



# Release Notes

for Version 11.1.0.0



## **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](http://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.

# Contents

---

<b>Introduction</b> .....	<b>5</b>
<b>What's New</b> .....	<b>6</b>
NetWitness Endpoint Insights .....	6
NetWitness Respond .....	7
NetWitness Investigate .....	7
Reporting .....	9
Health and Wellness .....	9
Event Stream Analysis and ESA Analytics .....	9
Core Services .....	9
User Interface .....	10
Platform .....	10
Administration .....	10
Log Parsing .....	11
Unified Data Model .....	12
<b>Upgrade Instructions</b> .....	<b>13</b>
<b>Fixed Issues</b> .....	<b>14</b>
Security .....	14
Investigate .....	14
Log Collector, Virtual Log Collector .....	15
Context Hub .....	16
Respond .....	16
Event Stream Analysis and ESA Analytics .....	16
<b>Features Not Supported</b> .....	<b>17</b>
Features Not Supported in 11.1.0.0 or later releases .....	17
Features Available in Future Releases .....	17
<b>Known Issues</b> .....	<b>19</b>
Known Issues During Upgrade to 11.1 .....	19
Context Hub .....	25
General Application Issues .....	26
Endpoint .....	26
Respond .....	28

Log Collector .....	33
Investigate .....	34
Workbench .....	38
Custom Feeds .....	38
Malware Analysis .....	38
Event Stream Analysis .....	39
Reporting .....	42
Administration .....	43
Event Source Management .....	43
Core Services .....	44
<b>Product Documentation .....</b>	<b>46</b>
<b>Contacting Customer Care .....</b>	<b>47</b>
<b>Revision History .....</b>	<b>48</b>

## Introduction

---

This document lists enhancements and fixes in RSA NetWitness Suite 11.1.0.0. Read this document before deploying or updating to RSA NetWitness Suite 11.1.0.0.

- [What's New](#)
- [Upgrade Instructions](#)
- [Fixed Issues](#)
- [Features Not Supported](#)
- [Known Issues](#)
- [Product Documentation](#)
- [Contacting Customer Care](#)
- [Revision History](#)

## What's New

---

The RSA NetWitness Suite 11.1.0.0 release provides RSA NetWitness Endpoint Insights as part of the RSA NetWitness Suite thus presenting a common platform for investigations on logs, packets and endpoints.

### NetWitness Endpoint Insights

RSA NetWitness Endpoint Insights provides visibility to vital host and user information. A new RSA NetWitness Endpoint Insights agent facilitates endpoint data to licensed RSA NetWitness Suite customers. It also transforms the collected endpoint data into powerful metadata that is correlated with network data across the entire suite. This helps to drive and prioritize investigation and response analyst workflows.

**NetWitness Endpoint Insights Agent.** This solution includes a lightweight agent for collecting host inventories, processes, user activity, and Windows logs thus reducing overall complexity of capturing logs and saving valuable time and resources for Security Operations Center (SOC) operations. This endpoint agent can be installed on Windows, Mac, or Linux hosts. It scans the hosts and sends data to the Endpoint Hybrid or Endpoint Log Hybrid over HTTPS. For more information, see the *Endpoint Insights Agent Installation Guide*.

NetWitness Endpoint Insights introduces two new services, Endpoint Hybrid and Endpoint Log Hybrid. You can deploy either one of these services.

**Endpoint Hybrid.** Is used for collection of endpoint data. There is no license required to collect endpoint data. The Endpoint Hybrid consists of an Endpoint Server, a Log Decoder, and a Concentrator. It can:

- Perform instant scans to understand the host behavior at any point in time.
- Store multiple scan snapshots.
- Process endpoint metadata for analysis and aggregation.
- Optimally store and manage scan data using retention policies.

