RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness® Platform 11.4

Contact Information

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

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

September 2020

Contents

What's New

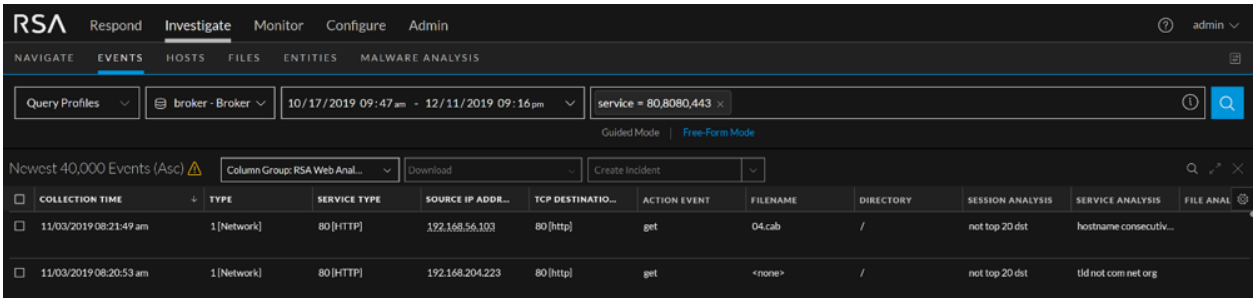
The RSA NetWitness® Platform 11.4 release provides new features and enhancements for every role in the Security Operation Center. The RSA NetWitness Platform 11.4 release delivers expanded platform-wide detection and analyst usability improvements to make it easier for analysts to find and respond to threats that target their enterprise, with improvements to Investigate functionality, expanded nodal visualization of incidents in Respond, and new distributed analyst user interfaces that can be deployed across multiple geographic locations to reduce latency.

The following sections are a complete list and description of enhancements to specific capabilities:

Investigation - SIEM and Network Traffic Analysis

Streamlined Workflow to Analyze Events

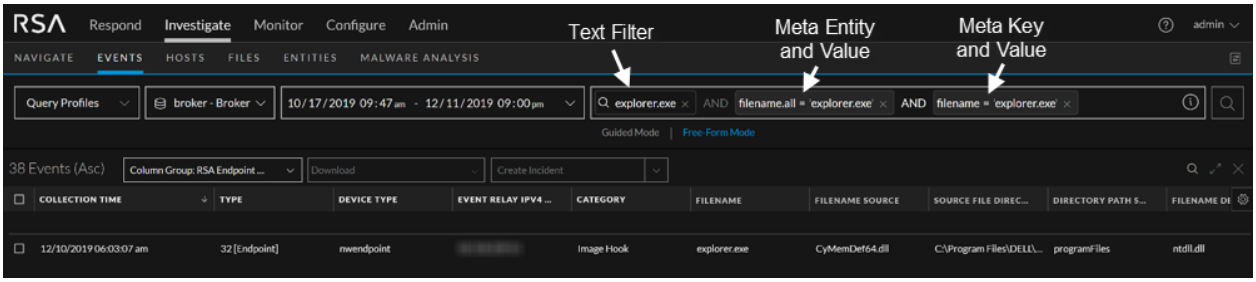
The default workflow for analysts interacting with events is optimized to limit the need to transition from one view to another. By combining capabilities (highlights spelled out further in this document) that were previously in two distinct workflows, referred to as Event Analysis and Events, the analyst now has a single workflow for analyzing events. By default, the previous workflow is not in the Investigate menu, but an administrator can re-enable it if they desire a transitional period for existing analysts. For more information, see How NetWitness Investigate Works.



Text Search Filter in a Query

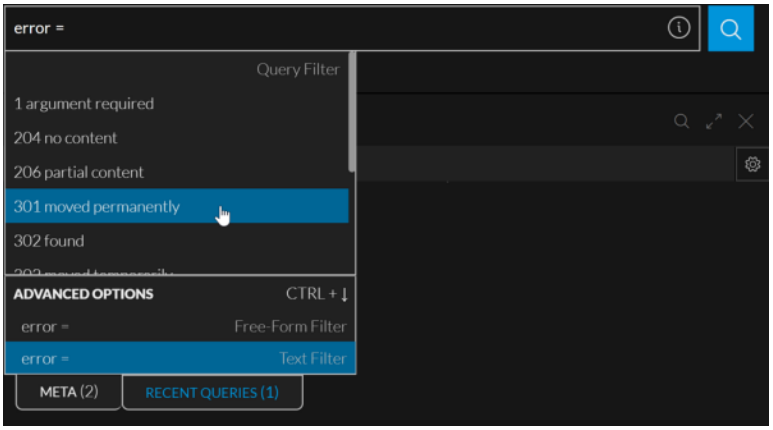
Analysts create filters and submit queries to limit the set of events being viewed. Usually this requires knowledge of meta keys; however, a text filter is useful when you have some idea of what you are looking for, but are not sure where to look (which meta key). The text filter initiates a case-insensitive search against all the data for meta keys that are indexed by value. As an example, if you are interested in looking for a file name, click in the query bar, type the complete text string, and click **Text Filter**. The text filter initiates a search against all the data in the index, within the services and time range being investigated, and returns exact matches to the text string.

The figure below illustrates the multiple ways for an analyst to search for a value. The use of a text filter requires no knowledge of the meta keys. Use of meta entities requires limited knowledge of several high level meta keys, while using a specific meta key associated to the value requires further knowledge of the available indices. For more information, see "Add a Text Filter to Find a Value Anywhere in the Data Set" in Filter Results in the Events View.



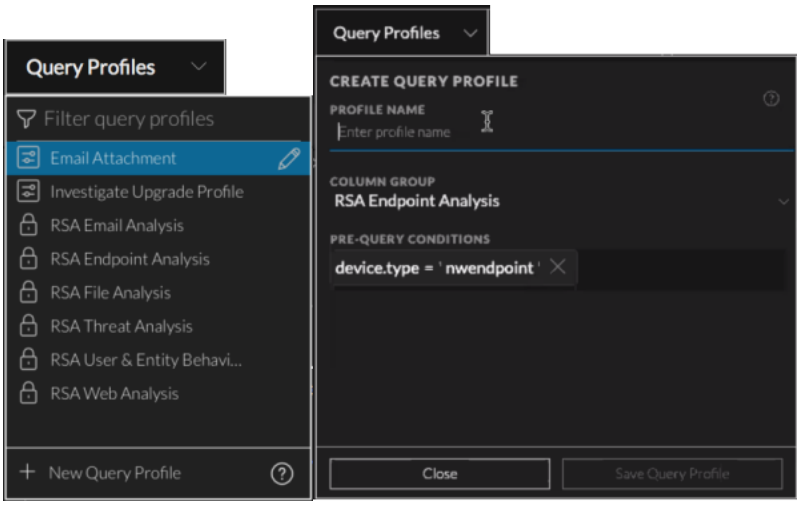
Auto-Suggestion of Meta Values While Constructing a Query

When constructing a query in the Events view query bar, knowing a meta value or the format of that meta value is not always intuitive. When analysts are typing a query, auto-suggestion of values helps them construct queries relevant to the data in their environment without requiring prior knowledge of the data. For more information, see "Build a Query in Guided Mode" in Filter Results in the Events View.



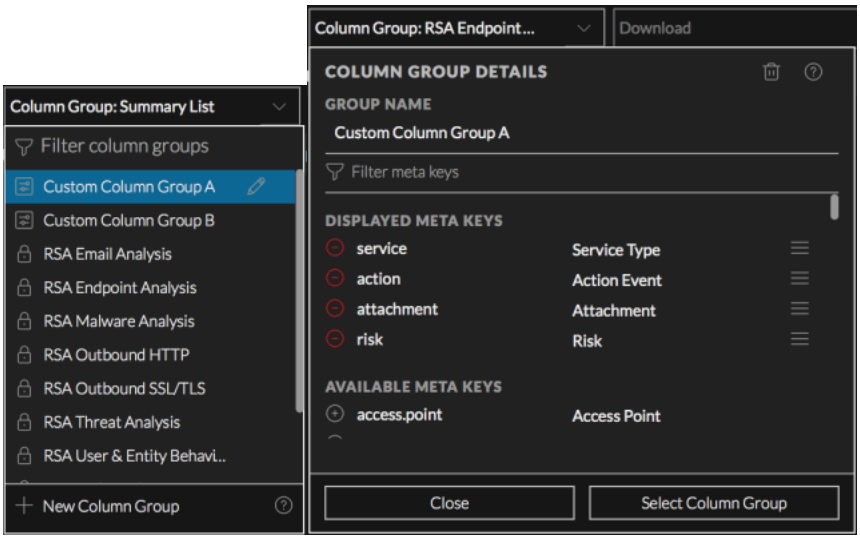
Query Profiles in the Events View

Analysts working in Investigate can refine results using column groups and filters in the query bar. When analysts find a column group or filter useful, they can save it as a query profile for reuse. To get started, beginning analysts can apply the built-in query profiles for common types of investigation. As they gain experience, analysts can create, edit, delete, and save custom query profiles. Both built-in profiles and custom profiles are globally available to all analysts. For more information, see Use Query Profiles to Encapsulate Common Areas for Investigation.



