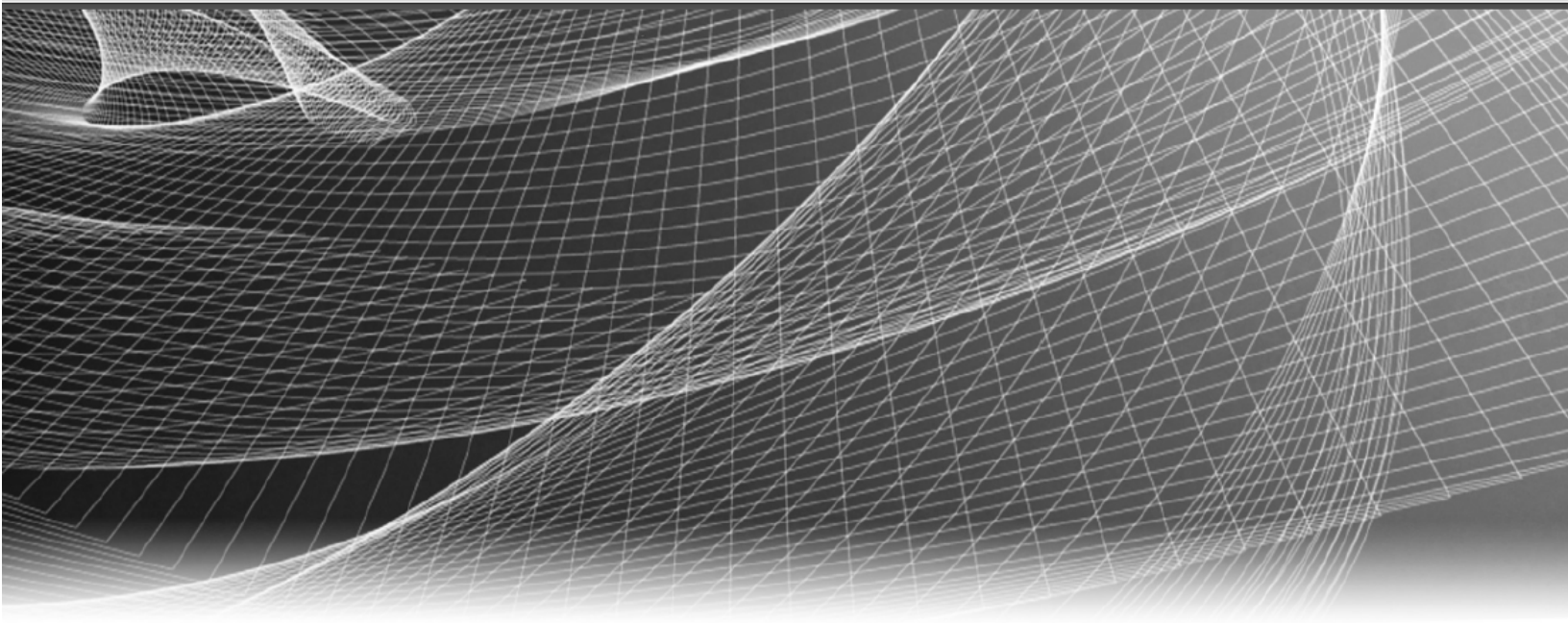


RSA | Security Analytics

Investigation and Malware Analysis Guide

for Version 10.6.5

RSA

EMC²

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

July 2019

Contents

How Investigation Works

The Investigation module provides the data analysis capabilities in Security Analytics, to that analysts can analyze data and identify possible internal or external threats to security and the IP infrastructure.

Data and Metadata for Investigation

Security Analytics audits and monitors all traffic on a network. In the RSA network, Decoders ingest, parse, and store the packets and logs traversing the network. Concentrators store the metadata that is generated by the parsers and feeds as Decoders ingest packets logs and endpoint. In the majority of environments all queries from Investigation, Event Stream Analysis (ESA), Malware Analysis (MA), and Reporting Engine (RE) are processed on the Concentrator. The analyst's first interaction is with the metadata, and the Concentrator handles most queries, only going to the Decoder when a full reconstruction of sessions, endpoint events or raw logs is required. ESA, Malware Analysis, and Reporting Engine also query the Concentrator, where they can quickly get all the pertinent metadata associated with an event and generate information on it without having to go to each Decoder.

Note: While a hybrid appliance can perform the Concentrator function, a separate Concentrator appliance is required for any large environment that needs greater bandwidth or events per second (EPS). The Concentrator appliance has storage layout that uses solid state drives for the index, which increases read performance.

Analysis Methods

Analysts can investigate captured data, open query results from other Security Analytics modules in an investigation, and import data from other collection sources. During the course of an investigation, analysts can move seamlessly between the three views in Investigation: Navigate view, the Events view, and the Malware Analysis view.

Note: Specific user roles and permissions are required for a user to conduct investigations and malware analysis in Security Analytics. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

Analysts use Investigation to hunt for incidents to drive their workflow or to do strategic analysis after another tool has generated an event. In both cases, the analyst drills or pivots into the metadata to filter the number of logs, packets, endpoint and see suspicious events, while focusing on certain combinations of metadata that lead to incident.

Navigate View

The Navigate view provides the capability to drill into and query data on a Security Analytics service. Every situation is unique in terms of the types of information the analyst is attempting to find. Investigation presents the contents of captured packets, logs or endpoint as a collection in the Navigate view. The defined meta keys are queried, and values are returned along with the number of sessions. Clicking on a value at any given level, reveals the results in detail.

For example, if there is a concern regarding suspicious traffic with foreign countries, the Destination Country meta key reveals all destinations and the frequency of the contact. Drilling into those values yields the specifics of the traffic, such as the IP address of the originator and the recipient. Checking other metadata can expose the nature of attachments exchanged between the two IP addresses. Event reconstruction can reveal the content of any conversations.

Events View

The Events view provides a view of events in list form so that you can view events and reconstruct events safely. You can open the Events view for a meta value in a current drill point from the Navigate view. For analysts without sufficient privilege to navigate a service, the Events view is a standalone investigation view in which analysts can access a list of network events, log events and endpoint events from a Security Analytics Core service without having to drill down through meta first.

The Events view presents event information in three standard forms, a simple grid listing of events, a detailed listing of events, and a log view. In addition to the standard forms, you can create a custom column group of selected meta keys, then assign the custom column group to a custom profile for viewing the events list. Once created, custom column groups and profiles are selectable from a drop-down list.

In the Events view, you can:

- Reconstruct an event from the event list.
- Use Investigation Profiles to tie together various Investigation settings into selectable sets, import and export Investigator meta groups, import and export Investigator column groups.
- Export events and associated files.

Malware Analysis View

The Malware Analysis view provides a means to analyze certain types of file objects (for example, Windows PE, PDF, and MS Office) to assess the likelihood that a file is malicious. The malware analyst can leverage the multilevel scoring modules to prioritize the massive number of files captured in order to focus analysis efforts on the files that are most likely to be malicious.

Malware Analysis Functions

Security Analytics Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows PE, PDF, and MS Office) to assess the likelihood that a file is malicious. Using Malware Analysis, the malware analyst can prioritize the massive number of files captured in order to focus analysis efforts on the files that are most likely to be malicious.

Security Analytics Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- Network Session Analysis (network)
- Static File Analysis (static)
- Dynamic File Analysis (sandbox)
- Security Community Analysis (community)

Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

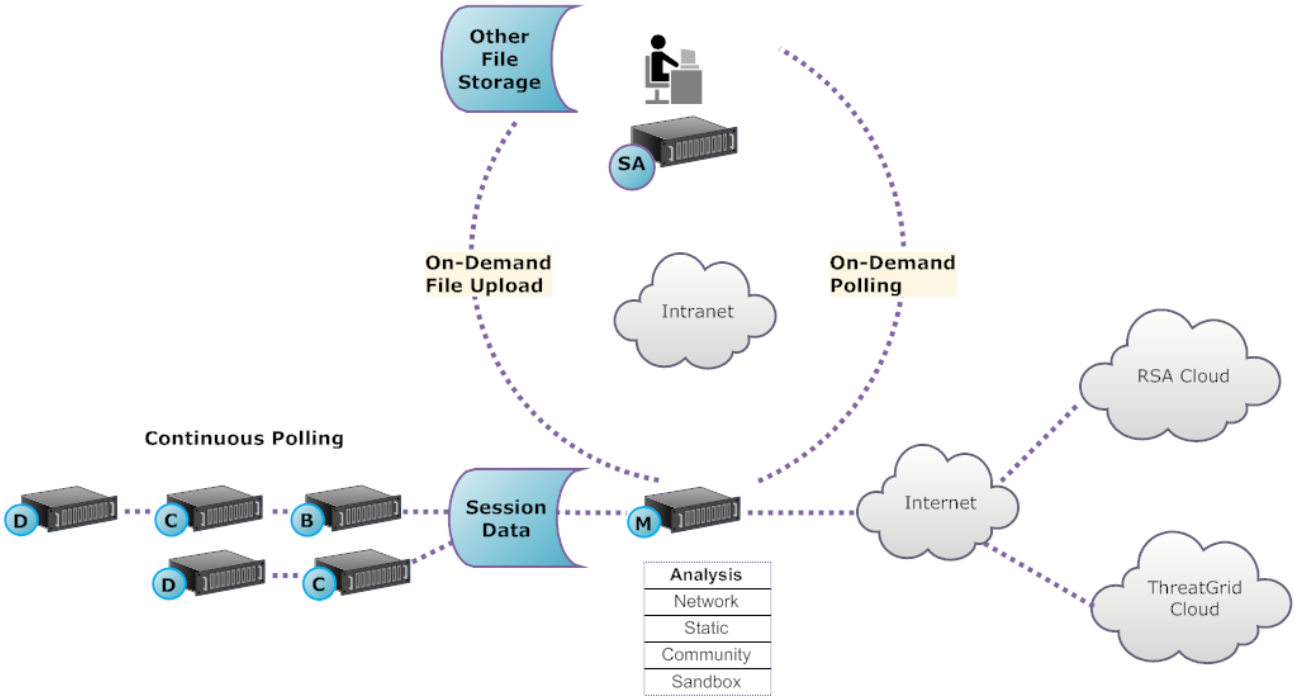
In addition to the built-in indicators of compromise, beginning with Security Analytics 10.3, Malware Analysis also supports indicators of compromise written in YARA. YARA is a rule language, which allows malware researchers to identify and classify malware samples. This allows IOC authors to add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live. These YARA-based IOCs in RSA Live will automatically be downloaded and activated on the subscribed host, to supplement the existing analysis that is performed in each analyzed file.

Beginning with Security Analytics 10.4, Malware Analysis has features that support alerts for Incident Management.

Functional Description

This figure depicts the functional relationship between the Security Analytics Core services (the Decoder, Concentrator, and Broker), the Security Analytics Malware Analysis service, and the Security Analytics server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



The Malware Analysis service analyzes file objects using any combination of the following methods:

- **Continuous automatic polling of a Concentrator or Broker** to extract sessions identified by a parser as potentially carrying malware content.
- **On-demand polling of a Concentrator or Broker** to extract sessions identified by a malware analyst as potentially carrying malware content.
- **On-demand upload of files** from a user-specified folder.

When automatic polling of a Concentrator or Broker is enabled, the Malware Analysis service continuously extracts and prioritizes executable content, PDF documents, and Microsoft Office documents on your network, directly from data captured and analyzed by your Security Analytics Core service. Because the Malware Analysis service connects to a Concentrator or Broker to extract only those executable files that are flagged as possible malware, the process is both rapid and efficient. This process is continuous and does not require monitoring.

When on-demand polling of a Concentrator or Broker is chosen, the malware analyst uses Security Analytics Investigation to drill into captured data and choose sessions to be analyzed. The Malware Analysis service uses this information to automatically poll the Concentrator or Broker and to download the specified sessions for analysis.

On-demand upload of files provides a method for the analyst to review files captured external to the Core infrastructure. The malware analyst uses Security Analytics to choose a folder location and identify one or more files to be uploaded and analyzed by Security Analytics Malware Analysis. These files are analyzed using the same methodology as files automatically extracted from network sessions.

Analysis Method

For the Network analysis, the Malware Analysis service looks for characteristics that seem to deviate from the norm, much as an analyst does. By looking at hundreds to thousands of characteristics and combining the results into a weighted scoring system, legitimate sessions that coincidentally have a few abnormal traits are dismissed, while the actual bad ones are highlighted. A user can learn patterns that indicate anomalous activity in the sessions as indicators that warrant further investigation, Indicators of Compromise.

The Malware Analysis service can perform Static analysis against suspicious objects it finds on the network and determine whether those objects contain malicious code. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. For Sandbox analysis, the services can also push data into major security, information and event management (SIEM) hosts (the ThreatGrid Cloud).

Security Analytics Malware Analysis has a unique method for analysis that is partnered with industry leaders and experts, so their technologies can enrich the Security Analytics Malware Analysis scoring system.

Security Analytics Server Access to the Malware Analysis Service

The Security Analytics server is configured to connect to the Security Analytics Malware Analysis service and import tagged data for deeper analysis in Security Analytics Investigation. Access is based on three subscription levels.

- Free subscription: All Security Analytics customers have a free subscription, with a free trial key for ThreatGrid analysis. The Malware Analysis service is rate-limited to 100 file samples per day. The number of samples (within the set of files from above) submitted to the ThreatGrid Cloud for sandbox analysis is limited to 5 per day. If one network session had 100 files in it, customers would hit the rate limit after processing the one network session. If 100 files were manually uploaded, that would cause the rate limit to be reached.
- Standard subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 1000 per day.

- Enterprise subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGrid Cloud for sandbox analysis is 5000 per day.

Scoring Method

By default, the Indicators of Compromise (IOC) are tuned to reflect industry best practices. Each IOC is assigned a score ranging from -100 (good) to +100 (bad). During analysis, the IOCs that trigger cause the score to move upward or downward to indicate the likelihood that the sample is malicious. The tuning of IOCs is exposed in Security Analytics so that the malware analyst can choose to override the assigned score or to disable an IOC from being evaluated. The analyst has the flexibility to either use the default tuning, or to completely customize the tuning to specific needs.

YARA-based IOCs are interleaved with the built-in IOCs within each built-in category and are not distinguished from native IOCs. When viewing IOCs in the Service Configuration view, administrators can select YARA from the Module selection list to see a list of YARA rules.

After a session is imported into Security Analytics, all of the viewing and analysis capabilities in Security Analytics Investigation are available to further analyze Indicators of Compromise. When viewed in Investigation, YARA IOCs are distinguished from the built-in native IOCs by the tag `Yara rule`.

Deployment

The Security Analytics Malware Analysis service is deployed as a co-located service on a Security Analytics Server or with a dedicated RSA Malware Analysis host.

The dedicated Malware Analysis host has an onboard Broker which connects to the Security Analytics Core infrastructure (either another Broker or a Concentrator). Prior to this connection, a collection of parsers and feeds must be added to the Decoders that are connected to the Concentrators and Brokers from which the Malware Analysis service pulls data. This allows suspicious data files to be marked for extraction. These files are `malware analysis` tagged content available through the RSA Live content management system.

Malware Scoring Modules

RSA Security Analytics Malware Analysis analyzes and scores sessions and the embedded files within these sessions by scoring four categories: Network, Static Analysis, Community, and Sandbox. Each category comprises many individual rules and checks that are used to calculate a score between 1-100. The higher the score, the more likely the session is to be malicious and worthy of more in-depth follow-on investigation.

Security Analytics Malware Analysis can facilitate a historical investigation into events leading up to a network alarm or incident. If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections. You can also modify behavior for each scoring category based on the scoring category or the file type (Windows PE, PDF, and Microsoft Office).

Once you become familiar with data navigation methods, you can explore the data more completely through:

- Searching for specific types of information
- Reviewing specific content in detail.

Category scores for Network, Static Analysis, Community, and Sandbox are maintained and reported independently. When events are viewed based on the independent scores, as long as one category detects malware, it is evident in the Analysis section.

Network

The first category examines each Security Analytics Core core network session to determine if the delivery of the malware candidates was suspicious. For example, benign software being downloaded from a well-known safe site, using proper ports and protocols, is considered less suspicious than downloading software known to be malicious from a known dubious download site. Sample factors used in the scoring of this criteria set may include sessions that:

- Contain threat feed information
- Connect to well-known bad sites
- Connect to high-risk domains/countries (for example, .cc domain)
- Use well-known protocols on non-standard ports
- Contain obfuscated JavaScript

Static Analysis

The second category analyzes each file in the session for signs of obfuscation in order to predict the likelihood of the file behaving maliciously if allowed to run. For example, software that links to networking libraries is more likely to perform suspicious network activity. Sample factors used in the scoring of this criteria set may include:

- Files found to be XOR encoded
- Files found embedded within non-EXE formats (for example, PE file found embedded in a GIF format)
- Files linking to higher risk import libraries
- Files highly deviating from the PE Format

Community

The third category scores the session and files based on the collective knowledge of the security community. For example, files whose fingerprint/hash is already known to be good or bad by respected anti-virus (AV) vendors is scored accordingly. Files are also scored based on knowledge that a file was delivered from a site known to be good or bad by the security community.

Community scoring also indicates whether the AV on your network flagged the files as malicious. It does not indicate that the resident AV product acted to protect your system.

Sandbox

The fourth category examines the behavior of the software by actually running it in a sandbox environment. By running the software to watch its behavior, a score can be calculated by identifying well-known malicious activity. For example, software that configures itself to autostart on each reboot and make IRC connections would score higher than a file with no known bad behavior.

Roles and Permissions for Malware Analysts

This topic identifies the user roles and permissions required for a user to conduct malware analysis in Security Analytics. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

Required Roles and Permissions

RSA Security Analytics manages security by providing access to views and functions using both system permissions and permissions on individual services.

On the system level, the user needs to be assigned a system role, in the Administration > System view, that provides access to specific views and functions. The default `Malware_Analysts` role in Security Analytics 10.5 is assigned all of the permissions listed below. If necessary, an Administrator can create a custom role with some combination of the following permissions:

- Access Investigation Module (required)
- Investigation - Navigate Events
- Investigation - Navigate Values
- Access Incident Module
- View and Manage Incidents
- View Malware Events (to view events)
- File Download (to download files from the Malware Analysis service)
- Initiate Malware Scan (to initiate a one-time service scan or one-time file upload)
- Dashlet permissions for convenience: Dashlet - Investigate Top Values Dashlet, Dashlet - Investigate Service List Dashlet, Dashlet - Investigate Jobs Dashlet, Dashlet - Investage Shortcuts Dashlet.

Note: When upgrading from Security Analytics 10.4 to Security Analytics 10.5, the Security Analytics 10.4 default `MalwareAnalysts` role is renamed to `Malware_Analysts` with no changes to the assigned permissions.
When upgrading from Security Analytics 10.3 and earlier, the `Malware Analyst` role includes a subset of these permissions. The default `Malware Analyst` role is renamed to `MalwareAnalysts` if it exists and the new permissions are added. If the `Malware Analyst` role did not exist, the new `MalwareAnalysts` role is created.

A use case for creating a custom role would be a Junior Malware Analyst role, with limited permissions that do not include the File Download permission.

On specific services, a malware analyst needs to be a member of the **Analysts** group, or to a group that has the two default permissions assigned to the Analyst group: **sdk.meta** and **sdk.content**. Users who have these permissions can use specific applications, run queries, and view content for purposes of analysis on the service.

Configure Investigation Views and Preferences

Analysts can configure some aspects of Security Analytics Investigation views and behavior. You can customize the way that Investigation views appear, the types of information displayed, and factors that affect performance in returning results and reconstructing events. All configurable settings have default values that are effective in most deployments; however, analysts have the option to adjust these if necessary.

Analysts who conduct analysis using Security Analytics Investigation need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles and permissions as described in Roles and Permissions for Analysts in the *Malware Analysis Configuration Guide*.

These topics provide details:

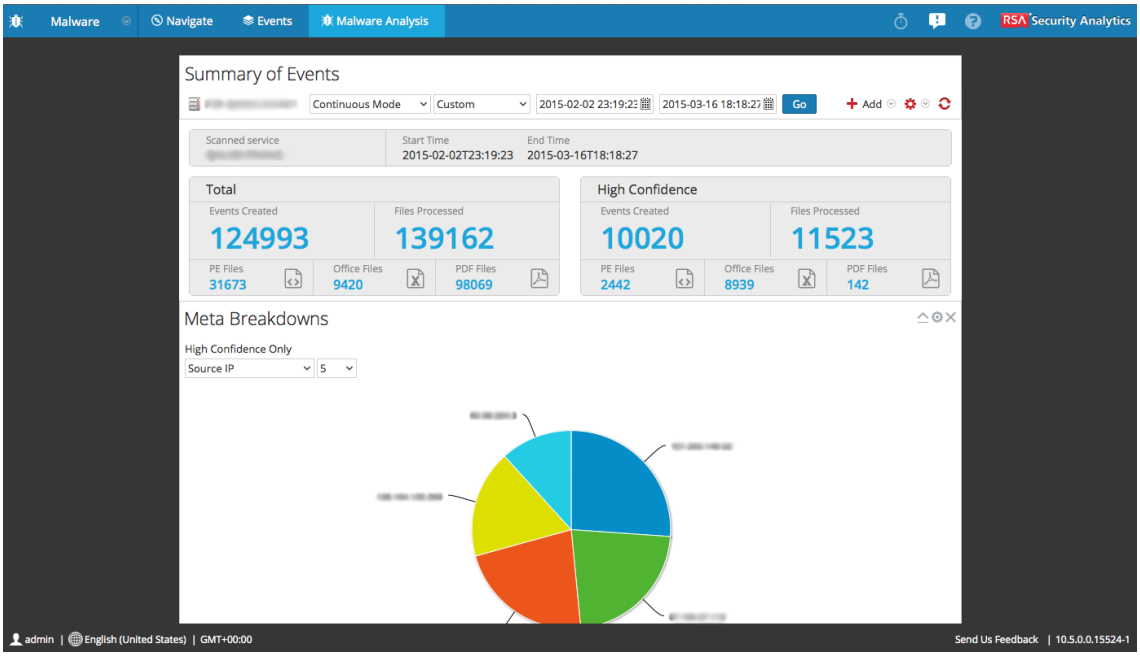
- Configure Navigate View and Events View
- Configure Malware Summary of Events View

Configure Malware Summary of Events View

The Summary of Events provides a summary of the scan being investigated, and below the summary are configurable dashlets such as visualization charts and listings. By default, the Summary of Events for a scan opens with the default dashlets displayed. You can customize the view by adding, modifying, and deleting default dashlets. The configured customization of dashlets persists through different scan investigations, and you can restore default dashlets at any time. The default dashlets are:

- Summary of Events (Fixed)
- Event Timeline
- Top Listing of Highly Suspicious Malware
- Meta Treemap
- Score Wheel
- Meta Breakdowns

The following figure is an example of the default Summary of Events.

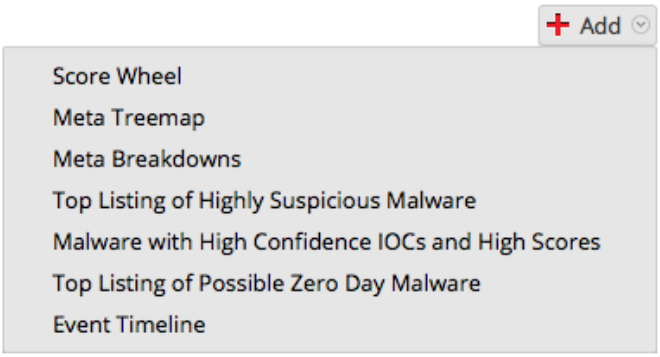


The rest of this topic provides instructions for managing and configuring dashlets.

Add a Dashlet

You can add multiple copies of dashlets in the Malware Analysis Summary of Events. To add a dashlet:

1. In the toolbar, select **Add**.
   The drop-down list of dashlets is displayed. There are four visualization options: Score Wheel, Meta Treemap, Meta Breakdowns, and Event Timeline. The other three dashlets are the same dashlets available in the Unified dashboard: Malware with high Confidence IOCs and High Scores, Top Listing of Highly Suspicious Malware, Top Listing of Possible Zero Day Malware.



2. Select a dashlet.
   The new dashlet is added as the last dashlet below the existing dashlets.
3. If the dashlet is a duplicate of an existing dashlet, change the name of the new dashlet so that it is unique.

Modify or Delete a Dashlet Using Toolbar Options

Each dashlet has a toolbar that offers options for modifying the dashlet. The visualization charts have the same configuration settings, while some of the other dashlets have different additional settings.

To use the toolbar options:

- To close a dashlet so that only the title bar is displayed, click .
- To open a dashlet that is closed, click .
- To display the configurable settings for a dashlet, click .

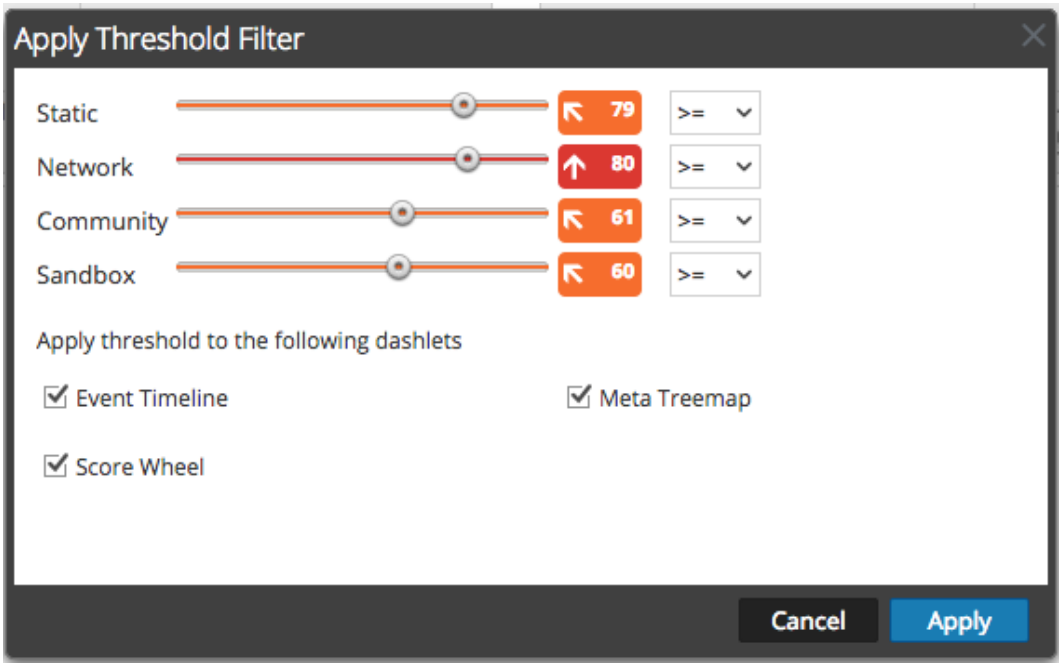
The settings dialog for the dashlet is displayed.

- To delete a dashlet, click .

Apply Threshold Filter to Multiple Dashlets

Within dashlets, you can set a threshold to show only events equal to, above, or below a certain score in the four categories (Static, Network, Community, and Sandbox). This procedure sets the thresholds by dashlet type for these dashlets: Event Timeline, Score Wheel, and Meta Treemap. You can also set the threshold for individual dashlets.

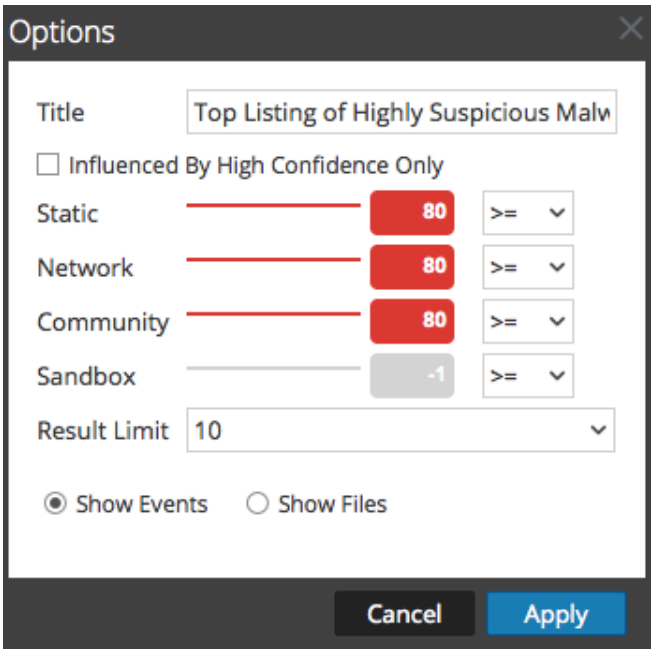
1. In the toolbar, select > **Apply Threshold Filter**.
   The Apply Threshold Filter dialog is displayed.



2. Select one or more dashlet types: Event Timeline, Score Wheel, and Meta Treemap.
3. Drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.
4. Click **Apply**.
   The threshold filters are applied to the selected dashlet types in the Summary of Events.

Set Title and Category Options for a Dashlet

1. To display the configurable settings for a dashlet, click .
   The Options dialog for the dashlet is displayed.

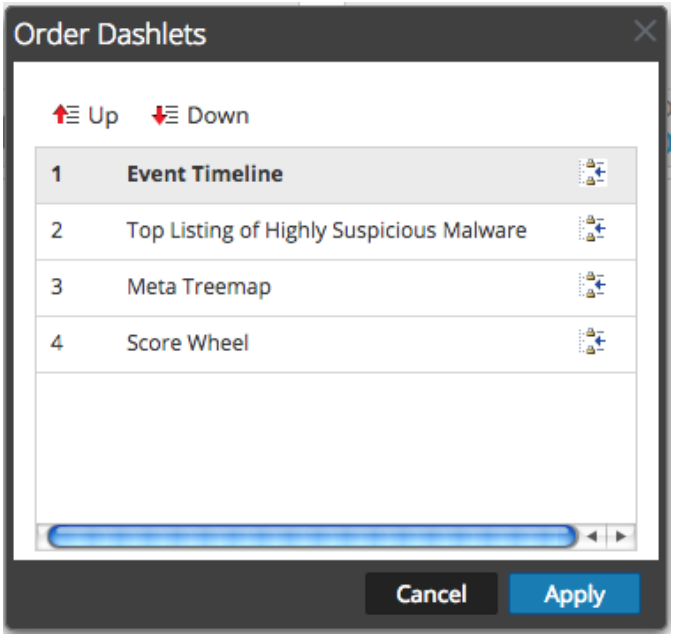


2. Type a new title for the dashlet in the **Title** field.
3. If you want to see only events that are influenced by a High Confidence tag, which means there is high confidence that the event contains harmful code, check the **Influenced By High Confidence Only** option.
4. If you want to see only events that were given a score above a certain score in the four categories (Static, Network, Community, and Sandbox), drag the corresponding slider or enter a numeric value, then select an operator in the drop-down list: =, >=, or <=.
5. Click **Apply**.
   The title and filters are applied to the dashlet.

Order Dashlets

To change the order of dashlets as they appear beneath the Summary of Events:

1. In the toolbar, select > **Order Dashlets**.
   The Order Dashlets dialog is displayed.



2. Select a dashlet that you want to move up or down, and click Up or Down.
3. When you are satisfied with the order, click **Apply**.
   The dialog closes and the order of dashlets below the Summary of Events is changed to match your choices.

Restore Default Dashlets

Once you have added, modified, and arranged dashlets, you can revert to the default settings for dashlet display. To restore the default dashlets:

1. In the toolbar, select > **Restore Default Configuration**.
   A dialog requests confirmation that you want to restore the configuration.
2. Do one of the following:
   a. If you decide to keep the dashlet arrangement you have configured, click **No**.
   b. If you are sure that you want to restore the defaults, click **Yes**,
      The dashlet display reverts to the default display.

Configure Navigate View and Events View

Analysts can set preferences that affect performance and behavior of Security Analytics when analyzing data using the Investigation > Navigate view and Events view.

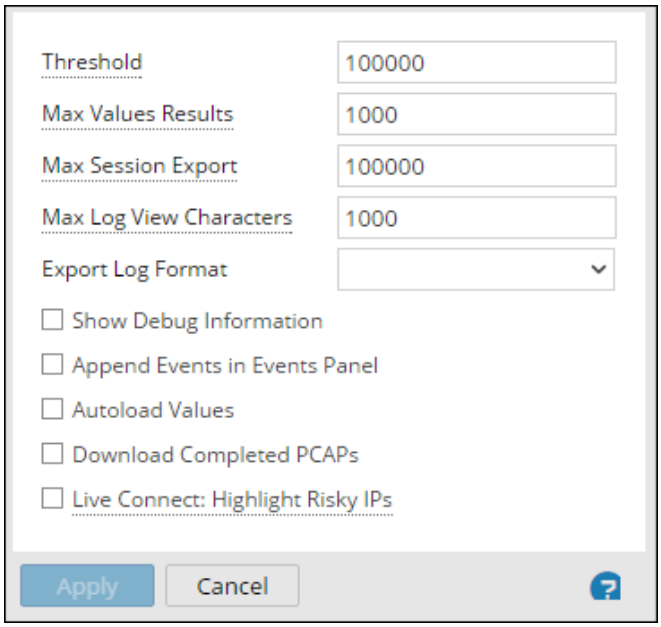
These settings are available in two places in Security Analytics, and changes made in either location are applied in the other view:

- Investigation view > Settings dialog and Search field for the Navigate view and the Events view.
- In the Profiles > Preferences panel > Investigations tab.

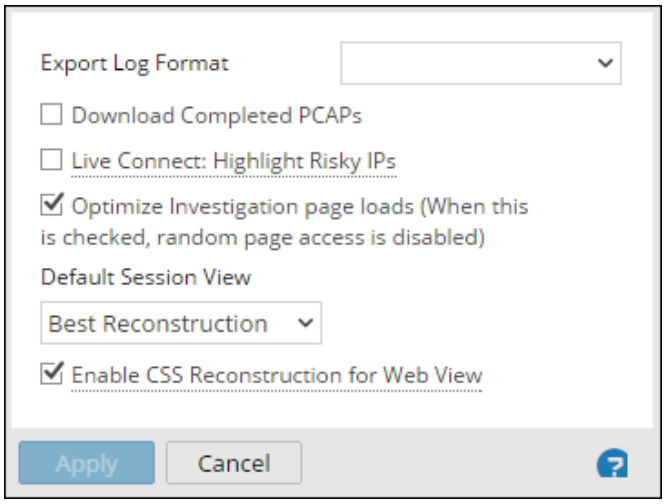
Access the Investigation Settings

To access the settings, do one of the following:

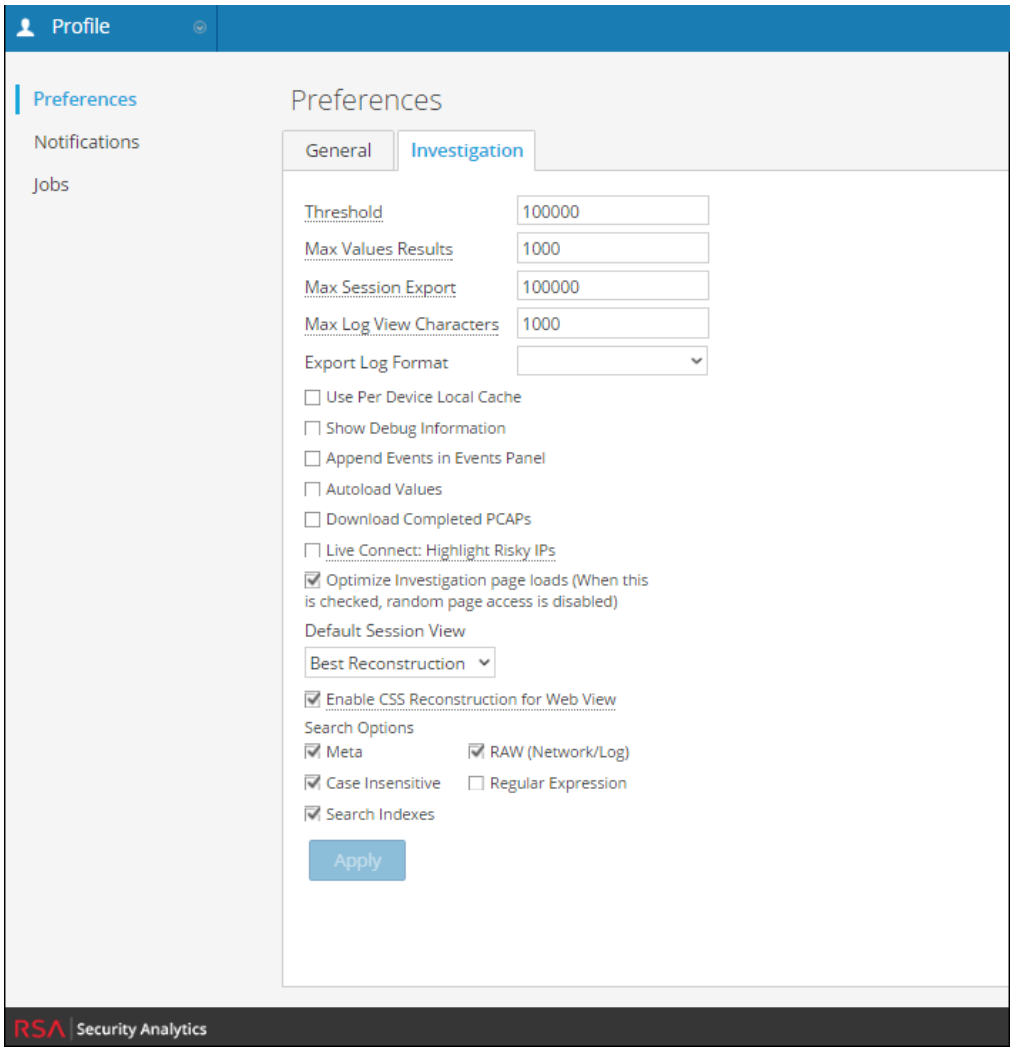
- In the **Navigate** view toolbar, select the **Settings** option.
  The Settings dialog for the Navigate view is displayed.



- In the **Events** view toolbar, select the **Settings** option.
  The Settings dialog for the Events view is displayed.



- In the **Security Analytics** menu, select **Profile**. Then in the **left navigation** panel select **Preferences.** Click the **Investigations** tab.
  The Investigation tab is displayed.



Calibrate Navigate View Value Loading Parameters

Several Investigation settings influence the performance of Security Analytics when loading values in the Values panel. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations.

To adjust these settings:

1. Navigate to the **Investigation** tab or to the **Settings** dialog for the Navigate view.
2. Adjust the following parameters:

- Threshold: Set the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.

- Max Values Results: Set the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
- Max Session Export: Specify the number of events that can be exported in a single PCAP or Log file.
- Max Log View Characters: Set the maximum number of characters to be displayed on **Investigation > Events > Log Text**. The default value is **1000**.
- Show Debug Information: If you want Security Analytics to display the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker, select this option. The default value is **Off.**
- Autoload Values: If you want Security Analytics to automatically load values for the selected service in the Navigate view, select this option. When not selected, Security Analytics displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.
- Live Connect: Highlight Risky IPs: If you want Security Analytics to highlight and display only IP addresses that are considered as risky by RSA community, select this option. When not selected, Security Analytics displays all IP addresses. By default, this option is not selected (**Off**).

3. Click **Apply**.

The settings become effective immediately and are visible the next time you load values.

Configure PCAP Download Behavior in Investigation

You can automate the downloading of extracted PCAPs in the Investigation module so that the browser downloads the extracted PCAP and opens it in the default application for opening PCAP files, such as Wireshark.

To configure this:

1. Ensure that an application that can open PCAPs is installed on your local file system and that the application is set as the default application to handle PCAP file formats.
2. Navigate to the **Investigation** tab or to the **Settings** dialog for the Navigate view or the Events view.
3. Select the **Download Completed PCAPs** option.
4. Click **Apply**.
   The setting becomes effective immediately.

Configure the Default Log Export Format in Investigation

You can export logs from Investigation in different formats. Available options are Text, XML, CSV, JSON. There is no built-in default value for the log export format. If you do not select a format here, Security Analytics displays a selection dialog when you invoke export of logs.

To select the format for exported logs:

1. Navigate to the **Investigation** tab or to the **Settings** dialog for the Navigate view.
2. Select one of the options from the **Export Log Format** drop-down menu.
3. Click **Apply**.
   The setting goes into effect immediately.

Configure the Default Meta Export Format in Investigation

You can export meta values from Investigation in different formats. Available options are Text, XML, CSV, JSON. There is no built-in default value for the meta export format. If you do not select a format here, Security Analytics displays a selection dialog when you invoke export of meta values.

To select the format for exported meta values:

1. Navigate to the **Investigation** tab or to the **Settings** dialog for the Navigate view.
2. Select one of the options from the **Export Meta Format** drop-down menu.
3. Click **Apply**.
   The setting goes into effect immediately.

Calibrate Events View Retrieval and Default Reconstruction

You can configure several parameters that control the how Security Analytics retrieves events and reconstructs events in the Events view. To do so:

1. Navigate to the **Investigation** tab or to the **Settings** dialog for the Events view.
2. Configure the following parameters.

Optimize Investigation page loads	Set a paging option. When optimized, results are returned as quickly as possible, sacrificing the original ability to go to a specific page in the event list. Deselecting this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is **enabled**.

Append Events in Events Panel	When this option is selected, the events displayed in the **Events Panel** are added incrementally. For example, each time you click the next page icon, the next increment of events is added, at first you see 1 to 25, then 1 to 50, then 1 to 75 and so on. **Note:** This option is available only if the Optimize Investigation Page Loads option is enabled.
Default Session View	Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.

3. To activate the changes immediately, click **Apply**.

Enable or Disable Cascading Style Sheet Rendering in Web Content Reconstructions

Analysts can enable the use of cascading style sheets (CSS) when reconstructing web content. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Disable this option if there are problems viewing specific websites.

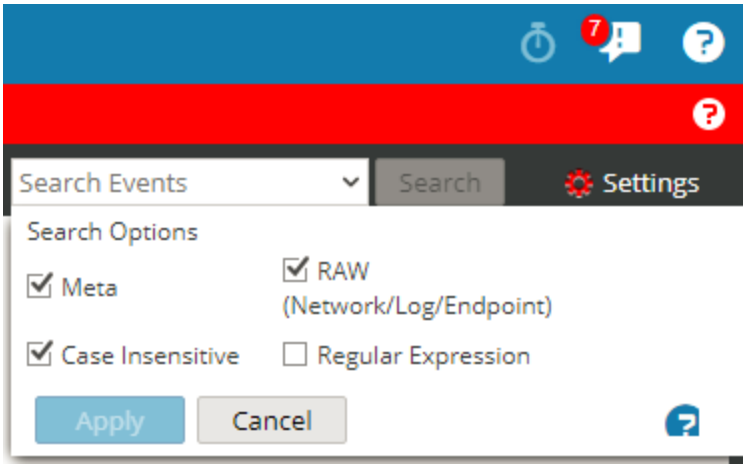
Note: The appearance of the reconstructed content may not match the original web page perfectly if related images and style sheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically via client side javascript will not render in the reconstruction because all client side javascript is removed for security purposes.

To enable or disable this option:

1. Navigate to the **Investigation** tab.
2. Select the **Enable CSS Reconstruction for Web View** checkbox.
3. Click **Apply**.
   The setting becomes effective immediately and is visible in the next web content reconstruction.

(Optional) Configure Search Options

1. Click in the **Search** field to display the Search Events drop-down menu.



2. Select one or more search options to apply to the search. Investigation - Search Options provides detailed information about each option.
3. To save the search settings, click **Apply**.
   The preferences are saved and effective immediately.

Conduct an Investigation

You can begin an investigation in several ways in Security Analytics. After you begin an investigation, there is no specific order in which to conduct the investigation. Instead, Security Analytics offers various methods of displaying the data, filtering the data, querying the data, acting on a drill point, and inspecting specific events.

- Analysts who conduct analysis using Security Analytics Investigation need to have the appropriate system roles and permissions set up for their user accounts. See Roles and Permissions for Analysts. An administrator must configure roles and permissions.

  Detailed procedures are:

  Begin an Investigation of a Service or Collection

  Filter Information in Navigate View

  Query Data in Navigate View

  Act on a Drill Point in the Navigate View

  Examine Events

Begin an Investigation of a Service or Collection

Analysts can begin an investigation of data on a Security Analytics service or collection, which results in the loading of values.

To begin an investigation in Security Analytics, a service must be specified.

- Security Analytics opens the Navigate view with the user-specified default service selected.
- If no default service is currently specified and the service id is not in the URL, Security Analytics presents a dialog for selecting the service or collection to investigate.
- When a service has been selected manually or by default in the Navigate view, you can change the service or collection to investigate by selecting the service name in the toolbar. Security Analytics presents the dialog for selecting the service to investigate.

Note: The Archiver service does not appear in the Navigate view to minimize user experience of slow performance when performing investigations. The Archiver is available in the Events view for log exports and enhanced search capabilities.

With a service or collection selected, Security Analytics is ready to load data for the service or collection. Several settings in the Navigate View and Events View Settings dialog or the Profiles > Preferences panel > Investigations tab affect the loading process: Threshold, Max Values Results, Show Debug Information, Autoload Values, and Optimize Investigation page loads (see Configure Investigation Views and Preferences).

Note: If you specified Autoload Values, Security Analytics populates the data automatically. Otherwise, you must select the Load button. Security Analytics populates the meta data in the Navigate view Values panel and results become visible almost immediately.

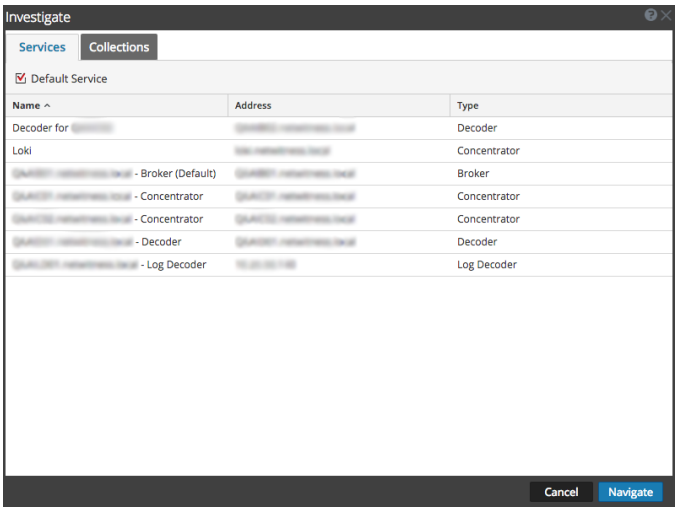
The rest of this topic provides instructions for beginning the investigation of data on a service.

Note: Only users with the administrator role can create a collection, and only the creator of the collection is able to investigate a collection.

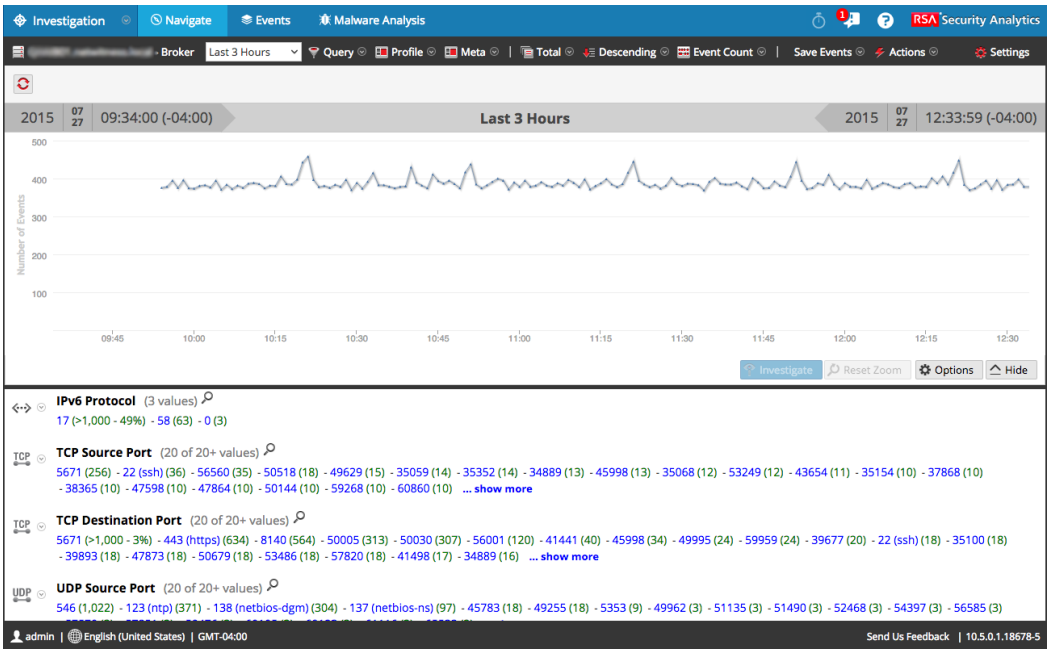
Procedures

Begin an Investigation (No Default Service)

1. In the **Security Analytics** menu, select **Investigation > Navigate**.
   The Investigate dialog is displayed.



2. Double-click a service or select a service and click **Navigate**.
   The resulting panel displays the activity for the selected service.
3. If you want to modify investigation options before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query as described in Filter Information in Navigate View.
4. When ready, click Load Values.
   The data for the selected service begins loading.

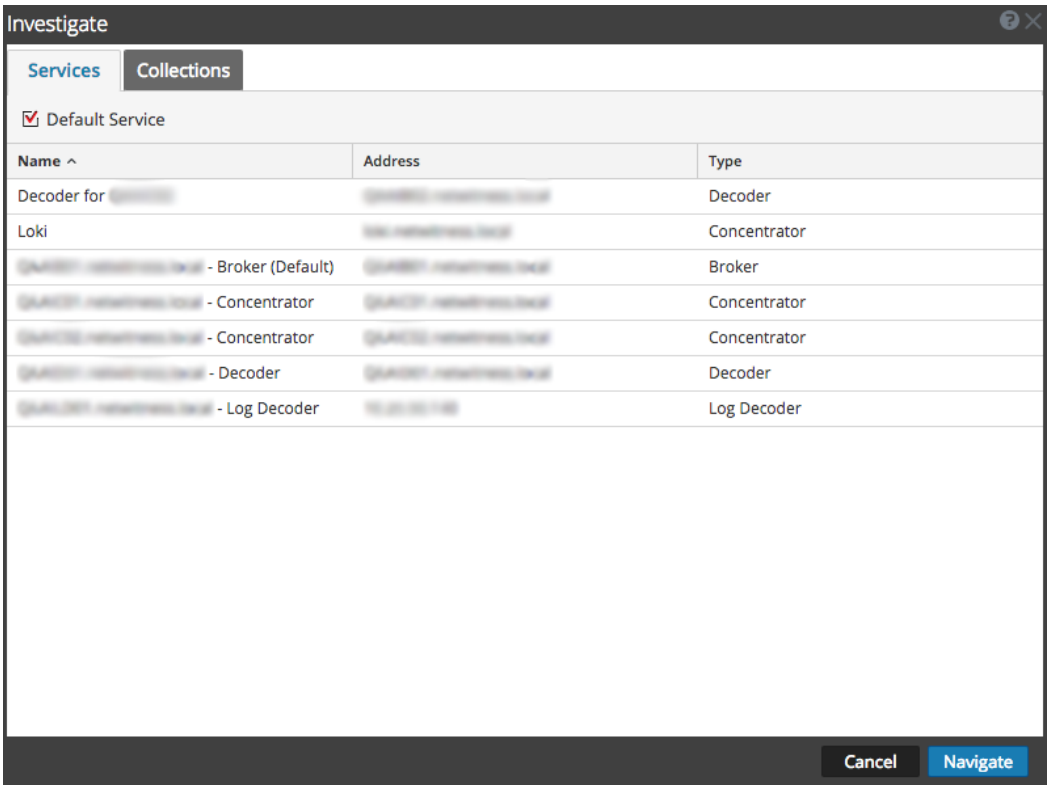


With the service selected and data loaded, you are ready to begin analyzing the data.

Set or Clear the Default Service

You can set the default service and clear the default service in the Investigate a Service dialog.

1. Click the service name in the toolbar.
   The Investigate dialog is displayed.



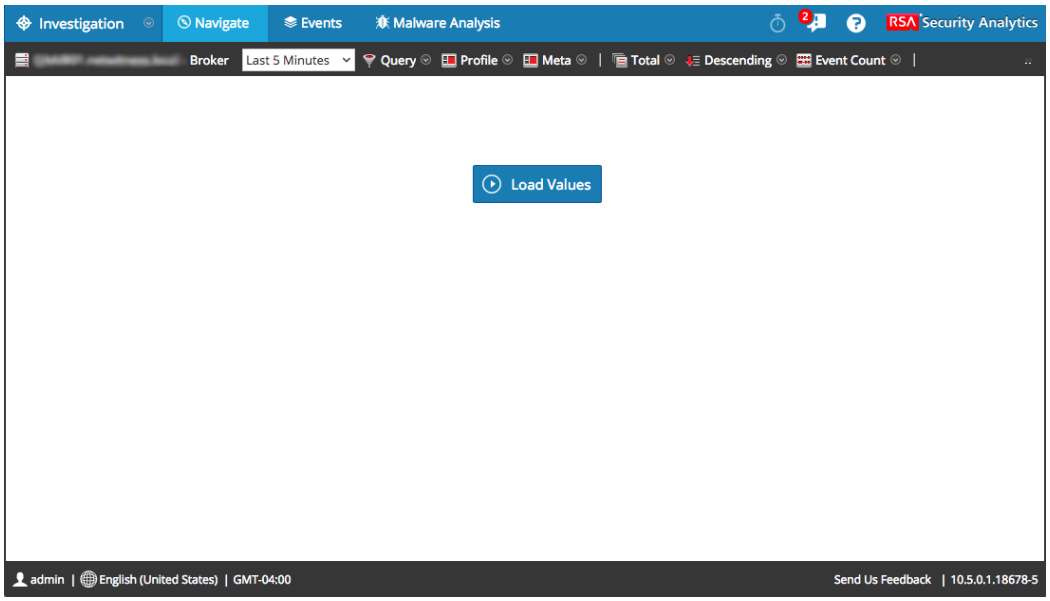
2. Select a service on the **Services** grid, and click Default Service.
   The service becomes the default, (indicated by **Default** in parentheses after the service name).

3. To clear the default service, select the default service in the grid, click Default Service, and click **Cancel** to close the dialog.
   No default service is set.

> **Note:** The Cancel button does not cancel your selection of the default service. It simply closes the dialog without navigating to the currently selected service in the grid. Setting a default service that is different from the service currently being investigated, does not refresh the Navigate view. You must explicitly select and Navigate to a different service.

Begin an Investigation (Default Service Specified)

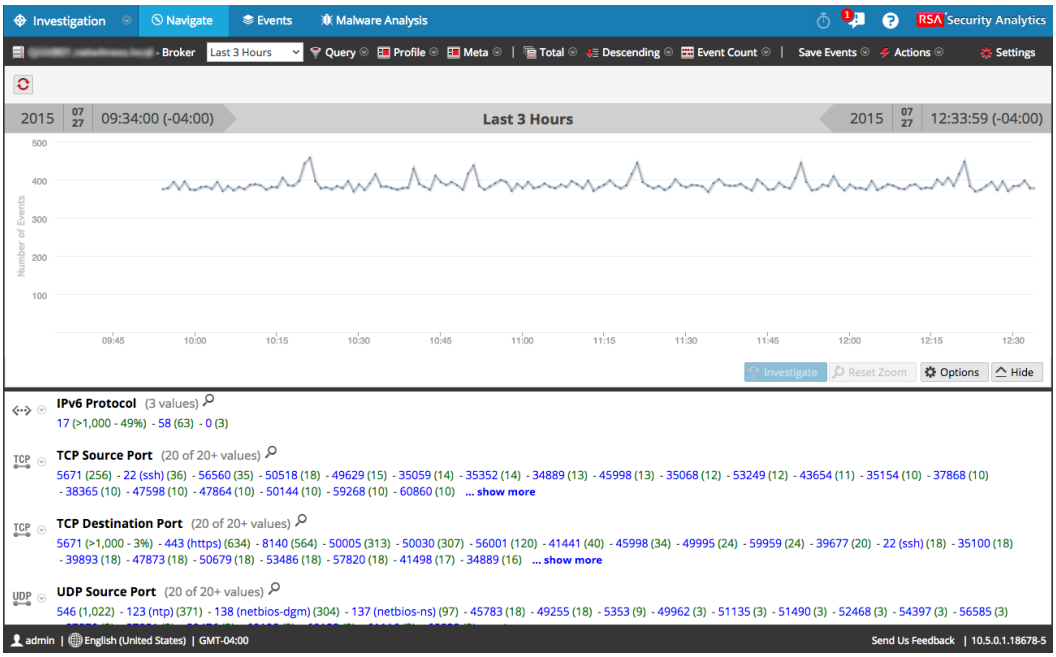
1. In the **Security Analytics** menu, select **Investigation > Navigate**.
   If the Autoload Values setting is set to off, the Navigate view is displayed with the default service selected, and ready to load data. If the Autoload Values setting is on, the values are loaded as shown in Step 3.



2. If you want to modify investigation options before loading, you can create or modify a custom profile, apply a different time range, create or apply a meta group, and perform a custom query.

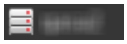
3. When ready, click 

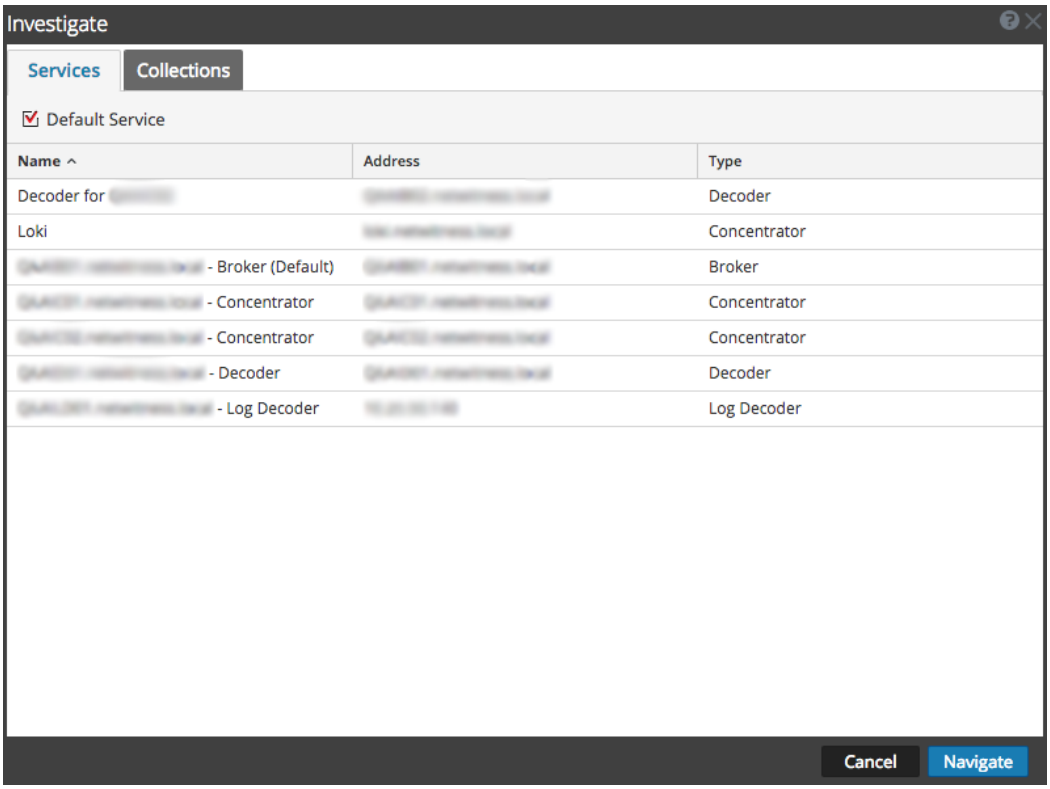
.
   The values for the service are loaded in accordance with the selected options.



With the service selected and data loaded you are ready to begin analyzing the data.

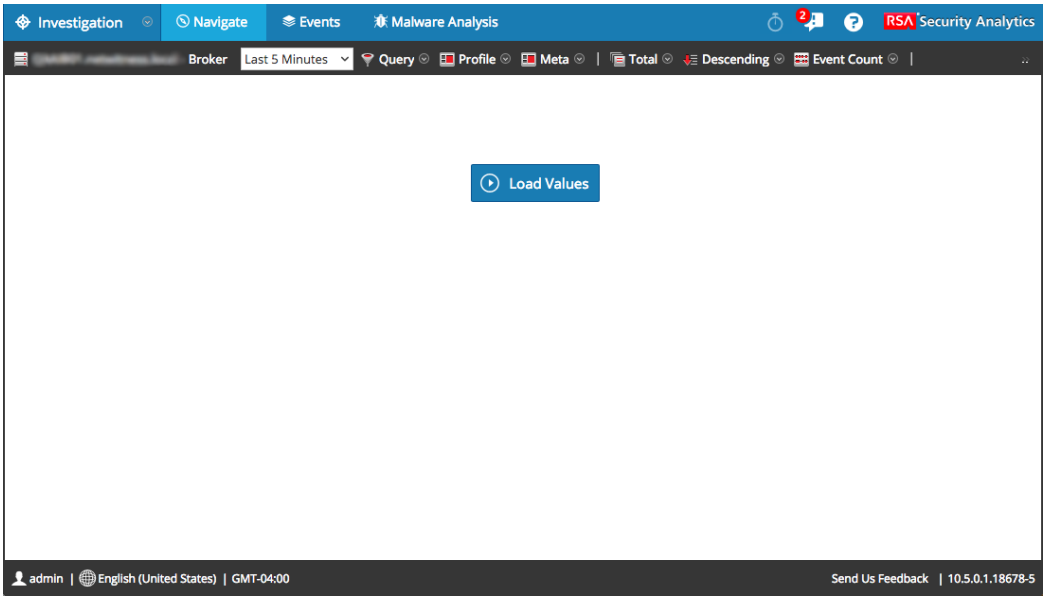
Change the Service or Collection to Investigate

1. In the Navigate view, click  (the service name) at the top of the options panel. The Investigate dialog is displayed.



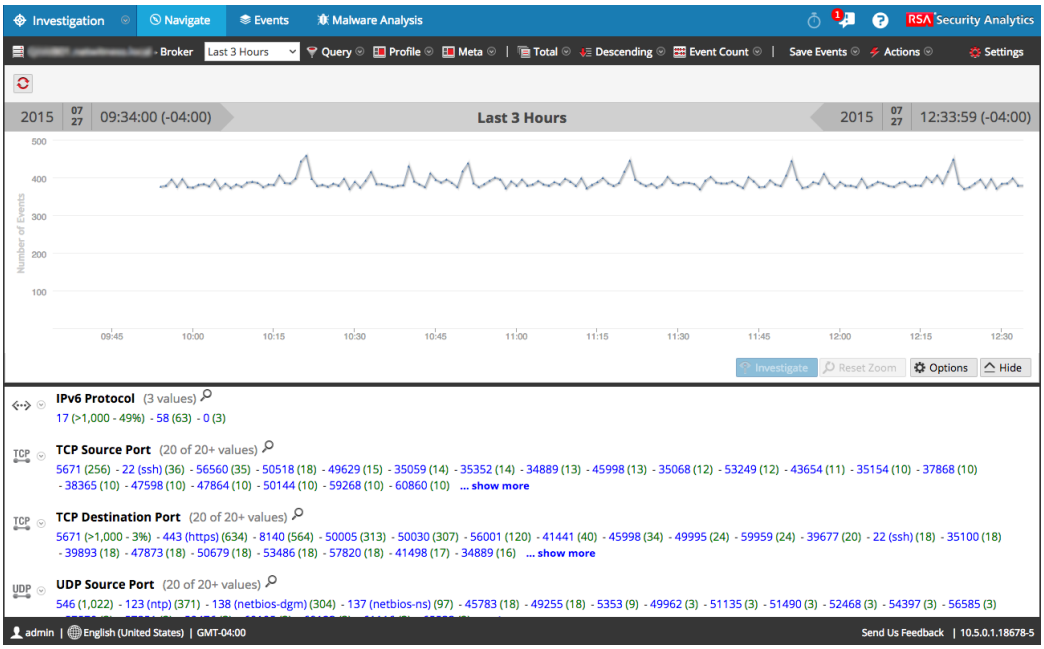
2. Double-click a service or select a service and click **Navigate**. The resulting panel displays the activity for the selected service.

   If the Autoload Values setting is on, the values are loaded as shown in Step 3. Otherwise, the Navigate view is displayed with the default service selected, and data ready to load.



3. When ready, click Load Values.

   The values for the service begin loading in accordance with the selected options.



   With the service selected and data loaded you are ready to begin analyzing the data.

Investigate Workbench Restoration Collections

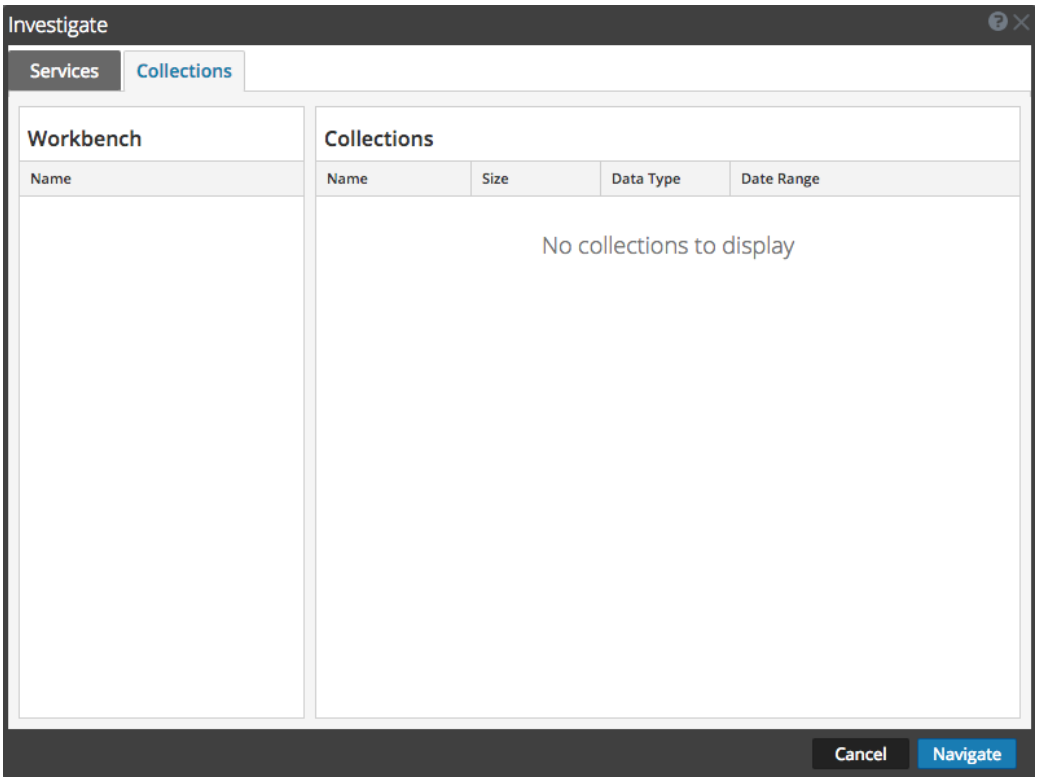
This procedure enables Administrators to select content from an existing collection to reprocess for further investigation.