**Endpoint Log Hybrid.** Is used to collect both endpoint and log data. In addition to the capabilities of an Endpoint Hybrid, this service can collect logs from Windows hosts through Endpoint agents, and all other event sources that are supported for log collection. The agent forwards the collected logs to a Log Decoder or Remote Log Collector. A license is required to collect log data. If you have throughput or perpetual licenses for Log Decoders, you can use them. If not, you must procure a license to collect logs both from the endpoint agent and any other log events collected using a Log Collector or Log Decoder. The Endpoint Log Hybrid consists of an Endpoint Server, Log Decoder, Concentrator, and Log Collector. For more information, see the *Endpoint Insights Configuration Guide*. Log collection capability can be enabled during agent installation. Logs can be filtered based on channels and a list of events that you want to collect. For more information, see the *Endpoint Insights Agent Installation Guide* and *Log Collection Configuration Guide*.

**Endpoint Metadata.** Data collected can be forwarded as metadata to a Log Decoder for seamless investigation for analysts along with log and packet data. You can generate reports and alerts with this metadata. For more information, see the *Endpoint Insights Configuration Guide*.

## NetWitness Respond

**Unassign Incidents.** You can now change an incident assignee to “(unassign)” (RESPOND > Incidents).

**Filter for Unassigned Incidents.** You can now filter the Incidents List to show only unassigned incidents (RESPOND > Incidents – Filters panel).

**Add Alerts to Incidents.** In addition to creating incidents from alerts, you can now add alerts to existing incidents from the Alerts List view (RESPOND > Alerts).

**Improved Search for Related Indicators.** In the Related Indicators panel for an incident, when searching for related indicators, it is no longer necessary to specify a Source, Destination, and Detector. The search for related indicators now queries all fields applicable to the search (Incident Details view - Related Indicators panel). For more information, see the *NetWitness Respond User Guide*.

**New Incident Rules User Experience.** Aggregation rules are now called Incident Rules. The Incident Rules pages have been redesigned for ease of use and there is now an Incident Rules List view and an Incident Rule Details view (CONFIGURE > Incident Rules). To better differentiate incident rule enabled status, the icons now have different shapes as well as different colors.

**Added a User Behavior Default Incident Rule.** The User Behavior default incident rule captures network user behavior. This rule uses deployed RSA Live ESA Rules to create incidents from alerts. You can select the RSA Live ESA Rules that you want to monitor.

**Updated Some Preconfigure (Default) Incident Rules with the Source IP Address Group by Value.** The following default incident rules changed slightly and now have “Source IP Address” as the Group By value:

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

For more information, see the *NetWitness Respond Configuration Guide*.

**Send Respond Email Notifications.** You can now send email notifications to Analysts assigned to incidents and to SOC Managers when incidents are created or updated (CONFIGURE > Respond Notifications). For more information, see the *NetWitness Respond Configuration Guide*.

## NetWitness Investigate

**Integrated User Interface for Endpoints.** The new Hosts and Files views (available in the Investigate submenu) provide a view of all hosts and files found in the deployment. For more information, see the *NetWitness Investigate User Guide*.

**Direct Access to Event Analysis in the Investigate Submenu.** The Event Analysis view is accessible from the Investigate submenu, in addition to the previous methods of opening the view. For more information on the investigation activities and features of Event Analysis, see the *NetWitness Investigate User Guide*.

**Meta Entities in Investigate.** Administrators can create meta entities (groups of meta keys) that represent two or more meta keys. Meta entities can be used in the same ways that a meta key is used in Investigate, except in Parallel Coordinates visualizations. Predefined meta entities are available for typical scenarios. For example, to find entities such as all IP addresses, all user names, all files, or all hosts, analysts can use the meta entity to build a simple query without having to know the specific meta keys in the entity. For more information, see "How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*.