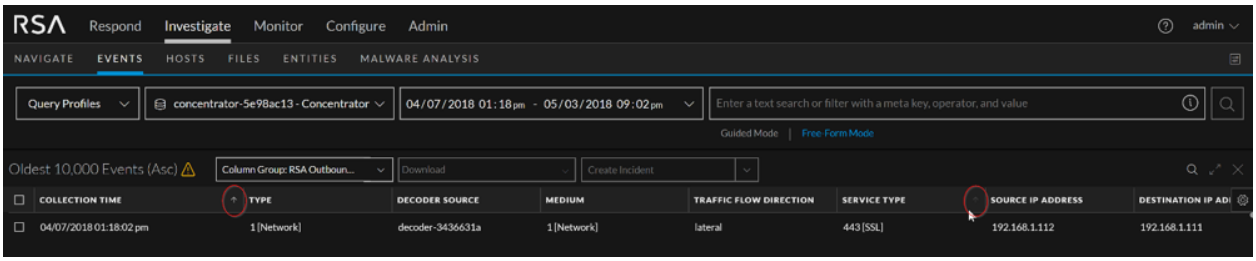
Custom Column Groups in the Events View

When analysts investigate and examine thousands of events, they can use and manage built-in or custom column groups to provide the desired results layout for specific investigation scenarios. Analysts can also manually select columns that identify patterns for certain types of investigation. Saving that set of columns as a custom column group makes it available for reuse. Custom column groups are available globally and editable by every analyst. For more information, see Use Columns and Column Groups in the Events List.



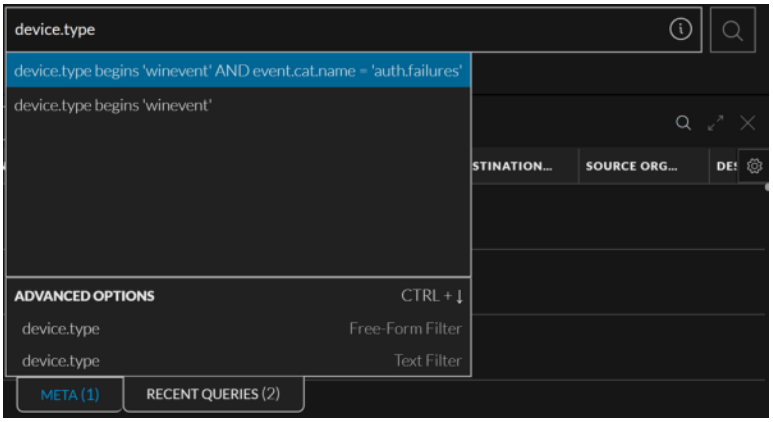
Sort Results in the Events List

Analysts viewing events in the Events view can sort events by selecting a sortable column and the direction of sorting. One use case is this: having retrieved a set of events that are sorted by default on collection time (meta key = `time`), analysts can sort by another column, for example, source IP address (meta key = `ip.src`) to determine which events had similar connections in the time range queried. For more information, see Use Columns and Column Groups in the Events List.



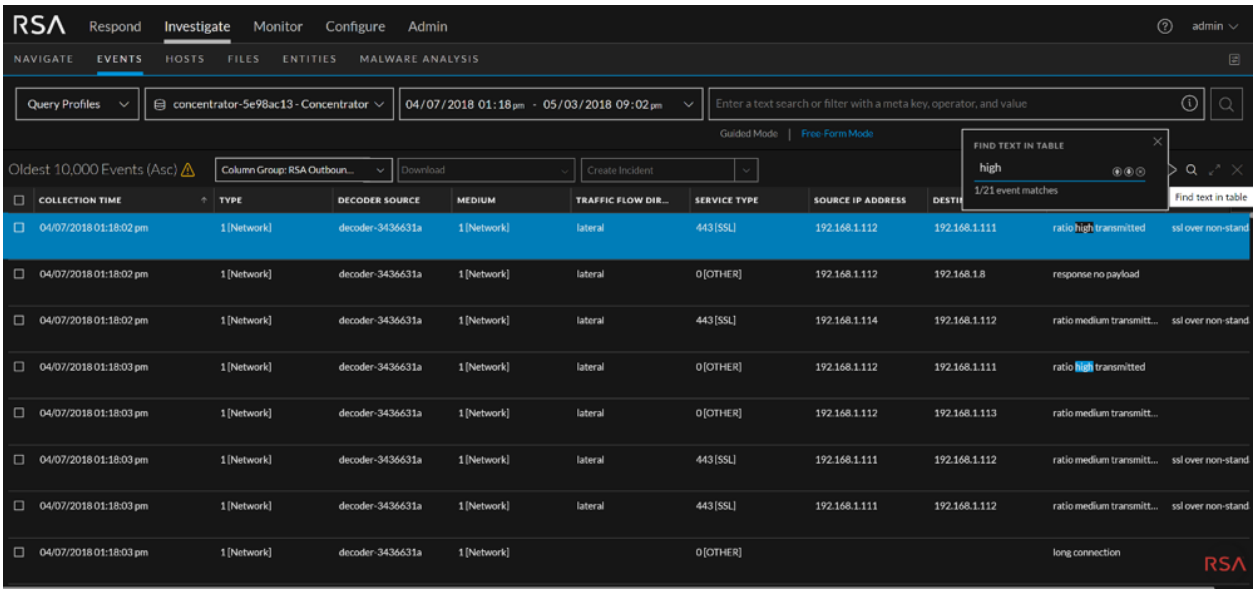
Use Recent Queries to Help with Query Construction in the Events View

As an aid to efficiency in constructing queries, analysts have access to recent queries in the Events view query bar. While typing a filter in the query bar, analysts see suggestions from a list of previous queries that may help to complete the construction of the query. The list is filtered as the analyst types to show the most relevant recent queries that include the typed text. Selecting a recent query adds it as a filter in the query bar, where the analyst can edit it if necessary. For more information, see "Insert a Filter Based on a Recent Query" in Filter Results in the Events View.



Find and Highlight Text in the Events List

When the result of a query provides too much data, analysts can find and highlight information without using filters to further limit the query and losing context of the surrounding events. Analysts can find and highlight characters in the Events list, and use keyboard strokes to move through the highlighted characters. For more information, see "Find a Text String in the Events Panel" in Analyze Events in the Events View.



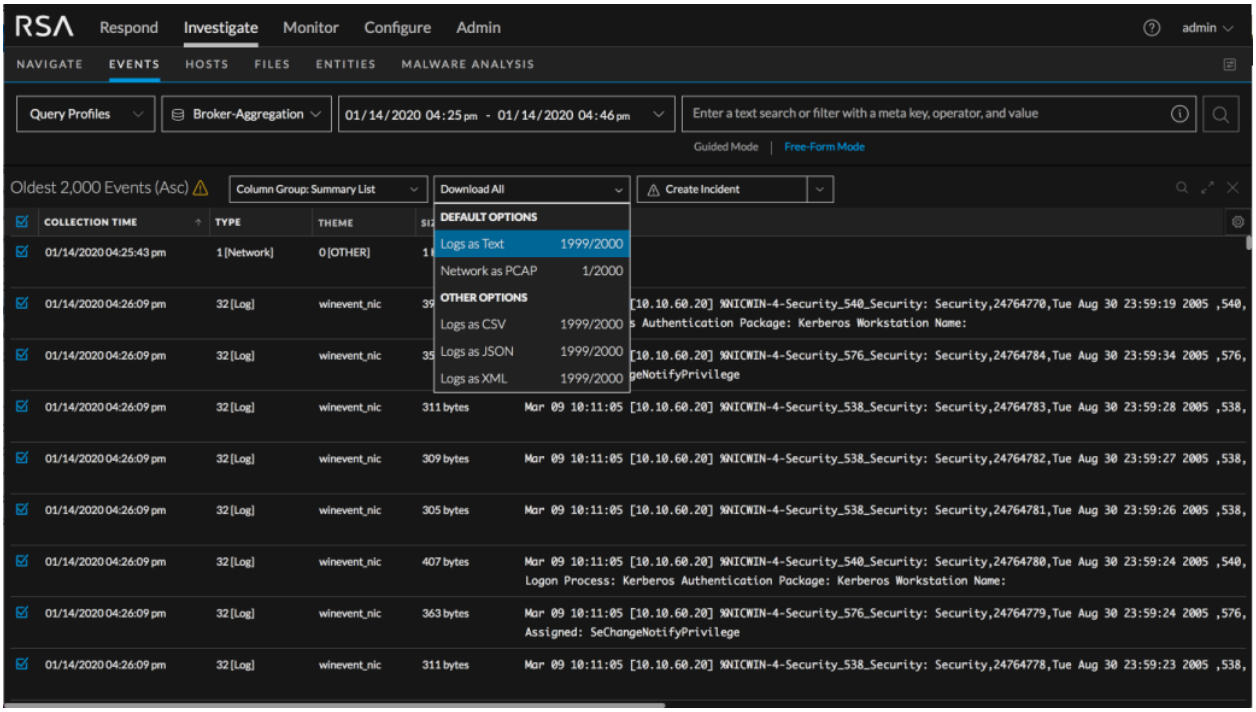
Shorthand Notations, Numerical Ranges, and Parentheses While Constructing Complex Queries in Guided Mode

