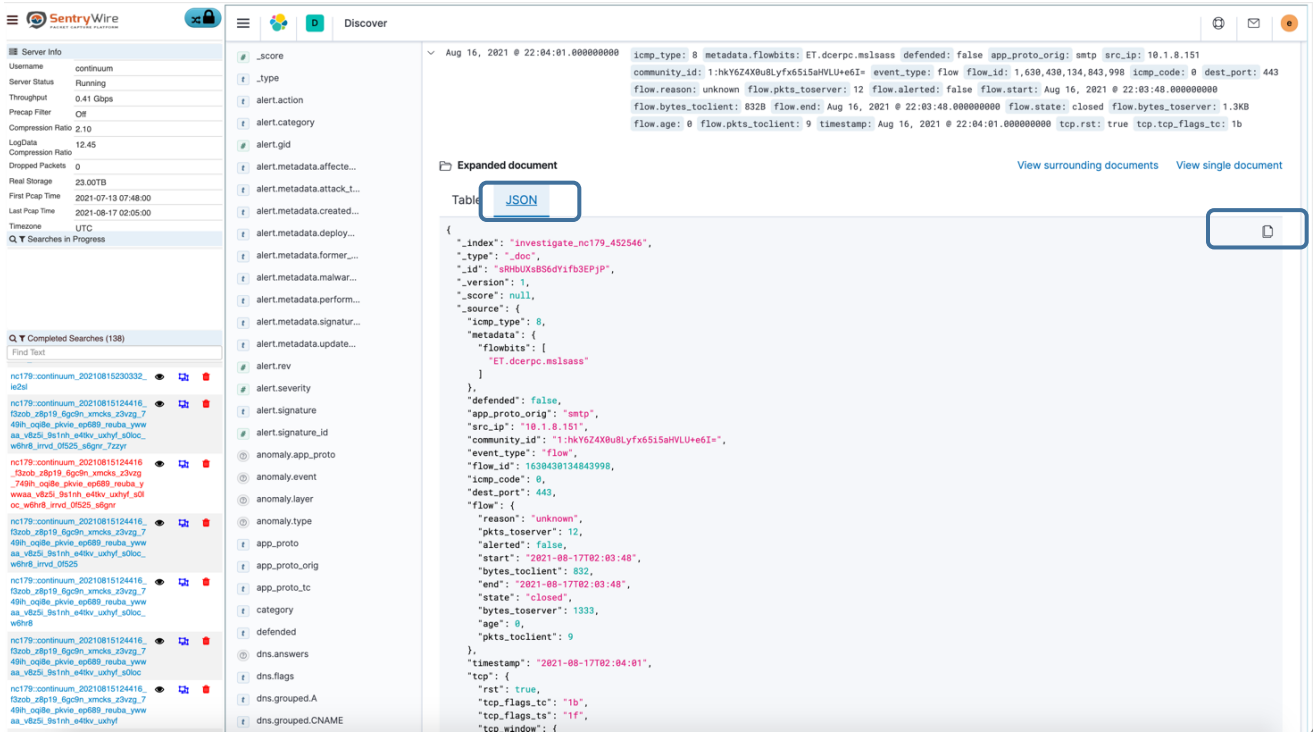
This method allows users to create searches without any prior knowledge of BPF syntax. Switch from the Dashboard view to Discover view by selecting Discover menu option as shown below:



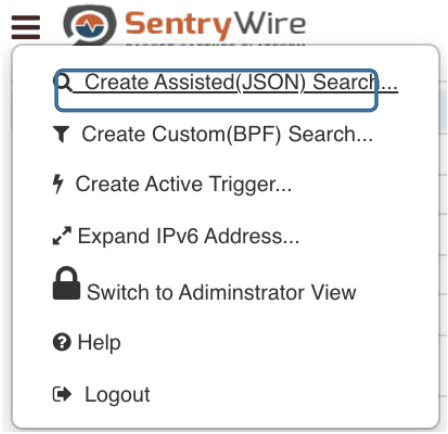
Once in Discover mode, navigate to a metadata event that you would like to use as the basis for the JSON-assisted search, and expand it.



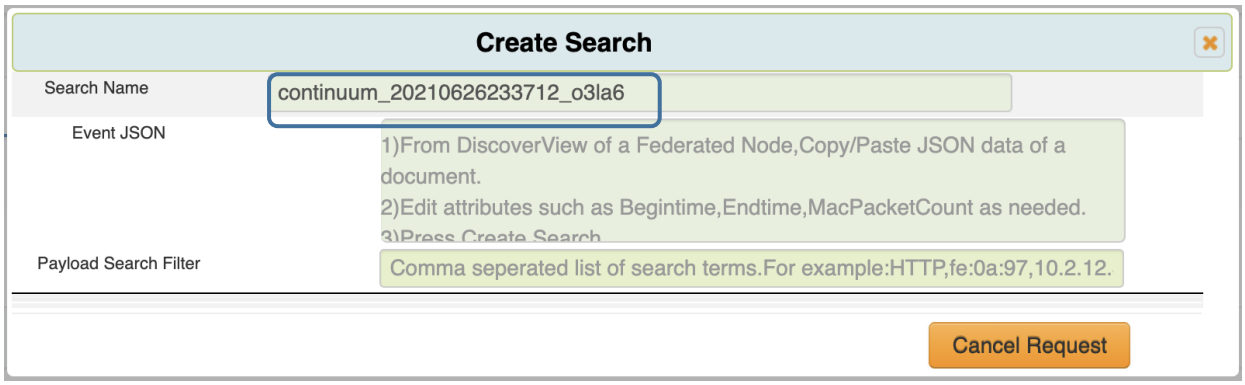
Select JSON option and click on the copy button to the right of the page:



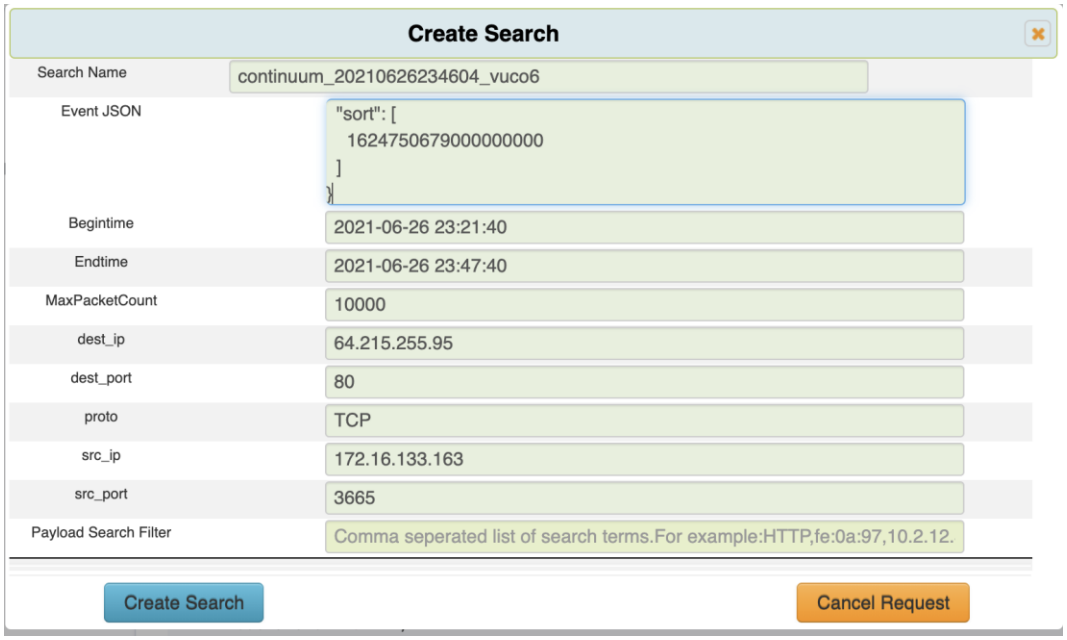
Select the Menu option:



Dialog box appears:



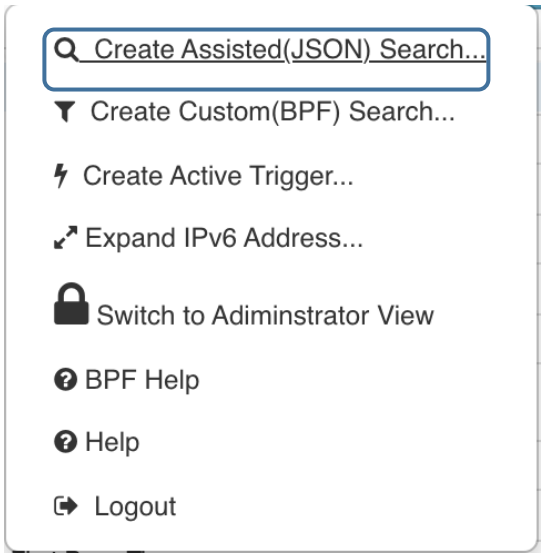
Paste the search details into the Event JSON, the other field data is extracted from the JSON data:



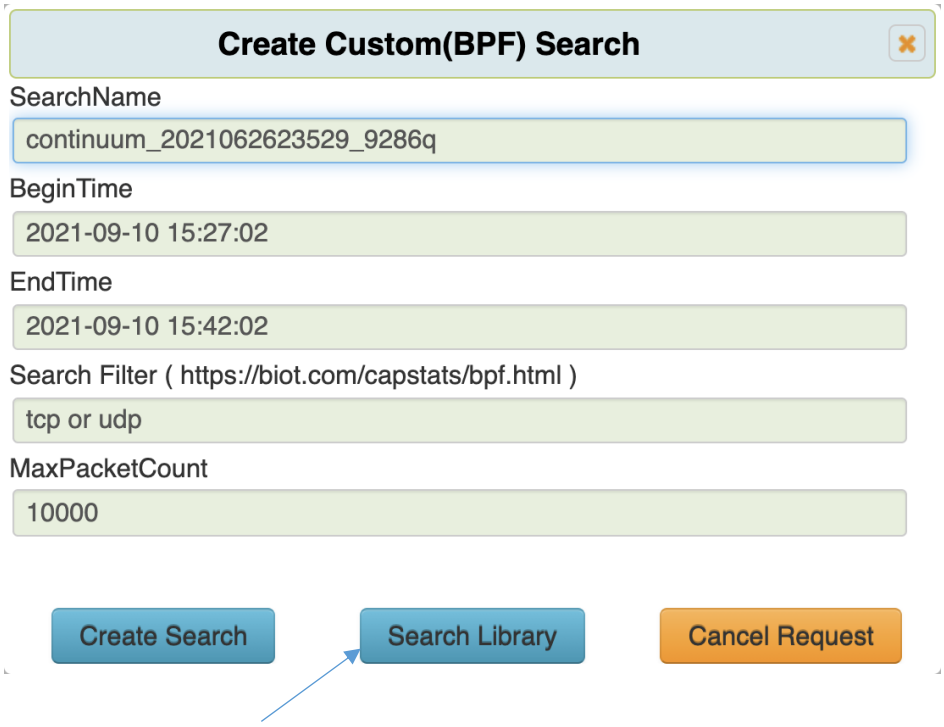
Click on the Create Search button to create the search named *continuum_20210626234604_vuco6.*This search will appear in Searches in Progress Panel. Once the search is complete, it will appear in Completed Searches panel.

2.1.3 CUSTOM (BPF) Search

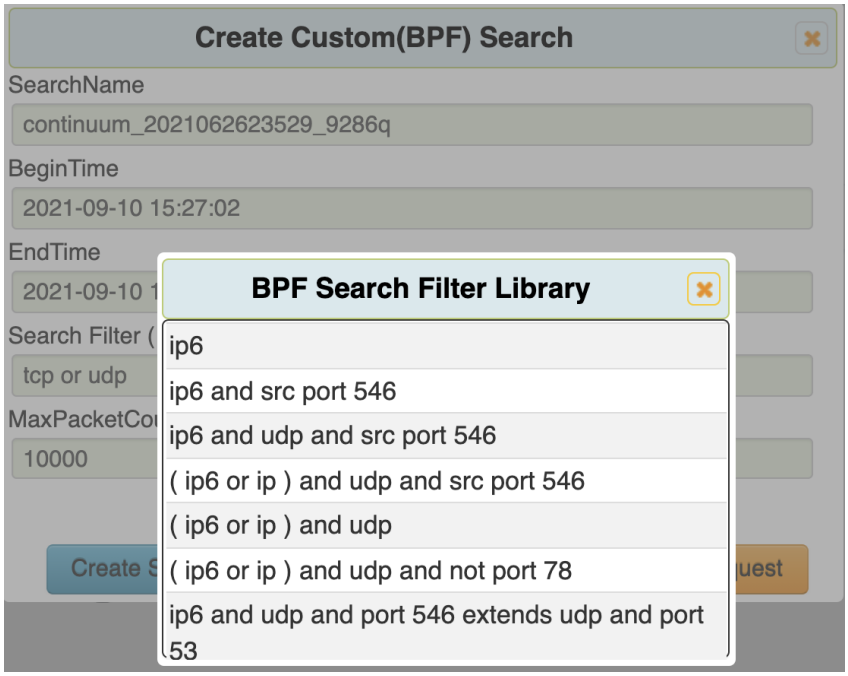
Berkeley Packet Filter (BPF) allows searching for pcaps based on various attributes of network traffic. Use the menu option Create Custom (BPF) Search for this purpose.



Dialog box appears:



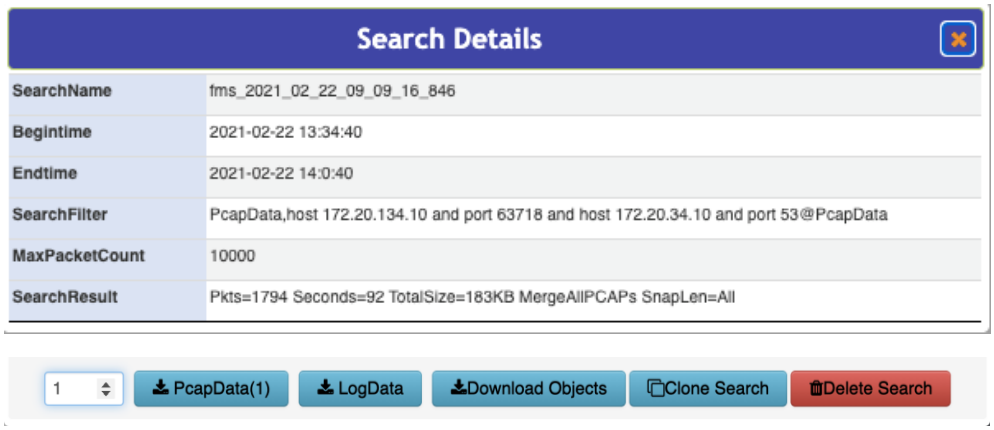
Search Library collects BPF Filters that were used previously used. Click on the Search Library button to see past search filters (if any). Copy/Paste one of these filters or enter your own.



Modify the Search Name, Begin/End time, BPF Search filter and Max Packet Count as needed, and press Create Search button. The new search appears in Searches In Progress panel:

Once the search is complete, it appears in Completed Searches panel:

Click on the Search Name hyperlink to see Search Info:

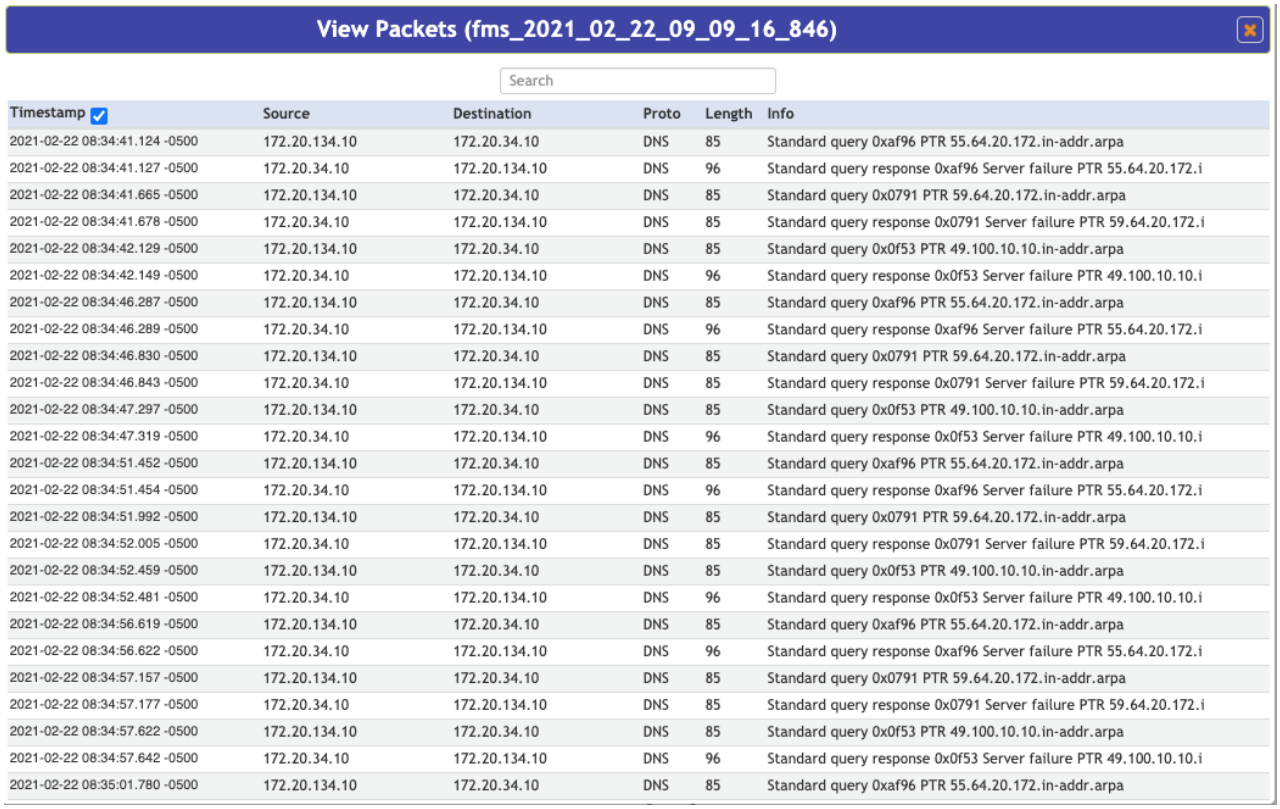


Search Details

SearchName	fms_2021_02_22_09_09_16_846
Begintime	2021-02-22 13:34:40
Endtime	2021-02-22 14:0:40
SearchFilter	PcapData,host 172.20.134.10 and port 63718 and host 172.20.34.10 and port 53@PcapData
MaxPacketCount	10000
SearchResult	Pkts=1794 Seconds=92 TotalSize=183KB MergeAllPCAPs SnapLen=All

1 | PcapData(1) | LogData | Download Objects | Clone Search | Delete Search

View Packets of the Search by clicking on :



View Packets (fms_2021_02_22_09_09_16_846)

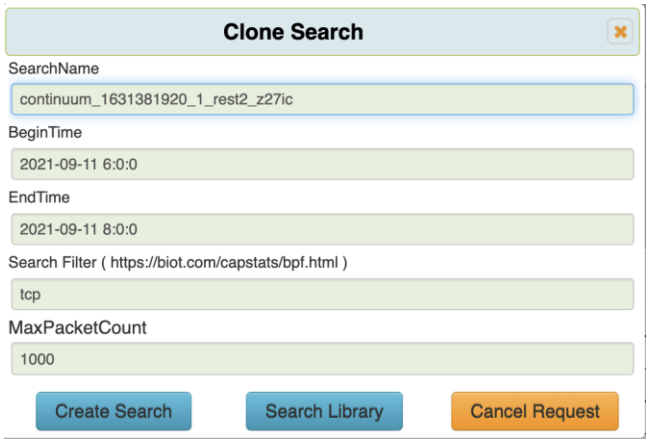
Search

Timestamp	Source	Destination	Proto	Length	Info
2021-02-22 08:34:41.124 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:41.127 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:41.665 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:41.678 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x0791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:42.129 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:42.149 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:46.287 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:46.289 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:46.830 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:46.843 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x0791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:47.297 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:47.319 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:51.452 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:51.454 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:51.992 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:52.005 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x0791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:52.459 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:52.481 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:56.619 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:56.622 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:57.157 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:57.177 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x0791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:57.622 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:57.642 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:35:01.780 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa

Click on Download icon ( ) to download the search pcap for further analysis using Wireshark or any other tools that accept standard pcap files, and Delete icon ( ) to delete this search.

Click on Clone icon ( ) to Clone this search. Any of the fields can be modified:

Note the URL next to the Search Filter that can be used to understand Berkeley Packet Filter (BPF) syntax. Click on **BPF Help** button to understand BPF syntax:

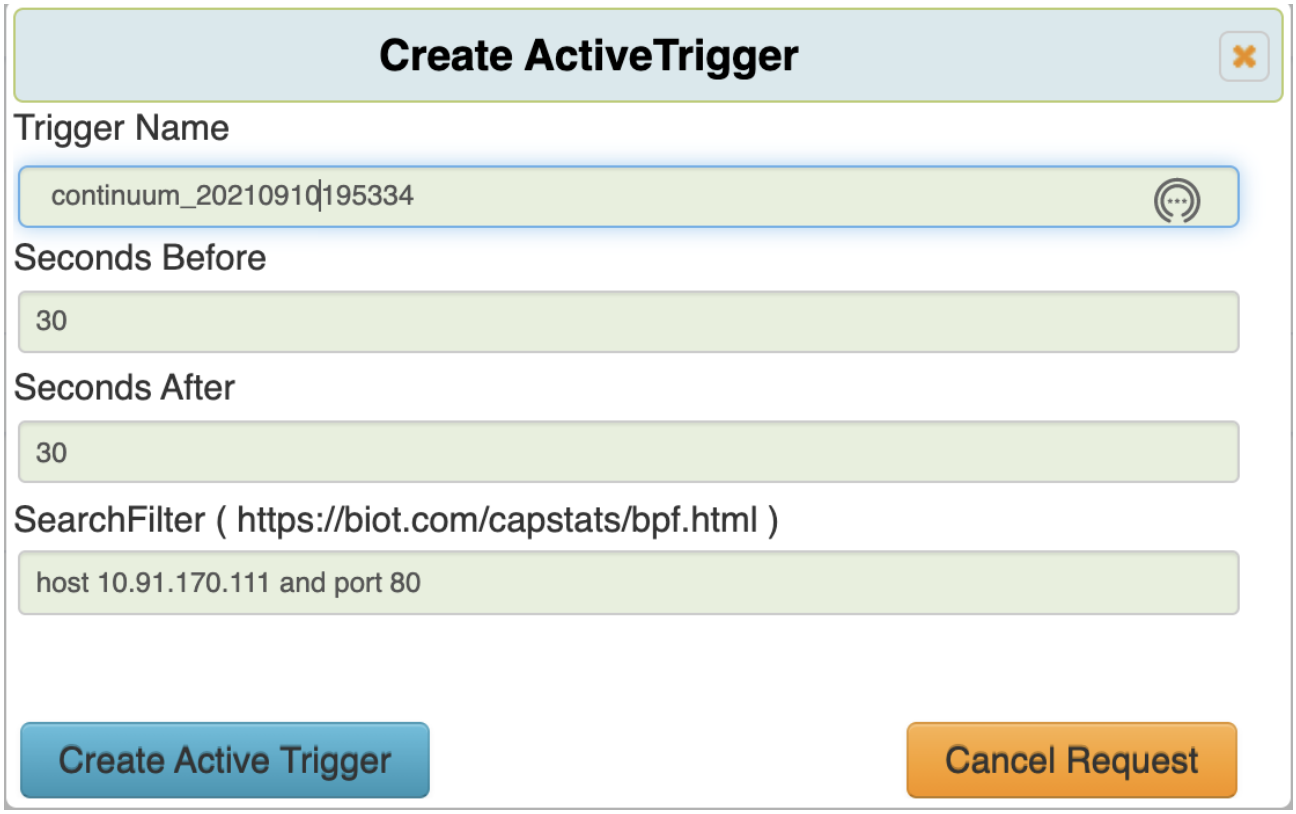


Click on **Create Search** button to create a new search.

2.1.4 Create Active Trigger

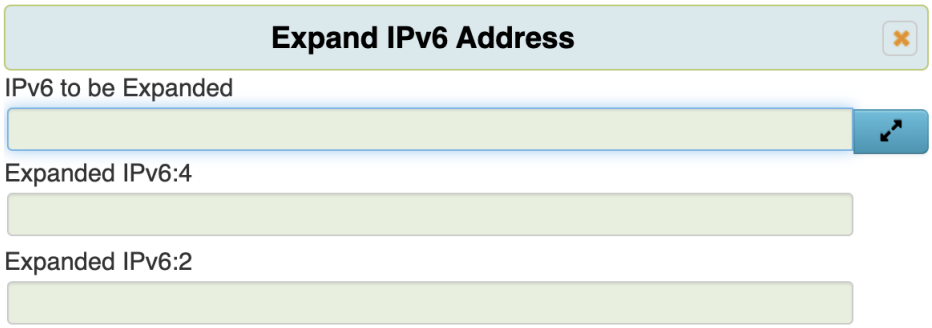
Active triggers allow users to get alerts when specified BPF filter matches payload of a packet. For example, you can specify an IP address as the search filter and you will see an alert when traffic containing the IP address is captured.

- To generate a trigger, specify the trigger name and time frame (Seconds Before and Seconds After) and a valid BPF filter.
- Seconds Before/After allow users to avoid generating too many alerts. An alert for the same trigger is generated only after this time is passed. Values of 30/30 indicate that minimum time between trigger generation is 1 min.
- The Add button allows the FM user to create a global active trigger (100 per node) for each configured node.

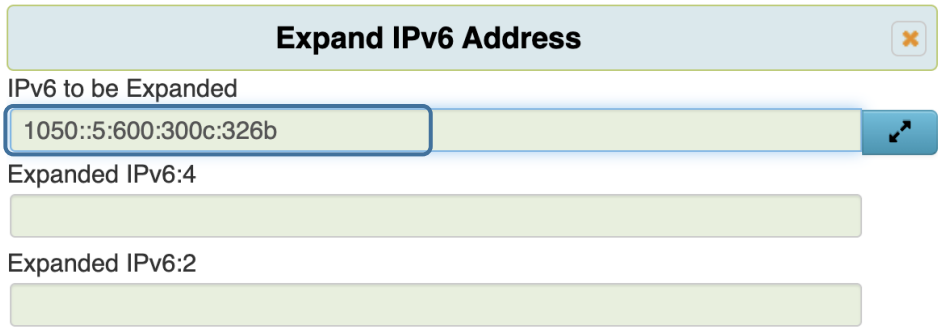

Create ActiveTrigger
Trigger Name
continuum_20210910195334
Seconds Before
30
Seconds After
30
SearchFilter (https://biot.com/capstats/bpf.html)
host 10.91.170.111 and port 80
Create Active Trigger
Cancel Request

2.1.5 Expand IPv6 Address

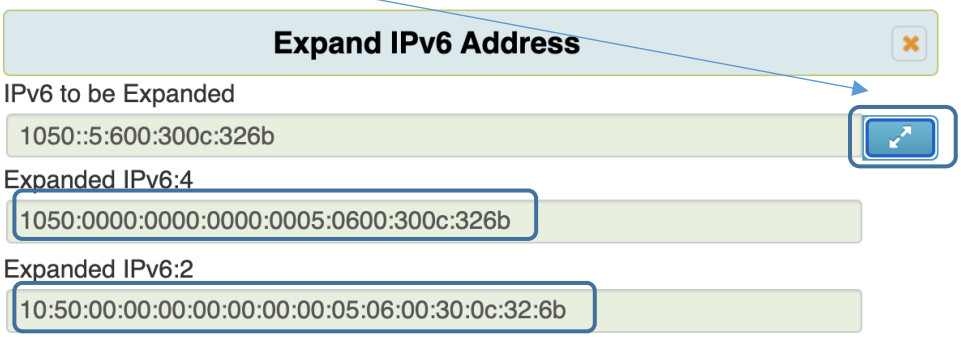
This menu option will pop up a resizable Dialog box that allows users to expand ipv6 addresses. More information about this feature is available in Appendix B.



Enter IPv6 address to be expanded:



Press Expand button:

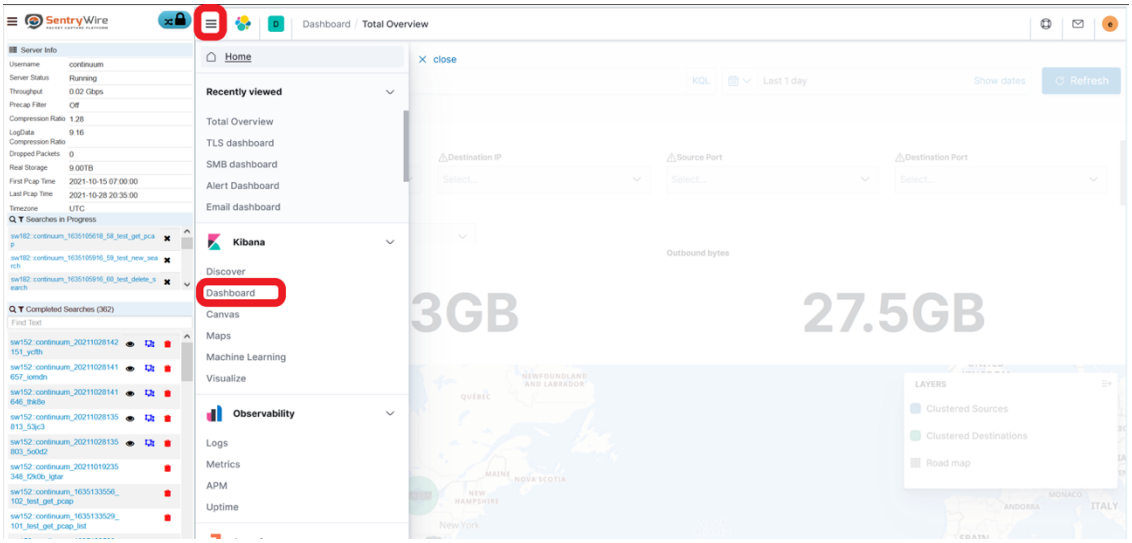


2.2 VISUALIZATIONS AND DASHBOARDS

The following are basic functionality operations for using Elastic Kibana within the SentryWire UI. Kibana allows users to easily and quickly visualize, explore, and search metadata logs generated by SentryWire and execute packet searches using the corresponding log files. This is not an all-encompassing guide to using Elastic Kibana but instead covers the most important features for use with the SentryWire Packet Capture appliance.

2.2.1 Viewing an existing dashboard

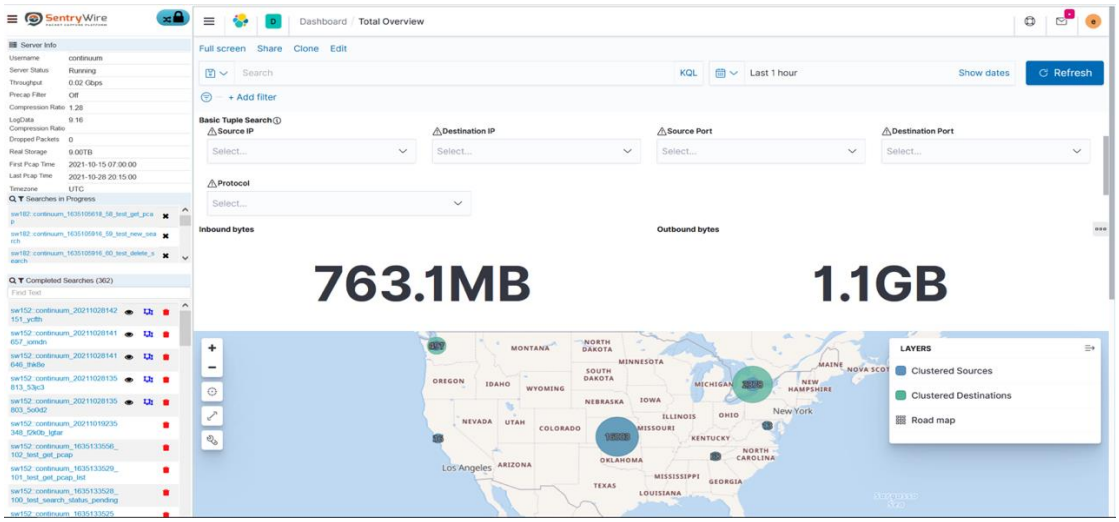
1. To view an existing dashboard object in Kibana, click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on dashboard



3. Find the desired dashboard and click on it
    a. This will redirect the user to the appropriate dashboard for exploration, drill-down, and pivot

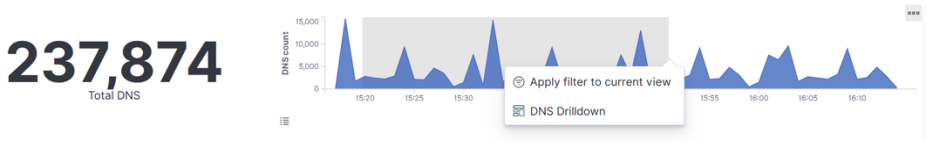
2.2.2 Overview dashboard

When visiting the platform, the “Total Overview” dashboard will be the landing page. On this page, it will show the sources, destinations, and flow rate of traffic over time. Scroll down the page to get a bird’s eye view of the traffic broken down by the most common fields.