> **Note:** Only a user with administrative privileges can create a collection, and you can view only those collections that you created.

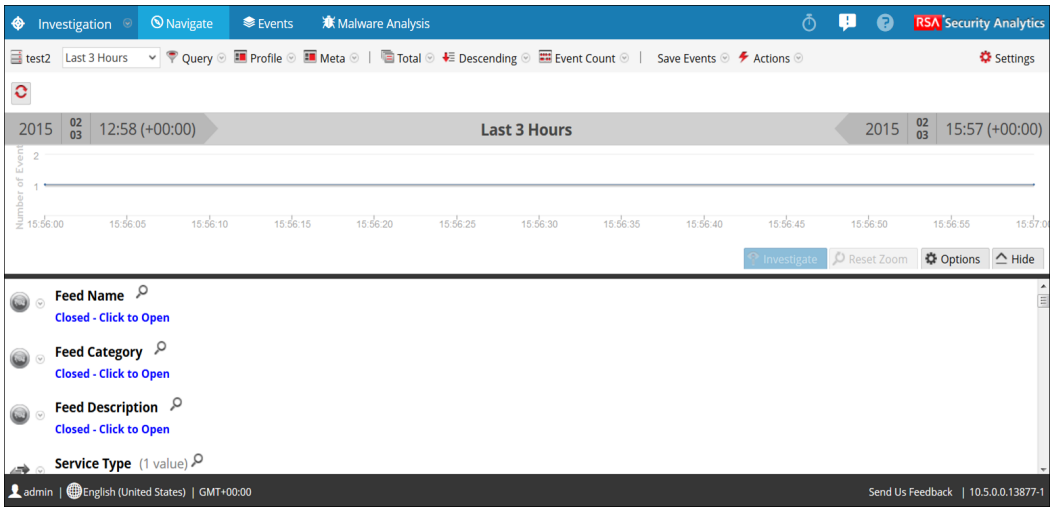
To reprocess data for further investigation:

1. In the **Security Analytics** menu, select **Investigation > Navigate**.

   The Investigate dialog is displayed.



2. Select a workbench service and workbench name that you want to investigate.
3. Click **Navigate** to perform an investigation on your selected workbench service.
   Click **Cancel** to select a different workbench service to investigate.
   The Investigation view is displayed.



With the collection selected and data loaded you are ready to begin analyzing the data.

Filter Information in Navigate View

This topic describes the methods available to filter results in the Investigation > Navigate view.

When conducting an investigation in Security Analytics, there are several methods available to refine the results displayed when meta key values are loaded in the Navigate view. Analysts can:

- Set the Time Range for an Investigation
- Set Quantification Method and Sort Sequence of Meta Key Results.
- Manage and Apply Default Meta Keys in an Investigation.
- Manage User-Defined Meta Groups
- Visualize Metadata as Parallel Coordinates
- Use Investigation Profiles to Encapsulate Custom Views.

Manage User-Defined Meta Groups

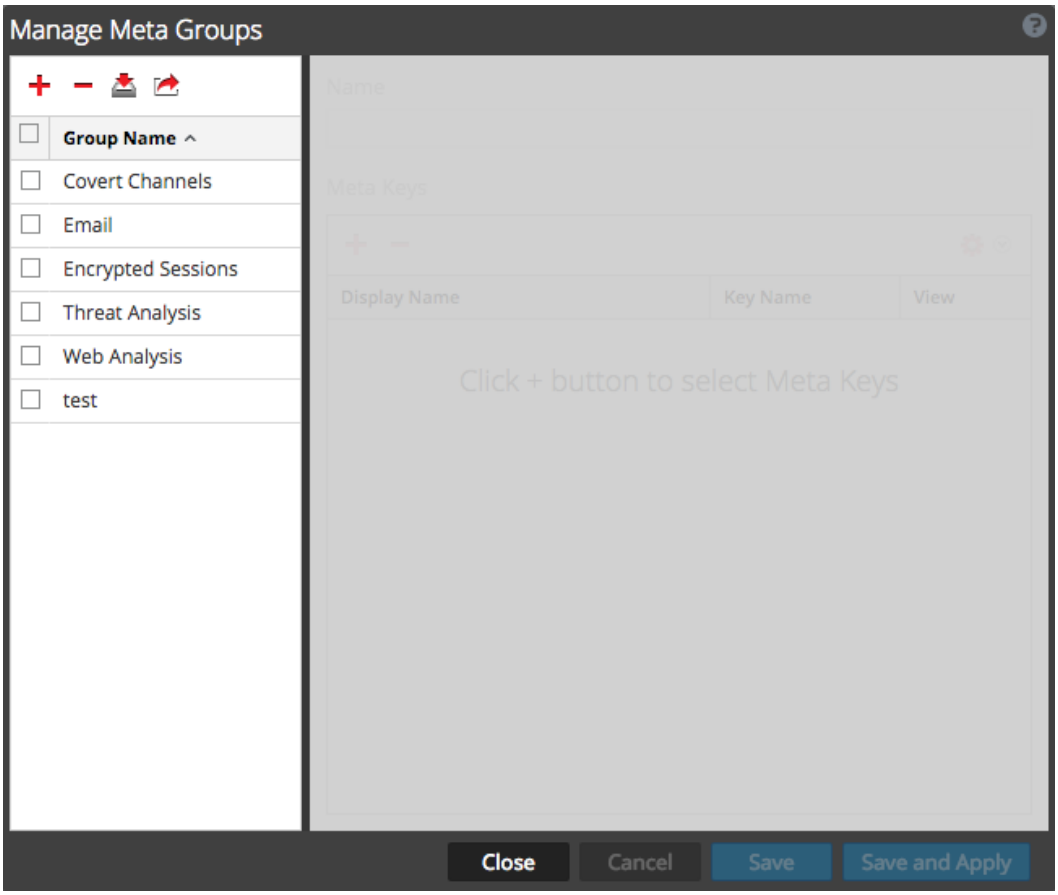
In the Investigation > Navigate view, you can define meta groups for filtering data displayed in an investigation. This section describes how to add, edit, import, export, and delete custom meta groups to be used during navigation on a specific service. In a Parallel Coordinates visualization, the meta keys in a group appear as axes from left to right. Custom meta groups are visible to all users of a service and may be exported for import to any service, limited by the available meta keys for that service.

Note: When an administrator adds custom meta groups manually by editing the custom index file for a service, the new groups become available to Investigation after the service is restarted.

Create a Meta Group and Add Meta Keys

1. While investigating a service in the **Investigation > Navigate view**, select **Meta > Manage Meta Groups** in the toolbar.

   The Manage Meta Groups dialog is displayed. Initially no groups are configured for a service. If groups have already been configured, they are listed under Group Name.

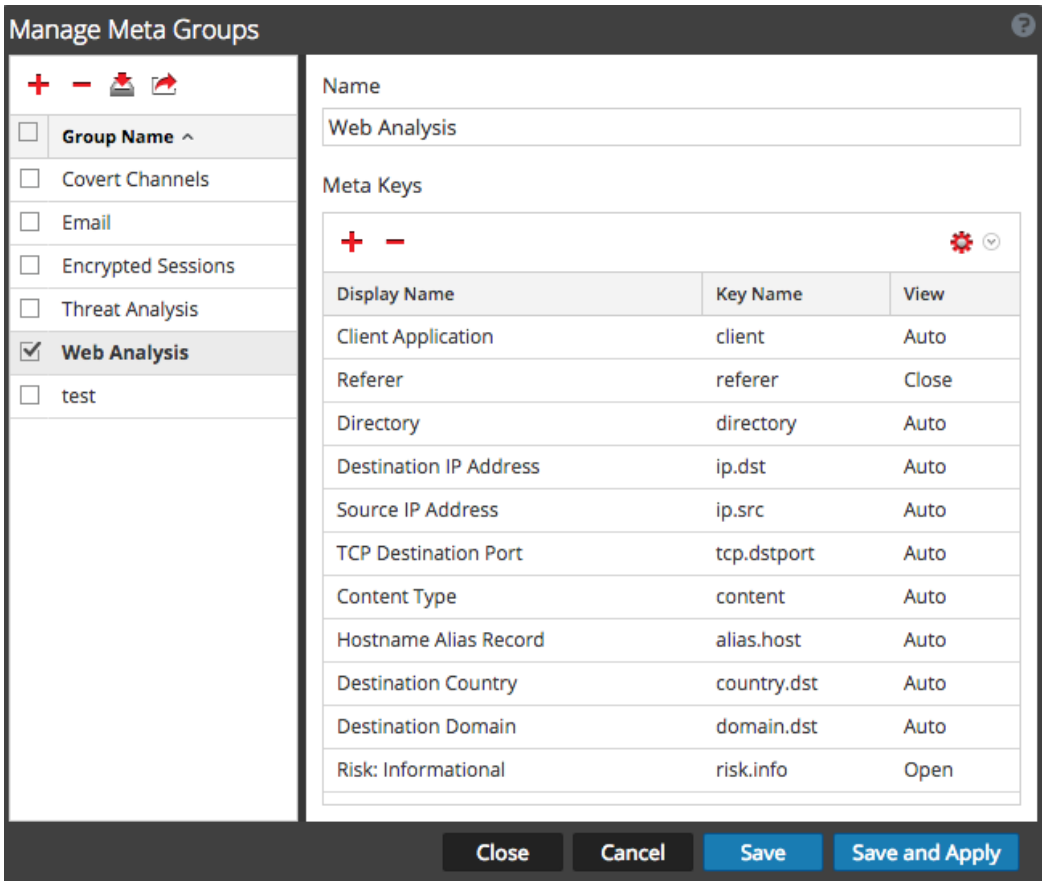


2. In the grid toolbar, click +.

   A new row is inserted at the top of the Meta Groups grid.

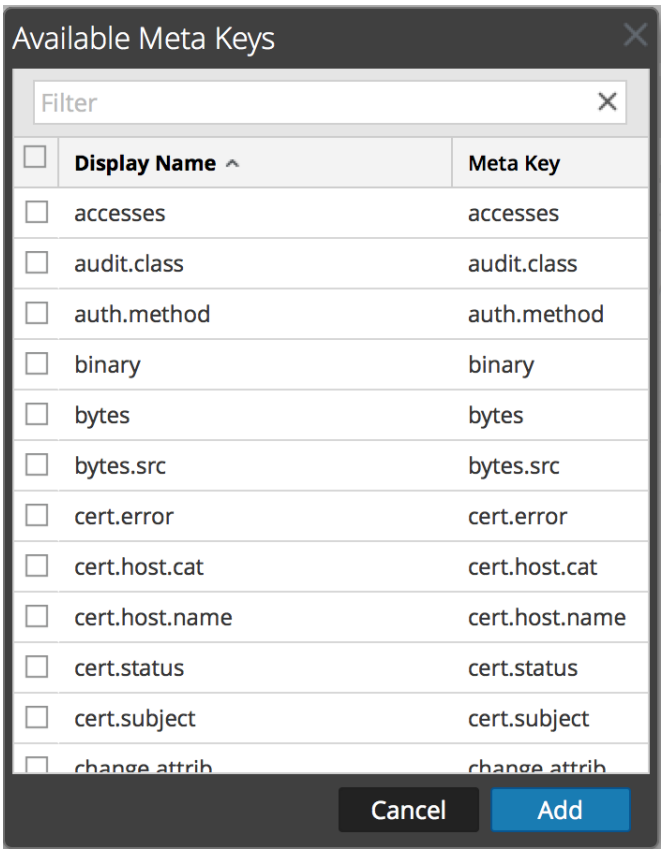
3. Type a name for the new meta group, and press **Enter**.

   The form to the right opens for editing.



4. (Optional) If you want to change the name of meta group, type a new value in the **Name** field.
5. In the **Meta Keys** toolbar, click **+**.

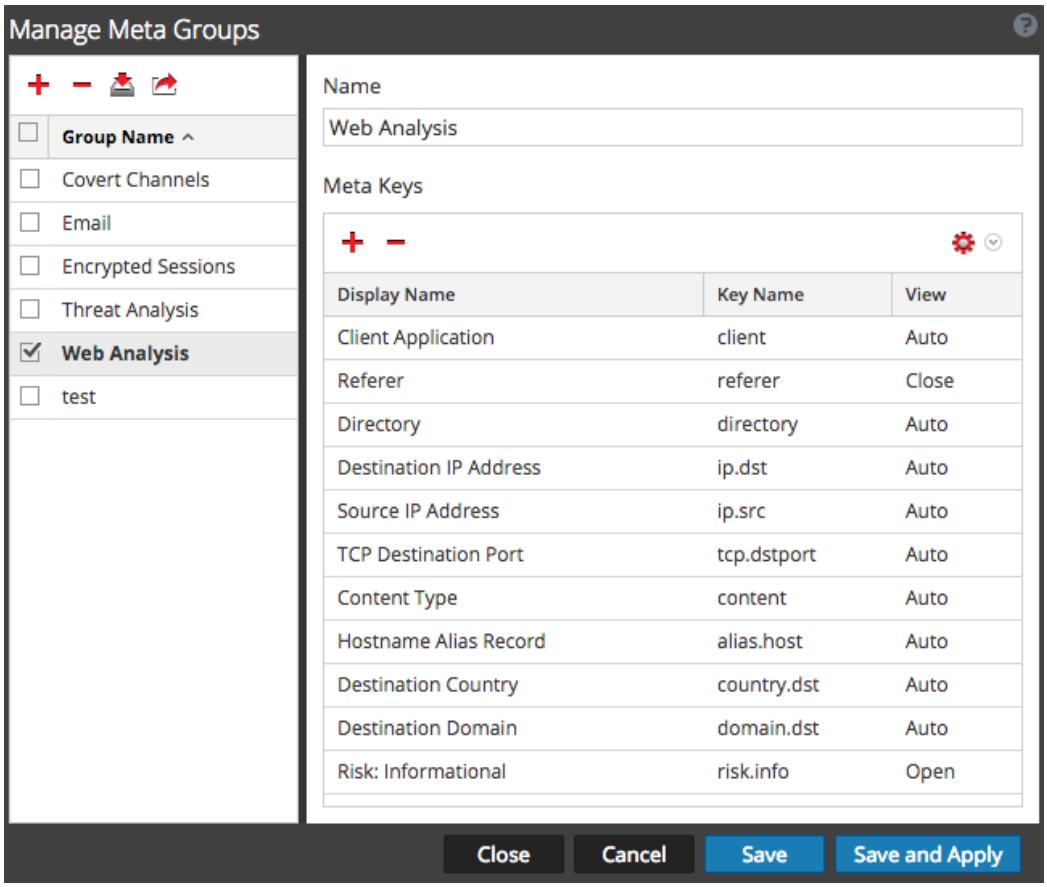
   The Available Meta Keys dialog is displayed, with keys in alphabetical order.



6. To filter the list of meta keys, type a word or phrase in the **Filter** field and select **Enter**.
   The list displays matching meta keys based on a case-insensitive search. Delete the filter text and press **Enter** to remove the filter.
7. To select meta keys to include in the meta group, click the checkboxes. To select all meta keys, click the checkbox in the title bar and click **Add**.
   The selected meta keys are added to the meta keys list.
8. (Optional) If you want to change the order in which the meta keys load and are listed in an investigation, click and drag one or more meta keys to a new position.
9. To finish creating the meta group do one of the following:
   a. To save the meta group, click **Save**.
      The group is created and available for use.
   b. To save and apply the meta group to the current Investigation view, click **Save and Apply**.
      The group is created and applied immediately to the current Investigation view.
10. Click **Close**.

Edit a Meta Group

1. Select a group from the **Meta Groups** grid.
   The form to the right opens for editing.



2. (Optional) Edit the Name of the group.
3. (Optional) Add new meta keys, as described above in Create a Meta Group and Add Meta Keys.
4. (Optional) To set the order for the keys, drag and drop one or more keys.
5. (Optional) To change the initial view of a meta key, click  and choose one of the possible views.
   When you modify the meta group, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.
   The value for the initial view is displayed in the View column.

6. To save, the changes, click **Save**.
7. To apply the changes to the current Navigation view, click **Save and Apply**.

Delete a Meta Group

1. In the **Meta Groups** grid, select the group to be removed.
2. Click − .

   A confirmation dialog provides an opportunity to cancel or complete the request.
3. Click **OK**.

   The meta group is deleted. When you close the window, if the deleted group was the currently applied meta group, it is removed and the default meta keys are used to build the view.

Export a Meta Group

User-defined meta groups are created on individual services. To make meta groups available to another service, you must export them to your local file system. To export one or more meta groups:

1. In the **Meta Groups** grid, select one or more groups to be exported.
2. Click .

   The selected groups are downloaded to your local file system as a **MetaGroups.jsn file**. Every download of meta groups has the same name with a numeral appended to avoid overwriting previous downloads.

Import a Meta Group

To make user-defined meta groups from another service available to the currently investigated service, you must import the **MetaGroups.jsn file** from the local file system. To import meta groups:

1. In the **Meta Groups** grid, select a file to export and click .

   The selection dialog is displayed.

2. Click **Browse** and navigate to the directory on your local file system where the downloaded MetaGroups.jsn files are stored. Select a file and click **Open**.
   The filename is displayed in the Upload File field.
3. Click **Upload**.
   The upload process begins, and a message indicates that the upload was successful. The meta groups are added to Meta Group grid. If the file is a duplicate of an existing meta group, a dialog tells you that the meta group already exists.

For information on OOTB Meta Groups, see Investigation - Manage Meta Groups Dialog.

Manage and Apply Default Meta Keys in an Investigation

When analysts are conducting an investigation of captured data in Investigation, a default set of meta keys is loaded and displayed in a default sequence in the Navigate view > Values panel. The default content and sequence is based on the meta keys for the service being investigated. Analysts can specify the meta keys to display during navigation by selecting the default meta keys or by selecting a user-defined group of meta keys, which provides great flexibility to define meta keys. This can help to drill down more directly to the desired data and to reduce the load time by preventing the loading of meta that is not of interest in the current investigation.

If no custom meta groups are in effect, the Navigate view is displayed with the meta key visibility specified in the Default Meta Keys dialog. To optimize loading of meta keys in the Navigate view > Values panel, Security Analytics does not open non-indexed meta keys by default. When you open a non-indexed meta key in the Values view, Security Analytics begins loading values for that meta key. If the load time is excessive, the load of the meta key times out with a message. Title, values, and counts for non-indexed meta keys are not drillable in the Values panel. Additional labeling in Investigation identifies the non-indexed meta keys, which were also present in prior releases.

To select the meta keys to apply to your investigation, you can.

- Select the default meta keys.
- Select a user-defined set of meta keys, called a meta group.

Note: Security Analytics has no built-in meta groups besides the default group. Additional meta groups must be defined before they appear in the Use Meta Group menu. Once created, user-defined meta groups can be edited, deleted, exported for use on other services, and imported to the service you are investigation. All of these procedures are provided in a separate topic: Manage User-Defined Meta Groups.

The Default Meta Keys dialog allows you to specify the default view and display sequence for meta keys during navigation in the Investigation > Navigate view for a specific service. For each key or for all keys, you can set the default view to:

- Hidden: Results for default meta key are hidden and are not available to load.
- Open: Results for default meta key are open with all values and counts displayed.
- Close: Results for default meta key are closed with only the meta name visible.
- Auto: The loading of default meta keys is controlled by the index level, which must be Indexed By Value.

When using the default meta keys, be aware that these can be modified for different services, and you may not be seeing the same set of default meta keys when navigating to a drill point on different services. If you do not see the expected data, you may need to change the initial view of the default meta keys.

When you change the initial state of default meta keys from within the Navigate view, the change persists for that service. When new keys are added to the custom index file for a Core service (for example, `broker-custom-index.xml`, `decoder-custom-index.xml`), the new keys are added to the default meta keys list. The changes made in the Navigate view apply only to the current service.

Use Default Meta Keys

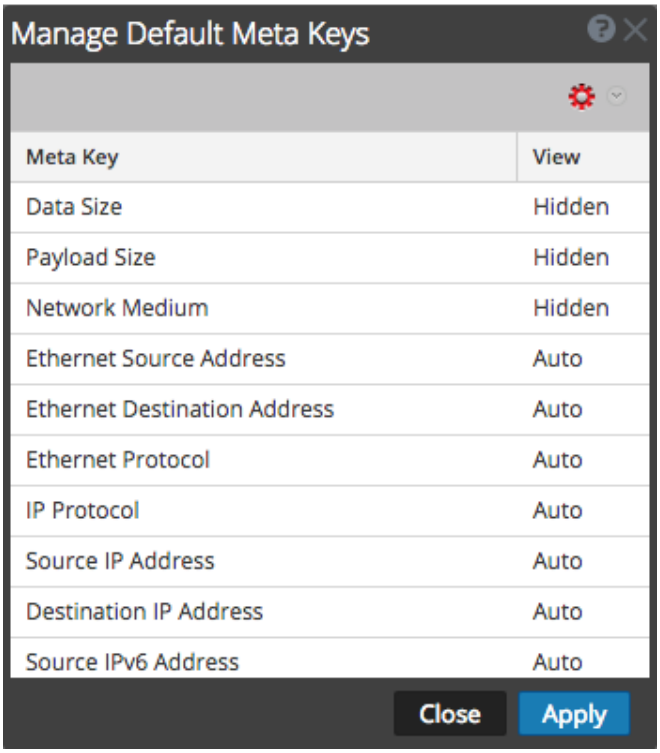
To specify that the initial Navigate view opens using default meta keys:

1. In the **Security Analytics** menu, select **Investigation > Navigate.**
2. Select a service, and select **Navigate**.
3. In the **Meta** menu, select **Use Default Meta Keys**.
   If an investigation is already in progress, the data is reloaded in the current view and an icon highlights the selected option. If no data is loaded yet, the default meta keys are used for the next load.

Configure Default Meta Keys

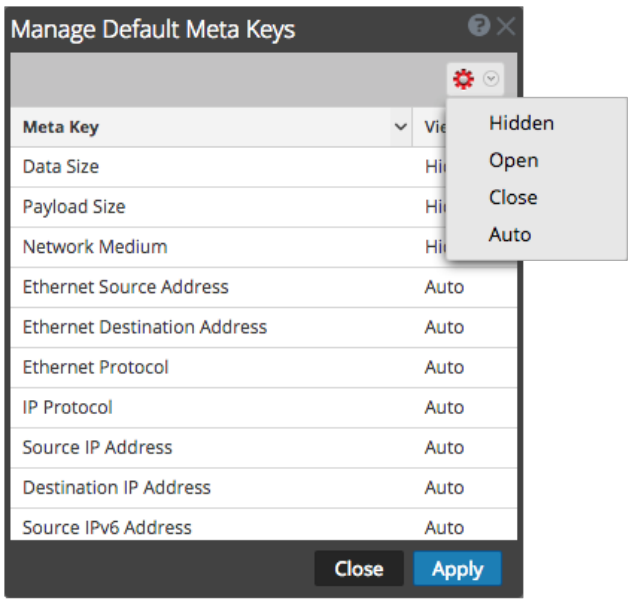
To configure the default view of default meta keys in the Investigation > Navigate view:

1. In the **Navigate View** toolbar, select **Meta > Manage Default Meta Keys**.
   The Manage Default Meta Keys dialog is displayed with the list of available meta keys for the service.



2. (Optional) To change the order of the keys, select one or more keys, and drag the values up or down through the list of keys.
3. Do one of the following:
   a. (Optional) To change the default view for all meta keys, make sure that no keys are selected and in the toolbar, select .
   b. (Optional) To change the default view for one or more keys, select the keys and in the toolbar, select .

      A drop-down of possible initial views for all default meta keys is displayed.
   c. (Optional) To revert to the default view for meta keys as specified in the service index file, make sure that no keys are selected and in the toolbar, select > **Auto**.



When you modify the default meta keys for a non-indexed meta key, you cannot set the key to OPEN. If you change the default view for a group of meta keys to OPEN and some of the meta keys are non-indexed, the non-indexed meta keys revert to AUTO. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are CLOSED until opened manually.

4. Select one of the views.
5. To save the changes, click **Apply**.

   The meta keys displayed in the Navigate view are set to your specifications. If the default meta keys are hidden, values for the meta keys are not shown in the investigation at all. If the default meta keys are closed, the values for the meta keys are not loaded by default, but you can load individual meta keys manually in the Navigate view.

Set Quantification Method and Sort Sequence of Meta Key Results

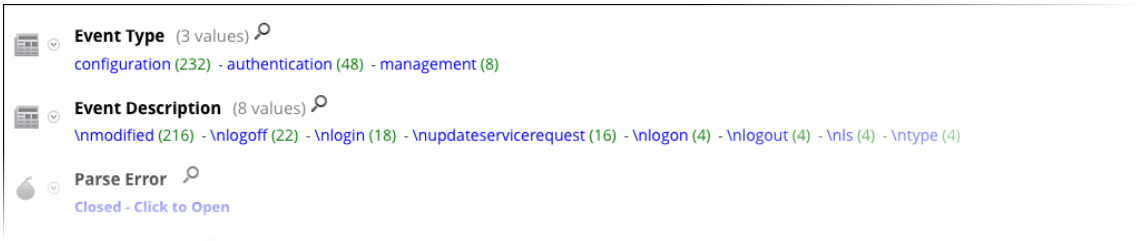
This topic provides a procedure for selecting the way results for each meta key are quantified and sequenced in the Investigation > Navigate view.

Each meta key section in the Investigation > Navigate view contains an ordered list of values showing each meta key value (Value) and its count (Total). You can specify whether:

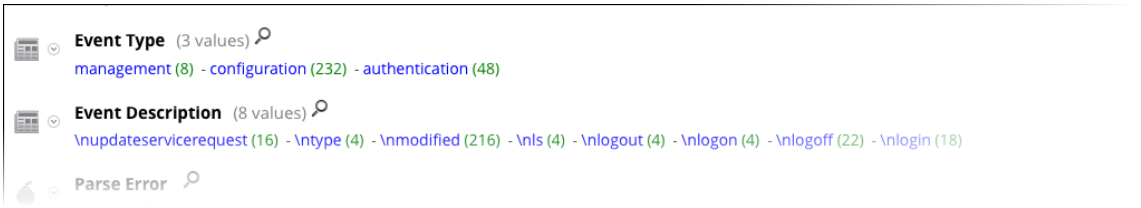
- The results in each meta key section are sorted based on Value or Total.
- The results are sorted in ascending or descending order.
- The values shown for each meta key are quantified by number of packets (Packet Count), number of sessions or logs (Quantify by Event Count) or by the size of events (Quantify by Event Size).

Note: If you have both a log decoder and a packet decoder for which you are viewing the metadata, the calculation of what is actually being counted is dependent on the type of key. If you select to Quantify by Packet Count and are looking at logs, the Navigate view output is the same output as if you had selected Quantify by Event Count (see Investigation - Navigate View for details).

This image shows the `Event Type` meta key presented in order by **Total** in **Descending** order. The value with the greatest count of matches is presented first. The value `configuration` has 232 matches and is listed first. The value `management` has only eight matches and is presented last. The quantification method is **Event Count**.

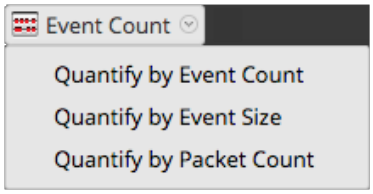


This image shows the `Event Type` meta keys presented in order by **Value** in **Descending** order. The value names are presented in alphabetical order starting at the end of the alphabet. The value `management` is listed first. the value `authentication` is presented last. The quantification method is **Event Count**.



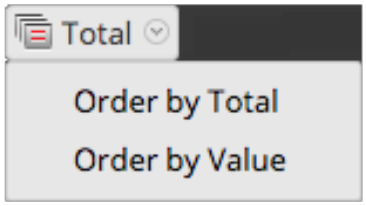
To select the quantification method of meta key count and ordering of meta key results displayed in the Navigate view:

1. In the toolbar, select **Event Count**, **Event Size**, or **Packet Count** and choose one of the quantification options in the drop-down menu. The label for the menu displays the selected option.



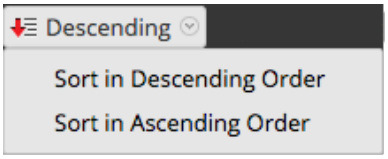
   The current view is reloaded according to your selection.

2. In the toolbar select **Total** or **Value** and choose one of the ordering methods in the drop-down menu. The label for the menu displays the selected option.



   The current view is reloaded according to your selection.

3. In the toolbar, select **Ascending** or **Descending** and choose one of the sort order options in the drop-down menu. The label for the menu displays the selected option.
   The current view is reloaded according to your selection.



Set the Time Range for an Investigation

When conducting an investigation in the Investigation > Navigate view, the time range options limit the results returned. You can select:

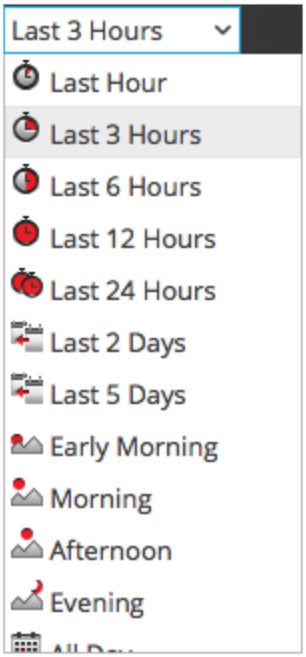
- A time range relative to the collection. Ranges relative to the collection are based on the last collection time for data.
- A time range relative to the calendar.
- A custom date range.
- All data.

The selected Date Range (type) is shown in the options panel as the Time Range label; by default the label is **Last 3 Hours**. The Time Range display shows the first and last timestamp for the date range being used for the Meta Data.

Note: Time range is based on the Time Zone configured in the Profile Preferences panel as described in "Configure User Preferences" in the *Security Analytics Getting Started Guide*.

Select a Built-In Time Range for the Investigation

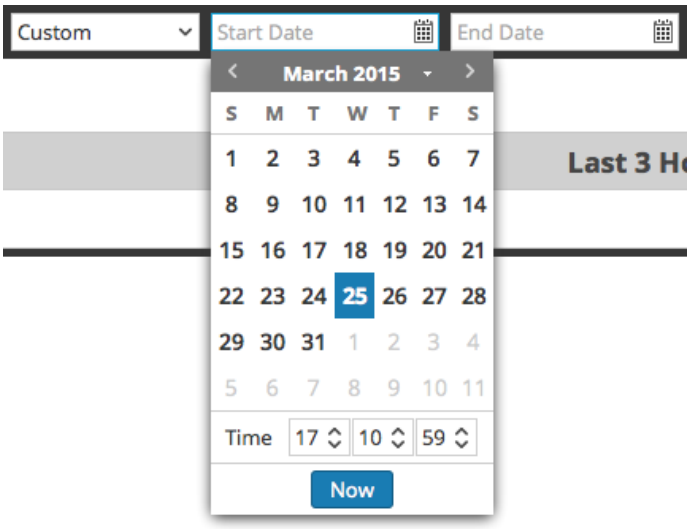
1. In the options panel, click the **Time Range** option in the Navigate view toolbar. The default time range is for the **Last 3 Hours**, but a different value from the selection list, for example, **All Data** or **Last Hour,** may already be selected and used as the label in the options panel.) The Time Range selection list is displayed.



2. Do one of the following:
   a. If you want to see all data, select **All Data**.
   b. If you want to set a time range in minutes, hours, or days that is relative to the collection, select a value such as **Last 10 minutes**, **Last 3 Hours**, or **Last 5 days**.
   c. If you want to set a time range relative to today, select **Yesterday**, **All Day**, or a part of the day such as **Early Morning**, **Morning**, **Afternoon**, or **Evening**.
   d. If you want to set a unique date range, select **Custom** in the **Time Range** menu and follow the procedure below.
      The selected time range is applied to the current results in the Values panel.

Specify a Custom Time Range for an Investigation

1. Select **Custom** in the **Time Range** menu.
   Date selection options are displayed in the toolbar.



2. Within the time **Start Date** and **End Date** fields, do the following to specify the date and time:

   a. Click a date from the calendar.

   b. (Optional) Select the time from the Hour, Minute, Second fields or click **Now**. The time selection defaults to the current time of day.

Note: If you specify custom start or end times in seconds, the value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time is interpreted as "HH:MM:00 - HH:MM:59." Seconds display in this format in **Investigation > Navigate** functions.

3. To apply the range, click **Go**.

   The selected time range is applied to the current results in the Values panel.

Use Investigation Profiles to Encapsulate Custom Views

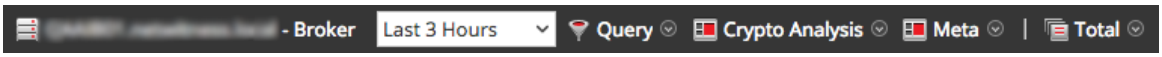
This topic tells analysts how to use Profiles that define a set of Investigation preferences for the Navigate and Events view.

Using profiles is a quick and easy way to customize which data is displayed in Investigation. In the Manage Profiles dialog, you can use a profile to specify which meta groups and column groups are displayed by default, to append queries to an investigation, and to import or export profiles.

Note: Profiles are shared across users in the same Security Analytics network. If one user modifies or deletes a profile it has an affect on what is available to the other users.

If you have multiple profiles, you can switch between them to quickly change to the selected profile's preferences. If a profile is currently active, the title of the Profile menu is replaced with the profile name.

The following figure illustrates this in the Navigate view. The profile name is displayed between Query and Meta.

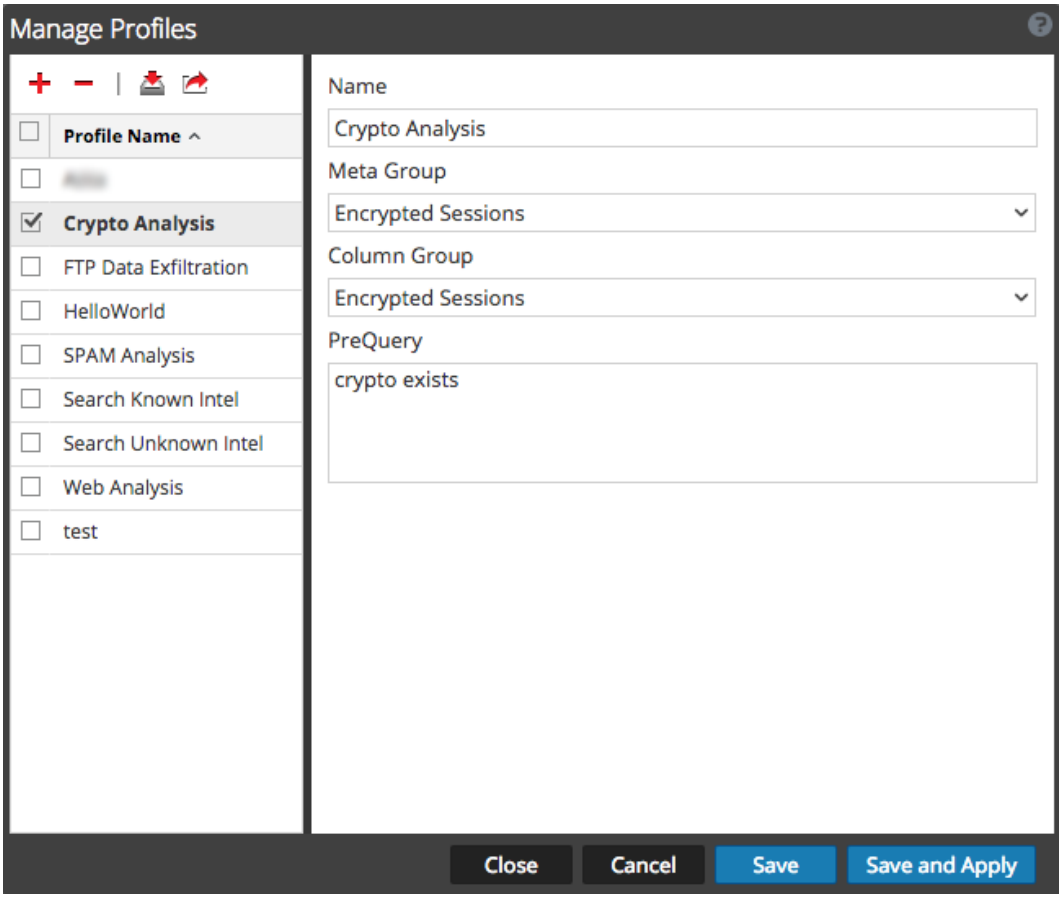


The following figure illustrates this in the Events view. The profile name is displayed between Query and List View.

Navigate to the Manage Profiles Dialog

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Investigation > Events**.
2. If the **Investigate** dialog is displayed, select a service and click **Navigate**.

3. In the toolbar, select **Profile > Manage Profiles**.
   The Manage Profiles dialog is displayed.



Create and Edit Profiles

1. In the **Manage Profiles** dialog, either select an existing profile by clicking the checkbox beside the name, or click + to create a new profile.
   The right panel is available.
2. Edit or enter the profile name by typing in the **Name** field. The name must be between 2 and 80 characters.
3. Select a meta group from the **Meta Group** drop-down list. You can add custom meta groups as described in Manage User-Defined Meta Groups.
4. Select a column group for the **Column Group** drop-down list. You can add custom column groups as described in Manage Column Groups in the Events View.

5. Type queries to filter results in the **PreQuery** field. PreQuery follows the same syntax as the Query builder. The PreQuery in the figure uses a meta group called **crypto exists**.
6. Click **Save** to save the profile without using it, or click **Save and Apply** to save the profile and use it immediately.
   If you click **Save and Apply**, a confirmation dialog is displayed before setting the selected profile as active.

Change Active Profile

If you do not see enough results or the right results in the Navigate or Events views, you may have a profile active. If you do not want to use any profiles, you can click **Deactivate Profiles** in the **Profiles** drop-down menu.

To use a different profile:

1. In the **Navigate** or **Events** view toolbar, open the **Profiles** drop-down menu.
2. Hover over the **Profile** option to display a drop-down list of available profiles.
3. Select the profile you want to use.
   The profile settings are applied immediately.

If you want to change the active profile from the Manage Profile dialog:

1. In the **Navigate** or **Events** view toolbar, select **Profiles > Manage Profiles**.
   The Manage Profiles dialog is displayed.
2. Select a profile from the left panel and click **Save and Apply**.
   A confirmation dialog is displayed.
3. Click **Yes**.
   The profile settings are applied immediately.

Import Profiles

You can upload or import .jsn files that have been downloaded from another service.

1. In the **Manage Profiles** dialog, click  in the left panel toolbar.
2. The Profile Import dialog is displayed.
3. Click **Browse** or the **Upload File** field to select a file from your computer.
4. When the file is selected, click **Upload**.
   The profile is displayed in the left panel.

Download Profiles

Profiles are downloaded as .jsn files.

1. In the **Manage Profiles** dialog, select one or more profiles from the left panel.
2. In the left panel toolbar, click  .

   The download begins immediately.

Visualize Metadata as Parallel Coordinates

This topic tells analysts how to use the parallel coordinates visualization in the Navigate view to focus the investigation on combinations of meta keys and values that may indicate events are abnormal and worth investigation.

The parallel coordinates chart is a way of visualizing the current drill point in Investigation to examine more than two meta keys simultaneously. Visualizing multiple meta keys simultaneously can help in identifying security issues associated with multivariate patterns and comparisons, such as when individual meta keys and values may not be of concern, but combining them together may bring an abnormal pattern or relationship to light.

Best Practices for Effective Parallel Coordinates Charts

To create effective parallel coordinates charts, follow these recommendations:

- Start from a drill point in the Navigate view rather than attempting to visualize all data.
- Limit the time range if necessary.
- Choose the smallest useful set of meta keys to display as axes.
- Specify the sequence of axes to highlight anomalies between the meta values as you follow a line across the chart.
- When you can identify a useful set of meta keys and sequence, create a custom meta group to use for future investigations. For example, you can create a custom meta group for Windows executable file types.
- Import custom meta groups that RSA has distributed through the RSA community.
- Re-use and share custom meta groups by importing and exporting groups as .jsn files.
- It may be useful to create two versions of each custom meta group. One for analysis of meta values and one for creating a parallel coordinates chart focusing on a smaller subset of the same use case.

Note: When importing meta groups meta groups into Security Analytics server, Security Analytics displays an error message if any of the groups are already present in Security Analytics. To import a group that is a duplicate, you must first delete the existing group. If you want to delete a meta group, it can not be in use by a profile.

To help build better parallel coordinates charts, several optimizations are included in Security Analytics10.5 and above.

- Analysts can specify that only sessions in which all meta keys exist are rendered in the chart.
- The administrator can increase the number of meta values rendered in the Parallel Coordinates Settings in the Administration System view.

RSA Meta Groups for Parallel Coordinates Use Cases

A set of predefined custom meta groups is available through the RSA community as a jsn file: MetaGroups_ootb_w_query.jsn. To get started with some meta groups that RSA has configured to highlight certain activities, you can import this .jsn file in the Manage Meta Groups dialog. Some of the targeted activities that lend themselves well to Parallel Coordinates visualizations are:

- Botnet Beaconing
- Covert Channels
- Email
- Encrypted Sessions
- File Analysis
- Malware Analysis
- Query Files
- Query Hosts
- Query IPs
- Query Mail
- Query Users
- Query Web
- SQL Injection Attacks
- Threat Analysis
- Web Analysis

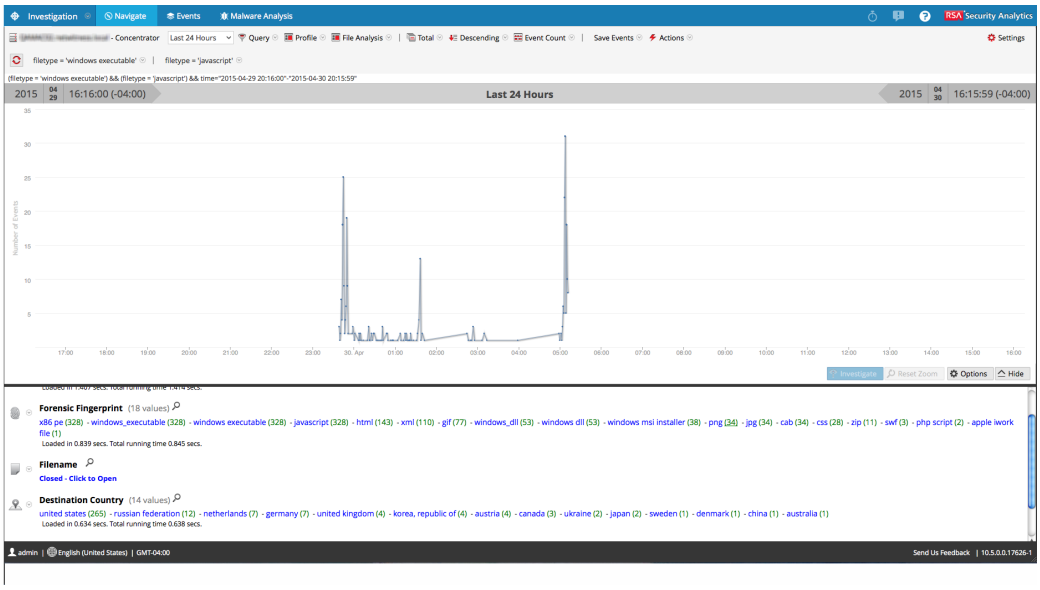
View a Parallel Coordinates Visualization

From an investigation in the Investigation > Navigate view:

1. If the Visualization panel above the Values panel is closed, select **Visualization**.
2. In the toolbar, select **Use Meta Group > File Analysis**.

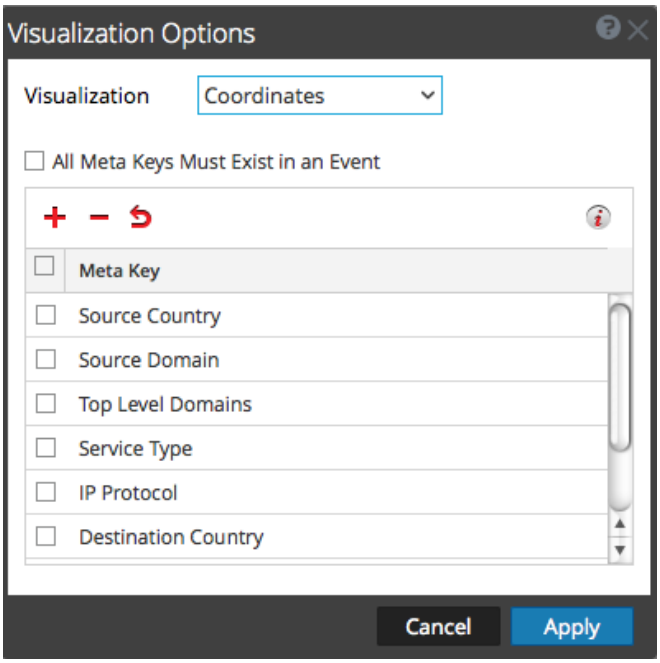
3. In the **Values** panel, in the **Forensic Fingerprint** meta key, click `windows_executable` and then `javascript`, so that the breadcrumb reads `filetype = 'windows_executable' | filetype = 'javascript'`.

4. A default visualization for the current drill point is displayed as a timeline.

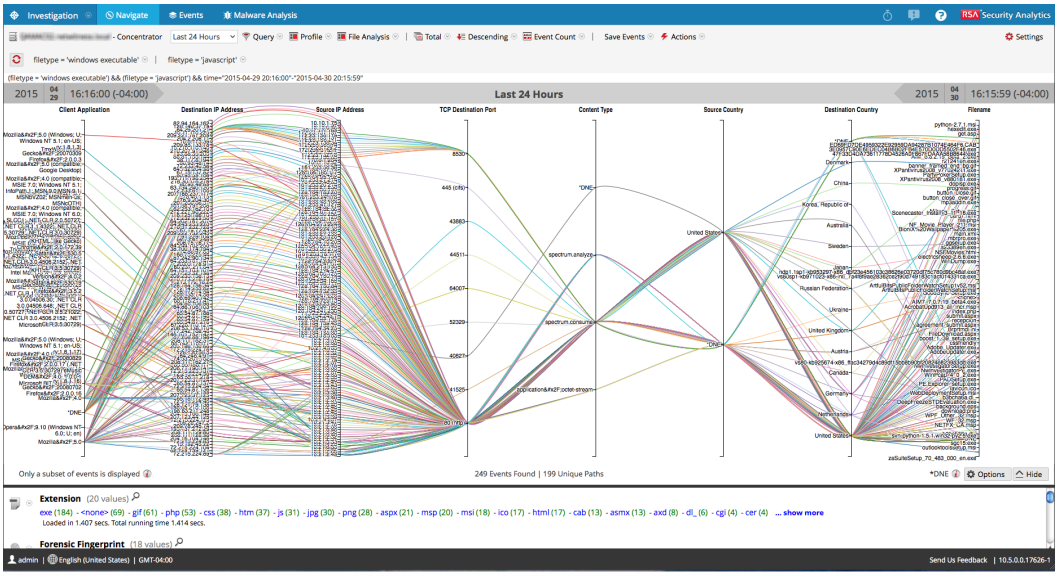


5. In the **Visualization** panel, select **Options**.
   The Visualization Options dialog is displayed.

6. In the **Visualization** drop-down list, select **Coordinates** and click **Apply**.



The visualization is loaded. In this example, 249 events are found and 199 unique paths are visualized.

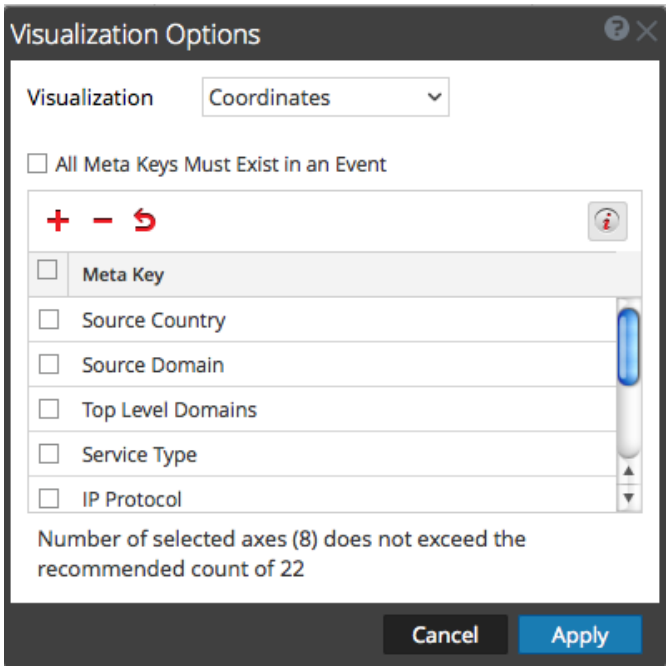


Select Meta Keys for a Parallel Coordinates Visualization

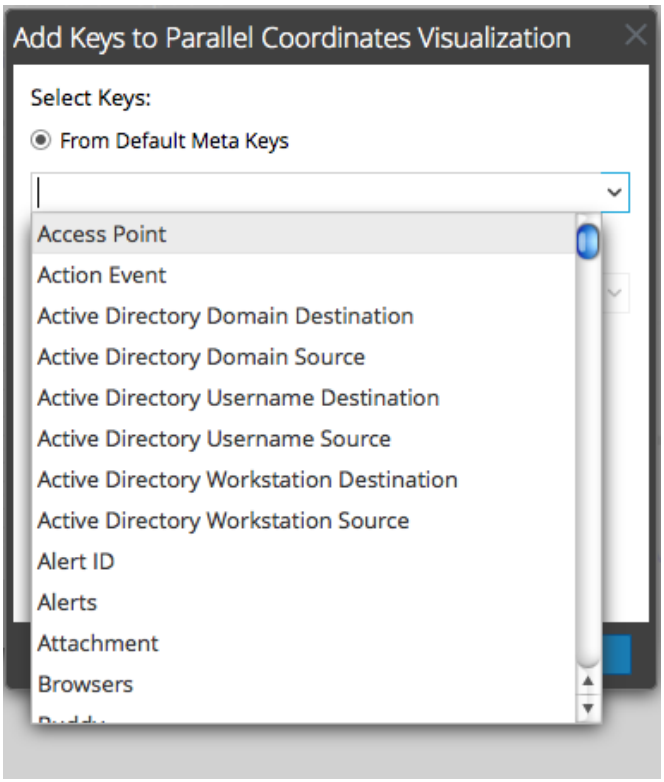
With a Parallel Coordinates visualization open, do the following:

1. In the Visualization panel, select **Options**.
   The Visualization Options dialog is displayed. In the toolbar, click to display the

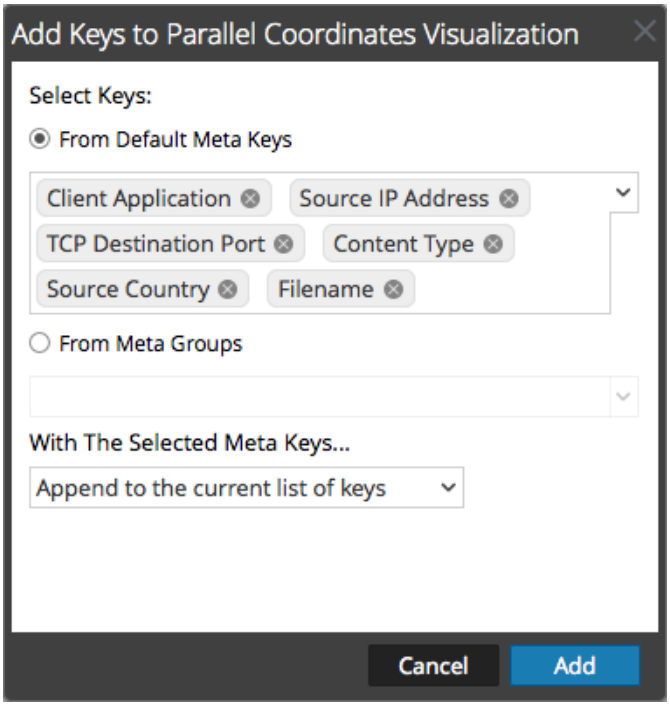
recommended number of axes for a readable visualization. When a recommended count of keys is displayed, the count changes based on the browser size. If you make the browser window larger, the recommended count is increased.



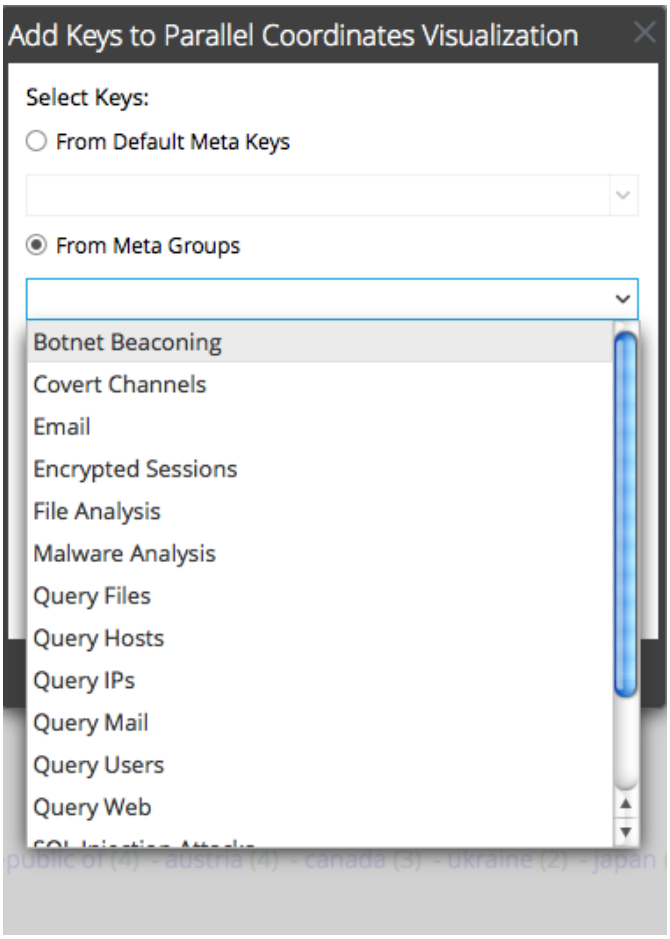
2. If you want to change the sequence of the meta keys, drag meta keys up or down to the desired sequence.
3. If you want to delete any meta keys, click in the selection box, and click −.
   The meta keys are removed, but the change has not been applied.
4. If you want to revert to the previous state, click ↩.
   Any meta keys you have deleted are restored and any changes that you made are removed.
5. If you want to select individual meta keys, click +, select **From Default keys**, and in the drop-down list, select the meta keys.



The selected keys are listed.

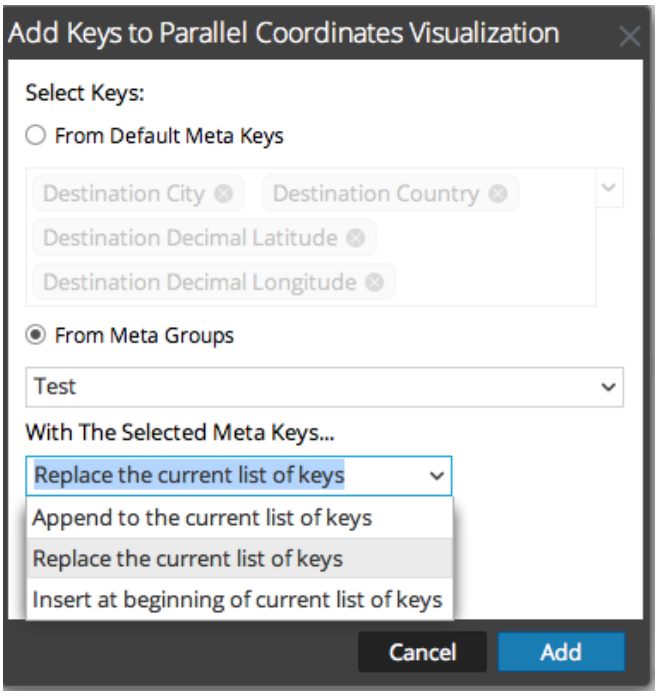


6. If you want to add all the keys in a meta group, you cannot add individual meta keys. Select **From Meta Groups**, and select a group from the drop-down list.



The selected meta groups are listed in the field.

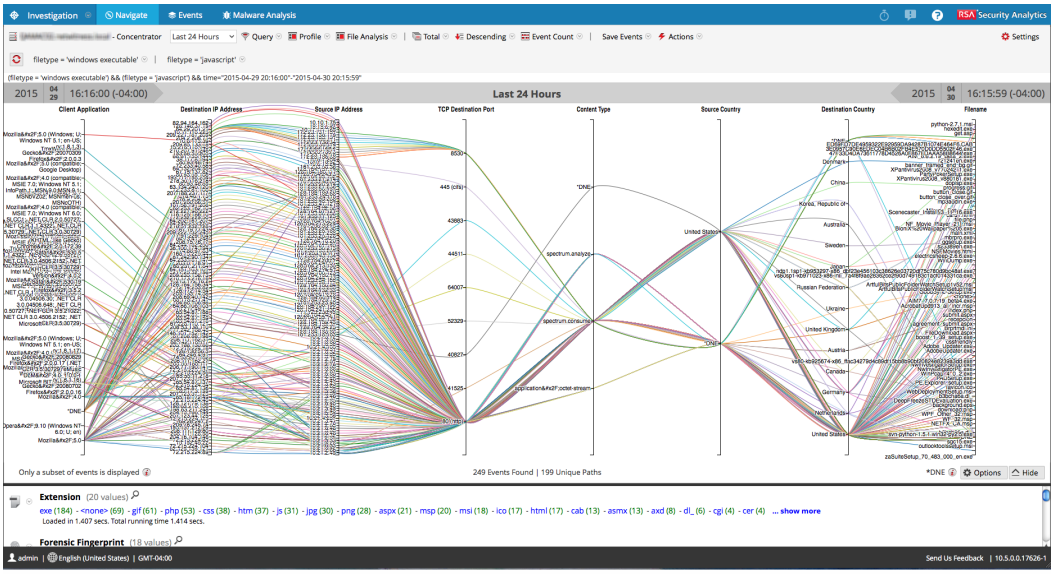
7. Select the method of adding the keys or groups: **Replace the current list of keys**, **Append to the current list of keys** (at the end), or **Insert at the beginning of current list of keys.**



8. To complete the procedure, click **Add**.

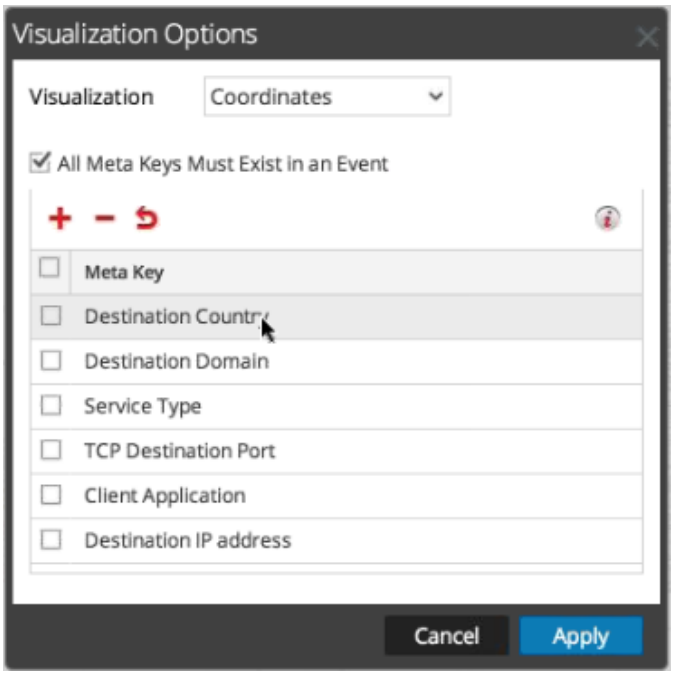
   The Visualization Options dialog is displayed with the meta keys or groups you selected.

9. To display the new visualization chart, click **Apply**.



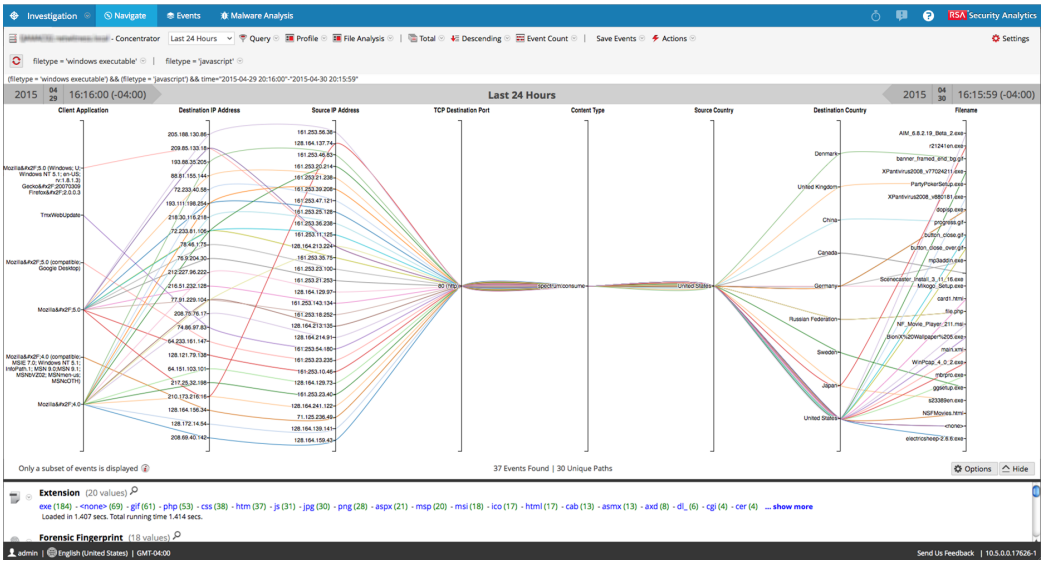
Optimize a Parallel Coordinates Visualization

1. To optimize the visualization by removing events in which not all meta keys exist, select **Options.**



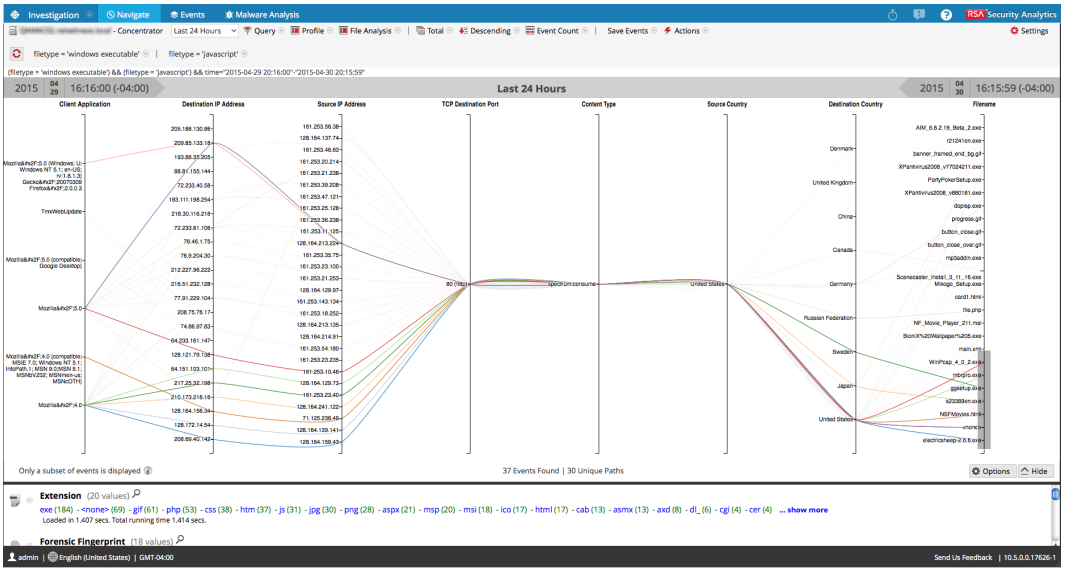
2. In the Visualization Options dialog, select **All Meta Keys Must Exist in an Event**. Click **Apply**.

   The resulting graph is more readable and useful and usually has fewer unique paths.



3. If you want to highlight a small set of points to see the path of the line from right to left, click on an axis. The cursor changes to cross hairs, which you can drag to select one or more

values. When you let go of the mouse, the lines are highlighted. In the example below, the SSL service type is highlighted by a gray box.



4. If you want to enlarge the visualization, drag the bottom edge of the panel down and drag the right edge of the browser window wider.

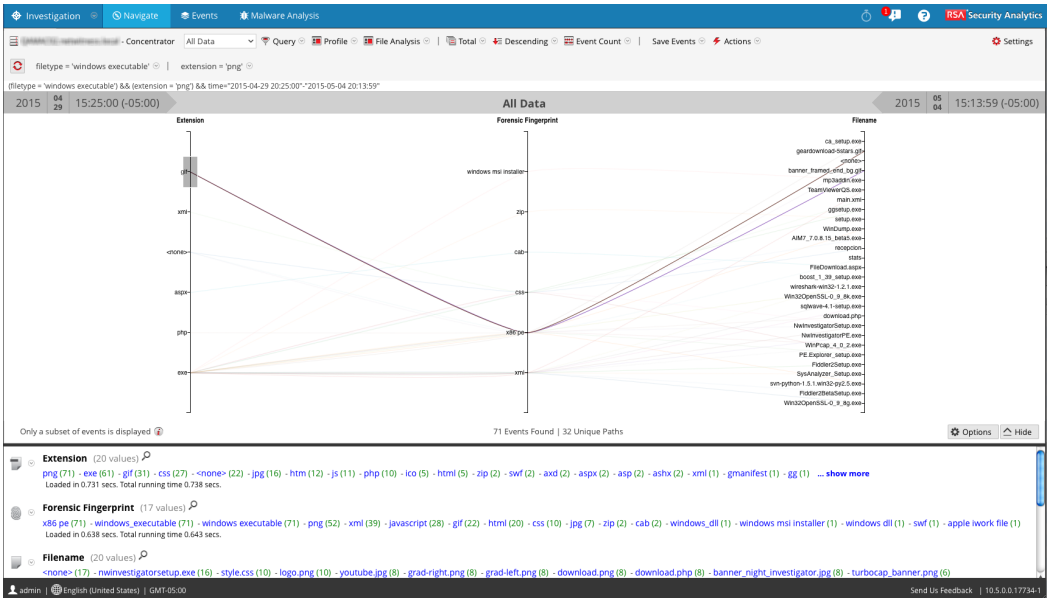
Sample Use Case

Below is an example of a parallel coordinates visualization of meta keys representing file metadata in a session. There are three meta keys or axes from left to right: Extensions, Forensic Fingerprint, and Filename with values listed along each axis. Values on the Extension axis show the file extension, and values on the Forensic fingerprint axis are windows executables. Normally the file type matches the expected forensics fingerprint; however, it is abnormal for a gif file type to be combined with the Windows executable fingerprint. The gif file type is selected to highlight the correlations of that file type, x86pe , and two filenames in the third axis so that an analyst can quickly identify the files that merit investigation.