Auto-completion of filters in the query bar is enhanced to support shorthand such as numerical ranges (`tcp.dstport=80-85`), a query with multiple `OR` [||] operators using commas (`src.port=0-1023, 1024-1050, 65535`), and an IPv4 or IPv6 subnet (`10.0.0.0/8`) as a value. The use of mapped aliases (`service = 'http'`) in place of their numerical values (`service=80`) is also supported. In previous versions, analysts had to enter this type of shorthand in Free-Form mode, without auto-completion, to help create valid, complex filters.

In addition, analysts can easily type or paste queries that contain parentheses, enclose several filters in parentheses, and delete parentheses while leaving the enclosed expressions in place. Parentheses are automatically balanced when you create and edit filters. For more information, see "The Version 11.4 Query Builder" in Filter Results in the Events View.

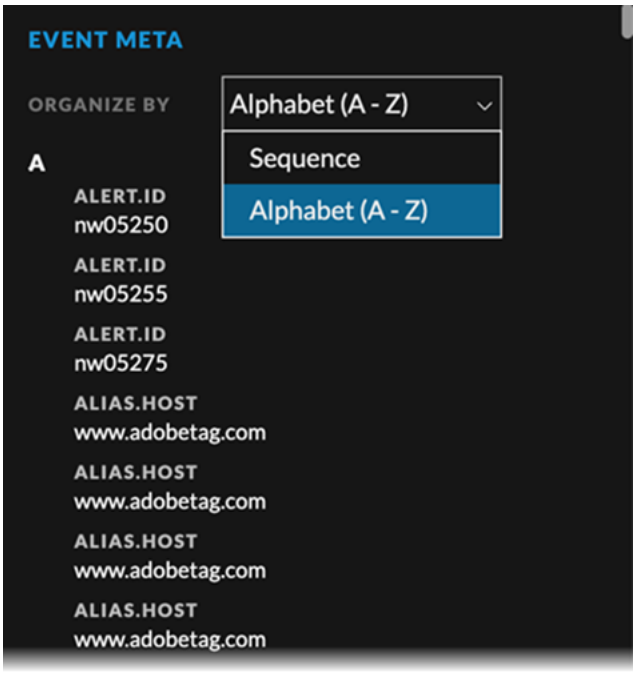
Download PCAPs, Metadata, and Logs in the Events View

Analysts can extract any subset of the Events list data and save it as evidence or for further investigations. Analysts can download the raw data (logs, packets) of any single event or multiple events. For more information, see Download Data in the Events View.



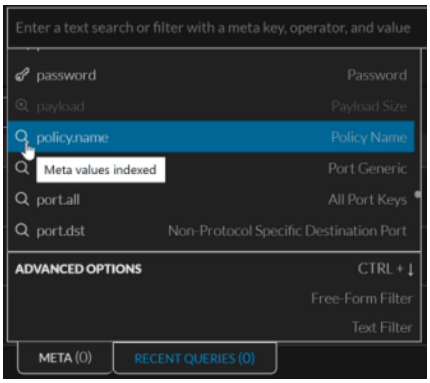
Event Meta Panel Layout

Analysts reviewing the metadata associated with results in the Events view can change the order of the metadata listed to find what they are looking for more easily. The layout of the list of metadata has been changed to be more intuitive, and metadata can optionally be grouped by the sequence in which they were generated or alphabetically. For more information, see "View Associated Metadata for an Event" in Analyze Events in the Events View.



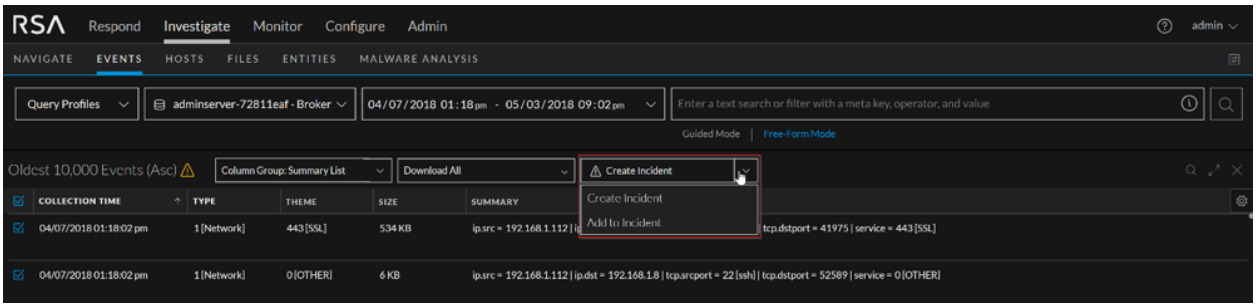
Query Auto-Complete Indicates Meta Key Index Level

During the creation of a query, analysts are given further details on how metadata is defined in the indices so they know what types of queries can and cannot be executed. As part of the auto-completion menu in Guided Mode, indicators on the meta keys depict at what level the meta keys are indexed. For more information, see "Visual Feedback in Guided Mode" in Filter Results in the Events View.



Create and Edit Incidents from Investigate

When investigating in the Events view, analysts can add events from their query results to a new or existing incident. By adding up to 1000 events at a time this improved workflow keeps an analyst from traversing between Respond and Investigate to add evidence to an incident. For more information, see Add Events to an Incident in the Events View.

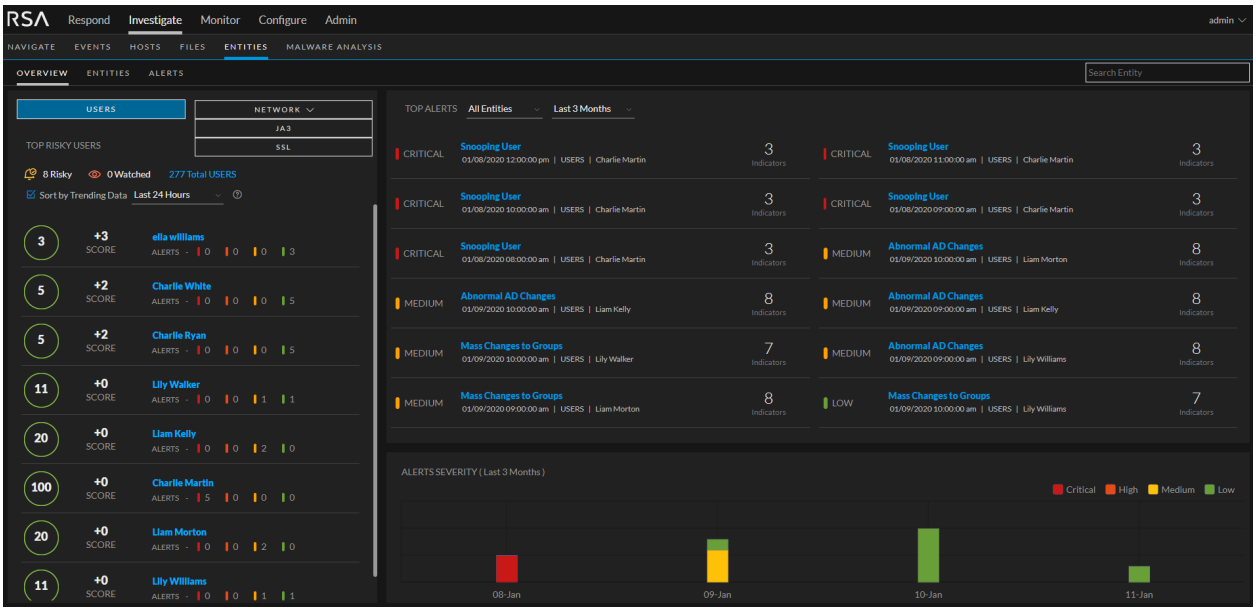


NetWitness User and Entity Behavior Analytics

Advanced Analytics Using Network Data

UEBA supports network models that use network (packet) data to detect potential malicious traffic masked within a legitimate HTTPS session. Organizations can detect various network abnormalities such as abnormal outbound traffic volume sent to a specific port, domain, organization or SSL Subject.