2.2.3 Drilldown example

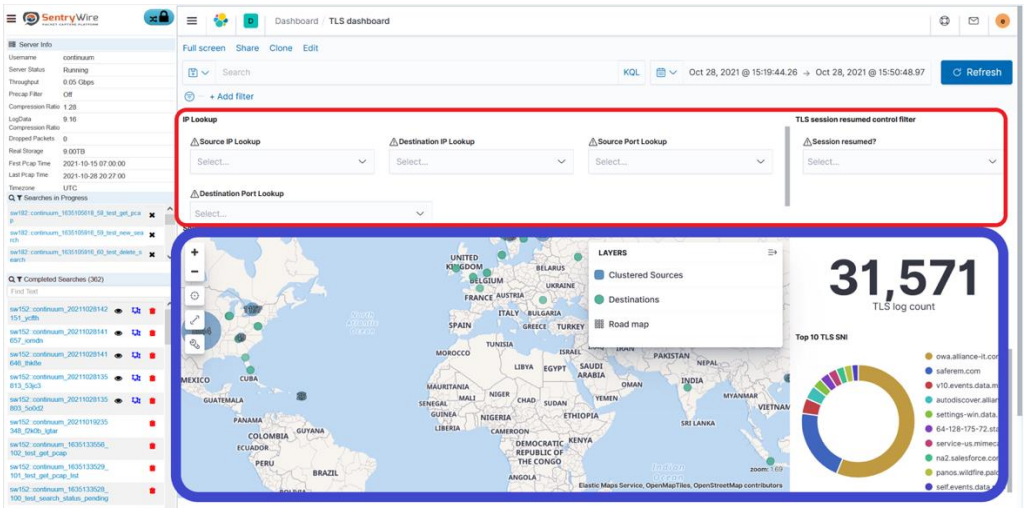
At the bottom of the overview are breakouts of different logs by protocol. By clicking and dragging over sections in the chart, the option to filter by the time span and the option to drill down deeper into the dedicated protocol dashboard will appear. Some protocols have multiple drill down dashboards associated. By clicking the “DNS Drilldown” option in the screenshot below, the system would navigate to the DNS dashboard, and apply a time filter based on the span selected.



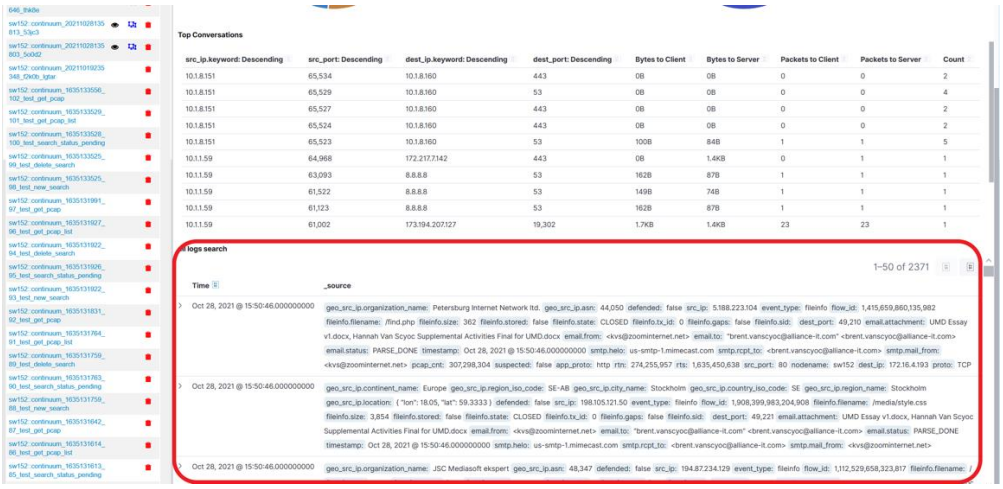
2.2.4 Dashboard structure

Pre-made dashboards follow a structure to ensure a consistent experience across the entire platform.

- Interactive packet filter at the top in case you do not want to type out a filter in the search bar
- Map, timeline, total log count, or other high level information next

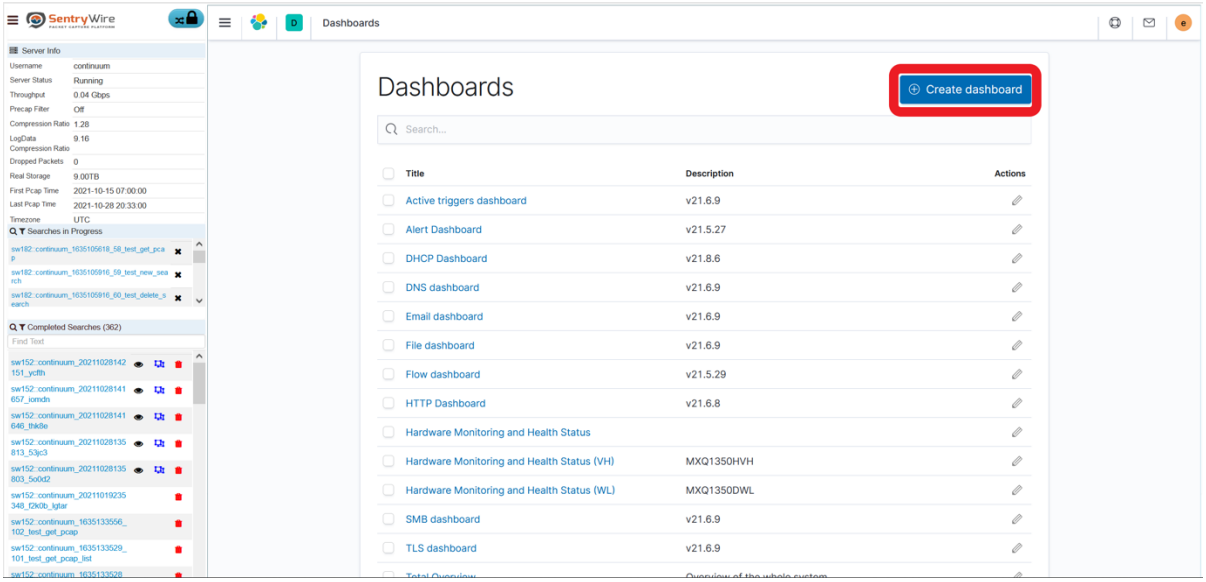


- "All log" viewer at the bottom includes more than the filtered protocols that the dashboard is named after so you can see associated traffic



2.2.5 Creating a new dashboard

1. Click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on “dashboard”
3. Click on the Create dashboard button
4. By default, the new dashboard will be blank and can be filled with existing or new visualization objects

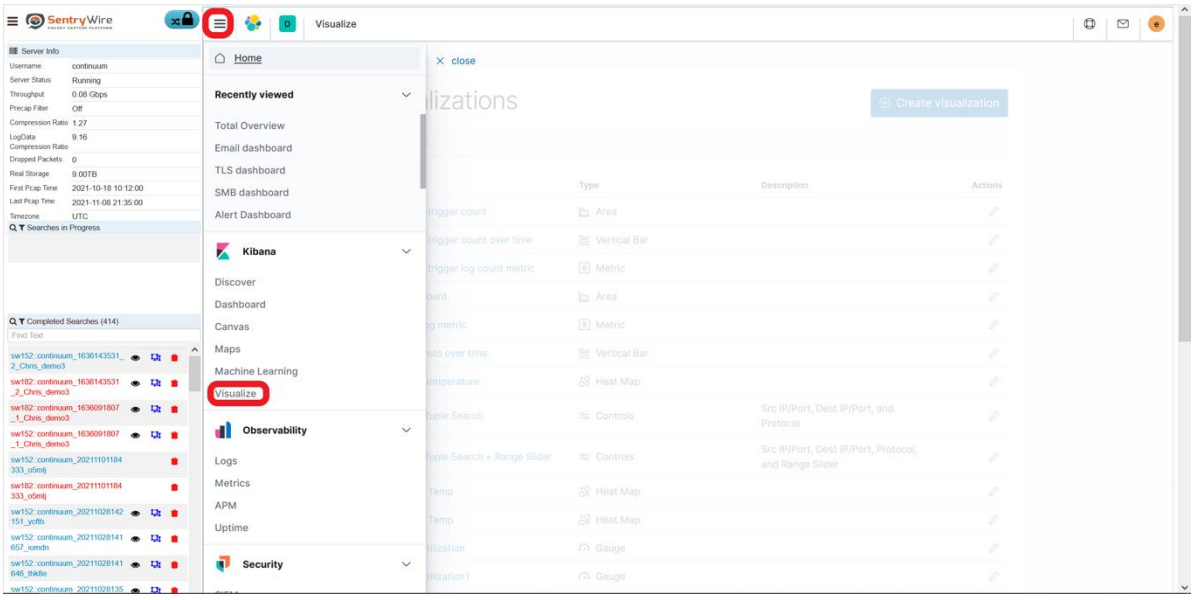


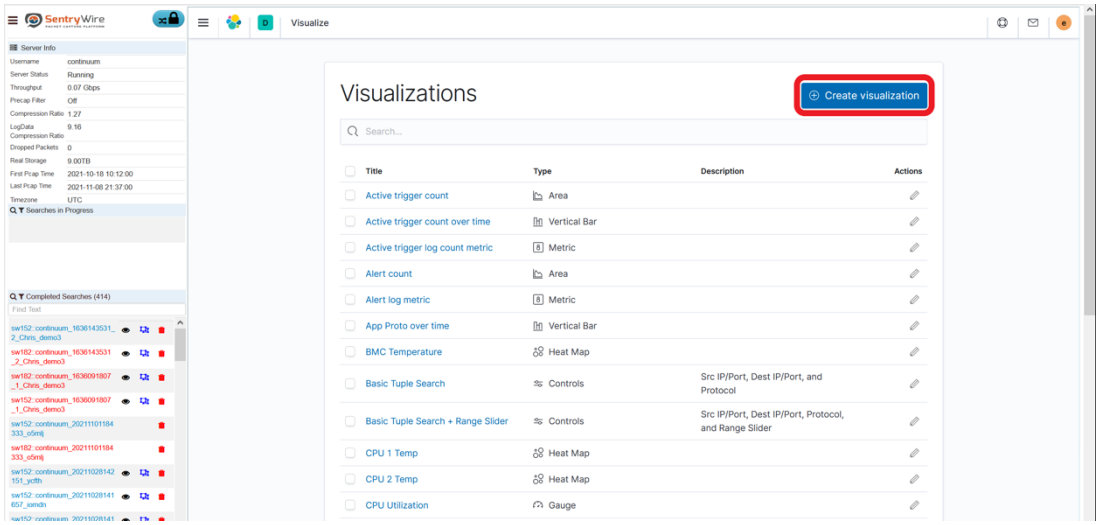
2.2.6 Creating a new visualization

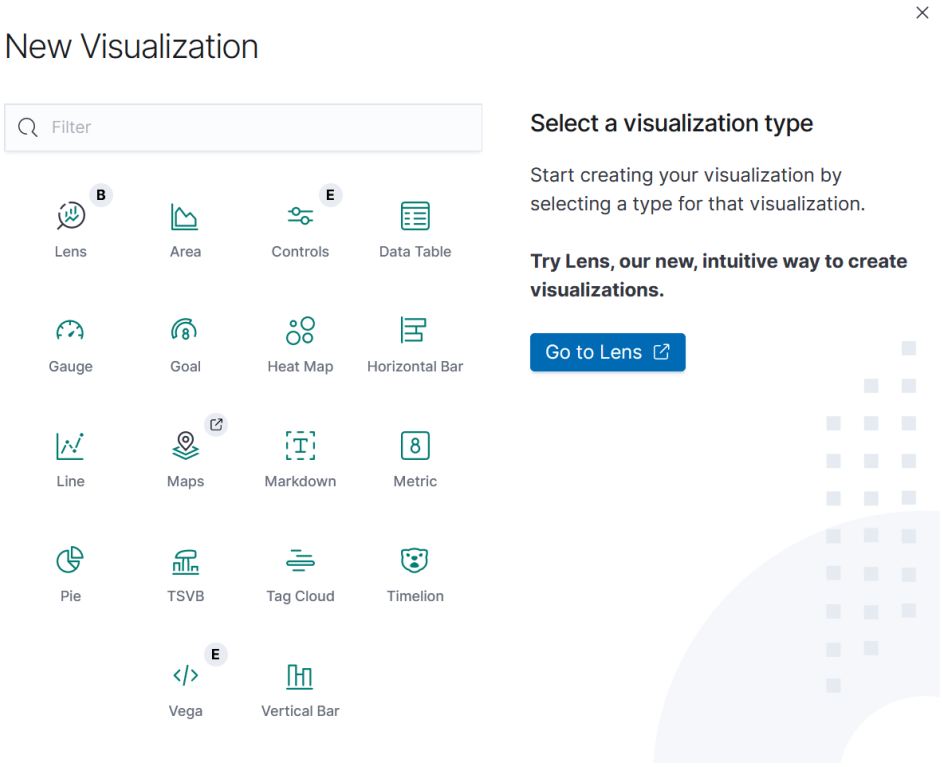
Visualization objects serve as the widgets that make up the various dashboard objects.

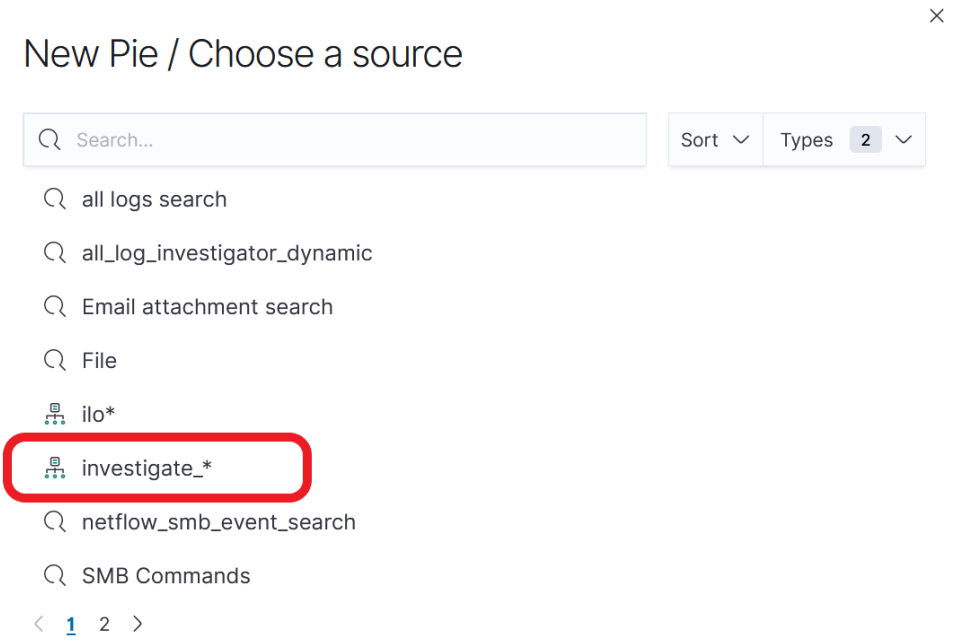
1. Click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on Visualize
3. Click on the Create visualization button
4. On the pop-up menu, select the desired style of visualization. This tutorial will use “Pie”.
5. Choose a saved index to use as the data set for the visualization
    a. The index will be “investigate-*” for almost all SentryWire visualizations
6. Fine tune the visualization to display the desired information
7. Scroll to the bottom and press “update”
8. Scroll back up and click the Save button
9. Name your visualization and save it. This visualization will be available to be added to any dashboards

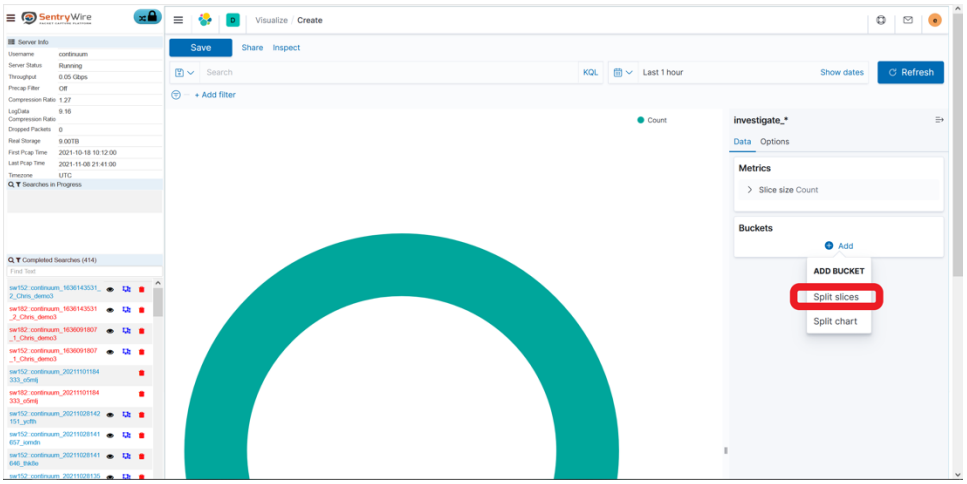
Walkthrough

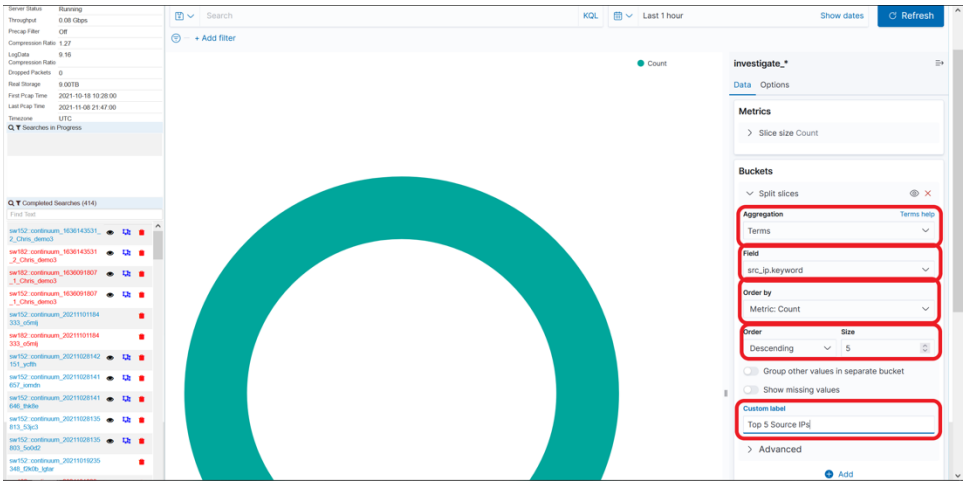




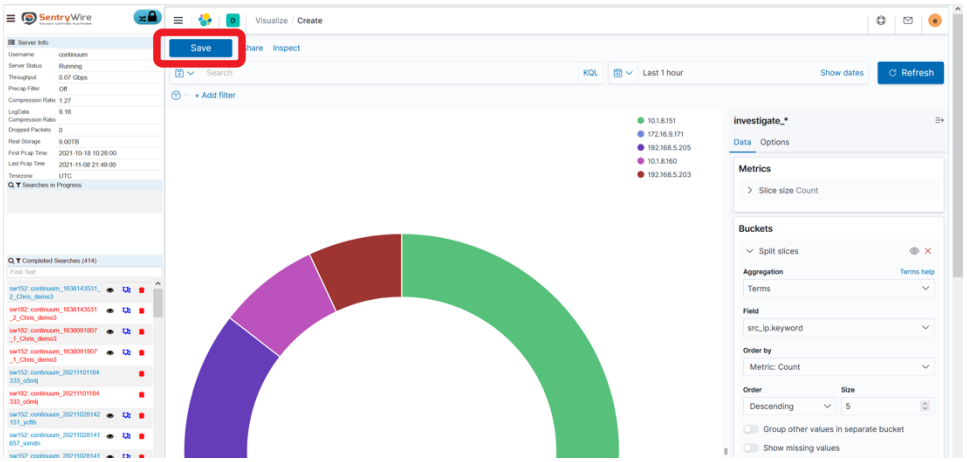

New Visualization
Filter
Lens
Area
Controls
Data Table
Gauge
Goal
Heat Map
Horizontal Bar
Line
Maps
Markdown
Metric
Pie
TSVB
Tag Cloud
Timelion
Vega
Vertical Bar
Select a visualization type
Start creating your visualization by selecting a type for that visualization.
Try Lens, our new, intuitive way to create visualizations.
Go to Lens

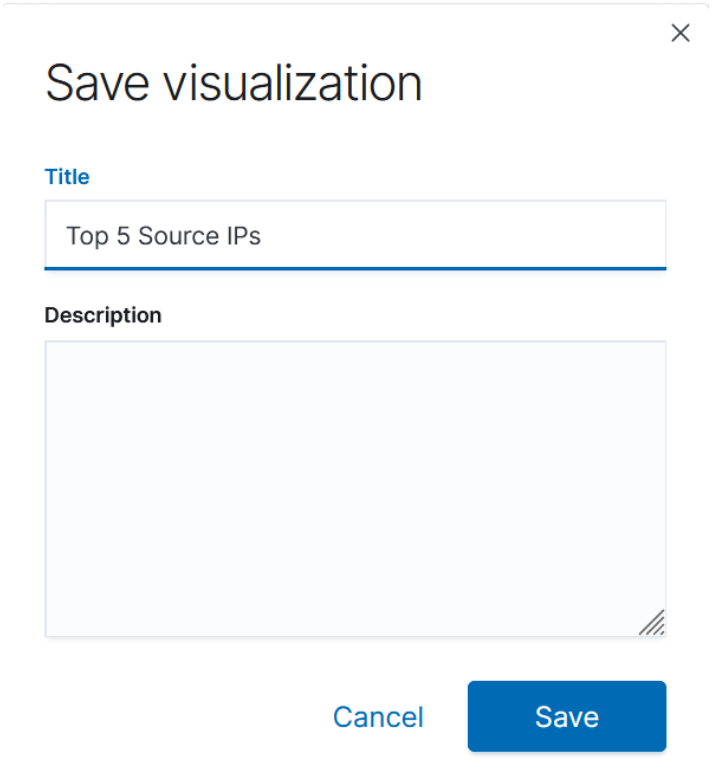

New Pie / Choose a source
Search...
Sort
Types 2
all logs search
all_log_investigator_dynamic
Email attachment search
File
ilo*
investigate_*
netflow_smb_event_search
SMB Commands
1 2


Visualize / Create
Save
Share
Inspect
Search
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
Count
investigate_*
Data
Options
Metrics
Slice size Count
Buckets
Add
ADD BUCKET
Split slices
Split chart


Search
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
Count
investigate_*
Data
Options
Metrics
Slice size Count
Buckets
Split slices
Aggregation
Terms
Field
src_ip.keyword
Order by
Metric: Count
Order
Descending
Size
5
Group other values in separate bucket
Show missing values
Custom label
Top 5 Source IPs
Advanced
Add


Order by
Metric: Count
Order
Descending
Size
5
Group other values in separate bucket
Show missing values
Custom label
Top 5 Source IPs
Advanced
Add
Discard
Update

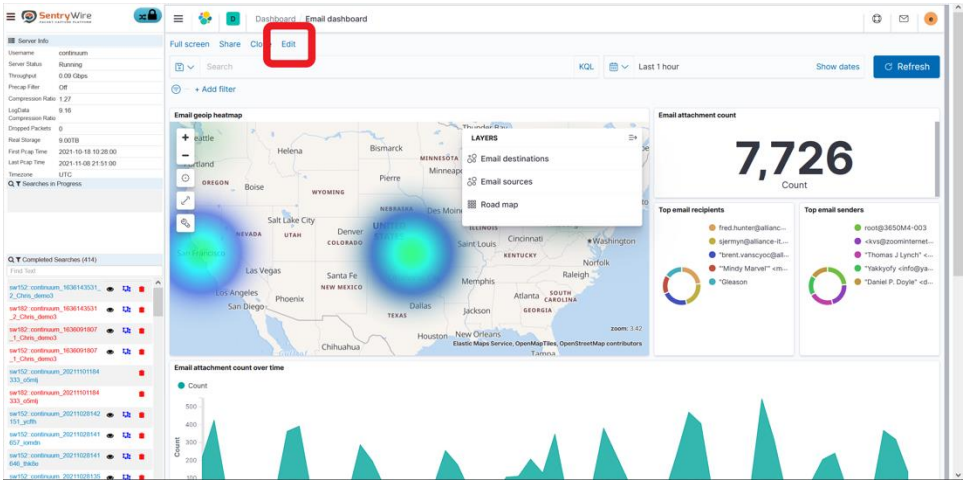

Save
Inspect
Visualize / Create
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
investigate_*
Data
Options
Metrics
Slice size Count
Buckets
Split slices
Aggregation
Terms help
Terms
Field
src_ip.keyword
Order by
Metric: Count
Order
Size
Descending
5
Group other values in separate bucket
Show missing values

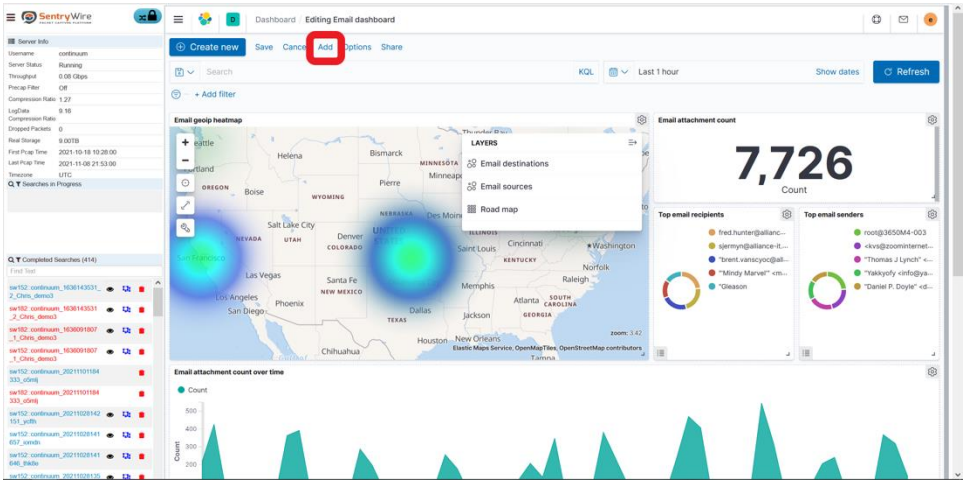

Save visualization
Title
Top 5 Source IPs
Description
Cancel
Save

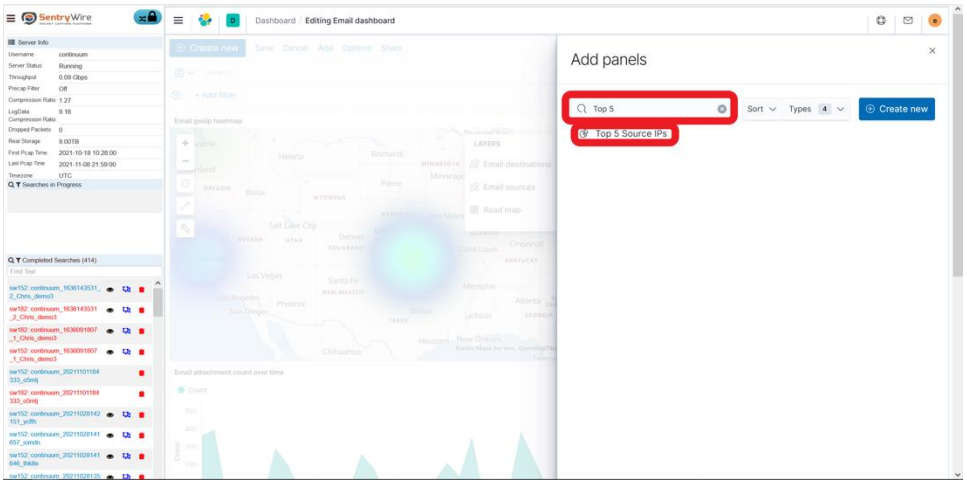
2.2.7 Adding a visualization to a dashboard

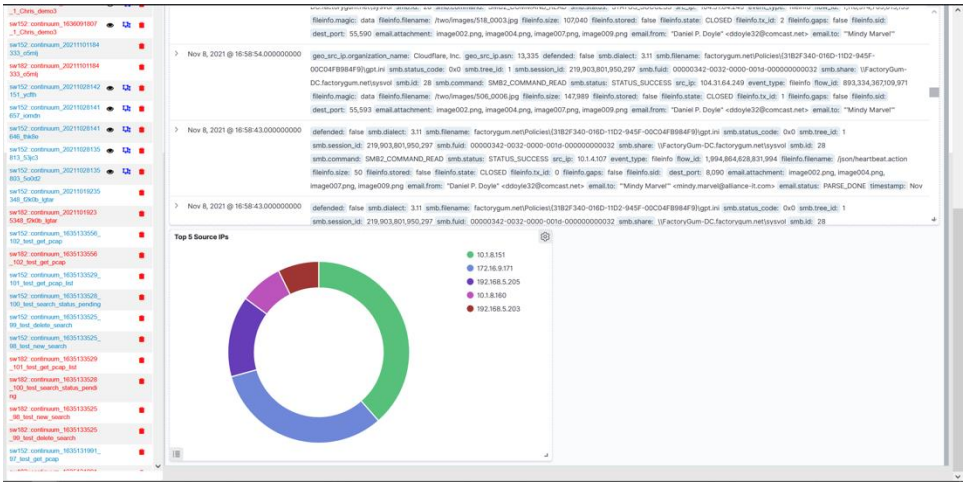
To add an existing visualization to a dashboard, click on the 3 bars at the top left of the screen to open the drop-down menu.