To reach this view:

1. Order by Value and Sort in Ascending order.
2. Apply two filters (file type = 'windows executable' and extension = 'gif') in the Navigate view to limit the amount of data.
3. Configure a parallel coordinates chart by choosing three axes: file extension, forensic

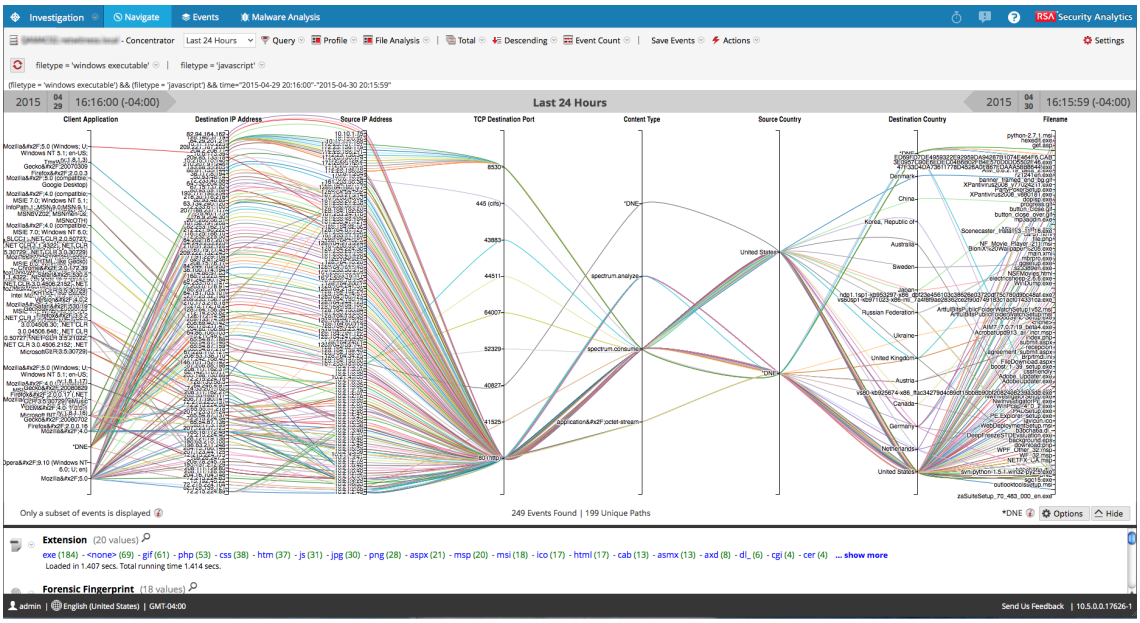
fingerprint, and filename.



Sample Visualization of a Large Data Set

This example of a parallel coordinates visualization applied to a larger set of data illustrates several messages that help analysts to understand what has been charted.

- To create a chart, Security Analytics begins scanning meta values and returning results. A typical time range could have up to 10,000,000 meta values. When the number of meta values returned reaches the Meta Values Result Limit, the chart is rendered even if Security Analytics has not scanned a number of meta values equal to the Meta Values Scan Limit.
- There is a fixed limit on the amount of data that can be rendered as a parallel coordinates chart. In Security Analytics 10.4 and prior, the limit is based on the number of axes times data values: 1000 x the number of axes to protect performance, but in Security Analytics 10.5 and above the administrator configures parallel coordinates limits as part of the Investigation settings In the Administration > System view.



With a larger set of data, the parallel coordinates chart takes longer to process than the smaller set of data and meta keys. To preserve performance, Security Analytics renders the meta values from the Values panel below until the limits set by the Administrator are reached. An informational message tells you: **Only a subset of events is displayed.**

Of all the data visualized for 249 events, there were only 199 unique parallel coordinates paths. Some events are included though they do not include some of the meta keys; these are labeled **DNE** because the meta does not exist in the event.

Query Data in Navigate View

This topic describes the methods available to query data in the Investigation > Navigate view.

When conducting an investigation in Security Analytics, there are several methods available to query results and drill into an area of interest in the Navigate view. Analysts can:

- Create a Custom Query, rather than clicking through meta keys and values.
- Drill into Data in the Navigate View Time Chart.
- Drill into Data in the Values Panel
- View and Modify Queries Using URL Integration

Create a Custom Query

In the Investigation > Navigate view options panel, you can create a query rather than clicking through the meta keys and values to drill down into the meta data. The dialogs for creating a query offer syntax help with drop-down lists of applicable meta keys and operators. When viewing the drop-down list, you can expand and collapse each meta group to view or hide the individual meta keys in that group.

When you select a meta group, Security Analytics generates the complex query equal to a query with all of the meta keys in that group ORed together. So if a meta group contains `ip.src` and `ip.dst`, the query generated is `ip.src = <value> OR ip.dst = <value>`. If the meta group contains meta keys that have different meta value types, the value input is disabled and the query uses `exists` statements. For example, a meta group that contains `ip.src`, `ip.dst`, and `alias.host` includes meta keys that have different value types; `ip.src` and `ip.dst` are ip addresses and `alias.host` is text. The generated query is `ip.src exists OR ip.dst exists OR alias.host exists`.

A basic query is in the following form:

`<metakey> <operator> [<metavalue>]`

These are a few examples:

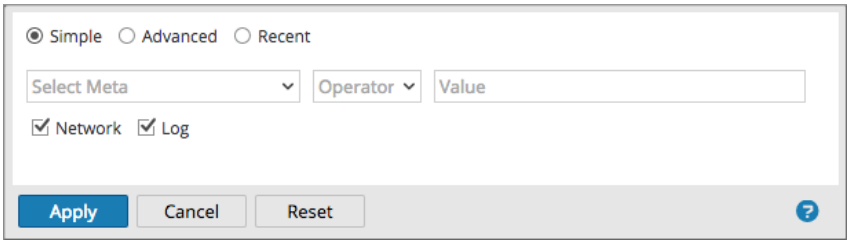
```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Create a Query Using the Basic Method

When you create a query using the basic method, Security Analytics provides drop-down lists of meta and operators.

1. In the **Navigation view** toolbar, select **Query.**

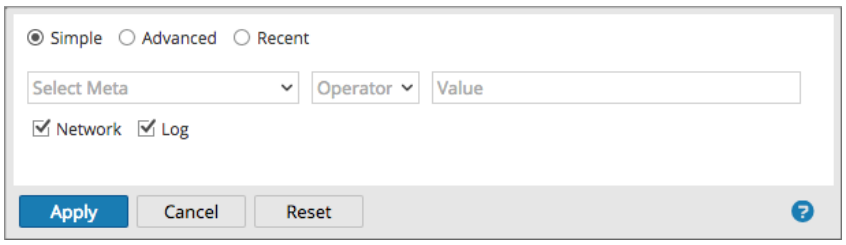
   The Query dialog is displayed, with the Simple option selected.



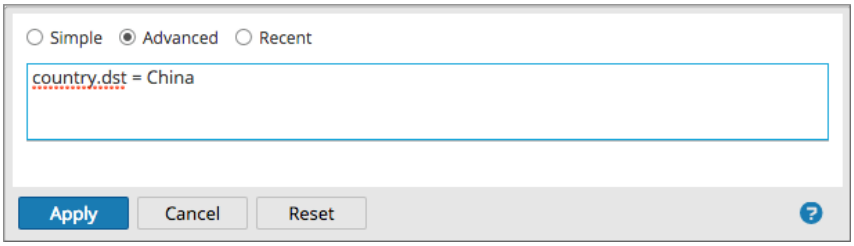
2. In the **Select Meta** field, click to display the drop-down list. The drop-down list has two sections: Meta Groups and All Meta.
3. Select a single meta key under **All Meta** or select a meta group under **Meta Groups**. You can also type in a meta key or meta group in the field.
4. In the **Operator** field, type an operator or click on the drop-down list to select a valid operator.
5. (Optional) If you selected an operator that requires a value, for example, begins, in the third field type the value for the meta key.
6. In the Network, Log and Endpoint checkboxes, choose the type of data to query. Do one of the following:
   a. To limit the query to packets select **Network** and de-select **Log** and **Endpoint**. In the query medium 1 = packet.
   b. To limit the query to logs, select **Log** and de-select **Network** and **Endpoint**. In the query, medium 32 = logs.
   c. To limit the query to endpoint events, select **Endpoint** and de-select **Network** and **Log**. In the query, medium = 32 && nwe.callback_id exists.
   d. To apply the query to packets, logs and endpoint select **Network**, **Log** and **Endpoint**.
7. Do one of the following:
   a. Click **OK**.
   The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.
   b. Click **Cancel**.
   The window is closed and no changes are made to the view or current query.

Create a Query Using the Advanced Method

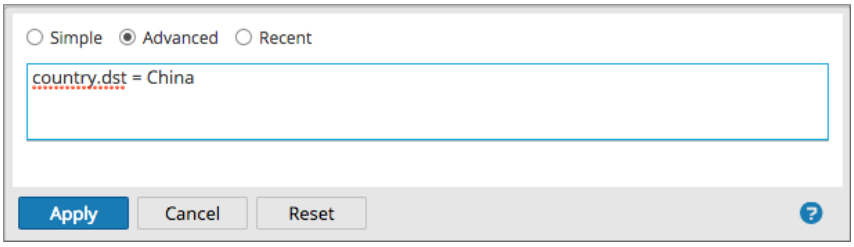
1. In the **Navigate view** toolbar, select **Query.**
   The Query dialog is displayed.



2. Select **Advanced**.
   The advanced query field is displayed.



3. In the field, create a query, which can include the meta key, operator, and value. When you begin typing a meta key in the field a drop-down list of available meta keys for the selected service is displayed.
4. Select the meta key for your query.
   The display is updated. If the expression is not yet complete, the status indicates that the query is invalid.
5. Continue with an operator, from the drop-down list, then a value if necessary. The display is updated as you continue to enter the query. If you enter an operator, such as **exists** or **!exists**, which does not use the value field, the value field is disabled and the invalid status is cleared. If you enter an operator, such as =, which requires the value field, the invalid status remains until you enter a value. When the query is valid the invalid status is no longer displayed.



6. Do one of the following:
   a. Click **OK**.
      The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.

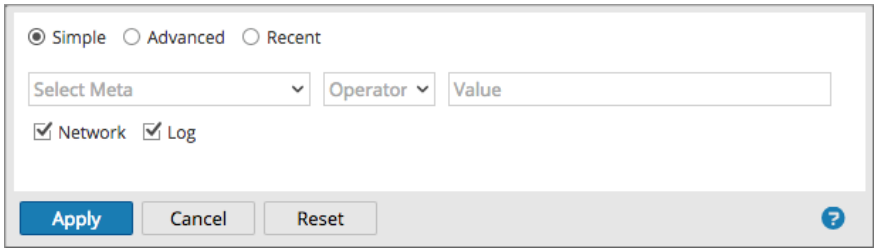
   b. Click **Cancel**.
      The window is closed and no changes are made to the view or current query.

Apply a Recent Query

You can view recent queries and select one to apply to the current service being investigated. To select a recent query:

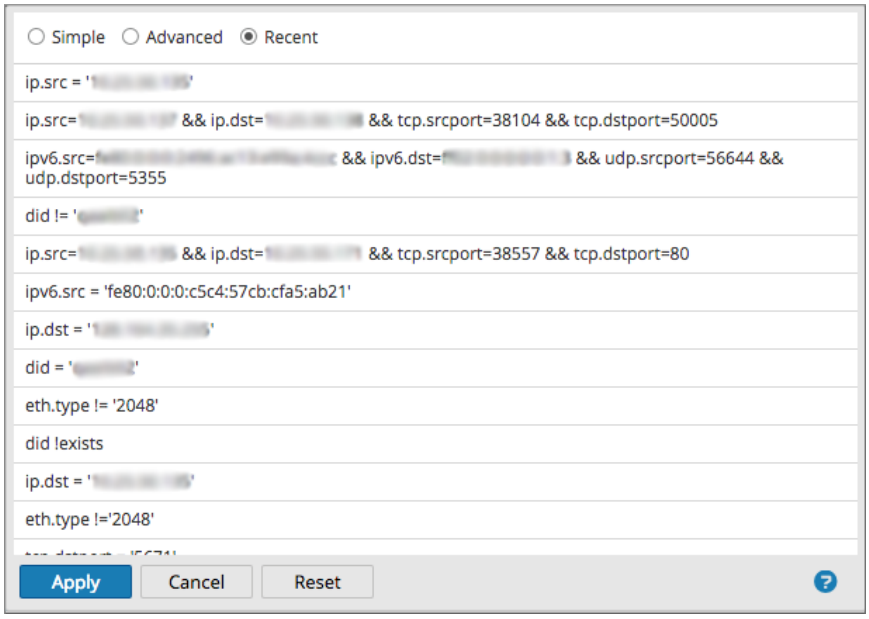
1. In the **Navigate view** toolbar, select **Query.**

   The Query dialog is displayed, with the Simple option selected.



2. Select the **Recent** option.

   The list of recent queries is displayed in the bottom portion of the dialog.



3. In the list of recent queries, click to select a query.
4. Do one of the following:
   a. Double-click a query.
   b. Select a query and click **OK**.

      The window is closed and the view is updated with the results of the new query. The query is displayed in the breadcrumb.

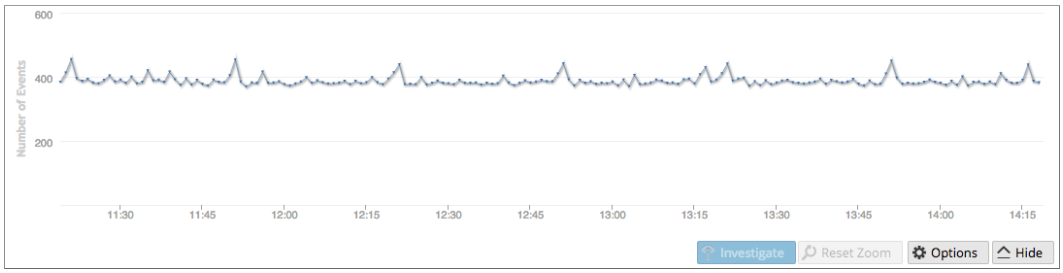
c. Click **Cancel**.

The window is closed and no changes are made to the view or current query.

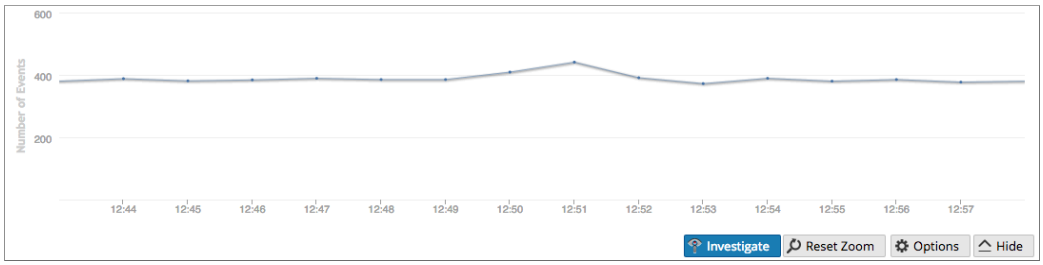
Drill into Data in the Navigate View Time Chart

The Time Chart visualization allows analysts to visualize activity over time. You can zoom into the data by selecting a time window then selecting the Investigate option. You can then reset the navigation to the time range that was in effect before zooming.

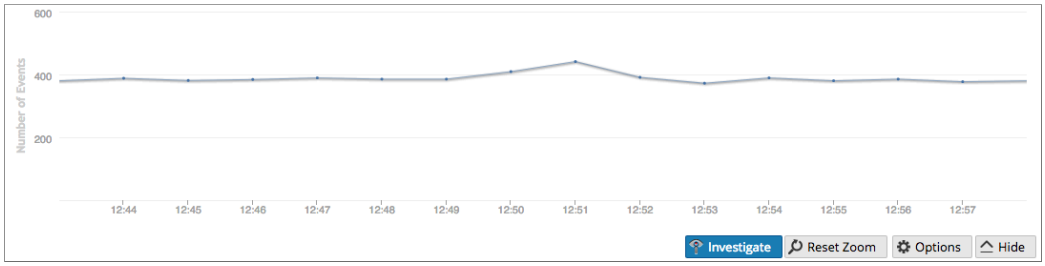
1. In the **Security Analytics** menu, select **Investigation > Navigate**.
   The Time Chart for the current drill point and selected time range is displayed.



2. To highlight a period of time on the Time Chart, click over the desired time period and drag the mouse.
   The Time Chart is redrawn for the selected time range, however the meta values are unchanged.

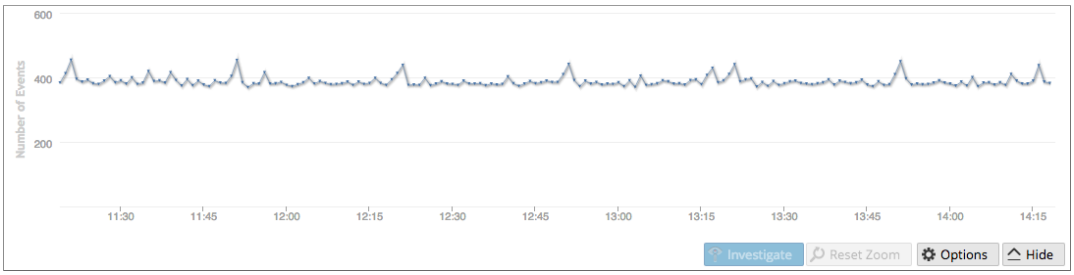


3. To drill into the data for the selected time range, click **Investigate**.
   The URL is updated to reflect the time range override. and the Investigation options panel is updated to reflect the custom time range. The Time Chart is redrawn and the meta values are loaded for the selected time range.



4. To reset the Time Chart to original time range, click **Reset Zoom**.
   The URL is updated to reflect the original URL prior to zooming into the data, and the

Investigation options panel is updated to reflect the time range selected before zoom. The Time Chart is redrawn for the selected time range and the meta values are loaded for that time range.

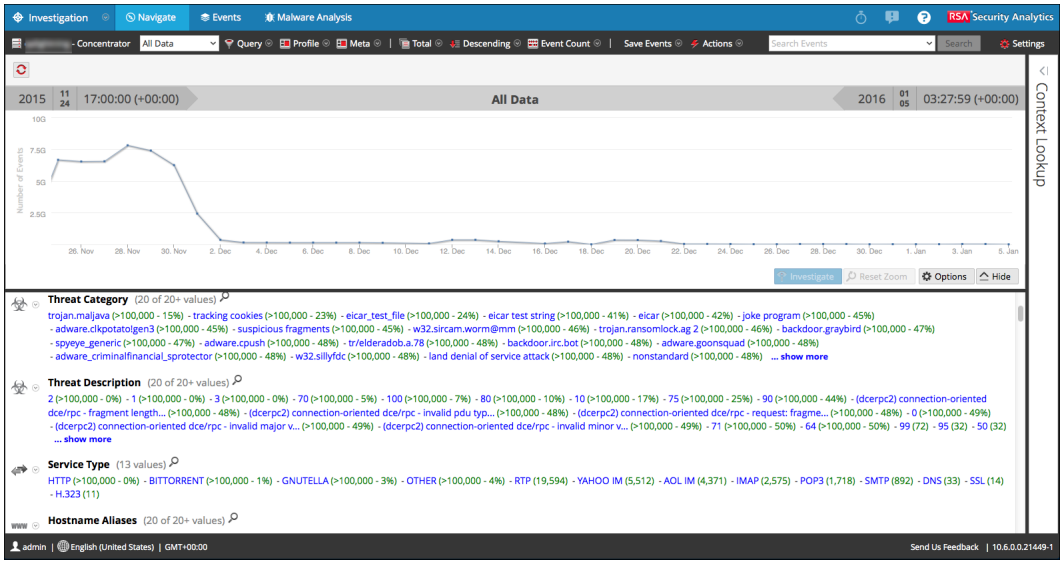


Drill into Data in the Values Panel

Security Analytics displays the activity and values for the selected service in the Investigation > Navigate view. To investigate data, analysts drill into data by clicking on a meta key or a meta value, which is treaty as a query. In the Values panel, each query is added to the breadcrumb data in the Values panel. This results in a breadcrumb at the top with a crumb for each query. You can edit the breadcrumb to insert or remove a query.

Drill into a Subset of the Metadata

1. Begin an investigation so that metadata is displayed in the Navigate view.

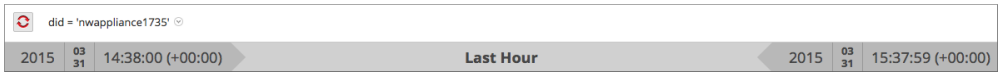


2. To drill down into the metadata, do any combination of the following:

   a. Click a **meta key**, for example, Source Country or Destination Country.

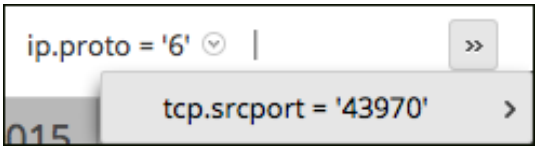
   b. Click a **meta value**, the blue text in the results. For example, Italy.

   Each time you click a meta key or meta value, the investigation query pivots to a narrowed focal point, or drill point, in the data. At each drill point, the Values panel is updated and the new drill point is displayed in the breadcrumb. Below is an example of the first breadcrumb.



   This is an example of a long breadcrumb that does not fit in the toolbar. The last query that fits is followed by a drop-down menu that lists additional queries. To select a drill

point within the overflow, click the overflow icon and a query in the drop-down list.



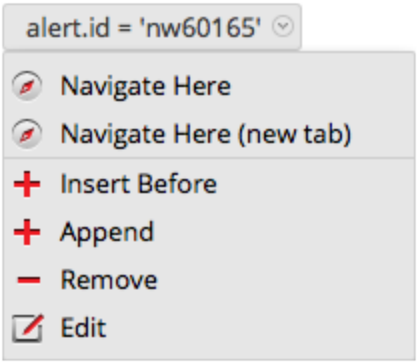
Add a Query in the Breadcrumb

In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, Security Analytics refreshes the results.

To add a query in the breadcrumb:

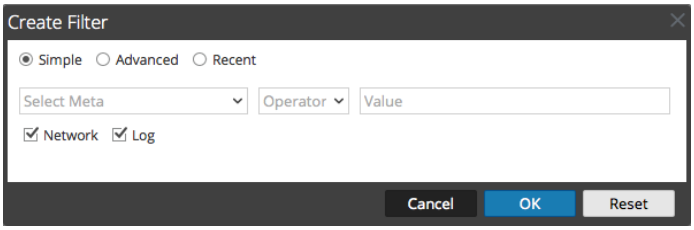
1. Click a crumb.

   The Breadcrumb menu is displayed.



2. To add a query in the breadcrumb, select **Append** or **Insert Before**.

   The Create Filter dialog is displayed.



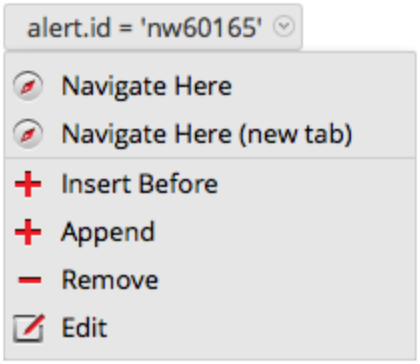
3. Create the Query as described in Create a Custom Query.

Edit a Query in the Breadcrumb

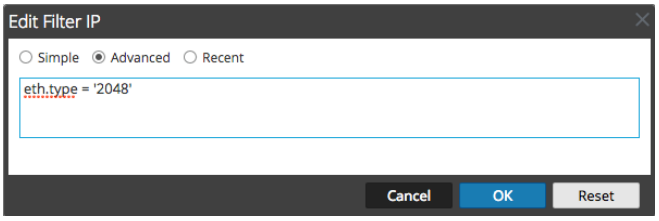
In the breadcrumb, you can click any of the crumbs to display the Query menu. You can delete a crumb and edit a query in a crumb. After each edit in the breadcrumb, Security Analytics refreshes the results.

To work with queries in the breadcrumb:

1. Click a crumb.
   The Breadcrumb menu is displayed.



2. To edit a query in the breadcrumb, select **Edit**.
   The Create dialog is displayed with the selected query open for editing.



3. Edit the fields as described in Create a Custom Query.

Quick Search within a Meta Key

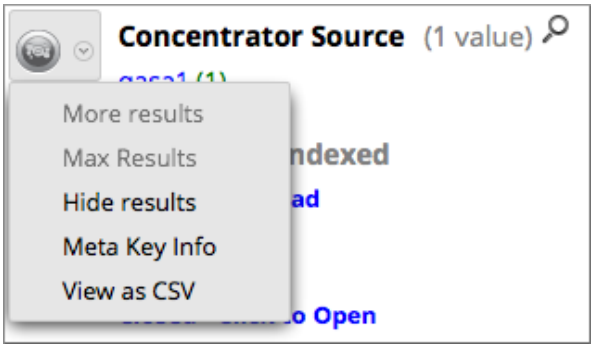
1. Move the mouse over a meta key section and click the magnifying glass.
   The Quick Search form, which contains a comparator and an optional operand for the search, is displayed.

2. (Optional) If you want to close the search form, click the magnifying glass again.
3. Select the operation from the drop-down list on the left and type the text value to search for. Then click **Drill** to perform the execution.
   The metadata for that meta key is used to drill down in the current metadata.

View Meta Key Information in the Navigate View

To view details about a meta key, specifically the key name, index level set for displaying the meta key, and the default view set for the meta key:

1. Click the drop-down menu next to the meta key.

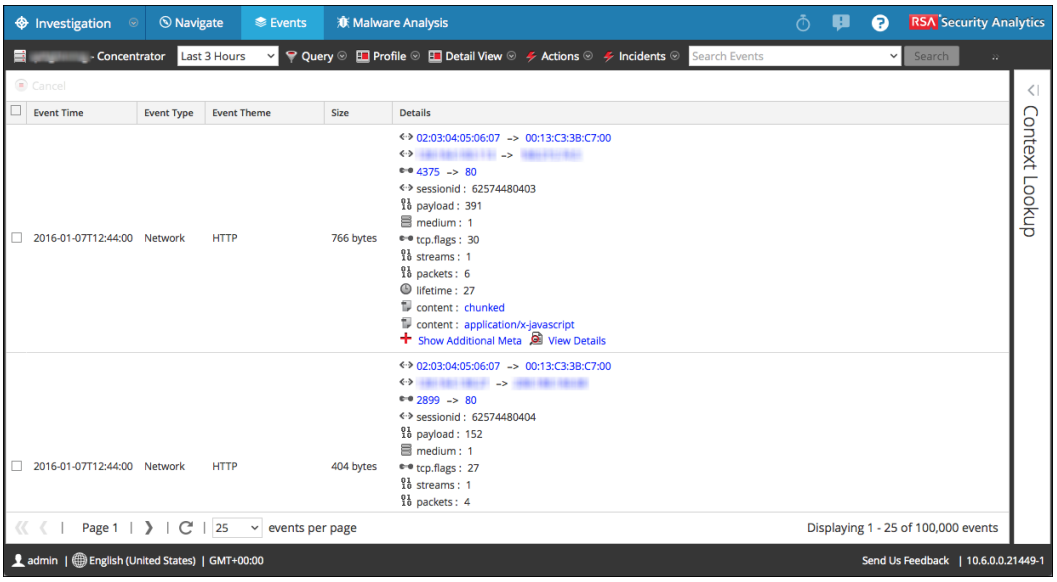


2. Select **Meta Key Info**.
   The Meta Key Info dialog is displayed.
3. When finished viewing, click .
4. (Optional) To view meta names found for the meta key as a comma-separated value list, click the drop-down menu next to the meta key and select **View as CSV**.
   The Showing Values in CSV Format dialog is displayed.
5. When finished viewing, click **Close**.
6. (Optional) If you want to hide the results for the meta key in the current drill point, click the drop-down menu next to the meta key and click **Hide Results**.

Display Events Associated with a Meta Value

The Events view provides additional details for an event in two different views: Events List and Detail View.

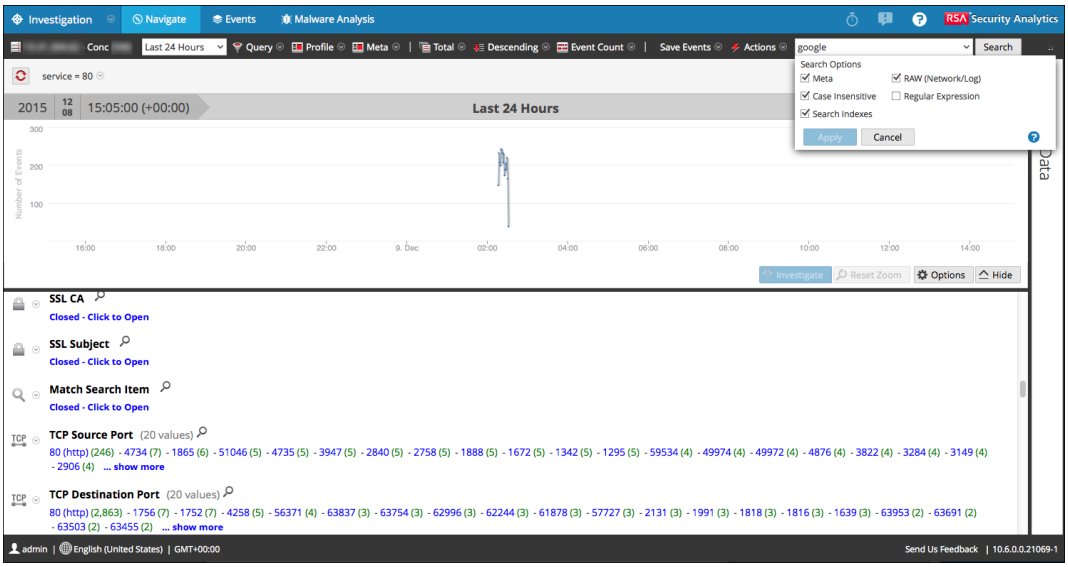
1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Click the count (the number in green) next to a blue meta value.
   The Events view corresponding to the current drill point is displayed.



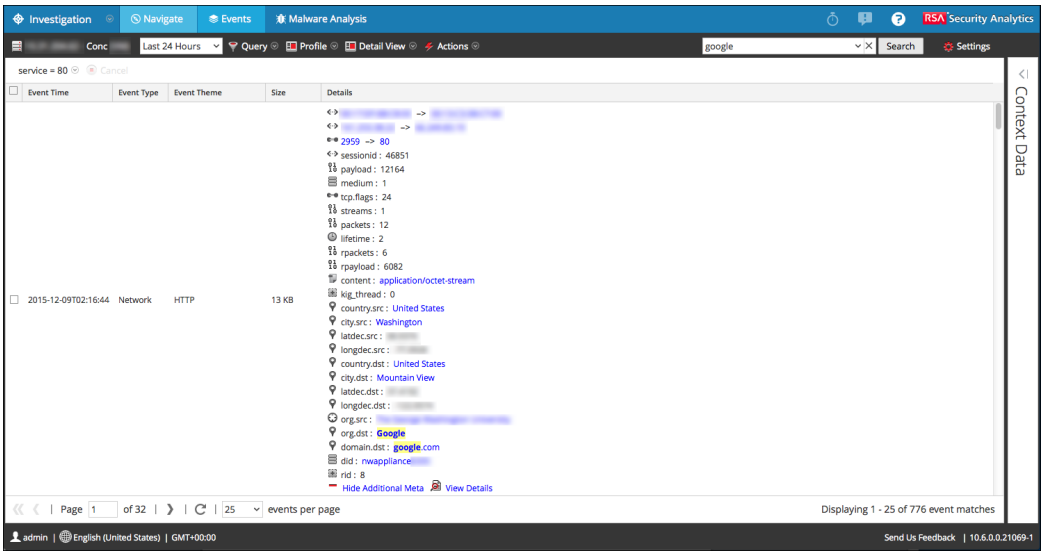
The operations that you can perform in the events view are described in Examine Events.

Search for Specific Events Associated with a Meta Value

1. In the Navigate view, drill into metadata that is the focus of your investigation (click a meta value or add a query).
2. Type a search string in the Search box and press **Enter** or click **Search**.
   You can also select and set your search mode preferences for your searches.
   See Investigation - Search Options for detailed search information.

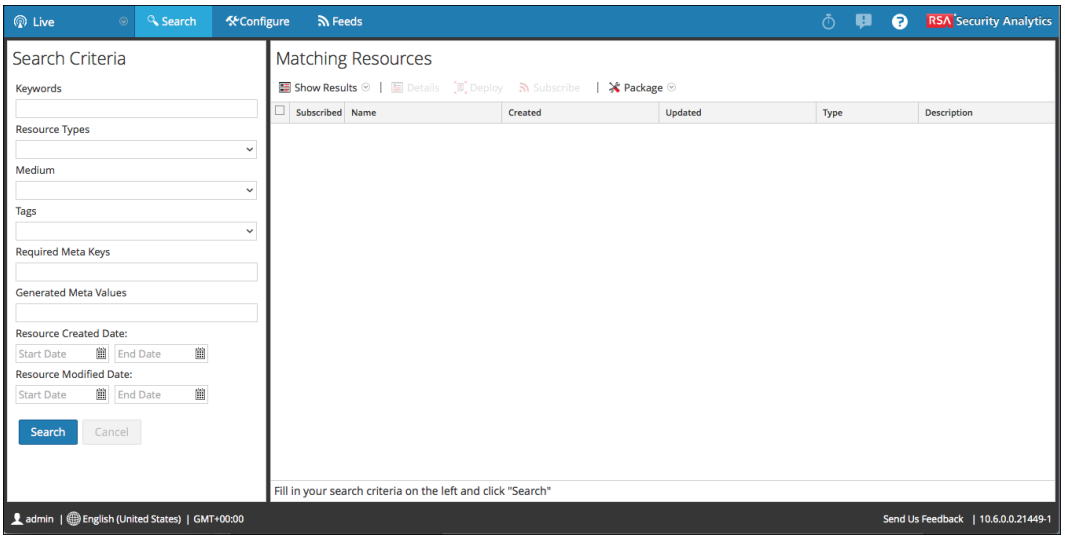


The Events view opens in a new tab and shows the search results. Your time range selection and drills (queries) carry forward to the Events view.



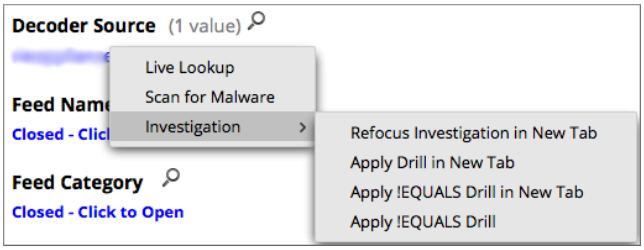
View a Selected Meta Value in Live

1. In the Navigate view, drill into metadata that is the focus of your investigation.
2. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.
3. To look up the meta value in Security Analytics Live, select **Live Lookup**.
   The Live Search view is displayed with the meta value entered in the Generated Meta Value(s) field, and ready for a search.



Refocus the Investigation in a Drill Point

1. Right-click a meta value (the text in blue).
   The Meta Value drop-down menu is displayed.



2. Choose one of the refocus options.
   The drill is refocused according to your choice.

Look at a Specific Count in a New Tab

To view a count for a meta value in a new tab or view a Geomap of the locations for the selected meta value:

1. Right-click a count for a meta value (the green number following the blue meta value).
   The context menu is displayed.
2. (Optional) To open a separate investigation for the specific meta value, select **Open in New Tab**.
3. (Optional) to open a geomap showing the locations where the selected meta value originated, select **Geo-Map Locations in New Tab**.

View and Modify Queries Using URL Integration

Investigation includes anExternal URL Integration that facilitates integration with third-party products by allowing a search against the Security Analytics architecture. By using a query in a URI, you can pivot directly from any product that allows custom links, into a specific drill point in the Investigation view in Security Analytics. This integration provides an internal presentation of the user's query.

URL Integration allows the user to identify the service either by the host id or by the service and port, as defined in Security Analytics. If Security Analytics is unable to resolve the service, the analyst is redirected to the Navigation view, showing the Service selection dialog. Once the service is selected, the Navigation view is loaded with the drill point, defined by the query.

Service Id Known

When the ID of the service to use for investigation is known, the format for entering a URI using a URL-encoded query is:

http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>

where

- <sa host: port> is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- <deviceId> is the internal Service ID in the Security Analytics instance for the service to query against. The service ID can be represented only as an integer. You can see the relevant service ID from the URL when accessing the Investigation view within Security Analytics. This value changes based on the service being connected to for analysis.
- <encoded query> is the URL-encoded Security Analytics query. The length of query is limited by the HTML URL limitations.
- <start date> and <end date> define the date range for the query. The format is <yyyy-mm-dd>T<hh:mm:ss>Z. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported. All times are run as UTC.
  For example:
  http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z

Host and Port Known

When the host and port of the service to use for investigation is known, the format for entering a URI using a URL-encoded query is:

```
http://<sa host:port>/investigation/<device
host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

where

- `<sa host: port>` is the IP address or DNS, with or without a port, as appropriate (ssl or not). This designation is needed only if access is configured over a non-standard port through a proxy.
- **`<device host:port>`** is the host and port of a service defined in Security Analytics instance for the service to query against. Security Analytics attempts to resolve the host and port as a service ID defined in Security Analytics.
- `<encoded query>` is the URL-encoded Security Analytics query. The length of query is limited by the HTML URL limitations.
- `<start date> and <end date>` define the date range for the query. The format is `<yyyy-mm-dd>T<hh:mm:ss>Z`. The start and end dates are required. If no date is provided then the user defaults for that service are used. Relative ranges (for example, Last Hour) are not supported in this version. All times are run as UTC.
  For example:
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Examples

These are query Examples where the SA Server is 192.168.1.10 and the deviceID is identified as 2.

All activity on 03/12/2013 between 5:00 and 6:00 AM with a hostname registered

- Custom Pivot: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

All activity on 3/12/2013 between 5:00 and 5:10 PM with http traffic to and from IP address 10.10.10.3

- Custom Pivot: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Encoded Pivot Dissected:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Additional Notes

Some values may not need to be encoded as part of the query. For example, commonly the IP src and dst is used for this integration point. If leveraging a third-party application for integration of this feature, it is possible to reference those without encoding applied.

Act on a Drill Point in the Navigate View

This topic describes the actions available to analysts who want send a drill point to some form of output or view the drill point from a different perspective in the Investigation > Navigate view.

When conducting an investigation in Security Analytics, there are several actions available once a drill point has been reached in the Navigate view. Analysts can:

- Export a Drill Point.
- Print the Current Drill Point.
- Open the Events List for a meta value.
- Launch an External Lookup of a Meta Key
- Launch a Malware Analysis Scan from the Navigate View.
- View Additional Context for a Data Point
- Manage Context Hub Lists and List Values in Investigation
- Visualize the Current Drill Point in Informer

Export a Drill Point

In Security Analytics Investigation, when you have the data for a drill point displayed in the Navigate view, you can:

- Extract files from a session and choose the type of files to extract: archives, audio BitTorrent, documents, executable, images, other, video, and web.
- Export the drillpoint as a packet capture (PCAP) file, a log file, or a meta file.

The details being exported are affected by both the time range and drill point at the time of exporting.

Note: When you export the drill point as a log file, only the log sessions are exported. The job queue message refers to the total number of sessions in the drill point rather than the number of logs. For example, if the drill point has 505 sessions and only five log sessions, the job queue message states that Security Analytics is extracting logs for 505 sessions.

To export a drill point from the Navigate view:

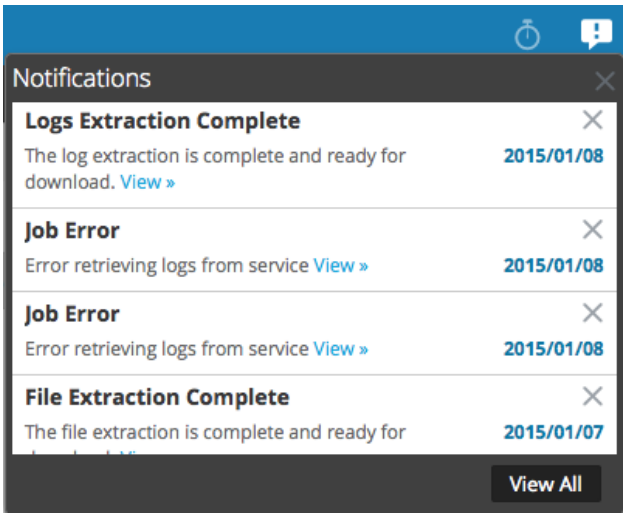
1. Conduct an investigation until you reach the desired drillpoint.
2. In the **toolbar**, select **Actions > Export** and select one of the export options:

- PCAP
- Logs
- Meta

  The drill point is extracted, and a message advises that the job is scheduled. You can check the jobs page for the status.

Note: If you upgraded from previous version of 10.6.X.X, to export data, in **Navigate** > **Query** > **Advanced** query field, ensure that the meta key value for strings IPv4, IPv6 and MAC are in quotes. For example, user.dst='username'.

3. When the scheduled file extraction is complete, it is displayed in the Job Notifications tray.



4. Click the **View** link to the Jobs Tray and download the specific extraction file requested.

Launch an External Lookup of a Meta Key

This topic provides instructions for using out-of-the-box Investigation plugins to launch an external lookup of specific meta keys using tools external to Security Analytics while investigating data in the Navigate view or Events view.

Analysts can use out-of-the-box Security Analytics Investigation external lookups to save time during investigations. The out-of-the-box lookups are available by right-clicking one of the these meta keys: IP address (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, and `file-hash`.

For all `IP` and `host` meta keys, the following lookups are built in to Security Analytics:

- Google Malware: Opens a Google Malware search in a new tab.
- McAfee SiteAdvisor: Opens a McAfee SiteAdvisor search in a new tab.
- BFK Passive DNS Collection: Opens a BFK Passive DNS collection search in a new tab
- CentralOps Whois for IPs and Hostnames: Opens a CentralOps Whois search for IPs and hostnames
- Malwaredomainlist.com Search: Opens a Malwaredomainlist.com search in a new tab
- Malwaredomains.com Search: Opens a Malwaredomains.com search for in a new tab
- Robtex IP Search: Opens a RobtexIP search in a new tab
- SamSpade Search: Opens a SamSpade search in a new tab
- ThreatExpert Search: Opens a ThreatExpert search in a new tab
- UrlVoid Search: Opens a UrlVoid Search in a new tab n a new tab

For the `file-hash` and `alias-host` meta keys, the Google lookup opens a Google search in a new tab.

For the `client` meta key, the ECAT Lookup option opens an ECAT client in a new tab if the ECAT client is installed on the same system on which the browser is being used.

Administrators can add additional external lookups and other custom actions as described in "Add Custom Context Menu Actions" in the *System Configuration Guide*.

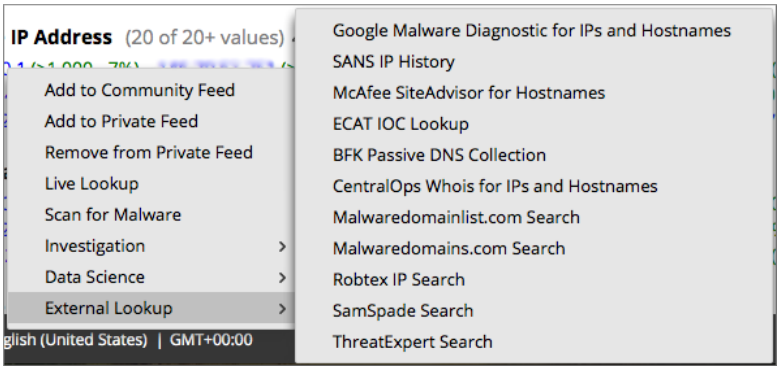
Lauch an ECAT IOC Lookup

To launch an ECAT lookup of data from the Investigation > Navigate view:

1. Right-click a meta value for one of the following meta keys: `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client`.

2. Select **External Lookup** in the context menu.

   A submenu of external lookup options is displayed.

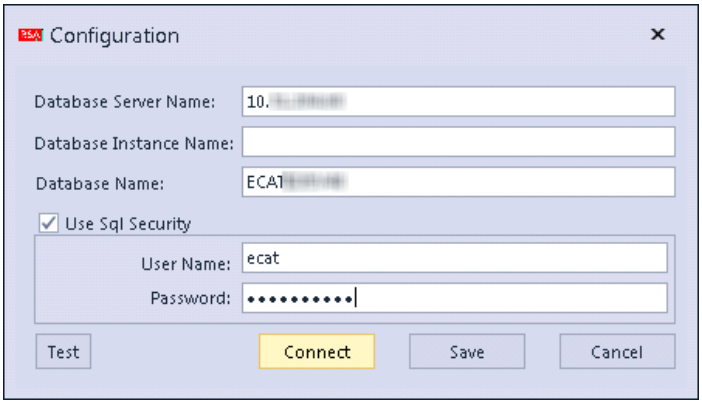


3. Select **ECAT IOC Lookup**.

   A dialog asks you to choose an application.

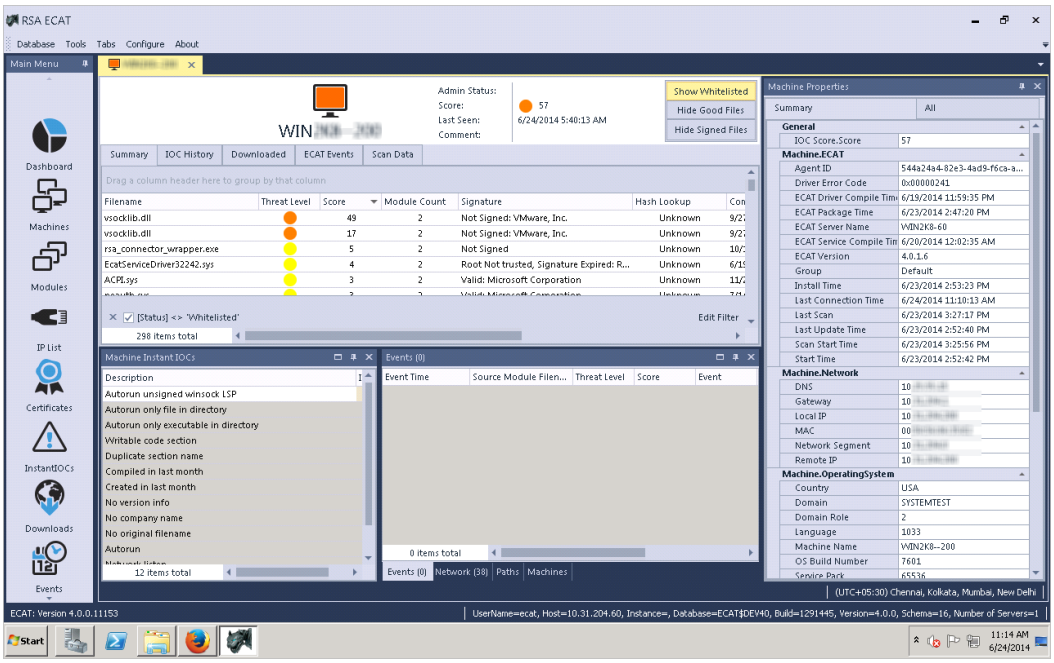
4. Select ECAT and click **OK**.

   The RSA ECAT Configuration dialog is displayed.



5. Enter the user name and password required to log on to the ECAT client, and click **Connect.**

   The drill point opens in RSA ECAT.

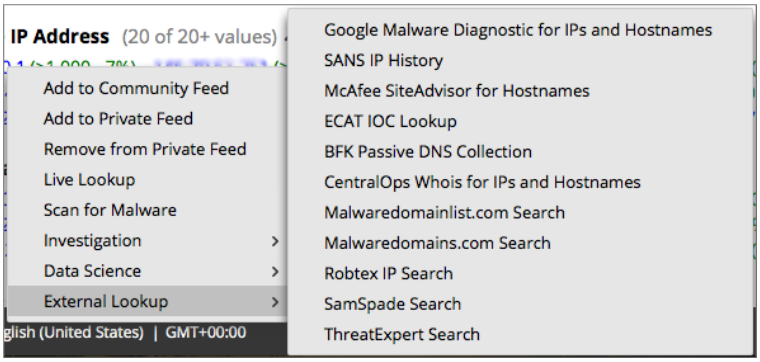


Lauch Other External Lookups

To launch an external lookup (other than ECAT IOC) of data from the Investigation > Navigate view:

1. Right-click a meta value for one of the following meta keys: `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`
2. Select **External Lookup** in the context menu.

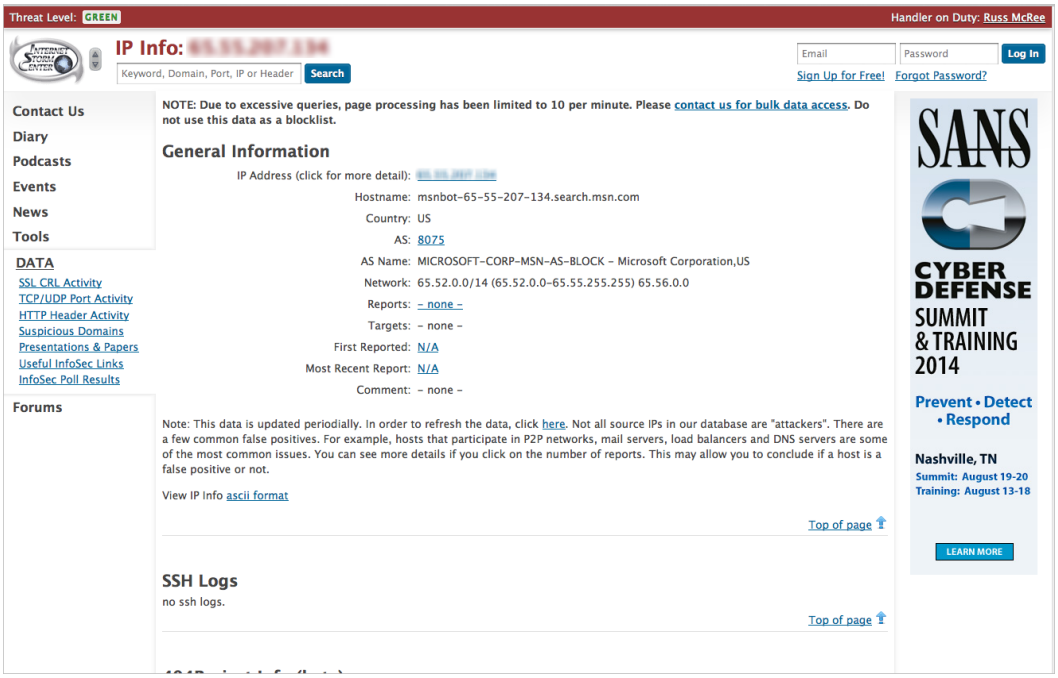
   A submenu of external lookup options is displayed.



3. Select one of the lookup options.

   The selected meta value opens in the selected lookup, for example, if you selected SANS IP

History, the drill point information is displayed in SANS Internet Storm Center.

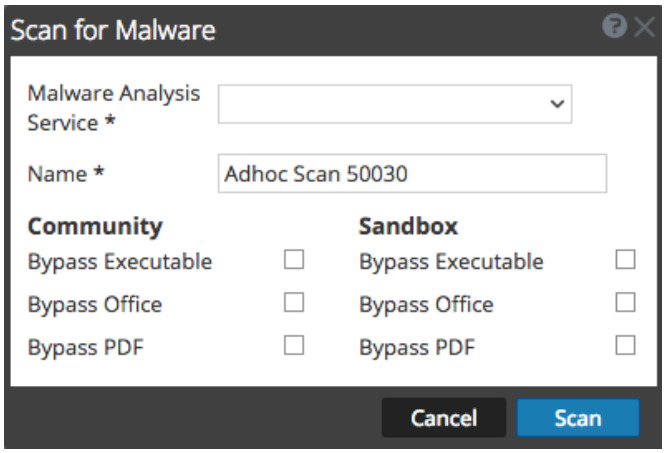


Launch a Malware Analysis Scan from the Navigate View

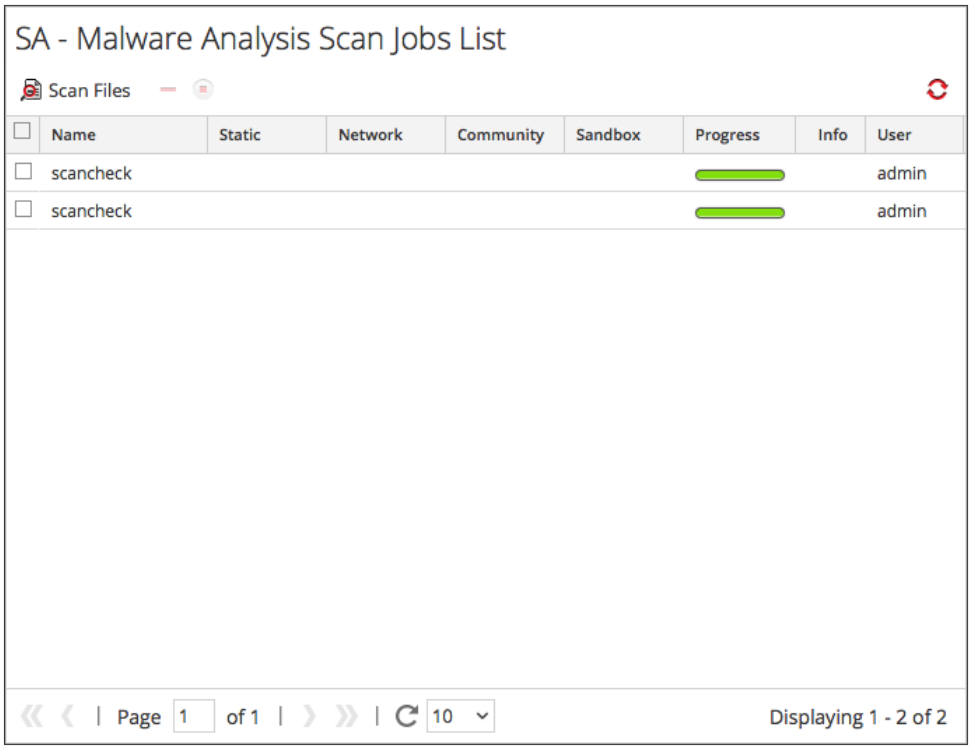
From within Investigation, analysts can launch an on-demand Malware Analysis scan by selecting a service and meta value, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis.

To launch a Malware Analysis scan of data from the Investigation > Navigate view:

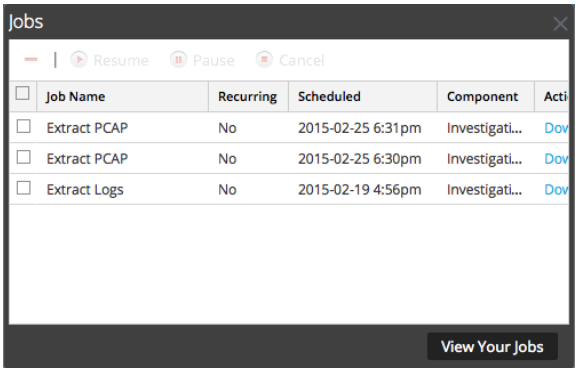
1. Right-click a meta value (for example, OTHER, DNS, or FTP) and select **Scan for Malware** in the context menu.
   The Scan for Malware dialog is displayed with a suggested name for the on-demand scan and no service selected.
2. In the Scan for Malware dialog, select a service to perform the scan, edit the name, and select the types of files to bypass under community and sandbox.



3. Click **Scan**.
   The scan request is added to the Scan Jobs List dashlet and the Jobs Tray. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.
4. To view the jobs, do one of the following:
   a. Navigate to the Scan Jobs List in the Malware Analysis view or in the Unified dashboard. Double-click a scan to view the scan.



b. To view the job in the Jobs tray, click  in the Security Analytics toolbar. When the job is complete, scroll to the left and click **View**.



The Malware Summary of Events for the selected scan is displayed. The scan is also added to the list of available scans in the dialog for selecting scans in the Investigation > Malware tab.

Manage Context Hub Lists and List Values in Investigation

Analysts can add lists and list values for Context Hub enrichment in the Investigation views. The Context Hub service is included in RSA Security Analytics 10.6 and above.

When the Context Hub service is enabled and configured, Security Analytics provides enrichment data from Incident Management, custom lists,and ECAT directly in the Navigate view and Events view. A visual cue highlights meta values for which enrichment data is available in the Investigation views, and you can click on the highlighted value to look up the contextual information and intelligence.

In addition, from the Values panel in the Navigate view and Events view, you can view lists, edit meta values in an existing list, or create a new list. When you add meta values to a list, you can investigate the meta values using the context lookup option.

Prerequisites

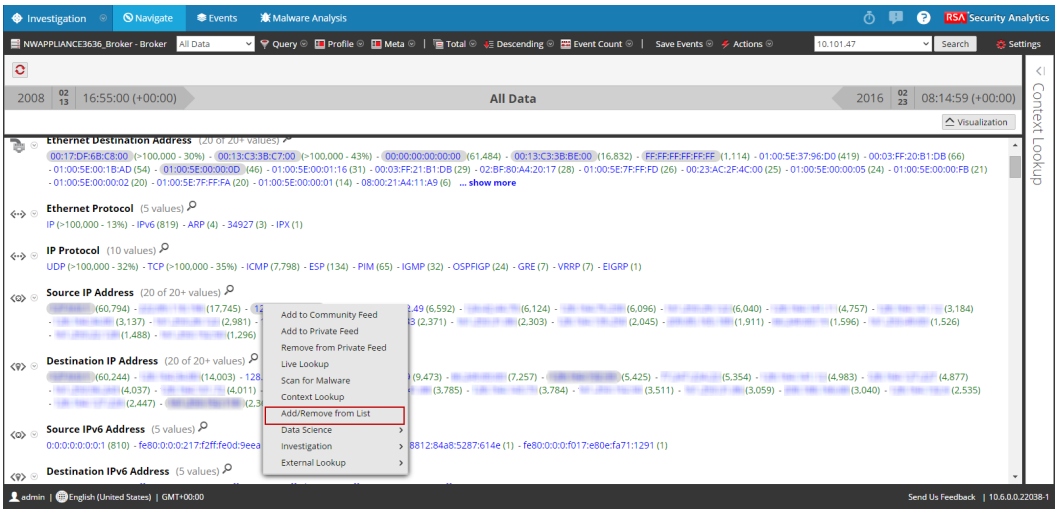
For an analyst to manage lists in Investigation, the Administrator must:

- Enable the Context Hub service.
- Assign an analyst role with permission `Manage List from Investigation` to the user who will perform Context Lookup from Investigation views.
- Configure appropriate roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Add Meta Values to an Existing List

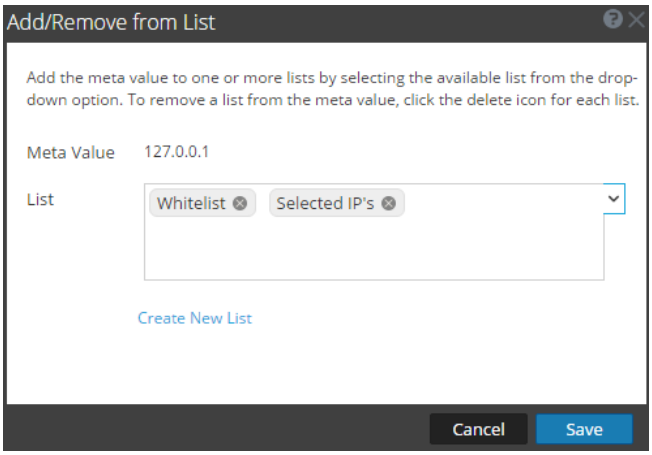
To add meta value to an existing list in Context Hub:

1. While investigating a service in the **Navigate** view, right-click a meta value (for example, values under Source IP, Destination IP, or Username) and select **Add/Remove from List** in the context menu.



The Add/Remove from List dialog is displayed.

2. In the **List** field, select one or more lists from the drop-down option to which the meta value must be added.



3. Click **Save**.

   The meta value is added to the selected lists.

Remove a Meta Value from a Context Hub List in Investigation

To remove a meta value from list:

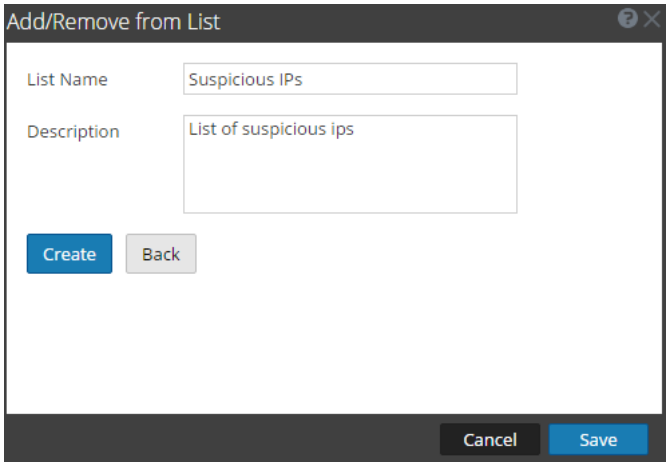
1. In the **Add/Remove from List** dialog, in the **List** field, view the lists which include the meta value.
2. Click the delete icon (x) for each list that should not include the meta value.
3. Click **Save**.

   The meta value is removed from the deleted list.

Create a New List in Investigation

To create a Context Hub list in Investigation:

1. In the **Add/Remove from List** dialog, click **Create New List**.



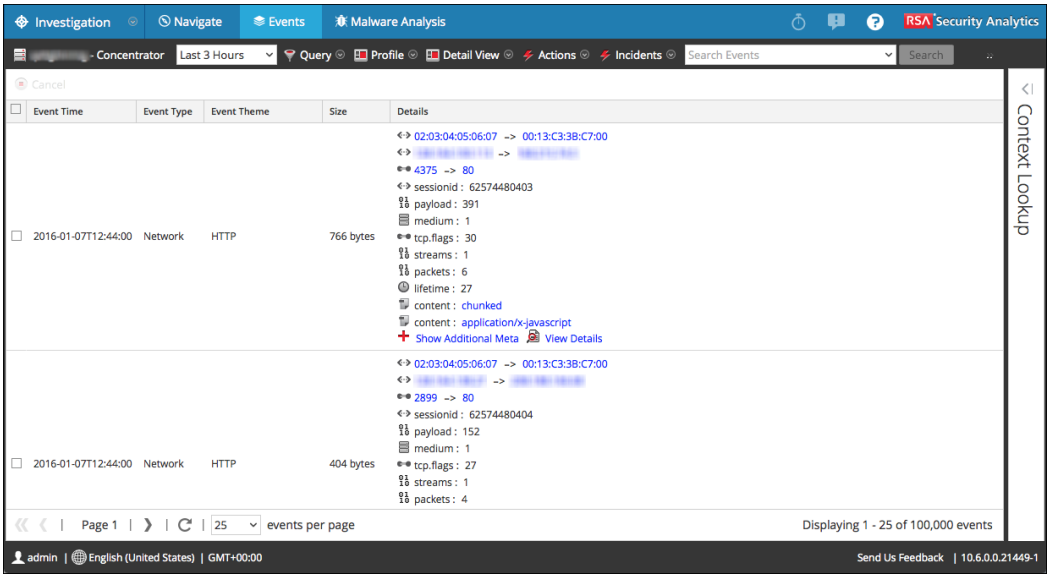
2. In the **List Name** field, enter an unique name for the list.
3. In the **Description** field, enter the description of the list.
4. Click **Create** to create the list.
5. Click **Save** to add the meta value to the created list.

   These lists are considered as data sources for retrieving context information.

Open the Events List

Analysts can view a list of events associated with a session in the Investigation > Events view. There are two ways to display the Events view:

1. Select **Investigation > Events** in the **Security Analytics** menu. Security Analytics runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
2. In the **Navigate** view, click a meta value, which in fact represents an event. The Events view displays the events on the selected service based on the drill point in the Navigate view. The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view.



You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can extract files, export events, export logs, and open the Event Reconstruction panel by double-clicking an event. See Examine Events for detailed information about these capabilities.

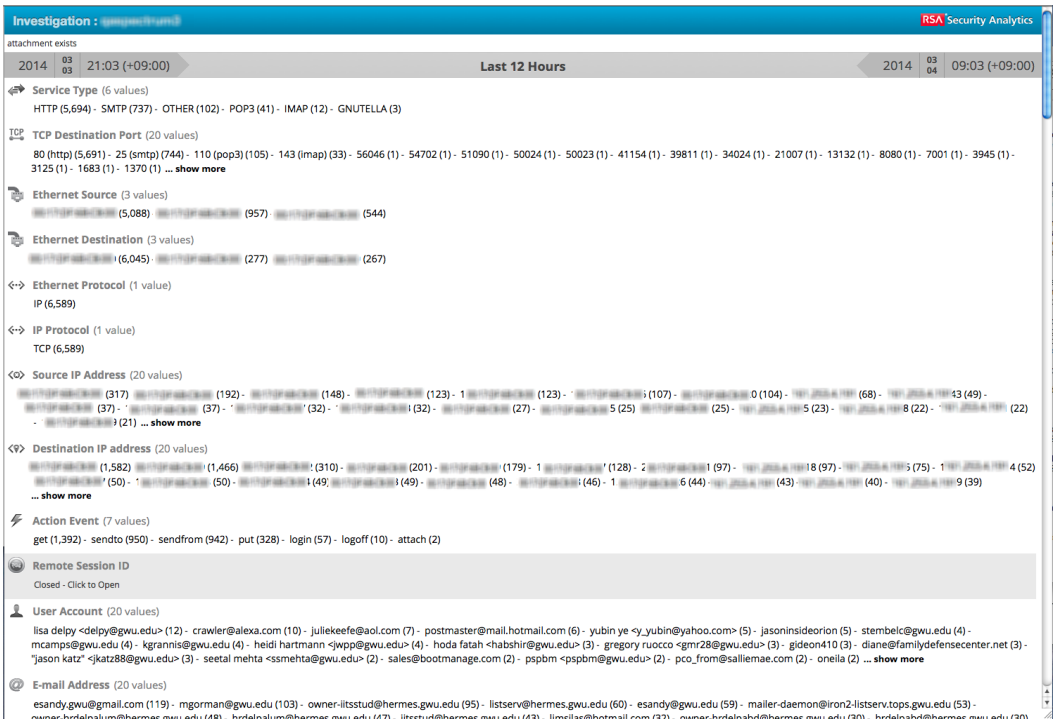
Print the Current Drill Point

In the Investigation > Navigate view, you can display the contents of the current drill point in printer friendly format in the browser window.