A new TLS data source that supports two new entities, JA3 and SSL Subject, are introduced to detect anomalies that are classified into an alert type, that is data exfiltration or phishing.



Filtering Entities to Investigate

The UEBA user interface is enhanced for a better analyst experience for investigating user or network entities. Multiple filtering options for user or network entities enable analysts to narrow down their investigation.

Trending Data Support

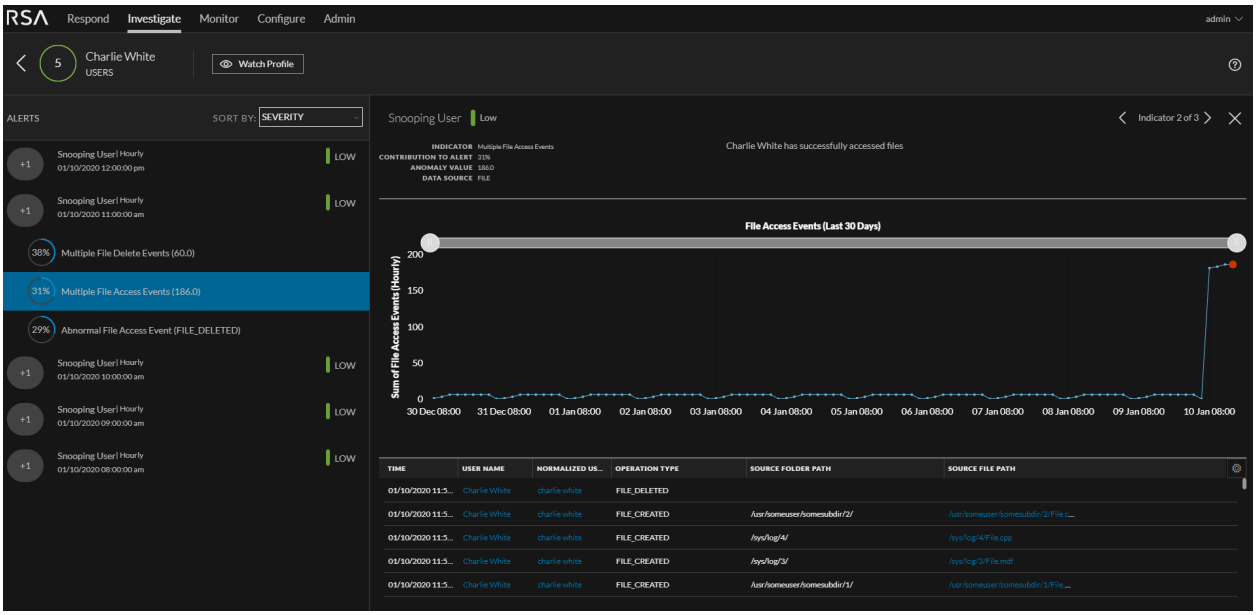
On the dashboard, the analyst can now view the top trending data of entities. Trending data represents the increase in a user or network entity score in the last day or the last week.

Quick Sorting Options

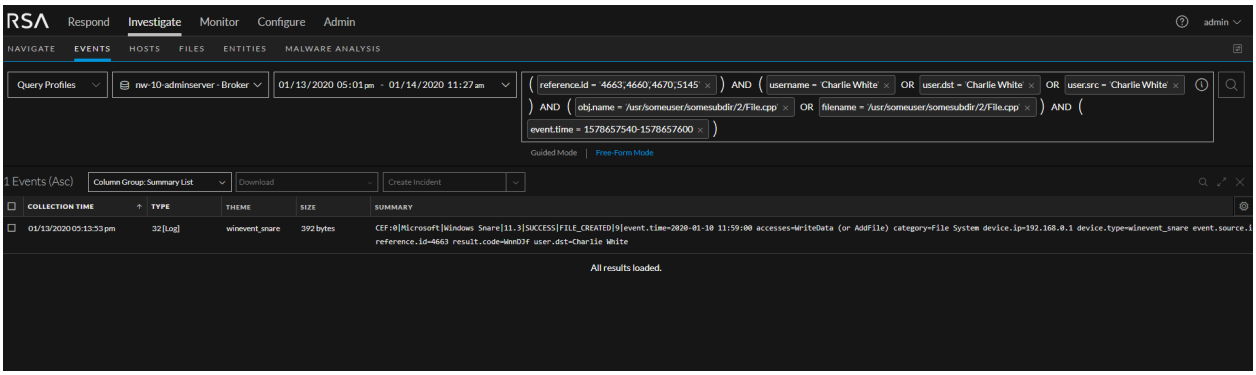
New filters sort the Top Alerts data based on the entity type and the duration of data you want to view are introduced. For example, you can select, All Entities, Users, JA3 and SSL and view the data for the Last 24 Hours, Last 7 Days, Last Month or Last 3 Months.

Improved Pivoting Option from UEBA to Events

Multiple pivoting options are introduced for an analyst to investigate threats in detail by viewing raw events. Analysts are presented with the events that contributed to the indicator to make investigation easy. As an example, if you are interested in investigating a user, click on the name under the USER NAME column.



The details of the selected user is displayed in the **Investigate** > **EVENTS** view.



Incident Response

Nodal Graph Improvements

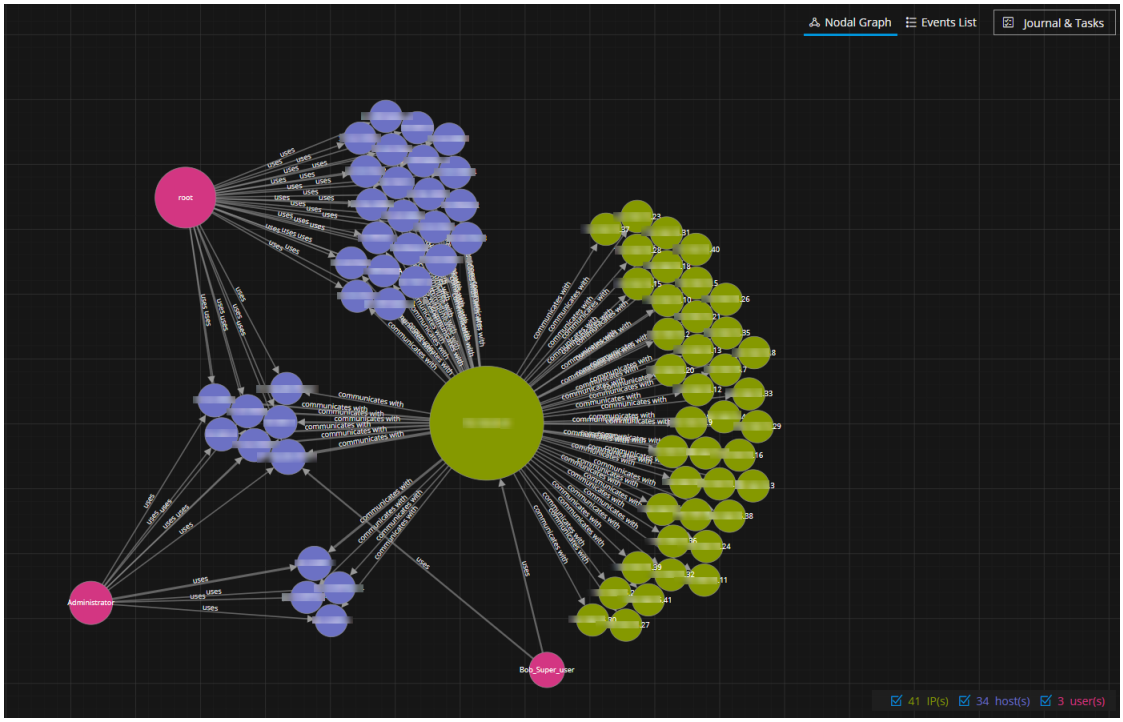
Nodal graph improvements in this release make it easier for an analyst to get an initial understanding of an incident with minimal effort.