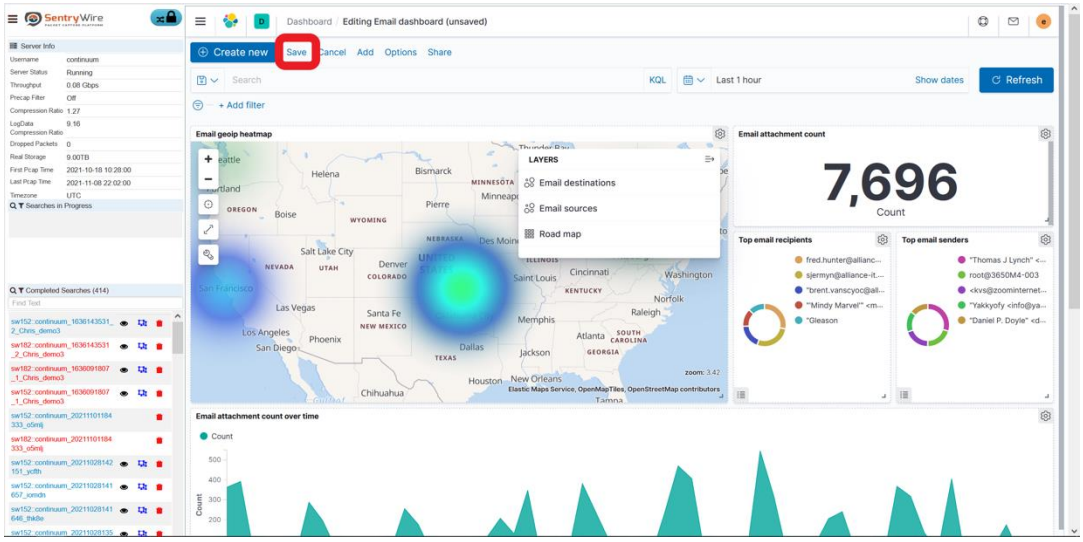
1. Visit any dashboard
2. Click “Edit”
3. Click the “Add” to add an existing visualization
    a. You can also select “Create new” to make a new visualization and automatically have it added to this dashboard.
4. Find the desired visualization by name and click on it to add it to the dashboard
5. Once the visualization is added, it will appear at the bottom of the entire dashboard. It can be freely moved and resized within the dashboard.
6. Click the Save button at the top of the page to save as an existing or new dashboard
7. “Save as new dashboard” will save as a copy
8. “Store time with dashboard” ensures that every time you visit it, the time selection is consistent
9. Click the Save button

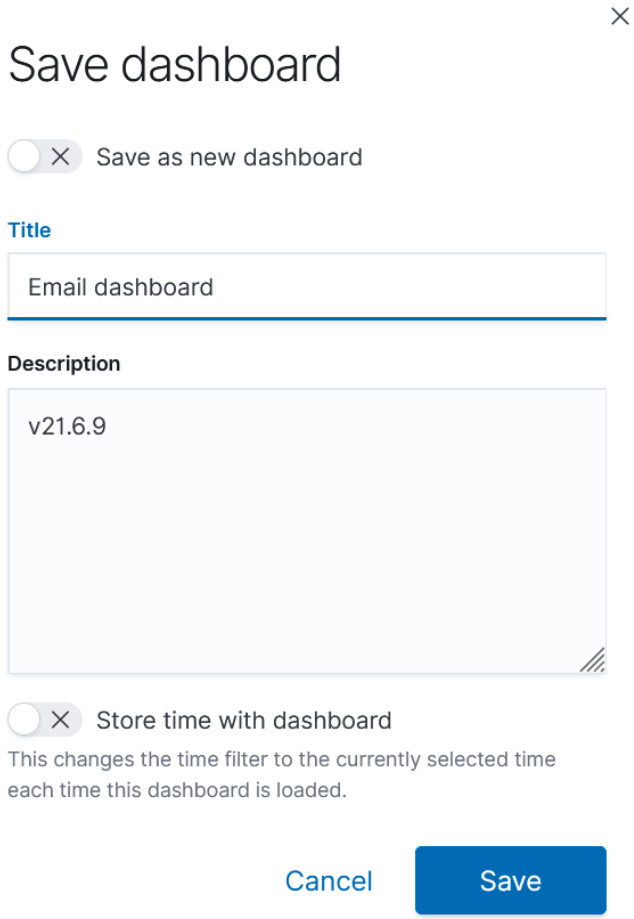





Dashboard / Editing Email dashboard
Add panels
Top 5
Top 5 Source IPs
Sort
Types
Create new

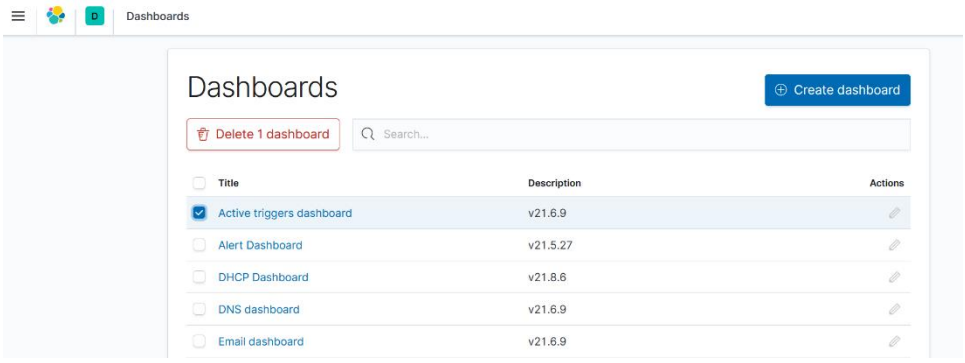

Top 5 Source IPs
10.1.8.151
172.16.9.171
192.168.5.205
10.1.8.160
192.168.5.203


Dashboard / Editing Email dashboard (unsaved)
Create new
Save
Cancel
Add
Options
Share
Refresh
Email geoip heatmap
LAYERS
Email destinations
Email sources
Road map
Email attachment count
7,696
Count
Top email recipients
Top email senders
Email attachment count over time



2.2.8 Deleting a dashboard or visualization

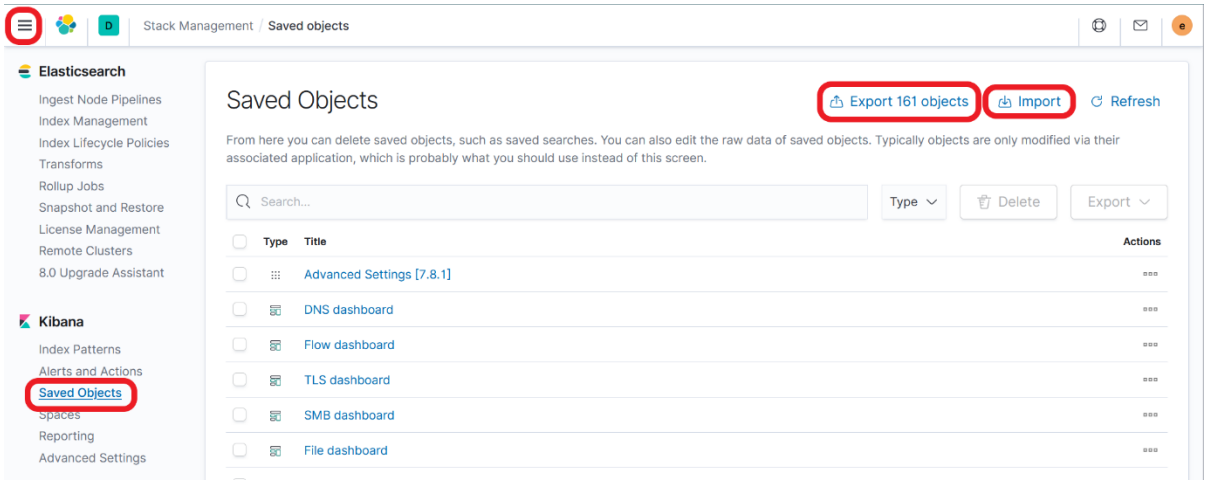
1. Navigate to “Dashboards” or “Visualizations” section.
2. Add check marks to the items you wish to delete
3. Click the red “Delete N dashboard(s)” button

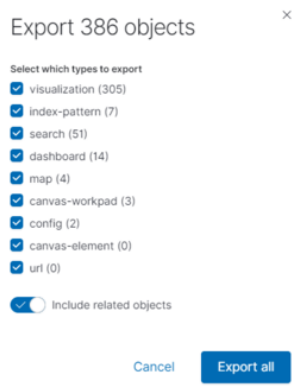


2.2.9 Backup and restore custom dashboards

1. To import existing visualization and dashboard objects, click on the 3 bars at the top left of the screen to open the drop-down menu

2. Click on Stack Management (found at the bottom of the drop-down menu)
3. Click on the Saved Objects button within the Kibana category of options
4. Backing up objects
    a. Select the checkboxes by items you wish to backup. Then click “Export N Objects” at the top of the page. Clicking the export button without selecting any will export everything.
    b. Ensure that you select “include related objects”
    c. Dashboard and visualization objects are saved in .ndjson format
5. Restoring a backup
    a. Click the import button
    b. Choose the file to import
    c. Once the files are imported, any new dashboards and visualizations will automatically populate the lists of dashboards and visualizations and will be viewable and editable





2.2.10 Discover

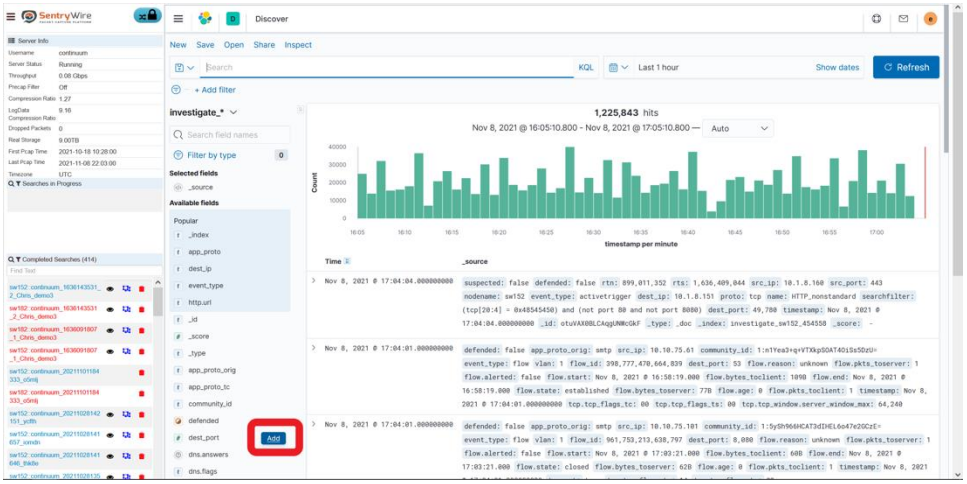
The Discover panel allows for full exploration, search, and drill-down of all metadata logs within Elastic.

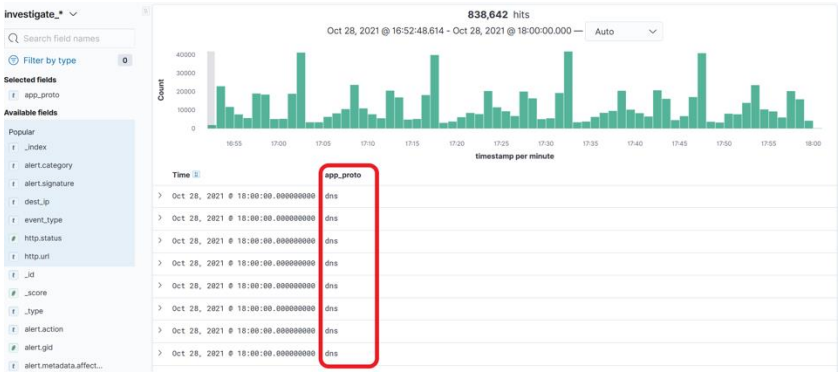
1. Click on the 3 bars at the top left of the screen to open the drop-down menu.
2. Click on Discover
3. From here, custom KQL searches and filters as well as custom time ranges can be applied to navigate through the metadata and find the desired logs
4. These logs can then be used to execute a packet search directly within the SentryWire UI or to confirm events or alerts seen on other appliances

2.2.11 Pin a field to a column

To make a field appear as a column in searches, add the field from the panel on the left.

Hover over the desired field and click “Add” to add a column in the results panel focused on that field.





2.2.12 Searches

Kibana uses KQL, which is further defined in the documentation, but below are the basics.

Accessing fields

Fields are accessed by name, where sub-fields are appended with a period after the parent, and before the child.

Example:

ttp.status

A full list of available fields is shown on the left of the results. This shows the full name of the field, and an icon displaying the type of field it is.

Checking for existence

Wildcards can be placed anywhere in the search bar e.g. wild cards in fields or values.

A colon denotes that you are referencing the value of a specific field.

Example query to return results that contain an http status code:

http.status : *

Negating a clause

If you want to exclude specific results, prepend “not” before the term to exclude.

Example query to show all destination ports that are not port 80:

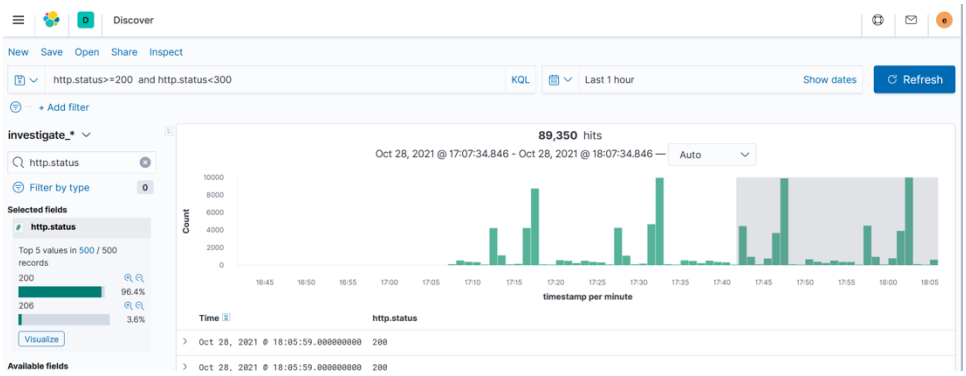
not dest_port : 80

Numerical values

Comparisons can be made to immediate values on the fly.

Example query that returns results where a http status is between 200 and 299 inclusive:

http.status>=200 and http.status<300



Boolean queries

“and” and “or” can join search terms. This can create much more complex searches than would otherwise be possible.

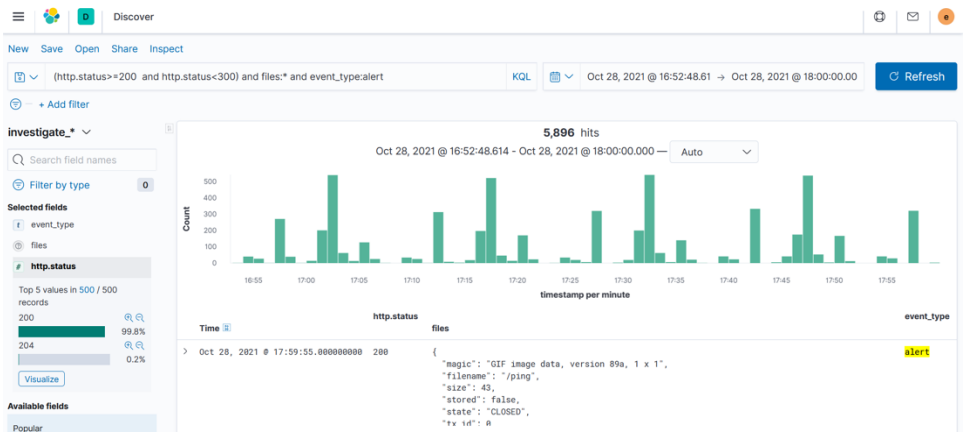
Example query to return all DNS logs for a specific source:

src_ip:192.168.5.205 and event_type:dns

Combining these techniques

By combining these techniques, we can create queries to show results like the following:

(http.status>=200 and http.status<300) and files:* and not dest_port:(80 or 443)

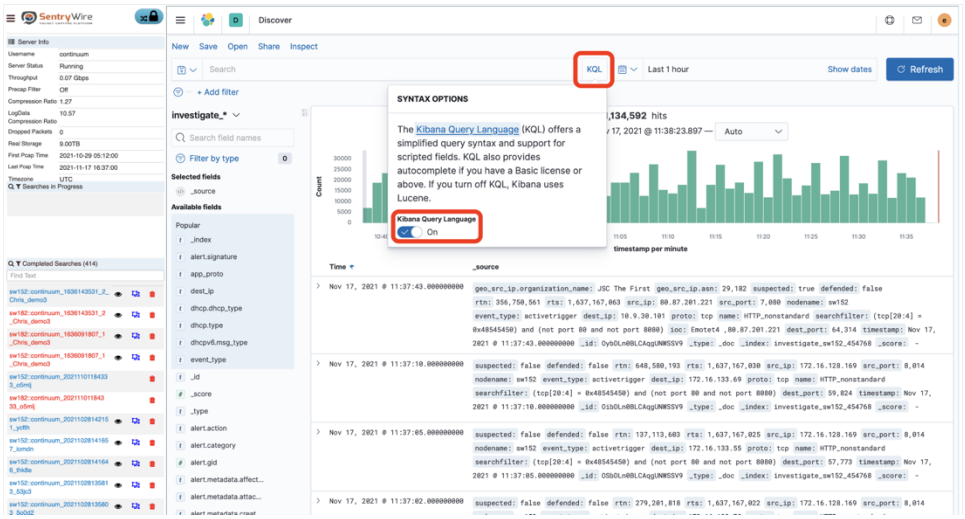


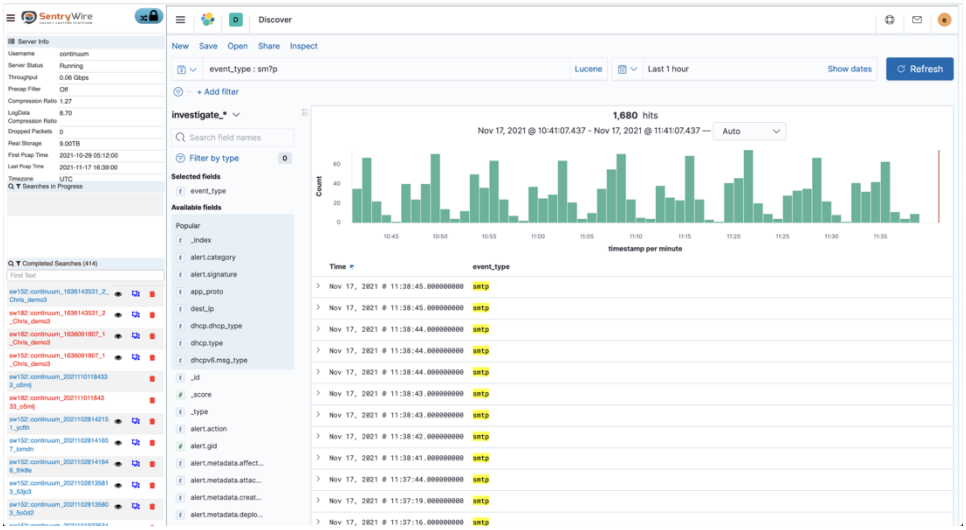
This query displays results that do not use destination port 80 or 443 but contain successful http status codes where at least one file was seen.

Single character wildcard

Single character wildcard works when there are no spaces in the value, as spaces would separate the terms in the search, and enclosing the value in quotes will not parse the "?" as a wildcard character.

1. Turn off Kibana Query Language to switch to Lucene query syntax.
2. Use a "?" character to denote the wildcard character in your search





3 ADMINISTRATOR VIEW

This group of menu options allow authorized users to configure federation groups/nodes, set precapture filter and manage active triggers.

3.1 CONFIGURATION

3.1.1 Home

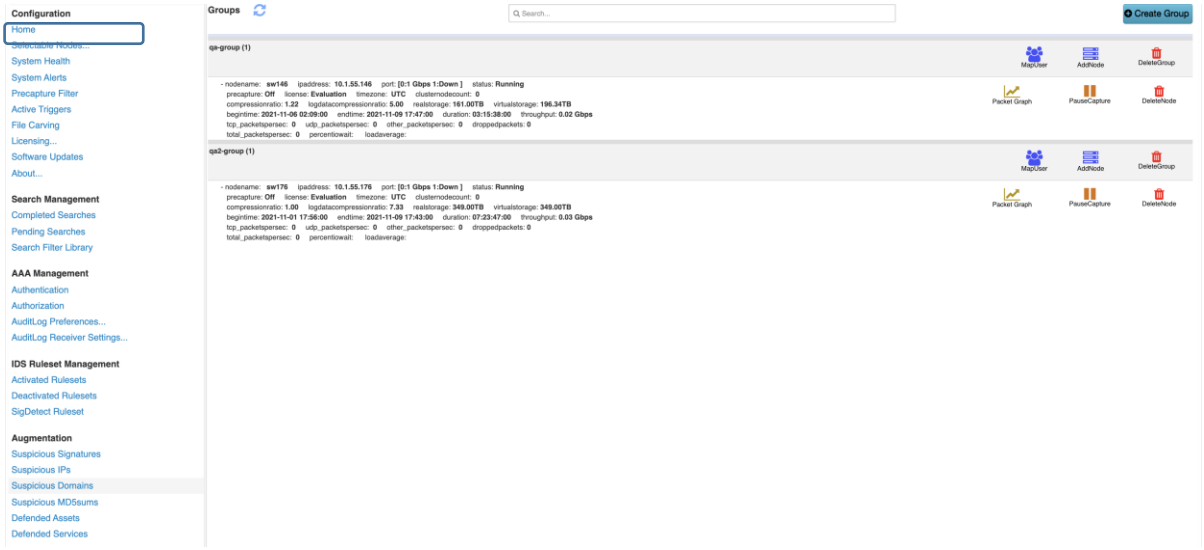
The Home button shows the Groups and Nodes of the Federation Manager. Top of the Admin UI page shows the currently logged in user's name, user's role, authentication mode and product version. The following sections describe each of the options available on the left panel and the actions/views based on the selected option.

The following actions are available on this page. Each of these actions on this page are permitted only to the users with *Groups* permission.

- Groups:
    - Create Group – Authorized users can create groups using **Create Group** button. A group can consist of zero or more nodes. Each group has an Add Node and a Delete Group button.
    - Add Node – Add one or more Federation Nodes to a group using button. Enter IP address of the node.
    - Delete Group – A group can only be deleted when it is empty. Delete all nodes from a group before deleting a group.
    - Map User – This allows which users are allowed to view/manage the nodes of the group.
- Nodes:
    - Each Federation Node can be added to a single group at a time. A node can be added to a group by clicking on the group's **Add Node** button. A dialog box appears with the name of the group shown in the top box. Enter the IP Address of the node to be added and click on **Add Node**.

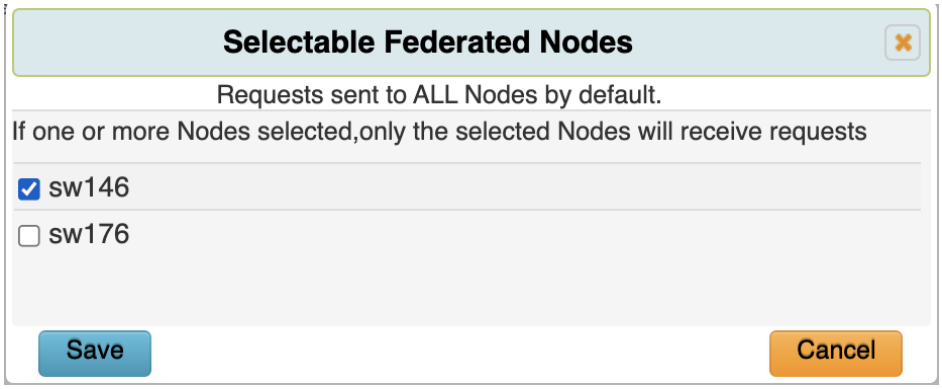
Once a node is added, its details (including the nodename) are displayed. Federated Nodes (appliances) support MTU size of up to 1600. Each node supports packet decoding of these protocols: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, VLAN, ERSPAN, VXLAN, VNTAG, HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP

- The advertised throughput includes system resource calculations for packet processing. As such, the throughput is measured as it reaches the interface, not after internal processing. This allows us to ensure we do not drop packets, while still giving accurate metrics.
- Delete Node: A node can be deleted by selecting **Delete Node** button. This does not cause any change in the capture state of the node. This node can now be added to the same group or to a different group.
- Pause/Resume Capture: A node's capture can be paused and resumed if necessary, using the button **Pause Capture** that toggles to **Resume Capture** on being Paused and vice versa.

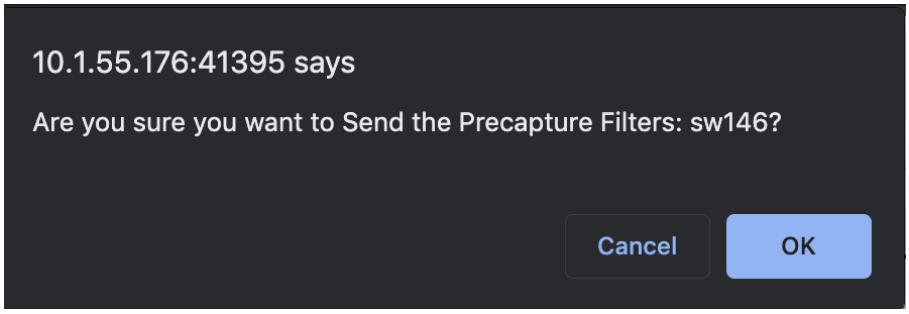


3.1.2 Selectable Nodes

By default, every request to the FM server is sent to all connected federation nodes. This menu option allows restricting the list of the federation nodes that receive a request.

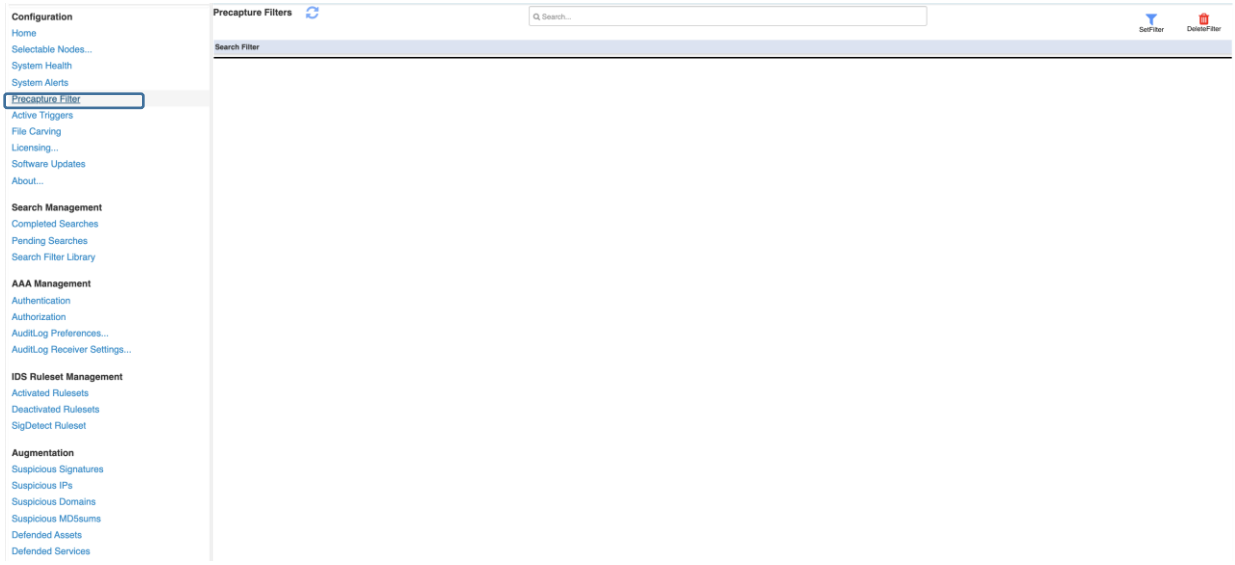


From this point on, when a request such as SetPrecapture is initiated, the user is presented with the list of nodes that are going to receive this request:

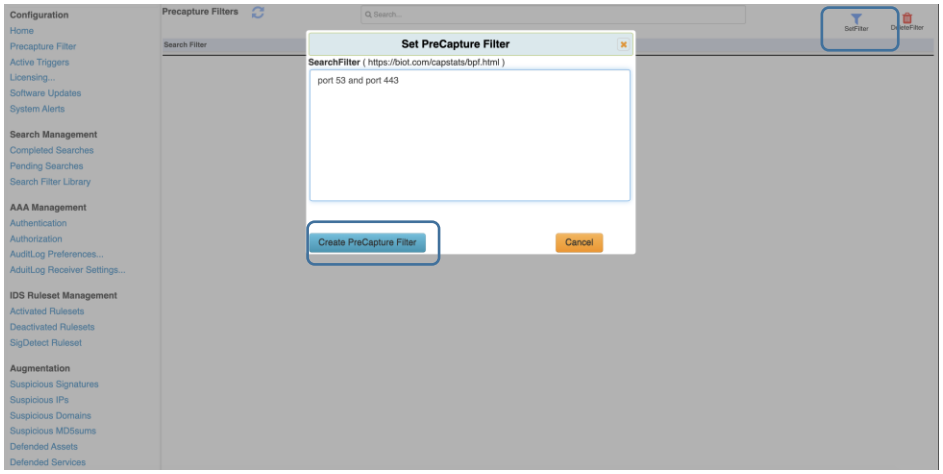


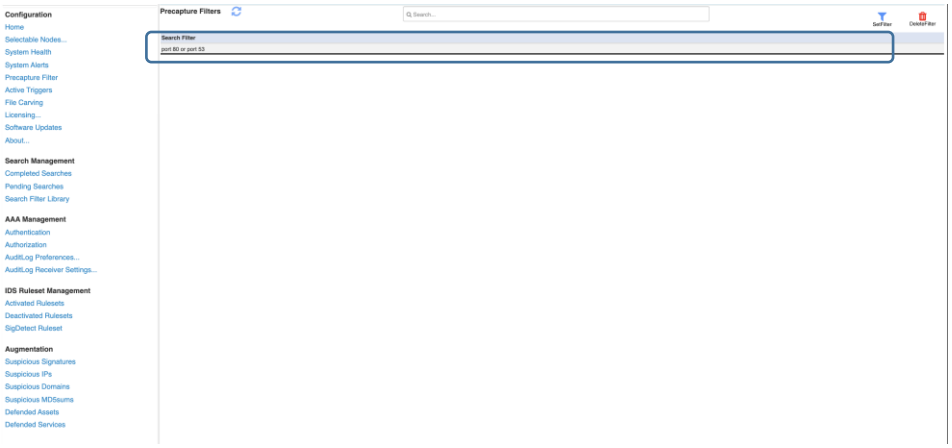
3.1.3 Precapture Filter

By default, all the received traffic is captured and stored. A precapture filter can be applied to receive only the traffic that needs to be captured.



Click on SetFilter button to set a precapture filter. The following filter will result in is capturing traffic that has port 53 or port 80 as either source or destination port.

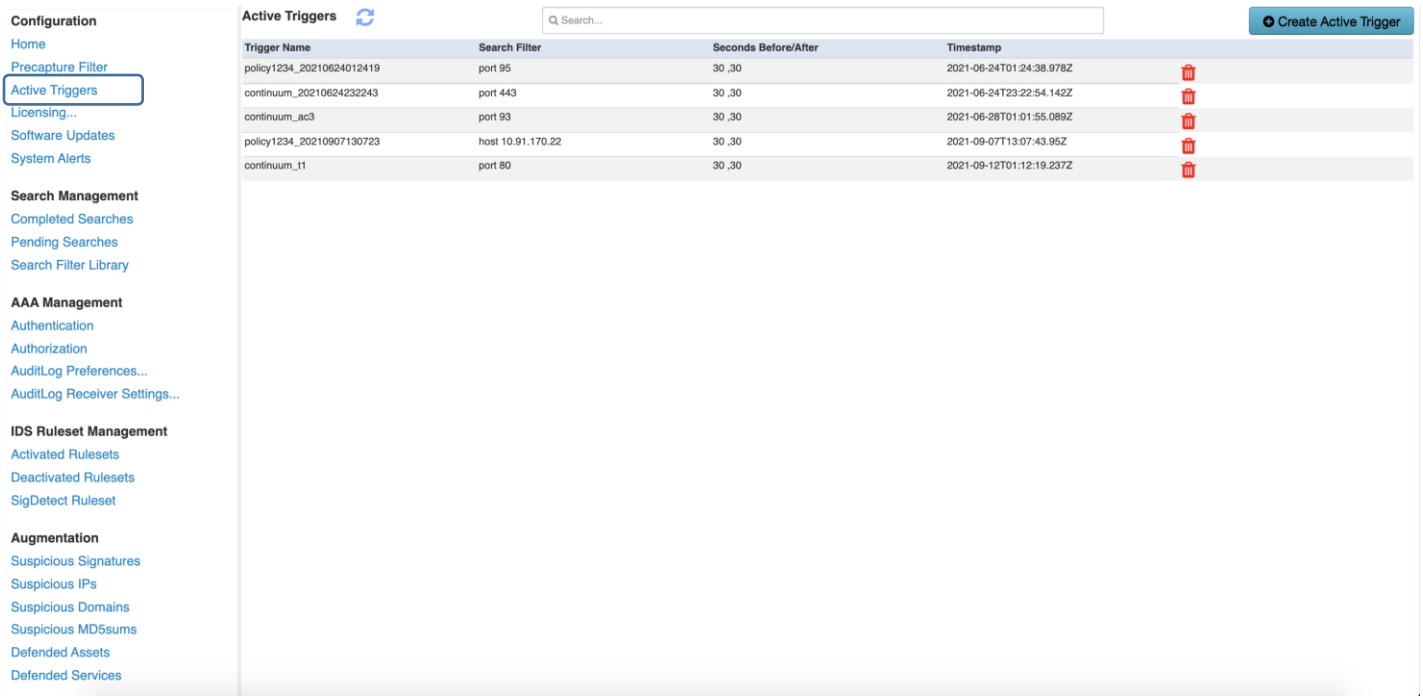



Configuration
Home
Selectable Nodes...
System Health
System Alerts
Precapture Filter
Active Triggers
File Carving
Licensing...
Software Updates
About...
Search Management
Completed Searches
Pending Searches
Search Filter Library
AAA Management
Authentication
Authorization
AuditLog Preferences...
AuditLog Receiver Settings...
IDS Ruleset Management
Activated Rulesets
Deactivated Rulesets
SigDetect Ruleset
Augmentation
Suspicious Signatures
Suspicious IPs
Suspicious Domains
Suspicious MD5sums
Defended Assets
Defended Services
Precapture Filters
Search...
Set Filter
Delete Filter
Search Filter
port 80 or port 53

3.1.4 Active Triggers

Active Triggers offer a simple mechanism to generate alerts based on Berkeley Packet Filter (BPF).

Authorized users can create, view, and delete active triggers. The alerts generated by these triggers have the event_type: **activetrigger**



A user must have a role with Policy permission enabled to be able to create and delete active triggers. Other users can view created triggers.

Active trigger name can only have alphanumeric characters and underscore (_). Duplicate names are not allowed.

Active trigger filter must be a valid BPF filter. It cannot be ip, tcp, udp, tcp or udp as these are trivial filters.

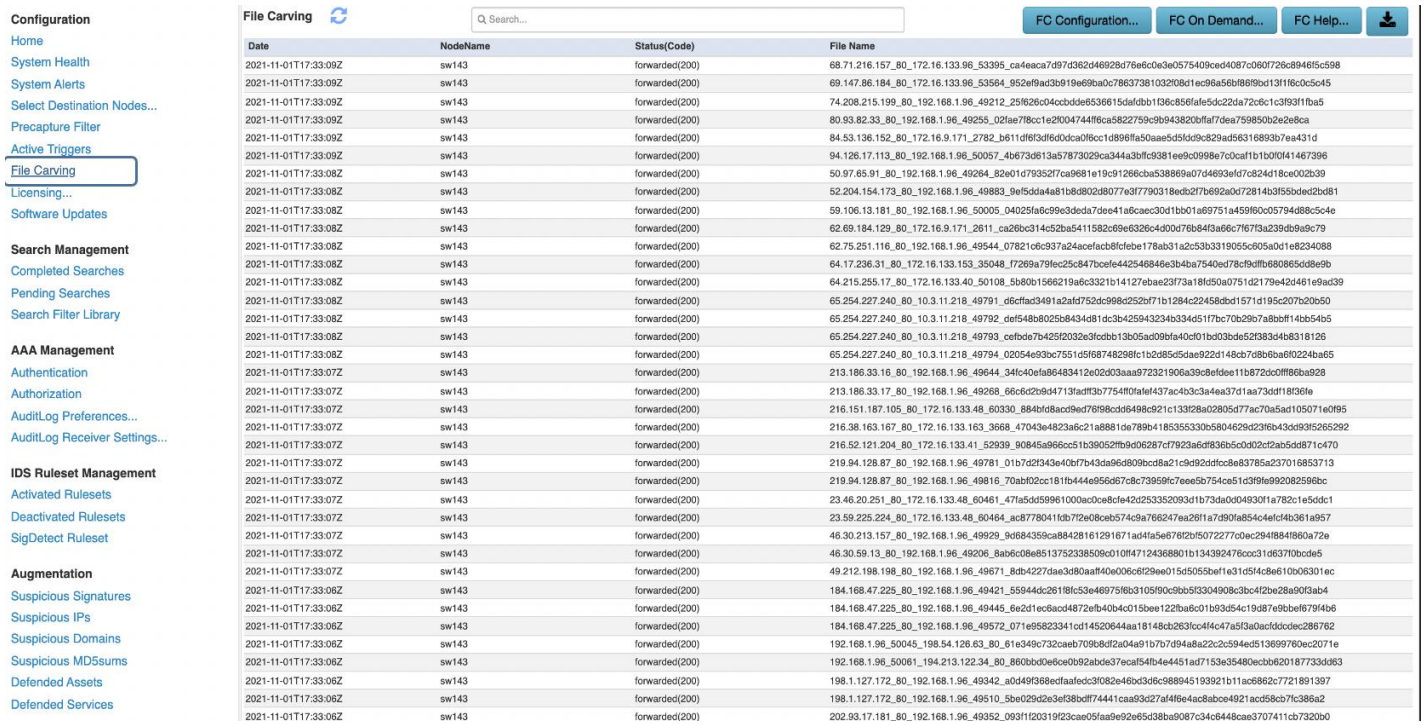
Seconds before and Seconds after fields help avoid active trigger storms if the matches are occurring too frequently.