To display the current drill point in a print view:

1. With a drill point open in the **Investigation > Navigate** view, select **Actions > Print** in the toolbar.

   A new tab is created with the print view of the current drill point.



2. Use the print option in your browser to send the printable view to the printer.

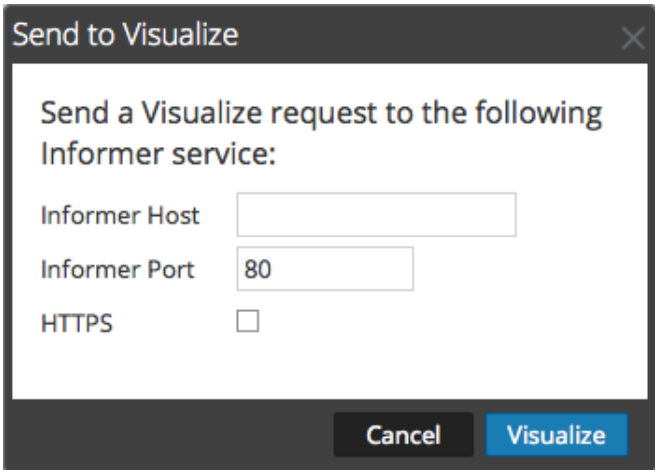
Visualize the Current Drill Point in Informer

This topic provides instructions for sending a drill point in the Investigation > Navigate view to an Informer visualization.

Informer must be installed in your network and accessible by the service being investigated. You need to supply the host name and the port used on the Informer host to communicate with Security Analytics.

To display a visualization in Informer of the current drill point:

1. With a drill point open in the Investigation > Navigate view, click **Actions > Visualize**.
   The Send to Visualize dialog is displayed.



2. Type the Informer hostname or IP address, and verify the Security Analytics server port used to communicate with the Informer host.
3. (Optional) Select the HTTPS option if the Informer host uses secured communications.
4. Click **Visualize**.
   The visualization is displayed in a new tab.

View Additional Context for a Data Point

When conducting an investigation in the Navigate view or Events view, analysts can look up additional context information and intelligence for a meta value or data point from various configured sources, such as ESA.

An Analyst with permission `Context Lookup` can perform Context Lookup from Investigation views. An administrator must configure roles and permissions as described in "Role Permissions" and "Manage Users with Roles and Permissions".in the *System Security and User Management Guide*.

To perform context lookup, the administrator must:

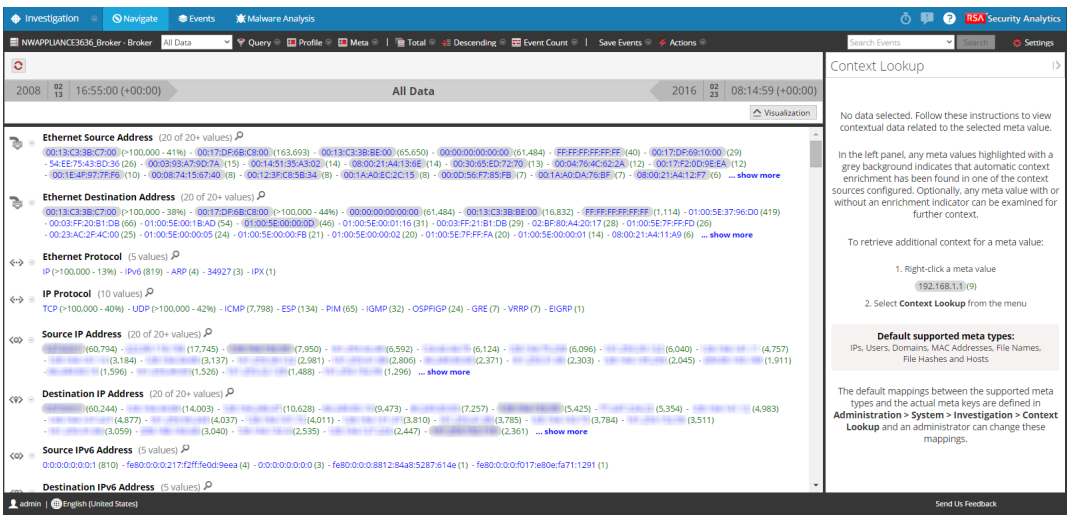
- Add the Context Hub service in Security Analytics. (The Context Hub service is included in Security Analytics 10.6 and above.)
- Configure data sources for the Context Hub service as described in the *Context Hub Configuration Guide*.

View Additional Context using Context Lookup

To view the additional context for a data point from the Investigation views:

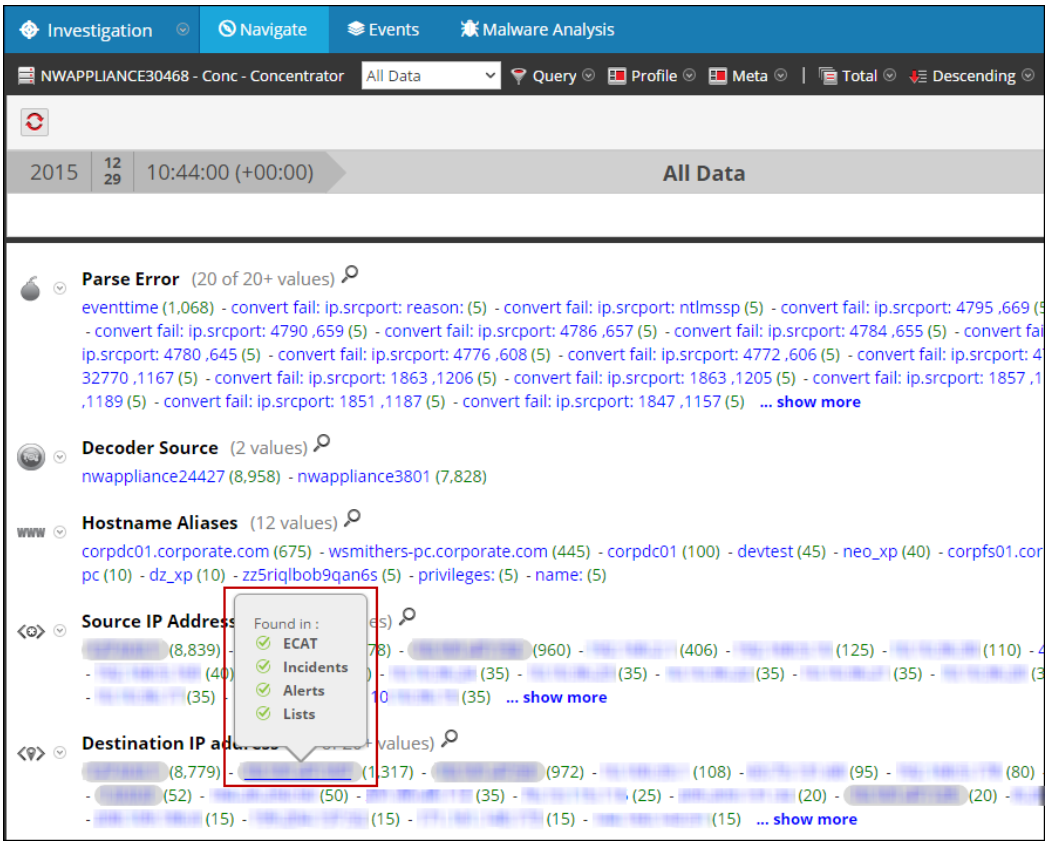
1. While conducting an investigation or examining events in **Security Analytics** menu, go to the Navigate view.

   The Navigate view has the Values panel on the left and the Context Lookup panel on the right as shown below. The Context Lookup panel does not display any data until you perform a Context Lookup. Meta values that have associated context information are highlighted with a gray color background.

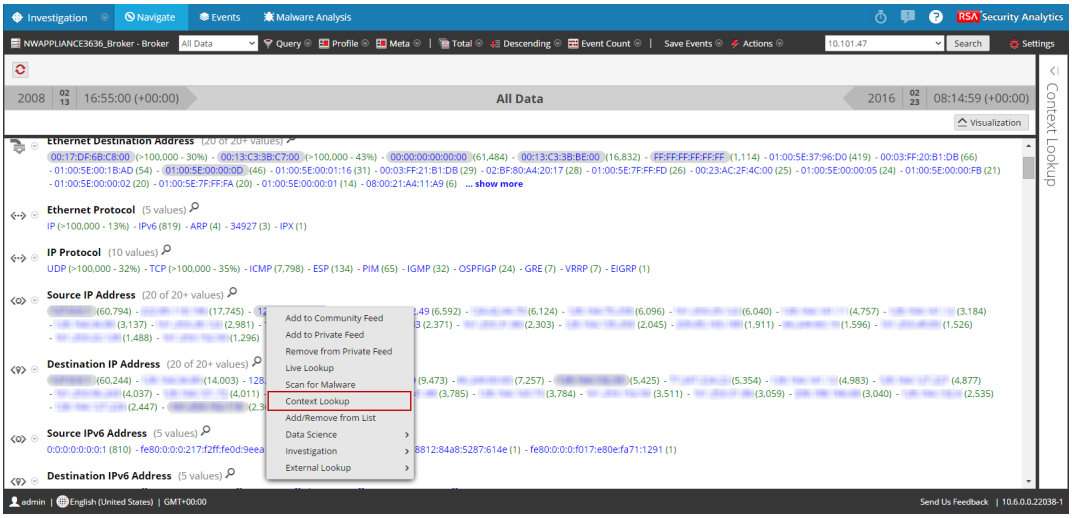


2. To view the type of context data that is available for a highlighted meta value, hover the mouse over a highlighted meta value.

   An inline indicator shows which type of context data is available for the meta: ECAT, Incidents, Alerts, or Lists.



3. To view the Context Lookup data from the Values panel, right-click a highlighted meta value and select **Context Lookup** in the context menu.



The Context Lookup panel displays the lookup results based on the data available on the configured sources.

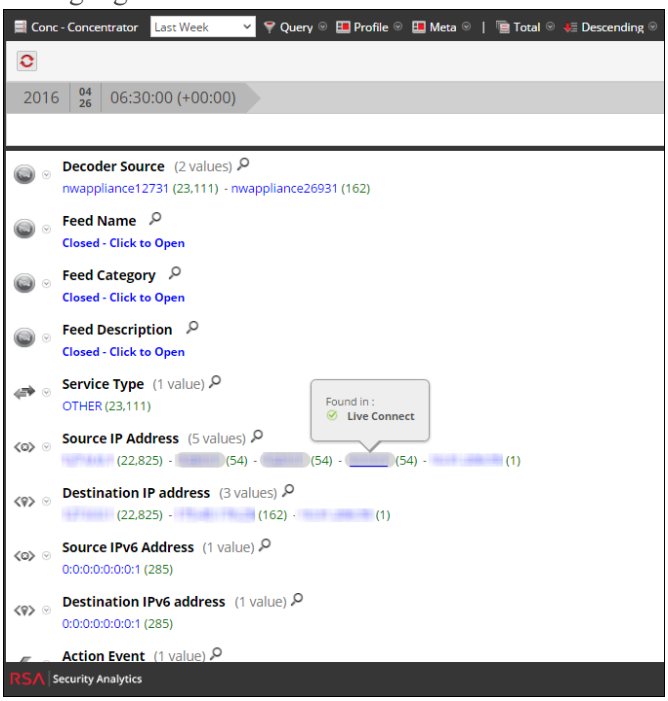
Note: The inline indicator for meta values is supported only in the Navigate view. For the Events view, you must perform an on-demand lookup against the meta values.

Context Lookup for Live Connect

For Live Connect, context lookup is supported only for IP meta type (device.ip, ip.src, ip.dst, paddr, ip.addr, alias.ip). The IP addresses that has live connect data can be identified by using the in-line indicator when you hover the mouse over highlighted IP addresses.

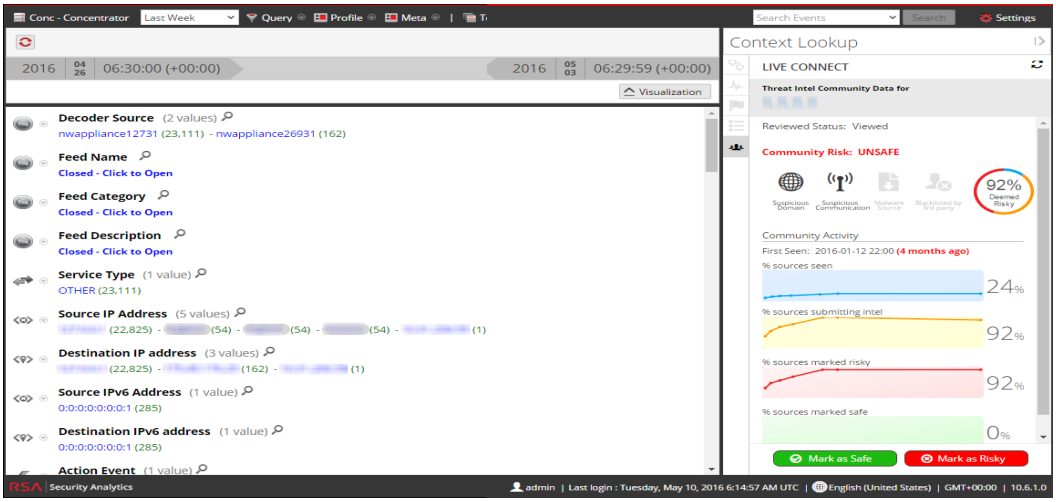
To view live connect contextual data:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**.
   The Investigate dialog is displayed.
2. Select a service and click **Navigate**.
3. View and select an IP address that has Live Connect data by using the in-line indicator on the highlighted IP addresses.



4. Right-click the IP address and select Context Lookup in the context menu.

   The Context Lookup panel displays the lookup results.



5. Alternatively, if you want to highlight only risky IP addresses, from the **Settings** dialog, select the option **Live Connect: Highlight Risky IPs**.

6. From the lookup panel, you can view the contextual data for the IP address. If the IP address is known within the Live Connect community, you can view community related activities and also provide your feedback based on your investigation.

The following table describes the available options for Live Connect Context Lookup panel:

Field	Description
IP Address	Displays the IP address for which the lookup results are displayed.

Field	Description
Reviewed Status	Displays the reviewed status of the IP address based on the analyst activity. This gives the visibility of the analyst activity within an organization. Below are the types of status: • **New:** If lookup results for an IP address is viewed for the first time within the organization. • **Viewed:** If any analyst within the organization has already viewed the lookup results for an IP address. • **Marked as Safe:** If any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • **Marked as Risky:** If any analyst within the organization has already viewed the lookup results and marked the IP address as risky.
Community Risk Rating and Reasons	Displays the community risk rating for an IP address such as: • **Safe:** An IP address is marked as "Safe" if it is considered safe based on the Live Connect analysis and analyst feedback. • **Unknown:** The risk rating for an IP address is displayed as "Unknown" if there is no enough information to calculate the risk rating. • **Unsafe:** An IP is rated unsafe if it is associated with one or more of the following community risk reasons: ◦ Suspicious Domain ◦ Suspicious Communication ◦ Malware Source ◦ Blacklisted by 3rd Party The risk reasons are represented by appropriate icons. The icons appear normal if it is matched with the IP, else its grayed out.

Field	Description
Community Activity	If the IP address is known within the RSA community, a graphical representation of the community activity trend is displayed for the following: • Users (in %) who have viewed the IP address in the Live Connect community over time. • Users (in %) who submitted feedback for the IP address. • Users (in %) who marked the IP address as risky over time. • Users (in %) who marked the IP address as safe over time.
Community Activity Statistics	Community activities such as: • Date first seen in the community. • Time since the IP was seen for the first time (Current time - First seen time). • A Pie chart based on the community activity trend graph. The pie chart shows the correct breakdown of the % of Live Connect customers that have seen the IP (blue), the % who have submitted feedback (yellow), the % who marked risky (red), and the % who have marked safe (green). The number in the middle of the chart reflects the percent who have marked the IP as risky.
IP Rating Feedback	Provides an option for the analyst to give feedback on the IP address if the IP address was already known within the RSA Community. The options are: • Mark as Safe • Mark as Risky Based on the feedback, the "Reviewed Status" changes to "Marked as Safe" or "Marked as Risky".

View Results from Context Lookup Panel

In the Context Lookup panel, you can view the lookup results and explore individual data for further investigation. For example, when you click on a particular Incidents value, the incident details are displayed in the Incident Management view.

For a detailed description of the information displayed on the Context Lookup panel, see Investigation - Context Lookup Panel.

Examine Events

Analysts who are investigating data in the Investigation can view and reconstruct events associated with a session.

- Analysts who conduct analysis using Security Analytics Investigation, and have the appropriate system roles and permissions set up for their user accounts, can go from a Navigate view drill point to the Events view.
- Analysts who do not have access to the Navigate view or want to go directly to the Events view, can open sessions and examine the events that make up the session in the Investigation > Events tab.

Separate topics describe methods of working in the Events view.

- Combine Events from Split Sessions
- Export Events and Extract Files
- Filter and Search Results in the Events View
- Manage Column Groups in the Events View
- Reconstruct an Event

Combine Events from Split Sessions

Analysts can identify sessions that have been split due to session size in the Events view, and combine the fragmented sessions so that the complete session is viewable as a single query result in the Events view. When split sessions are recombined, a single packet export of the session in the Events view includes all of the session fragments.

Version 10.4 and earlier Decoders are configured with a default session size of 32 MB. When a session exceeds the 32 MB limit, the Decoder splits the session and all subsequent packets become part of a new session, fragmenting the actual network session across multiple Decoder sessions. Split sessions are parsed without the context that it is a fragment of the larger network session, sometimes resulting in session fragments with source and destination addresses and ports reversed and with unidentified application protocols. Another result of split sessions can be difficulty viewing all of the session fragments as a single query result or creating a single packet export of all the session fragments.

Decoder enhancements in Security Analytics 10.5 provide improved processing of fragmented sessions:

- Contextual fragment parsing.
- Session fragments highlighting.
- Finding session fragments.
- Exporting all packets to a single PCAP.

Contextual Fragment Parsing

In Security Analytics 10.5 and later, the Decoder completes session parsing before splitting the session based on the configured maximum session size (32 MB) or the configured timeout (60 seconds). When parsing is complete, the parsed results include the proper address directionality and application protocol, which are propagated to each subsequent session fragment to ensure consistency with the logical network session they represent.

Note: All of the necessary Decoder configuration changes are made when upgrading to 10.5. However, Find Session Fragments requires that the tcp and udp source port meta keys (tcp.srcport and udp.srcport) be fully indexed, which was not the default configuration prior to 10.5. This functionally limits the ability to find session fragments to sessions captured after the Decoder was upgraded to 10.5.

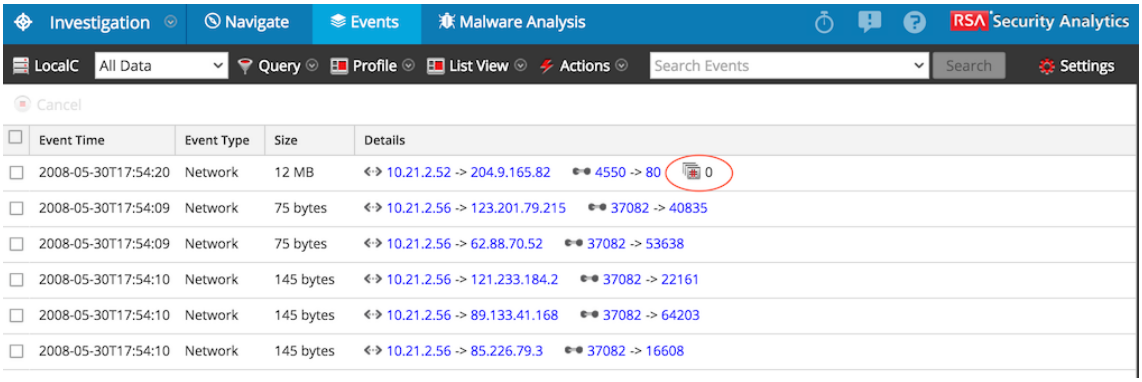
Session Fragments Highlighting

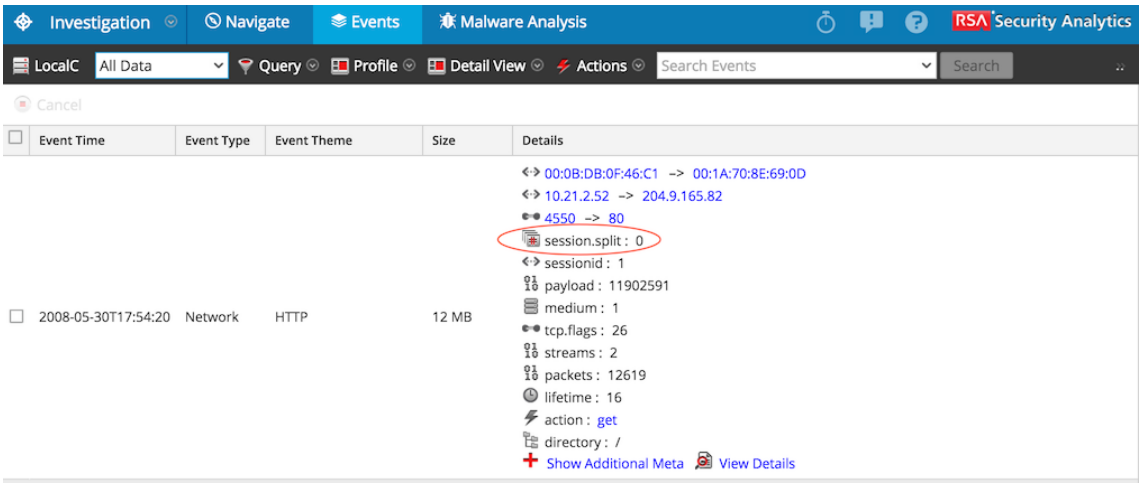
Each session fragment has an additional meta, `session.split`. The value of the `session.split` meta for a particular session fragment indicates how many fragments precede that fragment. When viewing sessions in the Events view, the `session.split` meta clearly identifies sessions that are fragments in the Events List view and the Events Detail view.

The session split happens when the configured Decoder `assembler.size.max` or `assembler.timeout.session` (latency between sessions) is reached. The earliest fragment is session 0 and sessions with a later time stamp are incrementally numbered 1, 2, 3, and so on. The `session.split` meta indicates the number of preceding sessions fragments; however, it does not always indicate that there are subsequent session fragments, even with a value of 0. It is also possible for the first fragment of the session to not have `session.split` meta if the session is parsed before exceeding the maximum session size.

Once you view the session fragments, you can determine the maximum session size or session timeout necessary for parsing to combine the split sessions into one again. For example, if you have four fragments at 32 MB, you need to configure your test Decoder (usually a virtual machine set up separate from main production service) with a maximum session size greater than 128 MB. The steps are the same to find all fragments based on a session timeout. The figures below show the Events List view and the Events Detail view with fragmented session information highlighted.

Note: A maximum session size of 12 MB was configured at the time the screen captures below were created.





The `session.split` metadata is always displayed immediately following the address and port metadata in the details view. It is never hidden as additional metadata.

These enhancements make it possible to quickly:

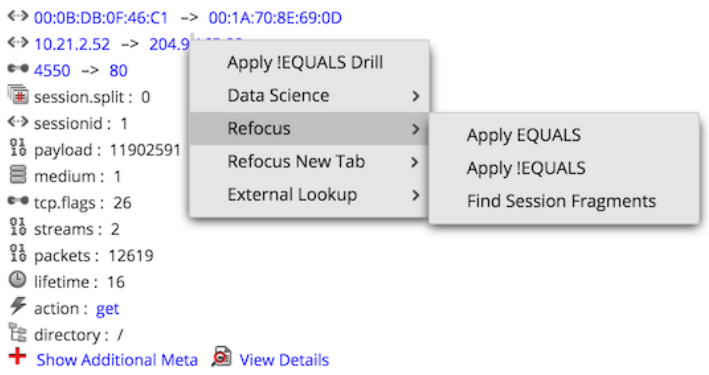
1. Identify sessions that are fragments of a network sessions.
2. View all of the session fragments of a network session given a single session fragment.
3. Export the packets for the entire network session as a single PCAP file.

Find and Combine Fragments

From within the Events view, you can find fragments of a session using the Refocus > Find Session Fragments context menu option. Security Analytics composes a query using the source and destination addresses and ports of the selected session and displays all sessions that match that query within the current time window.

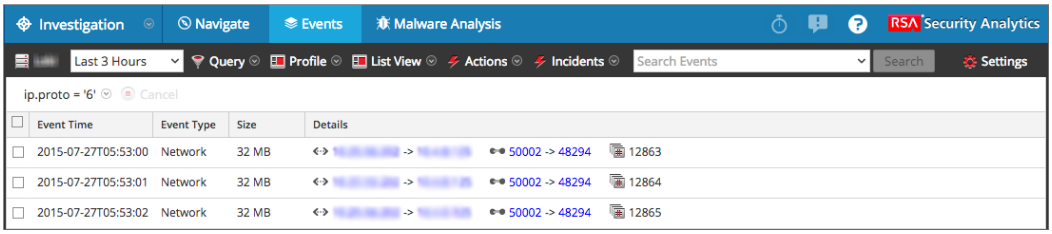
To find session fragments:

1. In the **Investigation > Events** view, right-click any of the source and destination address and port values: `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport`, and `udp.dstport`) as well as `session.split` values.
   The context menu is displayed.



2. Select **Refocus > Find Session Fragments** or **Refocus New Tab > Find Session Fragments**.

   Security Analytics repopulates the Events list with session fragments for a single session within the current time range. Depending on the option you selected, the refocus replaces the current view or opens in a new tab. (All data is used in these examples but is not recommended on production systems).



3. If necessary, adjust the time range to include any session fragments that may precede or follow the current time window. You can tell that the time range needs to be expanded if the fragments occur near the time boundary, especially if the first visible fragment does not have a split value of 0 (or none). Alternately, inspecting the packets of the last visible session may lead you to believe that the session continues. Here is an example:

   a. If you are looking at fragments that are obviously not the first fragment, for example, 1, 2, 3, and 4 in time range 10:30 to 10:35, there should be a fragment 0. You can increase the time range to start earlier (for this example, 10:25) to find the additional fragment.

   b. If the session size of last fragment is close to maximum session size (12 MB in this example), look for additional fragments by increasing the time window to include a later time (for this example, 10:40).

      When all of the session fragments of a network session are included within a single Events list, the list can span multiple pages.

4. (Optional) To export the packets for every session fragment to a single PCAP file, select **Actions > Export All PCAP**.

A message informs you that the PCAP is being downloaded. When download is complete, PCAP file includes the entire network session that was fragmented.

Export Events and Extract Files

When analysts are viewing an event reconstruction in Security Analytics Investigation, the Actions menu has an option to extract files from the event being viewed and export them to an archive.

Note: You can only export session files that you have permission to view or access.

The file export function queries the service for all sessions inside the selected time range and drill point to extract the content of each session. The details being exported are affected by both the time range and drill point at the time of exporting. In the File Extraction dialog, you can choose:

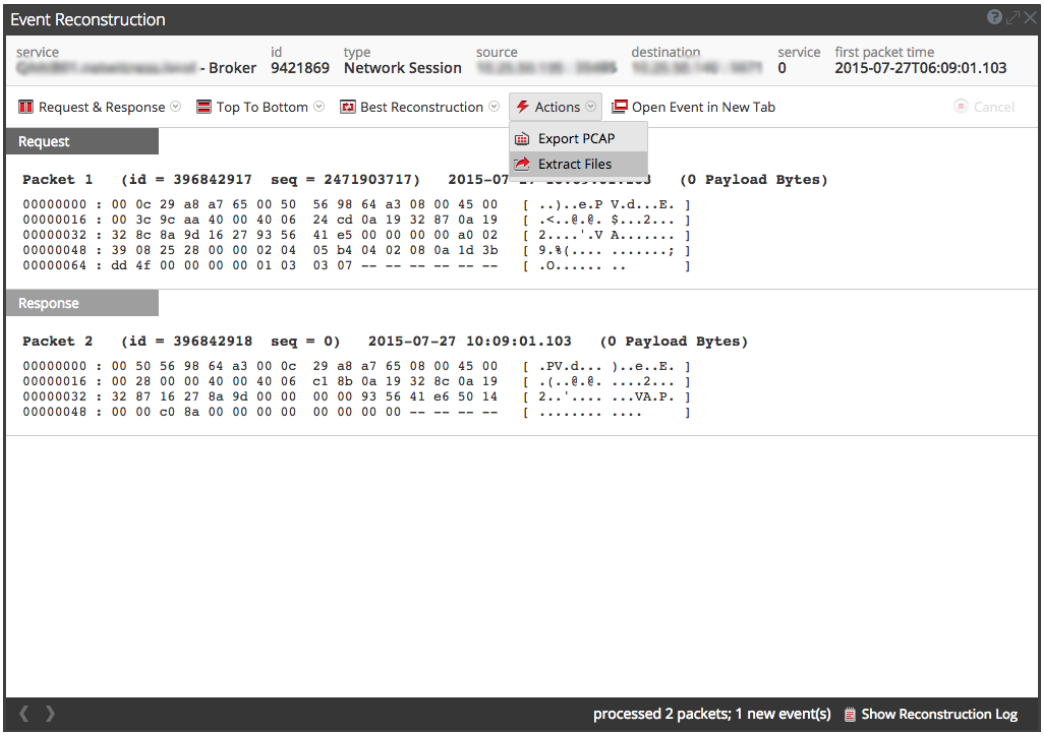
- The type of the content to export: archives, audio BitTorrent, documents, executable, images, other, video, and web.
- The format of the exported archive: ZIP or GZIP file.

After you send the request, a job is scheduled and you can track the job in in the Jobs tray. If there is an error retrieving the log or PCAP from the service, Security Analytics displays an error notification.

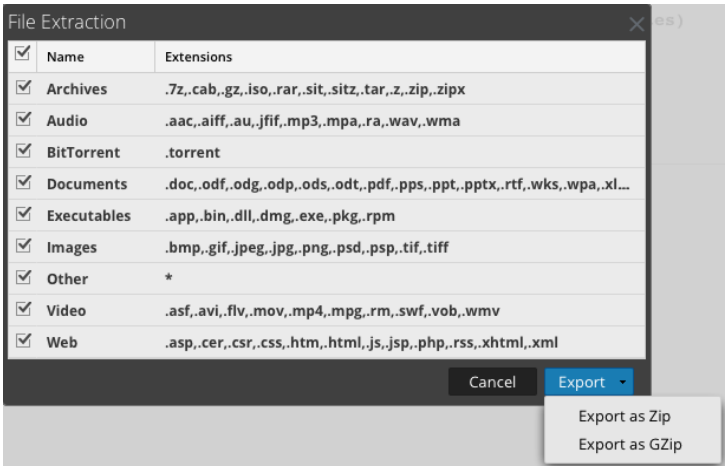
To extract files from an event:

1. While in the **Detail View** or **List View** of an event reconstruction, click an event.
2. Click **Actions** menu in the Event Reconstruction toolbar.
3. If you want to export the event, select **Export PCAP** in the drop-down menu.
   A message informs you that the PCAP is being downloaded.

4. If you want to extract files, select **Extract Files**.



5. The **File Extraction** dialog is displayed.



6. In the **Name** column, select the types of content that you want to extract.

7. To generate an archive of the selected file types contained in the event, click **Export**.
   A drop-down list of archive types for the export is displayed.

8. Select **Export as Zip** or **Export as Gzip**.
   The content that you specified is extracted to an archive and downloaded to the local file system.

Filter and Search Results in the Events View

Analysts can filter the results in the Investigation > Events view and, by searching for events or selecting the service on which to view events, set the time range, and query meta data.

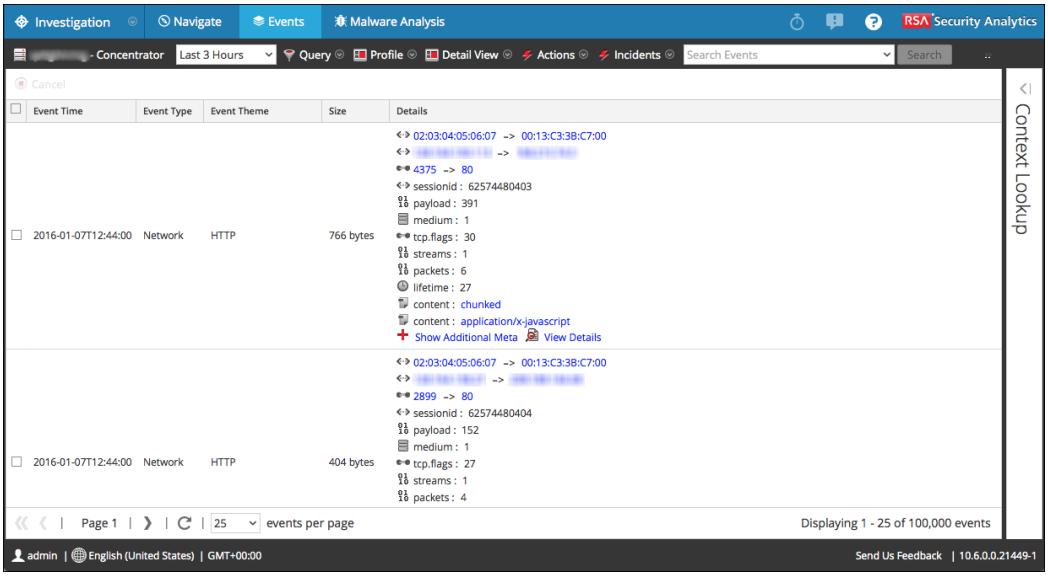
If you opened the Events view from a Navigate view drill point, the view opens to the Detail view of events by default. Analysts who do not have permissions to use the Navigate view can query services directly from the Events view. There are several configuration options to filter the information displayed in the Events view.

Note: When an Archiver is the currently selected service in the Events view and you are searching against a Broker or Concentrator, the search is slower than if searching against a Broker or Concentrator because the data on the Archiver is compressed and there is typically more data.

Filter Events Displayed in the Events View

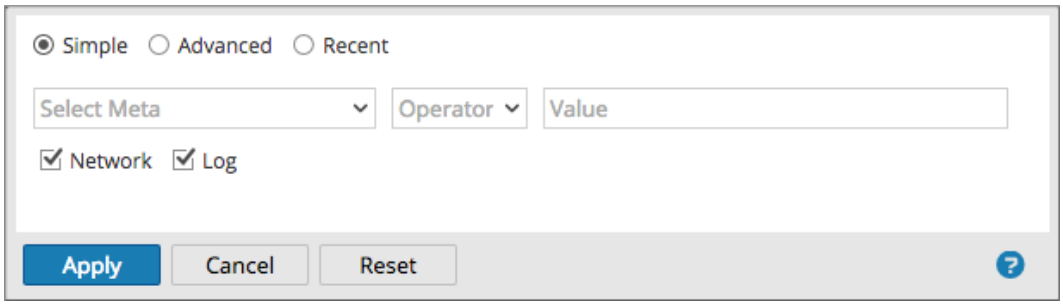
To filter the data displayed in the Events view:

1. In the **Security Analytics** menu, select **Investigate > Events**.
   The Events view is displayed.

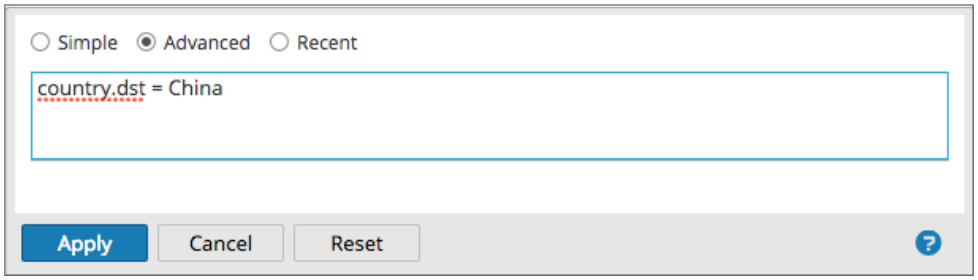


2. To select a time range other than the default (**Last 3 Hours**), in the toolbar, click the time range field and select a value. For example, **Last Hour**.
   The Events view is refreshed with the selected time range.

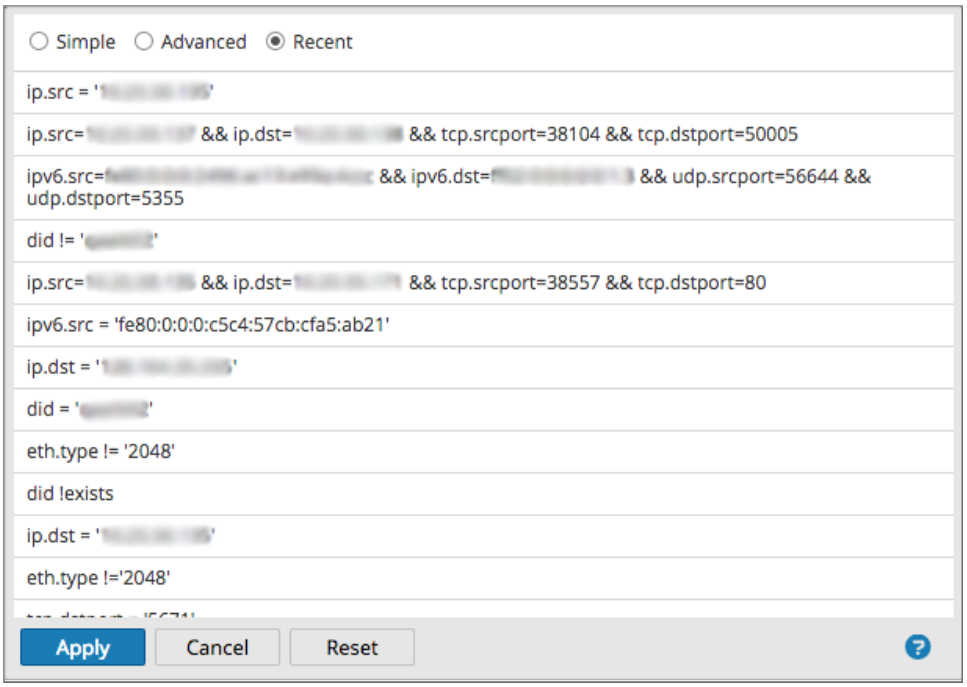
3. To enter a query for the selected service and time range, in the toolbar, click **Query**.
   The Simple Query dialog is displayed.



4. If you want to enter a simple query using the auto-complete feature to select meta and operators, do one of the following:
   a. Click in the **Select Meta** field and select a meta key from the drop-down list.
   b. Select an operator from the drop-down list in the **Operator** field.
   c. Type a value to match in the **Value** field.
   d. Select **Network**, **Log** or **Endpoint** data, and click **Apply**.
      The matching data is displayed in the Events view.
5. If you want to enter a more complex query based on your knowledge of the meta and operators:
   a. Click **Advanced**.
      The Advanced Query dialog is displayed.

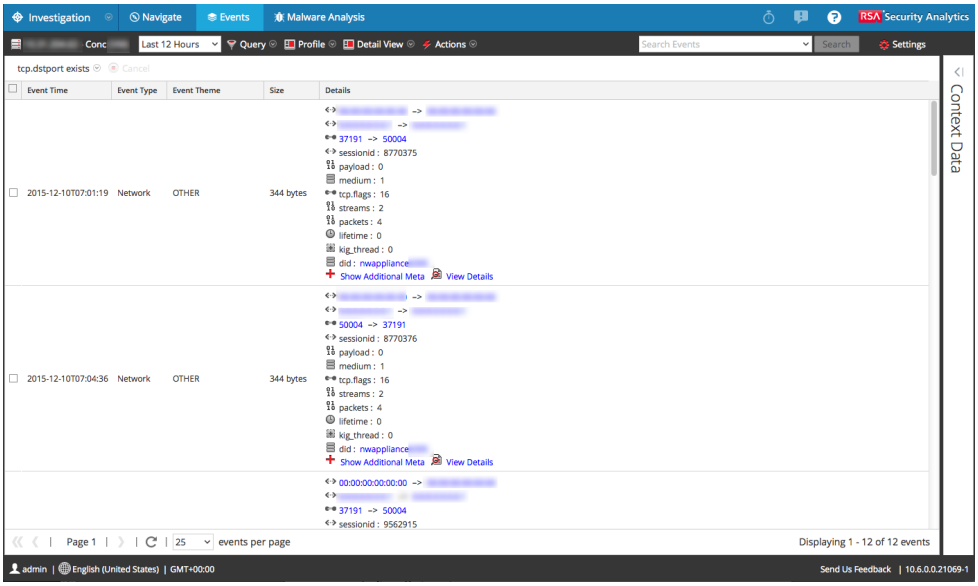


   b. Type a query. As you type the query, beginning with the meta key, drop-down lists of available meta keys and operators are displayed. When finished, click **Apply**.
6. If you want to select a query from a list of recent queries:
   a. Select **Recent**.
      The Recent Query dialog is displayed.



b. Select a query and click **Apply**.

The matching results for the query are displayed in the Detail View in the Events view. Notice that the breadcrumb reflects the query (tcp.dstport exists, in the example).



c. In the breadcrumb, you can click any of the crumbs to display the Query menu. You can insert a new query before a crumb, and append a new query to the end of breadcrumb. After each edit in the breadcrumb, Security Analytics refreshes the results.

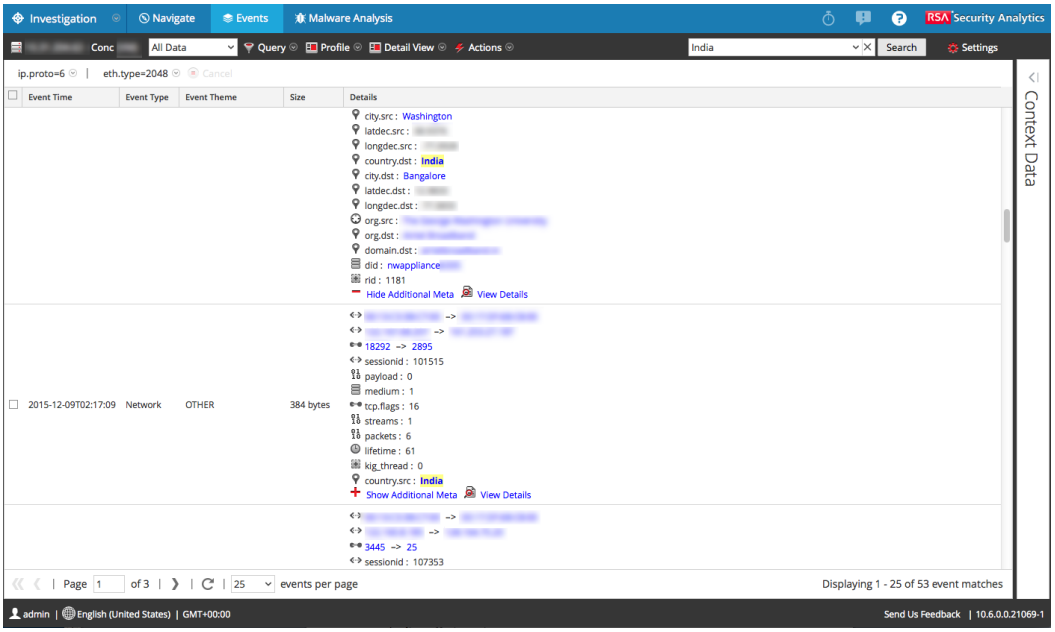
Search for Events in the Events View

You can search the currently displayed data in the Events view by entering a search string in the Search field. The search string can be a regex (Regular Expression) or it can be a simple text search. Investigation - Search Options provides detailed information on these search types.

To search within the currently displayed data in the Events view:

1. To execute the search, place the cursor in the Search box, type a search string, and press **Enter** or click **Search**.

   The search results are displayed in the Events view. Events that match the search criteria are displayed in the Event view grid. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column. Below is an example of the search results for the search term **India** in the Events Detail view. Note that search matches are not highlighted in any Event Reconstruction.



2. If you want to narrow the search, change the query and time as described above in Filter Events Displayed in the Events View.
3. If you want to stop the search and return to the Events view, click **Cancel**.

   Any results that are displayed remain.
4. To clear the search box and return to the normal Events view, click the **X** in the search box.

Manage Column Groups in the Events View

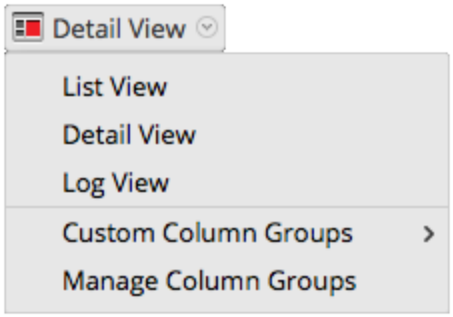
This topic provides instructions for an analyst to create and manage custom column groups for displaying data in the Navigation > Events view.

When viewing a list of events in Security Analytics Investigation > Events view, you can customize the way data is displayed by defining the meta to display in a column, the position of the column in the grid, and the default width of the column.

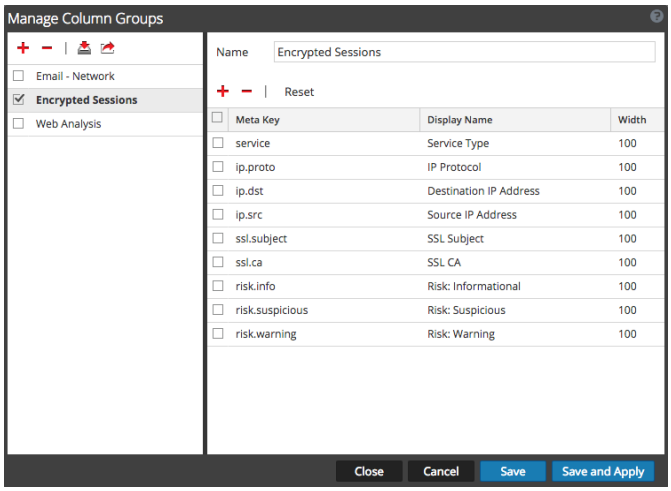
Note: Investigation profiles can include custom column groups. If a custom column group is used in a profile and you are viewing events in the Events view using a custom column group, you cannot change the view type (Detail, List, or Log).

Create Custom Column Group

1. In the **Security Analytics** menu, select **Investigation > Events.**
   The Events view is displayed.
2. Select **Manage Column Groups** in the toolbar (the option name is the default value (Detail View or the current value).



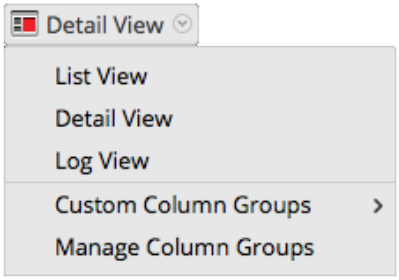
   The Manage Column Groups dialog is displayed. This example has one column group already defined.



3. To add a new column group in the column group panel, click + and type the name of the new group in the resulting field.
4. The column definition panel opens on the right with the group name filled in. You can edit the group name.
5. To add a column to the group, click +, and click in the empty **Meta Key** field to display the **Meta Key** drop-down list.
6. Select a meta key field from the list, and repeat this step until the column set is complete.
7. (Optional) To delete a meta key from the column group, click −.
8. (Optional) To rearrange the sequence in which the columns appear in the Events list, drag meta keys to the desired position.
9. (Optional) To set the default width for a column, click in the corresponding value in the **Width** column, and type a new column width.
10. (Optional) To revert to the previous settings for the column group, and undo all of your changes, click **Reset**.
11. When ready to save, do one of the following:
    a. To save the the edited column group and refresh the Events view with the column group settings, click **Save and Apply**.
    b. To save the edited column group without refreshing the Events view, click **Save**.

Select a Custom Column Group

1. With the Events view open, select **Custom Column Groups** in the toolbar (the option name is the default value (Detail View or the current value).



2. Select one of the custom groups from the submenu.
   The Events view is refreshed to reflect the custom column group.

Reconstruct an Event

When viewing a list of events in Security Analytics Investigation > Events view, you can safely create a reconstruction of the event in a readable form that matches the original. By default, the initial view of a reconstructed event is the most suitable format (Best Reconstruction); for example, web content is reconstructed as a web page; an IM conversation is displayed with both parts of the conversation. Each user can select a different default reconstruction in the Profile > Preferences view.

In the reconstruction, you can:

- Select event information to view. Possible values are: request data, response data, both request and response data.
- Select the reconstruction type: details, text, hex, packets, web, mail, or IM.
- Export raw logs.
- Export the event as a PCAP file.
- Extract any files available in the event.

  Caution: Be careful when clicking a link to a file in the Reconstruction. If your system has an application associated with the file , or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

- Display the event in a separate window or tab (depending on your browser configuration).
- If you are viewing the reconstruction as a preview in the current view, you can page forward to the next event and back to the previous using the navigation buttons in the bottom left corner.

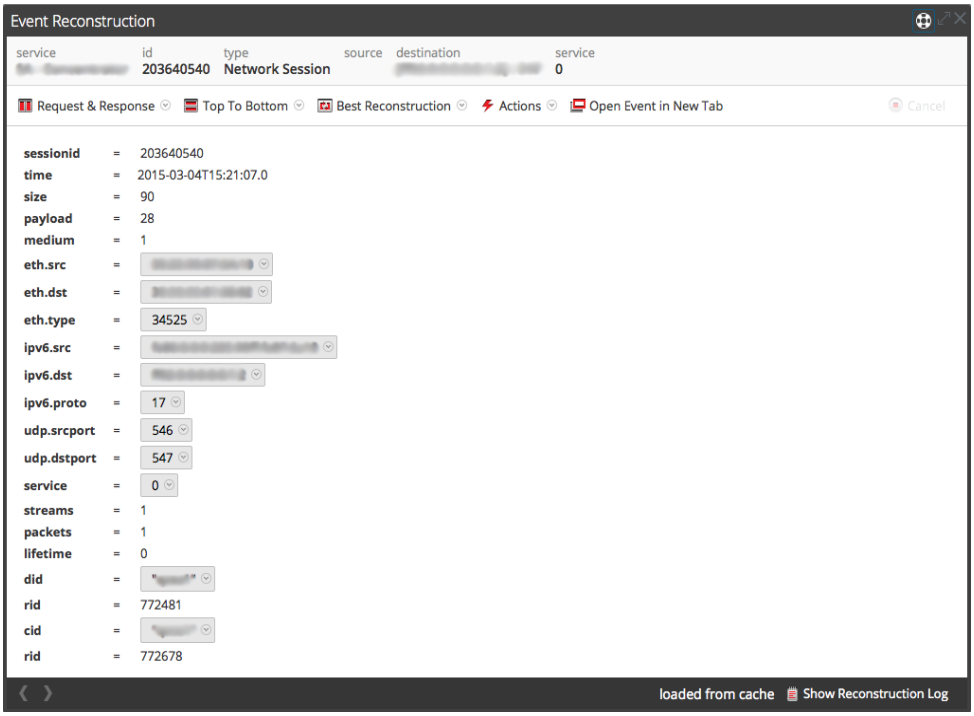
Note: Security Analytics Reconstruction Settings and Reconstruction Cache Settings allow an administrator to manage application performance for Investigation. As analysts reconstruct sessions that they are investigating, two situations can affect performance and results.
-Some events can be very large and contain many thousands of source packets. Reconstructing these types of sessions can degrade application performance.
- In some cases, the reconstruction cache can present incorrect content; for this reason, a Security Analytics cleans cache that is older than a day every 24 hours. Between the daily cache cleanings, certain actions my result in stale cache being used for a reconstruction, and if the need arises, administrators can manually clear cache for one or more services that are connected to the current Security Analytics server.

Reconstruct an Event

1. Open a drill point in the **Events** view.
2. To show all meta data, click Show Additional Meta.
3. To open an event reconstruction in the current view, do one of the following:

   a. At the end of the event, select View Details.

   b. Select an event to reconstruct and select **Actions > View Event > Preview Inline**.
   The Event Reconstruction opens in a popup window in the same view. By default, Security Analytics displays the best reconstruction for the event determined by the event content or the reconstruction that you have selected in the Default Session View setting for Investigation. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view side-by-side results, export an event, open an email attachment, extract files, and open the event in a new tab.

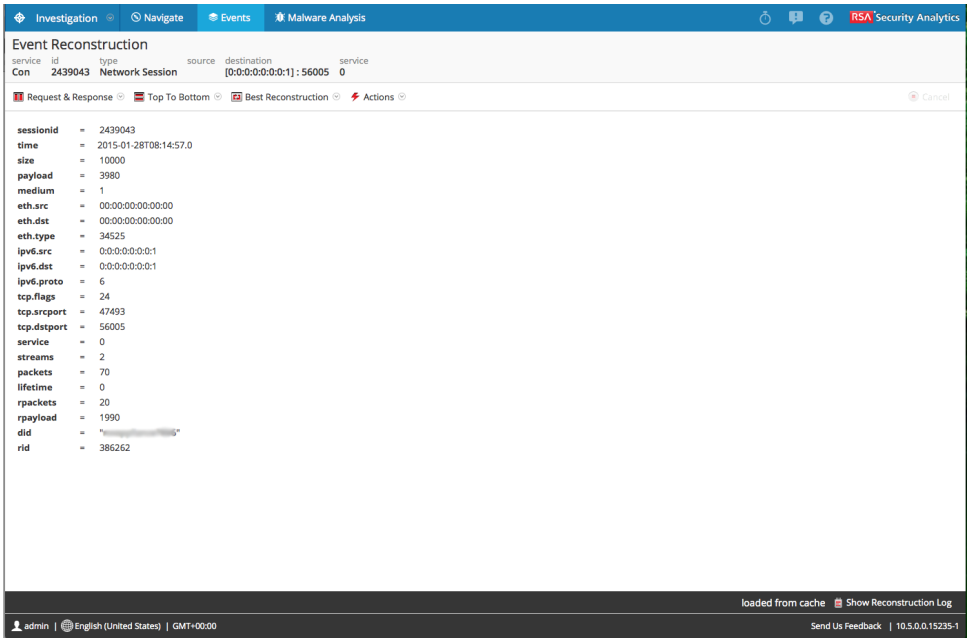


4. To preview a reconstruction of the next event, click ❯ or to preview a reconstruction of the previous event, click ❮.
5. To open an event reconstruction in a new tab, do one of the following:

   a. In the **Events** view, select an event to reconstruct and select **Actions > View Event> Open in New Tab**.

   b. In the **Event Reconstruction** toolbar of previewed reconstruction, click **Open Event in New Tab** in the toolbar.

The Event Reconstruction opens in a new tab.



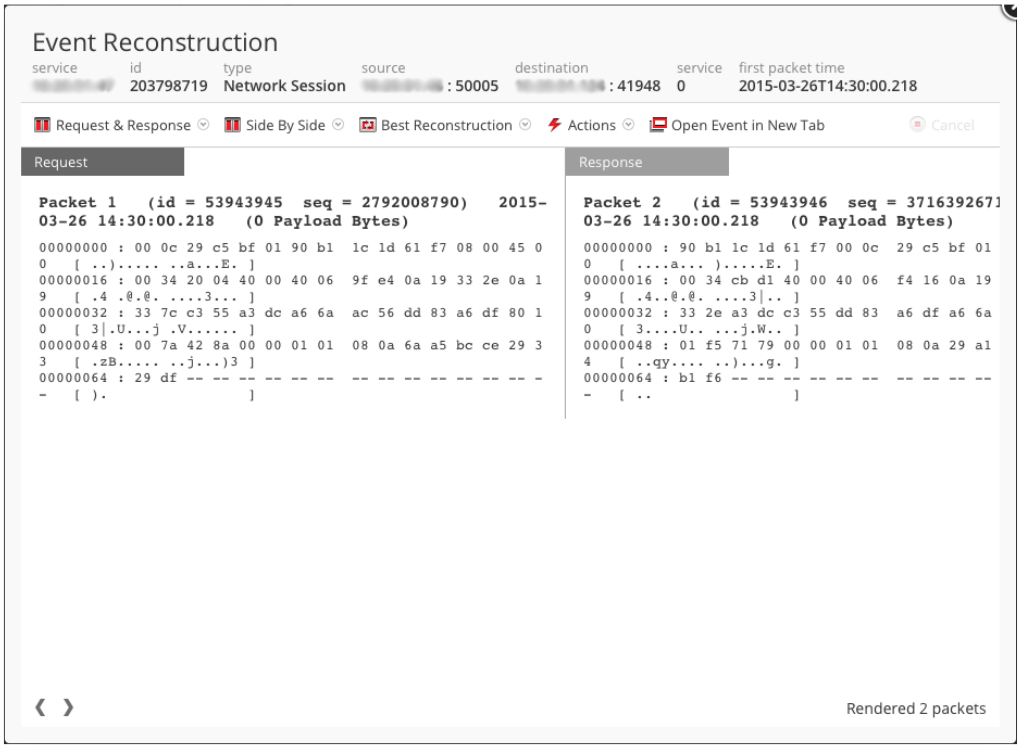
Note: In case of masqueraded files, the meta view in the event reconstruction view might show the masqueraded file extensions, while the files view in the event reconstructions view display the actual file extension (true file type), as that is detected and set by the decoder. For example, if a malware executable of type .exe is being masqueraded and sent as a .jpg file to the network, when you reconstruct that session, in the files view of event reconstruction view, file extension is displayed as .exe instead of .jpg as.exe is the actual extension of a file. And, the file type will also be displayed as executable.

View Side by Side or Top to Bottom

To select the way requests and responses for an event are displayed:

1. In the **Event Reconstruction** toolbar, click **Top to Bottom** or **Side by Side**.
2. In the drop-down menu, select the information you want to see in the event: **Side by Side** or **Top to Bottom.**

The reconstruction is refreshed with the selected information.



Select Event Information to View

To select what event information to view:

1. In the **Event Reconstruction** toolbar, click **Request & Response**.
2. In the drop-down menu, select the information you want to see in the event: **Request & Response**, **Request**, or **Response**.
   The reconstruction is refreshed with the selected information.

Select Event Reconstruction Type

To select the reconstruction type for an event:

1. In the **Event Reconstruction** section toolbar, click **Best Reconstruction**.
2. In the drop-down menu, select the reconstruction type to view: **meta**, **text**, **hex**, **packets**, **web**, **mail**, or **files**.
   The reconstruction is refreshed with the selected reconstruction type.

Open or Download an Email Attachment

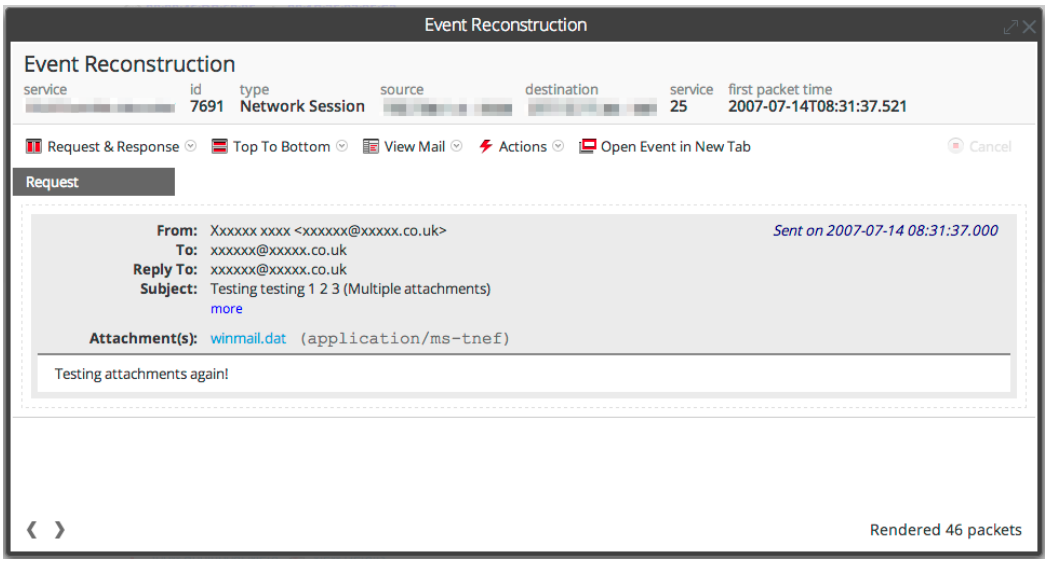
When viewing a reconstruction of an email that has attachments, you can open supported file types or download the files to the local system.

Caution: Be careful when selecting file attachments. If your system has an application associated with the file attachments, or the browser is capable of opening them, and the attachments are malicious, they can negatively affect your system.

To open or download email attachments:

1. In the **Event Reconstruction** section toolbar, select the View drop-down and select **View Mail**.

   The Event Reconstruction is displayed.



2. In the **Event Reconstruction** section of the email, click the Attachment.

   If the file type is supported by the browser, the attachment will open in a new tab.

   If the file type is not supported, the Download dialog is displayed so that you can download the attachment.

Export an Event as a PCAP File

The PCAP export option downloads the sessions for the current time range and drill point to a PCAP file. To export an event as a pcap file:

1. In the **Event Reconstruction** section toolbar, click **Actions**.
2. Click **Export PCAP**.
3. A confirmation dialog is displayed.

4. Click **OK**.
   The job is scheduled and when complete the PCAP is downloaded to the local file system. In the Profile > Jobs tab, you can download the PCAP.

Extract Files from a Reconstructed Event

The Extract Files option extracts and downloads the files associated with the event. To extract files:

1. In the **Event Reconstruction** section toolbar, click **Actions**.
2. Click **Extract Files**.
   The File Extraction dialog is displayed.
3. Select the types of files to extract,and click **OK**.
4. The job is scheduled and when complete the selected file types are downloaded to the local file system. In the Profile > Jobs tab, you can download the files.

Conduct Malware Analysis

Analysts can use the RSA Security Analytics Malware Analysis service to detect malware.

Once you initiate a Malware Analysis investigation, there is no specific order in which to conduct the investigation. Instead, Security Analytics offers various methods of displaying the data, filtering the data, querying the data, acting on a drill point, and inspecting specific events. This topic provides information and procedures for analysts who are using the RSA Security Analytics Malware Analysis service to detect malware in selected data and files.

Analysts who conduct analyses using Security Analytics Malware Analysis need to have the appropriate system roles and permissions set up for their user accounts. See Roles and Permissions for Analysts in the *Malware Analysis Configuration Guide*.An administrator must configure roles and permissions.

This document groups investigation tasks according to high-level functions of an Investigation:

- Begin a Malware Analysis Investigation.
- Upload Files for Malware Analysis Scanning.
- Implement Custom YARA Content.
- Filter Dashlet Data in the Summary of Events View.
- Examine Scan Files and Events in List Form
- View Detailed Malware Analysis of an Event.

Begin a Malware Analysis Investigation

This topic provides instructions for investigating data scanned by Malware Analysis in Security Analytics Investigation.

You can investigate data that has been scanned, flagged, and rated by Security Analytics Malware Analysis as containing Indicators of Compromise. This includes all types of Malware Analysis scans: continuous mode polling, on-demand polling, and on-demand uploaded files. Continuous mode polling must be enabled when the administrator configures basic settings for the Malware Analysis service.

Security Analytics provides several methods of launching a Malware Analysis investigation.

Fastest: Instant Launch from Malware Analysis Dashlets

The fastest way to begin a Malware Analysis investigation is an Instant launch from the Security Analytics Dashboard using one of the Malware Analysis dashlets that lists events or files that are likely to contain malware. From one of these dashlets, you can go directly to the Analysis Results for a specific event that has been listed as worthy of investigation:

- Top Listing of Highly Suspicious Malware
- Top Listing of Possible Zero Day Malware
- Malware with High Confidence IOCs and High Scores Dashlet

On-Demand Polling from a Meta Value in the Navigate View

You can initiate on-demand polling from within an investigation by right-clicking a meta value in the Navigate view, and choosing an option from the context menu. When polling is complete, the scanned data is available for malware analysis (see Launch a Malware Analysis Scan from the Navigate View).

Investigate a Specific RSA Service

You can also begin a Malware Analysis investigation of a service in the Investigation > Malware Analysis view. For Malware Analysis investigation on a service basis, a service must be specified in the Investigation > Malware Analysis view:

1. Security Analytics opens the Malware Analysis view with the user-specified default service selected.
2. If no default service is currently specified, Security Analytics presents a dialog for selecting the Malware Analysis service to investigate.

3. When a service has been selected manually or by default in the Malware Analysis view, Security Analytics opens the Summary of Events for the selected service and continuous scan data for the service.

This topic provides instructions for all methods of launching a Malware Analysis investigation.

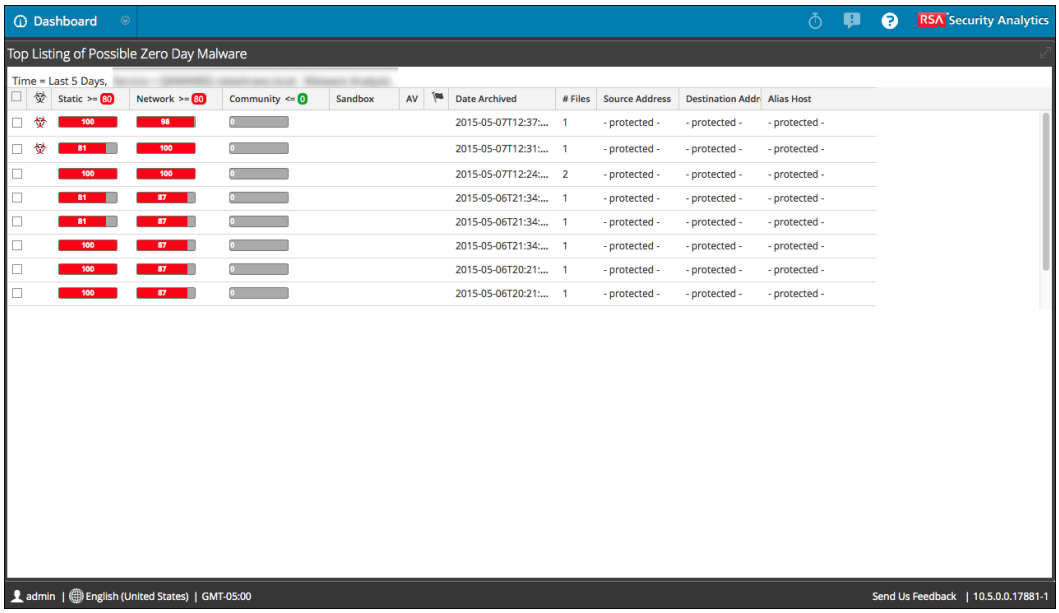
Launch a Malware Investigation from a Malware Analysis Dashlet

A prerequisite for this procedure is that one of the following dashlets must be visible in the Unified dashboard or in the Malware Analysis view, and must be populated with listed events or files. If you do not see the dashlets, add them and configure the dashlets.