The nodal graph now provides the following benefits to an analyst when responding to an incident:

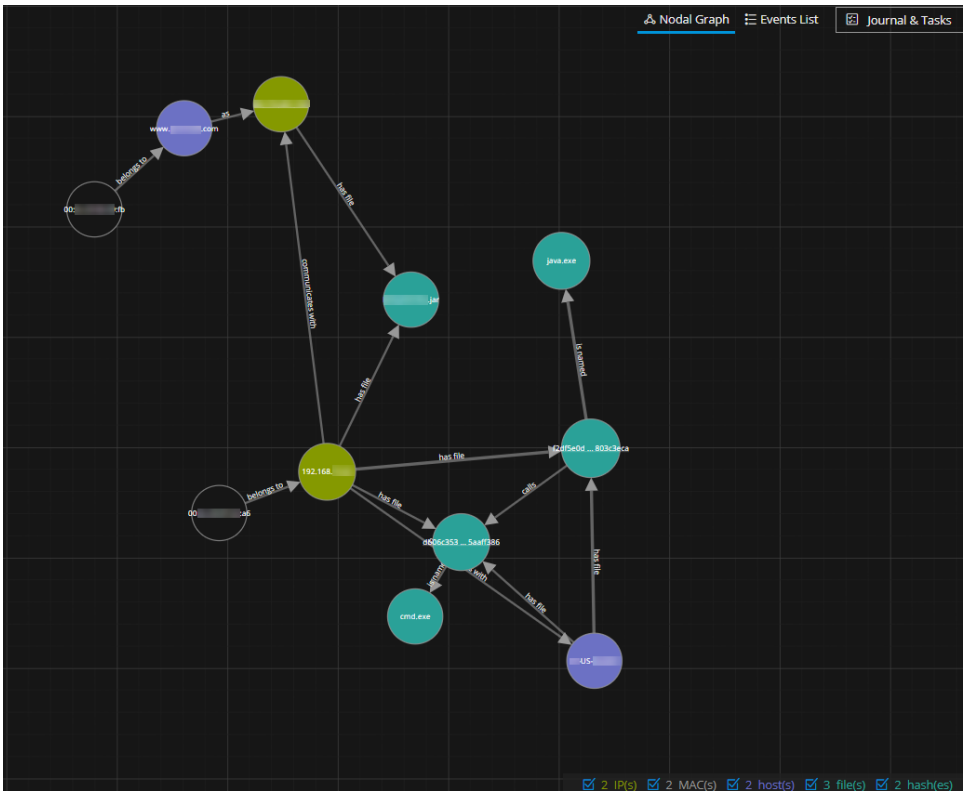
- The nodal graph helps determine scope, commonalities, and outliers in a given dataset, which can be useful context for an analyst.
- In many cases, the initial nodal graph layout presents valuable insight without any interaction from the analyst.
- In cases where the initial layout does not give enough clarity or when an analyst wants to view things differently, a few nodal mouse-drag position adjustments along with the new nodal forces can provide a much faster method of exposing insightful relationships and clusters. Previously, an analyst could adjust the nodes manually to create a more readable structure, but that was very time consuming.

The following behaviors and characteristics are now part of the graph:

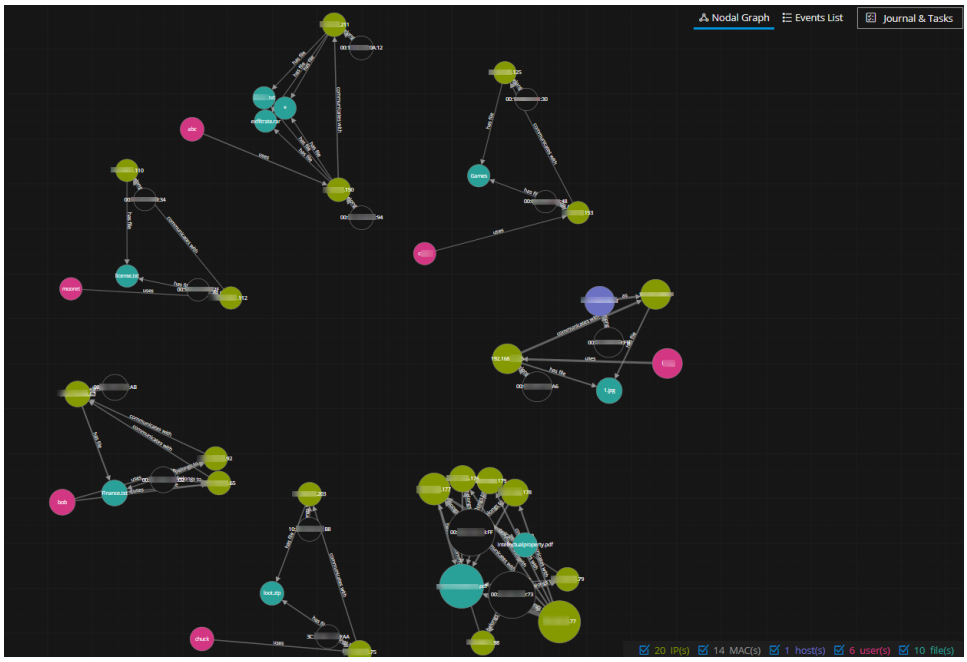
- Entities of similar types tend to cluster together visually. Previously, all nodes were laid out evenly on the Nodal Graph panel regardless of entity type, relationship, or size.



- Attributes and actions are better differentiated. Arrows that represent attributes ("as", "is named", "belongs to", and "has file") tend to be shorter than those representing actions ("call" and "communicates with").



- "Leaf nodes," which are nodes that only have a single relationship to a single entity, have a stronger force between them, which tends to keep these nodes closer together. Previously, the equal forces resulted in many crossed relationships making it hard to tell which nodes had relationships with each other.
- Disjointed graphs, such as clusters of entities and relationships that do not have connections with one another, are forced apart. Previously, disjointed graphs would bundle together making it seem like there were interactions among all nodes.



Dragged nodes are pinned in place. Double-click a node to unpin it and allow the forces to apply again to the node.

Alert Search Improvements

The Alerts List view (Respond > Alerts) displays a list of all alerts received by the Respond Server database in NetWitness Platform. Filtering by alert name is now improved. For example, if you want to use the filter to search for alerts generated by certain rules, instead of scrolling through a very long list of alert names to make your selections, you can now just start typing each alert name and select it. The alert names that you select are now the only names visible in the Filter panel, which makes it easier to see the alert names being filtered and to remove alert names.

Incident Search Improvements

Incidents List view (Respond > Incidents) filter improvements enable analysts to save time when searching for an incident. Analysts no longer have to type the "INC-" prefix when searching for an incident. To locate an incident, they can just type the incident number, such as "1050," instead of "INC-1050."

Improvements to Respond Email Notifications

Incident response email notifications now provide more relevant information to the users receiving the emails. After receiving an email notification, it is no longer necessary to log in to NetWitness Platform to determine if an incident was updated or created and who made the changes. Incident response email notifications are now more informative:

- You can differentiate easily between email notifications for created and updated incidents.
- You can see the Incident ID and Incident Name in the subject lines of email notifications for incident creation and updates.
- The body of the email notifications for incident creation and updates identify the user who created or updated the incident and shows the incident assignee.

Export and Import Incident Rules

You can now export and import incident rules from the Incident Rules view (Configure > Incident Rules). Exporting incident rules enables you to share incident rules with other NetWitness Servers on the same release version. The exported incident rules file is a ZIP file that contains two JSON files: one file contains the incident rules and the other file contains the incident rule schema. If necessary, advanced users can edit the incident rules in the exported ZIP file.

You cannot export Advanced incident rules; the export function only allows incident rules created using Rule Builder.

For more information, see the NetWitness Respond Configuration Guide.

Enable or Disable Multiple Incident Rules at the Same Time

To quickly enable or disable incident rules, SOC managers and analysts can now multi-select incident rules from the Incident Rules view (Configure > Incident Rules). Previously, you could only enable incident rules one at a time from within the incident rule details.

Access to Incidents Can Be Restricted

By default, all users with Respond view access can see all incidents, alerts, and tasks. If incident access is restricted, restricted users can only see their own incidents and the alerts and tasks associated with those incidents. Incident access restrictions are configured in the Admin > Security > Settings tab.

For more information on the specific restrictions this feature implements, see “Restrict Access to Incidents” in Step 2. Assign Respond View Permissions.

Health and Wellness (BETA)

The Health and Wellness (BETA) feature is an advanced, robust, and a simplified solution for hosts and services monitoring, such as performance or resource utilization. Health and Wellness provides great visualizations and allows you to easily alert or notify anomalies on critical hosts and services in a large NetWitness deployment. For 11.4, you can only deploy Health and Wellness Search (BETA) on a dedicated, virtual host.

Note: This is a BETA version of this feature and it is not completely implemented in 11.4 (for example, it does not have integrated authentication to Kibana and it cannot post alerts to output actions).

The following are the key benefits of Health and Wellness (BETA):

1. Dashboards with interactive visualization.
2. Easy-to-create customized content (visualization, alerts, dashboards, and so on).
3. Alerts on your data and customize alert conditions.

Presentation of large volumes of metrics is simplified on the Kibana user interface (UI) which enables administrators to easily create dynamic Health and Wellness visualizations in real-time.

Built-in content, such as dashboards and interactive visualization, are available to quickly set up monitoring. For more information, see Monitor Health and Wellness Beta Using Kibana. Deployment instructions are in Health and Wellness (BETA for Standalone Virtual Host Only).