3.1.5 File Carving

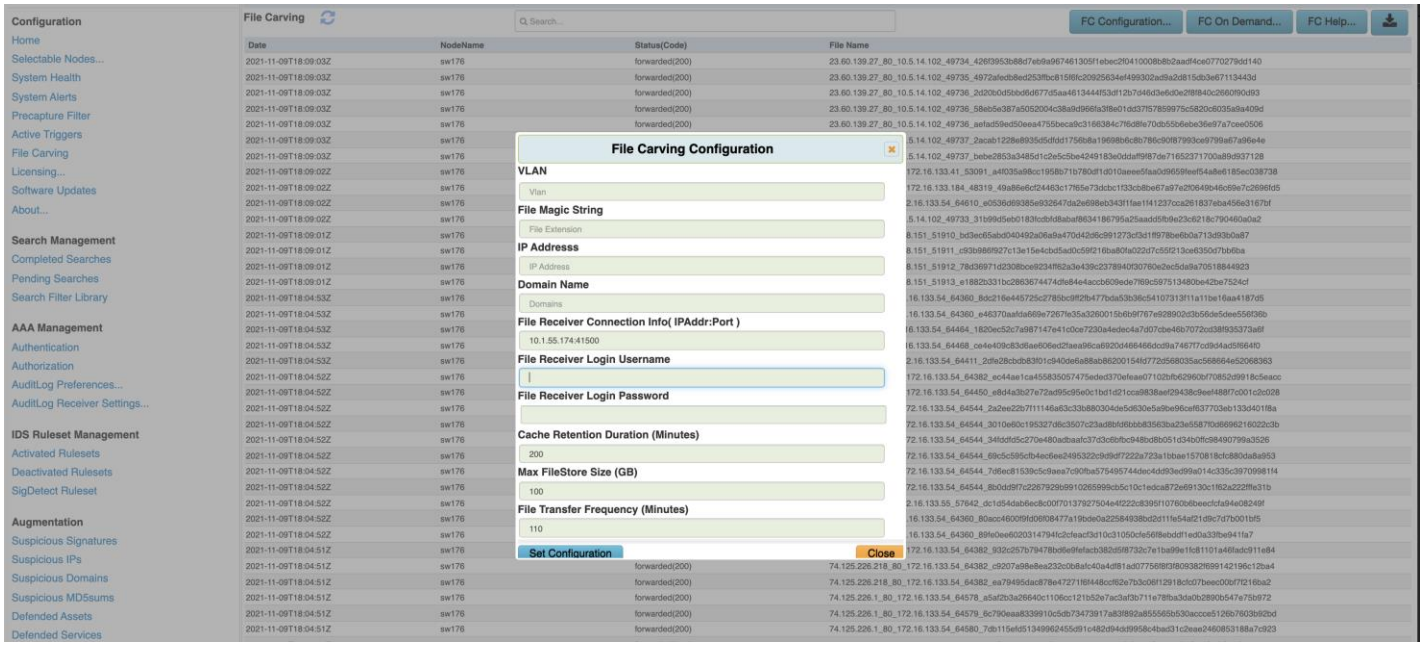
The SentryWire Capture Server extracts files from captured traffic stream and stores them to the disk, based on various configuration parameters. File Carving (**FC**) does not impact capture, indexing, or search performance.

There are three types of FC Workflows:

- Streaming FC Workflow
  Files extracted from traffic stream, de-duplicated and sent to a file handler
- On-demand FC UI Workflow
- On-demand FC REST Workflow



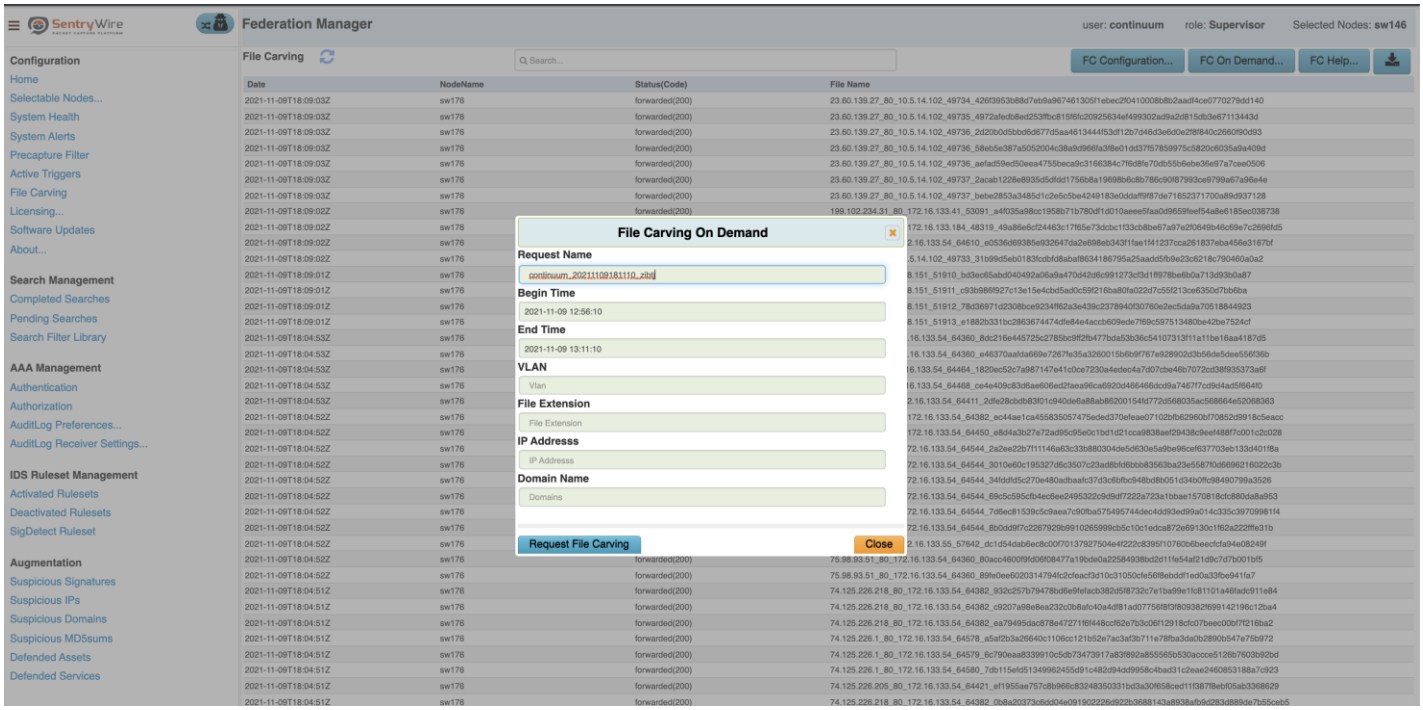
The File Carving configuration for streaming workflow can be updated by clicking on FC Configuration button:



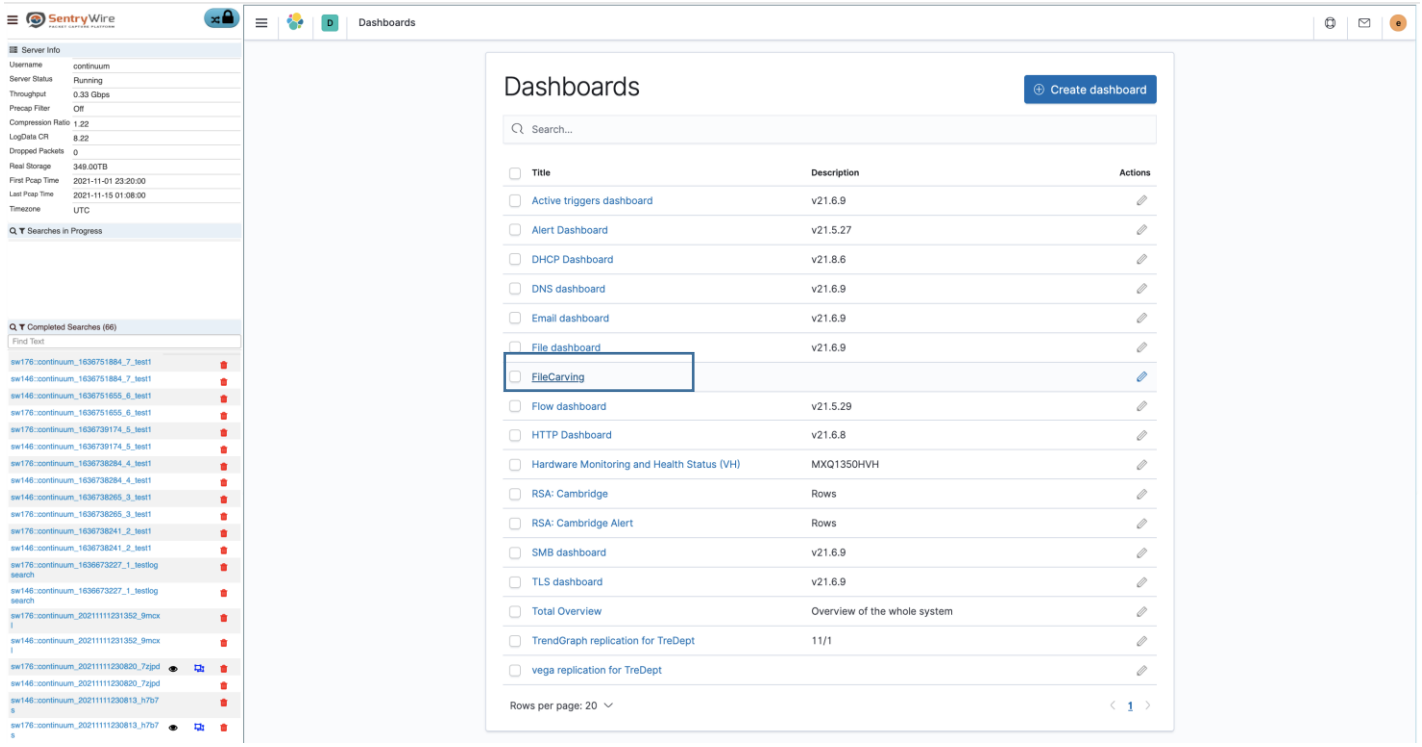
- VLAN list is comma separated. Accepts individual vlans, or ranges.
  Example: 1,17-22,30
- IP Address list is comma separated. Accepts individual addresses, and CIDR

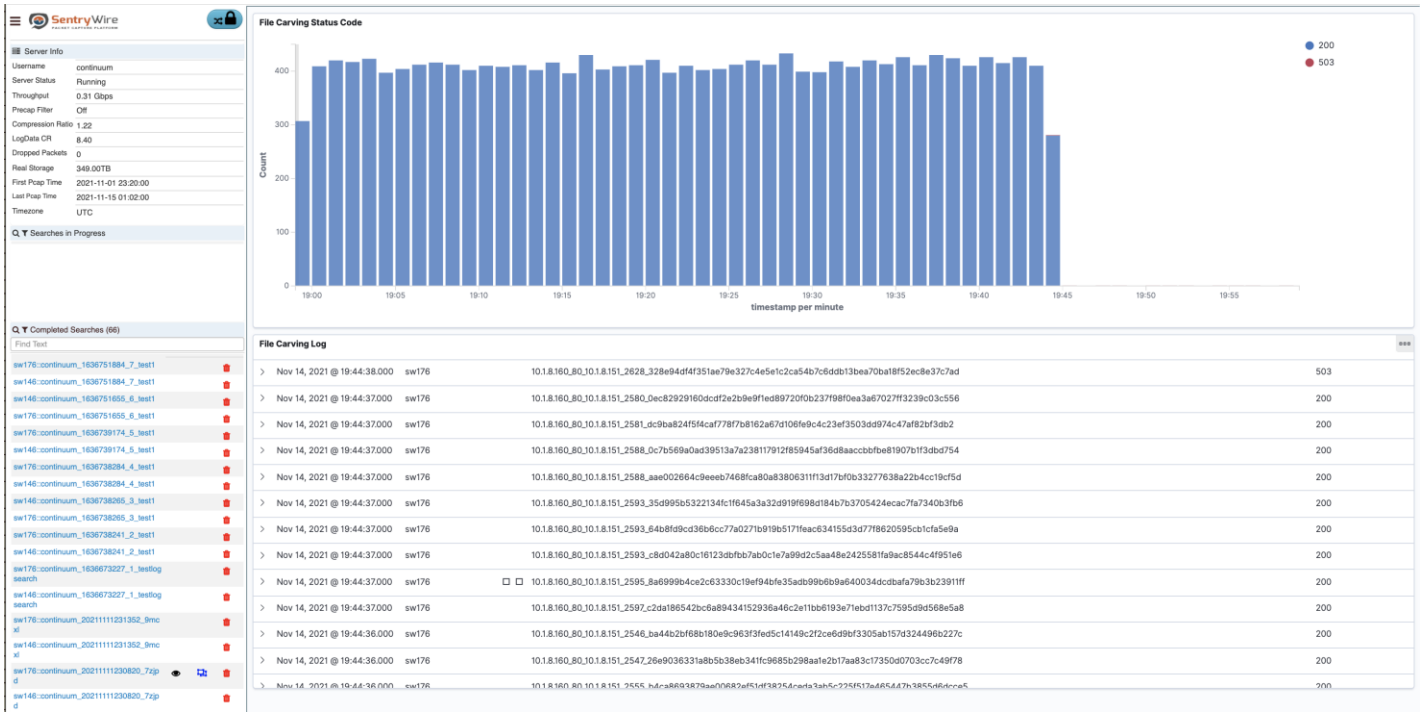
  Example: 10.1.2.3,10.1.1.0/24,11.2.4.100

File Carving on Demand allows users to request files from a specific time period to be sent to an external server.



File Carving is available as a dashboard in Investigator View:



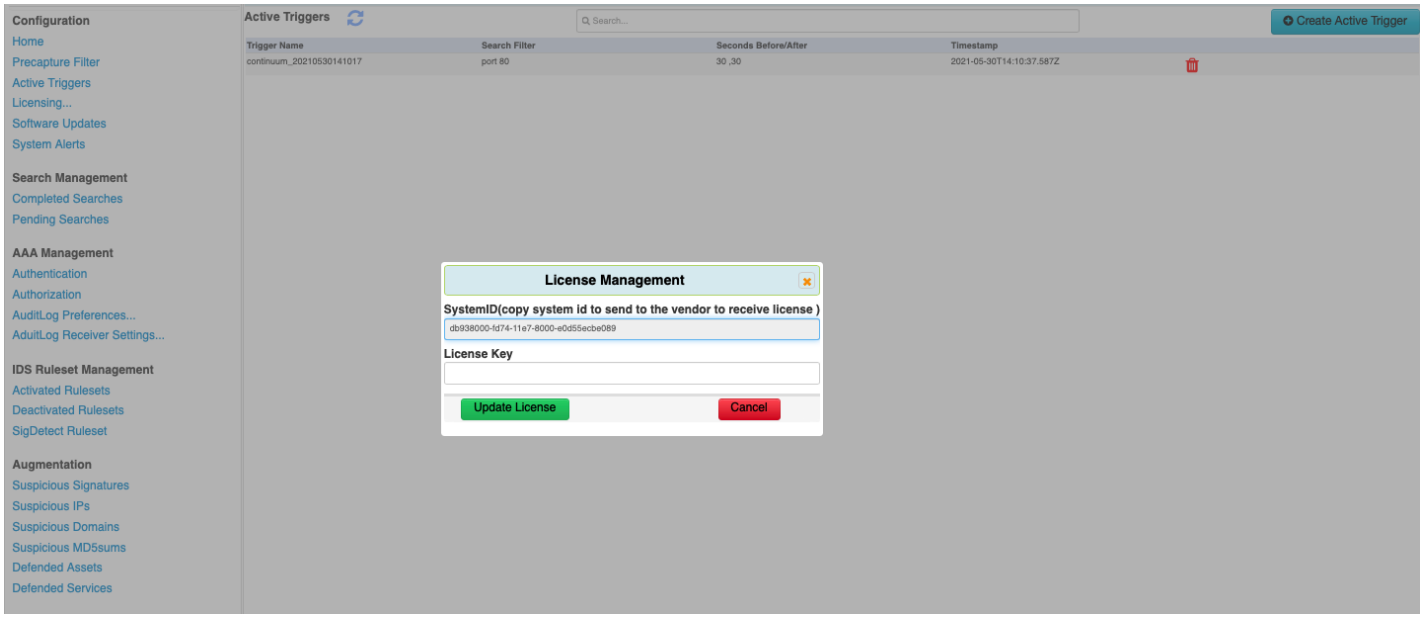

SentryWire
Server Info
Username continuum
Server Status Running
Throughput 0.31 Gbps
Precap Filter Off
Compression Ratio 1.22
LogData CR 8.40
Dropped Packets 0
Real Storage 349.00TB
First Pcap Time 2021-11-01 23:20:00
Last Pcap Time 2021-11-15 01:02:00
Timezone UTC
Searches in Progress
Completed Searches (66)
Find Text
sw176::continuum_1636751884_7_test1
sw146::continuum_1636751884_7_test1
sw146::continuum_1636751655_6_test1
sw176::continuum_1636751655_6_test1
sw176::continuum_1636739174_5_test1
sw146::continuum_1636739174_5_test1
sw176::continuum_1636738284_4_test1
sw146::continuum_1636738284_4_test1
sw146::continuum_1636738265_3_test1
sw176::continuum_1636738265_3_test1
sw176::continuum_1636738241_2_test1
sw146::continuum_1636738241_2_test1
sw176::continuum_1636673227_1_testlog search
sw146::continuum_1636673227_1_testlog search
sw176::continuum_20211111231352_9mcxl
sw146::continuum_20211111231352_9mcxl
sw176::continuum_20211111230820_7zjpd
sw146::continuum_20211111230820_7zjpd
File Carving Status Code
200
503
Count
0
100
200
300
400
19:00
19:05
19:10
19:15
19:20
19:25
19:30
19:35
19:40
19:45
19:50
19:55
timestamp per minute
File Carving Log
Nov 14, 2021 @ 19:44:38.000 sw176 10.1.8.160_80_10.1.8.151_2628_328e94df4f351ae79e327c4e5e1c2ca54b7c6ddb13bea70ba18f52ec8e37c7ad 503
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2580_0ec82929160dcdf2e2b9e9f1ed89720f0b237f98f0ea3a67027ff3239c03c556 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2581_dc9ba824f5f4caf778f7b8162a67d106fe9c4c23ef3503dd974c47af82bf3db2 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2588_0c7b569a0ad39513a7a238117912f85945af36d8aaccbbfbe81907b1f3dbd754 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2588_aae002664c9eeeb7468fca80a83806311f13d17bf0b33277638a22b4cc19cf5d 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2593_35d995b5322134fc1f645a3a32d919f698d184b7b3705424ecac7fa7340b3fb6 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2593_64b8fd9cd36b6cc77a0271b919b5171feac634155d3d77f8620595cb1cfa5e9a 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2593_c8d042a80c16123dbfbb7ab0c1e7a99d2c5aa48e2425581fa9ac8544c4f951e6 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2595_8a6999b4ce2c63330c19ef94bfe35adb99b6b9a640034dcdbafa79b3b23911ff 200
Nov 14, 2021 @ 19:44:37.000 sw176 10.1.8.160_80_10.1.8.151_2597_c2da186542bc6a89434152936a46c2e11bb6193e71ebd1137c7595d9d568e5a8 200
Nov 14, 2021 @ 19:44:36.000 sw176 10.1.8.160_80_10.1.8.151_2546_ba44b2bf68b180e9c963f3fed5c14149c2f2ce6d9bf3305ab157d324496b227c 200
Nov 14, 2021 @ 19:44:36.000 sw176 10.1.8.160_80_10.1.8.151_2547_26e9036331a8b5b38eb341fc9685b298aa1e2b17aa83c17350d0703cc7c49f78 200

3.1.6 Licensing

1. Contact your Security representative to obtain a license key for the Federation Manager.

   Note:

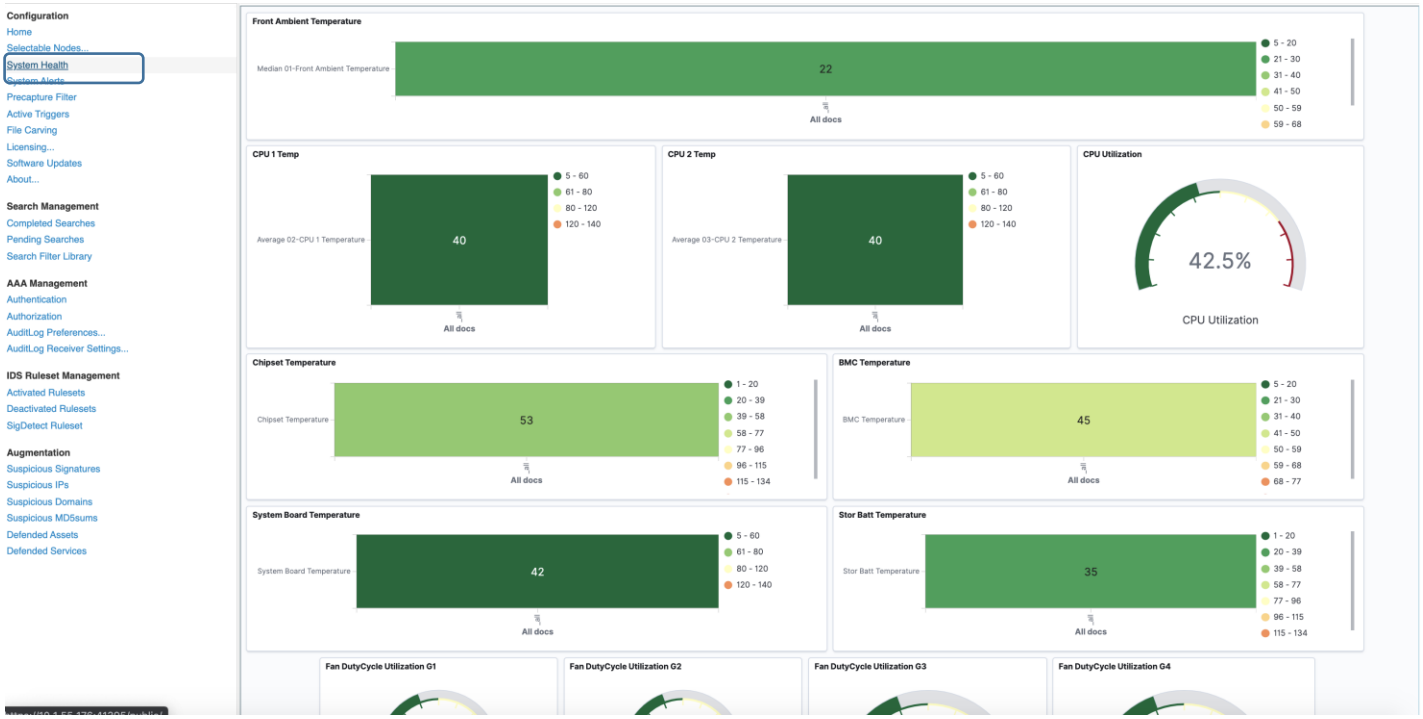
   - System Id is required to obtain a valid license key.
   - Only Admin or authorized users, can apply the license key.
2. Once a license key has been forwarded, copy and paste the provided string into the License Key text box in the web user interface.
3. Click “Update License” button to apply the new license.



Note: A user must have a role with licensing permission enabled to be able update software license.

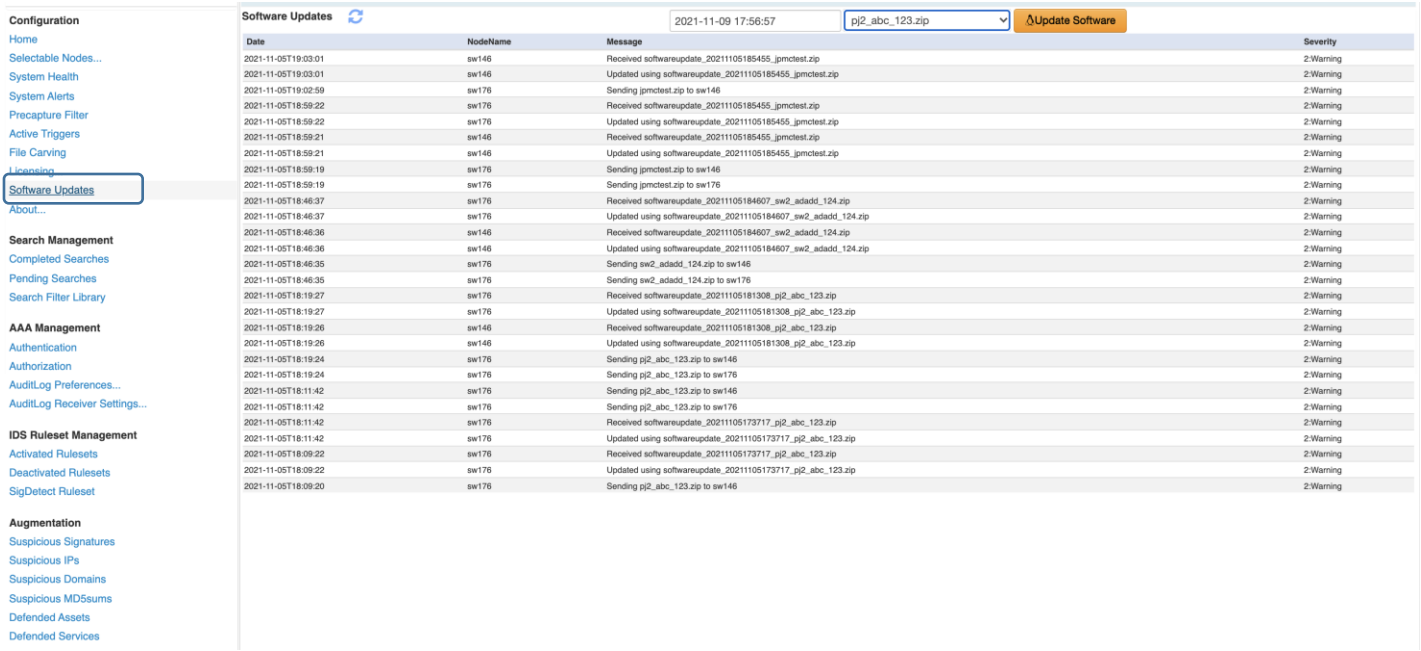
3.1.7 System Health

System Health dashboard shows various system monitoring details of the Federation Manager system.



3.1.8 Software Updates

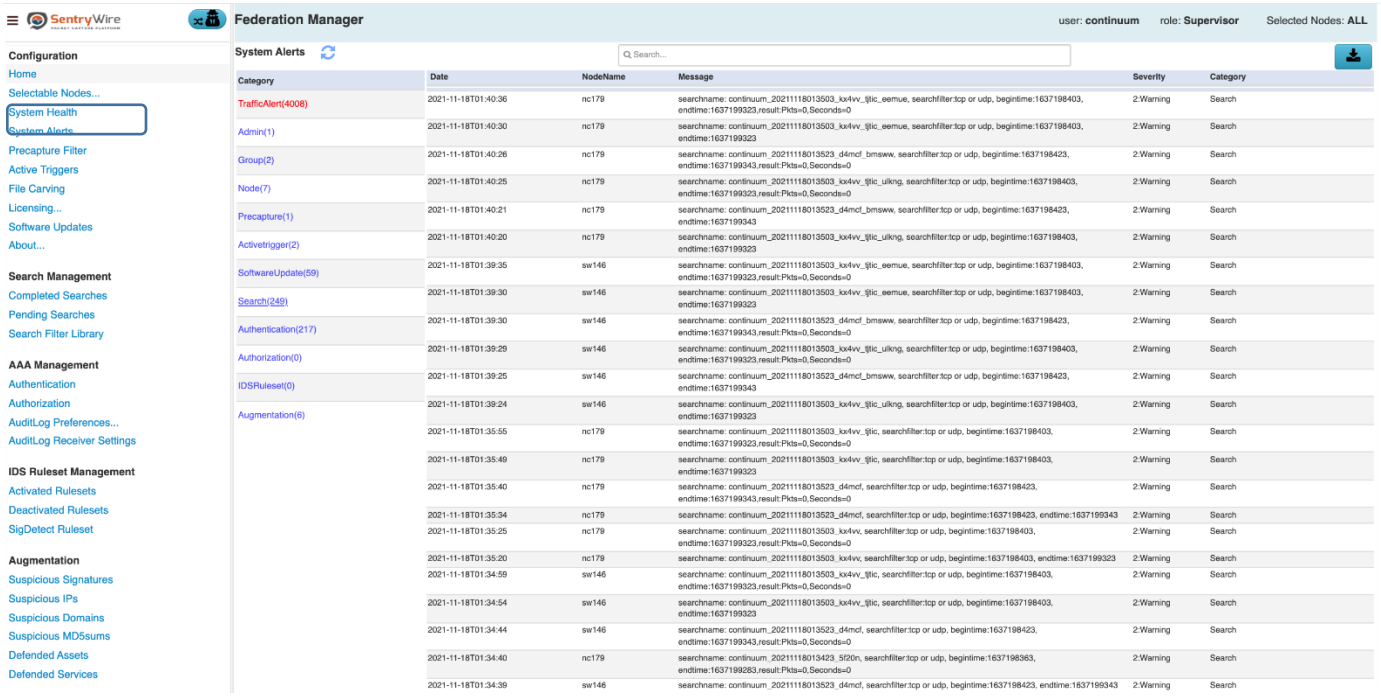
This page allows the user to perform FM license update, software updates and reboot/shutdown Federated Nodes. The software updates are specific to the Federation Manager and its nodes. Each software update must be made available in a specific folder accessible to the Federation Manager server. Authorized users can select the date and time of the software to be installed.



A user must have a role with Policy permission enabled to be able update software. Each package is a zip file that contains an installer script, a version.txt file, and a tgz file with all the files necessary files for completing the software update. Software update alerts are shown on this page when the update is scheduled to run, when it is running and the result of the update on each node.

3.1.9 System Alerts

This page shows system alerts from all the Federated Nodes. Severe alerts are displayed in descending order above all the alerts of other severity.



The search bar allows narrowing down alerts by date, nodename, severity, category, and terms inside the message. Any authorized user can download System Alerts. These cannot be deleted.

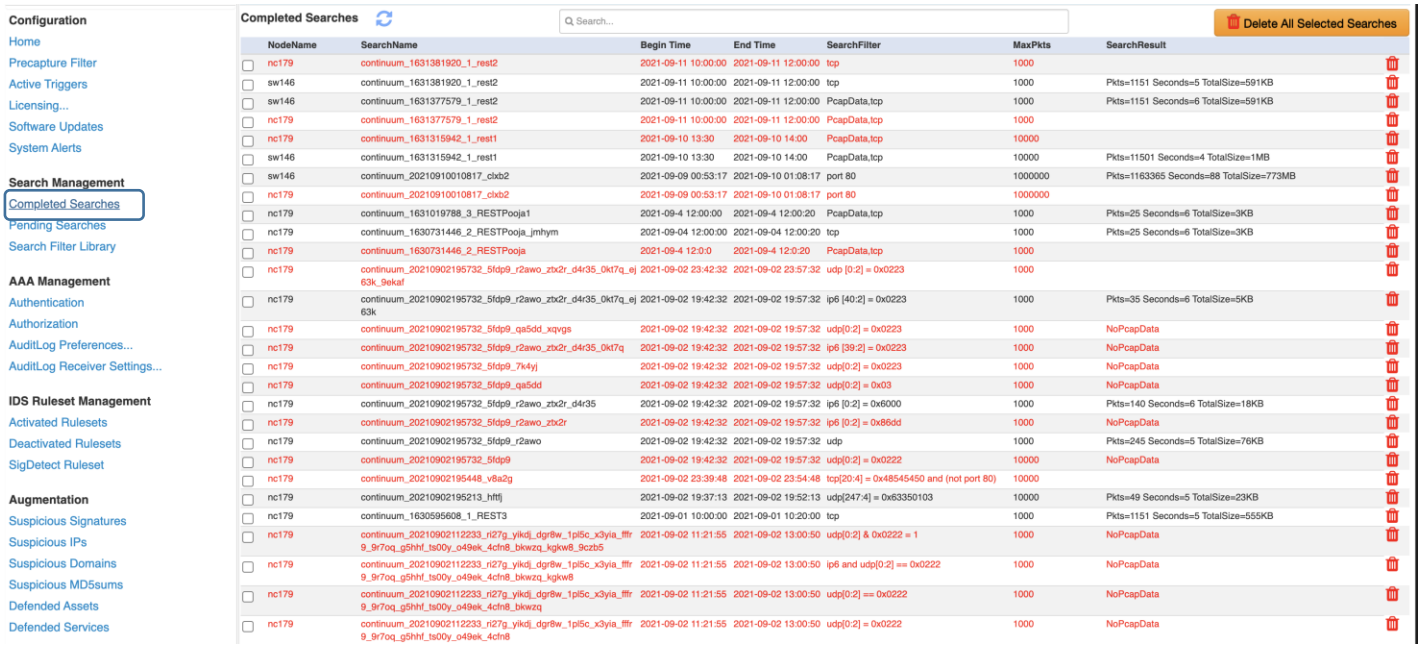
3.2 SEARCH MANAGEMENT

Investigator UI allows users to create a search, view packets, download data and clone a search.

FM Admin UI allows authorized users to delete multiple searches at a time.

3.2.1 Completed Searches

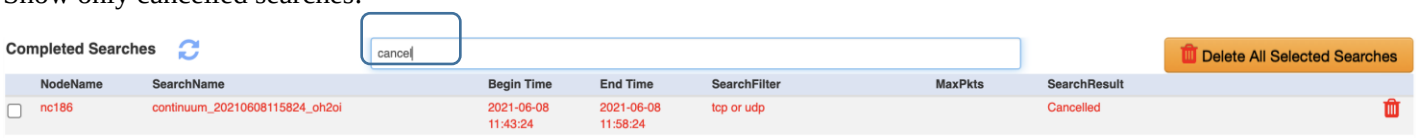
Completed searches from all the Federated Nodes are displayed on this page. Search name contains name of the user who created the search. Each node's search returns different set of packets; therefore, they are represented as a separate line.