**Interactive Breadcrumb in Event Analysis with Autocomplete and Validation.** The user interface lets analysts enter filters by clicking and typing, or using only keyboard actions. Analysts can add a `<meta key><operator><value>` filter to the breadcrumb, edit the filter, and delete one or more filters. Invalid filters are highlighted in a red box. Clicking the Query button executes the query, individual filters are ANDed, and the results are displayed in the Events List Panel. For more information, see "Filtering Events in the Events Analysis View" in the *NetWitness Investigate User Guide*.

**Default and Custom Column Groups in the Event Analysis view.** Column Groups have been enabled in the Event Analysis view. You can view and select default column groups and custom column groups, and the default is persisted per user. To manage column groups, go to INVESTIGATE > Events. In addition to the column groups in 11.0, the Endpoint Analysis, Outbound HTTP, and Outbound SSL/TLS groups have been added. For more information, see the *NetWitness Investigate User Guide*.

**Ability to Reconstruct an Event Directly from the Navigate View.** Given a known Event ID, analysts can reconstruct an event directly from the Navigate view. The **Actions > Go to event in Event Analysis** and **Actions > Go to event in Event Reconstruction** options in the Navigate view toolbar provide this capability. You can use this option without executing a query as you usually do when beginning an investigation. For more information, see "Reconstruct an Event from the Navigate View" in the *NetWitness Investigate User Guide*.

**Pagination in the Event Analysis view > Packet Analysis.** Pagination of packet data allows you to step through all the packets without rendering too much data at once. For more information, see the *NetWitness Investigate User Guide*.

**Configurable Event Analysis View Using Event Preferences Panel.** Analysts can personalize the Event Analysis views using the new Event Preferences panel. You can configure the default Event Analysis (Text, Packets, or File) and more display settings when you are analyzing an event. For more information, see "Configure User Preferences in Investigate" in the *NetWitness Investigate User Guide*.

**Direct Link to Events View Email and Web Reconstruction from Event Analysis View.** A link in the Event Analysis view opens the Web and email reconstructions of the selected event in the Events view reconstruction.

**Right-click Actions on Meta values in the Event Analysis View.** You can right-click a meta value in the Event Analysis view and launch actions such as look up the IP search and more. For more information, see the *NetWitness Investigate User Guide*.



**Right-Click Meta Value Count in the Navigate View.** Right-clicking the count next to a meta value in the Navigate view opens a context menu, from which you can send the event to a new tab in the Events view or the Event Analysis view. For more information, see the *NetWitness Investigate User Guide*.

## Reporting

**Reports for Endpoint Insights.** Analysts can define and generate reports using endpoint metadata for analysis. To generate reports, the endpoint metadata must be forwarded to a Log Decoder. For more information, see the *Reporting User Guide*.

## Health and Wellness

**Monitor Endpoint Server.** Administrators can monitor the health and wellness of the Endpoint Server from the Health and Wellness statistics. To monitor any statistics, you can create custom policies. For more information, see the *System Maintenance Guide*.

## Event Stream Analysis and ESA Analytics

**ESA Correlation Rules can use Context Hub data within rule logic.** Lists of values created as data sources in Context Hub can now be configured as data enrichment sources in ESA and used within correlation rules as blacklist or whitelist sources. New Context Hub lists are available by default in the ESA rules for NetWitness 11.1 users. Users upgrading from previous versions to 11.1 will see these default lists in addition to their previously created context hub lists. For more information, see “Configure Context Hub List as an Enrichment Source” in the *Alerting with ESA Correlation Rules User Guide*.

**Password change for ESA data source now available in UI.** When editing settings for a data source, users may now change the configured password through the UI for ESA services. For more information, see “Configure ESA Correlation Rules” in the *ESA Configuration Guide*.

## Core Services

**Truncation options added to balance analytic value and storage space.** An administrator can configure the system to save storage space by truncating data while still providing an analyst enough network data for analysis purposes. For more information, see “Configure Application Rules” in the *Decoder and Log Decoder Configuration Guide*.