Please direct any Health and Wellness Beta feedback to nw.health.wellness.feedback@rsa.com.

Endpoint Investigation

Isolate Infected Hosts from Network

Analysts can perform advanced investigation on a potentially suspicious host and control the spread of an attack by isolating the host from the network. Analysts can safely investigate the malware behavior on the host while the threat may still be active. In the isolated state, all events are reported to the Endpoint Server, retaining full visibility into activities on the host. For more information, see Isolating Hosts from Network.

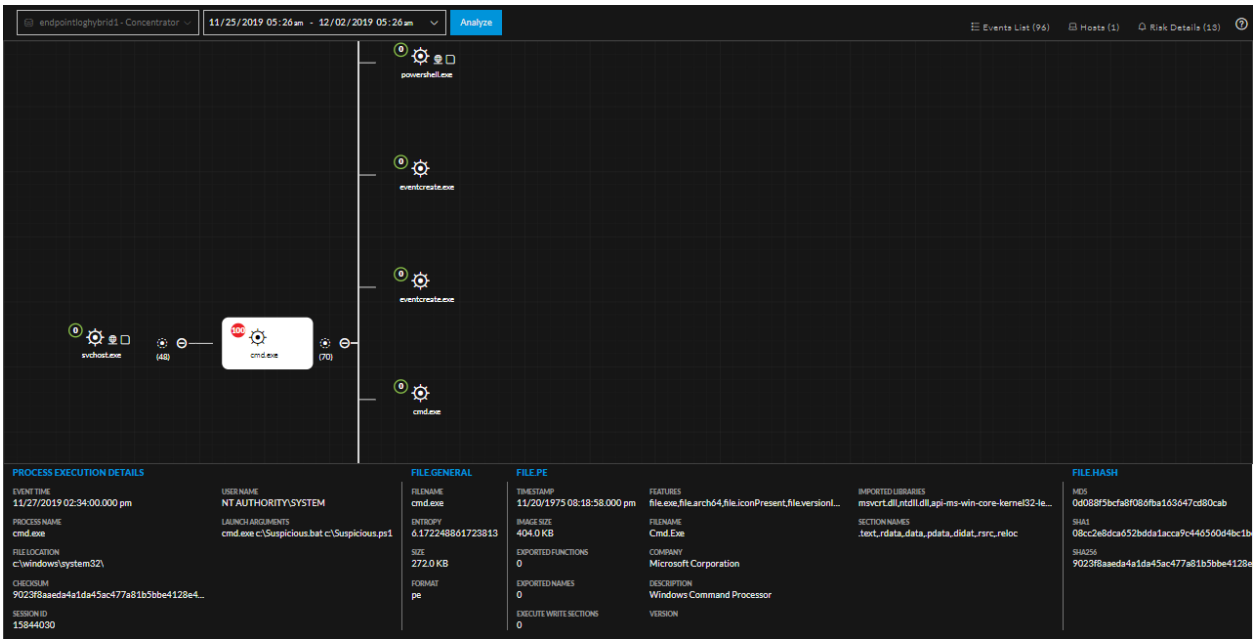
Advanced Forensic Investigation

If a host is suspicious, analysts can download the Master File Table (MFT) from a suspicious host for advanced forensic investigations, such as searching for files that are created during an attack time frame and searching for files based on the file name pattern, without logging in to the host. Analysts can also download suspicious files within MFTs for further analysis.

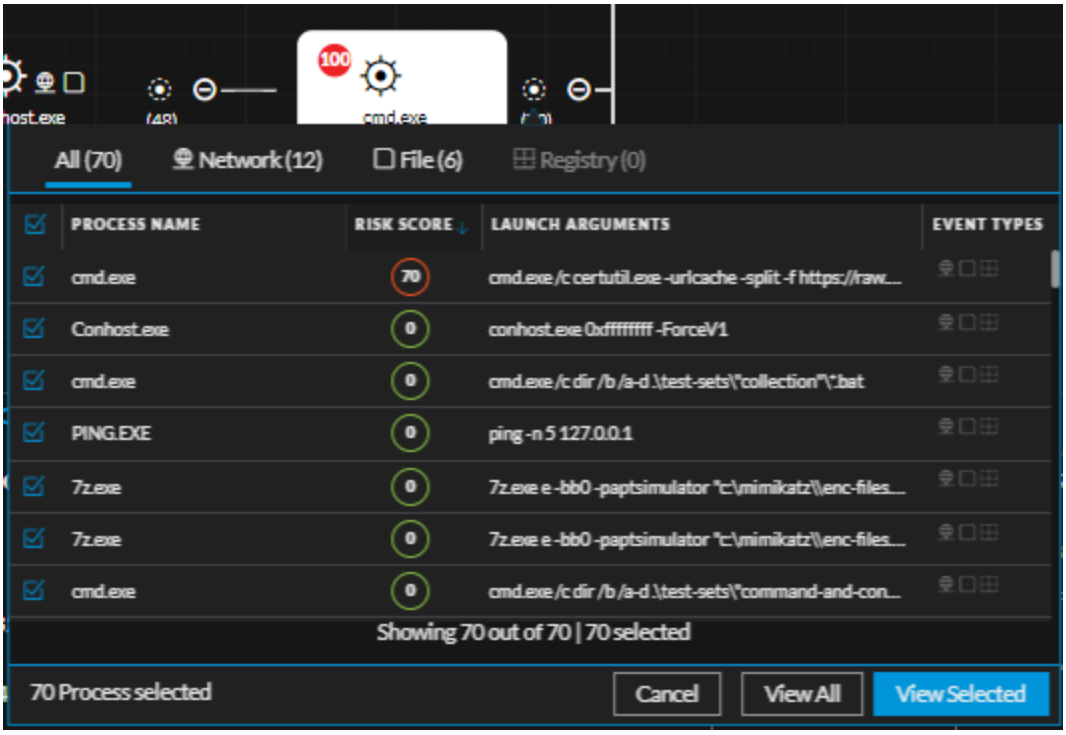
For forensic investigation of suspicious processes on a host, the analyst can download the process or system dump. For more information, see Performing Host Forensics.

Usability Enhancements for Process Analysis

For an easier and more intuitive analyst workflow, the process viewer is enhanced to provide more context, such as associated events, hosts on which the process is present, and risk details. Analysts can view risk score, event type (network, file, or registry), process execution details, and file properties for each node.



To reduce the clutter, analysts can narrow down the child processes by event type and select the required processes for further analysis. For more information, see Investigating a Process.



Usability Enhancements for Host Aggregation

For easier and more intuitive analyst workflow, host aggregation for files is enhanced so the analyst can sort or filter on the On Hosts column and view the number of hosts on which the file is present. If a file is present on fewer hosts, it may need further investigation.

The **Active On** Column is renamed to **On Hosts** in Host views and the Files view.

For more information, see Investigating Files.

Support of Additional REST APIs

To enhance Security Orchestration Automation and Response capabilities and to integrate NetWitness Endpoint with third-party applications, new APIs are introduced to request system dump download, process dump download, and for network isolation. For more information, see the API User Guide for RSA NetWitness Platform.

Filters in Host Details

With the extensive list of files that have no filtering options, analysis results in a cumbersome user interface and takes more time than required. For faster file analysis, analysts can narrow down files within the host details using filters, such as file or process name, file status, reputation, signature, and risk score. For more information, see Investigating Hosts.

Support for Automatic File Download

Files are automatically downloaded for analysts to perform deeper analysis and identify any suspicious files. The automatic download is based on the configuration in the policy where you can limit the number of the files by allowing only the files matching criteria to be downloaded. By default, only a single copy of the file (unsigned) and files lesser than 1 MB are downloaded. For more information, see Create Groups and Policies.

Endpoint Configuration

Endpoint Agent Log File Collection

The agent now supports collection of File Logs (from event sources that use File Collection as a collection protocol), with Endpoint Detection and Response (EDR) capabilities and Windows Log Collection. This is the recommended way for collecting logs from the supported event source types, allowing centralized management. Switching to this collection method from SFTP is a simple, straightforward process, described in Replace Windows SFTP Agents. The SFTP Agent is still supported, but it will be deprecated in the future.

For a list of currently supported event source types, see Supported File Log Event Source Types.

Support for New Operating System Versions in Endpoint Agent

In addition to the operating system versions supported in 11.3, the agent now supports the following operating systems:

- macOS 10.15 Catalina
- CentOS 8.x
- Red Hat Enterprise Linux 8.x
- Windows 10 version 1909

For more information, see the NetWitness Endpoint Agent Installation Guide.

Broker, Concentrator, Decoder and Log Decoder Services

Berkeley Packet Filters (BPF) Supported for 10G Environments

You can now use Berkeley Packet Filters that are already implemented on Decoders in 10G environments for better control over which packets and logs are processed specifically for high-speed packet capture. For more information, see (Optional) Configure System-Level (BPF) Packet Filtering and Configure 10G Capability.