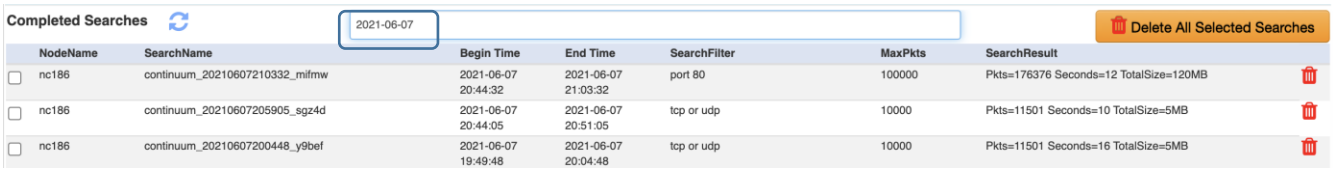
The Search bar is critical in narrowing down the results to view and delete searches.

Few examples of the search bar usage:

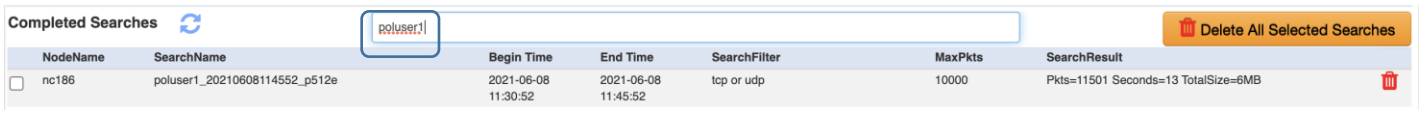
Show only cancelled searches:



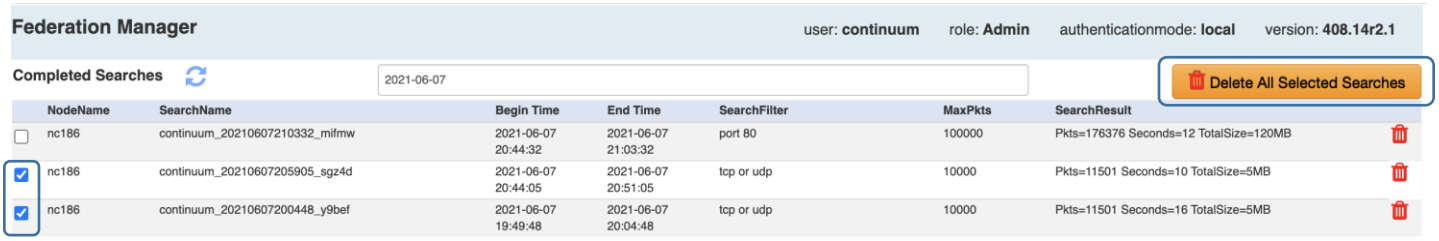
Show searches that were done on a particular day:



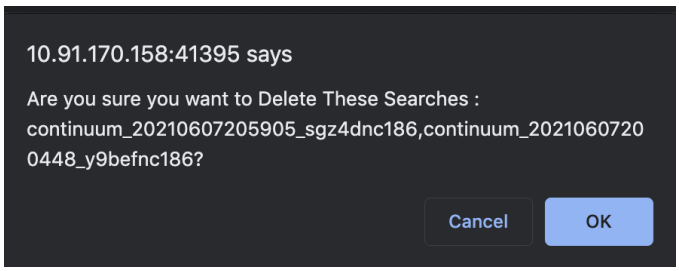
Show searches of a particular user:



Once searches are narrowed down as shown above, user can select one or more of the searches and click on Delete All Selected Searches button to delete them:

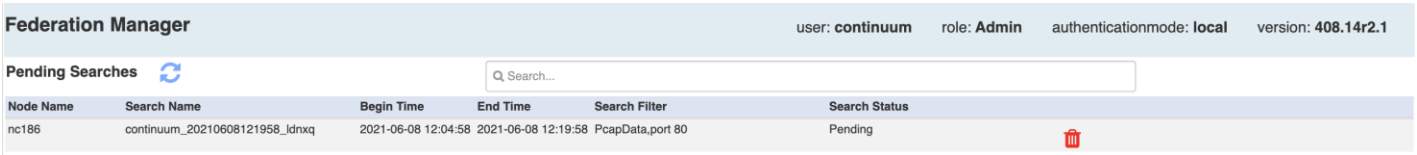


User is asked to confirm the selected list of searches to be deleted:



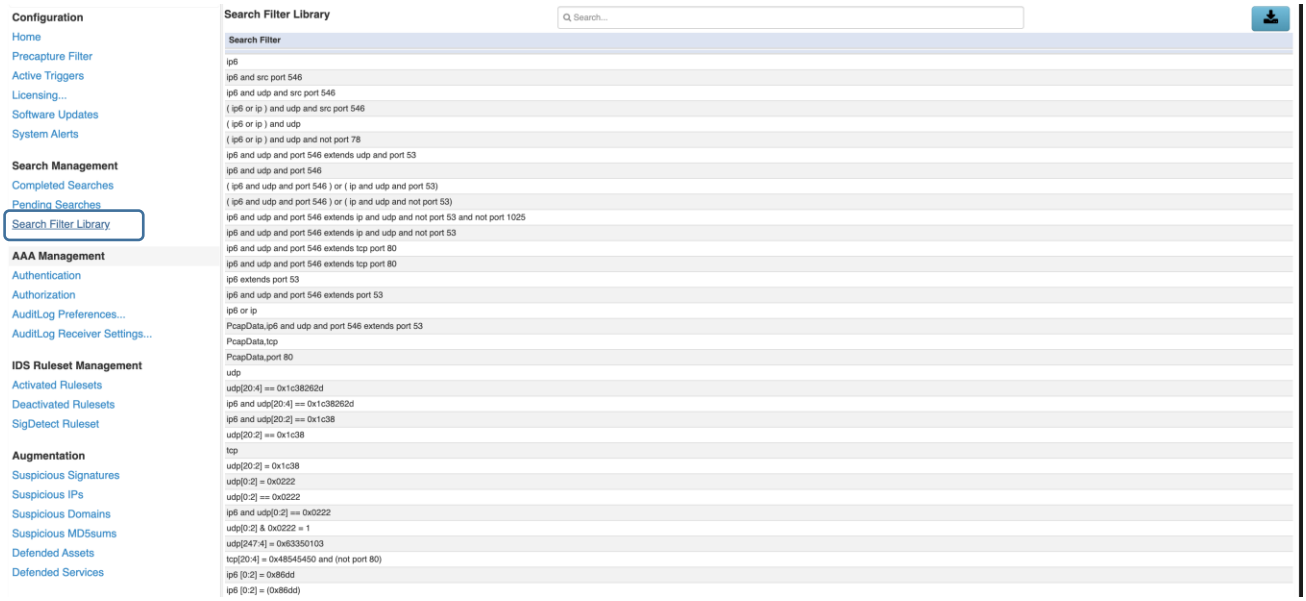
3.2.2 Pending Searches

This page shows all the searches that are currently queued or in progress. A search on this page can be cancelled. A cancelled search moves to Completed Searches page from which it can be removed. The search bar allows users to narrow down the pending searches. Pending searches can be cancelled one at a time.


Federation Manager
user: continuum
role: Admin
authenticationmode: local
version: 408.14r2.1
Pending Searches
Search...
Node Name
Search Name
Begin Time
End Time
Search Filter
Search Status
nc186
continuum_20210608121958_ldnxq
2021-06-08 12:04:58
2021-06-08 12:19:58
PcapData,port 80
Pending

3.2.3 Search Filter Library

This page shows the list of unique search filters from previous searches. These can be downloaded but not be deleted.

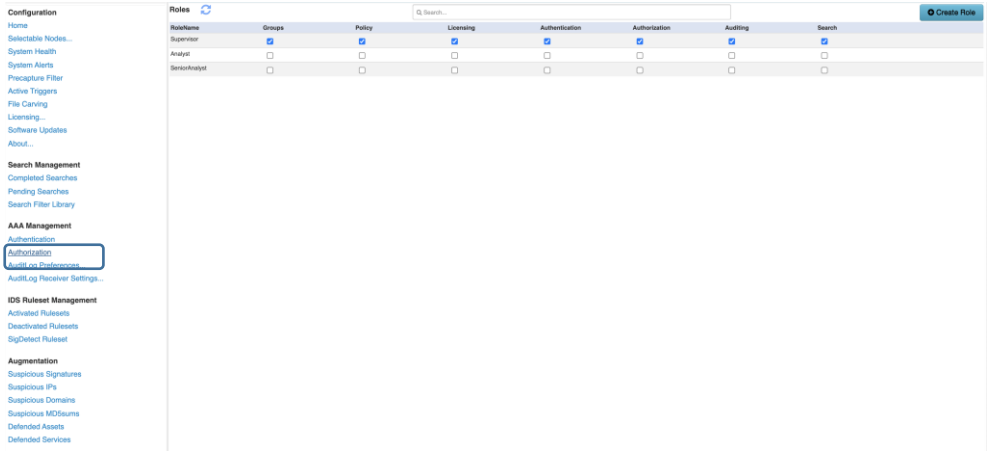


3.3 AAA MANAGEMENT

This group of menu items allows users to handle Authentication, Authorization and Auditing

3.3.1 Authorization

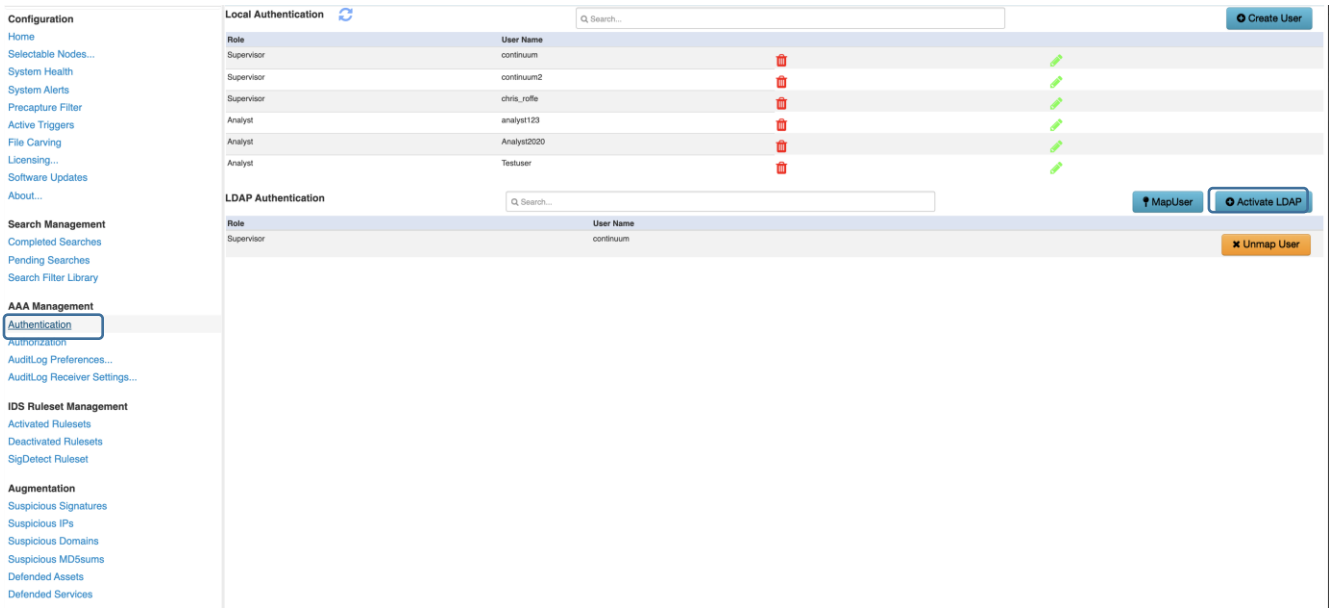
Authorization page allows creating new roles and setting permissions for each role. When a user is assigned a role, the FM UI actions are enabled/disabled based on the permissions of the role. Once created, these roles are provided as a dropdown list for each of the authentication modes under the Authentication tab and can be assigned to a user at the time of user creation or role mapping.



To add a role, click on the “Create Role” button at the top right of the panel. The above picture shows several roles created each with a specific permission. Each role can have multiple permissions.

3.3.2 Authentication

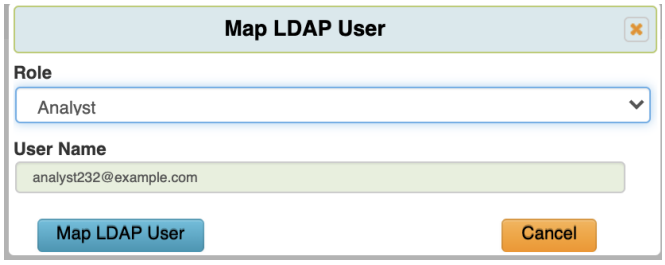
This page allows users to create, delete or update local users, map LDAP users to available roles.



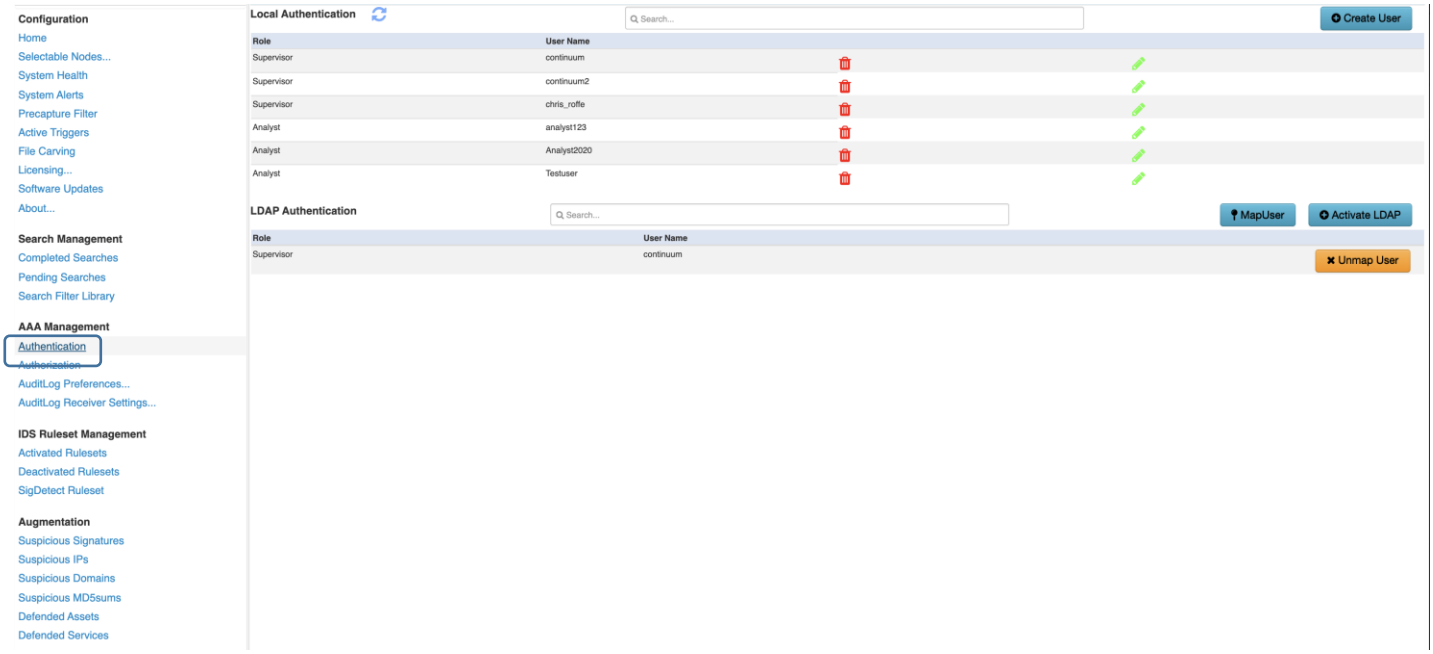
Local Authentication:
By default, FM and its nodes are in Local Authentication Mode. In this mode, users can login with a valid username and password maintained on the FM server.

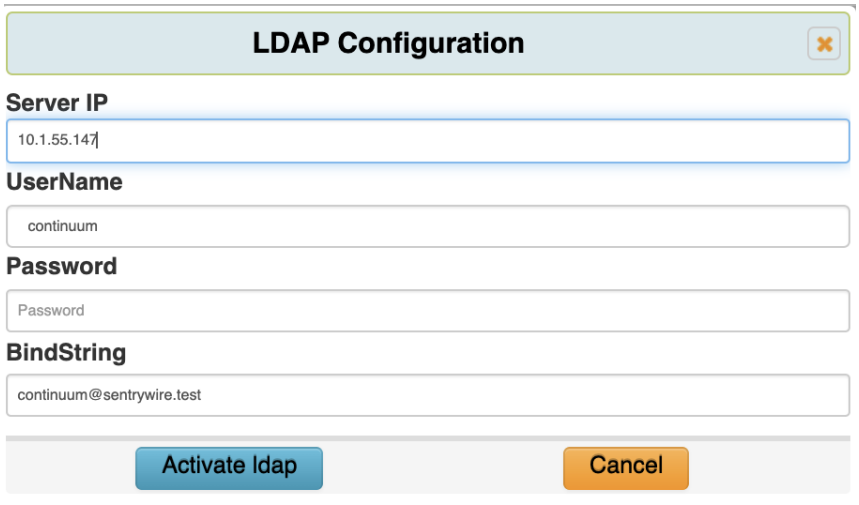
LDAP Authentication:
The image also shows LDAP Authentication section. One or more LDAP users must be mapped to FM Roles before activating LDAP authentication mode.

MapUser allows an LDAP user to be mapped to a FM role. The above image shows one LDAP user mapped user named continuum mapped to Supervisor role. Each mapped user is assigned their mapped role on logging in. An LDAP user is not allowed to login if there is no mapping enabled for that user. Click on the MapUser button to map a new LDAP user to a FM role. Select a role from the drop down, enter user name, click on Map LDAP User button.



LDAP authentication mode must be activated before being able to login using one of the mapped LDAP users. Click on Activate LDAP button to see LDAP Configuration dialog box.

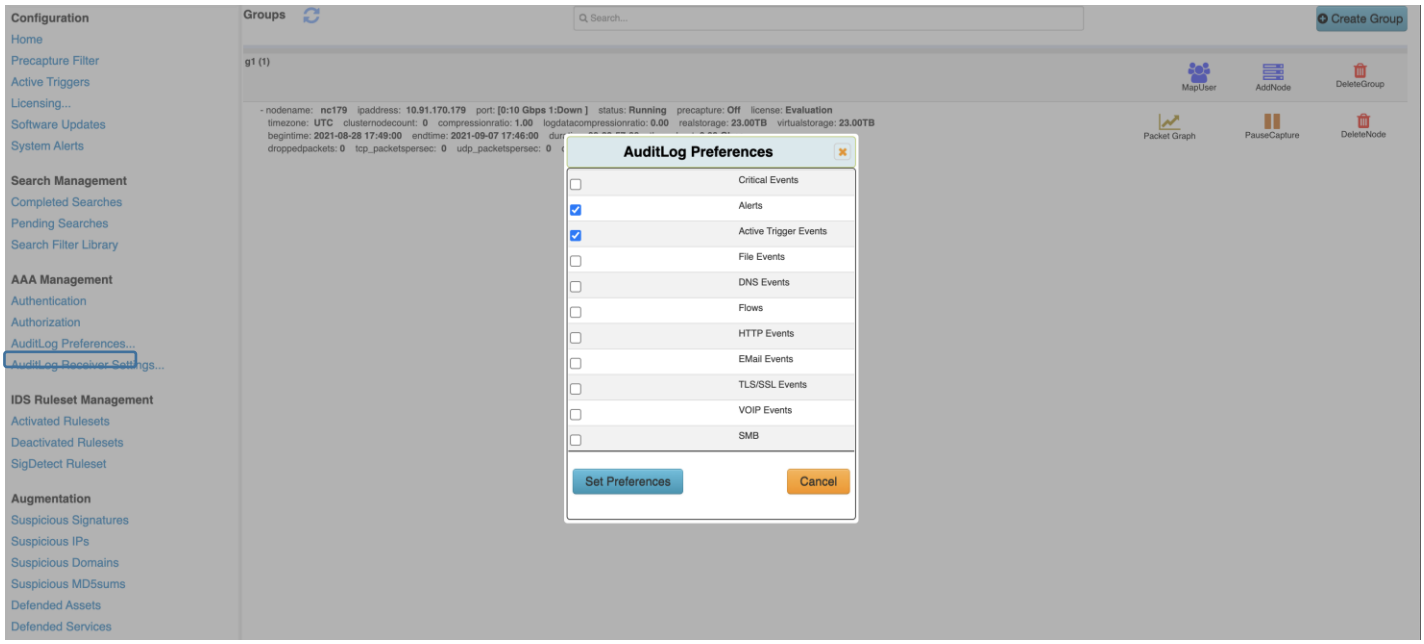




Once LDAP mode is activated successfully, the user must logout and log back in with valid LDAP credentials.

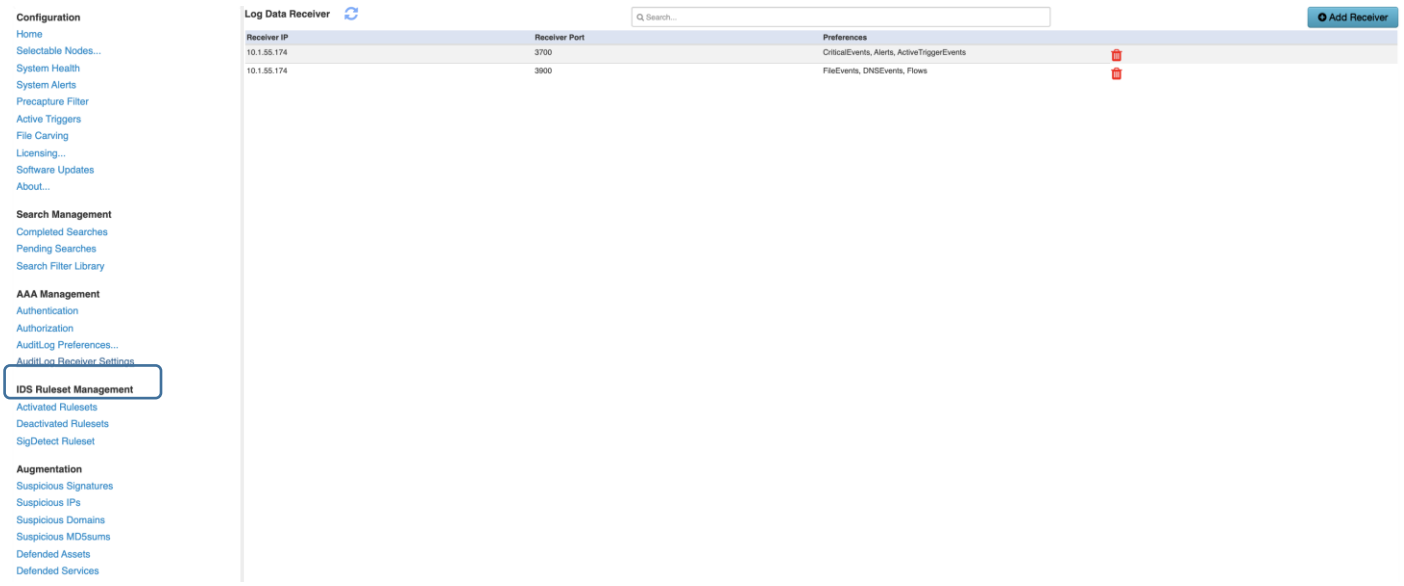
3.3.3 Auditlog Preferences

Logs of various event types are generated by the capture and analytics servers. Auditlog Preferences dialog box allows users to indicate which of the logs must be made available to the external applications such as Splunk.

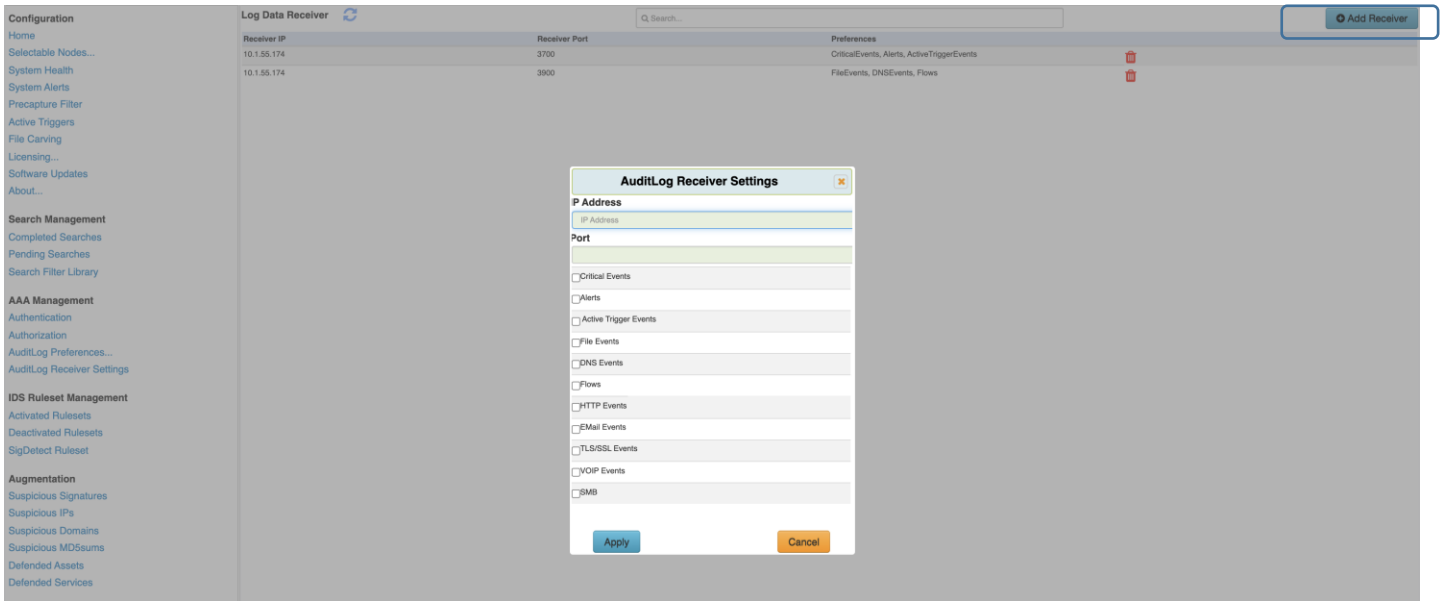


3.3.4 Auditlog Receiver Settings

These settings will allow the server to forward logs to be pushed to an external server running at the IPAddress:Port. The frequency of forwarding is once every 5 minutes by default. The receiver must be able to receive .zip files.



Multiple AuditLog Receivers can be active simultaneously. Each receiver can receive logs of different types. To add a new AuditLog Receiver, click on Add Receiver button, enter new receiver's IP Address and Port, select the event types to be forwarded, and click on Save button.



3.4 IDS RULESET MANAGEMENT

IDS Rulesets are list of extensive rules (signatures). The user also has the privilege to upload user defined rulesets based on their specific needs. The format of these rulesets can be found at https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html

This group has the menu options to upload, activate, deactivate and delete IDS Rulesets and SigDetect Rulesets.

- Activated Rulesets

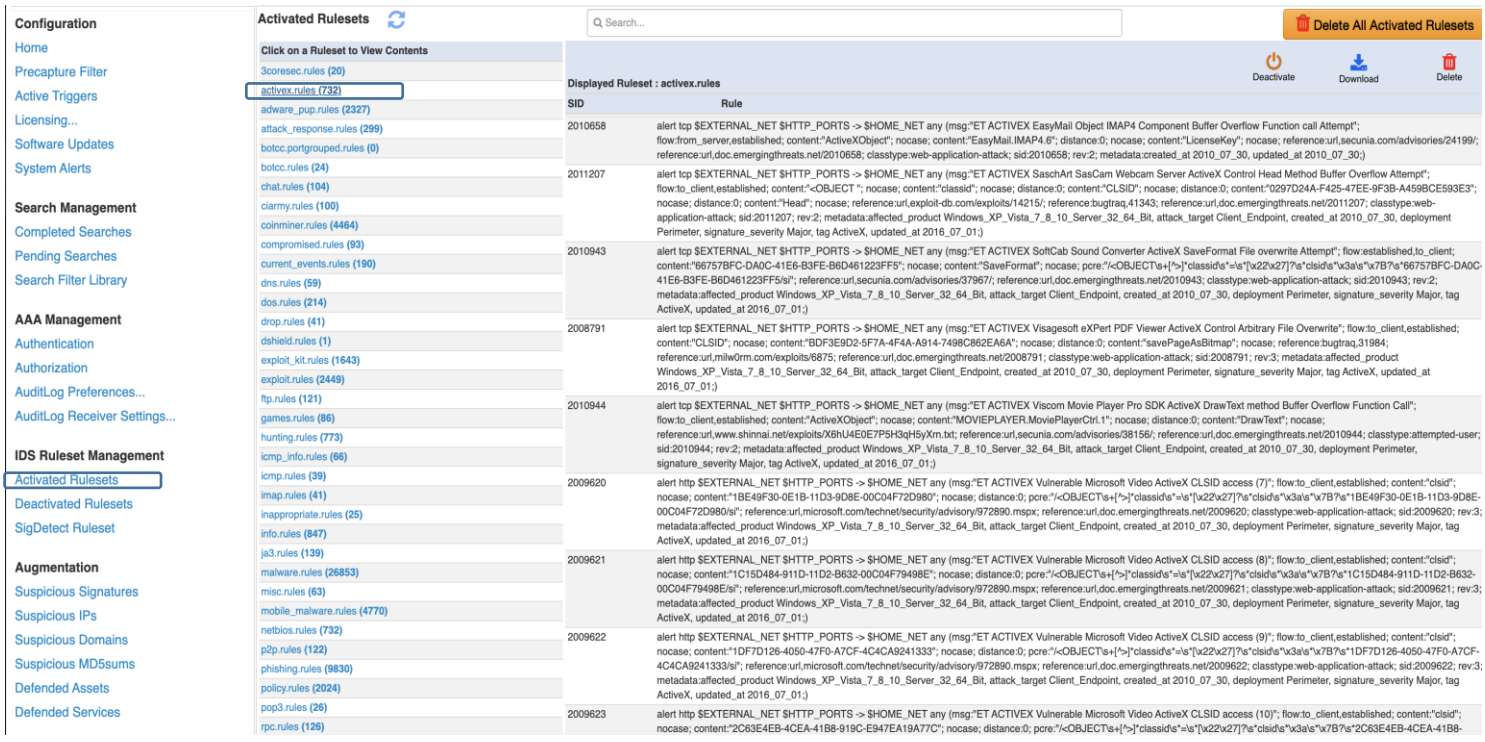
- Deactivated Rulesets
- SigDetect Rulesets

When an IDS ruleset is uploaded, it is part of the Deactivated Rulesets. The newly uploaded ruleset must be activated before its rules are made available to the server. If the uploaded ruleset has the same name as a ruleset that has already been uploaded, the new ruleset replaces the old ruleset.

3.4.1 Activated Rulesets

This page allows authorized users to view activated IDS Rulesets, deactivate rulesets to stop alerts from being generated.

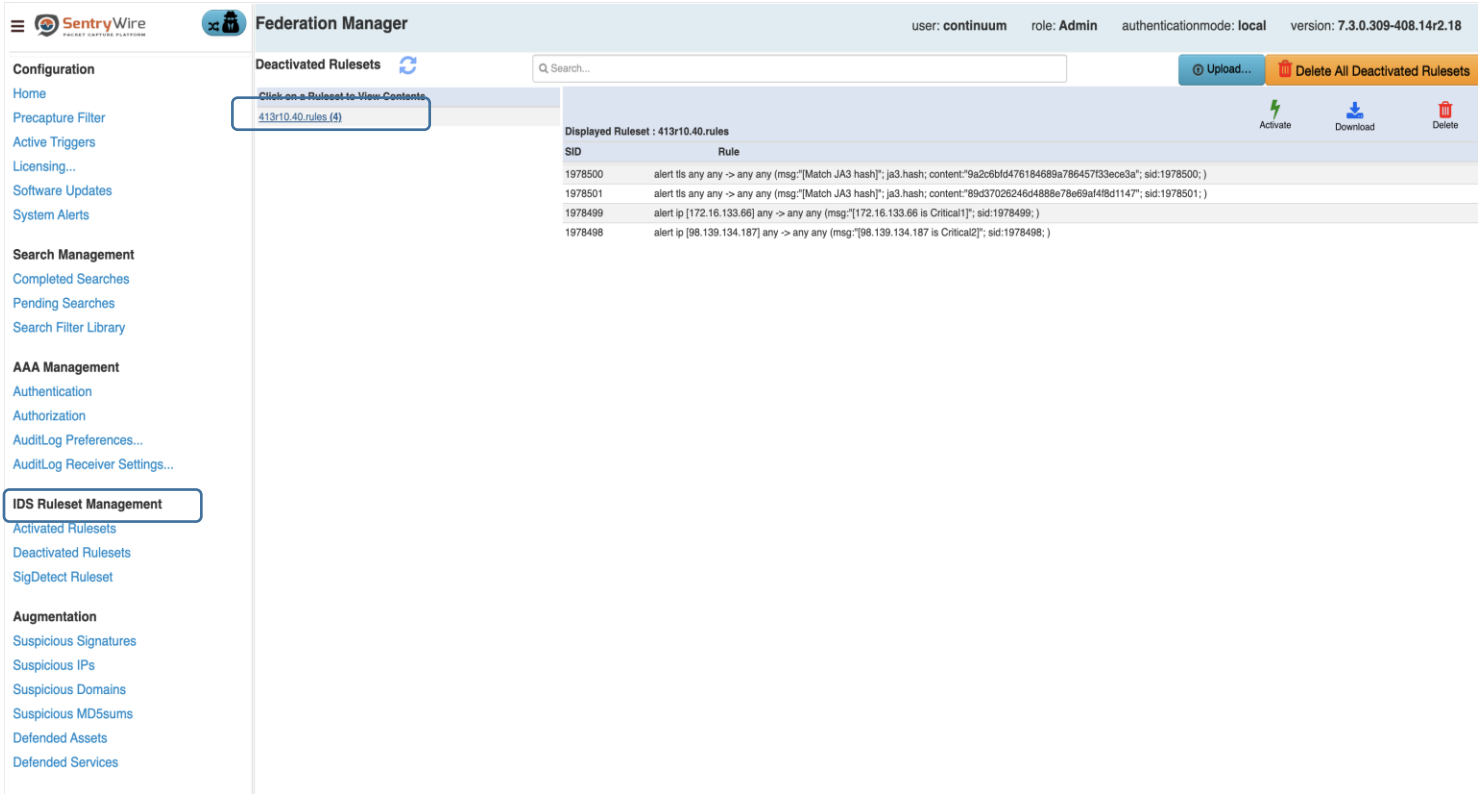
- Click on a activated ruleset to see its contents. The following image shows contents of a ruleset named activebunk2.rules file.
- Select a ruleset and click on Deactivate button. This ruleset will move to Deactivated Rulesets page. Each node removes the new ruleset from Suricata alert generation.
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset.