**Meta Entities in Correlation Rules and Application Rules.** Administrators can create meta entities that represent two or more meta keys, and meta entities can be used anywhere that a meta key is used in the Log Decoder, Packet Decoder, and Concentrator rule builder. See the *Core Database Tuning Guide* for details.

**Search API enhanced to return matches across entire word.** This feature enhances the existing search API (msearch) to implement substring searches. A substring search is defined as finding arbitrary text somewhere in the middle, end, or beginning of a meta item. For example, an analyst can now search for “ball” in addition to “basket” to match “basketball.” For more information, see the *Core Database Tuning Guide*.

**Size buckets created to index size-related meta keys at the value level.** This feature provides the option to use size buckets to index size-related meta keys at the value level, which facilitates doing further queries on the data not available when meta keys are indexed at the key level. For more information, see the *Core Database Tuning Guide*.

**Capability added to optimize read/write operations on NWDB when adding new storage.** The 10G Decoder now supports the capability to run a command on an existing NWDB (packet, log, meta, or session), that has at least two volumes, to stagger the files across all volumes in the most optimal read-write pattern. This is useful when adding new storage to an existing Decoder so the volumes can be staggered before restarting capture. For more information, see “Optimize Read/Write Operations When Adding New Storage” in the *Decoder Configuration Guide*.

**Filter and rule hit counts provided to aid in troubleshooting.** An administrator can now generate statistics in the form of hit counts for implemented rules and see the aggregate value to gauge the impact of specific rules or filters. This provides more insight into the impact of filters and rules on the local environment. For more information, see “Monitor Application Rules” in the *Decoder Configuration Guide*.

## User Interface

**Choose Light and Dark themes.** You can now change the appearance of selected areas of NetWitness Suite User Interface from the global User Preferences settings. You have the option of viewing either the light or dark theme. For more information, see the *NetWitness Suite Getting Started Guide*.

## Platform

**Upgrade to CentOS 7.4 version.** The OS version of NetWitness Suite is upgraded from CentOS 7.3 to CentOS 7.4 in the 11.1 release.

## Administration

**Manage Access for Endpoints.** New roles and permissions are configurable in the ADMIN > Security > Roles and Permissions tabs to manage access for Endpoint related tasks. For more information, see the *System Security and User Management Guide*.

**Introduced Respond Notification Settings permissions.** These permissions enable Respond Administrators, Data Privacy Officers, and SOC Managers to access Respond Notification Settings (CONFIGURE > Respond Notifications), which enable them to send email notifications when incidents are created or updated. For more information, see the *NetWitness Respond Configuration Guide* and the *System Security and User Management Guide*.

**Configurable Permissions to Manage Access to Reconstruction in the Event Analysis View.** New permissions for the investigate-server are configurable in the ADMIN > Security > Roles tab. A message is displayed in the Event Analysis view when the administrator has restricted parts of the user interface by blocking individual permissions for a user role. For more information, see the "Role Permissions" section in the *System Security and User Management Guide*.

## Log Parsing

**Introduced Default Log Parser and Log Parser Rules tab.** Logs that do not have a corresponding parser will be processed against rules and metadata is then extracted by those rules and is available for Enrichment, Investigation, Reporting, and Alerting. To view this new tab, go to ADMIN > Event Sources > Log Parser Rules. This will provide immediate visibility into logs from custom or unsupported sources. Administrators can view and test sample log messages and rules for their log parsers, including the newly added Default log parser. The default log parser is used to parse logs coming from the Log Decoder that do not match any of your configured log parsers. In this new Default log parser, you can:

- View the rules for a particular log parser, including the default log parser.
- View the names, literals, patterns, and meta for each configured log parser.
- Edit sample log messages to view how they would be parsed by a particular log parser.