IPv4 Index CIDR Range Optimization

Core Database indexes for IPv4 data types automatically index CIDR Ranges for the common /8, /16, and /24 subnet sizes. Query operations that search for these types of CIDR ranges are now significantly faster.

Gain Visibility into HTTP/2 Sessions

You can search for metadata items derived from headers in the HTTP/2 stream to gain visibility into HTTP/2 sessions. For more information, see HTTP Parsers.

Event Stream Analysis (ESA)

Added the Ability to Remove Sensitive Meta Keys from all Alert Output for Data Privacy

For data privacy reasons, you can now remove some sensitive meta keys from all alert output globally, regardless of the data source. In the ESA Correlation service, you can add sensitive meta keys to the `global-private-fields` parameter, which removes them from the output of all alerts. For more information, see Remove Sensitive Meta Keys Globally from All Alerts for Data Privacy.

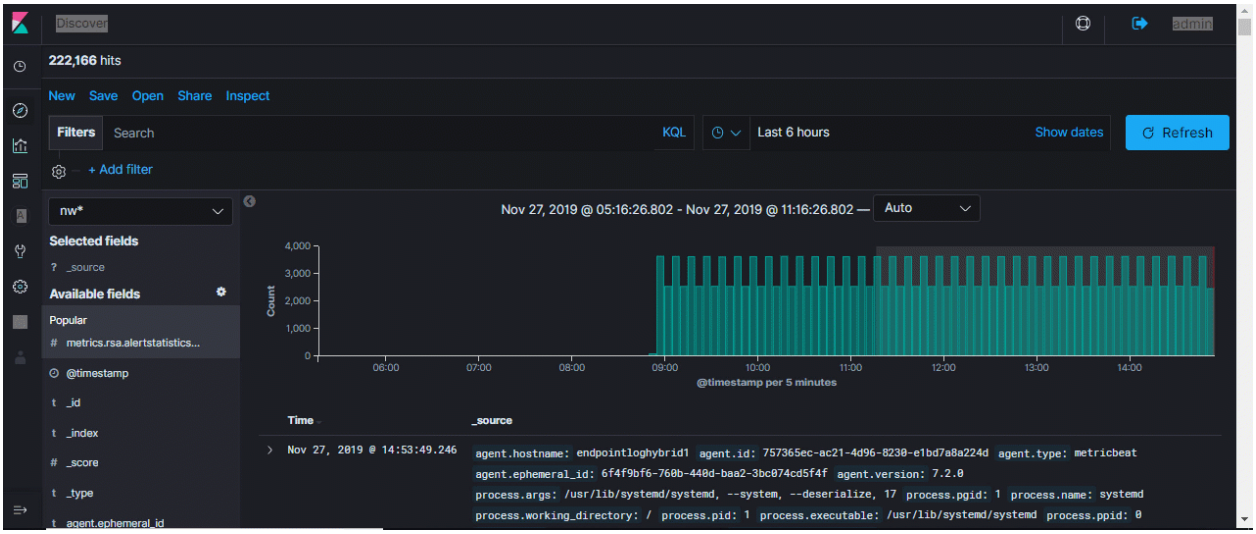
Esper Version Upgraded from Version 7.1.0 to 8.2.0

In NetWitness Platform version 11.4, ESA Correlation supports Esper version 8.2.0.

Log Collection

Export of Syslog RFC-5424 Logs Imported from the NetWitness Platform User Interface

The transport format, RFC-5424, is retained when saving the raw logs.



Because it is retained, you can replay these logs with the original source and collection context, allowing the NetWitness Platform to accurately reflect a log's true origin.

Log Stats Performance Improvements

The number of event source stats transmitted from a Log Decoder will drop as NetWitness prunes idle event sources in 11.4. Entries for these idle event sources will still appear in the Event Source Management tab, but will not affect storage nor access for logs.

Administration and Configuration

Single Sign-On Authentication

For Admins to streamline authentication for NetWitness Platform, Single Sign-On is supported. NetWitness Platform supports Active Directory Federation Services (ADFS) as an Identity Provider (IDP) and uses SAML 2.0 as the protocol for single sign-on. For more information, see Configure Single Sign-On.

With SSO, NetWitness users will not be asked every time to log in every time if they are successfully authenticated the first-time.

Configure Menu Improvements

Configure menu item adjustments benefit analysts and other RSA NetWitness Platform users:

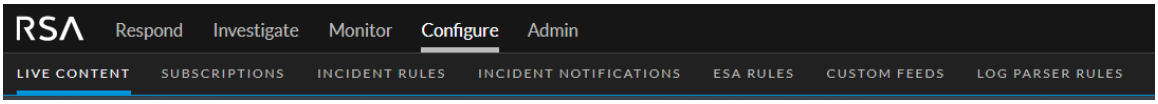
- **Respond Notifications** is renamed to **Incident Notifications** because it only pertains to incident notifications.
- **Live Content** and **Subscriptions** are next to each other because subscriptions only refer to content that comes through Live.

Previous Configure sub-menu item order:

Live Content | Incident Rules | Respond Notifications | ESA Rules | Subscriptions | Custom Feeds | Log Parser Rules

New Configure sub-menu item order:

Live Content | Subscriptions | Incident Rules | Incident Notifications | ESA Rules | Custom Feeds | Log Parser Rules



Multiple NW-Server Support for Distributed Analyst User Interface (UI)

You can now deploy multiple NetWitness Platform UI instances for analyst purposes. These Analyst UI instances can be deployed to span across multiple Geographic locations. The feature helps reduce latency and improve performance as compared to accessing all functionality from the Primary UI on the NW Server Host.

You are able to provision and orchestrate an Analyst UI instance or host in the same manner as the other NetWitness component hosts.

Features and Limitations

Each Analyst UI host:

- Can be deployed to specific organizational groups. For example: the Americas, EMEA, APAC, Tier 1 Analysts, Tier 3 Analysts.
- If Analyst UI hosts are deployed regionally, you have the capability of querying those regional brokers directly (less latency), rather than having to route through the Primary UI.
- Helps distribute load off the Primary UI.
- Has its own Reporting Engine (RE).
- If it becomes unavailable for any planned or unplanned reason, it will not affect the Primary UI or any other Analyst UI instances.
- Provides the same pre-query filter verification, Data Privacy protection, and RBAC functionality as the Primary UI.
- Points back to the primary NW Server for authentication and configuration.
- Does not have access to any administrative functions. All administration functions take place on the Primary UI.

- Does not allow you to create or manage Content (that is, ESA rules, app rules, feeds). All Content creation and management takes place on the Primary UI.

Deployment instructions are in Analyst User Interface. A description of the dashboard is in "Using Dashboards in the Analyst User Interface" in Managing Dashboards.

Capability to Provide Silent NetWitness Installation

Administrators may need to automate installation of NetWitness so that they can quickly deploy environments. Now they can use the `-silent` command with the installation `nwsetup-tui` script to run the script without getting prompted for input. This enables them to automate the installation of a host by supplying responses to the scripts' prompts through the command line.

New Retention Optimized Log Hybrid Option

In 11.4, RSA has introduced a new Log Hybrid option (for the Series 6E Hybrid only) which optimizes retention by:

- Enabling compression for raw logs and meta.
- Enabling Decoder indexing, which eliminates the need for meta cache volume so it can be allocated for usable capacity.
- Consolidating multiple RAID groupings into a single RAID 6 configuration.

You can provision and orchestrate the Retention Optimized Log Hybrid in the same manner as the other NetWitness Hybrid hosts.

Capability to Deploy the NW Server on Series 6 Analytics Hardware (Formerly ESA Physical Host)

You now have the option to deploy the NW Server host on Series 6 Analytics hardware. The Series 6 Analytics Hardware has more memory and storage capacity than the standard Core appliance on which NW Server has typically been deployed. This results in better overall responsiveness and larger retention capacity for Report Engine.

Install Endpoint Server on Existing Log Decoder Host

You can install an Endpoint Server on an existing Log Decoder host in 11.4. For more information, see “Install an Endpoint Service Category on an Existing Log Decoder” under "Post Installation Tasks" in the Physical Host or Virtual Host Installation Guides.