3.4.2 Deactivated Rulesets

This page allows authorized users to upload new IDS rulesets. The following image shows one such uploaded rulesets.

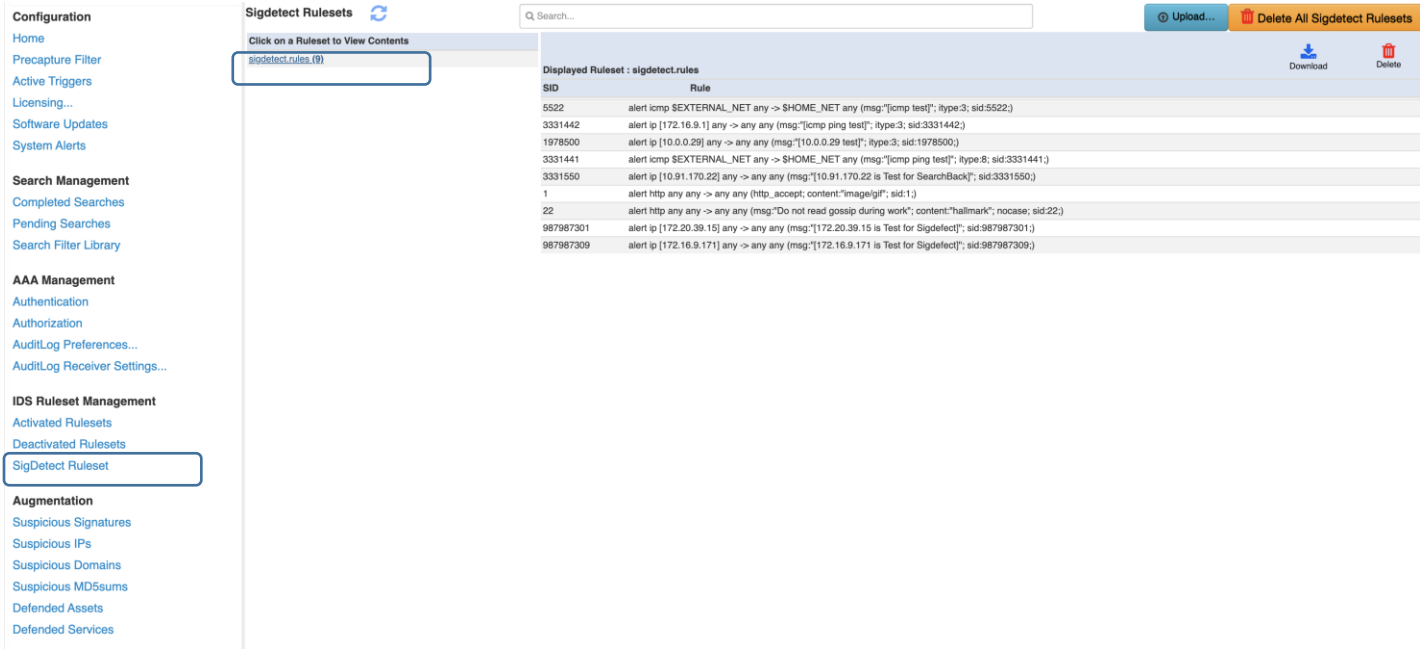
- Click on a deactivated ruleset to see its contents. The following image shows contents of a ruleset named 413.10.40.rules
- Select a ruleset and click on Activate button. This ruleset will move to Activated Rulesets page. Each node adds the new ruleset for Suricata alert generation.
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset.



3.4.3 SigDetect Ruleset

SigDetect Rulesets are used to generate alerts on pcap data of search. Once a search is complete, the server makes the all the uploaded SigDetect rules at the time of the search completion to Suricata for alert generation. This allows checking for alerts for signatures that were not available when the traffic was originally captured.

- Click on a SigDetect ruleset to see its contents. The following image shows contents of a ruleset named sigdetect.rules
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset. These rules will not be part of any future searches.



Once a search is completed, any Suricata alerts found for the search's pcap data are stored in sigdetect.json file.

3.5 AUGMENTATION

Augmentation allows users to upload additional data that can be used to enhance the value of stored data and allow data correlation. Augmentation has 6 menu items. The workflow and the interaction of each of the options in this section are like one another.

- Suspicious Signatures
- Suspicious Ips
- Suspicious Domains
- Suspicious MD5sums
- Defended Assets
- Defended Services

Only those users that have a role with Policy permission can upload augmentation data. Any authorized user can download augmentation data.

Authorized users can upload () a csv file for each of the augmentation types mentioned above. Each line contains a valid entry of the item being uploaded, a comma, and an optional description of this line's item. An example csv file for Suspicious IP Addresses is shown below:

110.22.34.24,suspip3424

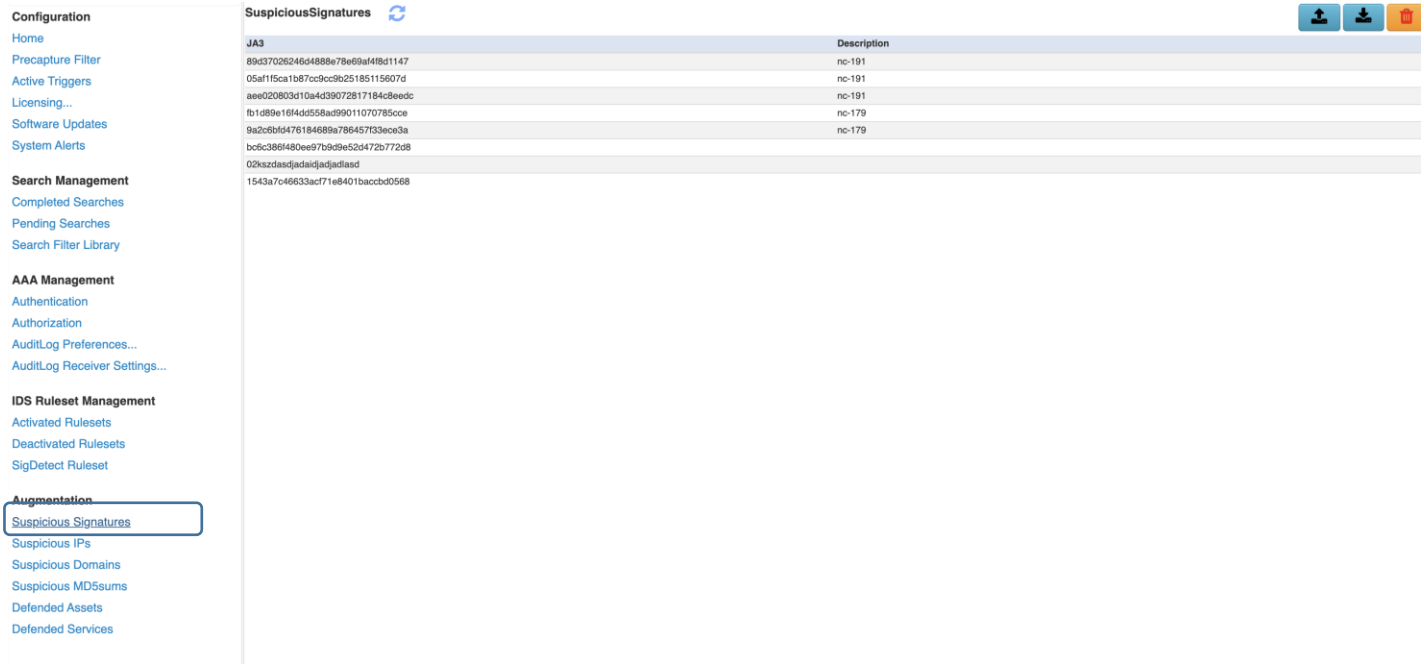
10.1.8.0/24,cidr test

When an event's source/destination IP Address either matches a suspicious IP Address or part of a suspicious CIDR block, the event's ioc field is augmented with the custom data uploaded. For example, the following image shows the augmented ioc value on matching an IP Address from 10.1.8.0/24 CIDR Block:

Time	src_ip	dest_ip	suspected	nodename	ioc
Nov 14, 2021 @ 11:29:59.303282000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.303274000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293695000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293672000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038037000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038025000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636885000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636874000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636579000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636568000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151

3.5.1 Suspicious Signatures

This shows the list of currently uploaded suspicious JA3 signatures. When a TLS event matches one of these signatures, that event is marked as **suspected**.



Authorized users can upload () new suspected signatures as a csv file with each line containing a ja3 signature, a comma, and an optional description of the signature. Each line of the csv file must have a JA3. Description of the JA3 is

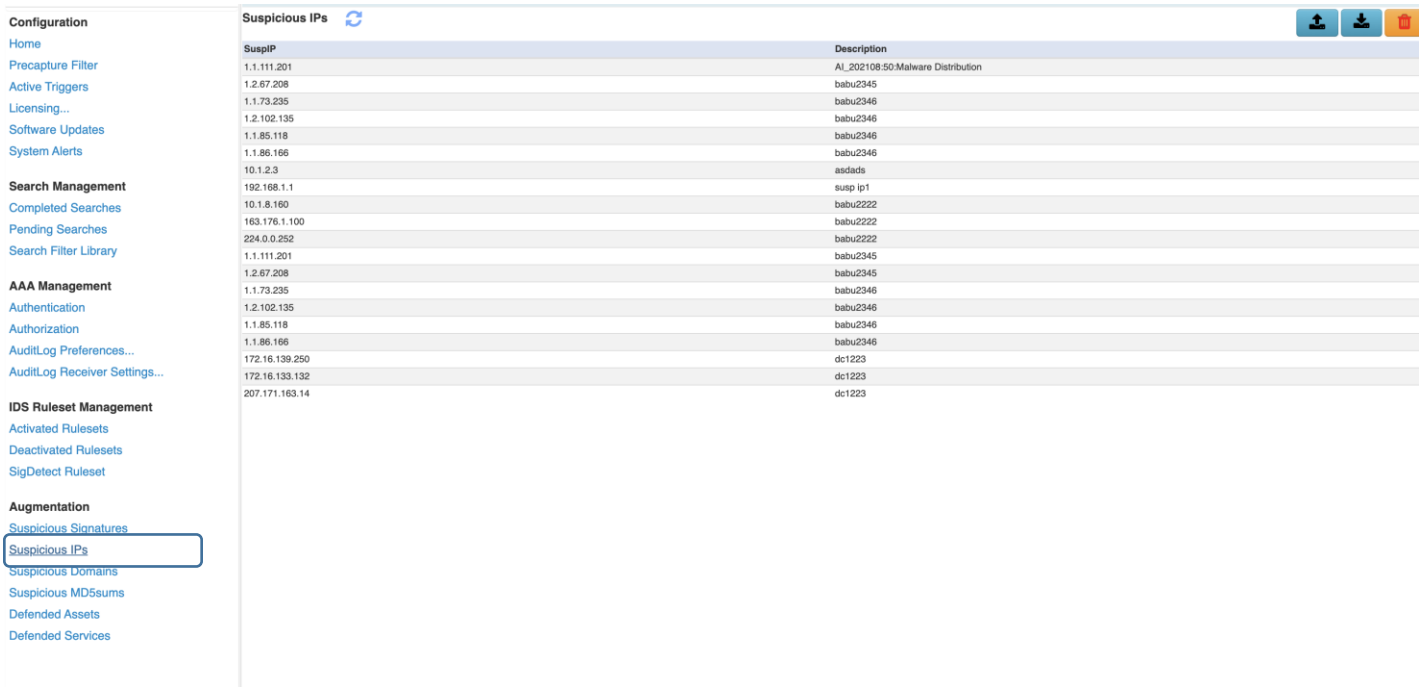
optional. If Description is provided, JA3 and Description values must be separated by comma. A sample csv file is shown below:

```
4192c0a946c5bd9b544b4656d9f624a4,db4
Acb741bcdffb787c5a52654c78645bdf
e1691a31bfe345d2692da75636ddfb00,deedeefbzero
```

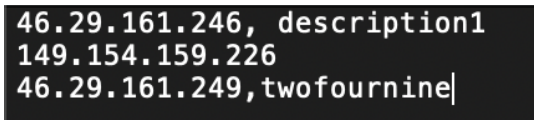
Currently available signatures can be downloaded () by any authorized user.

3.5.2 Suspicious IPs

These are class of IP addresses that are considered as unsafe and unreliable within a network traffic. When an IDS alert's source ip or dest ip matches one of the uploaded IP addresses, the alert is marked as **suspected**.



Authorized users can upload () new suspected IP Address as a csv file with each line containing an ip address, a comma, and an optional description of the ip address. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, IP Address and Description values must be separated by a comma. A sample csv file is shown below:



The uploaded file can include CIDR block too.

10.1.8.0/24, cidr test

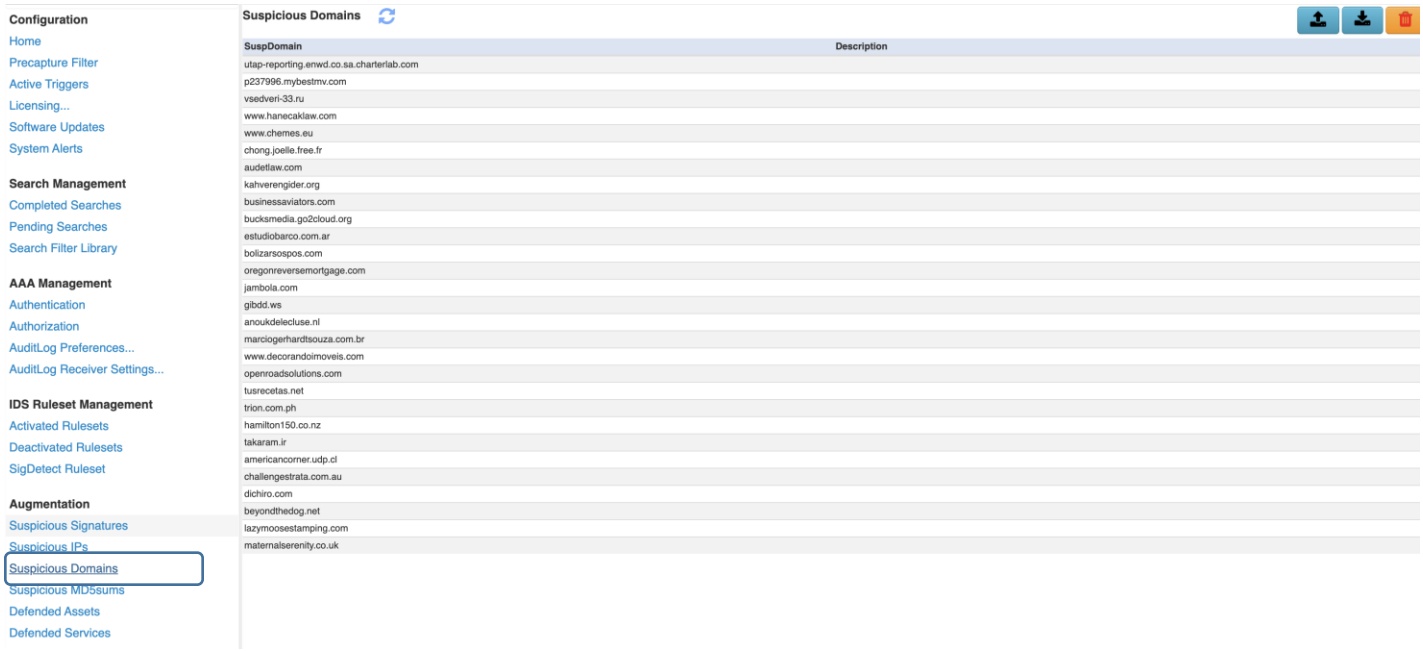
Currently available suspicious IP Addresses can be downloaded () by any authorized user.

When an event's source/destination IP Address either matches a suspicious IP Address or part of a suspicious CIDR block, the event's ioc field is augmented with the custom data uploaded. For example, the following image shows the augmented ioc value on matching an IP Address from 10.1.8.0/24 CIDR Block:

Time	src_ip	dest_ip	suspected	nodename	ioc
Nov 14, 2021 @ 11:29:59.303282000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.303274000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293695000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293672000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038037000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038025000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636885000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636874000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636579000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636568000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151

3.5.3 Suspicious Domains

Domain names are an important avenue to investigate security incidents or to prevent some malicious activity to occur on your network. When a DNS event's domain name matches one of the uploaded domains, the DNS event is marked as **suspected**



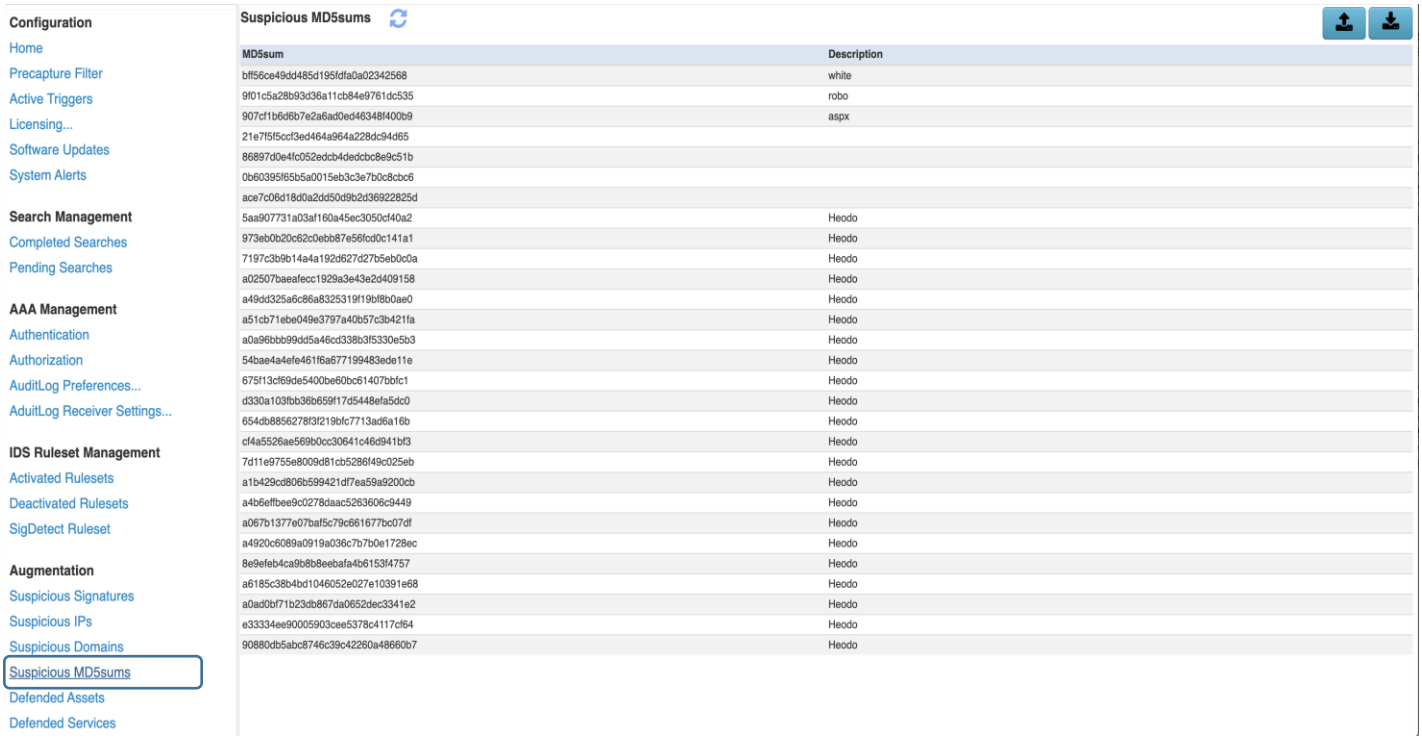
Authorized users can upload () new suspected domain names as a csv file with each line containing a domain name, a comma, and an optional description of the domain. Each line of the csv file must have a valid domain name. Description is optional. If Description is provided, IP Address and Description values must be separated by a comma. A sample csv file is shown below:

```
p237996.mybestmv.com
vsedveri-33.ru
www.hanecaklaw.com
www.chemes.eu
chong.joelle.free.fr
audetlaw.com
kahverengider.org
```

Currently available suspicious domain names can be downloaded () by any authorized user

3.5.4 Suspicious MD5sums

This page allows users to upload known bad md5sums for allowing the software to identify/alert when a file with bad md5sum is being transmitted.



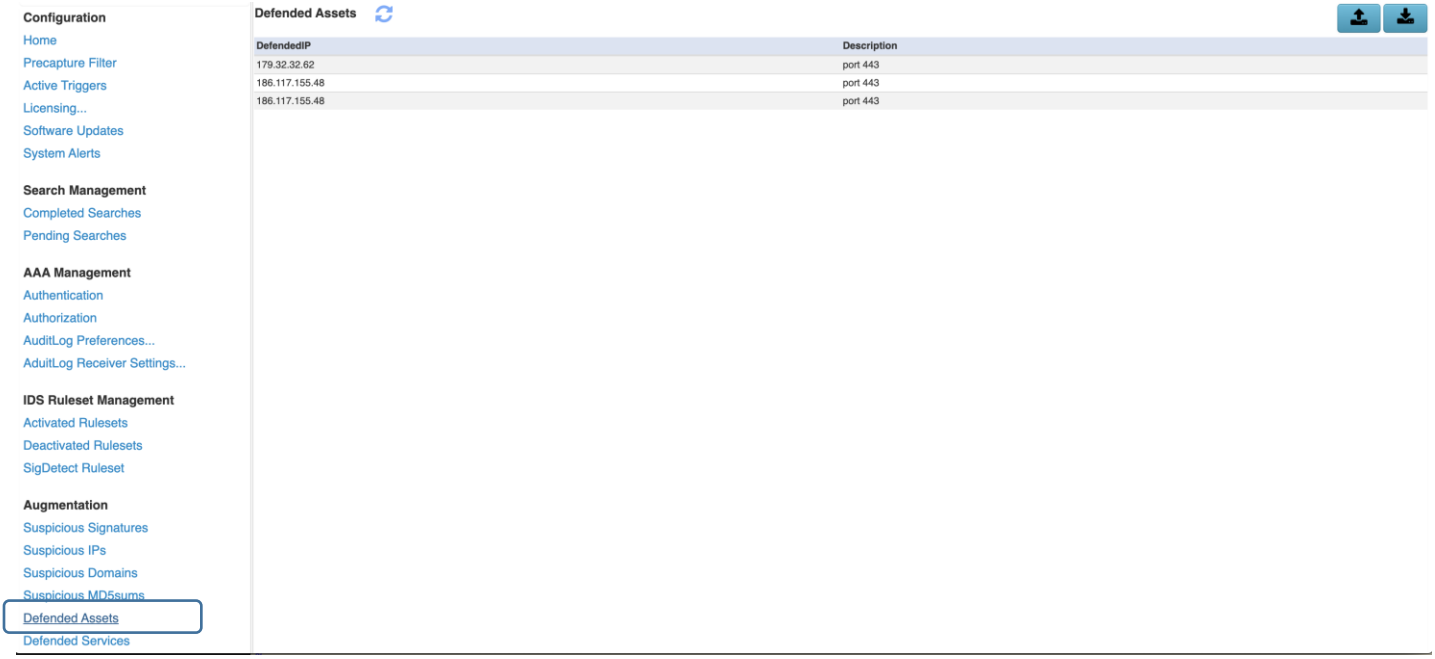
Authorized users can upload () new suspected md5sums as a csv file with each line containing a md5sum, a comma, and an optional description. Each line of the csv file must have a valid md5sum. Description is optional. If Description is provided, md5sum and Description values must be separated by a comma. A sample csv file is shown below:

```
bff56ce49dd485d195fdfa0a02342568,white
9f01c5a28b93d36a11cb84e9761dc535,robo
907cf1b6d6b7e2a6ad0ed46348f400b9,aspx
21e7f5f5ccf3ed464a964a228dc94d65,
```

Currently available md5sums can be downloaded () by any authorized user.

3.5.5 Defended Assets

Defended Asset lists are IP addresses of the systems that are approved, recognized and considered to be safe and may even be critical to the organization. If an alert's source ip or dest ip matches an ip address of a defended asset, this alert is marked as **defended**. It is quite possible for an alert to be marked both **defended** and **suspected**.



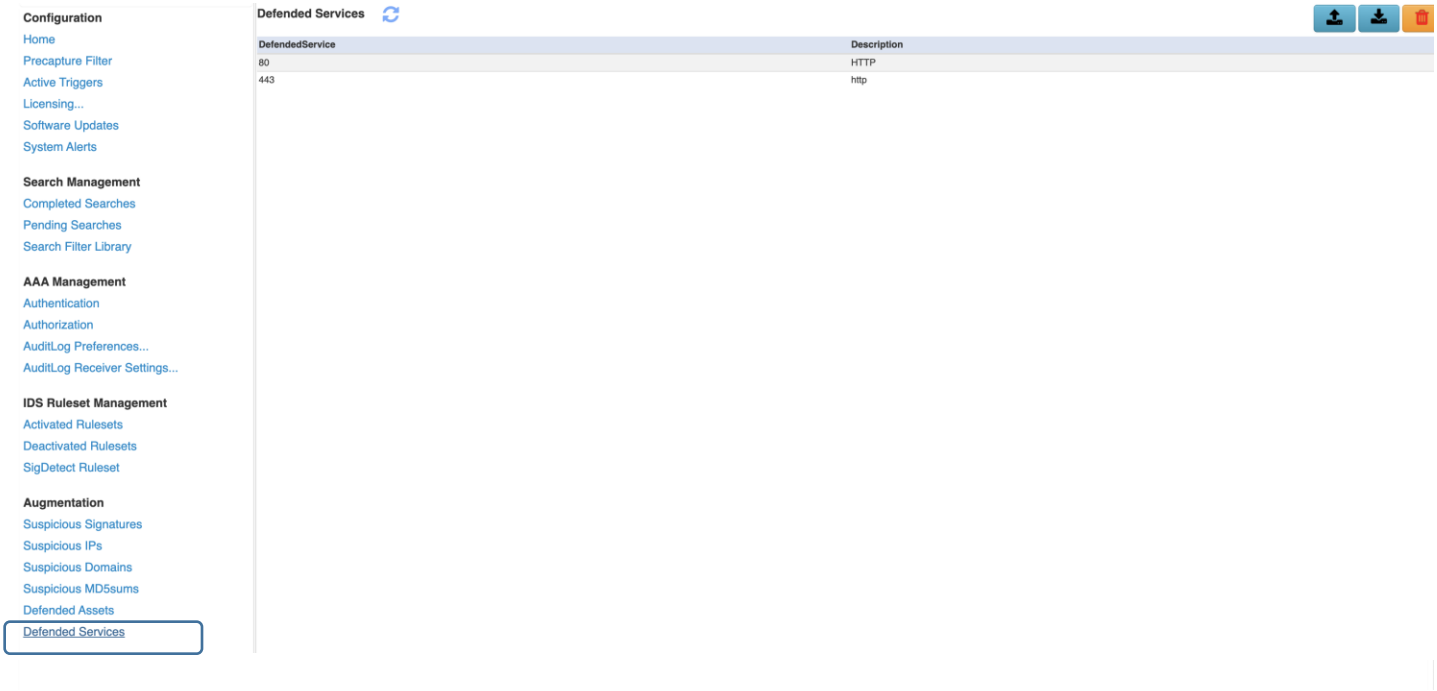
Authorized users can upload () new defended asset list as a csv file with each line containing an ip address of a defended asset, a comma, and an optional description. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, defended asset and Description values must be separated by a comma. A sample csv file is shown below:

```
176.32.32.62,system62
185.117.155.48,payroll
176.32.33.203
```

Currently available defended assets can be downloaded () by any authorized user.

3.5.6 Defended Services

Defended Service lists are port numbers of the applications that are approved, recognized and considered to be safe and may even be critical to the organization. If an alert's source port or dest port matches a port of a defended service, this alert is marked as **defended**. It is quite possible for an alert to be marked both **defended** and **suspected**.



Authorized users can upload () new defended service list as a csv file with each line containing port address of a defended service, a comma, and an optional description. Each line of the csv file must have a valid port number. Description is optional. If Description is provided, defended service and Description values must be separated by a comma. A sample csv file is shown below:

```
443,missioncritical
3306,essential
```

Currently available defended services can be downloaded () by any authorized user.

APPENDIX A – BPF FILTER

Berkeley Packet Filter (BPFs) are a raw interface to data link layers in a protocol independent fashion. They are a powerful tool for intrusion detection analysis. Using them will allow the user to quickly drill down specific packets to see and reduce large packet captures down to the essentials.

The BPF syntax consists of one or more primitives. Primitives usually consist of an *id(*name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

type

qualifiers say what kind of thing the id name or number refers to. E.g., **host**, **net**, **port**, **portrange.** If there is no qualifier**, host** is assumed.

dir

qualifiers specify a particular transfer direction to and/or from *id*. Possible directions are src,dst,src or dst. E.g., dst net 128.3

proto

qualifiers restrict the match to the particular protocol. Possible protocols are: **ether**, **fddi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp.**

1.1 Primitive Filters

Allowable primitives are given below for reference:

Primitive Filters	Description
[src|dst] host <host> E.g., src host <*host*> dst host <*host*> host <*host*> ip host <*host*>	Matches a host as the IP source, destination, or either. • These host expressions can be used in conjunction with other protocols like ip, arp, rarp or ip6
ether [src|dst] host <ehost> E.g., ether host <MAC> ether src host <MAC> ether dst host <MAC>	Matches a host as the Ethernet source, destination, or either
[src|dst] net <network> E.g., dst net 192.168.1.0 src net 192.168.1 dst net 172.16 src net 10 net 192.168.1.0 net 192.168.1.0/24 src net 192.168.1/24	Matches packets to or from source/destination or either, residing in a network. An IPv4 network number can be specified as: • Dotted quad (e.g., 192.168.1.0) • Dotted triple (e.g., 192.168.1) • Dotted pair (e.g., 172.16) • Or single number (e.g., 10)
[src|dst] net <network> mask <netmask> **or** [src|dst] net <network>/<len> E.g., dst net 192.168.1.0 mask 255.255.255.255 **or** dst net 192.168.1.0/24 src net 192.168.1 mask 255.255.255.0 **or** src net 192.168.1/24 dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0	Matches packets with specific netmask. /len can also be specified to capture traffic from range of IP addresses. • Netmask for dotted quad (e.g., 192.168.1.0) is 255.255.255.255 • Netmask for dotted triple (e.g., 192.168.1) is 255.255.255.0 • Netmask for dotted pair (e.g.,172.16) is 255.255.0.0 • Or single number (e.g.,10) is 255.0.0.0
[src|dst] port <port> **or** [tcp|udp] [src|dst] port <port>	Matches packets sent to/from port

E.g., src port 443 dst port 20 port 80	• Protocols (e.g., tcp/udp/ip etc.) can be applied to a port to get specific results
[src|dst] portrange <p1>-<p2> **or** [tcp|udp] [src|dst] portrange <p1>-<p2> E.g., src portrange 80-88 tcp portrange 1501-1549	Matches packets to/from a port in the given range • Protocols can be applied to port range to filter specific packets within the range
less <length> E.g., less 300 (or len <300)	Matches packets less than or equal to length
greater <length> E.g., greater 301(or len >300)	Matches packets greater than or equal to length
(ether|ip|ip6) proto <protocol> E.g., ether proto 0x888e ip proto 50	Matches an Ethernet, IPv4, or IPv6 protocol • Protocol can be a number or name. (Except for named protocols that bpf is aware of such as icmp, tcp, udp, dns, etc)
(ip|ip6) protochain <protocol> E.g., ip6 protochain 6	Matches IPv4, or IPv6 packets with a protocol header in the protocol header chain
(ether|ip) broadcast	Matches Ethernet or IPv4 broadcasts
(ether|ip|ip6) multicast E.g., ether[0] & 1 != 0	Matches Ethernet, IPv4, or IPv6 multicasts
vlan [<vlan>] ○ E.g., vlan 100 && vlan 200 (filters on vlan 200 encapsulated within vlan 100)	Matches 802.1Q frames optionally with a VLAN ID of vlan

○ vlan && vlan 300 && ip (filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher order vlan)	
mpls [<label>] ○ E.g., mpls 100000 && mpls 1024 (filters packets with outer label 100000 and inner Label 1024) ○ mpls && mpls 1024 && host 192.9.200.1(filters packets to and from 192.9.200.1 with an inner label of 1024 and any outer label)	Matches MPLS packets, optionally with a label of label • mpls expression may be used more than once, to filter on MPLS hierarchies.

1.2 Protocols

- Various protocols can be combined with primitive BPF filters using modifiers and operators.