**Introduced Log Parser Customization.** You may need to modify one or more of your log parsers. For example, you may need to fix an unknown message, or to parse certain fields differently than in the manner provided by default. Log Parser Customization allows you to add a new file with new parser elements or modify existing custom files. All customizations in this separate file do not get removed or overwritten by Log Decoder upgrades or the updating of parsers through RSA Live. This feature is described in detail in the [Log Parser Customization](#) topic in the RSA Content space on RSA Link

**Remote Log Collector accepts secure Syslog.** The RLC now accepts secure Syslog messages, and can optionally verify the peer.

**Improved capture rate performance of Checkpoint Logs.**

**Note:** The following new features are located on the Event Source Discovery page.

**Introduced filtering by event source type.** Administrators can filter the event source discovery grid by device types to ensure that no extra event source types are included.

**Introduced acknowledging multiple event sources.** Administrators can select multiple event sources that have been discovered correctly and acknowledge them by clicking on the **Toggle Acknowledge** button. Acknowledged event sources are filtered from the view by default.

**Introduced mapping multiple event sources.** Administrators can select multiple event sources that have the same types that are not being discovered correctly and bulk map them to the appropriate parsers. This provides the ability to compare the event sources to an external list and quickly remediate the ones that do not match the list.

**Introduced Automatic Mapping.** The system automatically maps incoming events to a type based on previous logs received from that address, reducing the number of items that need attention in the Discovery workflow. The UI indicates that an address has been auto-mapped in the Discovery workflow.

**Moved the Acknowledge and Map filters to the Filter Panel on the Event Source Discovery page.** Administrators can quickly view and manage event sources.

**Introduced searching for event sources on the Event Source Discovery page.**

## Unified Data Model

**Unified Data Model for organizing various data.** Unified Data Model (UDM) in RSA NetWitness Suite provides a combined insight from Logs, Packets, and Endpoints. It organizes the various elements of data coming into NetWitness from disparate sources into one standardized data model. The Analysts can then look for data concepts in one place as defined by the Unified Data Model. Meta concepts defined in the UDM should be used uniformly across the suite to get the best consistent results. NetWitness uses Meta Keys as a way to retain context of the raw data after its parsed and stored on disk. Hence, it's extremely important to parse out data in the most accurate Meta key to retain context that's needed for Threat Detection, Analytics and Response. For more information, see the [UDM content on RSA link](#).

## Upgrade Instructions

---

The following upgrade paths are supported for RSA NetWitness Suite 11.1.0.0:

- RSA NetWitness Suite 10.6.5.x to 11.1.0.0
- RSA NetWitness Suite 11.0.0.x to 11.1.0.0

For more information on upgrading to 11.1.0.0, see the upgrade instructions in the [Product Documentation](#) section.

## Fixed Issues

This section lists issues fixed since the last major release.