Upgrade Improvements

Respond Service Normalization Scripts are Automatically Backed Up before being Refreshed After an Upgrade

Manual backups are no longer required for Respond service normalization script customizations. Respond normalization scripts are automatically backed up to the **/var/lib/netwitness/respond-server/scripts.bak-<timestamp>** directory, where **<timestamp>** is the time that the backup completed:

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_ueba_alerts.js
normalize_wtd_alerts.js
utils.js
```

To prevent overwriting future customizations, custom normalization script files are available in NetWitness Platform 11.4 and later releases. If you have any customizations in the normalization files, you now add them to the normalization files with the “custom” prefix (**custom_normalize_<alert type>.js**):

```
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
```

Fixed Issues

This section lists issues fixed after the last major release.

Security Fixes

Tracking Number	Description
ASOC-86436	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:3834
ASOC-86435	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:3872
ASOC-85738	CentOS 7 sudo security update (Important) - https://access.redhat.com/errata/RHSA-2019:3197
ASOC-85372	CentOS 7 java-11-openjdk security update (Important) - https://access.redhat.com/errata/RHSA-2019:3127
ASOC-85371	CentOS 7 java-1.8.0-openjdk security update (Important) - https://access.redhat.com/errata/RHSA-2019:3128
ASOC-85296	CentOS 7 kernel security and bug fix update (Important) - https://access.redhat.com/errata/RHSA-2019:3055
ASOC-85267	CentOS 7 libcgroup security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2047
ASOC-85266	CentOS 7 libjpeg-turbo security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2052
ASOC-84843	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:2829
ASOC-84228	CentOS 7 libmspack security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2049
ASOC-83893	CentOS 7 kernel security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:2029
ASOC-83892	CentOS 7 pango security update (Important) - https://access.redhat.com/errata/RHSA-2019:2571
ASOC-83891	CentOS 7 httpd security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2343
ASOC-83890	CentOS 7 kernel security and bug fix update (Important) - https://access.redhat.com/errata/RHSA-2019:2600
ASOC-82840	CentOS 7 glibc security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2118

Tracking Number	Description
ASOC-82839	CentOS 7 elfutils security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2197
ASOC-82838	CentOS 7 dhcp security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2060
ASOC-82837	CentOS 7 curl security and bug fix update (Low) - https://access.redhat.com/errata/RHSA-2019:2181
ASOC-82836	CentOS 7 binutils security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2075
ASOC-82835	CentOS 7 bind security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2057
ASOC-82834	CentOS 7 libssh2 security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2136
ASOC-82833	CentOS 7 libtiff security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2053
ASOC-82832	CentOS 7 Xorg security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2079
ASOC-82831	CentOS 7 linux-firmware security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:2169
ASOC-82830	CentOS 7 mariadb security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2327
ASOC-82829	CentOS 7 nss, nss-softokn, nss-util, and nspr security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2237
ASOC-82828	CentOS 7 ntp security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2077
ASOC-82827	CentOS 7 openssh security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2143
ASOC-82826	CentOS 7 openssl security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2304
ASOC-82825	CentOS 7 polkit security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2046
ASOC-82824	CentOS 7 procps-ng security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2189
ASOC-82823	CentOS 7 python security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2030
ASOC-82822	CentOS 7 python-requests security update (Low) - https://access.redhat.com/errata/RHSA-2019:2035

Tracking Number	Description
ASOC-82821	CentOS 7 python-urllib3 security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2272
ASOC-82820	CentOS 7 rsyslog security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2110
ASOC-82819	CentOS 7 samba security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2099
ASOC-82818	CentOS 7 systemd security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2091
ASOC-82817	CentOS 7 unixODBC security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2336
ASOC-82816	CentOS 7 unzip security update (Low) - https://access.redhat.com/errata/RHSA-2019:2159
ASOC-72421	CentOS 7 bind security update (Moderate) https://access.redhat.com/errata/RHSA-2019:0194
ASOC-72419	CentOS 7 systemd security update (Low) - https://access.redhat.com/errata/RHSA-2019:0201
ASOC-72418	CentOS 7 kernel security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:0163
ASOC-70086	CentOS 7 samba security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3056
ASOC-70079	CentOS 7 kernel security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3651
ASOC-69381	CentOS 7 libmspack Security Update (Low) - https://access.redhat.com/errata/RHSA-2018:3327
ASOC-69302	CentOS 7 fuse Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3324
ASOC-69297	CentOS 7 openssl Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3221
ASOC-69294	curl and nss-pem security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3157
ASOC-68872	GNOME security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3140
ASOC-68844	X.org X11 security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2018:3059
ASOC-68833	CentOS 7 xorg-x11-server Security Update (Important) - https://access.redhat.com/errata/RHSA-2018:3410

Tracking Number	Description
ASOC-67478	CentOS 7 xorg-x11-server Security Update (Moderate) - https://lists.centos.org/pipermail/centos-announce/2018-October/023075.html
ASOC-59640	CentOS 7 python Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:2123

Log Collection Fixes

Tracking Number	Description
ASOC-82596	**Title:** Plugin transform parameter `<includeNullValueParameters>` not replacing null tokens to empty string. RSA has added a parameter to the Transform XML File. This file is used for creating and configuring plugins. The new parameter is "includeEmptyValueParameters". If you set this parameter to **true**, empty parameters, and empty lists, are included in the output of the transform. If set to **false**, which is the default, excludes empty parameters in the output of the transform. Additionally, the existing parameter "includeNullValueParameters" has been updated to behave as expected. Previously this parameter incorrectly included or excluded empty value parameters and did nothing for "null" valued parameters. Now this parameter, if set to **true**, includes null tokens items in the output of the transform. If set to **false**, which is the default, excludes null value parameters in the output of the transform.

Event Stream Analysis (ESA) Fixes

Tracking Number	Description
ASOC-87267	**Title:** Disabled ESA Trial Rules in the Services view get enabled after an upgrade This issue is now resolved. Previously, ESA Trial rules could change status after an upgrade or when they were redeployed. In NetWitness Platform 11.4, ESA trial rules no longer change status after an upgrade or deployment. For example, if you change the status of a trial rule to `disabled` (Configure > ESA Rules > Services tab) and redeploy the ESA rule deployment (Configure > ESA Rules > Rules tab), the trial rule remains disabled.

Administration Fixes

Tracking Number	Description
ASOC-86557 ASOC-87065	Updating "Effective Date" daily causes scan schedules to restart.
ASOC-59607	Syslog server config updates are making duplicate entries in the `rsa-audit-server-output.conf` log file.
ASOC-59240	In Audit Logs, when Common Event Format (CEF) template is applied, backslash characters (“\”, “\n”, “\r”) are not escaped properly in the meta values. For example, CORP\user is displayed as CORPuser, CORP\nancy is displayed as CORP ancy and CORP\randy is displayed as CORP andy.

Investigate Fixes

Tracking Number	Description
ASOC-73826	In the Event Analysis view, the query console does not replace the information icon with an error icon when a service is offline.
ASOC-73224	When retrieval of events for a query is in progress in the Event Analysis view, events that are already displayed disappear if the query takes more than five minutes to finish.
ASOC-60464	When a large PCAP is extracted from the Events view, and it times out after five minutes, the query time is displayed as eight hours in the Jobs tray error message.

Known Issues

Issues that remain unresolved in this release are documented here: https://community.rsa.com/community/products/netwitness/documentation/known-issues. Wherever a workaround is available, it is noted or referenced in detail.

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.4.0.0:

- RSA NetWitness® Platform 11.2.x.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.0.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.1.x to 11.4.0.0
- RSA NetWitness® Platform 11.3.2.x to 11.4.0.0

For more information on upgrading to 11.4.0.0, see "Installation and Upgrade Guides" on the NetWitness Platform documentation page on RSA Link. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.4 Online Documentation	https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform 11.4 Installation and Upgrade Instructions	"Installation & Upgrade Guides" section of https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Feedback on Product Documentation

You can send an email to sahelpfeedback@emc.com to provide feedback on RSA NetWitness Platform documentation.

Features Not Supported

The following tables provide information on features no longer supported in RSA NetWitness® Platform 11.2 or later releases.

Features Not Supported in 11.2.0.0 or later releases

Feature	Notes
Some Event Stream Analysis service features from 11.2 and earlier	The following Event Stream Analysis service features (11.2 and earlier) are not in the 11.3 and later ESA Correlation service: 1. Memory snapshot for trial rules 2. ESA SNMP notification method 3. Database as an enrichment source (replaced by Context Hub list) 4. Warehouse Analytics as an enrichment source (replaced by Context Hub list) 5. Database Connection as an enrichment source (replaced by Context Hub list) 6. Recurring In-Memory Tables as an enrichment source (replaced by Context Hub list) 7. Capture time ordering 8. Memory pool
Endpoint Hybrid	Endpoint Hybrid host type is not supported in 11.3.0.0 and later releases.

Support Information

There are several options that provide you with help as you need it for installing and using NetWitness Platform:

- See documentation for all aspects of NetWitness Platform here: https://community.rsa.com/community/products/netwitness/documentation
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here: https://community.rsa.com/welcome
- If you need further information, contact Customer Care.

If you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com In the main menu, click **My Cases** from the list at the bottom of the browser.
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Revision History

Revision	Date	Description
1.0	January 2020	Release To Operations