Types of valid Protocols are given below:

arp	ip6	udp	fddi	link	slip	rarp
ether	ip	wlan	icmp	tcp	radio	ppp

1.3 Modifiers

Types of valid modifiers/operators:

Parentheses	( )
Negation	!=
Concatenation	'&&' or 'and'
Alteration	'||' or 'or'

1.4 Examples of some filters using operators and modifiers:

udp dst port not 53	UDP not bound for port 53
host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts
Tcp dst port 80 or 8080	Packets to either tcp ports
ether[0:4] & 0xffffff0f > 25	Range based mask applied to bytes greater than 25
ip[1] != 0	Captures packets for which Types of Service(TOS) field in the ip header is not equal to 0
ether host 11:22:33:44:55:66	Matches a specific host with that Mac address
ether[0] & 1 = 0 and ip[16] >= 224	Captures ip broadcast or multicast broadcast that were not sent via Ethernet broadcast/multicast
icmp[icmptype] != icmp-echo	Captures all icmp packets that are not echo requests
ip[0] & 0xf !=5	Catches all IP packets with options
ip[6:2] & 0x1fff = 0	Catches only unfragmented IPv4 datagrams and frag zero of fragmented ipv4 datagrams
tcp[13] & 16 != 0	Captures tcp-ack packets
tcp[13] & 32 !=0	Captures tcp-urg packets
tcp[13] & 8!=0	Captures tcp-psh packets
tcp[13] & 4!=0	Captures tcp-rst packets
tcp[13] & 2!=0	Captures tcp-syn packets
tcp[13] & 1!=0	Captures tcp-fin packets
tcp[tcpflags] & (tcp-syn|tcp-fin) != 0	Captures start and end packets (the SYN and FIN packets) of each TCP conversation
not host 1.2.3.4	any ip not matching 1.2.3.4
not host 1.2.3.4.and not host 2.3.4.5	Any ip not equal to 1.2.3.4 and not equal to 2.3.4.5
vlan and not host 1.2.3.4 and not host 2.3.4.5	Same as above with 1 vlan id

APPENDIX B - EXTENDING BPF SEARCH FILTERS

Multiple BPF search filters can be combined with the word **extends.** This feature allows each bpf filter to be independent of other filters in the same search. This is primarily useful when each filter has its own payload or some filters have payload and some do not.

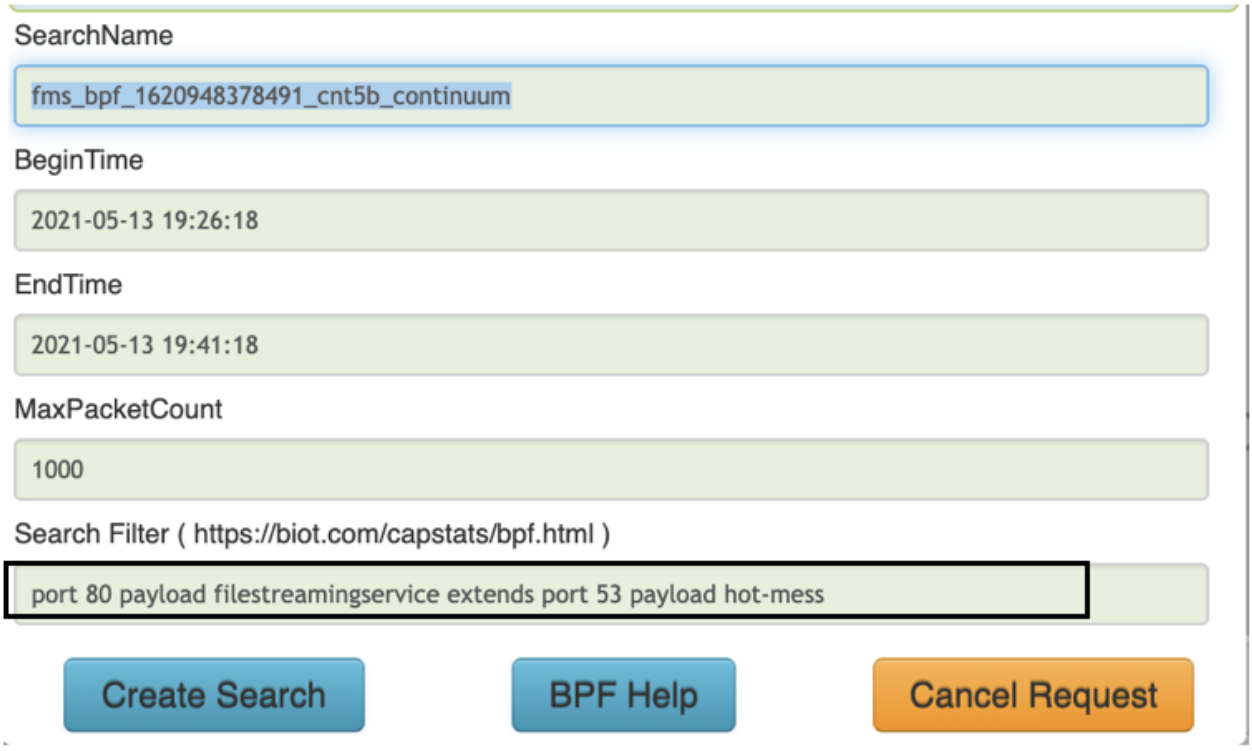
Without extends, the user will be required to create multiple searches, merge the resulting pcaps - a multi-step process that is slow and inconvenient. Some examples shown below:

1. To get packets with destination or host ip 1.2.3.4 and payload HTTP or packets with port number 53

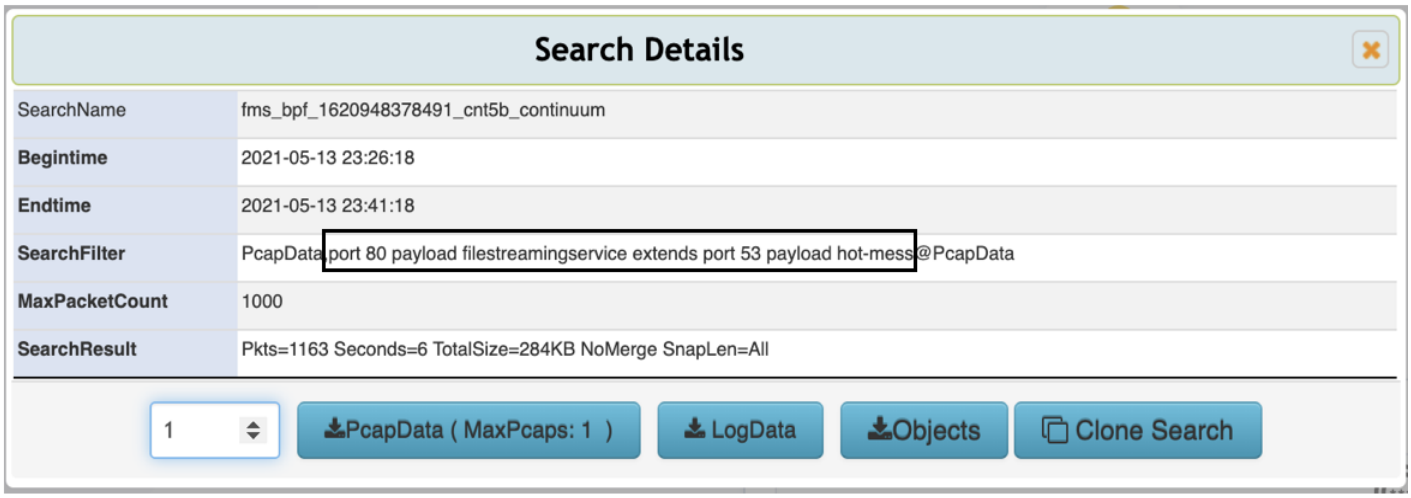
   host 1.2.3.4 payload HTTP extends port 53

2. To get packets with source or destination port 80 and packets with port 53 with payload microsoft.com
   port 80 extends port 53 payload microsoft.com

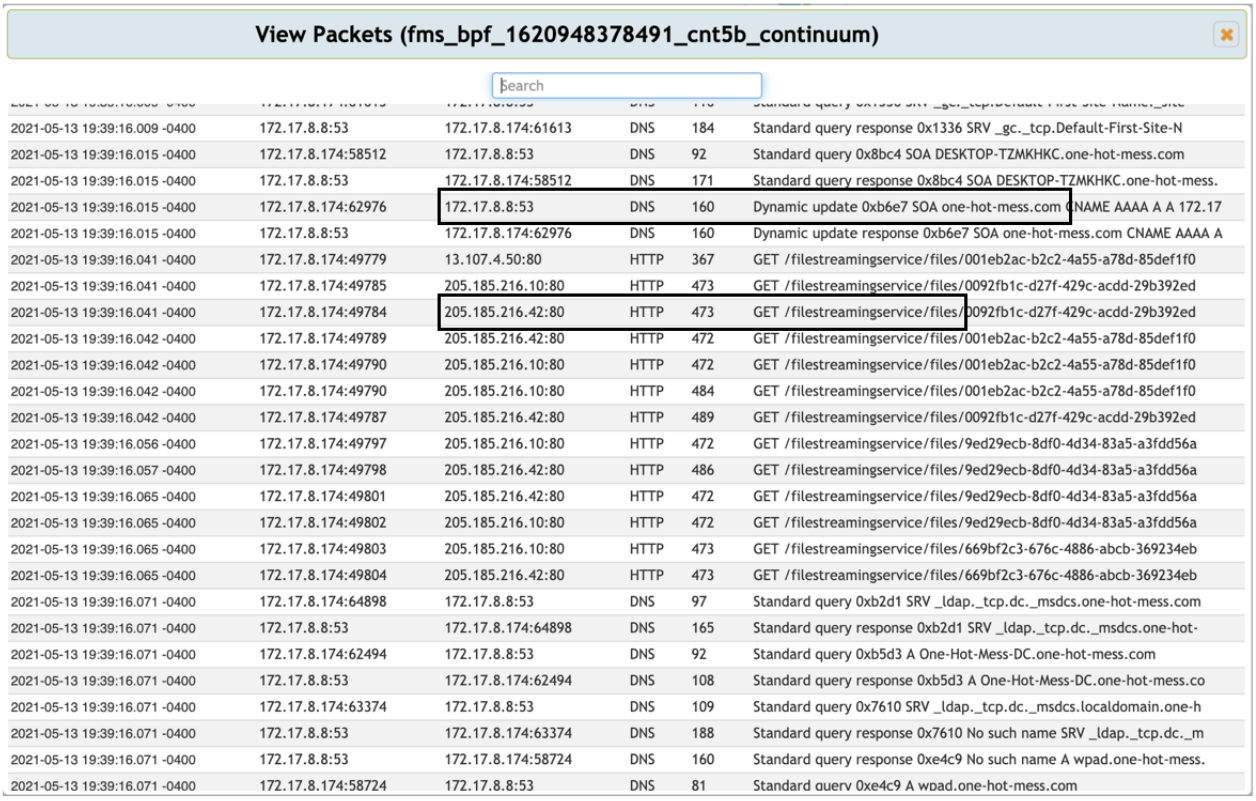
Step 1) User creates a compound search with zero or more extends



Step 2) Packets for both bpf strings are saved into the search pcap.

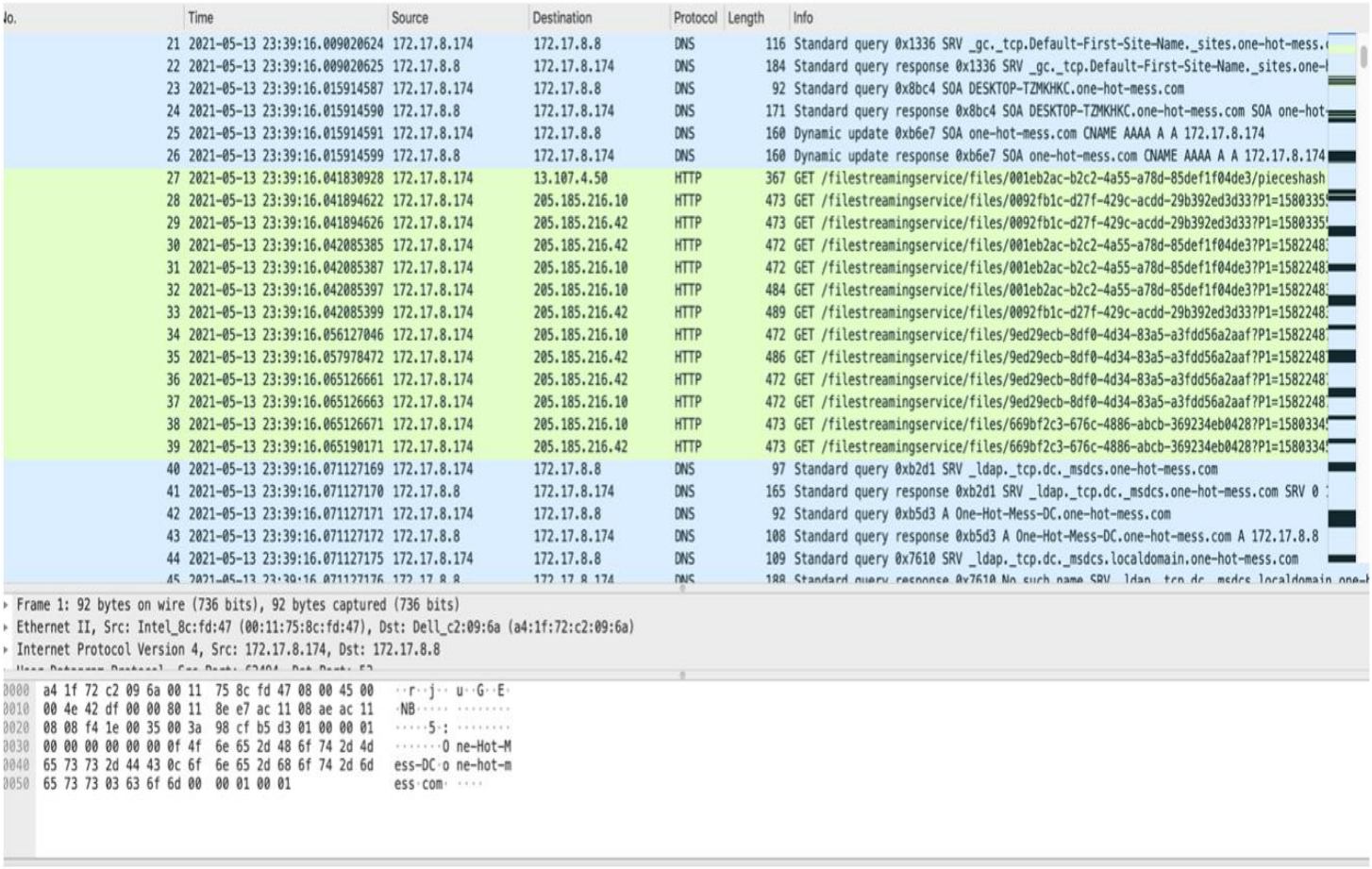


Step 3) These packets can be viewed without downloading to the local system. Each packet with only the matching payload and port is retrieved to be part of the resulting pcap.



2021-05-13 19:39:16.009 -0400	172.17.8.8:53	172.17.8.174:61613	DNS	184	Standard query response 0x1336 SRV _gc._tcp.Default-First-Site-N
2021-05-13 19:39:16.015 -0400	172.17.8.174:58512	172.17.8.8:53	DNS	92	Standard query 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com
2021-05-13 19:39:16.015 -0400	172.17.8.8:53	172.17.8.174:58512	DNS	171	Standard query response 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.
2021-05-13 19:39:16.015 -0400	172.17.8.174:62976	172.17.8.8:53	DNS	160	Dynamic update 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17
2021-05-13 19:39:16.015 -0400	172.17.8.8:53	172.17.8.174:62976	DNS	160	Dynamic update response 0xb6e7 SOA one-hot-mess.com CNAME AAAA A
2021-05-13 19:39:16.041 -0400	172.17.8.174:49779	13.107.4.50:80	HTTP	367	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.041 -0400	172.17.8.174:49785	205.185.216.10:80	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.041 -0400	172.17.8.174:49784	205.185.216.42:80	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.042 -0400	172.17.8.174:49789	205.185.216.42:80	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49790	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49790	205.185.216.10:80	HTTP	484	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49787	205.185.216.42:80	HTTP	489	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.056 -0400	172.17.8.174:49797	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a
2021-05-13 19:39:16.057 -0400	172.17.8.174:49798	205.185.216.42:80	HTTP	486	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49801	205.185.216.42:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49802	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49803	205.185.216.10:80	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb
2021-05-13 19:39:16.065 -0400	172.17.8.174:49804	205.185.216.42:80	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb
2021-05-13 19:39:16.071 -0400	172.17.8.174:64898	172.17.8.8:53	DNS	97	Standard query 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:64898	DNS	165	Standard query response 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-
2021-05-13 19:39:16.071 -0400	172.17.8.174:62494	172.17.8.8:53	DNS	92	Standard query 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:62494	DNS	108	Standard query response 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.co
2021-05-13 19:39:16.071 -0400	172.17.8.174:63374	172.17.8.8:53	DNS	109	Standard query 0x7610 SRV _ldap._tcp.dc._msdcs.localdomain.one-h
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:63374	DNS	188	Standard query response 0x7610 No such name SRV _ldap._tcp.dc._m
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:58724	DNS	160	Standard query response 0xe4c9 No such name A wpad.one-hot-mess.
2021-05-13 19:39:16.071 -0400	172.17.8.174:58724	172.17.8.8:53	DNS	81	Standard query 0xe4c9 A wpad.one-hot-mess.com

Step 4) The pcap can be downloaded and viewed with any application that reads pcap files (eg., Wireshark, Tshark)



No.	Time	Source	Destination	Protocol	Length	Info
21	2021-05-13 23:39:16.009020624	172.17.8.174	172.17.8.8	DNS	116	Standard query 0x1336 SRV _gc._tcp.Default-First-Site-Name._sites.one-hot-mess.
22	2021-05-13 23:39:16.009020625	172.17.8.8	172.17.8.174	DNS	184	Standard query response 0x1336 SRV _gc._tcp.Default-First-Site-Name._sites.one-
23	2021-05-13 23:39:16.015914587	172.17.8.174	172.17.8.8	DNS	92	Standard query 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com
24	2021-05-13 23:39:16.015914590	172.17.8.8	172.17.8.174	DNS	171	Standard query response 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com SOA one-hot
25	2021-05-13 23:39:16.015914591	172.17.8.174	172.17.8.8	DNS	160	Dynamic update 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17.8.174
26	2021-05-13 23:39:16.015914599	172.17.8.8	172.17.8.174	DNS	160	Dynamic update response 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17.8.174
27	2021-05-13 23:39:16.041830928	172.17.8.174	13.107.4.50	HTTP	367	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3/pieceshash
28	2021-05-13 23:39:16.041894622	172.17.8.174	205.185.216.10	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1580335
29	2021-05-13 23:39:16.041894626	172.17.8.174	205.185.216.42	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1580335
30	2021-05-13 23:39:16.042085385	172.17.8.174	205.185.216.42	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
31	2021-05-13 23:39:16.042085387	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
32	2021-05-13 23:39:16.042085397	172.17.8.174	205.185.216.10	HTTP	484	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
33	2021-05-13 23:39:16.042085399	172.17.8.174	205.185.216.42	HTTP	489	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1582248
34	2021-05-13 23:39:16.056127046	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
35	2021-05-13 23:39:16.057978472	172.17.8.174	205.185.216.42	HTTP	486	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
36	2021-05-13 23:39:16.065126661	172.17.8.174	205.185.216.42	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
37	2021-05-13 23:39:16.065126663	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
38	2021-05-13 23:39:16.065126671	172.17.8.174	205.185.216.10	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb0428?P1=1580334
39	2021-05-13 23:39:16.065190171	172.17.8.174	205.185.216.42	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb0428?P1=1580334
40	2021-05-13 23:39:16.071127169	172.17.8.174	172.17.8.8	DNS	97	Standard query 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com
41	2021-05-13 23:39:16.071127170	172.17.8.8	172.17.8.174	DNS	165	Standard query response 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com SRV 0
42	2021-05-13 23:39:16.071127171	172.17.8.174	172.17.8.8	DNS	92	Standard query 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com
43	2021-05-13 23:39:16.071127172	172.17.8.8	172.17.8.174	DNS	108	Standard query response 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com A 172.17.8.8
44	2021-05-13 23:39:16.071127175	172.17.8.174	172.17.8.8	DNS	109	Standard query 0x7610 SRV _ldap._tcp.dc._msdcs.localdomain.one-hot-mess.com
45	2021-05-13 23:39:16.071127176	172.17.8.8	172.17.8.174	DNS	188	Standard query response 0x7610 No such name SRV _ldap._tcp.dc._msdcs.localdomain.one-h

```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: Intel_8c:fd:47 (00:11:75:8c:fd:47), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
▸ Internet Protocol Version 4, Src: 172.17.8.174, Dst: 172.17.8.8
```

```
0000  a4 1f 72 c2 09 6a 00 11  75 8c fd 47 08 00 45 00   ··r··j·· u··G··E·
0010  00 4e 42 df 00 00 80 11  8e e7 ac 11 08 ae ac 11   ·NB····· ········
0020  08 08 f4 1e 00 35 00 3a  98 cf b5 d3 01 00 00 01   ·····5·: ········
0030  00 00 00 00 00 00 0f 4f  6e 65 2d 48 6f 74 2d 4d   ·······O ne-Hot-M
0040  65 73 73 2d 44 43 0c 6f  6e 65 2d 68 6f 74 2d 6d   ess-DC·o ne-hot-m
0050  65 73 73 03 63 6f 6d 00  00 01 00 01              ess·com· ····
```

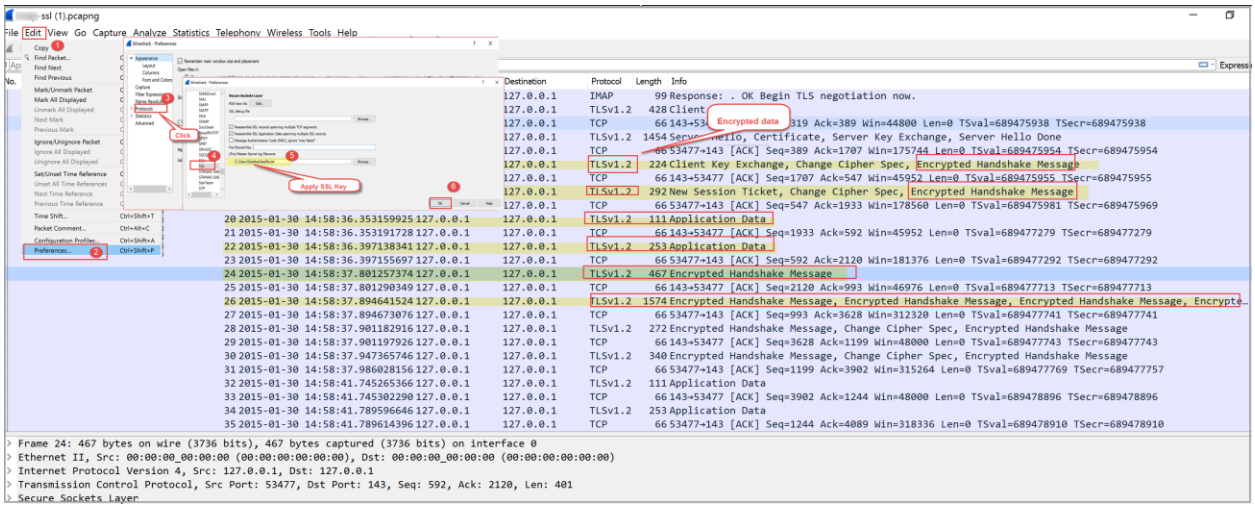
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS

This workflow presumes the user has:

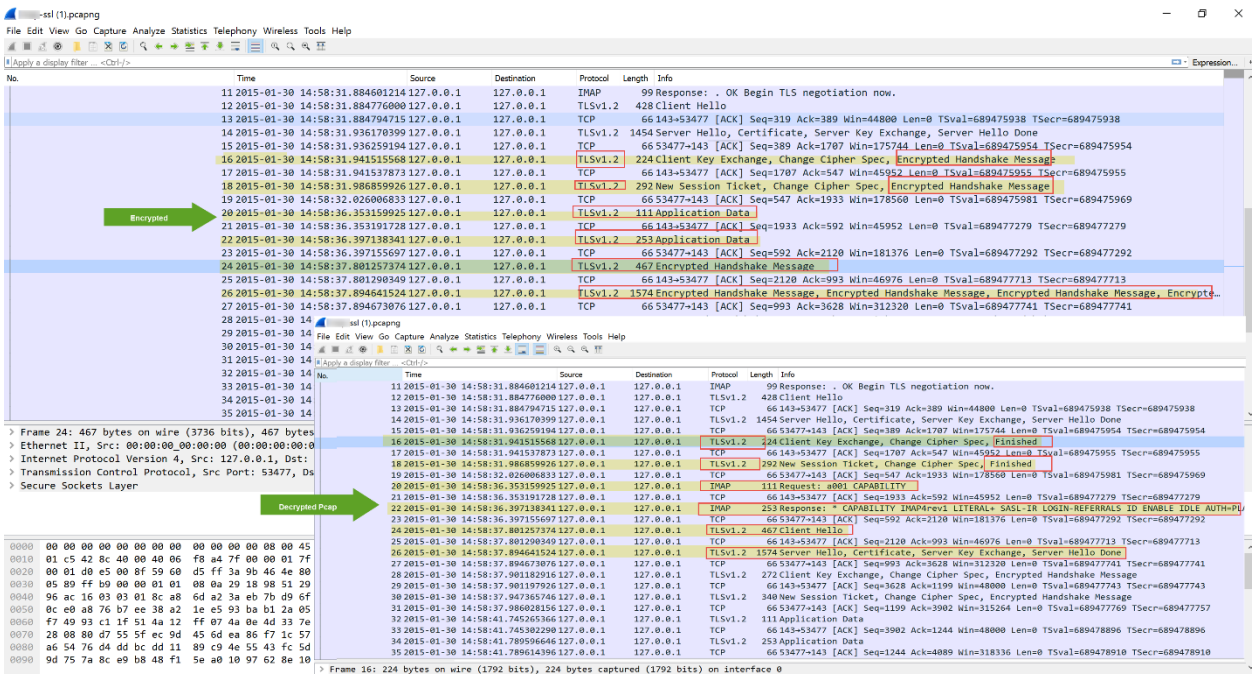
- A set of SSL Session keys for decrypting pcap data
- Downloaded one or more (encrypted) pcaps from a completed pcap search

Workflow

1. Open Wireshark application
2. Load the encrypted pcap file
3. Select **Edit->Preferences…**
4. Select and expand **Protocols**, scroll down and select SSL (or type ssl)



5. Click Browse button under (Pre)-Master-Secret log filename.
6. Select the Session Key filename to be loaded.
7. [Optional] To produce a debug file, click Browse button under SSL debug file and provide a location/filename for a debug file. **Note:** Wireshark will write to this file.
8. Click OK
9. If the Session Key is correct/matching, the loaded pcap file will be decrypted.



Notes

- Wireshark automatically tries to decrypt any other pcaps using the SSL Session Key loaded currently. To remove this file or replace with a new file, repeat the steps 3 through 8.
- Wireshark can only decrypt SSL/TLS packet data if RSA keys are used to encrypt the data.
- Wireshark can only decrypt SSL/TLS packet data if the capture includes the initial SSL/TLS session establishment. Re-used sessions cannot be decrypted; you can identify these as the server will not send a certificate or alternatively, the Wireshark SSL debug file will display a ssl_restore_session can't find stored session error message.
- Duplicate packets may cause issues and prevent all relevant packets being decrypted.

APPENDIX D - SENTRYWIRE SPLUNK ADVANCED SYNTAX

Lucene Query Syntax

Lucene query syntax is available to Kibana users who opt out of the Kibana Query Language. Full documentation for this syntax is available as part of Elasticsearch query string syntax.
The main reason to use the Lucene query syntax in Kibana is for advanced Lucene features, such as regular expressions or fuzzy term matching. However, Lucene syntax is not able to search nested objects or scripted fields.

Kibana Query Language

The Kibana Query Language (KQL) is a simple syntax for filtering Elasticsearch data using free text search or field-based search. KQL is only used for filtering data, and has no role in sorting or aggregating the data.
KQL is able to suggest field names, values, and operators as you type. The performance of the suggestions is controlled by Kibana settings.

KQL has a different set of features than the Lucene query syntax. KQL is able to query nested fields and scripted fields. KQL does not support regular expressions or searching with fuzzy terms. To use the legacy Lucene syntax, click **KQL** next to the **Search** field, and then turn off KQL.

Switching Between KQL and Lucene in Kibana

You can switch between Kibana Query Language and Lucene Syntax by clicking on the square on the right end of the search bar in Kibana. It will either read KQL or Lucene depending on which is activated. Once clicked, you can toggle the Kibana Query Language button either on or off.
We recommend that you start with KQL and use Lucene for more complex searches

Finding Values

Find data where **any field matches any of the words/terms** listed. The term must appear as it is in the data, e.g. this query won't match data containing the word "darker".
KQL
orange and (dark or light)
ℹ Use quotes to search for the word "and"/"or"
"and" "or" xor

Lucene
⚡ AND/OR must be written uppercase
orange AND (dark OR light)

Use **and/or and parentheses** to define that multiple terms need to appear. This query would find all data that have the term "orange" and either "dark" or "light" (or both) in it.
KQL
orange and (dark or light)
ℹ Use quotes to search for the word "and"/"or"
"and" "or" xor

Lucene
⚡ AND/OR must be written uppercase
orange AND (dark OR light)

To **find values only in specific fields** you can put the field name before the value e.g. this query will only find "orange" in the color field.
KQL

color : orangetitle : our planet or title : dark

Lucene
color:orange
⚡ Spaces need to be escaped
title:our\ planet OR title:dark

Putting quotes around values makes sure they are found in that specific order (**“match a phrase”**) e.g. if you want to make sure to only find data containing “our planet” and not “planet our” you’d need the following query:
KQL
"our planet"title : "our planet"

Lucene
"our planet"
ℹ No escaping of spaces in phrases
title:"our planet"

You can use the **wildcard *** to match just parts of a term/word, e.g. this query will find anything beginning with “dark” like “darker”, “darkest”, “darkness”, etc.
KQL
dark*

Lucene
dark*

Wildcards can be used anywhere in a term/word.
⚡ *Using a wildcard in front of a word can be rather slow and resource intensive for your Elasticsearch — use with care.*
KQL
d*k *les

Lucene
d*k *les

You can use the * wildcard also for searching over multiple fields in KQL e.g. this query will search “fakestreet” in all fields beginning with “user.address.”.
KQL
user.address.* : fakestreet

Lucene
Not supported

Comparing values

Compare numbers or dates. Those operators also work on text/keyword fields, but might behave not very intuitive and thus I’d recommend avoiding usage with text/keyword fields.
KQL
vlan >= 42 and vlan < 100
time >= "2020-04-10"

Lucene
vlan:>=42 AND vlan:<100
⚡ No quotes around the date in Lucene
time:>=2020-04-10

Lucene supports a special **range operator** to search for a range (besides using comparator operators shown above).
KQL is not supported.
Lucene
vlan:[511 TO 514]
ℹ Excluding sides of the range using curly braces
vlan:[511 TO 514}
vlan:{511 TO 514}
ℹ Use a wildcard for having an open sided interval
vlan:[10 TO *]
vlan:[* TO 514]

Special queries

Find data in which a specific field **exists** (i.e. that does have a non `null` value for that field).
KQL
destination : *

Lucene
exists:destination

Querying **nested fields** is only supported in KQL. The syntax is a bit more complex given the complexity of nested queries. Thus I'd recommend reading the official documentation.
KQL
products:{ name:pencil and price > 10 }

Lucene
Not supported

Lucene has the ability to search for **regular expressions**. *⚡ This can be rather slow and resource intensive for your Elasticsearch — use with care.*
KQL
Not (yet) supported (see #46855)

Lucene
mail:/mailbox\.org$/

Fuzzy search allows searching for strings, that are very similar to the given query.
KQL
Not (yet) supported (see #54343)

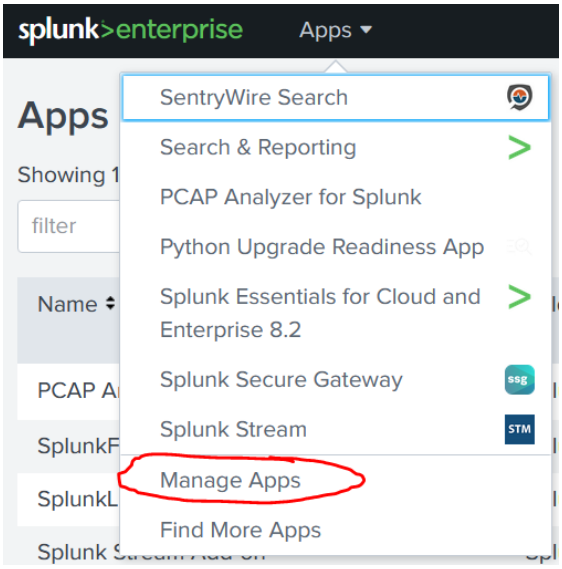
Lucene
user:maria~

APPENDIX E - SENTRYWIRE SPLUNK APP DOCUMENTATION

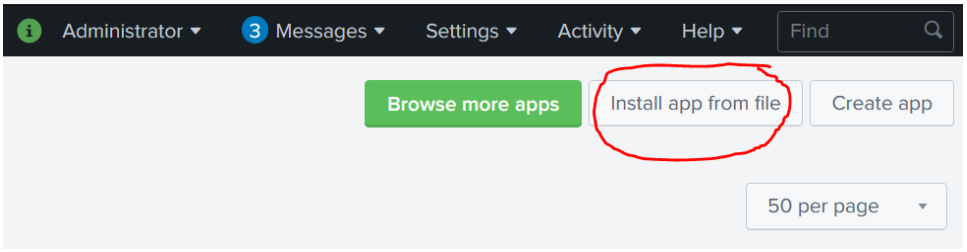
Installation

The SentryWire Splunk app currently comes as an SPL file that must be manually installed on the system.