- Top Listing of Highly Suspicious Malware
- Top Listing of Possible Zero Day Malware
- Malware with High Confidence IOCs and High Scores Dashlet

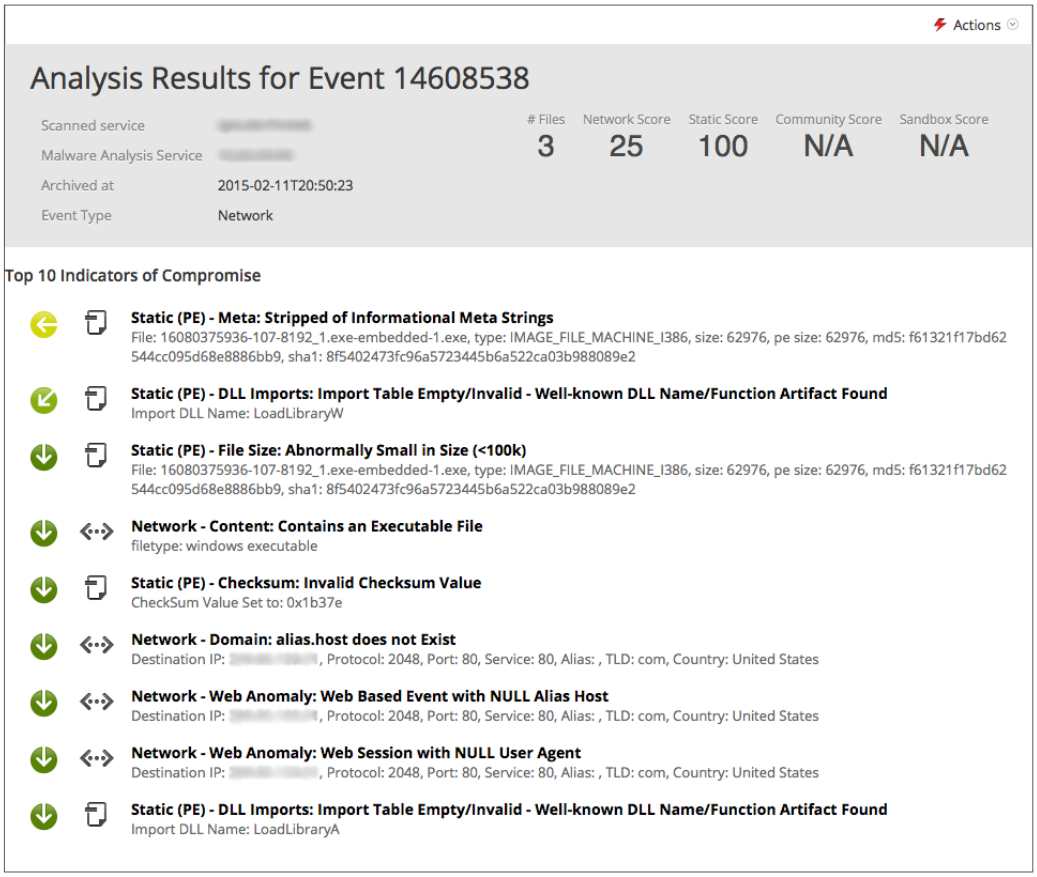
To launch a Malware Analysis investigation from a dashlet:

1. Log on to Security Analytics and look for one of the above dashlets in the main dashboard or in the Malware Analysis view. Below is an example of the Top Listing of Possible Zero Day Malware Dashlet configured to show files.



2. In the dashlet, double-click an event or file for deeper analysis. A detailed analysis of the event in the Events List or the event with which the file in the File List is associated is

displayed in the Malware Analysis view.



To learn more about configuring the Malware Analysis dashlets in the Unified dashboard, see "Dashlets" in the *Getting Started with Security Analytics Guide*.

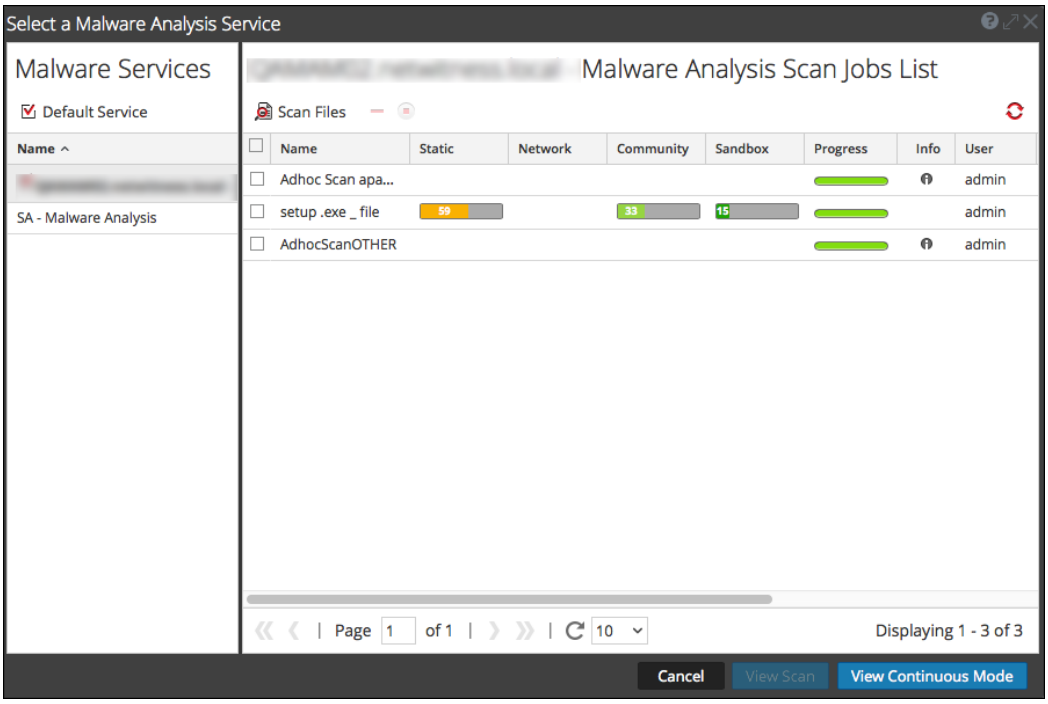
To learn about the ways you can configure and filter information in dashlets in the Malware Analysis view, refer to Filter Dashlet Data in the Summary of Events View.

To learn about the actions you can perform in the Analysis Results, refer to View Detailed Malware Analysis of an Event.

Begin a Malware Analysis Investigation (No Default Service)

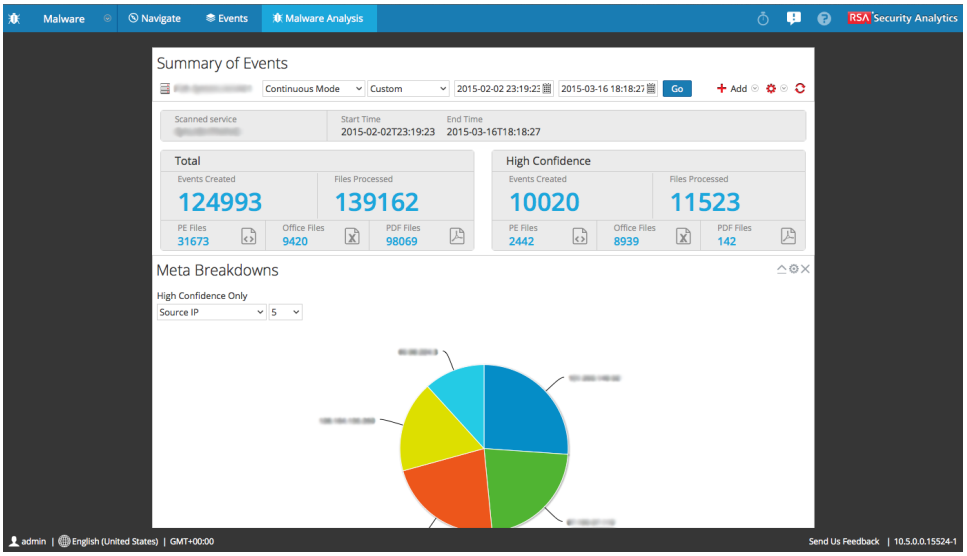
To begin an investigation with no default service specified:

1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.
   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel and available scan jobs in the right panel. This scan jobs panel contains the same columns as the Malware Scan Jobs dashlet in the Unified dashboard. In addition, it has a toolbar and View options, which are described in Investigation - Select a Malware Analysis Service Dialog.



2. In the list of Malware Analysis hosts, select a host and a list of scan jobs is displayed in the right panel.
3. To begin analyzing a scan, do one of the following:
   a. Select a scan and click **View Scan**.
   b. Click **View Continuous Mode**.
      The Summary of Events for the selected scan is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter

Dashlet Data in the Summary of Events View.



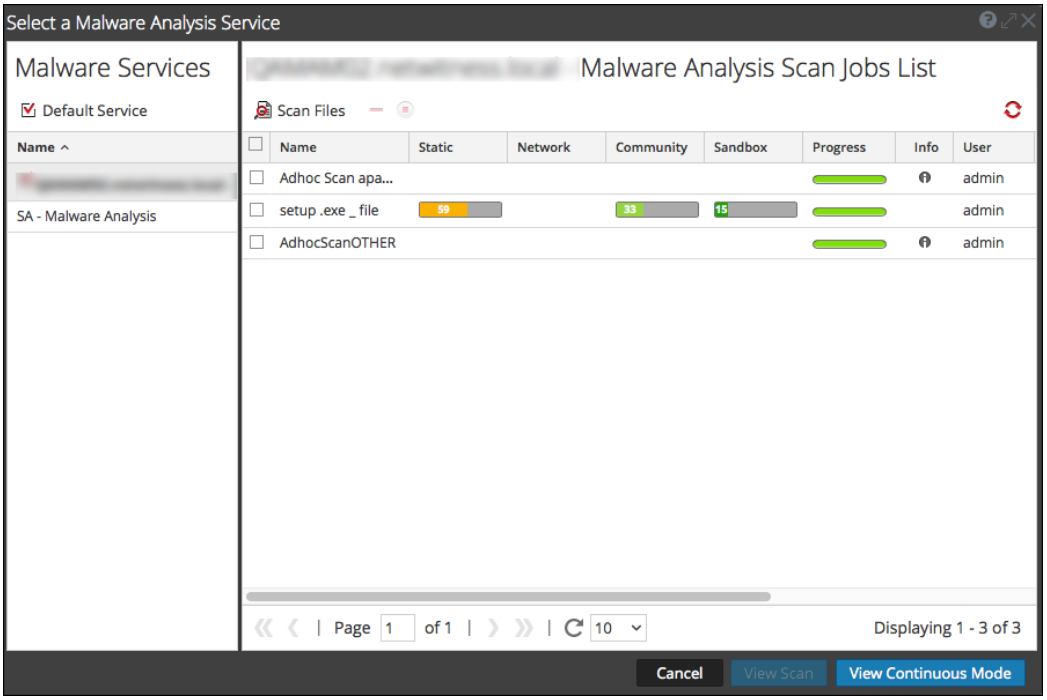
Set or Clear the Default Service

You can set the default service and clear the default service in the Select a Malware Analysis Service dialog.

To set a default service:

1. Click the service name in the Summary of Events toolbar.

   The Select a Malware Analysis Service dialog is displayed.



2. Select a service on the list of available Malware services, and click Default Service.

   The service becomes the default, (indicated by ☑ in front of the host name).

3. To clear the default service, select the default service in the grid, and click Default Service.

   No default service is set.

Upload and Scan Files

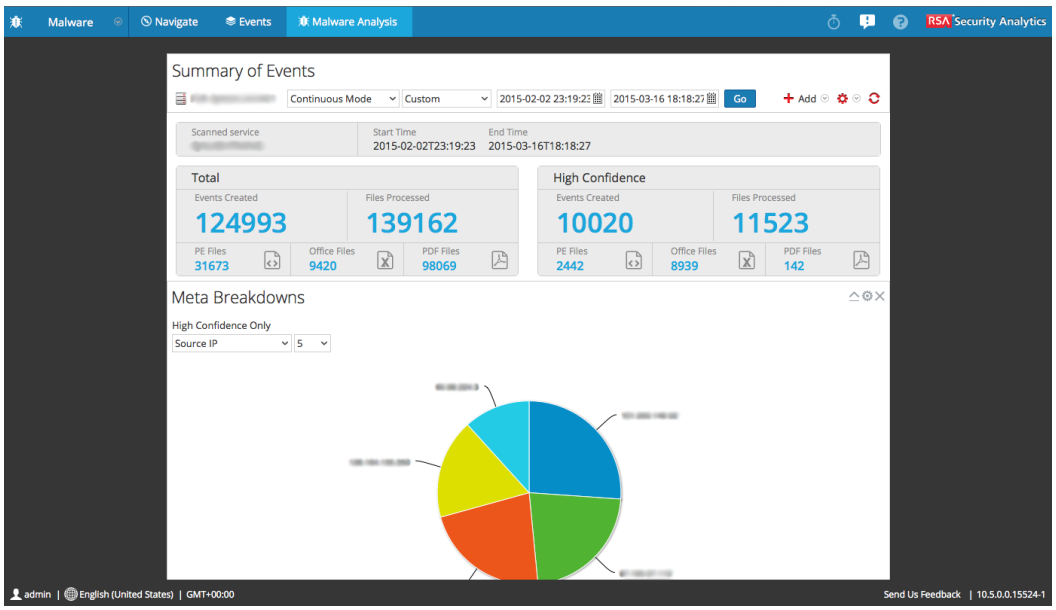
A Malware Analyst with permission to `Initiate Malware Analysis Scan` can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog (see Upload Files for Malware Analysis Scanning. An administrator can upload packet capture files to a Decoder for Malware Analysis in the Services System view as described in "Upload Packet Capture File" in the *Decoder and Log Decoder Configuration Guide*.

Begin an Investigation (Default Service Specified)

To begin an investigation with a default service specified:

1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.

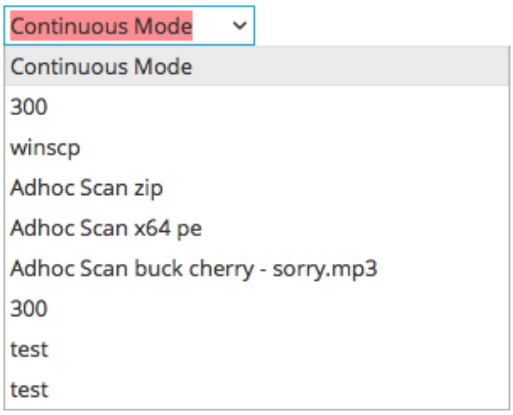
   The Summary of Events for a continuous scan of the selected service is displayed with the default dashlets open. Each user can add, modify, and delete default dashlets, which persist through different scan investigations. Users can also restore default dashlets as described in Filter Dashlet Data in the Summary of Events View.



Apply Time Parameters Filter for Results

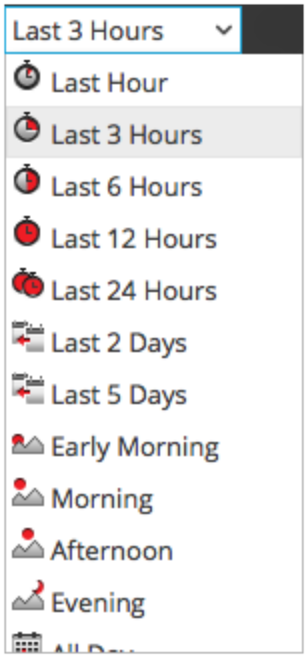
You can apply a Threshold filter to refresh the results of the chosen dashlets.

1. To select a different time range, select either **Continuous Mode** or a different scan from the toolbar.



   The Malware Summary of Events for the selected scan is displayed.

2. To select a new time range for the scan, click in the range selection list in the toolbar. Ranges available are: Last 5 minutes, Last 10 minutes, Last 15 minutes, Last 30 minutes, Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 5 Days, Early Morning, Morning, Afternoon, Evening, All Day, Yesterday, This Week, Last Week, or Custom.



The results are updated immediately.

3. To refresh a continuous mode scan with new data, click  .

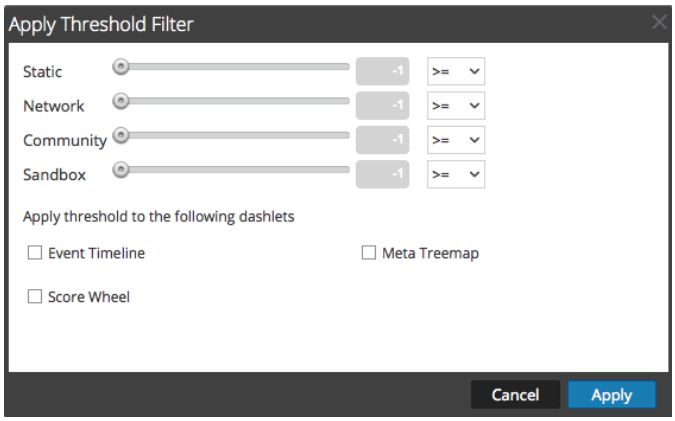
Apply a Threshold Filter to Continuous Mode Results

You can apply a new threshold filter to an instance of the Malware with High Confidence IOCs and High Scores dashlet, the Meta Treemap dashlet, the Score Wheel dashlet, and the Event Timeline dashlet.

To customize the scoring applied to the scan, in the toolbar, do the following:

1. Select **Settings > Apply Threshold Filter.**

   The Apply Threshold Filter dialog is displayed.



2. If you want to limit the number of events displayed to events that were given a score above a certain number, do the following:

   a. Drag the slider in the Static, Network, Community, and Sandbox slider bars.

   b. To select the dashlets in which the thresholds apply, select the appropriate checkboxes.

   c. Click **Apply**.

Delete or Resubmit an On-Demand Scan with New Bypass Settings

You can delete an on-demand scan or resubmit an on-demand scan with different bypass settings than those specified in the Service Configuration view for a Malware Analysis service.

To delete a scan while viewing an on-demand scan, do the following:

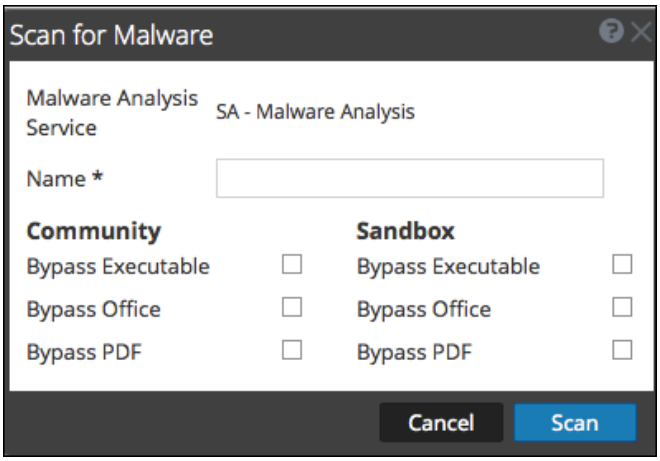
1. Select **Actions > Delete Scan**.

   Security Analytics asks for confirmation that you want to delete the scan.

2. Click **Yes**.
   The selected scan is deleted.

To apply different bypass settings to the current scan:

1. Select **Actions > Resubmit Scan**.
   The Scan for Malware dialog is displayed.



2. Select the bypass settings that you want to use on the new scan, and click **Scan**.
   Malware Analysis resets cache and resubmits the file for a new scan, and Security Analytics adds the scan to the jobs queue.
3. When the job is complete, scroll to the left and select **View**.
   The Malware Summary of Events for the selected scan is displayed.

View the Files List

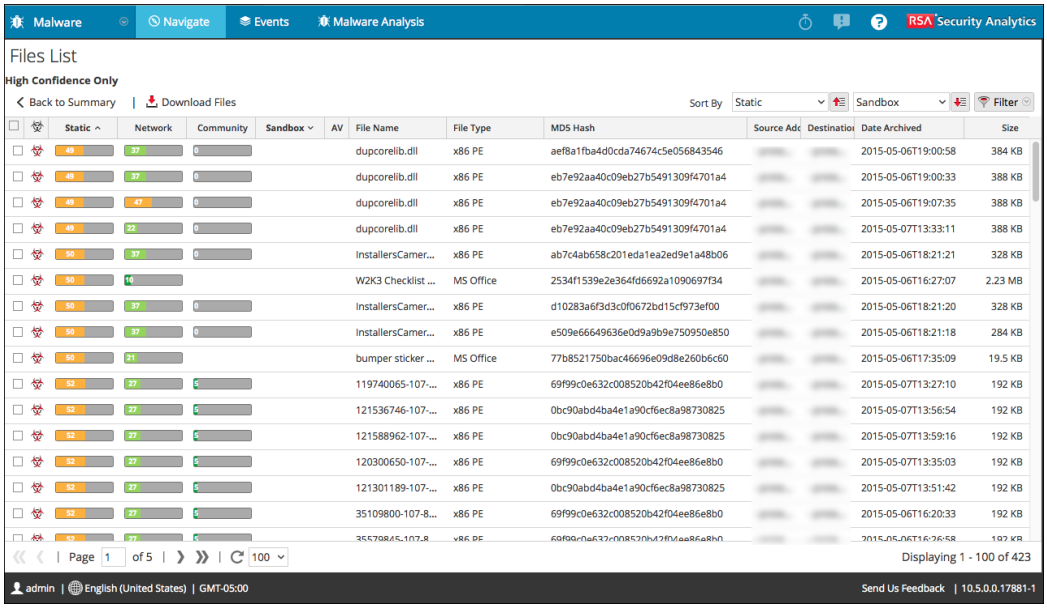
You can view a list of files for an event from the Malware Analysis Summary of Events and from each of the Visualization charts: Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel.

To view the Files List, do one of the following:

- In the Summary of Events, click on the number of files in the **Total** row or the **High Confidence** row under **Files Processed**, **PE Files**, **Office Files**, or **PDF Files**. The Files List is displayed.

- In any visualization dashlet, click the number next to the **Files** field in the top right corner of the dashlet.

The Files List for the selected drill point is displayed.



From the Files List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files as described in Examine Scan Files and Events in List Form.

To return to the Summary of Events, click **Back to Summary**.

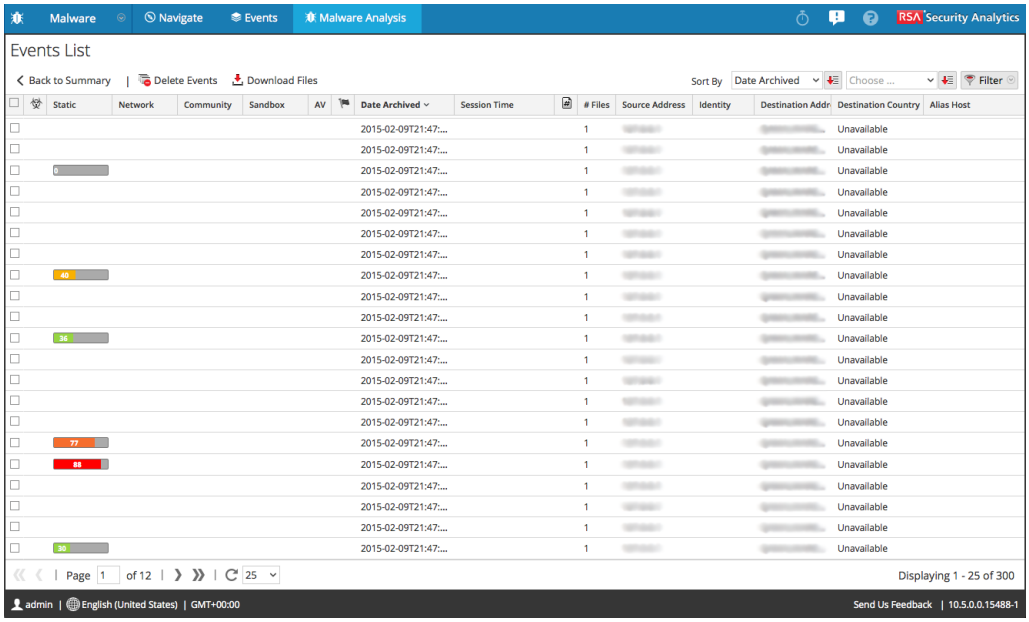
View the Events List

From the Malware Analysis Summary of Events and from each of the visualization charts (Event Timeline, Meta Breakdowns, Meta Treemap, and Score Wheel), you can select events to view in the Events grid.

To view the Events List, do one of the following:

- In the Summary of Events, click the number of Events Created in the **Total** row or the **High Confidence** row. The Events List is displayed.
- In any visualization dashlet, click the number next to the Events field in the top right corner of the dashlet.

The Events List for the selected time is displayed.



Implement Custom YARA Content

This topic provides instructions for implementing custom YARA content in Security Analytics Malware Analysis.

In addition to the built-in indicators of compromise, Security Analytics Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language that allows malware researchers to identify and classify malware samples. For more information on Yara version 3.5.0, see http://virustotal.github.io/yara/.

RSA makes built-in YARA-based Indicators of Compromise (IOCs) available in RSA Live; these are automatically downloaded and activated on subscribed hosts.

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the host to consume.

As malware and the threat landscape evolve, it is important to review and examine existing custom rules. Updates are often necessary to incorporate new detection methods. RSA also updates YARA rules in Live from time to time. To receive updates, you can subscribe to the RSA Blog and RSA Live at http://blogs.rsa.com/feed.

This document provides information to help customers implement custom YARA rules in Malware Analysis.

YARA Version and Resources

RSA Malware Analysis is packaged with YARA version 3.5.0. To find out the exact version, you can run `yara -v` on the Malware Analysis host as shown in this example:

```
[root@TESTHOST yara] # yara -v
yara 3.5.0
```

Meta Keys in YARA Rules

Malware Analysis (MA) is compliant with other sources of YARA rules, and it also consumes additional meta keys that are specific to Malware Analysis. Each YARA rule is equivalent to an Indicator of Compromise (IOC) within Malware Analysis. The example below illustrates the meta definitions in a rule:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Meta Key	Description
iocName	(Required) This is the name that MA uses as the rule name. It is specific to Malware Analysis and is required to add the rule to the IOC list.
fileType	Specifies the files type. Possible values are: WINDOWS_PE, MS_OFFICE, and PDF. If not specified, the default value is WINDOWS_PE.
score	This value that is added to the static score if the YARA rule is triggered. If not specified, the default value is 10.
ceiling	This is the maximum amount that is added to the static scores when a rule is triggered multiple times in one session. For example, if each time a rule is triggered, 20 points are added to the static, and you do not want more that 40 points added when the rule is triggered more than two times, you can specify a ceiling of 40. If not specified, the default value is 100.
highConfidence	This sets the High Confidence flag, which is set on IOCs when there are high confidence indicators that malware is present. If not specified, the default file value is false.

YARA Content

RSA Live contains 3 sets of Yara rules:

- PE Packers
- PDF Artifacts
- PE Artifacts

The following figure illustrates YARA content available as YARA rules in Security Analytics Live.

On the Malware Analysis host, the YARA rules reside in `/var/lib/rsamalware/spectrum/yara`, as shown in the example below.

```
[root@TESTHOST yara]# pwd
 /var/lib/rsamalware/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_
packers.yara
```

The individual rules are listed as IOCs in the Malware Analysis Service Config view > Indicators of Compromise tab. To view them, use the Yara module as the filter. You can adjust the configuration of an individual in the same way that you configure other IOCs.

Add Custom YARA Rules

To introduce custom YARA rules from other sources:

1. To ensure that the YARA rules follows the correct format and syntax, use the YARA command to compile the YARA rule as shown in the following example. If the rule compiles with no errors, this indicates that the YARA rule has the correct syntax.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
    [root@TESTHOST yara]#
   ```

2. Ensure that custom rules do not duplicate existing YARA rules from RSA or other sources. All YARA rules are in `/var/lib/rsamalware/spectrum/yara`.

3. Ensure that the meta keys that RSA supports are included to organize the YARA rules as part of the configurable IOCs, and name the file with the yara extension (<filename>.yara). For better organization, make sure that the `iocName` meta is included in the meta section as shown in the following example.

   Example:

   ```
   rule HEX_EXAMPLE
   {
       meta:
           author = "RSA"
           info = "HEX Detection"
          iocName = "Hex Example"
        strings:
           $hex1 = { E2 34 A1 C8 23 FB }
           $wide_string = "Ausov" wide ascii
        condition:
           $hex1 or $wide_string
   }
   ```

4. When ready, place the custom YARA file in the folder that the Malware Analysis service watches:

   `/var/lib/rsamalware/spectrum/yara/watch`

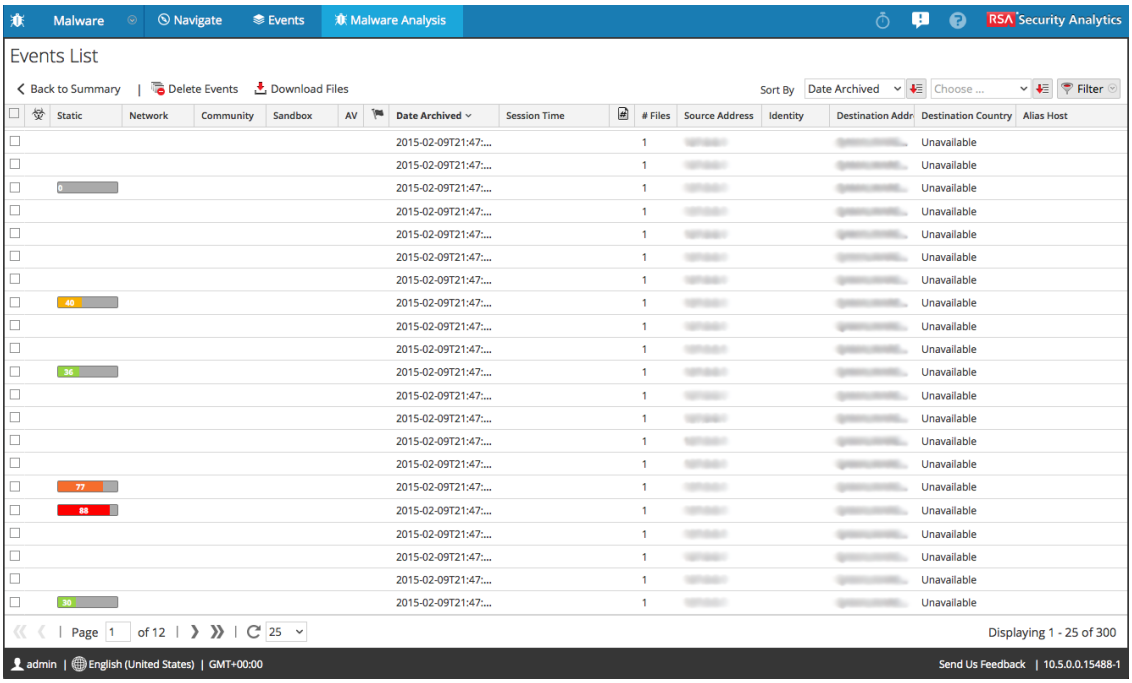
   The file is consumed within one minute.

   Once consumed, Security Analytics moves the file to the `processed` folder, and the new rule is added to the **Malware Analysis Services Config view > Indicators of Compromise tab**.

Examine Scan Files and Events in List Form

This topic provides instructions for viewing files associated with an event in the Security Analytics Malware Analysis Files List.

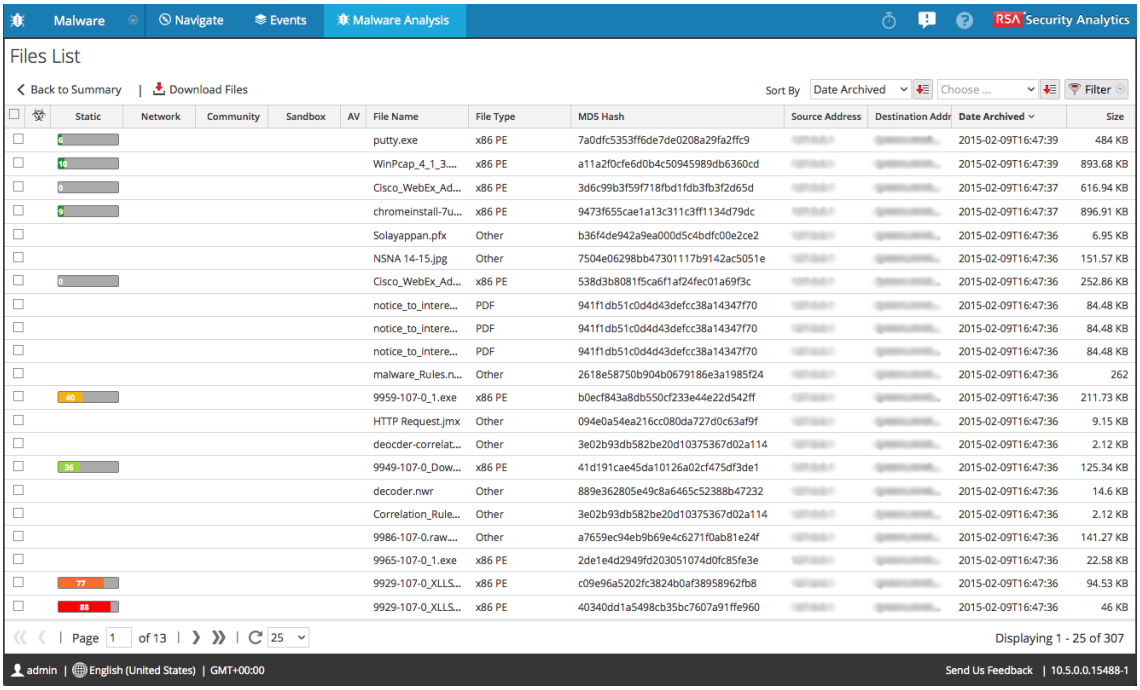
When viewing the Summary of Events in a Security Analytics Malware Analysis scan, you can click a file count or an event count to view the Files List or the Events List for the scan (see Begin a Malware Analysis Investigation). In the Files List and Events List, you can search for a file by filename or MD5 file hash, sort the list using two criteria and ascending or descending order, and download files. When you find an event or file of interest in the Events List or Files List, you can view many details about the event in the Event Details view.



For each event in the Events List, Security Analytics provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.
- Antivirus vendor scores.
- The Influenced by customized rule flag.
- The date the event was archived.
- The session time.
- The MD5 hash filter.

- The number of files in the event.
- The source IP address of the event.
- The Identity.
- The destination IP address.
- The destination country.
- The name of the alias host.
- The event type, for example, Network.
- The service used by the event.
- The destination organization



For each file in the Files List, Security Analytics provides the following information:

- Flagged as a High Confidence event, which is considered likely to contain Indicators of Compromise.
- The numeric score for each scoring module: Static, Network, Community, and Sandbox.
- Antivirus vendor scores.
- The filename.
- The file type.

- The MD5 hash filter.
- The source IP address of the event that contained the file.
- The destination IP address.
- The date the event that contained the file was archived.
- The file size.

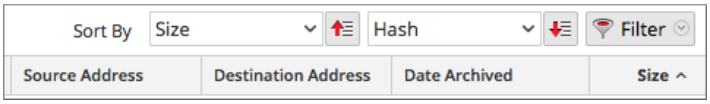
Sort the Files List or Events List

You can sort the Files List and Events List by column name in ascending and descending order. You can choose one or two columns.

To sort the list:

1. In the first **Sort By** drop-down list, choose a column name and sort direction:  for descending order or  for ascending order.
2. (Optional) In the second **Sort By** drop-down list, choose a column name, and sort direction,  for descending order or  for ascending order.

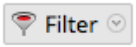
   The column titles reflect the selected sort order. In the following example, the Hash column is sorted in ascending order and the Size column is sorted in descending order.



Filter the List by Filename or MD5 File Hash

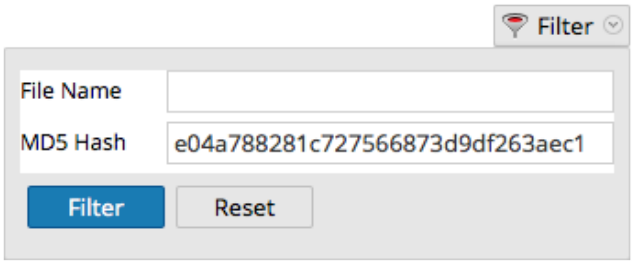
You can filter the Files List and Events List by filename or file hash. With this feature, you can specify a limited subset of the original data based on the search criteria.

Note: When you perform a search, you search the scan that you are currently displaying, not all scans.

1. Click 

.

   The Filter dialog is displayed.
2. Enter a value in **File Name** or **MD5 Hash** and click **Filter**. The File Name and Hash field are not case sensitive. Wild card or regular expressions are not supported. The filter is based on exact matches. You can drag across a filename or hash to select from the Files list or Events list, then copy and paste it in the dialog.



3. Click **Filter**.
   Malware Analysis filters the list to display only files or events with the selected hash
4. To revert to the unfiltered list, click 

. When the Filter dialog is displayed, click **Reset**.

Download Files from the Files List

Security Analytics lets you select and download files from the Files List or the Events List.

Caution: Use caution when downloading files from Malware Analysis; some files may contain harmful code. File Download is a specific permission that can be configured, refer to "Define Roles and Permissions for Malware Analysts" in the *Malware Analysis Configuration Guide* for more details.

To download files from the Files List or Events List:

1. In the **Files List** or **Events List**, select the checkbox next to one or more rows.
2. In the toolbar, select 

.
   The Malware File Download dialog is displayed.
3. Do one of the following:
   a. If you decide not to download the file, click **Cancel**.
   b. If you want to download the file, select click the **Download** button.
      The file or files selected are downloaded in a zip archive with the name `Malware_Files.zip`.

Delete Events from the Scan

In the Events List, you select one or more events and delete them from the scan. This is useful for removing events that are not of interest.

To remove an event from the scan being viewed:

1. In the **Events List**, select one or more events.
2. In the toolbar, click 

.

   Security Analytics asks for confirmation that you want to delete the events.
3. In the confirmation dialog, click **Yes**.

   The selected events are deleted.

Return to the Summary of Events

To leave the Files List or Events List and return to the Summary of Events, click **Back to Summary**.

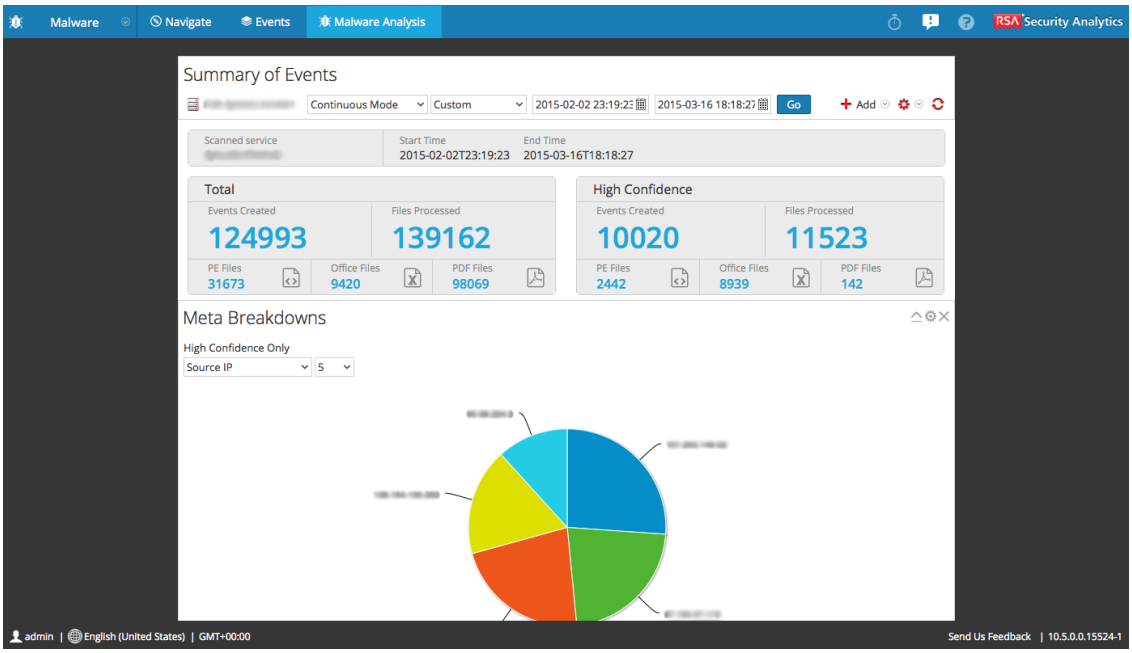
Open the Detailed Analysis for an Event

While you examine events or files in the Files List or Events List, you can double-click any event or file to open a detailed analysis of the event in the Events List or the event with which the file in the Files List is associated (see View Detailed Malware Analysis of an Event).

Filter Dashlet Data in the Summary of Events View

This topic provides instructions for analysts to filter data in the dashlets viewed in the Security Analytics Malware view Summary of Events.

The Summary of Events provides a summary of the scan being investigated with selectable dashlets. The Summary of Events is fixed, but Analysts can configure each dashlet to filter out information and drill into the data.



The rest of this topic provides instructions for managing and configuring dashlets.

Configure the Score Wheel Dashlet

The Score Wheel is a high-level visualization of analyzed sessions that scored high, medium, or low in each of the scoring categories: Static, Network, Community, and Sandbox. The Score Wheel is a quick way to drill into sessions to review them. Each ring represents a different scoring category so that you can visually compare results by category.

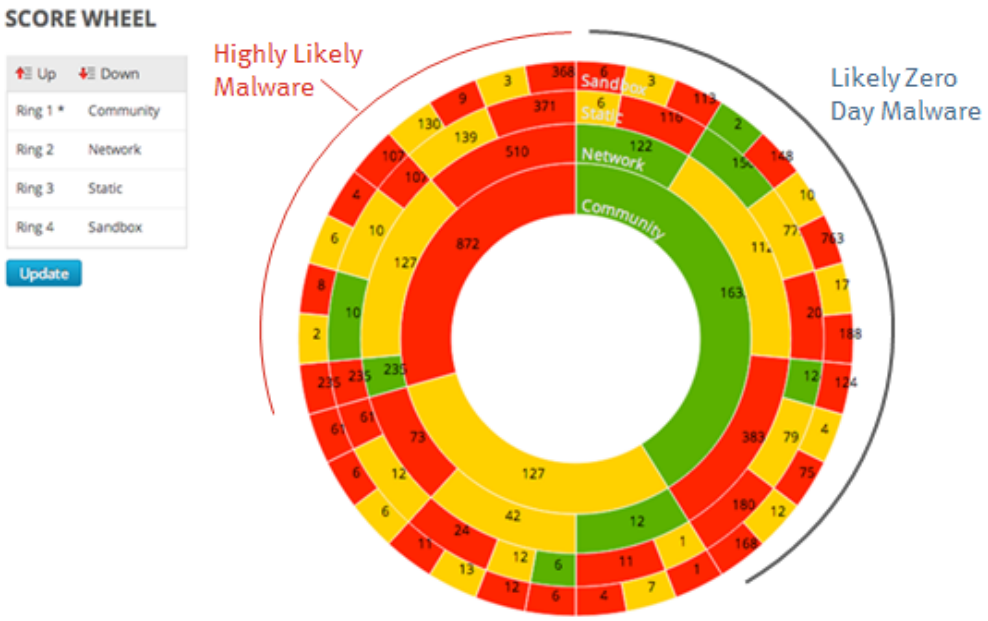
You can change the order of the rings to highlight indicators of compromise that were flagged in one category but not in another category. Comparing the same results in a different sequence of the rings provides visibility into additional vulnerabilities in a session, and you can drill into sessions of interest. The following examples show two possible use cases.

Zero-Day Candidates Example

This example shows how to drill into sessions that the Community did not flag as malicious, but all other scoring categories did. The resulting list of sessions highlights zero-day candidates.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)
2. Click the red slice in the outermost (Sandbox) ring that aligns with a green slice on the innermost ring (Community): green (innermost) -> **Static**: red -> **Network**: red -> **Sandbox**:

red (outermost).



Malicious Sessions Example

This example shows how to drill into sessions in which all scoring categories identify the resulting list of sessions as malicious, indicating Malware Analysis has the most confidence that they are malware.

1. Configure the Score Wheel rings in the following sequence:
   Community (innermost) > **Static** > **Network** > **Sandbox** (outermost)
2. Click the red slice of the outermost (Sandbox) ring that aligns within a red slice on the innermost ring (Community): red (innermost) -> Static: red -> Network: red -> Sandbox: red (outermost).

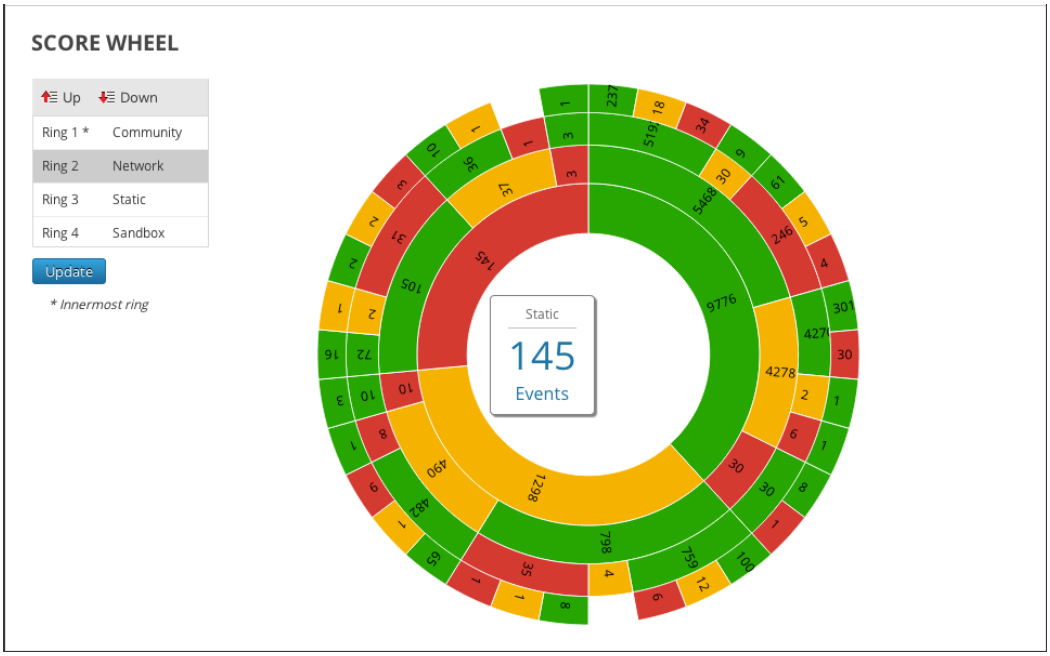
Arrange the Ring Sequence by Scoring Module

In the Score Wheel, you can arrange the sequence of the rings by scoring module. Initially, the sequence of rings from inside to outside is Static, Network, Community, and Sandbox.

To change the ring sequence:

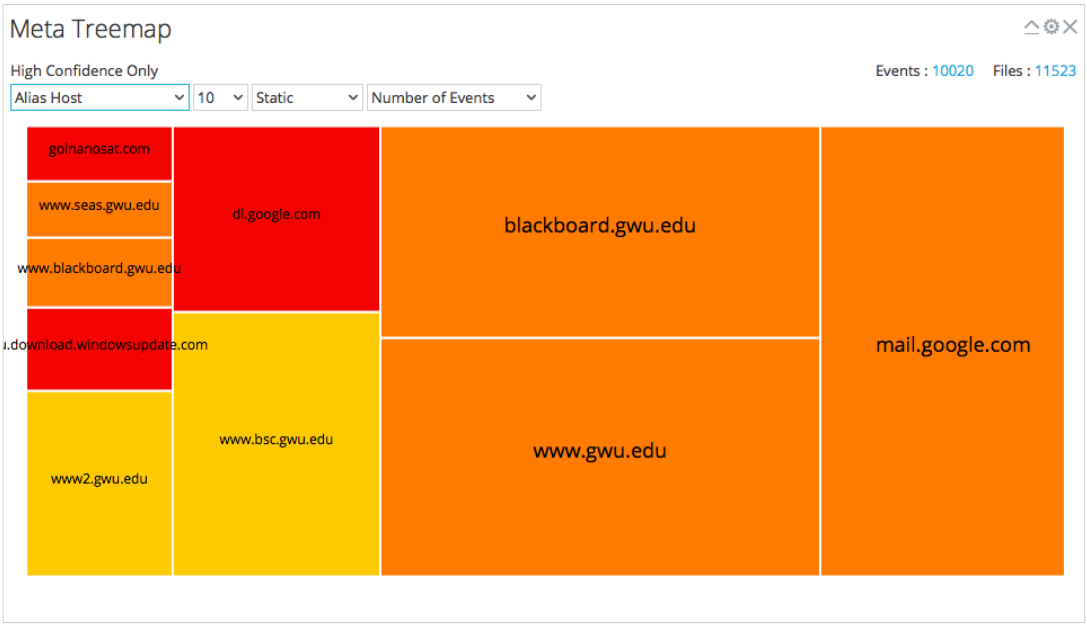
1. Do one of the following:
   a. Click and drag each scoring module up or down.
   b. Select each scoring module and use the Up and Down buttons to move it.

2. When the ring sequence is the way you want it, click the **Update** button.
   The Score Wheel is refreshed with the new sequence.



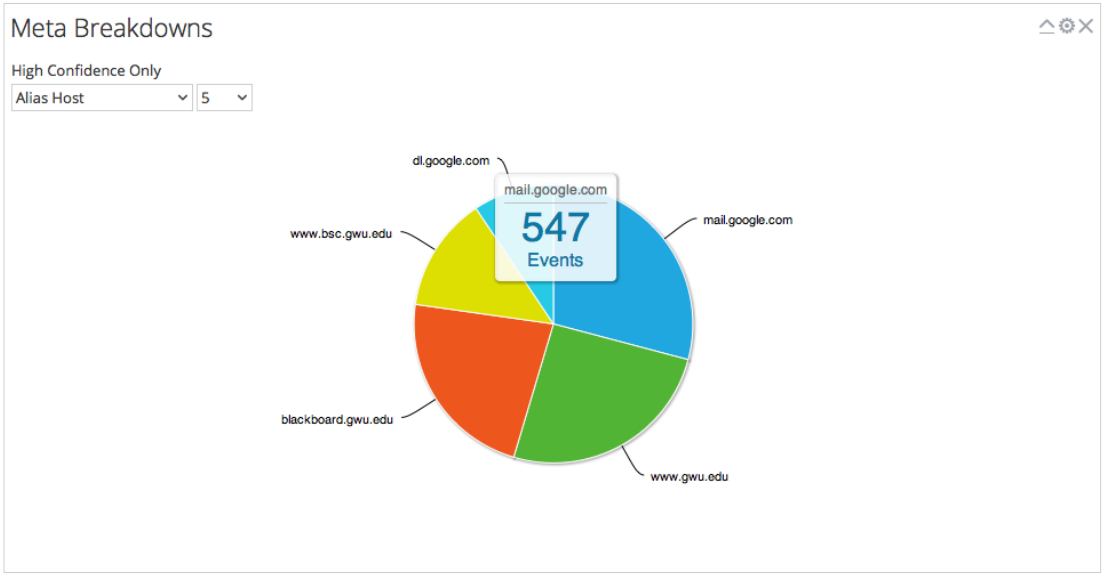
Configure the Meta Treemap Dashlet

In the Meta Treemap chart, you can visualize and filter meta breakdowns by meta type, count, and analysis type. Use the three selection lists to set the filter, and the Meta Treemap chart is refreshed immediately.



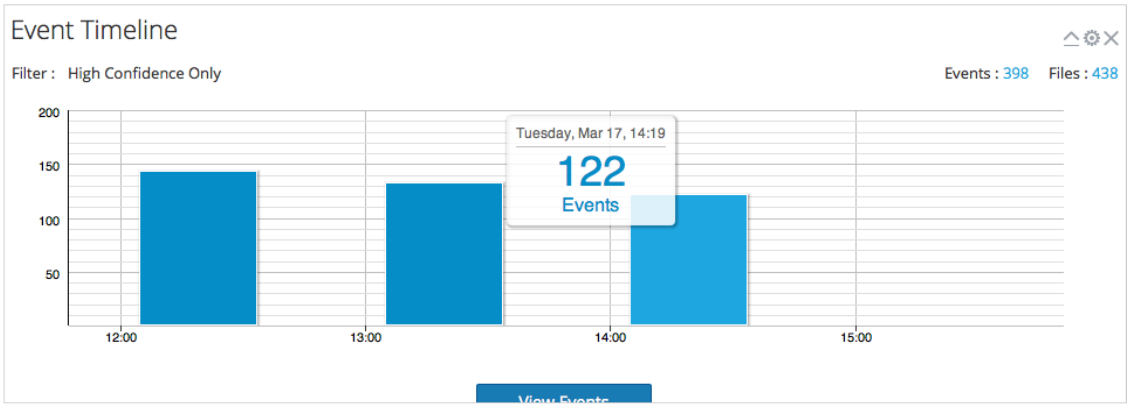
Configure the Meta Breakdowns Dashlet

The Meta Breakdowns dashlet is a visualization of values for a specific meta key in a pie chart. In the Meta Breakdowns chart, you can filter meta breakdowns by meta type and count. Use the two selection lists to set the filter, and the Meta Breakdowns chart is refreshed immediately.



Configure the Events Timeline Dashlet

The Events Timeline dashlet is a visualization of the events along a timeline. No additional filters are available for the Event Timeline.

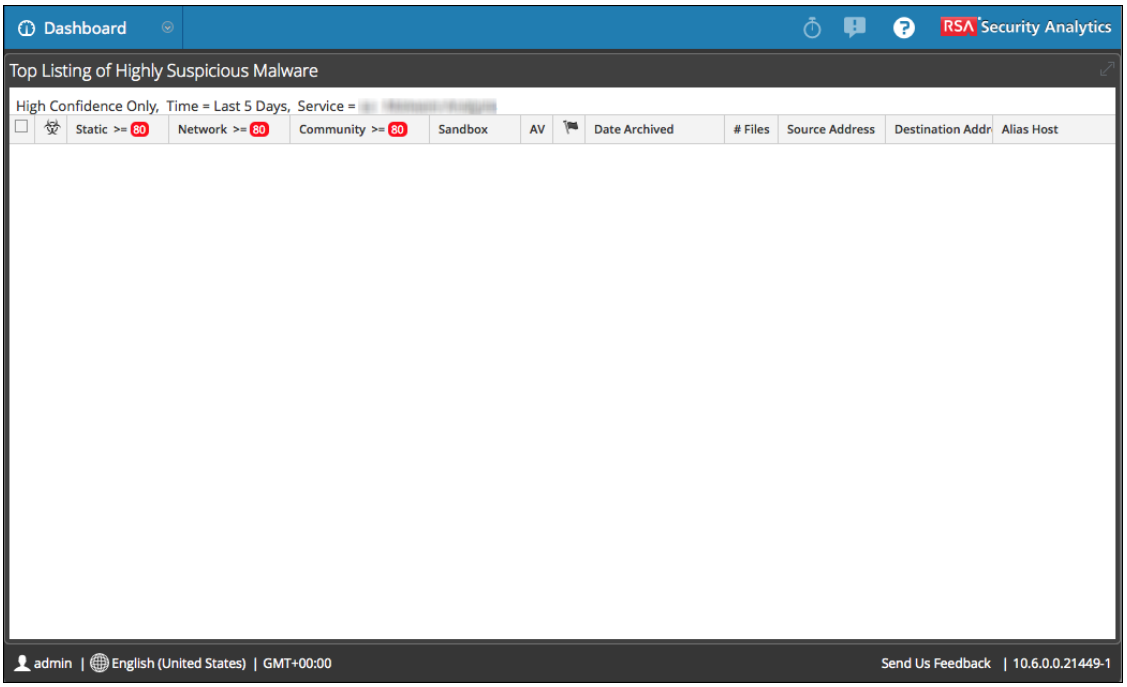


Open All Events in the Events List

From within the Event Timeline, you can open the entire list of events in the Events List. To do so, click View Events. This option is not the same as clicking the count next to Events, which is the same for all visualization charts and opens the current drill point in the Events List.

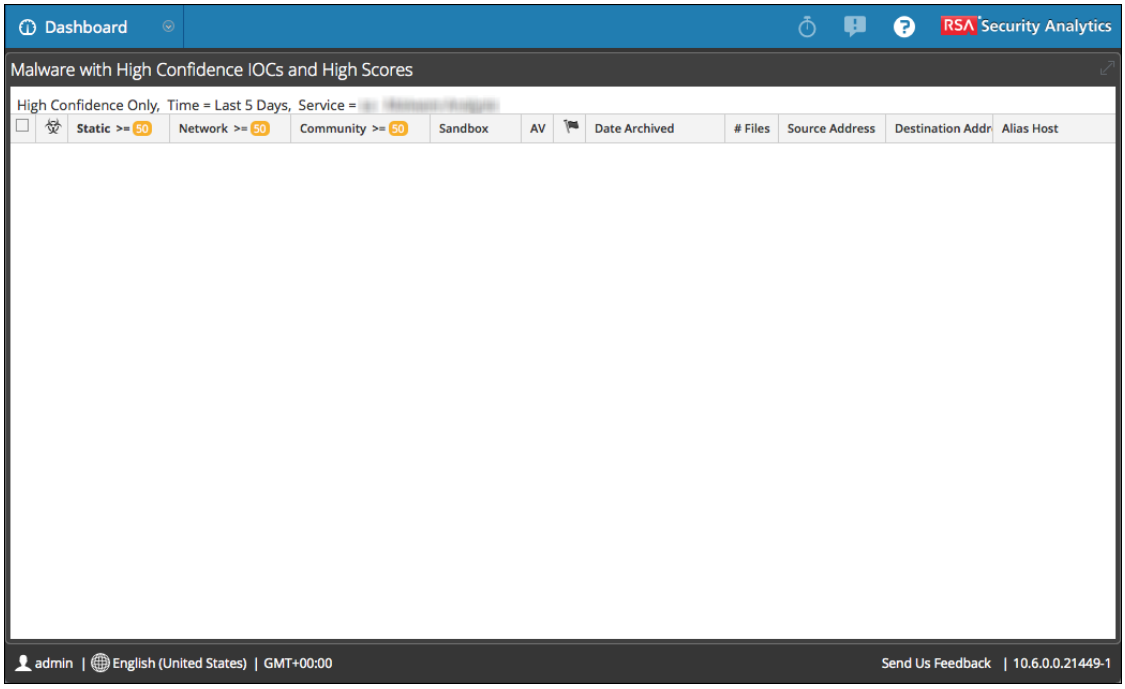
Configure the Top Listing of Highly Suspicious Malware Dashlet

The Top Listing of Highly Suspicious Malware Dashlet presents the Top 10 most suspicious events in the Events List or the Files List. This dashlet is also available in the Unified dashboard, and the configuration options are described in the *Getting Started with Security Analytics Guide*.



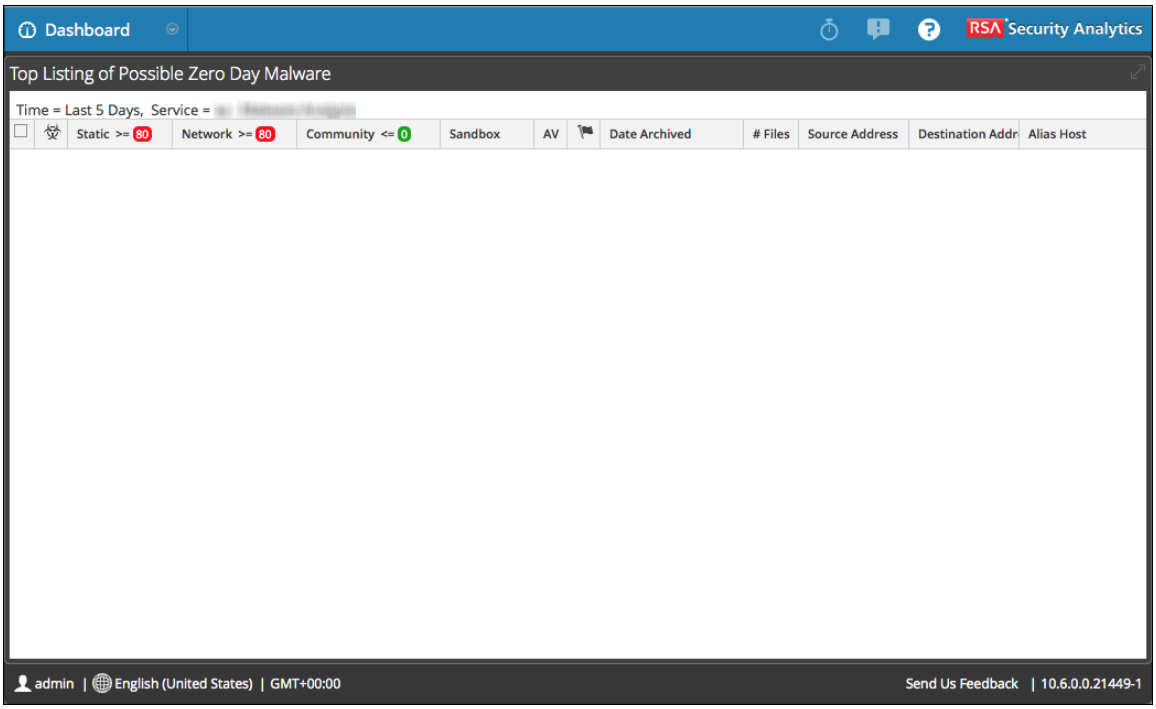
Configure the Malware with High Confidence IOCs and High Scores Dashlet

The Malware with High Confidence IOCs and High Scores dashlet presents Indicators of Compromise that have both high scores and high confidence that the events are likely to contain malware. The dashlet is also available in the Unified dashboard, and the configuration options are described in Malware with High Confidence IOCs and High Scores Dashlet in the *Getting Started with Security Analytics Guide*.



Configure the Top Listing of Possible Zero Day Malware Dashlet

The Top Listing of Possible Zero Day Malware dashlet presents potential zero day events in the Events List or the Files List. The dashlet is also available in the Unified dashboard, and the configuration options are described in the *Getting Started with Security Analytics Guide*.


Dashboard
RSA Security Analytics
Top Listing of Possible Zero Day Malware
Time = Last 5 Days, Service =
Static >= 80
Network >= 80
Community <= 0
Sandbox
AV
Date Archived
Files
Source Address
Destination Addr
Alias Host
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21449-1

Upload Files for Malware Analysis Scanning

There are two methods for analysts to upload files for Malware Analysis scanning.

A Malware Analyst with permission to **Initiate Malware Analysis Scan** can upload files to scan using the Scan Files option in the Select a Malware Analysis Service dialog.

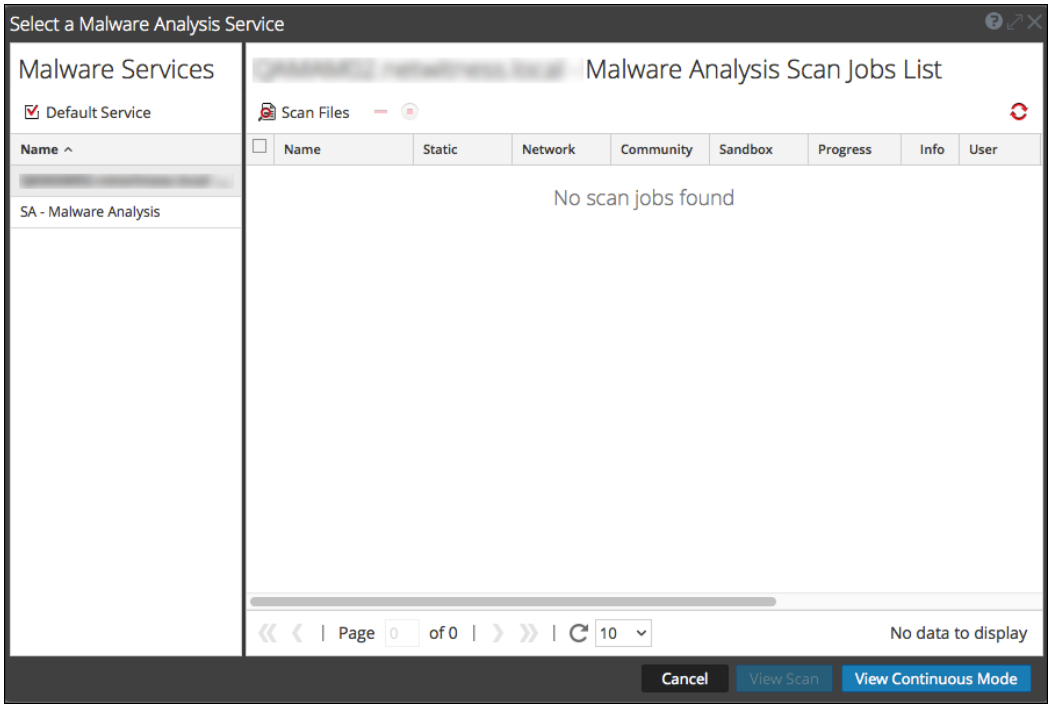
It is also possible to upload a file for scanning using a watched file share.

Upload Files Manually

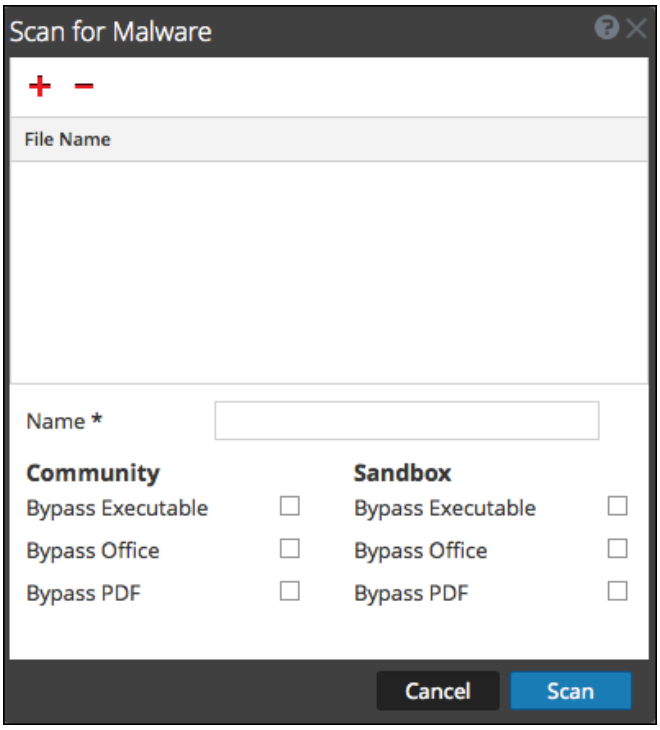
This topic provides instructions for initiating on-demand scanning of an uploaded file. When you upload a file for scanning, Security Analytics starts the upload job and adds it to the jobs queue. When the job is complete, you can view the scan in **Investigation** > **Malware Analysis**.

To upload a file to scan:

1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.
   The Select a Malware Analysis Service dialog is displayed, with available Malware Analysis hosts and services for the current user in the left panel.



2. Click **View Scan**.
   The Scan for Malware dashlet is displayed.



3. Click +

   A view of the files system is displayed so that you can choose files to upload.

   Note: Malware Analysis escape the filename characters before processing a file. The maximum limit of the filename characters after escaping is 200. If the filename character is greater than 200 Malware Analysis truncate the filename characters and displays the truncated filename in the Security Analytics UI.

4. Select one or more files from the list and click **Open**.

   The file names are added.

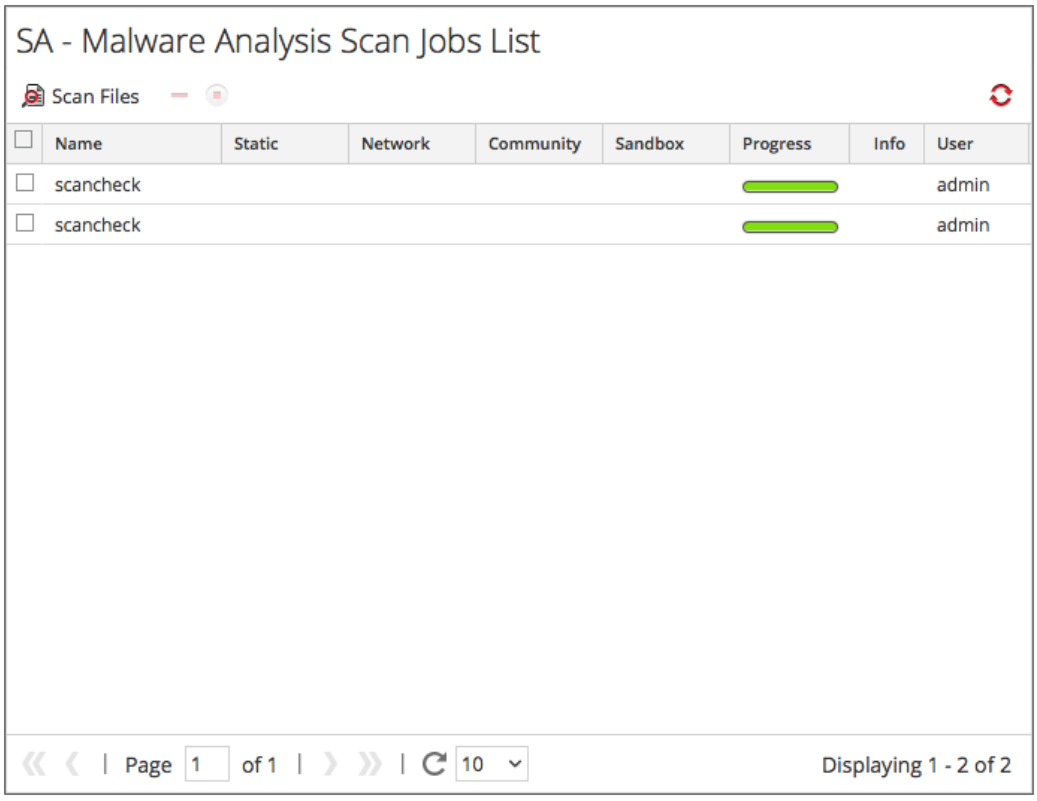
5. Continue adding and deleting files until you have a list of the files that you want to upload.

6. Name the scan and select the types of files to bypass. This is useful for a zip archive that contains different types of files, and overrides the default bypass settings.

7. Click **Scan**.

   The scan job is submitted and Security Analytics displays a confirmation message for successful submission. The scan request is added to the Scan Jobs List dashlet. The bypass settings in this dialog override the default settings in the basic Malware Analysis configuration settings.

8. The job is added to the Scan Jobs List in the Select a Malware Analysis Service dialog and in the Unified dashboard Scan Jobs List dashlet.



9. To view the scan when complete, double-click the scan.

   The Malware Summary of Events for the selected scan is displayed.

Upload Files from a Watched Folder

To upload files from a watched folder, you can drop files into a watched file share for Malware Analysis. Analysts can share YARA rules, hash files, and infected zip archives with Malware Analysis.

Security Analytics Malware Analysis watches a file share and automatically consumes files placed in specific folders in the file share. This feature is useful for:

- Bulk import of hash files from `/var/lib/rsamalware/spectrum/hashWatch`.
- Addition of custom-YARA rules to the Indicators of Compromise (IOC) list on the host from `/var/lib/rsamalware/spectrum/yara/watch`.
- Creation of on-demand scan jobs from a zip archive of infected zip files from `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Analysts need to prepare the files for consumption in accordance with requirements, the file extension must be correct, and the file must be copied to the correct watched folder in the file share.

Import a Hash List

To import a hash list from the watched directory, the hash list must be in the specified format and must be sorted on md5. You can drop a file formatted into a folder (/var/lib/rsamalware/spectrum/hashWatch) on the Malware Analysis host, and it is automatically imported into the local hash database.This is described in "Configure Hash Filter" in the *Malware Analysis Configuration Guide*.

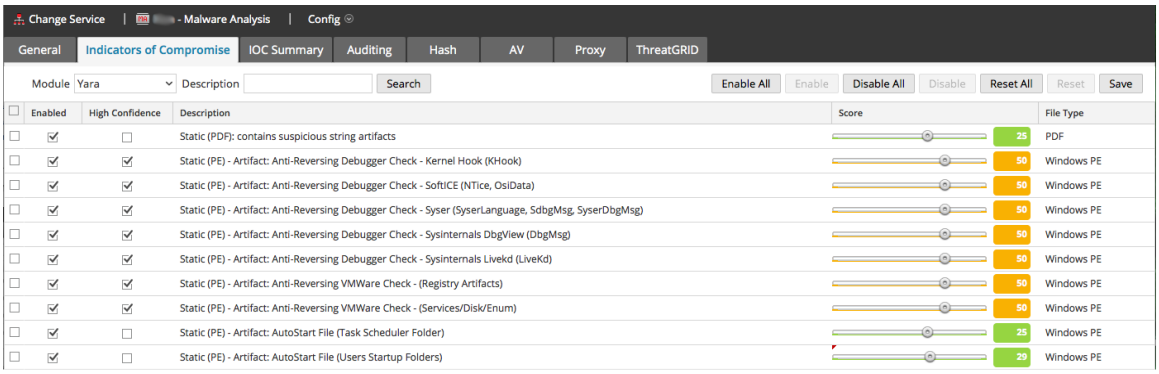
To import a hash list using the watched folder method:

1. Copy the hash lists that you want to import into the **/var/lib/rsamalware/spectrum/hashWatch** directory.
   Security Analytics Malware Analysis automatically watches this folder and processes files placed there.
   a. Security Analytics Malware Analysis adds every hash found in the hash lists to the hash filter.
   b. If there are processing errors, they are logged in: **/var/lib/rsamalware/spectrum/hashWatch/error**
   c. Processed files are cataloged here: **/var/lib/rsamalware/spectrum/hashWatch/processed**
   d. Processed files are not removed from the hashWatch directory.
2. After importing hashes in bulk, the System Administrator can use a cronjob to clean up old processed files.

Import YARA rules to the IOC List

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the host to consume. Implement Custom YARA Contentprovides complete information on the prerequisites for using custom YARA content and authoring rules.

When the rules are ready, place the custom YARA files in the folder that the Malware Analysis service watches:
`/var/lib/rsamalware/spectrum/yara/watch`
The file is consumed within one minute.
Once consumed, Security Analytics moves the file to the `processed` folder, and the new rule is added to the Malware Analysis Service Config view > Indicators of Compromise tab.



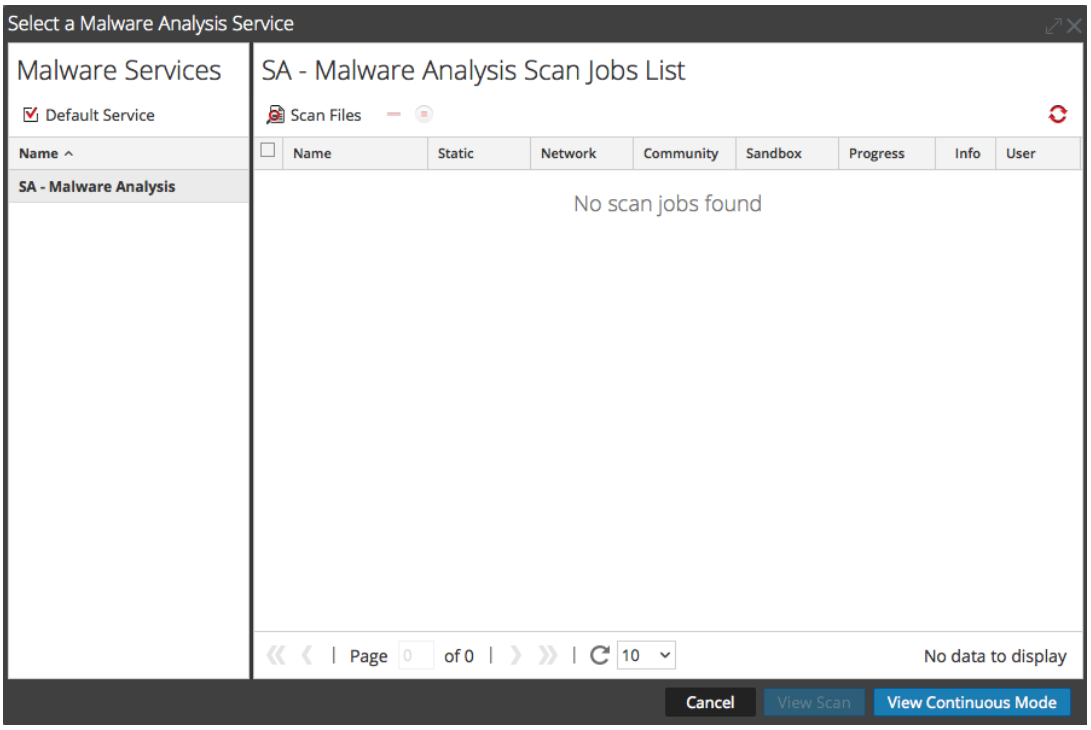
Import Files into the Scan Jobs List

When you obtain samples from perimeter security solutions and would like to perform further analysis on the files, you can zip the files and password protect the archive with `infected`, then add to the watched folder for consumption by Malware Analysis. This zipped archive is ready to be placed in the watched folder: `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Note: The maximum size of the archive is 100 MB.

To analyze infected, password-protected zip files, Malware Analysis consumes archives place in a watched folder and creates an on-demand job that is added to the Scan Jobs List.

1. While logged on as administrator, place the files to be processed in a zip file with password `infected` at `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   In a minute or two Malware Analysis consumes the archive and creates an on-demand job in the Scan Jobs List. The scan job name is the name of the file, the user is **file share**, and the Event Type is 1. The archive is moved to `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`



2. After the job is added to the Scan Job List, run a script or cronjob to clean up the zip file in `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

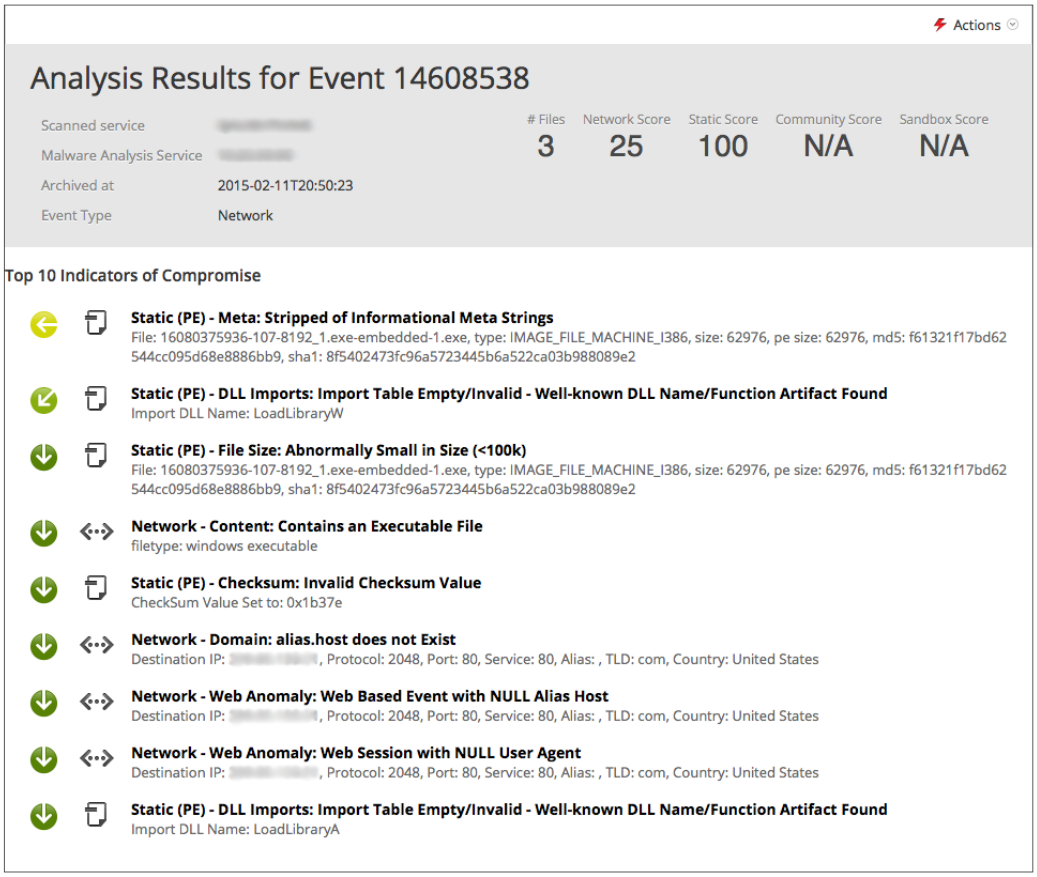
View Detailed Malware Analysis of an Event

This topic provides instructions for viewing details of an event in the Security Analytics Malware Analysis Events grid.

When viewing the list of individual events in a Security Analytics Malware Analysis scan in the Malware Analysis Events grid, you can double-click an event to view the detailed analysis results for the event.

View Malware Analysis Details for an Event

1. Start an investigation in the **Investigation > Malware Analysis** tab.
   The Malware Summary of Events is displayed, and includes four charts, including the Event Timeline.
2. Do one of the following:
   a. To view all events in the Event Timeline, click the **View Events** button. the Viewthe
   b. Double-click data in the **Meta Breakdown**, **Meta Treemap Chart**, or **Score Wheel**.
      The Events List is displayed.
3. Double-click an event.
   The Analysis Results for the event are displayed.



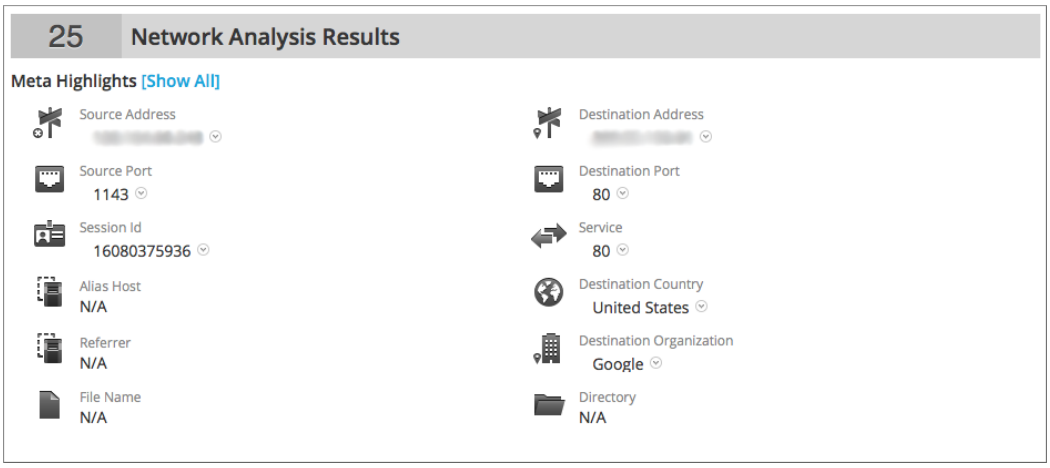
4. (Optional) If you want to delete an event, select **Actions > Delete Event**.
5. If you want to view a reconstruction of the network session, select **Actions > View Network Session**.

   The session opens in the Navigate view > Event Reconstruction.

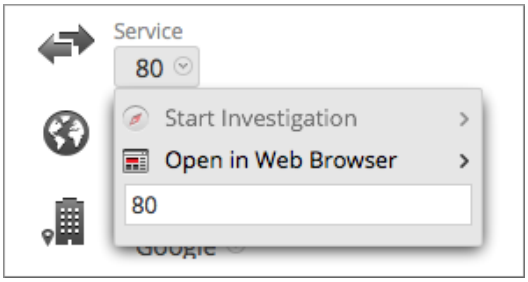
Pivot Network Analysis Results

You can pivot the Network Analysis Results in several ways:

1. Scroll down to the Network Analysis Results.



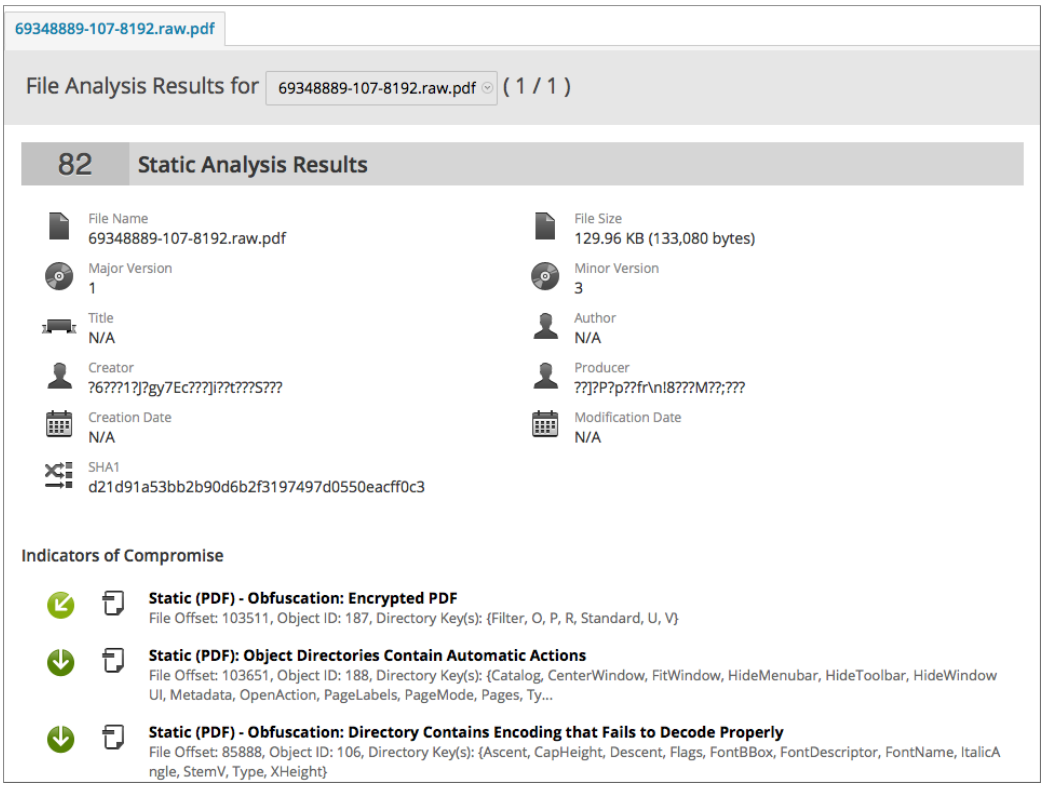
2. Hover over a meta value and left-click.
   The context menu is displayed.



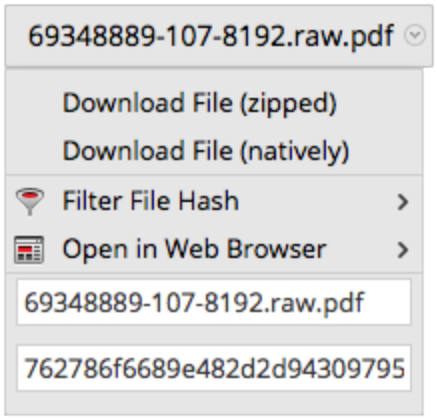
3. To view the selected meta value in the **Navigate** view, select **Start Investigation** and a time option.
4. To view the selected meta value in a browser, select **Open in Web Browser > Open in Google**.

Use File Actions in the Static Analysis Results

1. Scroll down to the Static Analysis Results.



2. If you want to download a file, select the file name and either **Download File (zipped)** or **Download File (natively)** in the drop-down menu. It is safer to download a file in zipped format.



3. If you want to mark the file as safe or unsafe in the hash list, select **Filter File Hash** and **Mark hash as good** or **Mark hash as bad**.

View Community Analysis Results Details

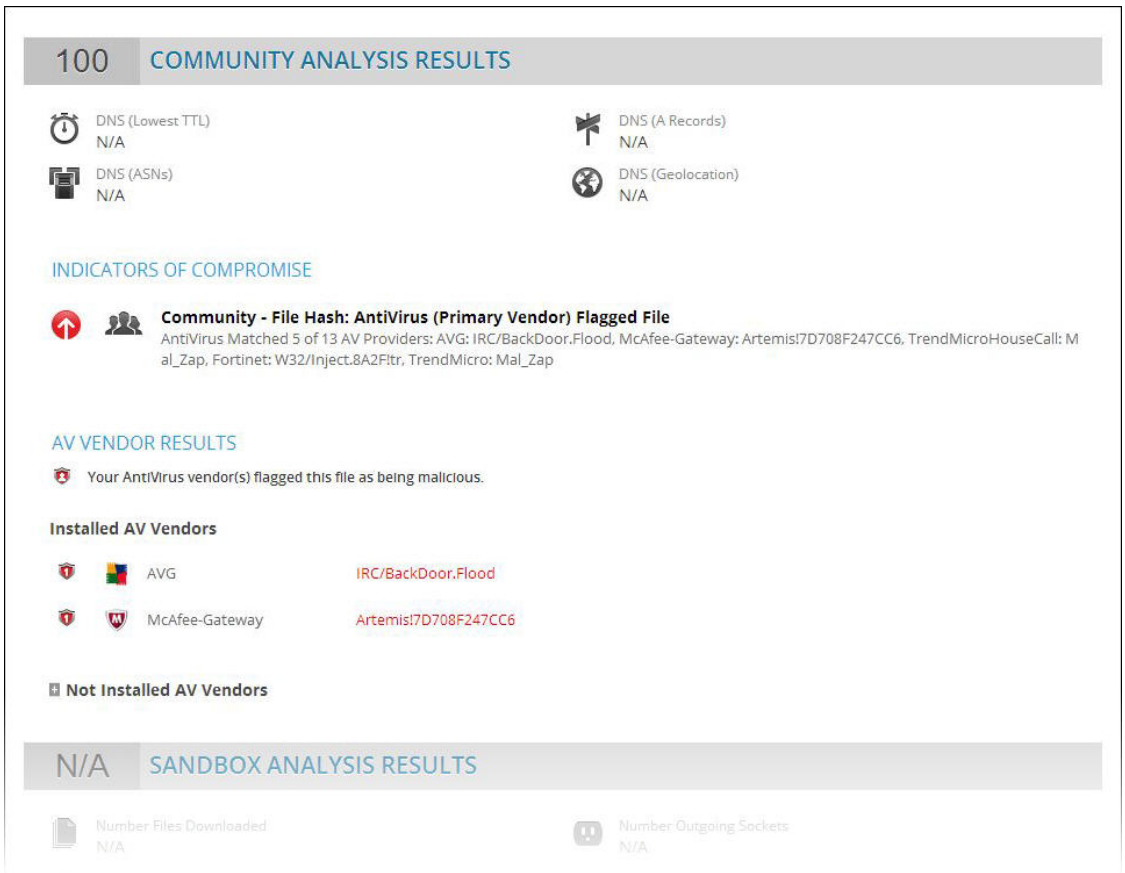
The Community Analysis Results summarizes results from the community, identifying Indicators of Compromise that were flagged as a risk or identified as good.

In addition, this view lists the results from Installed AV Vendors and Not Installed AV Vendors. You can compare results of the installed AV vendors that were configured for the current Malware Analysis service versus Community results. You can also see results from a list of AV vendors that are not configured as installed for the current Malware Analysis service.

Each row of AV vendor results includes the shield icon to show whether the IOC was discovered by a Primary ( ) or Secondary AV ( ) vendor in the community, the name of the Installed or Not Installed vendor, and the name of malware or risk detected by the community and AV vendor. If the AV vendor did not detect a risk, **-- Not detected --** is displayed instead of the name of the risk.

The Not Installed AV Vendors section is expandable to view all entries, but is collapsed by default to minimize the need to scroll. Clicking the + expands the list.

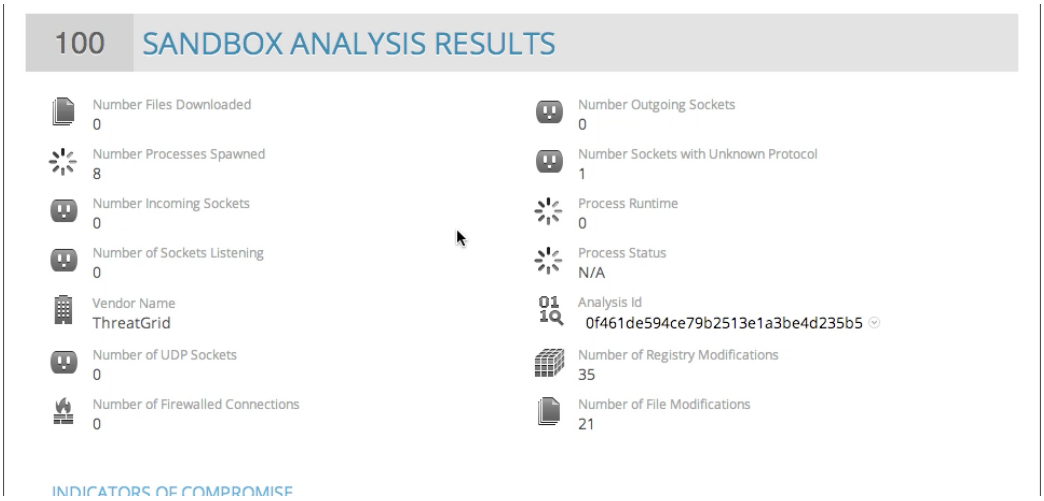
If no installed AV vendors have been configured for the current Malware Analysis service, the following message is displayed: No AV vendors were marked as installed. Please go to the Malware Analysis Service configuration page to identify installed AV vendors.



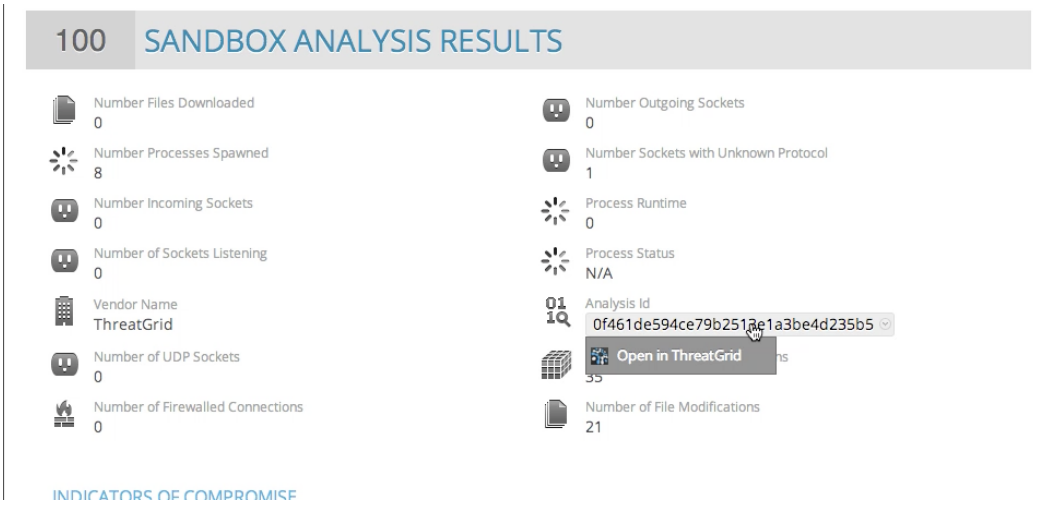
View Sandbox Analysis Results in the ThreatGrid User Interface

If you have registered with ThreatGrid, you can view the Sandbox results directly in ThreatGrid.

1. Scroll down to the Sandbox Analysis Results.

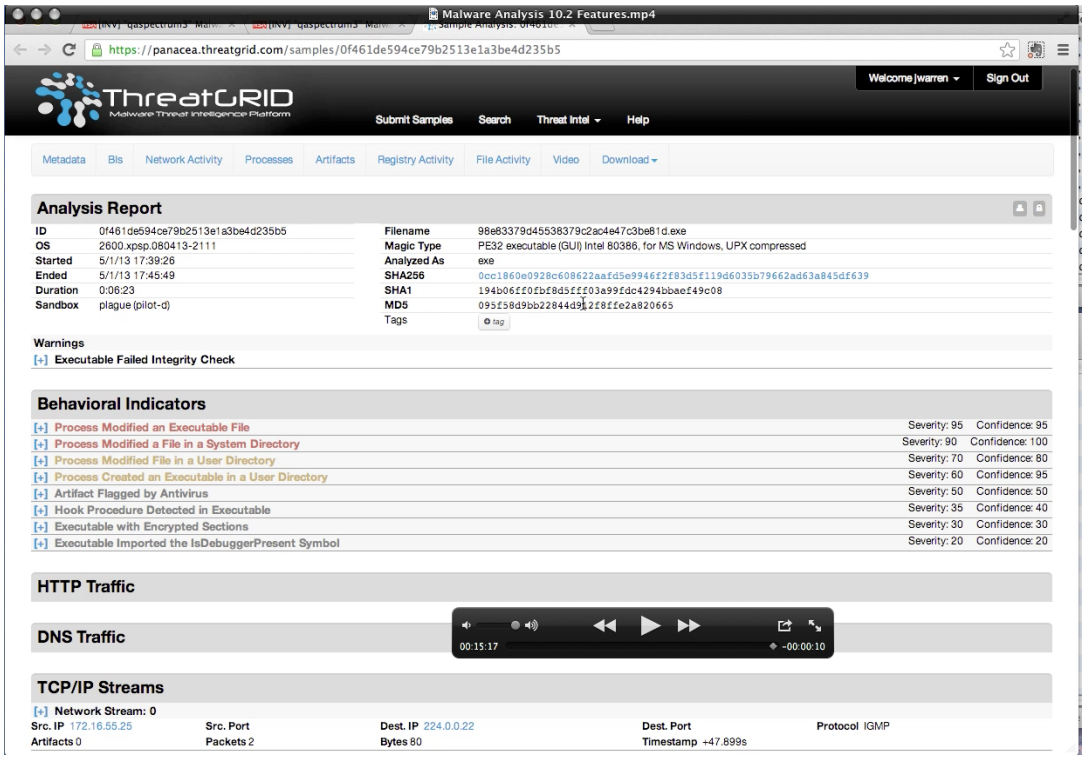


2. Hover over the **Analysis ID**, and right-click.



3. Select **Open In ThreatGrid**.

   The analysis report in ThreatGrid is displayed.


Malware Analysis 10.2 Features.mp4
https://panacea.threatgrid.com/samples/0f461de594ce79b2513e1a3be4d235b5
ThreatGRID
Malware Threat Intelligence Platform
Welcome jwarren
Sign Out
Submit Samples
Search
Threat Intel
Help
Metadata
Bls
Network Activity
Processes
Artifacts
Registry Activity
File Activity
Video
Download
Analysis Report
ID 0f461de594ce79b2513e1a3be4d235b5
OS 2600.xpsp.080413-2111
Started 5/1/13 17:39:26
Ended 5/1/13 17:45:49
Duration 0:06:23
Sandbox plague (pilot-d)
Filename 98e83379d45538379c2ac4e47c3be81d.exe
Magic Type PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Analyzed As exe
SHA256 0cc1860e0928c608622aafd5e9946f2f83d5f119d6035b79662ad63a845df639
SHA1 194b06ff0fbf8d5fff03a99fdc4294bbaef49c08
MD5 095f58d9bb22844d912f8ffe2a820665
Tags
tag
Warnings
[+] Executable Failed Integrity Check
Behavioral Indicators
[+] Process Modified an Executable File Severity: 95 Confidence: 95
[+] Process Modified a File in a System Directory Severity: 90 Confidence: 100
[+] Process Modified File in a User Directory Severity: 70 Confidence: 80
[+] Process Created an Executable in a User Directory Severity: 60 Confidence: 95
[+] Artifact Flagged by Antivirus Severity: 50 Confidence: 50
[+] Hook Procedure Detected in Executable Severity: 35 Confidence: 40
[+] Executable with Encrypted Sections Severity: 30 Confidence: 30
[+] Executable Imported the IsDebuggerPresent Symbol Severity: 20 Confidence: 20
HTTP Traffic
DNS Traffic
00:15:17
-00:00:10
TCP/IP Streams
[+] Network Stream: 0
Src. IP 172.16.55.25
Src. Port
Dest. IP 224.0.0.22
Dest. Port
Protocol IGMP
Artifacts 0
Packets 2
Bytes 80
Timestamp +47.899s

Investigation Reference Materials

Security Analytics offers several views into data when conducting an investigation. This section provides details on the user interface tools and options in Security Analytics Investigation.

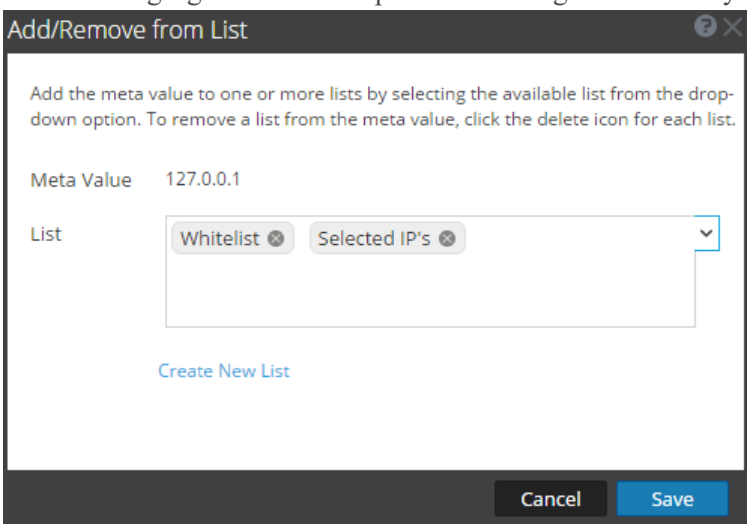
Investigation - Add/Remove from List Dialog

In the Investigation > Navigate view or Events view, you can add meta values to an existing list or create a list using the option Add/Remove from List . Related procedures are available in Manage Context Hub Lists and List Values in Investigation.

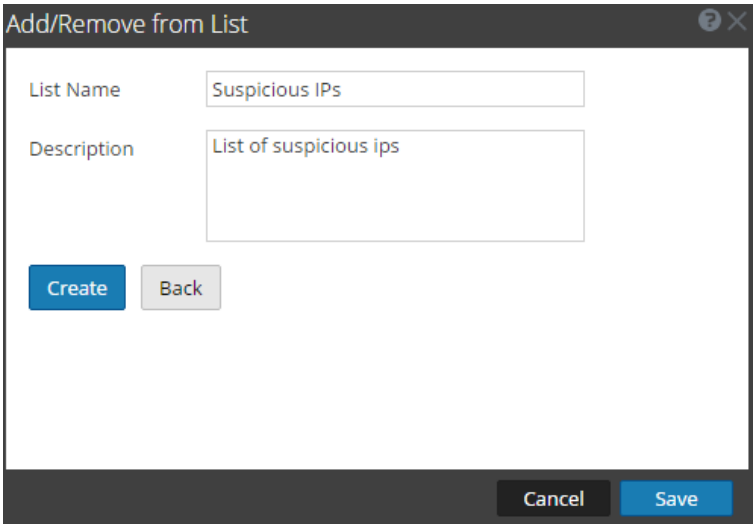
To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**. Both views provide access to the Add/Remove from List dialog.
2. Right-click a meta value (for example, values underSource IP, Destination IP, or Username) and select **Add/Remove from List** in the context menu.

The following figure is an example of the dialog when initially opened.



The following figure shows the dialog when you select Create New List.



Features

The following table describes the features of Add/Remove from List and Create New List dialogs.

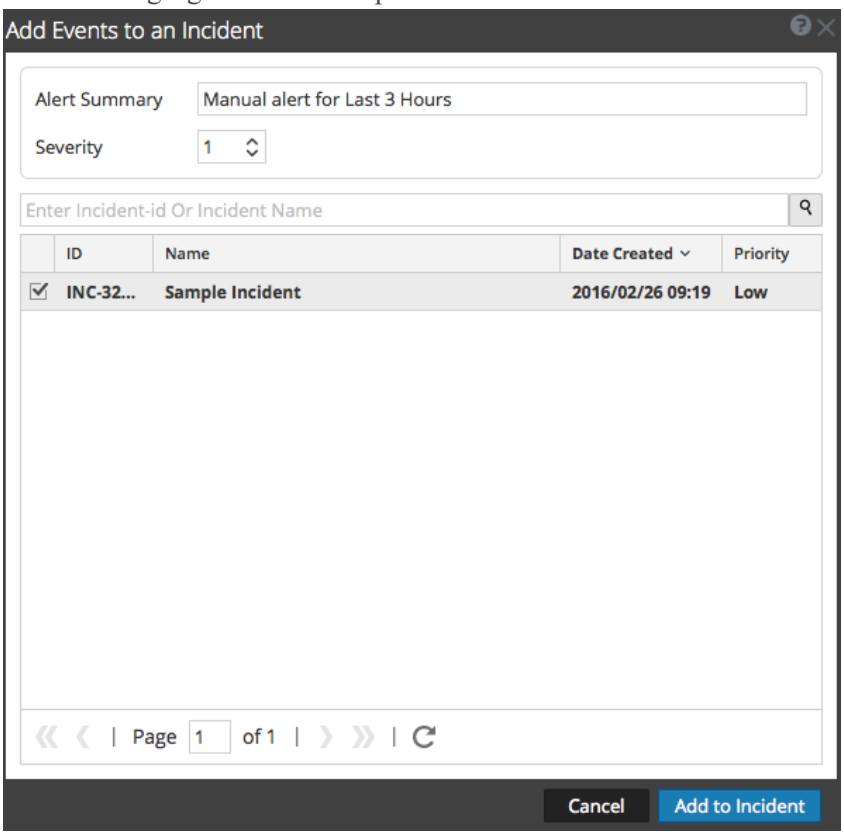
Feature	Description
Meta Value	The selected meta value to be added to the existing or new list.
List	The list to which the selected meta value must be added. A drop-down menu provides a list of available lists to which you can add the meta value.
Create New List	Opens a new dialog in which you can create a new list for the selected meta value.
List Name	The name of the new list.
Description	The description of the new list.
Create	Create a new list after entering the required fields.
Back	In the new list mode, cancels the new list creation and returns to the original dialog.
Cancel	Cancels the addition of the meta value to a list and closes the dialog.
Save	Saves the changes made to the lists and closes the dialog.

Investigation - Add Events to an Incident Dialog

In the Add Events to an Incident dialog, analysts can add alerts to an existing incident so that incident responders look at the associated events as part of an incident response. Related procedures are available in Manage Context Hub Lists and List Values in Investigation.

To access this dialog, while investigating a service in the Investigation > Events view, select **Incidents > Add to Existing Incident** from the toolbar.

The following figure is an example of the Add Events to an Incident dialog.



Features

The Add Alerts to an Incident dialog has features shown in the table below.

Feature	Description
Alert Summary	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.

Feature	Description
Search	Allows you to search for an existing event.
ID	The ID of the incident. You can sort IDs in ascending or descending order.
Name	The incident name. You can sort the Name in ascending or descending order.
Date Created	Displays the date and time the incident was created. You can sort the dates in ascending or descending order.
Priority	Displays the priority of the incident: either low or critical.
Cancel	Closes the dialog without saving changes.
Add to Incident	Adds the alerts to the incident. A dialog confirms that alerts are successfully added

Investigation - Context Lookup Panel

After you configure the Context Hub service, you can view the Context Lookup panel in the Navigate view and Events view of the Investigation module. For the first time when you view this panel, it displays the instructions for performing the Context Lookup. Later on, this panel gets minimized and can be expanded if required.

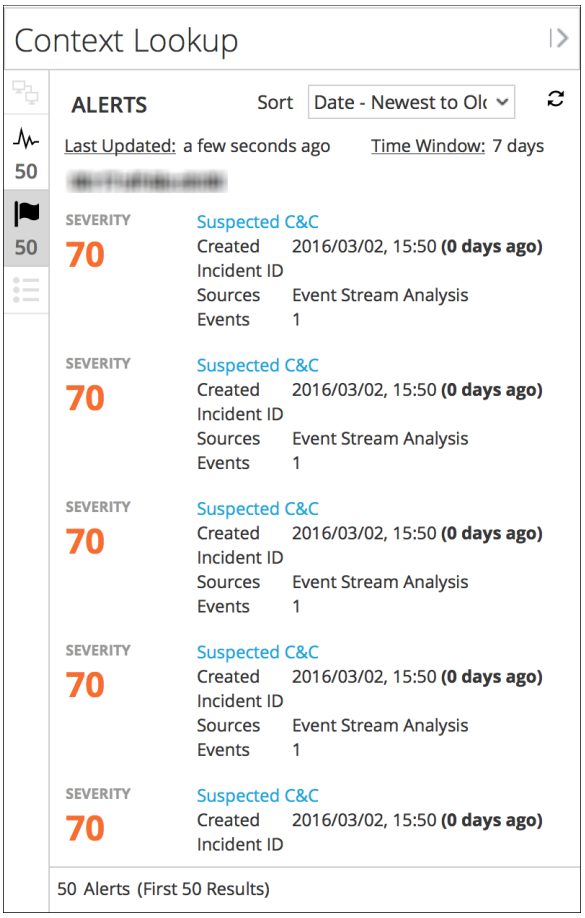
The Context Lookup panel does not display any data until you perform a Context Lookup on a meta value. Meta values that have associated context information are highlighted with a gray color background. The lookup results are displayed in the Context Lookup panel for different configured sources for the selected meta value. Procedures related to this panel are described in View Additional Context for a Data Point.

To access this panel:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**.
2. Right-click a meta value and select **Context Lookup** in the context menu.

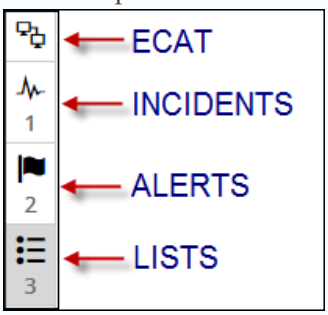
   The Context Lookup panel displays the contextual information.
3. From the Icon bar, select the source for which you want to view the contextual information by clicking the corresponding icon.

The following figure is an example of the Lookup panel.



Features

The Context Lookup Panel has the following controls and features:

Feature	Description
Source Options Bar 	Displays the icons for the available sources: ECAT, Incidents, Alerts, and Lists.

Feature	Description
Source Name	Displays the source name based on the selected icon: • ECAT • INCIDENTS • ALERTS • LISTS
Sort	Provides a drop-down of sort options for the listed context information. Possible sort options are Severity - High to Low, Severity Low to High, Date - Oldest to Newest. and Date - Newest to Oldest. The sorting options vary by source type.
	Refreshes the lookup results.
n items (First n Results)	The footer provides a count of the total number of results, and the count of results currently displayed. For example, 50 Alerts (First 50 Alerts).

Lookup Results

The Context Lookup panel displays the following information when retrieving the context data from different configured sources:

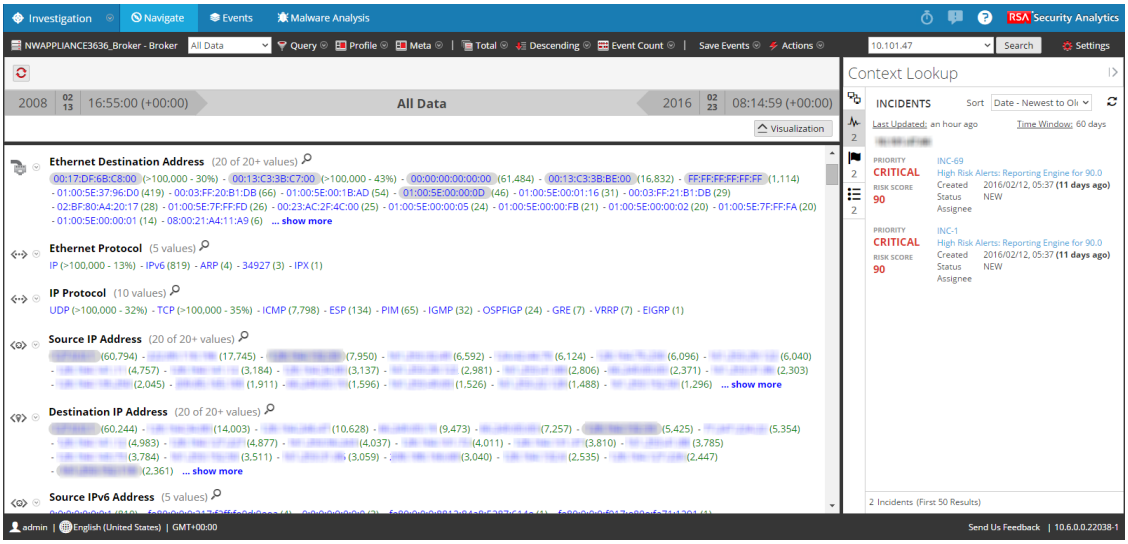
Incidents

Incidents are displayed based on time first (Newest to Oldest) and then priority status. The following information is displayed for incident lookups:

- Incident Name and ID
- Priority status of the incidents
- Risk Score value of the incidents
- Date when the incident was created
- Status of the incident
- Assignee for the incident

- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last" field in the **Configure Incident Management Responses** window. For details, see the **Configure Incident Management Responses** topic in the *Context Hub Configuration Guide*.
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

The following figure is an example of lookup results for Incidents.



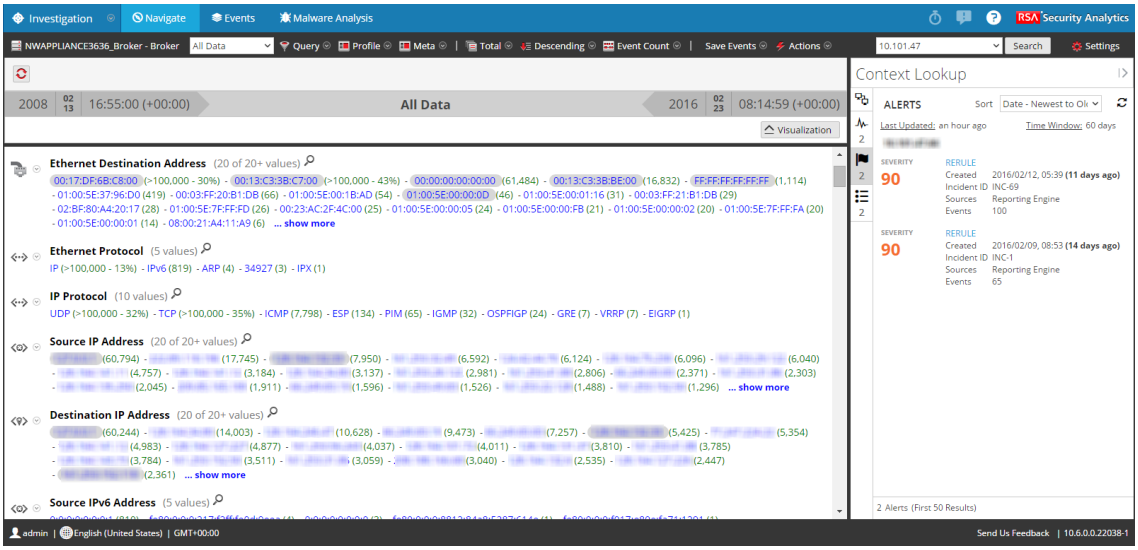
Alerts

Alerts are displayed based on the Severity. ;The following information is displayed for alert lookups:

- Alert Name
- Severity value of the alerts
- Date when the alert was created
- Incident ID: This is the ID of the incident that the alert is associated with (If any).
- Sources: Event source name
- Number of events associated with the alert.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.

- Time window: This is based on the value that is set for the "Query Last" field in the Configure Incident Management Responses window, which is described in the *Context Hub Configuration Guide*.
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

The following figure is an example of lookup results for Alerts.

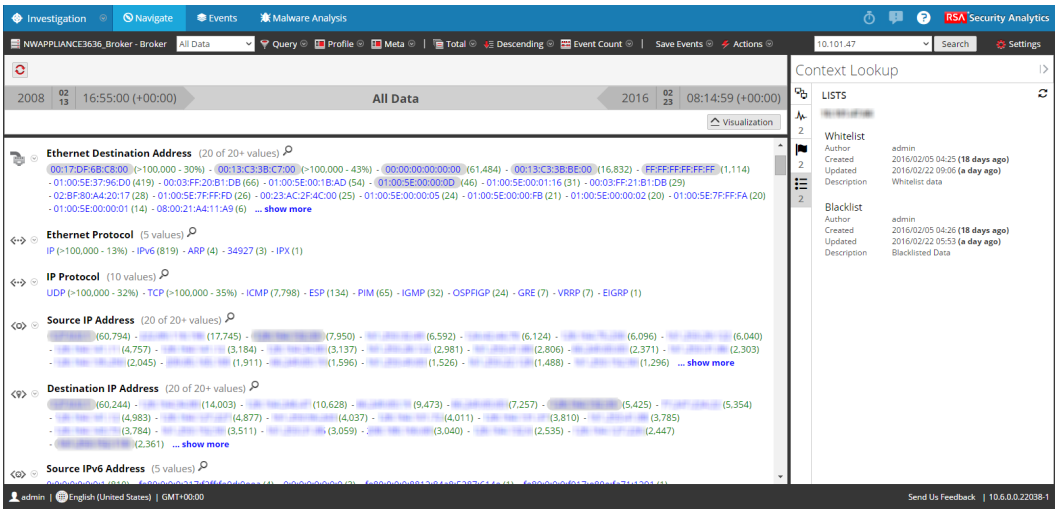


Lists

The following information is displayed for list lookups.

- List Name
- Owner who created the list
- Created Date
- Last Updated Date
- Description of the list

The following figure is an example of lookup results for Lists data source.

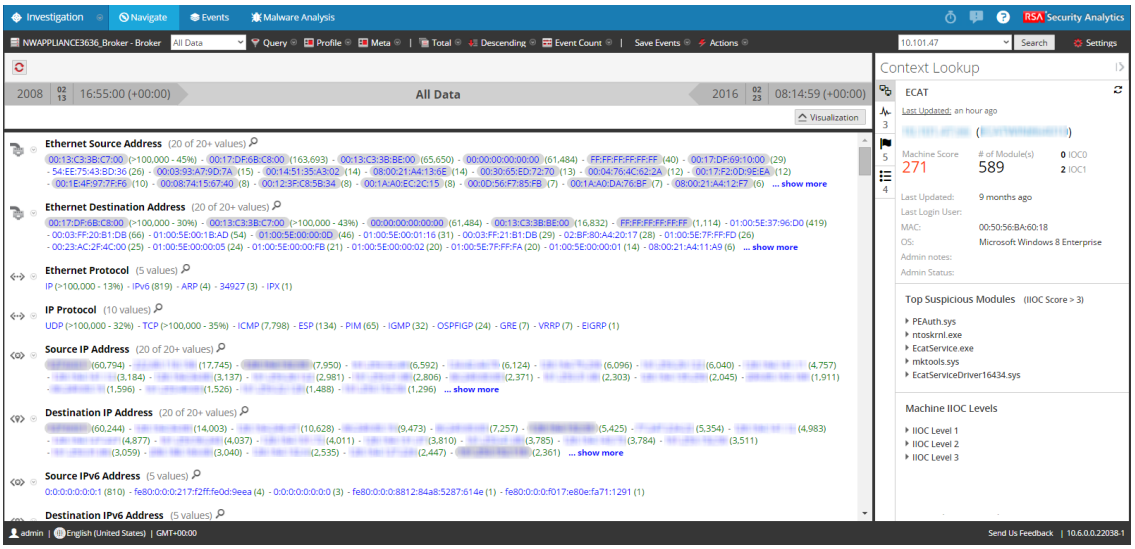


ECAT

The following information is displayed for ECAT lookups.

- Machine name and IP address of the machine.
  By clicking on the IP or ECAT machine name, you will be navigated to ECAT UI to perform further investigation.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Machine Score: A machine IIOC score is aggregated based on the module scores.
- Number of modules: Number of active files for the selected machine.
- Last Updated: Indicates when the scan results were last updated in ECAT database.
- Last Login User
- Machine MAC Address
- Operating System Version
- Admin Notes (if any)
- Admin Status (if any)
- Top Suspicious Modules (Modules that has IIOC score > 500). This is based on the value set for "Minimum IIOC Score" field in the Configure Incident Management Responses window. The default value for "Minimum IIOC Score" is 500.
- Machine IIOC Levels

The following figure is an example of lookup results for ECAT data source.

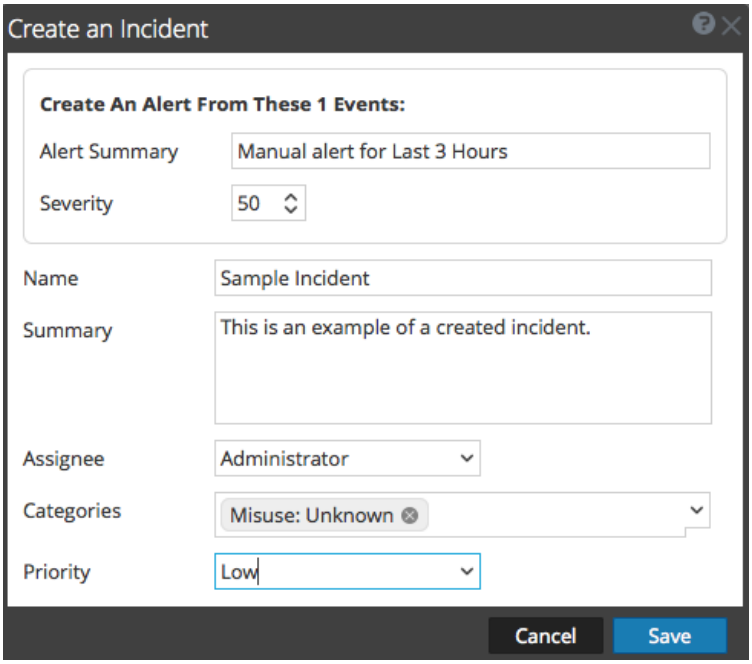

Investigation
Navigate
Events
Malware Analysis
RSA Security Analytics
NWAPPLIANCE3636_Broker - Broker
All Data
Query
Profile
Meta
Total
Descending
Event Count
Save Events
Actions
10.101.47
Search
Settings
2008
16:55:00 (+00:00)
All Data
2016
08:14:59 (+00:00)
Visualization
Ethernet Source Address (20 of 20+ values)
Ethernet Destination Address (20 of 20+ values)
Ethernet Protocol (5 values)
IP (>100,000 - 13%) - IPv6 (819) - ARP (4) - 34927 (3) - IPX (1)
IP Protocol (10 values)
UDP (>100,000 - 32%) - TCP (>100,000 - 35%) - ICMP (7,798) - ESP (134) - PIM (65) - IGMP (32) - OSPFIGP (24) - GRE (7) - VRRP (7) - EIGRP (1)
Source IP Address (20 of 20+ values)
Destination IP Address (20 of 20+ values)
Source IPv6 Address (5 values)
0:0:0:0:0:0:0:1 (810) - fe80:0:0:0:217:f2ff:fe0d:9eea (4) - 0:0:0:0:0:0:0:0 (3) - fe80:0:0:0:8812:84a8:5287:614e (1) - fe80:0:0:0:f017:e80e:fa71:1291 (1)
Destination IPv6 Address (5 values)
admin
English (United States)
GMT+00:00
Send Us Feedback
10.6.0.0.22038-1
Context Lookup
ECAT
Last Updated: an hour ago
Machine Score
271
# of Module(s)
589
0 IOC0
2 IOC1
Last Updated:
9 months ago
Last Login User:
MAC:
00:50:56:BA:60:18
OS:
Microsoft Windows 8 Enterprise
Admin notes:
Admin Status:
Top Suspicious Modules (IIOC Score > 3)
PEAuth.sys
ntoskrnl.exe
EcatService.exe
mktools.sys
EcatServiceDriver16434.sys
Machine IIOC Levels
IIOC Level 1
IIOC Level 2
IIOC Level 3

Investigation - Create an Incident Dialog

In the Create an Incident dialog, analysts can create an incident from selected events in the Events view. When creating the incident, analysts can identify the incident category and priority, and can assign handling of the incident to an SOC analyst.

To access this dialog, while investigating a service in the Investigation > Events view, select **Incidents > Create New Incident** from the toolbar.

The following figure is an example of the Create an Incident Dialog.



Features

The Create an Incident dialog has the features shown in the table below.

Feature	Description
Create Summary from These Events	The Alert Summary field is filled by the query that produced the select alerts, which you selected to create this incident. The Severity field reflects the Severity of the selected alert, an integer between 1 and 100.

Feature	Description
Name	(Required) Specifies a name to identify the incident. In the example, the name is Sample Incident. You can provide a name that clearly identifies the nature of events that will be added to this incident
Summary	(Optional) Specifies a description for the incident. A good summary clearly identifies the incident for other analysts and responders.
Assignee	(Optional) Assigns the incident to a user in the SOC. Clicking Assignee opens a drop-down list showing the user names of SOC personnel who respond to incidents.
Categories	(Optional) Identifies categories of incidents. Clicking Categories, opens a drop-down list of Incident categories and subcategories. You can select one or more categories to which the incident belongs. Categories fall into these major groups: Environmental, Error, Hacking, Malware, Misuse, and Social.
Priority	Identifies the priority for the incident. Clicking Priority opens a drop-down list of priorities: Critical, High, Medium, or Low displayed in the drop-down list.
Cancel	Closes the dialog without saving changes.
Save	Saves the incident and closes the dialog. A message confirms that the incident was created successfully.

Investigation - Event Reconstruction Panel

This topic describes the features available in the Investigation > Events view > Event Reconstruction panel.

By default, Security Analytics displays the best reconstruction for the event determined by the event content or the reconstruction that you have selected in the Default Session View setting for Investigation. You can use the options in the Event Reconstruction toolbar to change the reconstruction method, view side-by-side results, export an event, open an email attachment, extract files, and open the event in a new tab.

To access this panel in a new tab, do one of the following:

- In the Events view, select an event to reconstruct and select **Actions > View Event> Open in New Tab**.
- In the Event Reconstruction toolbar of previewed reconstruction, click **Open Event in New Tab** in the toolbar.

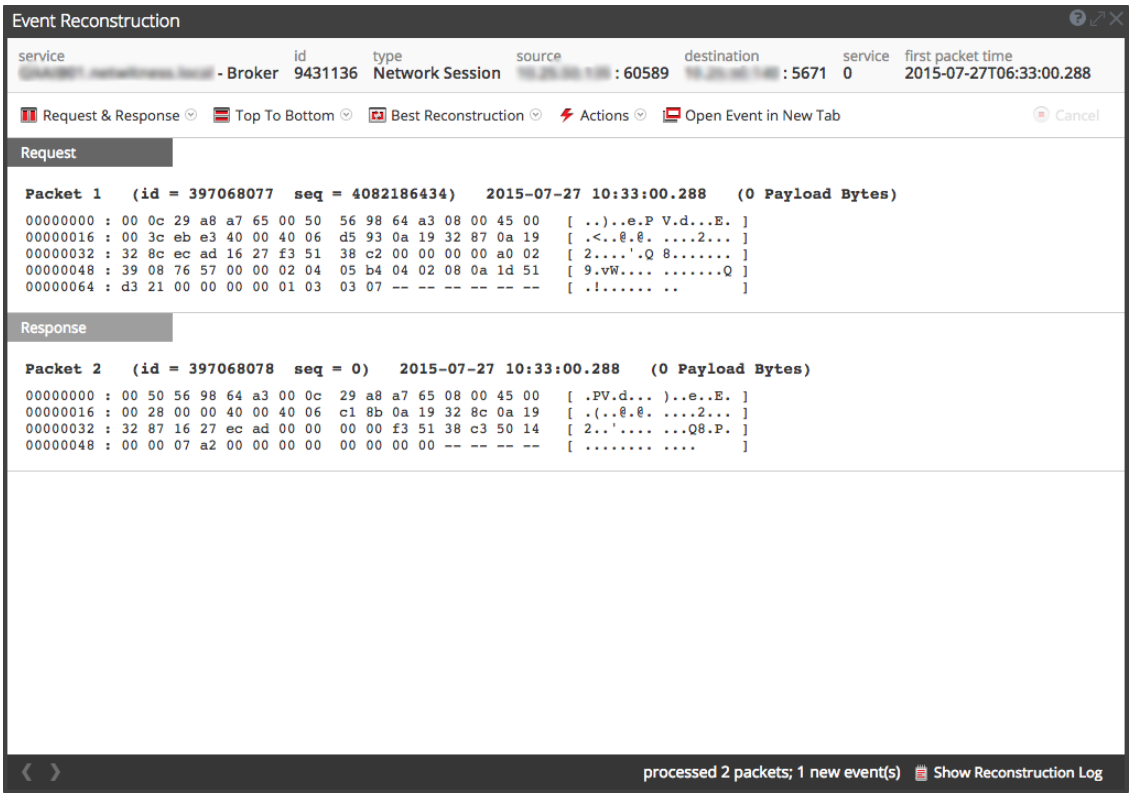
  The Event Reconstruction is displayed in a new tab.

To access this panel in the current tab, do one of the following:

- At the end of the event, select 

- Select an event to reconstruct and select **Actions > View Event > Preview Inline**.

The Event Reconstruction panel opens in a popup window in the same view.



Features

The Event Reconstruction panel has a toolbar at the top with the following options.

Feature	Description
Request & Response	Displays a drop-down menu for selecting whether the panel displays: • Request & Response • Request • Response
Organization	Displays a drop-down menu for selecting whether the information is displayed top to bottom or side by side.

Feature	Description
View	Displays a drop-down menu for selecting what information is displayed. By default, Best Reconstruction is selected. Other options are: • View Meta • View Text • View Hex • View Packets • View Web • View Mail • View Files
Actions	Displays a drop-down menu with the actions available in the Event Reconstruction panel.
Open Event in New Tab	Opens the event in a new browser tab.
Use More Packets	This button is visible on the Reconstruction panel only when you have enabled 'Allow Full Packet Reconstruction Override' checkbox in the Investigation Configuration Panel. This option renders sessions using large number of packets. **Note:** While rendering large sessions (as an Analyst), you get a confirmation message stating "Using larger number of packets might take time and cause system to slow down. Do you still want to continue?".

Beneath the toolbar is a list of meta keys and values. Some of the keys offer a drop-down menu with available actions.

The bar at the bottom of the panel offers several options.

Feature	Description
	Displays the previous event.
	Displays the next event.

Feature	Description
Show Reconstruction Log	Displays the reconstruction log at the bottom of the panel. Once you click this button, it changes to Hide Reconstruction Log.

Investigation - Events View

This topic describes the features available in the Investigation > Events view.

A list of events associated with a session is available in the Investigation > Events view. There are two ways to display the Events view:

- Select **Investigation > Events** in the **Security Analytics** menu. Security Analytics runs a default query on the last three hours for the default service (if one is set) or displays a dialog in which you can select a service and then runs the default query. The default query selects all events and the Events view displays events on the selected service, with the oldest events first.
- From within the Navigate view, click an event. The Events view displays the events on the selected service based on the drill point in the Navigate view.

The Events view provides three built-in presentations of event data: the Detail view, the List view, and the Log view. The List view and Detail view are intended for viewing packet data events, and they provide more information for each event including the timestamp, event type, event theme, and size.

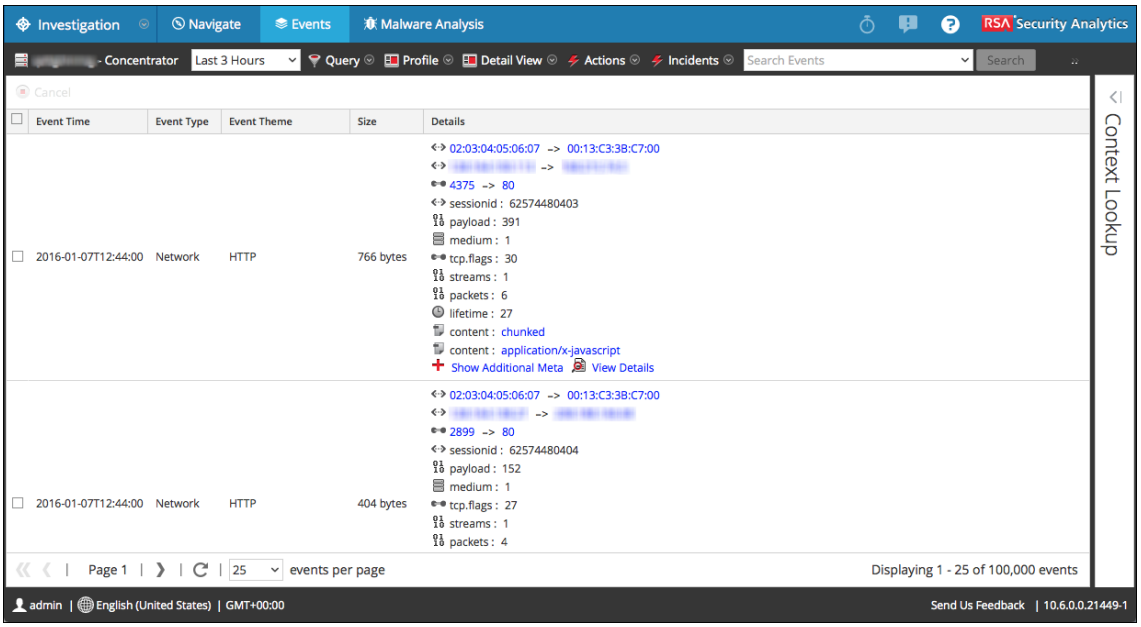
- The List View shows corresponding source and destination address and port information for events in summary form in a grid.
- The Detail View shows all metadata collected for the event in a paged view.

The Log View is optimized for viewing log information, and provides more information for each log including the timestamp, event type, service type, service class, and the logs.

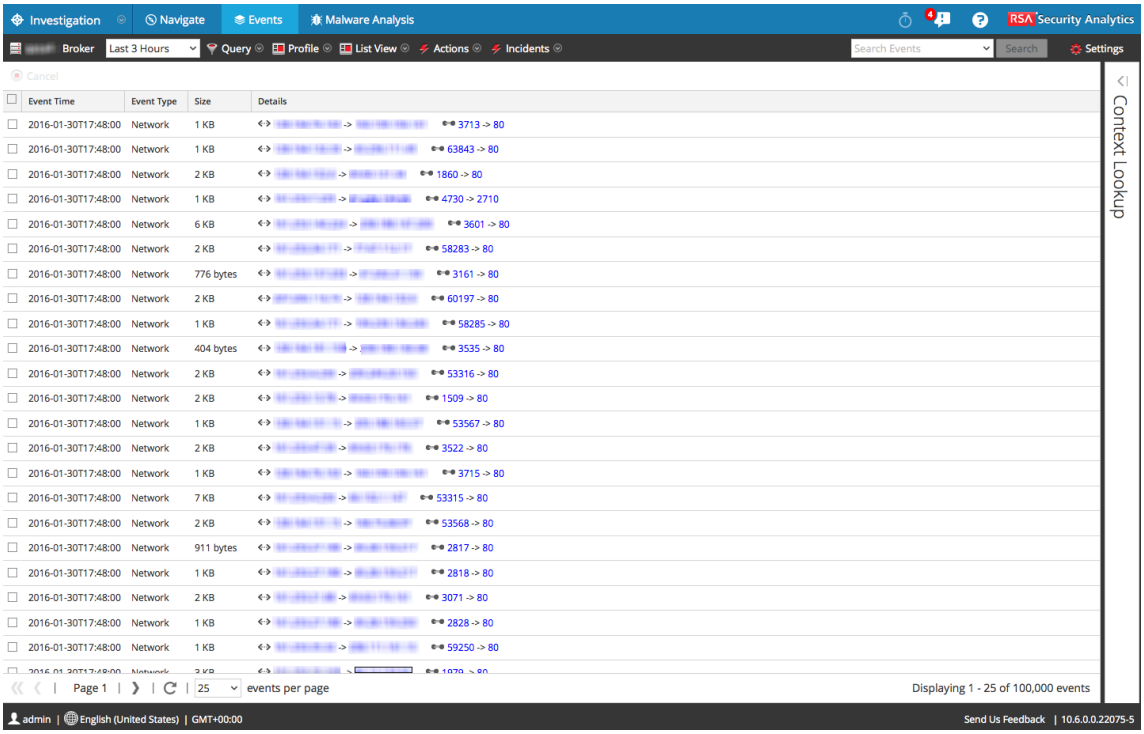
You can use queries, the time range setting, and profiles to filter the events listed in the Events view. From any view type in Events view, you can:

- Extract files
- Export events, logs, and meta values
- Open the Event Reconstruction panel by double-clicking an event

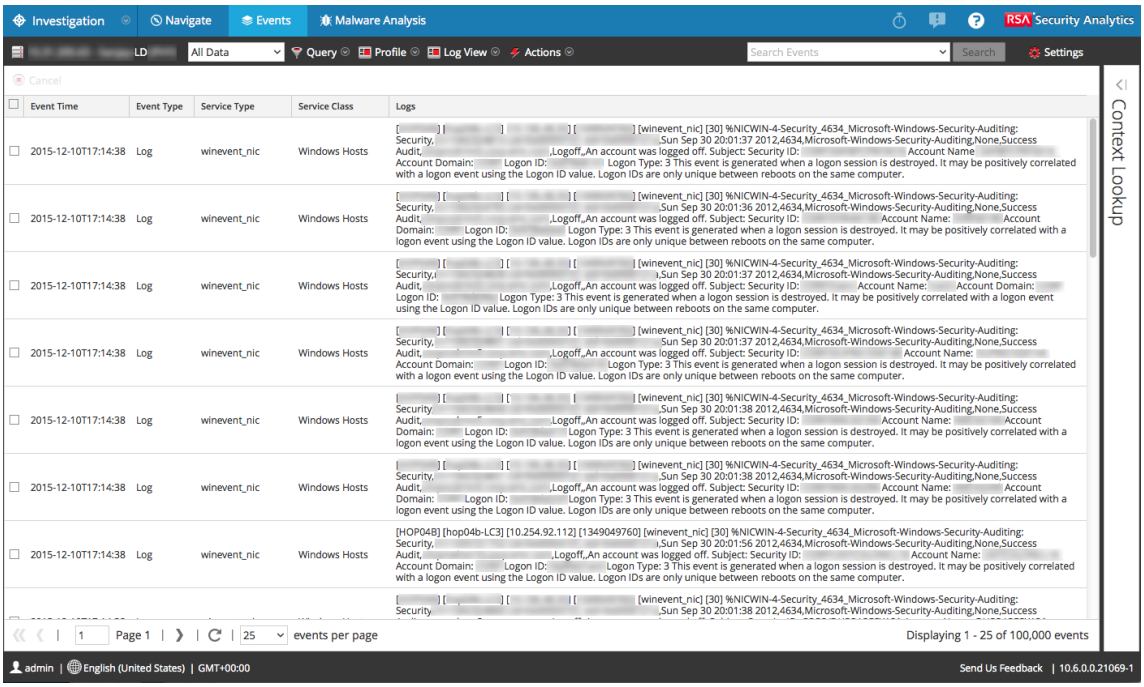
The following figure is an example of events in the Detail View. The Context Lookup panel is visible only if the Context Hub service is configured.



The following figure is an example of events in the List View.



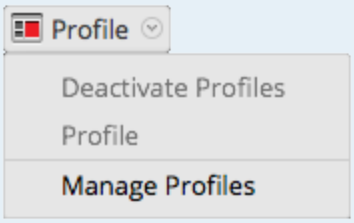
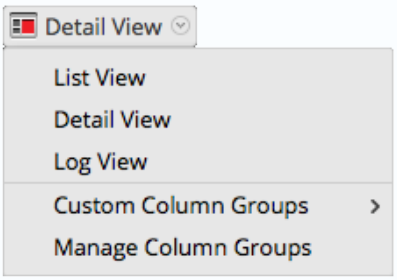
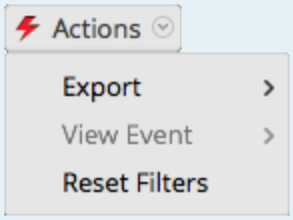
The following figure is an example of the Log View.



Features

The Events view has a toolbar at the top with the following options.

Feature	Description
Select Service	Displays the selected service name next to the icon. Opens the Select a Service dialog, in which you can select a service for which the event list is displayed.