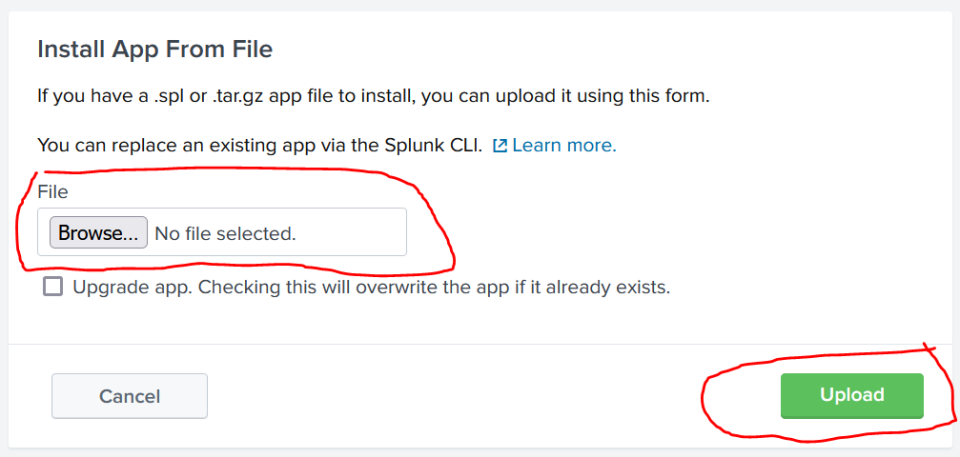
Navigate to the “Manage Apps” page



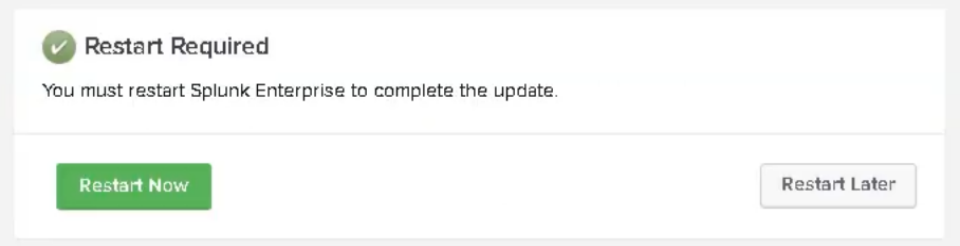
Click “Install app from file” near the top right



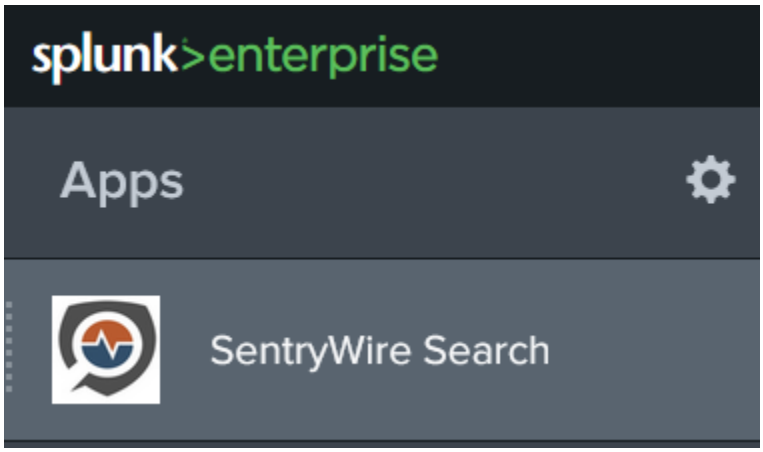
Browse to the .spl file provided by the SentryWire team.



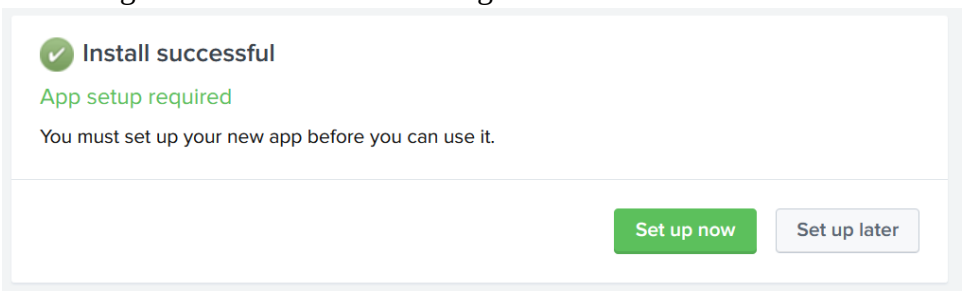
There may be a prompt to restart Splunk depending on the Splunk implementation.



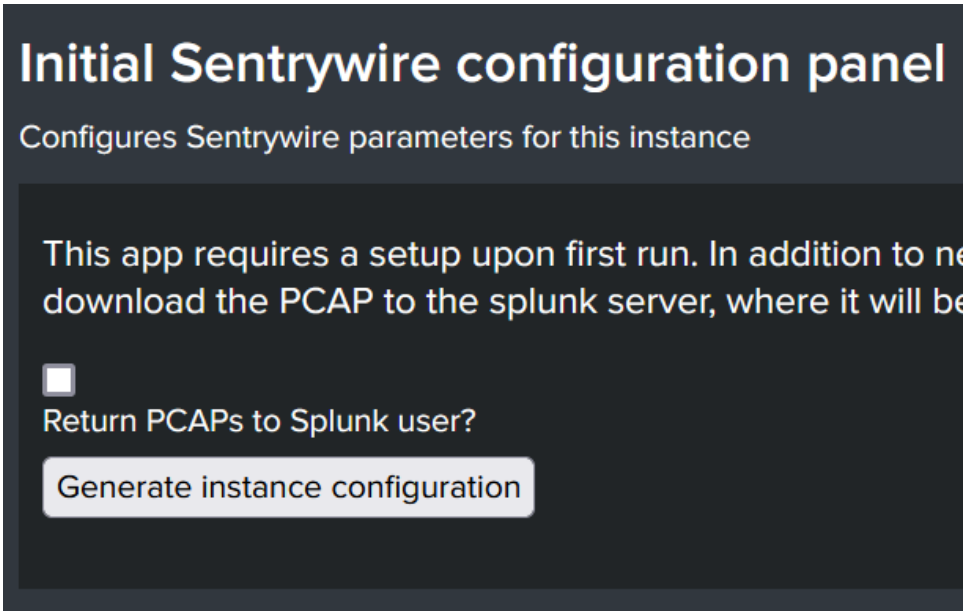
The app should now appear in the list of installed apps.



The first time the app is opened, the system will display a notification page explaining that the app requires additional information to configure the instance. Click the green button to continue.

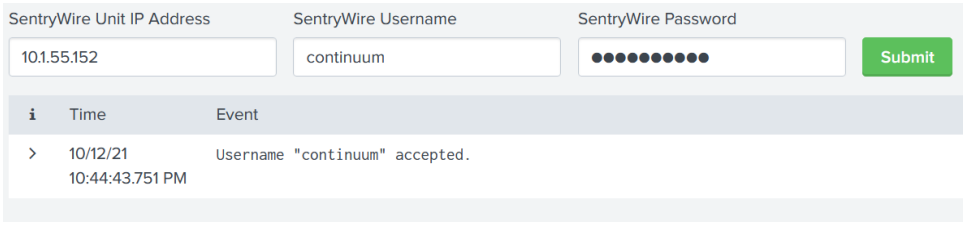


The system will transition to the “Initial SentryWire configuration panel”. Leave the checkbox unmarked if the system should not download PCAPs to the Splunk host for the Splunk user to retrieve. If left unmarked, users will need to retrieve the search results from the SentryWire cluster. Click “Generate instance configuration” after the selection is made.



The system will automatically transition to the SentryWire authentication tab. Enter the information for the SentryWire unit and click submit.

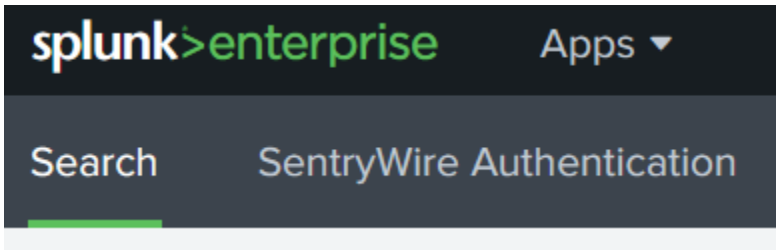
It is necessary to do this as every Splunk user that plans to use this app.



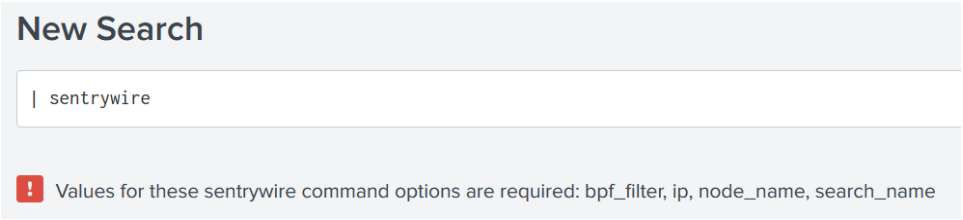
Setup is complete.

Running a search

Navigate to the search bar



We will craft a search using the SentryWire command. Place a vertical bar at the start of the search bar, and type SentryWire. This will run the SentryWire command with no input, as any events sent to the command are currently ignored.

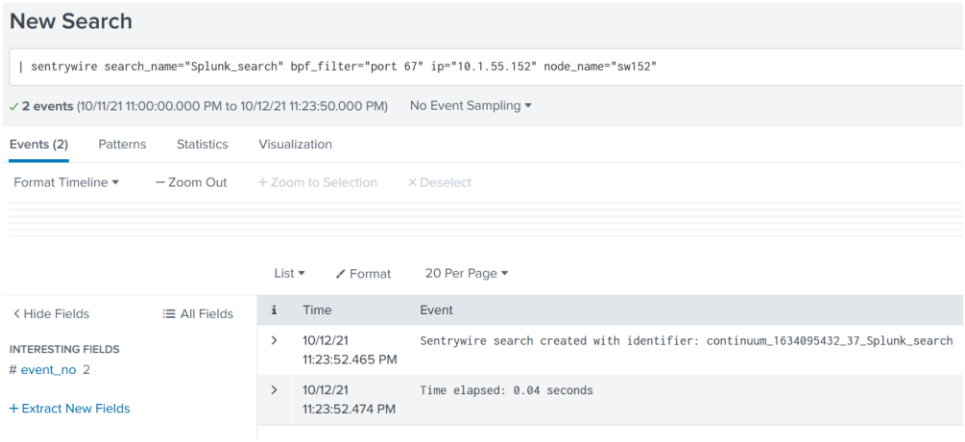


There are several required inputs, defined in any order. Variables use this format: ***<variable>=”<value>”***

Field	Description
search_name=”Splunk_search”	This is the name of the search. Data will be added to it to create the search token as it appears in the SentryWire UI.
bpf_filter=”port 67”	The BPF language filter to match packets that are desirable.
ip=”192.168.1.55”	IP address of the SentryWire unit to query.
node_name=”east_coast”	Node name of the unit to search.
Date range	Use the native Splunk input specified in the right of the search bar.

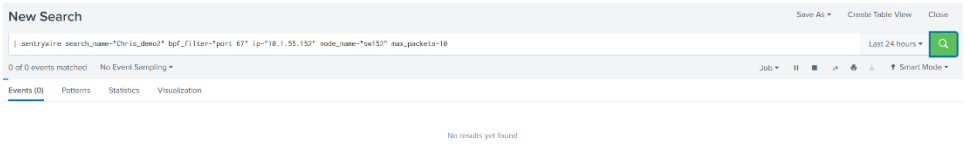
Example search

| sentrywire search_name="Splunk_search" bpf_filter="port 67" ip="172.155.0.22"

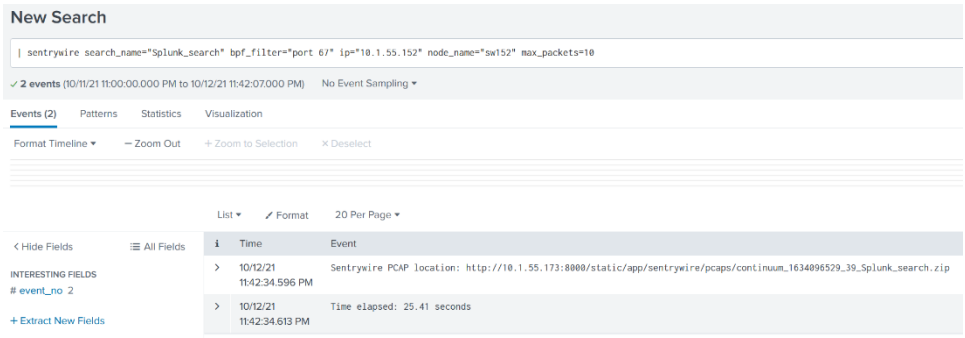


There may or may not have a link in the response, depending on how the system is configured.

If so, the link will contain a zipped copy of the first PCAP in the search. In searches that require the search to complete, the search will display “No results yet found” until the results are gathered and downloaded.



Right click to open link in new tab to download the link.



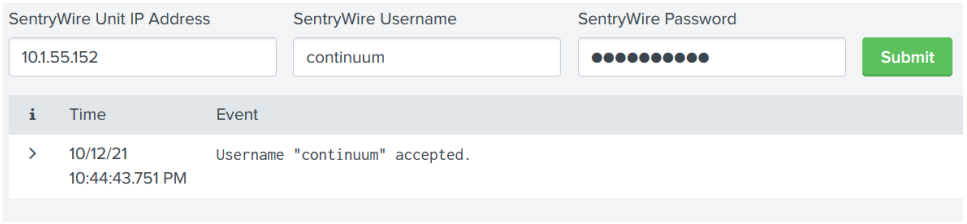
Available fields

There is no order to the fields. Those appearing in red are required for each search. If optional fields such as username + password, or start + end time are defined in the search, the variables presented in the search will take priority over alternatives.

Field	Description
search_name	Name of the search.
bpf_filter	BPF filter to apply to time span.
ip	Location of SentryWire unit.
node_name	Name of the SentryWire node
max_packets	The maximum number of packets to include in the results. May return slightly more or less depending on session data.
username	SentryWire username. Bind credentials to current user via login page. If manually specified, must use both username and password.
password	SentryWire password. Can bind credentials to current user via login page. If manually specified, must use both username and password.
start_time	Use the native Splunk input specified in the right of the search bar. Can be manually specified in ISO 8601 format • 2021-09-24T12:17:41 • YYYY-MM-DDTHH:mm:ss If manually specified, must use both start and end.
end_time	Use the native Splunk input specified in the right of the search bar. Can be manually specified in ISO 8601 format • 2021-09-24T12:17:41 • YYYY-MM-DDTHH:mm:ss If manually specified, must use both start and end.

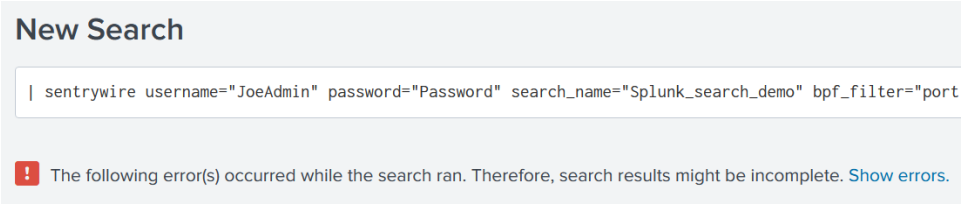
Updating SentryWire credentials

To update the credentials associated with a Splunk account, resubmit valid credentials in the SentryWire authentication page.

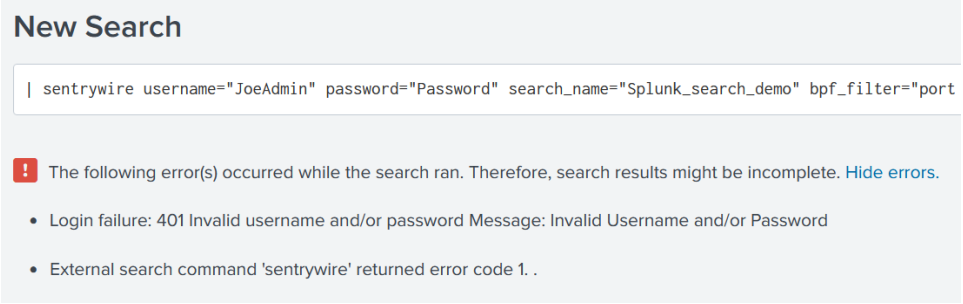


Error reporting

These things happen. Errors will appear in a dialog prompt under the search bar. In the case of a failed search, it is possible that the SentryWire unit started the search, but did not complete it in time. In this case, the successful search is still available on the SentryWire unit.



Show the error to gain insight into the issue.



Universal forwarder installation

This process will require back end console access. Run the following commands to set up the forwarder.

- Get the package
  - https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html
- rpm -i splunkforwarder-*.rpm
- cd /opt/splunkforwarder/bin
- ./splunk start
- mkdir to175
- ./splunk add monitor /opt/splunkforwarder/to175
- ./splunk add forward-server 192.168.1.175:9997
- ./splunk restart
- sudo firewall-cmd --zone=public --permanent --add-port=9997/udp
- sudo firewall-cmd --zone=public --permanent --add-port=9997/tcp
- systemctl restart firewalld
- ./splunk start
- cd /opt/splunkforwarder/
- ./splunk add monitor /storage0/logforwarder
- ./splunk add forward-server 192.168.1.175:9997
- ./splunk restart

Underlying system description

It is unnecessary for an average user to understand the remainder of the document.

Commands

There are two SentryWire commands that constitute the app.

SentryWire

This is the search function. Most users will be familiar with this.

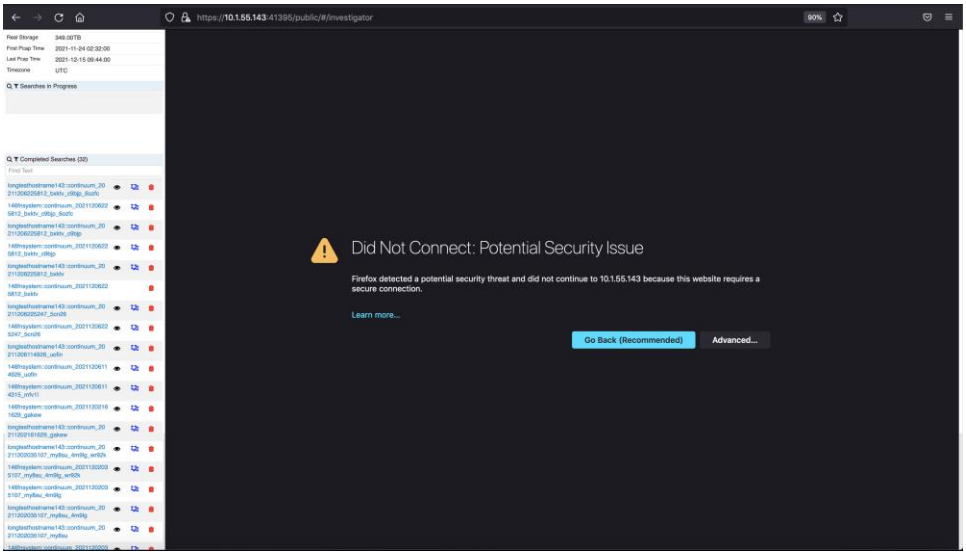
SentryWire-login

This command is run when the user presses submit on the SentryWire authentication page. It takes username, password, and ip as variables. It is recommended to use the UI as it does not show plaintext passwords on screen.

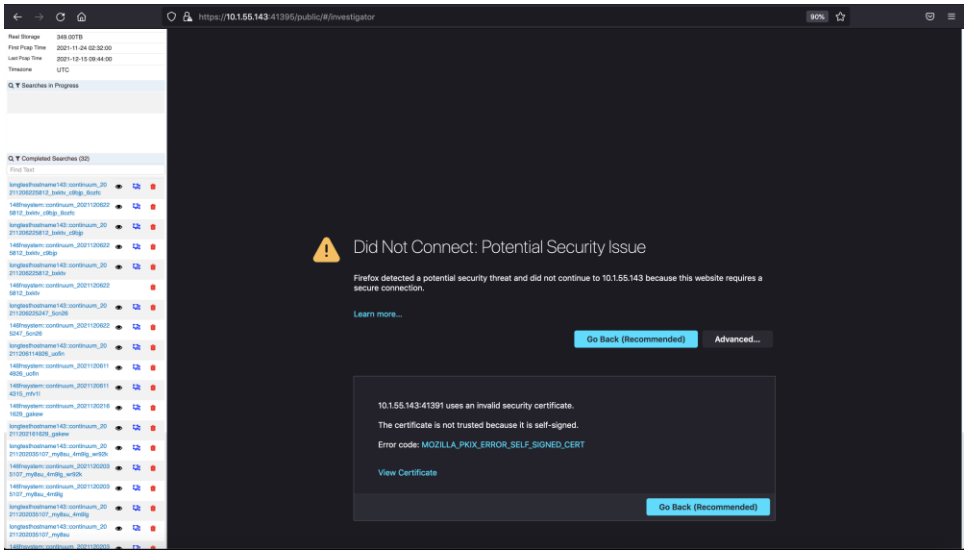
APPENDIX F – TROUBLESHOOTING RECOMMENDATIONS

Firefox Certificate Exception

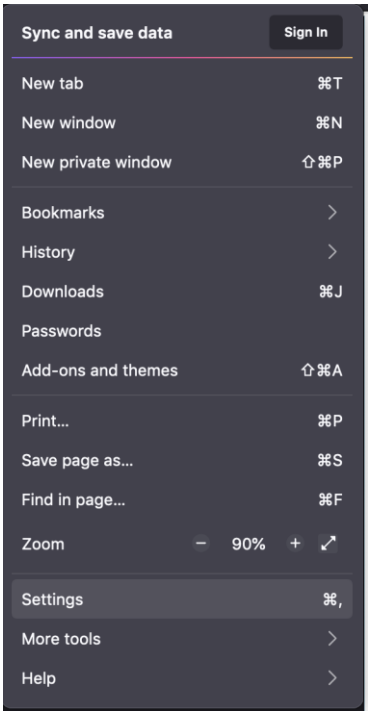
If Firefox browser shows Certificate error as shown below, follow the steps shown in this section. FM <serverip> Address is 10.1.55.143 for this example.



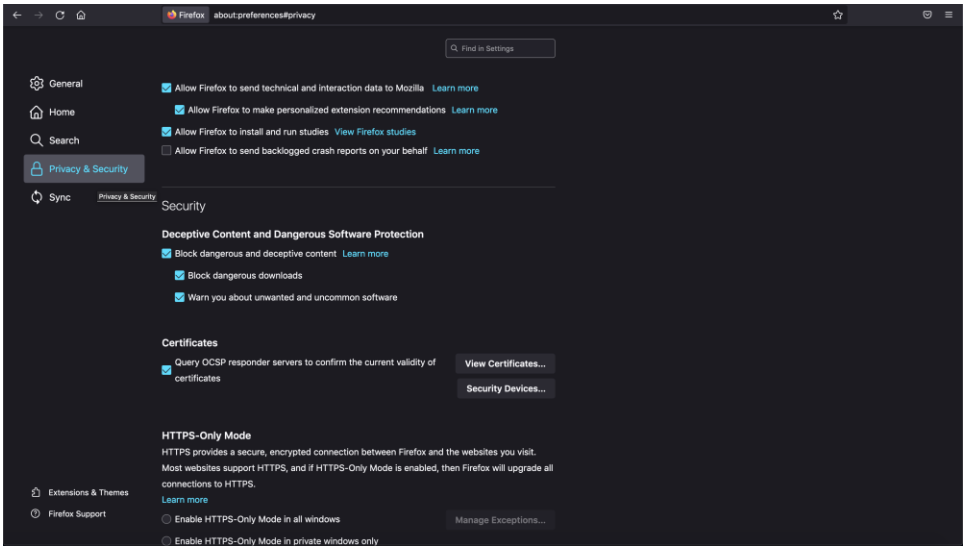
Click on Advanced… does not show Accept Risk and Continue option:



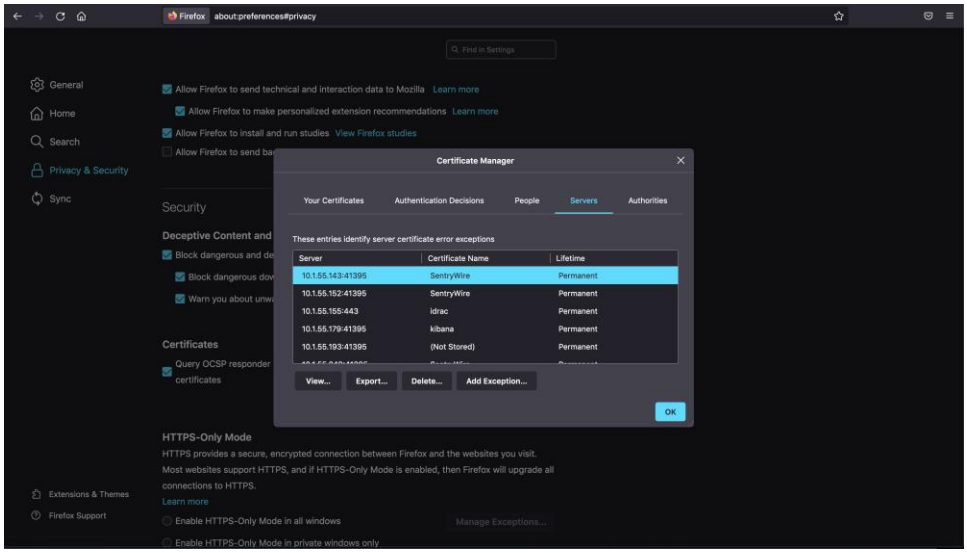
Select Browser Settings:



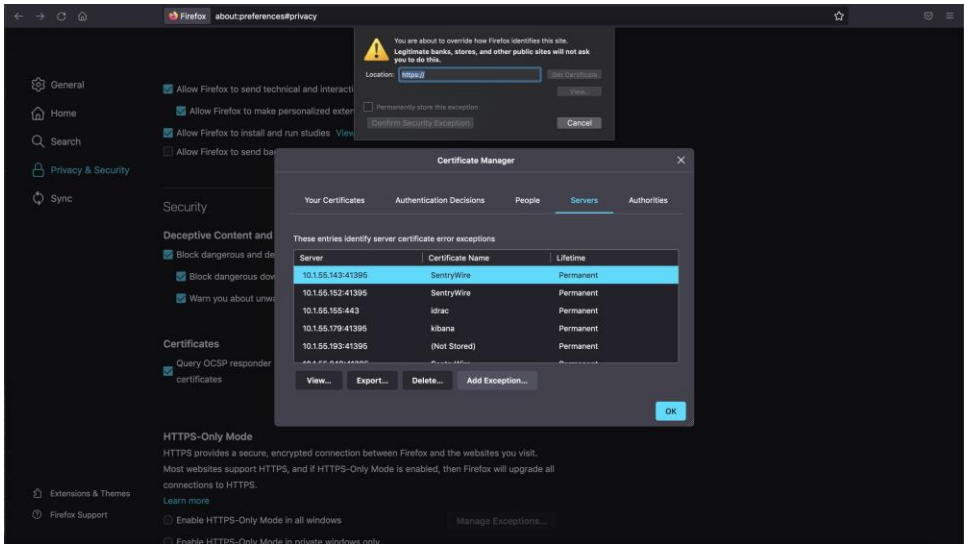
Select Privacy & Security and scroll to Certificates portion of the page:



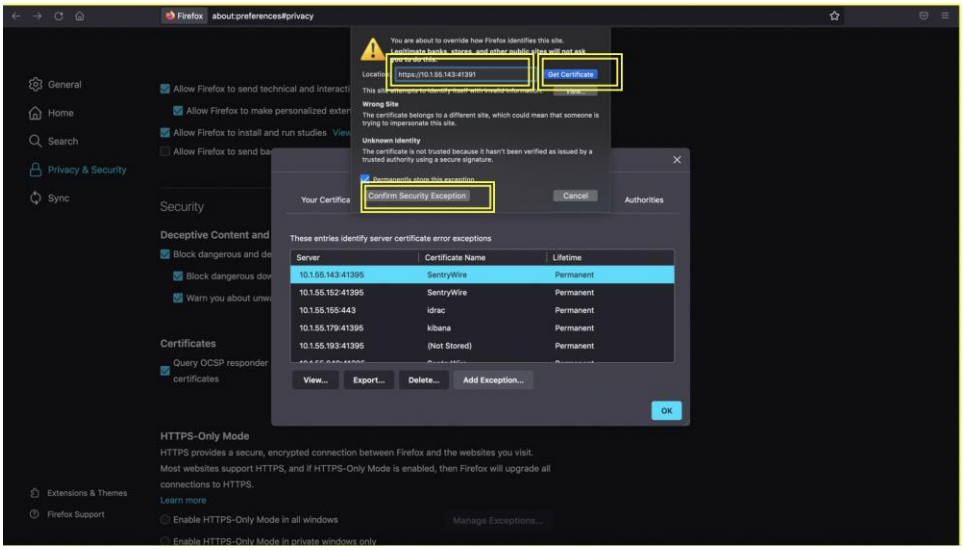
Click on View Certificates… to show Certificate Manager dialog box:



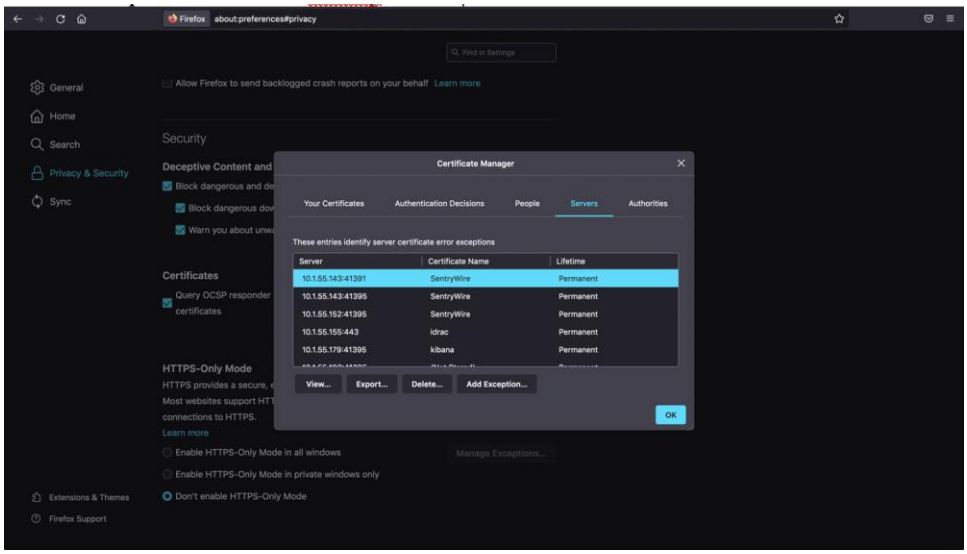
Click on Add Exception… button to add an exception:



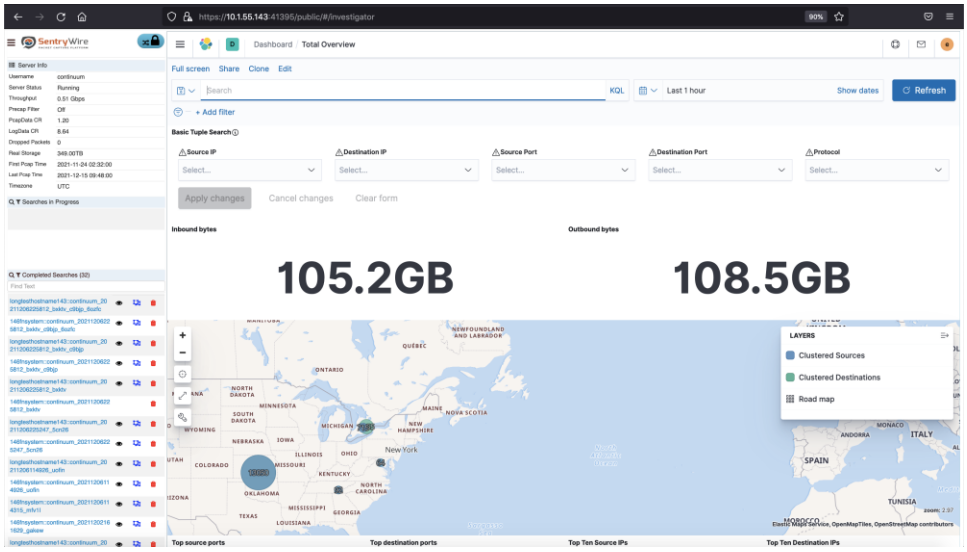
Enter https://<serverip>:41391, click on Get Certificate button, then click on Confirm Security Exception button:



The new exception is added for <serverip>:41391:



Refresh the Investigator page:



APPENDIX G – SYSTEM CONFIGURATION (NTP AND DNS)

To begin modifying the system NTP or DNS configuration, login to the OS (via SSH, KVM, etc).

NTP Configuration

1. Run the following command to open the config file
   $ vi /etc/ntpd.conf
2. Add the appropriate information to this file. For example:
   server 10.1.55.202 //set this to your primary NTP server
   server 0.pool.ntp.org //set this to your Secondary NTP server (Optional)
3. Restart the NTP process using the following command:
   $ systemctl restart ntpd
4. Ensure NTP loads on system startup using the following command:
   $ systemctl enable ntpd
5. To test that the changes have been applied and taken effect, run the following command and ensure the output matches the desired NTP servers:
   $ ntpq –p

DNS Configuration

1. Identify the system management interface using the “ifconfig” command. Most likely, the management interface will be “eno1”
2. Open the matching file /etc/sysconfig/network-scripts/ifcfg-<interface>. For example:
   $ vi /etc/sysconfig/network-scripts/ifcfg-eno1
3. Edit (or append) the “DNS1” and “DNS2” fields to the appropriate values
4. Save and close the configuration file
5. Reload the system networking using the following command:
   $ service network restart
6. (Optional) Attempt to ping the DNS server(s) to verify the connection.