Time Range	Displays a drop-down menu for selecting the time range to apply to the event list. You can choose one of the standard options or specify a custom time range.
Query 	Displays the Create Filter dialog, in which you can enter a custom query directly instead of drilling down the data (see Create a Custom Query)

Feature	Description
Use Profile 	Displays the Use Profile menu; the currently selected profile is displayed in the toolbar. A profile allows you to manage and use profiles that can include custom meta groups, a default column group, and a beginning query. The Profiles apply to the Navigate view (meta groups and queries) and the Events view (column groups and queries).
View Type Drop-down 	Displays a drop-down menu for selecting the event view type. • Detail View shows events in a paged format with detailed information for each event. • List view shows the events in grid form with a summary of each event in a separate row. • Log View shows a log-oriented events grid with a summary of each log in a separate row. • Custom Column Groups displays the event list using a column group selected from a drop-down list of custom column groups. • Manage Column Groups displays the dialog for creating and editing custom column groups.
Actions 	Displays a drop-down menu with actions in the Events view: • Extract Files, export events as a PCAP file, export logs or export meta values. • View an event reconstruction in a popup window or in a new tab. • Reset all filters in the Events view.
Incidents	Displays a drop-down menu in which you can create a new incident or add to an existing incident.

Feature	Description
Search Events	Enables you to search for text patterns within the current set of events displayed. If you click in the Search field, it shows a drop-down menu with search options. If you click Apply, it saves the selected options and also updates the search options in the Navigate view and the Investigations profile (see Investigation - Search Options).
Settings 	Displays the Investigation settings for the Events view (which are also available in the Profile view) so that you can change Investigation settings without navigating away from the Events view. When you change a setting In the Events view the setting is also changed in the Profile view (see Configure Navigate View and Events View).

The Events view pagination bar at the bottom of the page has options for paging through the Events list.

Feature	Description
	Displays the first page.
	Displays the previous page.
	If you have not enabled the **Paging in Investigation Event List optimized for speed** option in the Investigation Preferences dialog, paging by entering a specific page number is enabled.
	Displays the next page.
	Displays the last page.
	Refreshes the events list.

Feature	Description
Items per page	Displays a selection list for the number of items to display on a page.

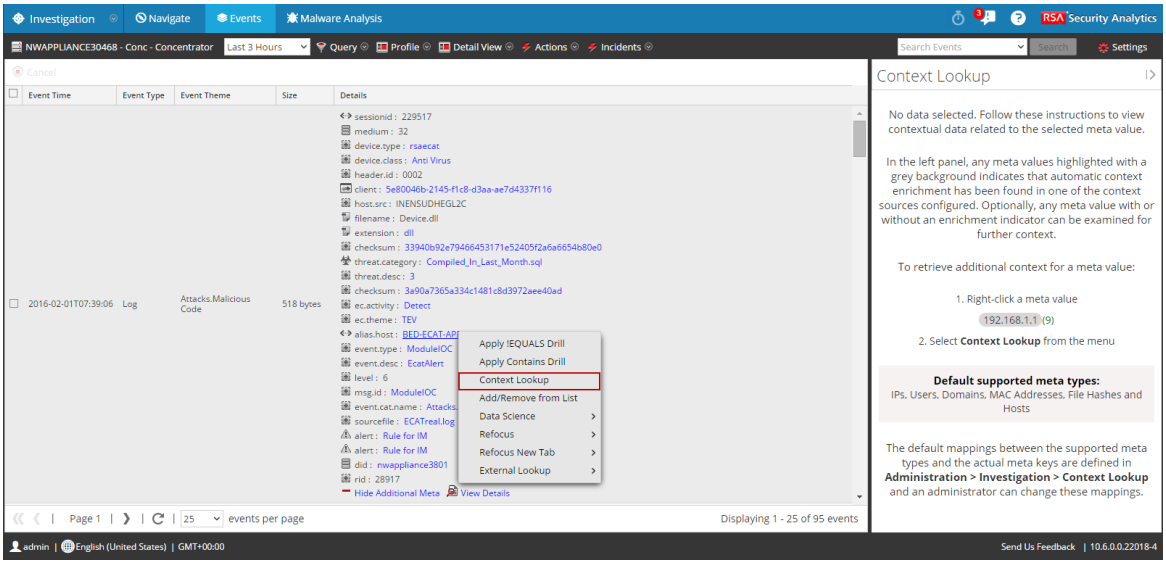
Context Lookup Panel

After you configure the Context Hub service, you can view the contextual information for the meta values in the **Navigate** view and the **Events** view of the Investigation module. For more information on configuring the Context Hub service, see *Context Hub Configuration Guide*.

For information about performing context lookup for meta values, see View Additional Context for a Data Point.

The Context Hub service is pre-configured with default meta type and meta key mapping. For information about the mapping of the context hub meta value with investigation meta key, see "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*.

The following figure illustrates the Context Lookup option when you right-click a meta value.

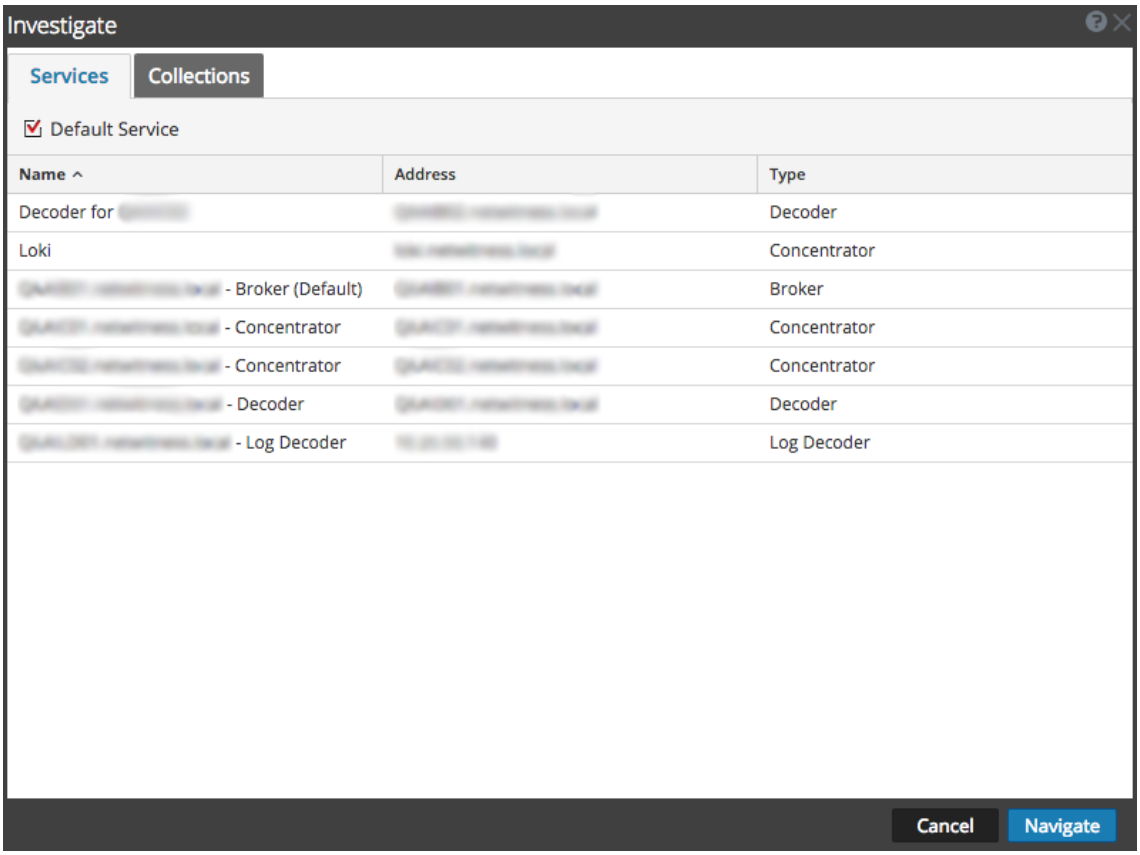


For more information about the lookup results and contextual information for different data sources, see "Context Lookup Panel" in the *Context Hub Configuration Guide*.

Investigation - Investigate Dialog

In the Investigate dialog, analysts can select a service or a collection to investigate.

The dialog is automatically displayed when you first go to the Navigate or Events view and have not selected a default service to investigate. To access the dialog from a current investigation, select the current service name in the toolbar.



Features

The Investigate dialog has two tabs: Services and Collections.

Note: Collections are also known as workbench collections. You can only view workbench collections that you have created, and only administrators can create a workbench collection.

Services Tab

The Services tab includes a list of services available for investigation, and three buttons. All features are described in the following table.

Feature	Description
Default Service	Clicking this button sets or clears the default service to investigate. When a service has been set as the default service, the word (Default) is appended to the service name.
Name	The name of the service.
Address	The IP address of the service.
Type	The type of service.
Cancel	Closes the dialog.
Navigate	Opens the selected service in the Navigate or Events view.

Collections Tab

The Collections tab has two buttons and two panels: Workbench and Collections.

The Workbench panel lists available Workbench services. Once a Workbench service is selected, you can select a collection from the Collections panel. The name is the name of the Workbench service.

The Collections panel lists available collections to investigate. Once a collection is selected, you can click Navigate to view the collection.

The following table describes the features of the Collections panel.

Feature	Description
Name	The name of the collection.
Type	The type of collection.
Size	The size of the collection.
Data Type	The type of data within the collection.
Date Created	The date the collection was created.

Investigation Tab - User Preferences Panel

This topic introduces the features of the Profile view > Preferences panel > Investigations tab.

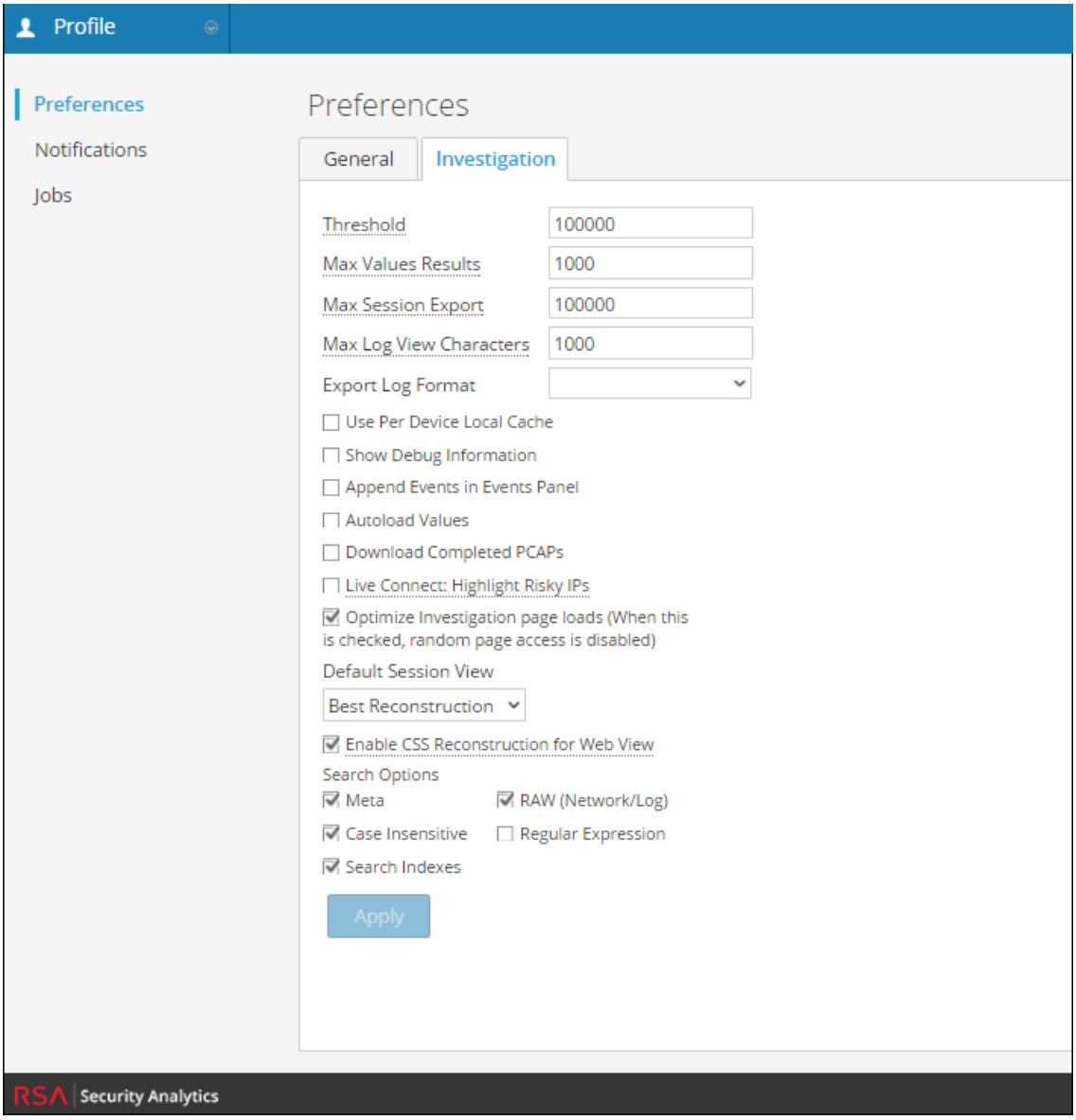
In the Profile view > Preferences panel > Investigation tab, users can set several preferences that affect the performance and behavior of Security Analytics when analyzing data, viewing events, and reconstructing events in Investigation.

Procedures related to this tab are described in Configure Navigate View and Events View.

To access this tab:

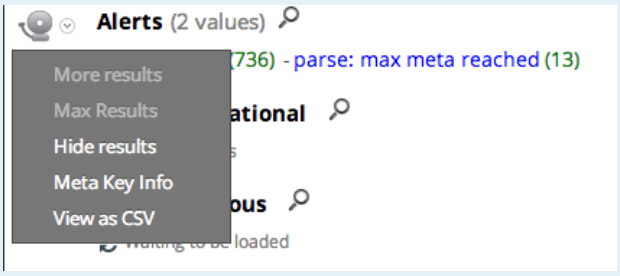
1. In the **Security Analytics** menu, select **Profile**.
2. In the **left navigation panel**, select **Preferences.**

3. In the **Preferences** panel, select the **Investigations** tab.



Features

The following table describes the Investigation preferences.

Feature	Description
Threshold	This setting controls the count shown for a Meta Key value in the Navigate view during the load. A higher threshold allows more accurate counts for a value. However, a higher threshold causes longer load times. When the threshold is reached, Security Analytics displays the count and the percentage of time used to reach the count in comparison to the time necessary to load all sessions with that value. For example, **(>100000 - 18%)** indicates that the threshold was set at 100000 and this load took only 18% of the time it would have taken with no threshold set. The default value is **100000**.
Max Values Results	This setting controls the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**. 
Max Session Export	This setting controls the maximum number of sessions that can be exported. The default value is **100000**.
Max Log View Characters	This setting controls the maximum number of characters to be displayed on **Investigation > Events > Log Text**. The default value is **1000**.
Export Log Format	This setting specifies the default format for exporting logs from Investigation. Available options are **Text**, **XML**, **CSV**, and **JSON**. There is no built-in default value for the log export format. If you do not select a format here, Security Analytics displays a selection dialog when you invoke export of logs. When you select one of the options from the Export Log Format drop-down menu and click Apply, the setting goes into effect immediately.

Feature	Description
Export Meta Format	This setting specifies the default format for exporting meta values from Investigation. Available options are **Text**, **XML**, **CSV**, and **JSON**. There is no built-in default value for the meta values export format. If you do not select a format here, Security Analytics displays a selection dialog when you invoke export of meta values. When you select one of the options from the Export Meta Format drop-down menu and click **Apply**, the setting goes into effect immediately.
Show Debug Information	When this option is selected, Security Analytics displays the where clause beneath the breadcrumb in the Navigate view. For each meta value load, the load time is displayed. If the service is a Broker, then the elapsed time for each aggregated service is reported. The default value is **Off.**
Append Events in Events Panel	When this option is selected, the events displayed in the **Events Panel** are added incrementally rather than overwriting the currently displayed events. For example, each time you click the next page icon, the events are displayed incrementally such as 1 -25, 1 -50, 1 -75 and so on. **Note:** This option is available, only if the Optimize Investigation Page Loads option is enabled.
Autoload Values	When this option is selected, the service values are automatically loaded in the Navigate view. When not selected, Security Analytics displays a **Load Values** button, allowing the user the opportunity to modify the options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigation module so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP format.

Feature	Description
Optimize Investigation Page Loads	This option is enabled by default (checked) and controls how the Events view retrieves events. When optimized, results are returned as quickly as possible. This sacrifices the original ability to go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). Being able to go to any page in the list sacrifices some speed in returning the results due to additional overhead determining the events in advance.
Default Session View	This setting selects the default reconstruction type for the initial reconstruction view. By default events are reconstructed using the reconstruction method most appropriate to the event.
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for stylesheets and images used in the target event. The option is enabled by default. Uncheck this option if there are problems viewing specific websites. **Note:** The appearance of the reconstructed content may not match the original web page perfectly if related images and stylesheets could not be found or were loaded from the web browser's cache. Also, any layout or styling that is performed dynamically via client side javascript will not render in the reconstruction because all client side javascript is removed for security purposes.
Search Options	This setting sets the default search options to apply to a search in the Navigate and Events views. Investigation - Search Options provides detailed information.
Apply	Saves your preferences and puts them into effect immediately.

Investigation - Manage Default Meta Keys Dialog

This topic provides a description of the Manage Default Meta Keys dialog.

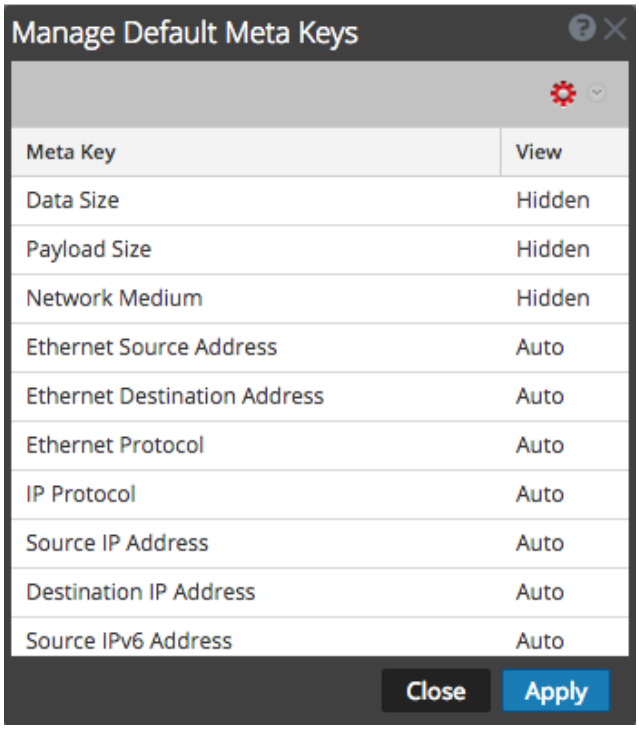
In the Manage Default Meta Keys dialog, analysts can specify the meta keys to be displayed during navigation for a specific service. This can help you find the desired data more quickly and prevents the loading of meta that is not of interest.

When you modify the default meta keys for a non-indexed meta key, you cannot set the key to **Open**. If you change the default view for a group of meta keys to **Open** and some of the meta keys are non-indexed, the non-indexed meta keys revert to **Auto**. As a result, the meta key is automatically loaded only if it is indexed, and non-indexed meta keys are **Closed** until opened manually.

To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Navigate**.
   The Investigate dialog is displayed.
2. To choose a service, do one of the following:
   - Double-click a service.
   - Select a service and click **Navigate**.
     The Navigate view for the selected service is displayed.
3. In the **Navigate View** toolbar, select **Meta > Manage Default Meta Keys**.

The Manage Default Meta Keys dialog is displayed.



Related procedures are available in Manage and Apply Default Meta Keys in an Investigation.

Features

The Manage Default Meta Keys dialog has a grid, toolbar, Close button, and Apply button.

Grid

In the grid, you can view, sort, and manage default meta keys. If you click and drag meta keys, you can rearrange their order. The following table provides descriptions of the grid features.

Feature	Description
Meta Key	This column displays the meta keys available for the service.

Feature	Description
View	This column displays the type of view assigned to each meta key. By clicking on the view in each row, you can assign the meta key a different default view. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default, and can be opened manually. • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default.

Toolbar and Buttons

The following table describes the toolbar and button features.

Feature	Description
	Clicking the Actions menu allows you change the default view of all the meta keys. There are four views: • Auto: Reverts to the default view for meta keys as specified in the service index file. • Close: The values of this meta key are closed by default. • Hidden: The values of this meta key are hidden by default. • Open: The values of this meta key are displayed by default.
Close	Closes the dialog. Any unsaved changes are lost.
Apply	Applies the changes, and they become effective immediately.

Investigation - Malware Analysis Events List and Files List

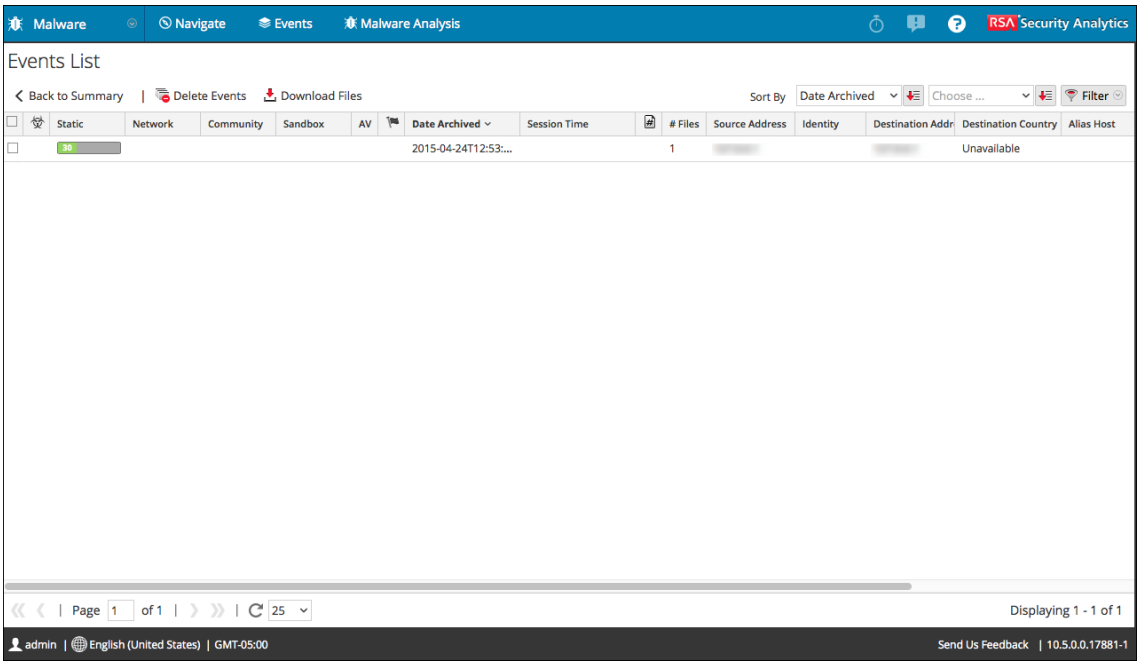
The Malware Analysis Events List and Files List provide a detailed view of events or files. You can double-click on an event or file in either of the lists to display the Analysis Results view in a new browser tab.

To access this view:

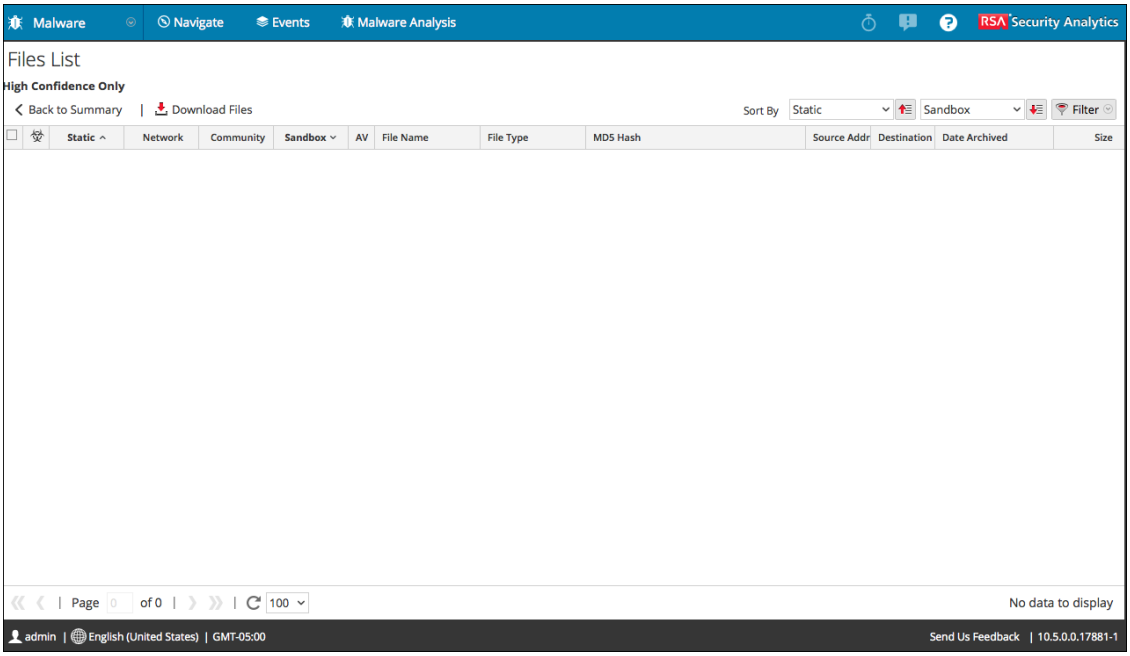
1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.
2. In the **Select a Malware Analysis Service** dialog, select a service from the left panel, then select a job from the right panel.
3. Click **View Scan**.
   The Summary of Events view is displayed.
4. In either the **Total** panel or the **High Confidence** panel, click the number in the **Events Created** section.
   If you want to view the Files List, click the number in the **Files Processed** section.
5. Depending on your choice, the Events List or the Files List is displayed.

Note: The Events list can be viewed by users who have submitted the scan job or an user with administrator privileges.

This is an example of the Events List view.



This is an example of the Files List view.



Related procedures are available in Examine Scan Files and Events in List Form.

Features

The **Events List** and **Files List** each have a grid and a toolbar.

Events List Toolbar

These are the features in the Events List toolbar.

Events List Grid

These are the features in the Events List grid.

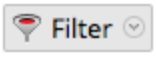
Feature	Description
	Indicates whether the event is influenced by the high confidence flag.
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.
	Indicates whether the event is influenced by a customized rule.
Date Archived	Displays the date and time the event was archived. **Note:** Archived time is the time when Malware Analysis stores the event in database. This time is not related to the session or analysis time in case of caching.
Session Time	Displays the time of the event's session.
	Indicates whether the hash value is marked as trusted.
# Files	Displays the number of files included in the event.
Source Address	Displays the address of the event source.
Identity	Displays the identity of the event source.
Destination Address	Displays the address of the event destination.

Feature	Description
Destination Country	Displays the country of the event destination.
Alias Host	Displays the hostname of the alias.
Event Type	Displays the type of event. For example, Manual Upload.
Service	Displays the service on which the event occurred.
Destination Organization	Displays the organization of the destination.

Files List Toolbar

These are the features in the Files List toolbar.

Feature	Description
Back to Summary	Returns to the Summary of Events view.
Download Files	Displays the Malware File Download dialog, which allows you to download available files.

Feature	Description
	Displays a drop-down menu from which you can decide how to sort the list. These are the options for sorting: • High Confidence • Static • Network • Community • Sandbox • AV • File Name • File Type • Hash • Date Archived • Size The button directly to the right of this drop-down indicates whether the list will be sorted by ascending or descending values.
	Displays a drop-down menu from which you can select a secondary sorting order. This menu includes an option for **None**, so selecting a secondary sorting order is not necessary.
	Displays a drop-down window in which you can filter the list by filename or MD5 Hash.

Files List Grid

These are the features in the Files List grid.

Feature	Description

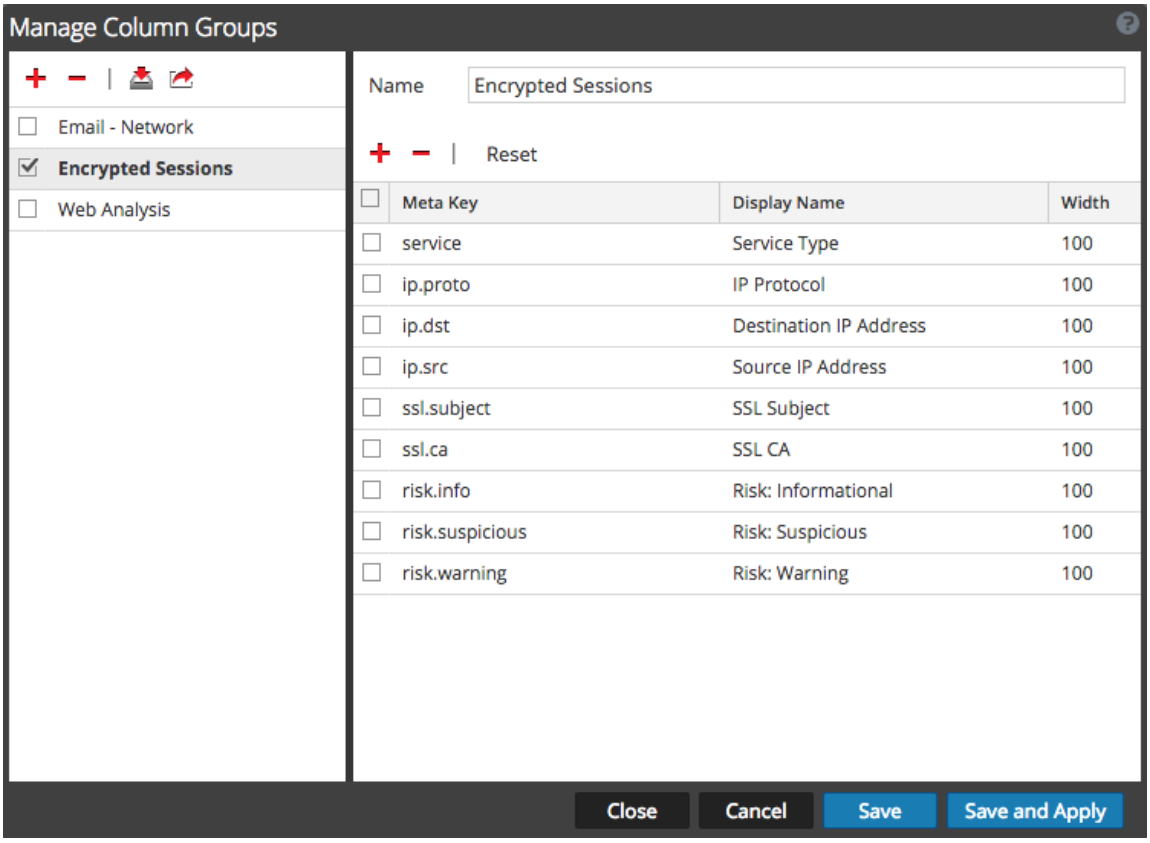
Feature	Description
	Indicates whether the event is influenced by high confidence flag.
Static, Network, Community, Sandbox	Displays the scores for each scoring module.
AV	Indicates whether the AV flagged this event as suspicious.
File Name	Displays the name of the file.
File Type	Displays the type of the file (for example, PDF or x86 PE)
MD5 Hash	Displays the MD5 hash.
Source Address	Displays the address of the file source.
Destination Address	Displays the address of the file destination.
Date Archived	Displays the date and time the file was archived.
Size	Indicates the size of the file.

Investigation - Manage Column Groups Dialog

In Manage Column Groups dialog, you can add, delete, import, export, and edit column groups to display specific meta keys.

To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Events**.
   The Investigate dialog is displayed.
2. Select a service and click **Navigate**.
3. In the toolbar, select **Detail View > Manage Column Groups**.
   The Manage Column Groups dialog is displayed.



OOTB Column Groups

At fresh installation, OOTB column groups are added for investigation in the Manage Column Groups dialog. The OOTB column groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted.

Custom Column Groups

The Custom Column groups drop-down are added for investigation in the Custom Column Groups dialog. The Custom Column groups lists all the custom and the OOTB column groups.

To access this dialog:

1. In the Security Analytics menu, select Investigation > Events.
   The Investigate dialog is displayed.
2. Select a service and click Navigate.
3. In the toolbar, select Detail View > Custom Column Groups.
   The Custom Column Groups drop-down is displayed.

Related procedures are available in Manage Column Groups in the Events View.

Features

The Manage Column Groups dialog has two panels: Groups and Settings.

At the bottom of this dialog are four buttons: Close, Cancel, Save, and Save and Apply. The following table provides descriptions of these buttons.

Feature	Description
Close	Closes the dialog without saving.
Cancel	Cancels all unsaved changes.
Save	Saves all changes without closing the dialog.
Save and Apply	Saves and applies all changes immediately, closing the dialog.

Groups Panel

The left panel is the Groups panel. This is where you can add, delete, import, or export column groups. At the top of the panel is a toolbar which provides actions. Below the toolbar is a list of added column groups, where you can select one or more groups.

The following table lists the actions in the toolbar.

Action	Description
	Adds a column group. Clicking this button highlights the Settings panel on the right, where you can name the column group and add or delete meta keys. At least one meta key is required to add a group.
	Deletes a column group. A confirmation dialog is displayed before the selected group is deleted.
	Displays the Import Column Groups dialog, where you can select a file to upload.
	Exports one or more selected groups to your computer.

Settings Panel

The right panel is the Settings panel. This is where you can create and edit column groups. This panel contains the Name field, a toolbar, and a grid.

The following table describes the features of the Settings panel.

Feature	Description
Name	The name of the selected column group.
	Adds a new row to the list of meta keys, where you can open a drop-down menu to select a new meta key.
	Deletes one or more selected meta keys. Displays a confirmation dialog before deleting.
Reset	Returns column group to its most recently saved settings.
Meta Key	Lists the meta keys added to the selected column group.
Display Name	Lists the names of the meta keys as they will be displayed in the Events view.
Width	Specifies the width of each meta key's column. The width can be set between **10** and **1000**. The default width is **100**.

Investigation - Manage Meta Groups Dialog

This topic describes the functions and features of the Manage Meta Groups dialog.

In the Manage Meta Groups dialog, you can add, delete, import, and export meta groups.

To access this dialog:

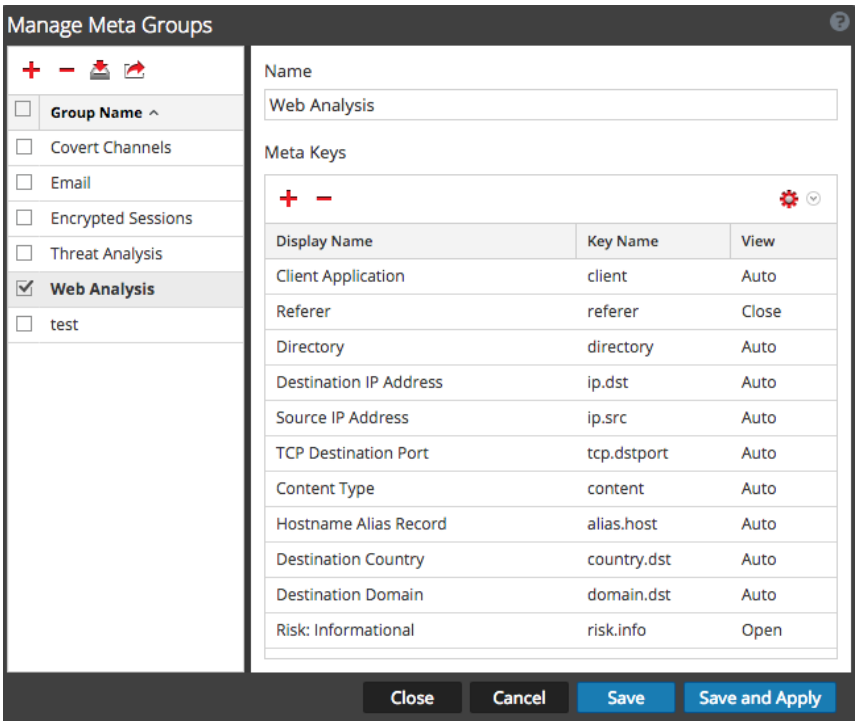
1. In the **Security Analytics** menu, select **Investigation > Navigate**.

   The Investigate dialog is displayed.

2. Select a service, then click **Navigate**.

3. In the **Navigate View** toolbar, select **Meta > Manage Meta Groups**.

   The Manage Meta Groups dialog is displayed.



OOTB Meta Groups

At fresh installation, OOTB meta groups are added for investigation in the Manage Meta Groups dialog. The OOTB meta groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted.

Procedures that you can perform in this dialog are described in Manage User-Defined Meta Groups.

Features

The Manage Meta Groups dialog has two panels. The following table describes the buttons at the bottom of the dialog.

Feature	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and immediately applies all changes.

Meta Groups Panel

The Meta Groups panel is on the left side of the Manage Meta Groups dialog. This is where you can add, delete, import, and export meta groups.

The following table describes the features of the Meta Groups panel.

Feature	Description
	Adds a meta group using the Settings panel on the right side of the Manage Meta Groups dialog.
	Deletes the selected meta group. A confirmation dialog is displayed before the meta group is deleted.
	Displays the Meta Group Import dialog, where you can upload a file.
	Exports the selected meta group to your computer.
Group Name	Lists all meta group names.

Settings Panel

The Settings panel is on the right side of the Manage Meta Groups dialog. This is where you create and edit meta groups. Below the Name field is the Meta Keys grid.

The following table describes the features of the Settings panel.

Feature	Description
Name	Displays the name of the selected meta group.
	Displays the Available Meta Keys dialog, where you can select meta keys to add to the group.
	Deletes the selected meta keys.
	Displays a drop-down menu, where you can select the view for all meta keys. There are four options based on the possible values for the `defaultAction` property used to define a key in the custom index file for the service: • Hidden: These meta keys are hidden by default, and are not shown in Investigation at all. • Open: The values of this meta key are displayed by default. • Close: The values of this meta key are closed by default, and can be opened manually. • Auto: Reverts to the default view for meta keys as specified in the service index file.
Display Name	Indicates the name that is displayed for the key in Investigation views, and is defined by the `description` property for the key in the custom index file for the service..
Key Name	Indicates the `name` of the meta key as defined in the custom index file for the service.
View	Indicates which view the meta key is set to. You can change this by either: • Clicking  , then selecting a view in order to change all meta key views. • Clicking a single meta key in the View column, then opening the drop-down menu in which all available views are displayed, in order to change an individual meta key view.

Investigation - Manage Profiles Dialog

In the Manage Profiles dialog, you can configure, add, delete, import, and export profiles.

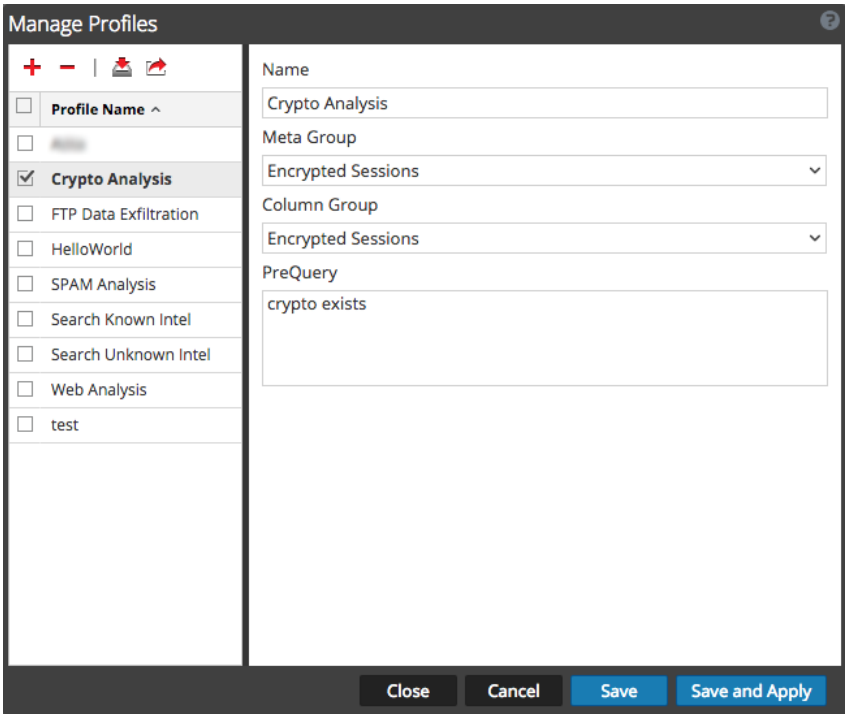
To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**. Both views provide access to the Manage Profiles dialog.

   The Investigate dialog is displayed.

2. Select a service, then click **Navigate**.
3. In the toolbar, select **Profile > Manage Profiles**.

   The Manage Profiles dialog is displayed.



OOTB Profiles

At fresh installation, OOTB profiles are added for investigation in the Manage Profiles dialog. The OOTB profile groups are prefixed with RSA for identification and can be duplicated but cannot be edited or deleted.

Related procedures are available in Use Investigation Profiles to Encapsulate Custom Views.

The Manage Profiles dialog has two panels. At the bottom of the dialog there is a row of buttons.

Buttons

The following table describes the buttons.

Field	Description
Close	Closes the dialog.
Cancel	Cancels all changes.
Save	Saves all changes.
Save and Apply	Saves and applies all changes immediately.

Profile Panel

The Profile panel on the left side of the dialog displays available profiles and allows you to add, delete, import, and export profiles.

The following table describes the fields in the Profile panel.

Field	Description
	Adds a new profile using the Settings panel on the right side of the Manage Profiles dialog.
	Deletes the selected profile. A confirmation dialog is displayed before the profile is deleted.
	Displays the Profile Import dialog, where you can upload a file.
	Exports the selected profile to your computer.
Profile Name	Lists all profile names.

Settings Panel

The Settings panel on the right side of the dialog offers options to configure profiles. It can only be used when one profile is selected.

The following table describes the fields in the Settings panel.

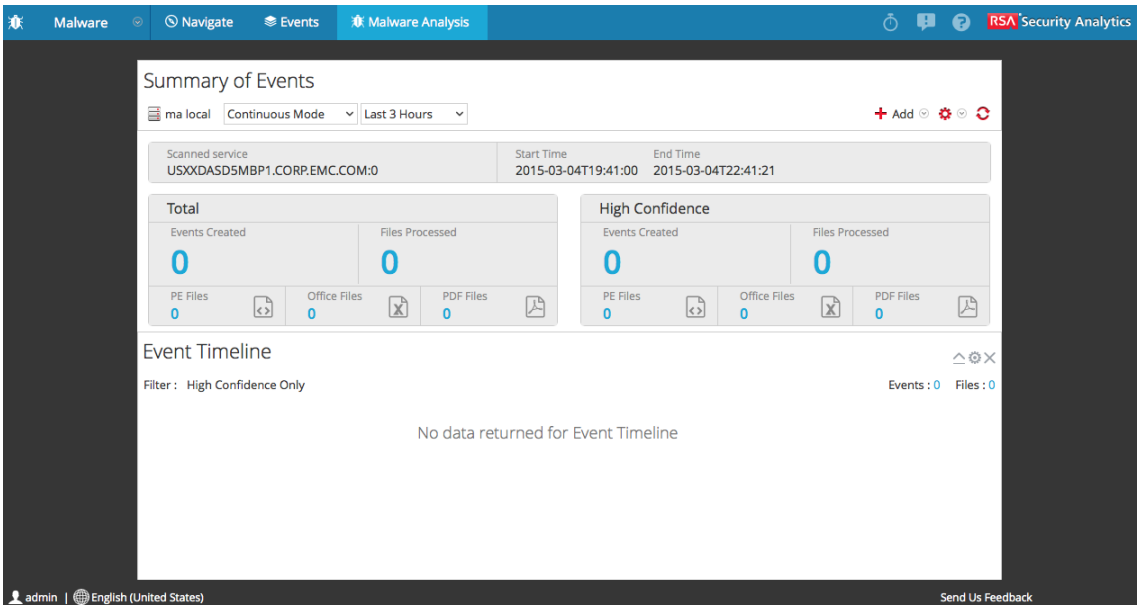
Feature	Description
Name	Displays the name of the profile.
Meta Group	Displays a drop-down menu listing available meta groups.
Column Group	Displays a drop-down menu listing available column groups. Three groups are available by default: • List View • Detail View • Log View
PreQuery	Defines a limiting query for filtering Investigation results. This query is used when the associated profile is activated and the preQuery applies to any queries used in the Investigation Navigate and Events views. This is an example of a preQuery: `'service=80,25,110'.`

Investigation - Malware Analysis View

Within Security Analytics Investigation, the Malware Analysis view provides the user interface for conducting a malware analysis. The Malware Analysis view is in the form of a customizable dashboard, in which default dashlets in the initial view are based on the user role (Administration or Analyst) and user customizations. Initially, the Summary of Events dashlet is displayed in the Malware Analysis view. Additional dashlets present different visualizations of the events being viewed, and each representation is configurable to further refine your view as you search for Indicators of Compromise. The Malware Analysis dashlets available in the Security Analytics Dashboard are also available in the Malware view.

To access this view:

1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.
   If a default service has not been selected, the Select a Malware Analysis Service dialog is displayed.
2. Select a service, then click **View Continuous Mode**.
   The Malware Analysis view is displayed.



Features

The Malware Analysis view consists of the Summary of Events panel and four dashlets unique to this view. Each of the unique dashlets have identical Options dialogs. The Malware Analysis dashlets in the Security Analytics dashboard are also available, and are described in Security Analytics Dashlets in *Security Analytics Geting Started Guide*.

Summary of Events Panel

In the Summary of Events panel, you can select the service, the scan mode, and the time range. In addition, you can select a data point and view the events associated with the event.

The following table describes all features in the Summary of Events panel.

Feature	Description
	Selects a service to display.
Scan Mode	Displays a drop-down list of available scan modes.
Time Range	Displays a drop-down list of time ranges to view events.
Start Date	When Time Range is set to custom, offers a calendar from which to choose the start date of the time range.
End Date	When Time Range is set to custom, offers a calendar from which to choose the end date of the time range.
	Displays a drop-down list of dashlets you can add to the view.
	Displays a drop-down list of actions you can perform in this view: • Restore Default Configuration • Order Dashlets • Apply Threshold Filter
	Refreshes the Malware Analysis view.

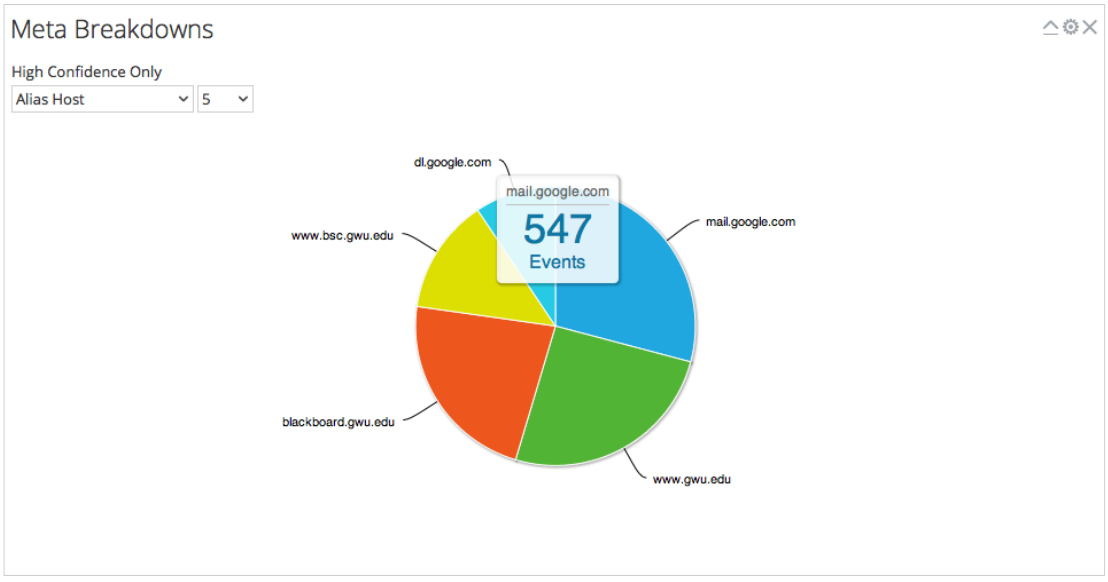
Options Dialog

In the Options dialog, you can customize the results displayed in the dashlet. This dialog can be accessed by clicking the  icon in the top right corner of each dashlet. The following table describes the features of the Options dialog.

Feature	Description
Title	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Influenced By High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence.
Static, Network, Community, Sandbox	Allows you to filter results based on the scores in the scoring modules.
Cancel	Closes the dialog without saving any changes.
Apply	Applies changes to the dashlet immediately and closes the dialog.

Meta Breakdowns

Meta Breakdowns presents events in the form of a pie chart, with each slice representing a meta value for the specified meta key. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta value having the most events. Hovering over an event displays the count.

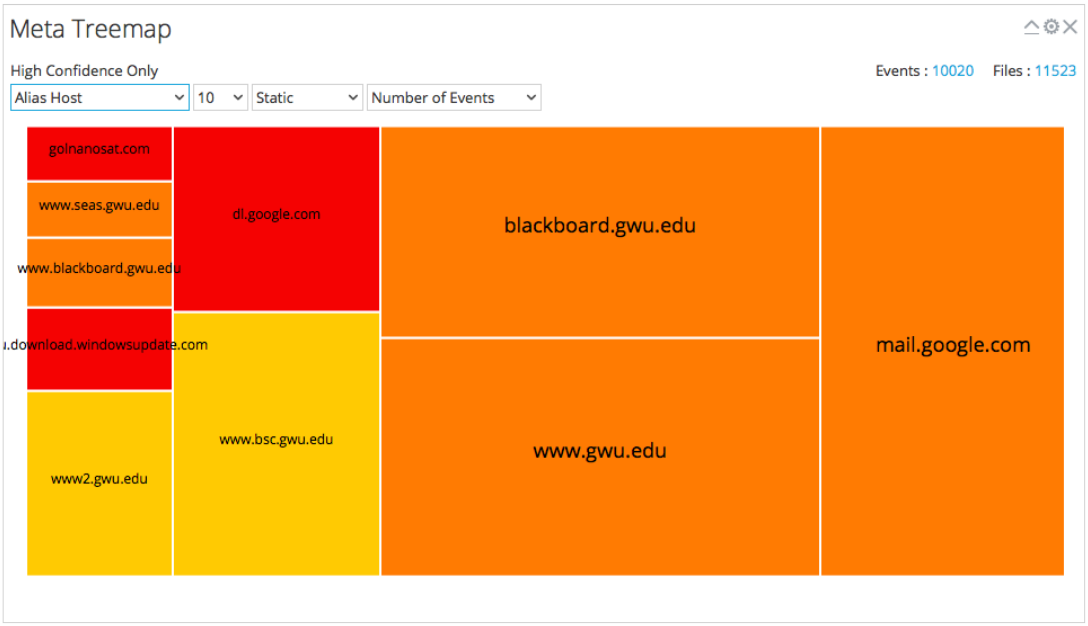


The following table describes the options in the Meta Breakdowns dashlet.

Feature	Description
High Confidence Only	Indicates whether the data shown is restricted to events flagged as high confidence or not. If the data is not restricted, this line will not be displayed.
Meta Key	Drop-down list of available meta keys.
Count	Drop-down list specifying how many of the top results are displayed.

Meta Treemap

Meta Treemap presents events in the form of a heat map. You can select the meta key and the count of meta values for that key to render in the chart, starting with the meta values having the most events. In addition, you can select the module that detected the meta value in the events: static, network community, or sandbox.



The following table describes the options in the Meta Treemap dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.

Feature	Description
Meta Key	Drop-down list of available meta keys to select as a filter.
Count	Drop-down list specifying how many of the top results are displayed.
Module	Drop-down list specifying which module results will be pulled from.
Value	Drop-down list specifying what information will be displayed when the mouse is hovering over a result (for example, Average Score).

Score Wheel

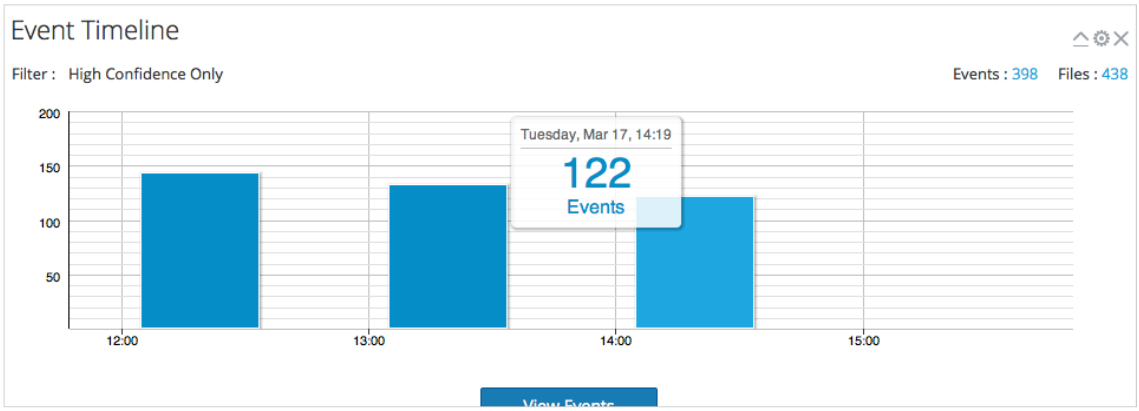
The Score Wheel offers a view of events as concentric rings with colors representing scores for events based on Indicators of Compromise and the scoring module. You can arrange the position of the rings using the Up and Down arrows to obtain a view that highlights events that were detected by one scoring module (red) and not detected by other scoring modules.

The following table describes the features of the Score Wheel dashlet.

Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
Module Order grid	Displays the order of the rings in Score Wheel, Ring 1 being the innermost ring and Ring 4 being the outermost ring. You can click the **Up** and **Down** buttons to reorder the modules, then click **Update** to apply the changes.

Event Timeline

The Event Timeline offers a view of events organized by the time of occurrence in a bar graph. Clicking and dragging to select a time range within the chart zooms in on the selected time.



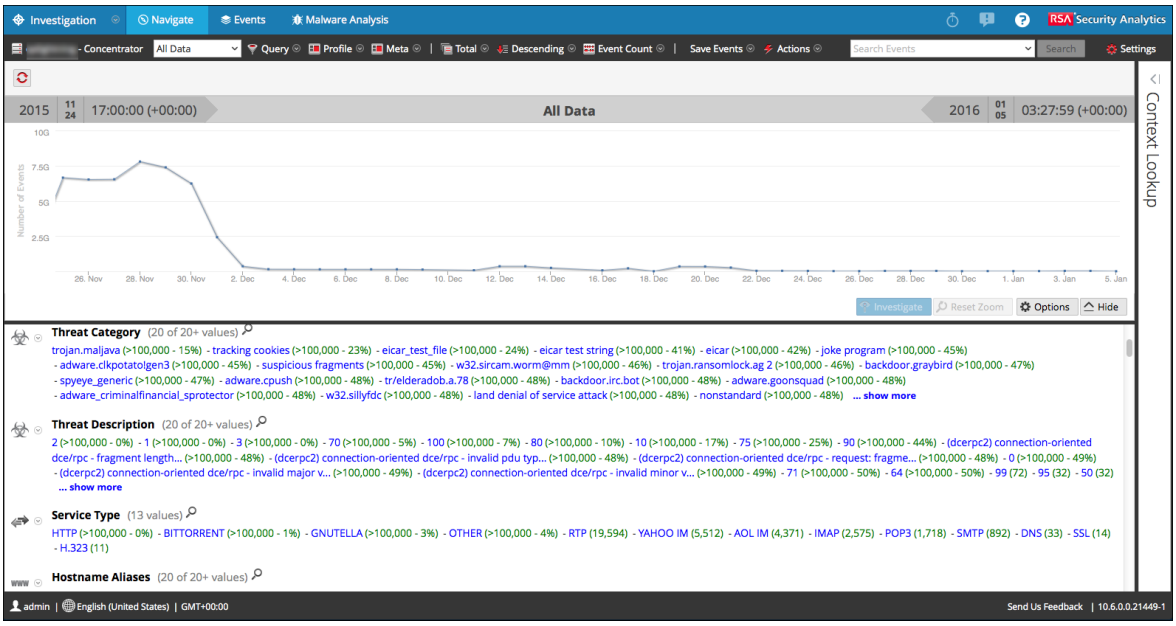
The following table describes the features of the Event Timeline dashlet.

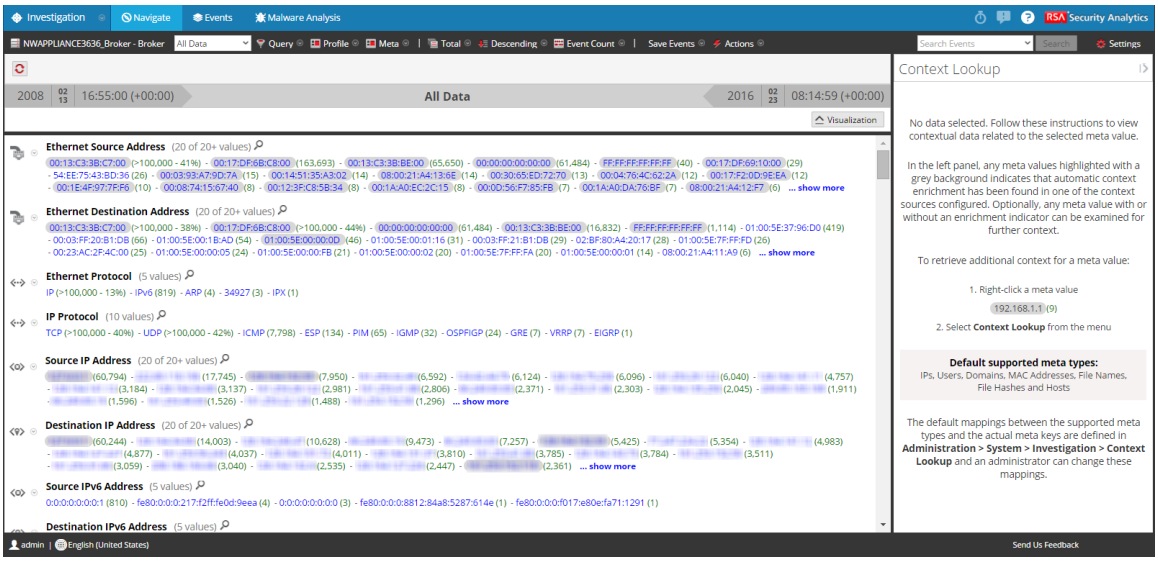
Feature	Description
High Confidence Only	Indicates whether or not the results are restricted to events flagged as high confidence or not. If the results are not restricted, this line will not be displayed.
View Events	Displays the Investigation > Events view.

Investigation - Navigate View

The Navigate view displays the activity and values for the selected service in accordance with the Investigation options in the Options panel: profile, time range, meta group, and query. As analysts investigate events of interest, the meta keys and values are displayed.

To access the Navigate view, select **Investigation > Navigate** in the **Security Analytics** menu. When a service investigation is open, the view is similar to the figure below.

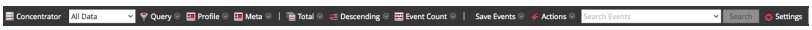




The Navigate view consists of these features:

- Toolbar
- Pause/reload button and breadcrumb
- Time banner
- Optional debug information.
- Collapsible Visualization panel
- Values panel
- Context Lookup panel

Toolbar



The toolbar provides a way to:

- Change the service being investigated.
- Control the range of data displayed: You can select use profiles, set a time range, use meta groups, and create queries to apply to the data.
- Set the quantification method and sorting method for data in the Values panel.
- Perform actions on the results. You can export and print results, navigate to an event for which you have an event ID, and pass a query to Informer.
- Configure Investigation settings without navigating away from the Investigation views.

Some of the toolbar options are labeled with the default value or the selected value rather than displaying the name of the option. For example, the time range option in the example above is labeled **All Data** to reflect the currently selected value. These are the tool bar options.

Option	Description
	Displays the selected service name next to the icon. Clicking the icon opens the Investigate a Service dialog, in which you can select a service to investigate and set the default service to investigate (see Begin an Investigation of a Service or Collection). Changing the service does not cause a reload of the data.

Option	Description
Time Range	Displays the Time Range options; the currently selected option is displayed in the toolbar (see Set the Time Range for an Investigation). Possible choices are: • All Data • Last 5, 10, 15, or 30 Minutes • Last Hour, Last 3, 6, 12, or 24 Hours • Last 2 or 5 Days • Early Morning • Morning • Afternoon • Evening • All Day • Yesterday • This Week • Last Week • Custom **Note:** If you specify custom start or end times in seconds, the value for start time in seconds always defaults to :00, and the value for end time in seconds always defaults to :59. For example, if you are using time to drill down into an issue, the drill time will be interpreted as `HH:MM:00 - HH:MM:59`. Seconds display in this format in Investigation > Navigate functions.
Query	Displays the Query dialog, in which you can enter a custom query directly instead of drilling down the data. See Investigation - Query Dialog for a description of the dialog.

Option	Description
Profile	Displays the Profile menu; the currently selected profile is displayed in the toolbar. A profile allows you to manage and use profiles that can include custom meta groups, a default column group, and a beginning query. The Profiles apply to the Navigate view (meta groups and queries) and the Events view (column groups and queries). See Use Investigation Profiles to Encapsulate Custom Views for more information.
Meta	Displays the Meta Group menu. You can use Default Meta Keys or a custom Meta Group. You also have the option to make changes to both group types (see Manage User-Defined Meta Groups).
Sort Field	Displays the Sort Field menu; the currently selected option is displayed in the toolbar. The menu has two options: Order by Total and Order by Value. The Sort Field is a complement to the Sort Order option; the data for each meta key is ordered based on the total (green number) or the meta value (blue text) (see Set Quantification Method and Sort Sequence of Meta Key Results).
Sort Order	Displays the Sort Order menu; the currently selected option is displayed in the toolbar. The menu has two options: Sort in Ascending Order and Sort in Descending. The Sort Order is a complement to the Sort Field option; the selected field for each meta key is ordered in ascending or descending order (see Set Quantification Method and Sort Sequence of Meta Key Results)).

Option	Description
Quantification Method	Displays the Quantification Method menu; the currently selected option is displayed in the toolbar. **Note:** The Quantification Method only applies to meta key results. It does not apply to the timeline. The drop-down menu contains three options for calculating the quantity (green number in parentheses) for a meta value: Quantify by Event Count, Quantify by Event Size, and Quantify by Packet Count (see Set Quantification Method and Sort Sequence of Meta Key Results)). These are applied differently depending on the type of data in view. For packet data: • Quantify by Event Count shows the number of sessions. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of packets. For log data: • Quantify by Event Count shows the number of logs. • Quantify by Event Size shows the size in bytes. • Quantify by Packet Count shows the number of logs.
Actions	The Actions menu includes various actions (Visualize, Go To Event, and Print) that you can perform in the Navigate view (see Act on a Drill Point in the Navigate View).
Save Events	Displays the Save Events menu, in which you can use options to: extract files associated with an event, export the current drill point as a PCAP file, and export the current drill point as a log file (see Export a Drill Point).
Search Events	Enables you to search for text patterns within the current set of events. If you click in the Search field, it shows a drop-down menu with search options. If you click Apply, it saves the selected options and also updates the search options in the Events view and the Investigations profile (see Investigation - Search Options).

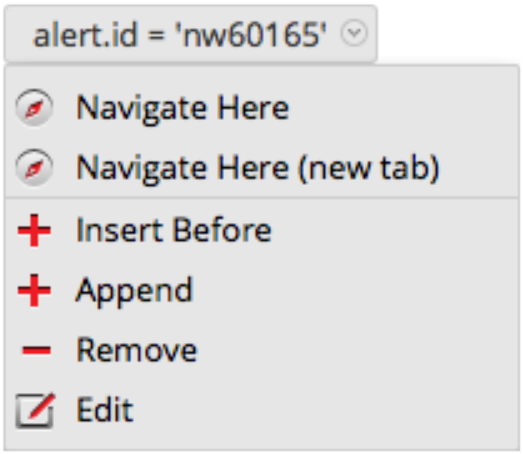
Option	Description
Settings	Displays the Investigation settings for the Navigate view (which are also editable in the Profile view) so that you can change Investigation settings without navigating away from the Navigate view. When you change a setting In the Navigate view the setting is also changed in the Profile view (see Configure Navigate View and Events View).

Pause/Reload Button and Breadcrumb

The breadcrumb tracks each query as you drill down through the metadata for the service. Each query is listed with a drop-down menu in a pipe separated string. The last point is the current point, also called the tip. The icon in front of the breadcrumb allows you to pause the loading of meta values and to reload meta values.

The breadcrumb does not include the service name and appears only if a query is in effect. If too many drill points exist for display, the overflow is shown as double angle brackets, >>, at the end of the breadcrumb.

Each drop-down menu in the breadcrumb is the same, with slight variation based on the position of the crumb.



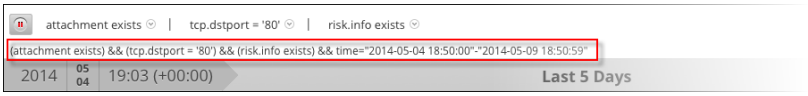
The following table describes the controls and menu options in the breadcrumb.

Feature	Description
Pause	Pause and Reload button. Controls the loading of data in the view. It has three possible functions: pause loading, continue loading, and reload.

Feature	Description
Navigate Here	Opens the selected drill point in the current Values panel.
Navigate Here (new tab)	Opens the selected drill point in a new tab.
Insert Before	Inserts a query before the current drill point. The Create Filter dialog opens and you can define a custom query to insert in the breadcrumb (see Create a Custom Query).
Append	Appends a query after the current drill point. The Create Filter dialog opens and you can define a custom query to append to the end of the breadcrumb (see Create a Custom Query).
Remove	Removes the selected drill point from the breadcrumb.
Edit	Opens the selected drill point in the Create Filter dialog so that you can edit the query.
>>	Clicking the angle brackets displays a drop-down menu of the breadcrumb overflow.

(Optional) Debug Information

If you have activated the Show Debug Information setting and the service you are navigating is a 10.4 or later Broker, Security Analytics displays the debug information beneath the breadcrumb.



The debug information is the `where` clause from the current query. The only time there is no `where` clause is when the time range is all data and there are no drill points. If the Broker has at least one aggregate service that is offline, the debug information also lists the offline service.

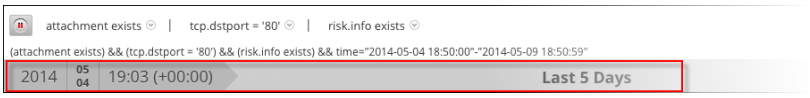
For example:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info
exists)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment
exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-
04 18:50:00"-"2014-05-09 18:50:59"
```

In addition, the time taken to load is displayed at the end of each meta key in the Values panel.

Time Banner

Just below the breadcrumb and debug information (if present), the time banner shows the time range used to create the chart.

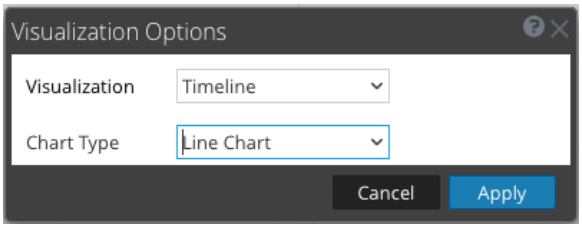


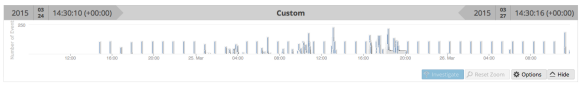
Visualizations

At the top of the Navigate view is a visualization of the current drill point. You can use this to drill into data from the Visualization panel (see Drill into Data in the Navigate View Time Chart). You can show or hide the visualization, and choose one of the the visualization options: Timeline or Coordinates. The Visualization opens initially to the last saved Visualization.

Timeline Chart

The timeline is the count of the number of events that occur at a specific instance. The timeline displays activity for the specified service and time range as a line chart or a bar chart based on your choice in the Options menu. The second figure illustrates a line chart and third figure illustrates a bar chart.



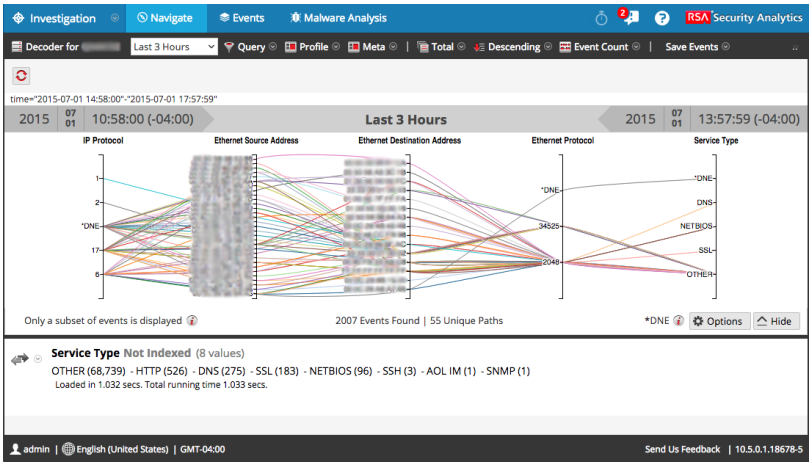


Feature	Description
Number of Events (Timeline)	The Y axis of the chart based on thousands of events.
Time Line (Timeline)	The X axis of the chart based on the time the events occurred.

Feature	Description
Event point (Timeline)	If you want to explore a specific section, simply select the range from the chart. The new time range will be reflected in the chart.
Investigate (Timeline)	Displays the meta values for the selected subset.
Reset Zoom (Timeline)	To return to the original time range, click Reset Zoom.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Hide	Collapses the chart.

Parallel Coordinates Chart

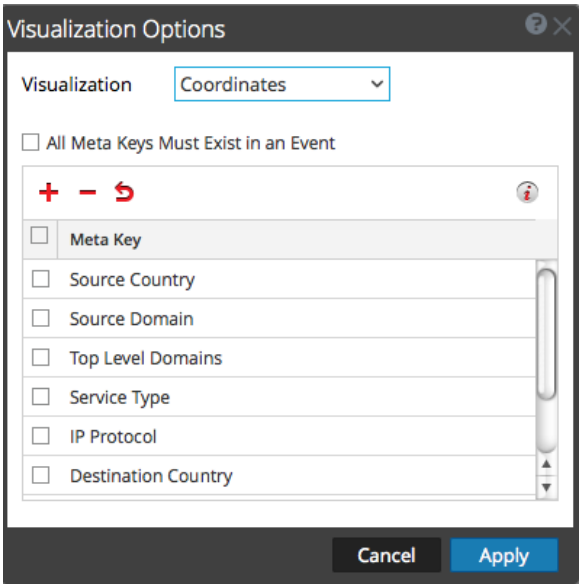
The Parallel Coordinates chart is one of the choices in the Options menu for visualizing the current drill point. With Coordinates selected in the Visualization Options dialog, you can select the meta data to be displayed (see Visualize Metadata as Parallel Coordinates).



Feature	Description
Axes	Each axis is a meta key. The number of meta keys affects the load time for the chart. All meta keys are loaded, but it there the number of events per meta key is limited.

Feature	Description
Lines	Lines represent events and they connect values on the axes to show the correlation between multiple meta keys.
Options	Displays the Visualization Options dialog. Data points can be displayed as a Line chart (default), a Bar chart, or Coordinates chart. When a chart type is select, the relevant options are displayed.
Only a subset of events is displayed.	This message is a notification that not all events in the values panel are drawn in the chart. Removing axes or filtering the data in the Values panel can help to display all events.
Events Found | Unique Paths	Displays the total number of events charted versus the number of unique paths charted. Setting the All Meta Keys Must Exist in an Event option redraws the chart so that it is more targeted and legible.
DNE	Indicates that there is no values for this meta key in the event.

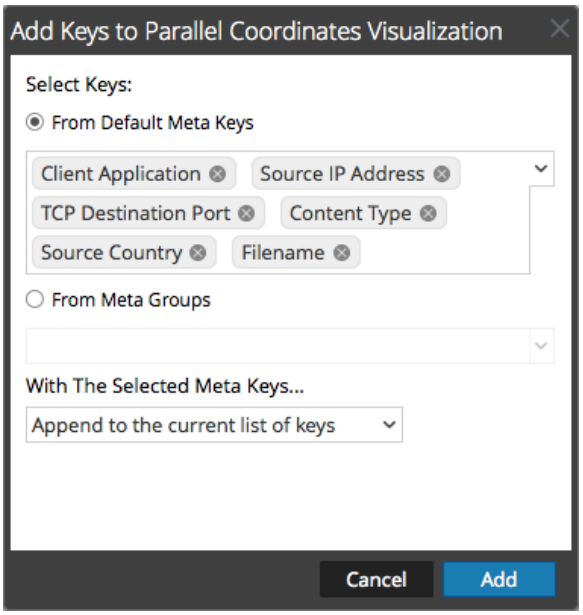
In the Visualization Options dialog for Coordinates, you can select the meta keys to chart.



Feature	Description
Visualization selection	Displays a drop-down list of visualization types: Timeline and Coordinates
All Meta Keys Must Exist in an Event	Limits the data represented in the visualization to only those events that include all selected meta keys. This can result in a cleaner, more targeted visualization.

Feature	Description
+	Displays the Add Keys to Parallel Coordinates Visualization dialog so that you can add axes to the visualization. This is useful if you are looking for relationships between the default meta keys and some additional ones.
−	Deletes the selected keys so that they do not appear as axes in the visualization. This can help to make the visualization less cluttered and allow for more data points to be included in the visualization.
	Reverts to the default meta keys for visualization, which consist of all meta keys in the current drill point.
	Controls the display of additional information about the number of selected axes versus the recommended count. This helps to make you aware of possible performance improvements by removing axes.
Axes	list Lists the meta keys selected as axes in the visualization.
Cancel	Cancels any changes made to the visualization options.
Apply	Saves the changes made to the visualization options and applies to the current visualization.

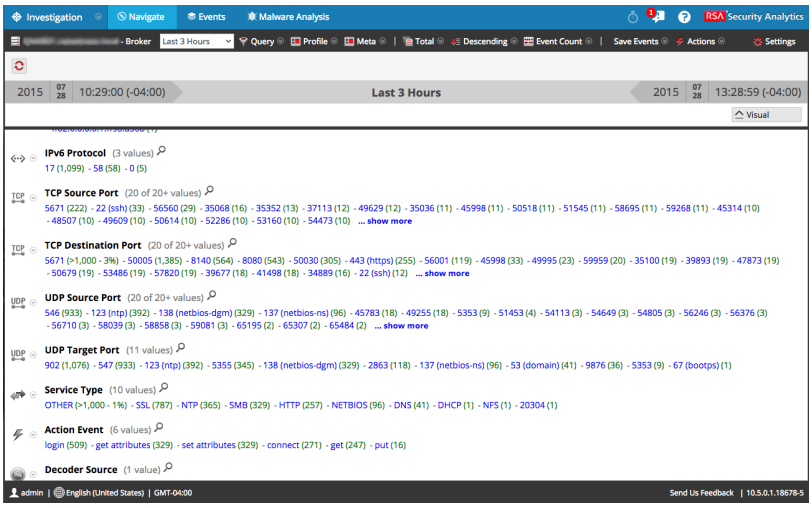
In the Add Keys to Parallel Coordinates Visualization dialog, you can select the meta keys or meta groups to use as axes the Parallel Coordinates visualization.

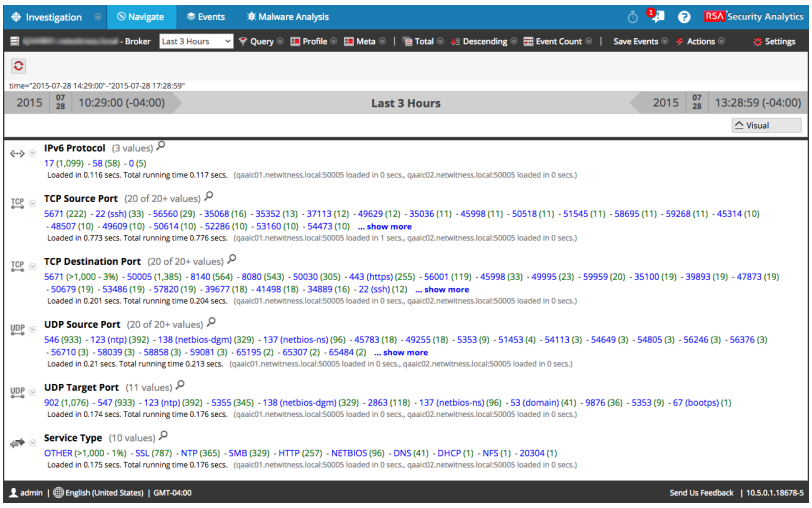


Feature	Description
Visualization selection	Select Keys: Two options for selecting meta keys are: • From Default Meta Keys • From Meta Groups Each option offers a drop-down list from which to select.
With the Selected Meta Keys...	The options for the method of adding meta keys allow you to: • Replace the current list of keys • Append to the current list of keys • Insert at beginning of the current list of keys
Cancel	Closes the dialog and does not add any keys.
Add	Closes the dialog and adds the selected keys as specified.

Values Panel

The major feature of the Navigate view is the Values panel, which you can use to analyze data (see Drill into Data in the Values Panel). The first figure below illustrates the Values panel in normal mode; the second figure illustrates the added information when the Show Debug Information setting is active.





The default view is for the last 3 hours of collection, using the default meta keys and non-indexed meta keys closed. The meta keys within the meta groups are displayed in the order that Security Analytics queries the keys. As the data loads into the Values panel, Security Analytics is optimized to show partial results, loading progress, and service status as the data loads.

The loading behavior is determined by several configuration settings. The highest level settings are configured by the administrator for each user. These are:

- The maximum amount of time allowed for this user to run a query (Query Timeout).
- The limit at which Security Analytics stops counting the number of meta values in a session (Session Threshold). If a threshold is set for a session, the Navigation view shows that the threshold was reached and the percentage of results loaded. Any session that does not show a percentage is accurate and was processed to completion. If there is a percentage, that reflects how much processing was completed. The percentage displayed is estimated by extrapolating from the value at the time processing finished, considering the amount of work remaining. Larger percentages are generally more accurate because they require less extrapolating.

Note: The values for non-indexed meta keys take longer to load in the Values panel. To optimize loading, Security Analyticsdoes not open non-indexed meta keys by default. Refer to Manage and Apply Default Meta Keys in an Investigation for a detailed description of non-indexed meta keys in Investigation.

When you have launched an investigation of a service, Security Analytics displays results in the Values panel.

1. Security Analytics loads meta keys and meta values in the Values panel. For each meta key load, the stages of load are:

a. **Waiting to Be Loaded** or **Closed**. If Closed, no data for that key is loaded.

b. **Loading**

i. **Loading progress**: Security Analytics is receiving and displaying progress messages.

ii. **Partial results**: Security Analytics is receiving values messages and partial results are displayed in the Values panel.

c. **Load Complete**: All results are finished loading.

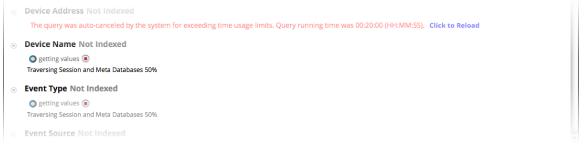
2. As each meta key load is completed, and final values are displayed, the next meta key is started. The number or values rendered for each meta key is specified by the Render Threads value in the Investigation Preference settings. Loading continues until all keys to be loaded have finished.

3. If **Show Debug Information** is active and the service you are navigating is a 10.4 or later Broker, Security Analytics displays load time information beneath the values for each meta key and displays additional load details for the aggregated services. Security Analytics also displays the debug information beneath the breadcrumb.

Iterative results

Iterative results provide feedback on the status of queries within the interfaces to provide additional context for how long the data load will take and if any service data is missing. For example, if you are querying a Broker that is aggregating from two Concentrators, Security Analytics starts displaying the results from the first Concentrator as soon as it is available, even if the second Concentrator is still waiting for results.

Iterative results also include a notification that service data is missing because the service is unreachable.

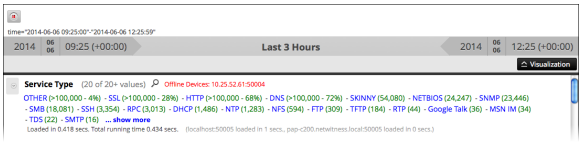


Partial results

When partial values from the Core service are returned but not completed, a message at the end of the meta key listing shows the progress of values loaded. In the example below, Currently looking at 38 ip.src values 71% indicates that loading of values for the meta key is 71% complete.

Debug Information

If the Show Debug Information setting is in effect, a field at the end of the values displays the status for the different systems against which you are querying within Security Analytics. For example, when you are querying against a 10.4 broker pulling from multiple concentrators, Security Analytics displays the status of the query on each of the Concentrators, which provides insight into the relative speed of data loading from each of the Concentrators. Each service that participated in the query is listed with the total elapsed time for the query.



Each service that participated in the query is listed with the total elasped time for the query. In the example above, two services returned in 3.207 seconds, localhost:50005 took 2 seconds to return the results. In addition, the where clause of the query is displayed below the breadcrumb. You can copy this syntax directly into an application rule or Reporting where clause of a rule.

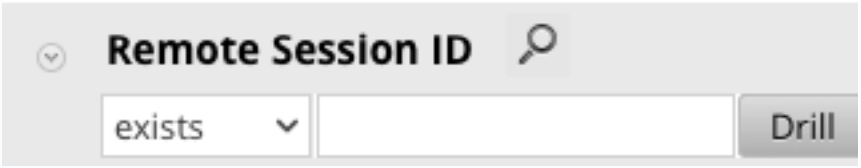
Load Complete

This is an example of values that have finished loading.

For each meta key, there is a list of values (blue text) and counts (green text) found in the current drill point. When you click a value to drill down into a subset of the currently selected data, the display is updated and the new drill point is recorded in the breadcrumb. You can specify the sorting and quantification methods for the values list using the option in the toolbar.

Note: Title, values, and counts for non-indexed meta keys are not drillable; the Values and counts are shown in black. Refer to Manage and Apply Default Meta Keys in an Investigation for a detailed description of non-indexed meta keys in Investigation.

Feature	Description
Meta Key	The name of the meta that is listed, for example, **Service Type** is a meta key.
Number of values rendered vs number of values available to load	The number or values rendered is specified by the Render Threads value in the Investigation Preference settings. In the example above, the meta key is **Service Type**, and 20 of 20+ values are currently displayed. You can display additional values by clicking **...show more**.

Feature	Description
	Clicking  on an indexed meta key opens the Search dialog in which you can enter a filter for the current meta key. The search function is not available for non-indexed meta keys, and is based on the actual meta value rather than the alias. Drilling in the Search dialog using aliases is not supported. NOTE: Check with your administrator to obtain a list of aliiases used for a meta key in Investigation. When an alias is used, this search dialog does not provide results. Instead, you must query the meta key using the Right-click query capability or the Query dialog. 
Offline Services: xxx.xxx.xxx.xxx:5000-4	Lists offline services queried by a 10.4 Broker.
Meta Count, for example (77)	The number of instances found for a particular meta in the session.
Meta Value, for example set attributes	The specific name associated with the found meta.
...show more	If the number of meta values has been limited (for example, 20), clicking this displays additional meta values for the selected meta key.
Loaded in 0.418 secs. Total running time 0.434 secs. (localhost:50005 loaded in 1 secs....	Debug stats display load times based on the Show Debug Information setting.

Meta Key Context Menus

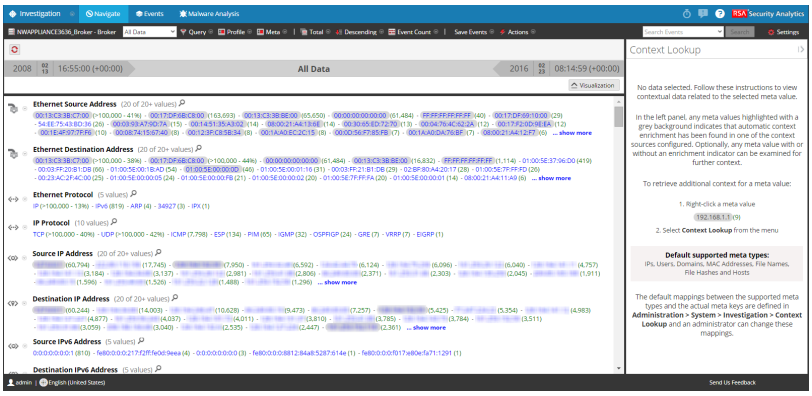
The Meta Keys in the Values panel have context menus. Next to each meta label, a drop-down arrow displays the options that can apply to that item. You can use these to change the way the results for the meta key are displayed in the current view. Changes made to meta keys are displayed in the current view during drill points persist until you refresh the page or select a new service in the Navigate view toolbar. Manage and Apply Default Meta Keys in an Investigation refresh reverts the current view of meta keys as defined in the Manage Default Meta Keys dialog (see Manage and Apply Default Meta Keys in an Investigation). If you have never made modifications in the Manage Default Meta Keys dialog, Security Analytics restores the default meta keys from the core service.

- More Results
- Max Results
- Hide Results
- Meta Key Info

Context Lookup Panel

With the addition of a new Context Hub service , the Navigate view has a panel on the right side called the Context Lookup panel. The Context Lookup panel is displayed only if you have installed and configured the Context Hub service. For more information on configuring the Context Hub service, see the *Context Hub Configuration Guide*.

The Context Lookup panel displays relevant data when an analyst looks up contextual data for a meta value in the Values panel.

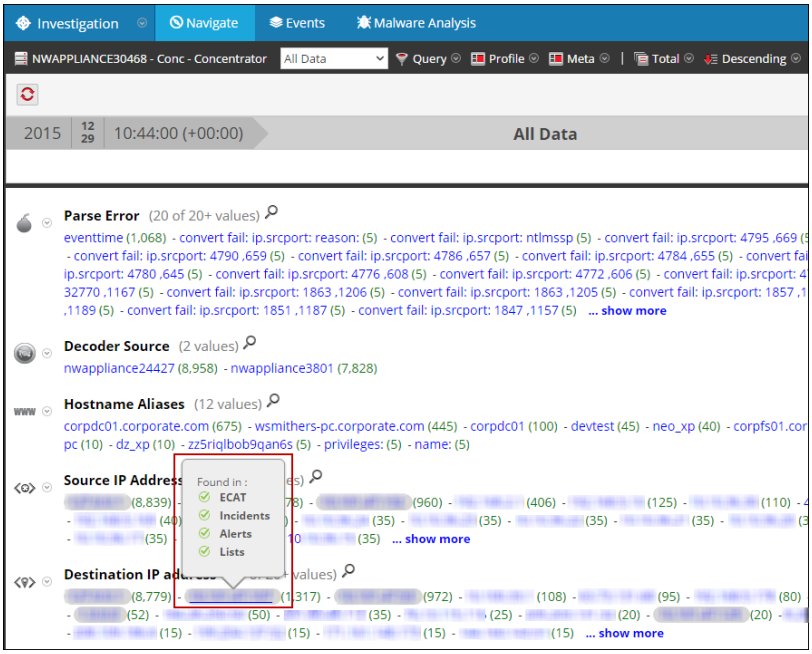


After the administrator configures the Context Hub service, you can view the contextual information for the meta values in the Navigate view and the Events view. For more information on configuring the Context Hub service, see the *Context Hub Configuration Guide*.

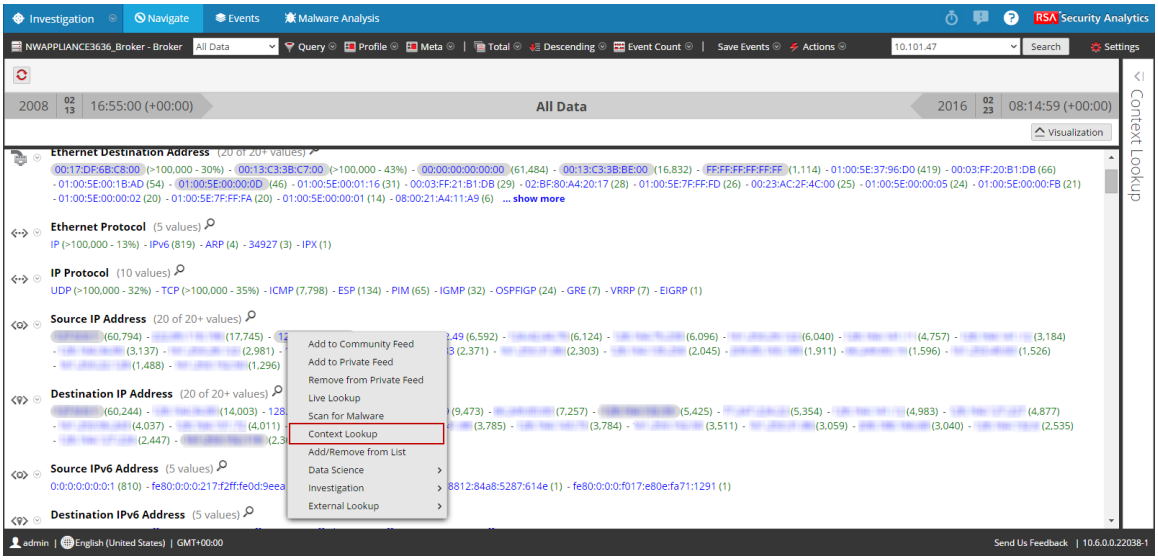
For information about performing Context Lookup for meta values, see View Additional Context for a Data Point.

The Context Hub service is pre-configured with default meta type and meta key mapping. For information about the mapping of the context hub meta value with investigation meta key, see "Manage Meta Type and Meta Key Mapping" in the *Context Hub Configuration Guide*

You can view the type of context data that is available for a highlighted meta value by hovering the mouse over a highlighted meta value. An inline indicator shows which type of context data is available for the meta: ECAT, Incidents, Alerts, or Lists.



Right-clicking a meta value opens a menu with the context lookup option. The following figure illustrates the Context Lookup option when you right-click a meta value.



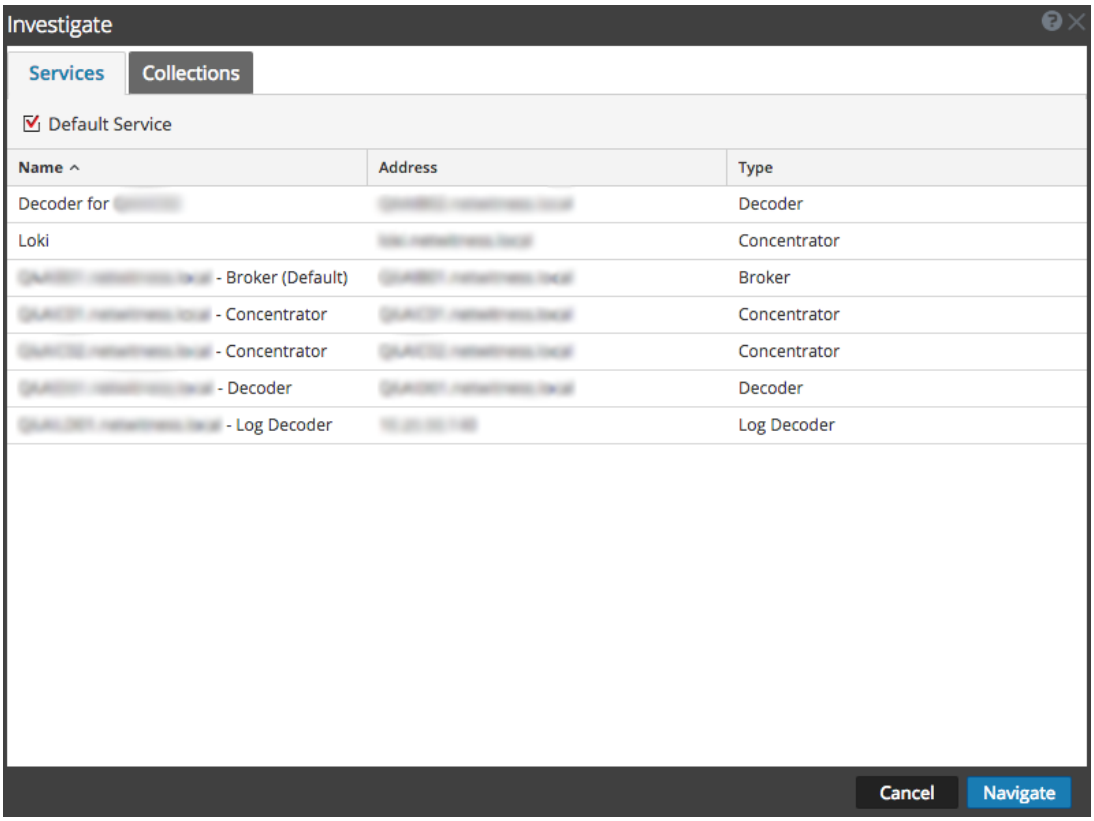
For more information about the lookup results and contextual information for different data sources, see Investigation - Context Lookup Panel.

Investigation - Query Dialog

In the Investigation > Navigate view or Events view, you can create a query rather than clicking through the meta keys and values to drill down into the meta data. The dialogs for creating a query offer syntax help with drop-down lists of applicable meta keys and operators. Related procedures are available in Query Data in Navigate View.

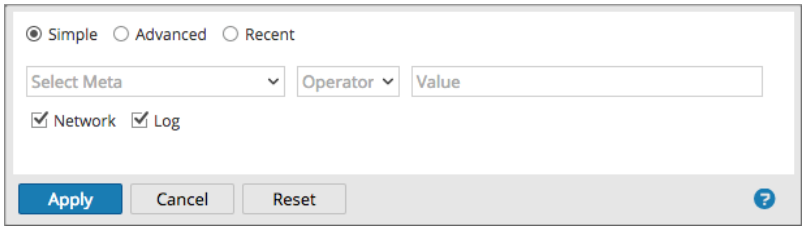
To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**. Both views provide access to the Query dialog.
   The Investigate dialog is displayed.



2. Select a service, then click **Navigate**.
3. In the toolbar, select **Query**.

The Query dialog is displayed.



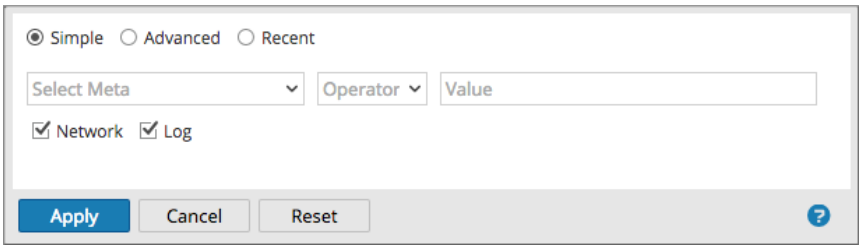
Features

The Query dialog has three views:

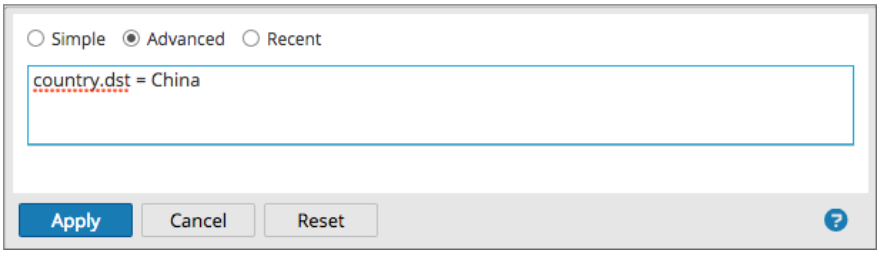
- Simple
- Advanced
- Recent

In the Simple view, you can create a query using the options displayed in the dialog. In the Advanced view, you can create a query without guidance. In the Recent view, you can select a query from a drop-down list of recent queries.

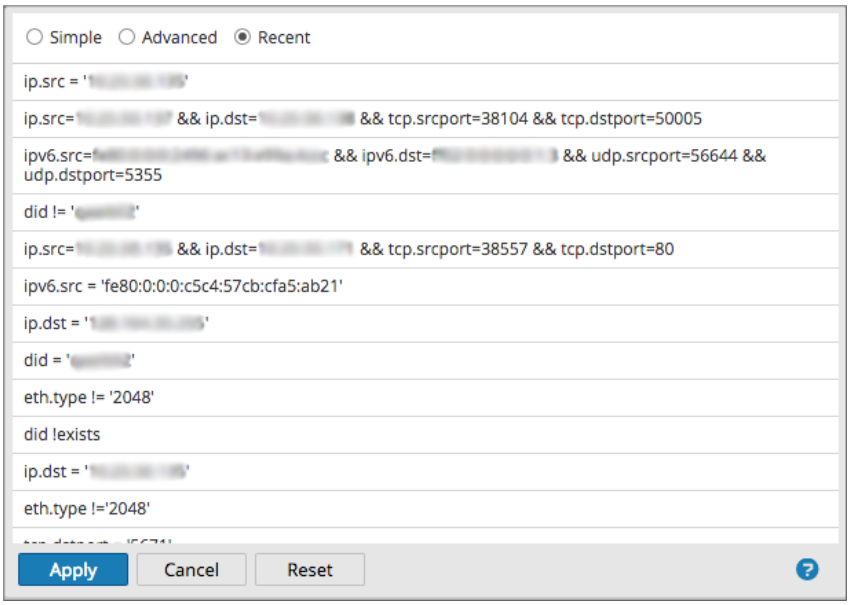
Simple View



Advanced View



Recent View



The following table describes of theQuery dialogs.

Feature	Description
Select Meta	Displays a drop-down list of meta groups.
Operator	Displays a drop-down list of operators `(=, !=, exists, !exists)`
Value	Allows you to enter a value to complete the query.
Network	Limits the query to packets if Log and Endpoint are not selected.
Log	Limits the query to logs if Network and Endpoint are not selected.
Endpoint	Limits the query to endpoint if Network and Logs are not selected.
Query box	Allows you to enter a query in the Advanced view. When you begin typing, a drop-down list of available meta keys for the service is displayed, then a drop-down of operators is displayed as you type. If the expression currently entered in the query box is invalid, a warning appears near the box. When the query is valid, the warning is removed.

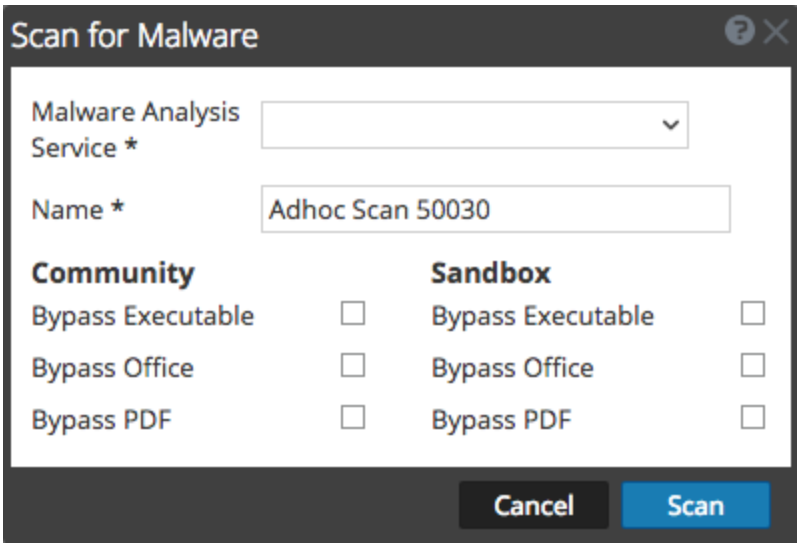
Feature	Description
Query list	Allows you to select a query from a list of recent queries in the Recent view. Double-clicking a query automatically applies it.
Apply	Applies the new query to the current Investigation view.
Cancel	Closes the dialog without applying changes.
Reset	Resets all fields.

Investigation - Scan For Malware Dialog

In the Scan for Malware dialog, Malware Analysis analysts can upload files to investigate in Malware Analysis.

To access this dialog:

1. In the **Security Analytics** menu, select **Investigation > Malware Analysis**.
   The Select a Malware Analysis Service dialog is displayed.
2. Select a service in the left panel, then click Scan Files in the right panel.
   The Scan for Malware dialog is displayed.



Related procedures are available in Conduct Malware Analysis.

Features

The following table describes the features available in the Scan for Malware dialog.

Feature	Description
+	Uploads a file from your computer.
−	Deletes a file from the list.
File Name	Displays the names of the files added to the list.

Feature	Description
Name	Allows you to name the scan job.
Community	Displays options for Community to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Sandbox	Displays options for Sandbox to bypass or ignore certain types of files: • Bypass Executable • Bypass Office • Bypass PDF
Cancel	Closes the dialog without performing any actions.
Scan	Scans the uploaded files.

Investigation - Search Options

You can search for events in both the Investigation Navigate view and the Events view. In the Navigate view, you can click a meta value, such as HTTP, to drill into the data and then enter a search string in the Search field to search for events within that subset of data. The search opens a tab in the Events view, brings your drill and time range forward, and shows your search results. You can also drill into the data using queries before starting a search.

Procedures related to searching in Investigation views are described in Configure Navigate View and Events View, Filter and Search Results in the Events View, and Drill into Data in the Values Panel.

The Investigation Navigate and Event views enable you to search for text patterns within the current set of events. You can perform a keyword text search or do regex (Regular Expression) matching.

Keyword Text Search

The text search provides these capabilities:

- Each whitespace delimited word is ANDed, so that every word must be found, but the order or location position in relation to the other words is irrelevant. For example, if you search on `Mark Albert`, both Mark and Albert must be found in the session, but they need not be together or in any specific order.
- The word OR is special. If you search `Mark OR Albert`, either Mark or Albert must be found in the session to match; both are not required.
- You can mix or match implicit ANDs and ORs together in the search string. The explicit OR has higher precedence than the implicit (whitespace) AND. The following examples make the same logical statement, which requires that both the terms cheese and dumplings be present in a match and one of toast or bread:

  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```

- You can exclude words from search results using the - operator. For example, searching for `cheese -toast` would return any result that has the word cheese, unless the word toast is also present.

- The keyword search can match metadata stored in the following patterns:
  - **IPv4 and IPv6 addresses**. Any term that can be recognized as an IP address will be converted to the native metadata format so that it can be found in indexed metadata.
  - **IPv4 CIDR ranges**. You can use CIDR notation to locate IPv4 addresses within a range.
  - **Timestamps**. Timestamps are matched against the native time meta, and any additional time meta fields stored with the Time type.
  - **Numbers**. The search function will attempt to automatically identify decimal search terms and match them against numeric meta data fields.

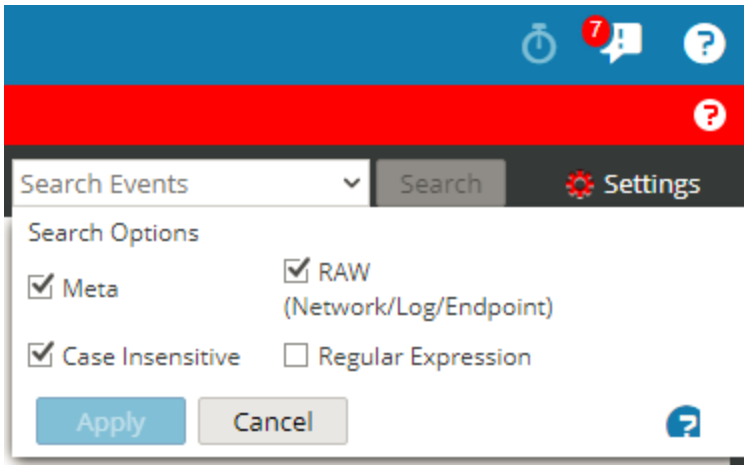
Options Controlling Search Behavior

To access the Search box and search options in the Navigate or Events views:

1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**.
2. In the Investigate dialog, select a service and click **Navigate**.
   You can see the Search Events field in the toolbar.

   Troubleshooting: If you cannot see the Search Events field in the toolbar, click ⋯ on the right side of the toolbar.

3. Click in the Search field to view the Search Events drop-down menu.



The options selected in this box change how the search is executed. The default search mode is to use the search indexes for text keywords within meta and raw.

Note:
Because the **Search Indexes** checkbox is selected by default, the search returns results based on data that is indexed.
If you want to search for a complete set of meta or raw data, select those checkboxes and clear the **Search Indexes** checkbox. There is no specific search order. The search will take longer, but it will contain a more complete set of data.
For more information, see the **Msearch call** topic in the *Core Database Tuning Guide*.

The following table describes the Investigation search options.

Feature	Description
Search Indexes	Searches the indexes first, before scanning the meta data or any raw data. Searching the index is the fastest way to locate keywords within a large data set. The index search utilizes any relevant indexes present within your data collection. **Caution:** - The index search only returns results on indexed data. - Substring matches will not be located by index searches. If you require substring matches, clear this checkbox and use a non-index search mode.
Meta	Searches the metadata. Your keyword or regex pattern will be matched against any parsed meta data.
RAW (Network/Log/Endpoint)	Searches the log text. Every event is decoded and content is searched for matches on the keyword or regex pattern. If you select all data with no filters on an Archiver, execution time may be excessive and a warning may be displayed. **Caution:** Searching raw network sessions causes sessions to be decoded, which is very time intensive. You may want to disable raw searches when looking at network-only collections.
Case Insensitive	Ignores case when searching.

Feature	Description
Regular Expression	Searches using a Perl regular expression, rather than text. By default Security Analytics executes a text search. To execute a regular expression search, select the Regular Expression option. **Caution:** - Regular expression searches can be very slow. - When combining regular expressions and index search options, the regular expression pattern is matched against unique index values instead of meta values. This produces results faster, but it is not an exhaustive search of all the meta data or raw data.
Apply	Sets the default search options to apply to a search in the Navigate and Events views. This also updates your Investigation preferences in your Profile (Profile > Preferences > Investigation tab). The preferences are saved and effective immediately. You can select search options to use for a particular search without changing your default search preferences.

Regular Expression Search Syntax

A regular expression search uses Perl regular expression syntax, which is documented in detail in http://perldoc.perl.org/perlre.html.

Raw Text Keyword Search (new for 10.6)

The Log Decoder has the capability to create a raw text index for unparsed log events. This functionality creates metadata items that form a full-text index on downstream services such as Concentrators and Archivers. When you enable the Search Indexes option in your search preferences, your search automatically utilizes the text index. Note that the text index produces meta items that have a coarse granularity. For example, the default text indexer configuration truncates text terms. By comparing the index matches against raw data, the search engine will find accurate results for your search. However, you can improve search times by disabling the raw search checkbox. If you do so, results will be returned faster, but you may see false positive hits in your search results.

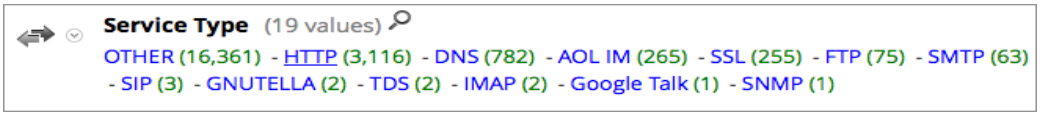
Search Examples

The following examples show searches from the Navigate and Events views.

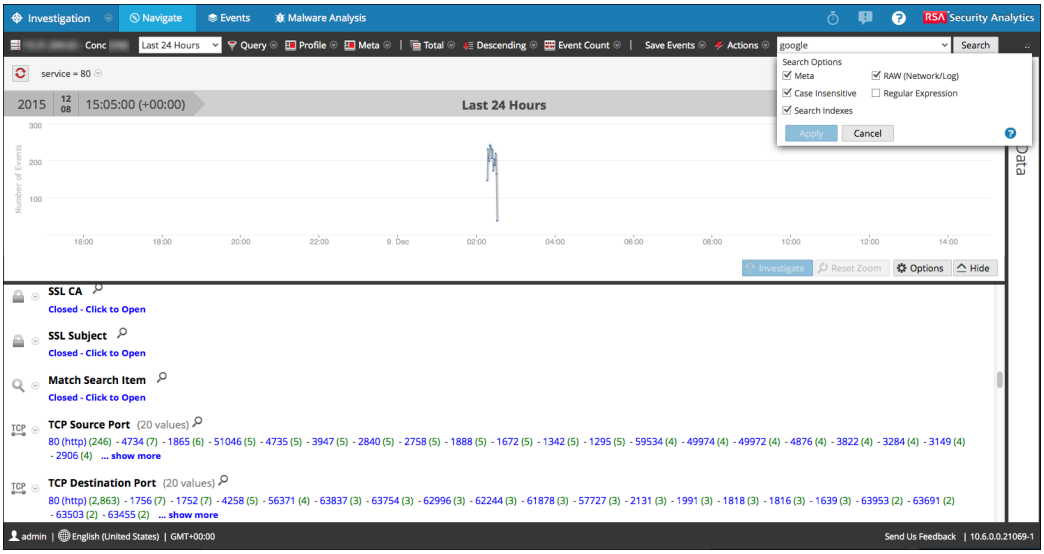
Search in the Navigate View

To search within the currently displayed data in the Navigate view:

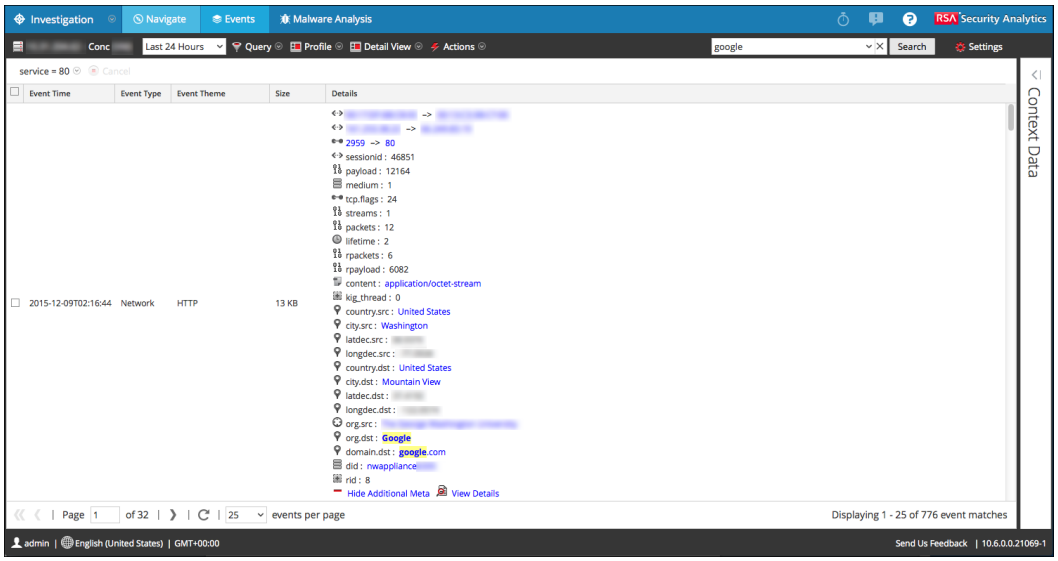
1. To drill into the data, click a meta value, such as HTTP, in the Navigate panel.



2. Type a search string in the Search field and press **Enter** or click **Search**.



The following example shows search results for the **google** search string in a new tab in the Events view. The drill (query) and time range from the Navigate view are brought forward into the Events view (**service=80** and **Last 24 Hours** in this example).

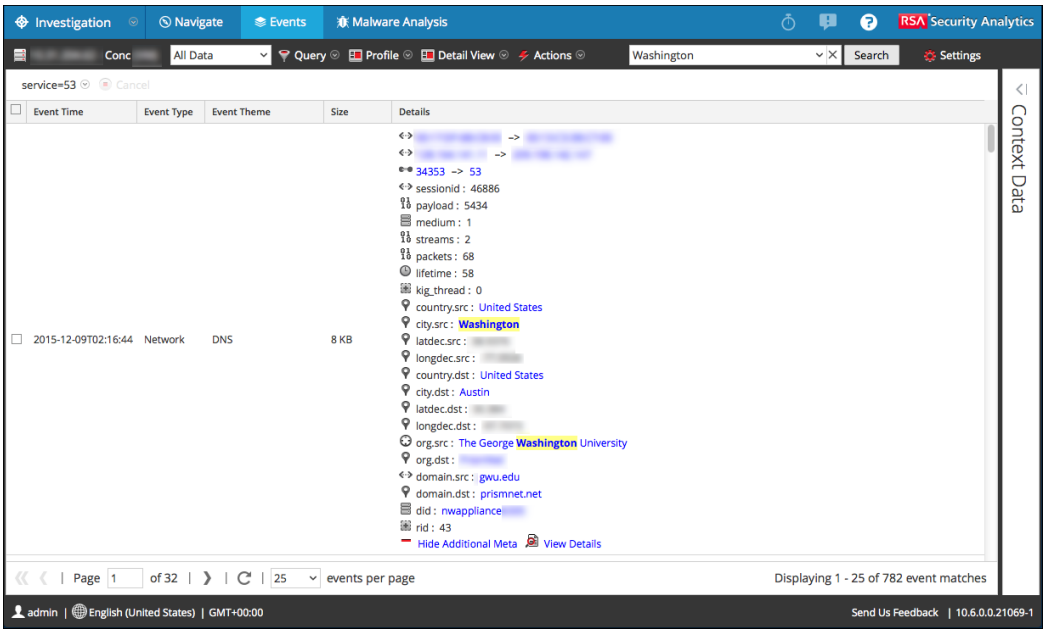


3. To clear the search box and return to the normal Events view, click the **X** in the search box.

Search in the Events View

To search within the currently displayed data in the Events view:

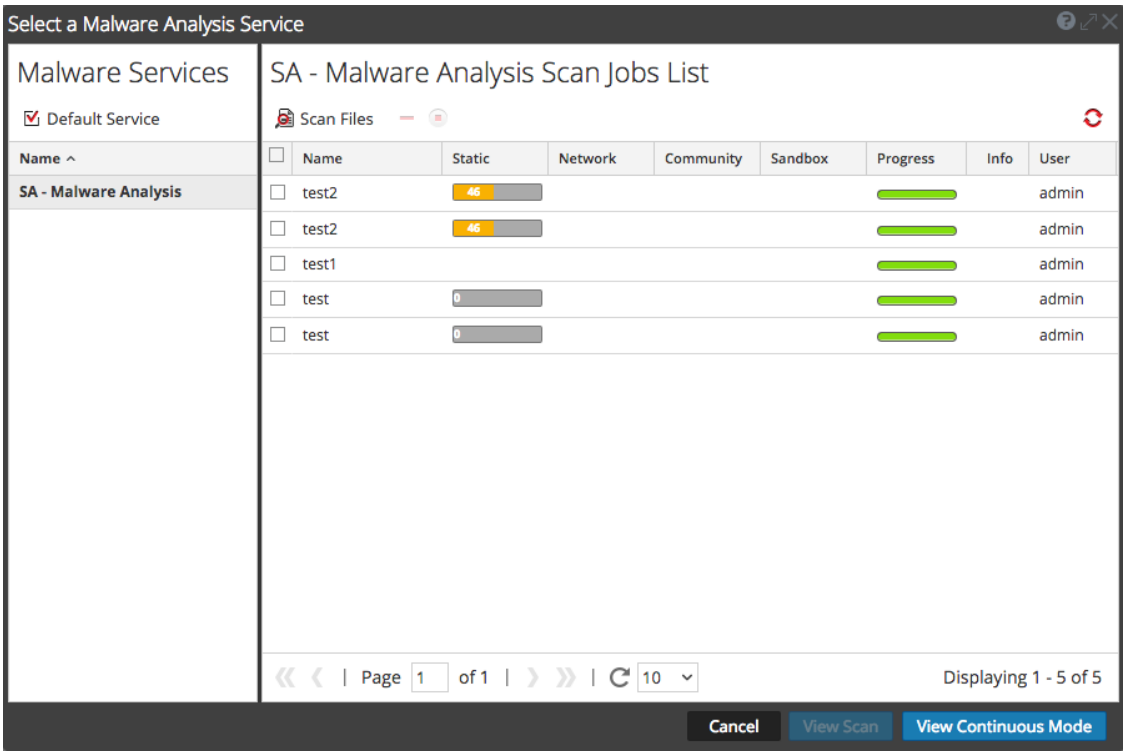
1. Type a search string in the Search box, and press **Enter** or click **Search**.
   The search results are displayed in the Events view. Events that match the search criteria are displayed in the Event view grid. In the Details view and List view, matches are highlighted in the Details column. In addition, when searching RAW, matches are highlighted in the Log view Logs column. Below is an example of the search results for the search term **Washington** in the Events Detail view. Note that search matches are not highlighted in any Event Reconstruction.



2. If you want to narrow the search, change the query and time.
3. If you want to stop the search and return to the Events view, click **Cancel**.
   Any results that are displayed remain.
4. To clear the search box and return to the normal Events view, click the **X** in the search box.

Investigation - Select a Malware Analysis Service Dialog

The Select a Malware Service dialog is accessible in the Malware Analysis view. In this dialog, Malware Analysis analysts can select a service to investigate, choose a scan on that service to investigate, and upload a file to investigate in Malware Analysis.



Features

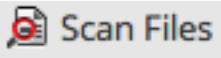
The Select a Malware Analysis Service dialog has a Malware Services panel on the left and a Scan Jobs List on the right. The Scan Jobs List panel has a toolbar, list, and buttons to view scans.

Malware Services Panel

The Malware Services panel is a list of services available for malware analysis. In this panel, you can select the service to investigate and you set a default service using the Default Service icon. When you select a service, the available scan jobs for that service are listed in the Scan Jobs list.

Scan Jobs List Toolbar

These are the features in the toolbar.

Feature	Description
	Displays the Scan for Malware dialog, in which you can upload a file to the service for scanning.
Delete scan job ( )	Deletes one or more selected scan jobs, Security Analytics displays a confirmation dialog before deleting scan jobs.
Cancel scan job ()	Pauses or continues one or more scan jobs.
Refresh ()	Refreshes the list of scan jobs.

Scan Jobs List

These are the columns in the Scan Jobs list. This list is also available in the Malware Scan Jobs dashlet.

Feature	Description
Name	Displays the name of the job.
Static, Network, Community, Sandbox	Filters the results based on the scores for each scoring module.
Progress	Displays the current progress made on the job. • Green: The job is finished. • Black: The job is in progress. • Red: An error occurred.
Info	Provides additional information. Displays the query for the job. If the job is not complete, it also displays more detailed description of the status.
User	Displays the name of the user who created the job.

Feature	Description
Events	Counts the number of events for the job.
Dropped	Counts the number of files/events in the job that were dropped because the scores are below their configured threshold.
Event Type	Displays the type of job: Manual Upload, On Demand, or Resubmit.
Scheduled	Displays the date and time when the job was executed.

Actions

These are the available actions in the dialog.

Feature	Description
Cancel button	Cancels the selected scan job.
View Scan button	Displays the Summary of Events for the selected scan with the default dashlets displayed.
View Continuous Mode button	Displays the Summary of Events for the selected scan with the default dashlets displayed.

Investigation - Settings Dialog for Navigate View and Events View

The settings in the Navigate view and Events view Settings dialogs are a subset of the Investigation settings made in the Profiles > Preferences panel > Investigations tab. By providing the settings within the Investigation view, Security Analytics saves time for Analysts. If you change a setting here, the same setting is changed in the Profiles view, and if you change a setting in the Profiles view, the same setting is changed here.

To access this dialog:

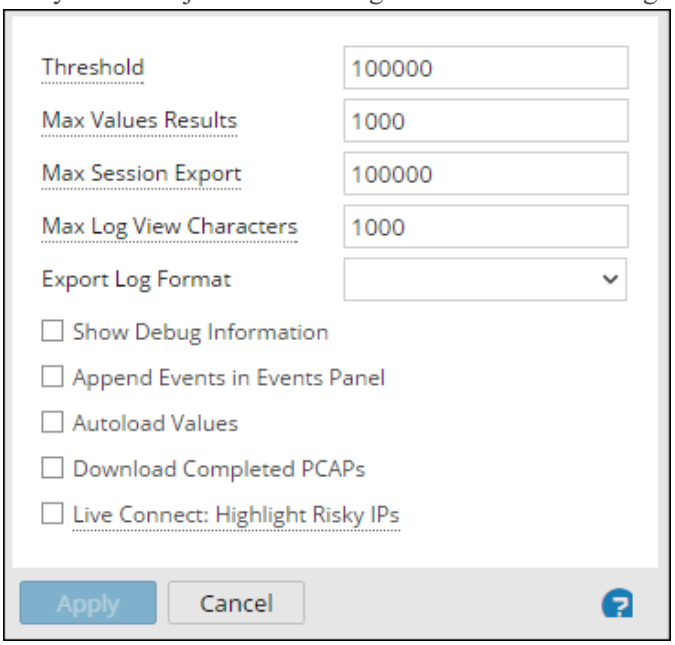
1. In the **Security Analytics** menu, select **Investigation > Navigate** or **Events**.
   The Investigate dialog is displayed.
2. Select a service and click **Navigate**.
3. In the toolbar, select the **Settings** option.
   The Settings dialog is displayed.

Features

The Settings dialog in the Navigate view and Events view have several features in common.

Navigate View Settings Dialog

Several Investigation settings influence the performance of Security Analytics when loading values in the Values panel. Default values are set based on common usage, and individual analysts can adjust these settings for their own investigations.



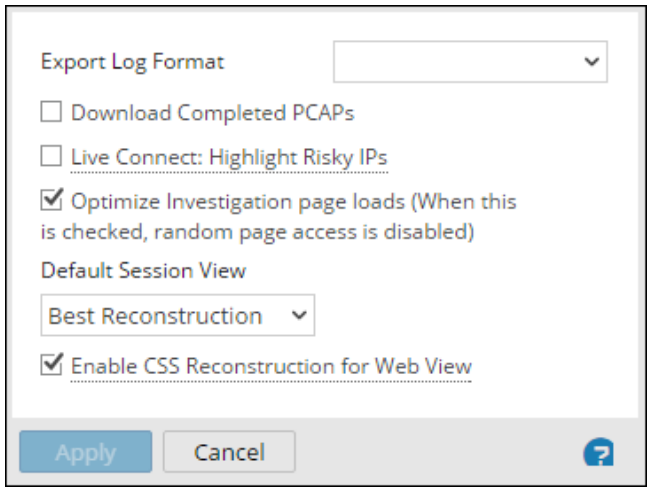
The following table describes the features.

Feature	Description
Threshold	Sets the threshold for the maximum number of sessions loaded for a meta key value in the Values panel. A higher threshold allows accurate counts for a value, and also causes longer load times. The default value is **100000**.
Max Values Results	Sets the maximum number of values to load in the Navigate View when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The default value is **1000**.
Max Session Export	Sets the maximum number of sessions able to be exported. The default value is **100000**.

Feature	Description
Export Log Format	Sets the file format of exported logs. There are four formats available: • Text • SML • CSV • JSON
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • Text • SML • CSV • JSON
Show Debug Information	If you want Security Analytics to display the `where` clause beneath the breadcrumb in the Navigate view and the elapsed load time for each aggregated service on a Broker, check this option. The default value is **Off.**
Autoload Values	If you want Security Analytics to automatically load values for the selected service in the Navigate view, check this option. When not selected, Security Analytics displays a **Load Values** button, allowing the opportunity to modify options. The default value is **Off**.
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigation module so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form.
Live Connect: Highlight Risky IPs	If you want Security Analytics to highlight and display only IP addresses that are considered as risky by RSA community, check this option. When not selected, Security Analytics displays all IP addresses. By default, this option is not selected (**Off**).

Feature	Description
Apply	Applies the settings immediately and they are visible the next time you load values. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.

Events View Settings Dialog



The following table describes the features.

Feature	Description
Export Log Format	Sets the file format of exported logs. There are four formats available: • Text • SML • CSV • JSON

Feature	Description
Export Meta Format	Sets the file format of exported meta values. There are four formats available: • Text • SML • CSV • JSON
Download Completed PCAPs	This setting automates the downloading of extracted PCAPs in the Investigation module so that you do not have to manually download and open extracted PCAP files in an application, such as Wireshark, that can handle viewing data in a PCAP form.
Live Connect: Highlight Risky IPs	If you want Security Analytics to highlight and display only IP addresses that are considered as risky by RSA community, check this option. When not selected, Security Analytics displays all IP addresses. By default, this option is not selected (**Off**).
Optimize Investigation page loads	Sets a paging option. When optimized, results are returned as quickly as possible, sacrificing the original ability to go to a specific page in the event list. Unchecking this box changes the Events list pagination to allow you to go to a specific page in the list (or to the last page). The default value is **enabled**.
Default Session View	Selects the default reconstruction type for the initial reconstruction in the Events view. The default value is **Best Reconstruction** in which events are reconstructed using the reconstruction method most appropriate to the event.

Feature	Description
Enable CSS Reconstruction for Web View	This setting controls how web content reconstruction is performed. If enabled, the web reconstruction includes cascaded style sheet (CSS) styles and images so that its appearance matches the original view in a web browser. This includes scanning and reconstructing related events, and searching for style sheets and images used in the target event. The option is enabled by default. Uncheck this option if there are problems viewing specific websites.
Apply	Applies the settings immediately and they are visible the next time you view events. The same changes are also applied in the Profiles view.
Cancel	Cancels the editing operation and closes the dialog, leaving the settings unchanged.