### Security

Tracking Number	Description												
Libraries updated in 11.1 to address security vulnerabilities	<ul style="list-style-type: none"> <li>• Apache Commons Collections: to 3.2.2</li> <li>• Apache Commons Validator: to 1.5.1</li> <li>• Salt: to salt-2017.7.2-1.el7</li> <li>• Jpython: to 2.7.1</li> <li>• Jetty: Java based HTTP, Servlet, SPDY, WebSocket Server: to 8.1.2</li> </ul>												
ASOC-49307	Samba <a href="https://access.redhat.com/errata/RHSA-2017:3260">https://access.redhat.com/errata/RHSA-2017:3260</a>												
ASOC-49306	Curl <a href="https://access.redhat.com/errata/RHSA-2017:3263">https://access.redhat.com/errata/RHSA-2017:3263</a>												
ASOC-43884	Logstash Upgraded to 5.6.4, vulnerabilities addressed: <table border="1"> <thead> <tr> <th>ESA ID</th> <th>CVE</th> </tr> </thead> <tbody> <tr> <td>ESA-2017-05</td> <td><a href="#">CVE-2017-5645</a></td> </tr> <tr> <td>ESA-2016-08</td> <td><a href="#">CVE-2016-10362</a></td> </tr> <tr> <td>ESA-2016-06</td> <td><a href="#">CVE-2016-10363</a></td> </tr> <tr> <td>ESA-2016-02</td> <td><a href="#">CVE-2016-1000221</a></td> </tr> <tr> <td>ESA-2016-01</td> <td><a href="#">CVE-2016-1000222</a></td> </tr> </tbody> </table>	ESA ID	CVE	ESA-2017-05	<a href="#">CVE-2017-5645</a>	ESA-2016-08	<a href="#">CVE-2016-10362</a>	ESA-2016-06	<a href="#">CVE-2016-10363</a>	ESA-2016-02	<a href="#">CVE-2016-1000221</a>	ESA-2016-01	<a href="#">CVE-2016-1000222</a>
ESA ID	CVE												
ESA-2017-05	<a href="#">CVE-2017-5645</a>												
ESA-2016-08	<a href="#">CVE-2016-10362</a>												
ESA-2016-06	<a href="#">CVE-2016-10363</a>												
ESA-2016-02	<a href="#">CVE-2016-1000221</a>												
ESA-2016-01	<a href="#">CVE-2016-1000222</a>												
ASOC-43718	Kernel <a href="https://access.redhat.com/errata/RHSA-2017:2930">https://access.redhat.com/errata/RHSA-2017:2930</a>												
ASOC-42524	Kernel <a href="https://access.redhat.com/errata/RHSA-2017:2679">https://access.redhat.com/errata/RHSA-2017:2679</a>												
ASOC-49308	Tcpdump <a href="https://access.redhat.com/errata/RHSA-2017:1871">https://access.redhat.com/errata/RHSA-2017:1871</a>												

### Investigate

Tracking Number	Description
-----------------	-------------

ASOC-41703	In a mixed mode environment the Event Reconstruction View > File View displays the word "terminated" instead of the list of files.
ASOC-41696	Analyst is unable to unzip the downloaded file archive due to the zip file not having the restricted content.
ASOC-37989	Right-click action in the Log View does not launch Event Reconstruction on Event Analysis when you click on a Logs column that wraps to more than one row.
ASOC-37348	In Event Analysis, the rendered packets message is not displayed for events with a small payload but large number of packets.

## Log Collector, Virtual Log Collector

Tracking Number	Description
ASOC-49091, SMC-13792	Rebranded the Security Analytics Netflow Collector to Netwitness Netflow Collector in the CEF parser. RSA has renamed the <b>product name</b> value from "Security Analytics Log Collector" to " <b>NetWitness NetFlow Collector</b> " for the Netflow protocol on LogCollector. If you have any rules that use "Product name" meta, and is matching on the value "Security Analytics Log Collector," then that rule will not fire when you upgrade your Log Collector to 11.1. In this case, manually update these rules to match the new product name " <b>NetWitness NetFlow Collector</b> " .
ASOC-45452	Reworded an ODBC test connect log message to be more clear.
ASOC-45451	Resolved a Log Collector crash when closing an ODBC connection.
ASOC-45448	Added an ODBC configuration option to select whether <b>device.ip</b> is the actual source IP address, or if Log Collector event source IP address should be used for the <b>device.ip</b> meta value.
ASOC-31313	Added better handling for Windows log messages that contain malformed XML.
ASOC-16717	Bandwidth throttling configuration changes to control the rate that the Remote Collector sends event data to a Local Collector did not persist after a reboot. This issue has been fixed. The <code>set-shoveltransfer-limit.sh</code> script is used to set the bandwidth throttle for event data transferred from a remote collector to local collector.

## Context Hub

Tracking Number	Description
ASOC-40944, ASOC-50159	Pivot to Investigate navigates to an incorrect URL when rabbitmq server is not reachable.

## Respond

Tracking Number	Description
ASOC-41855	Unable to create an incident using 1000 alerts.
ASOC-41934	<p>In 11.0, the “Suspected Command &amp; Control Communication By Domain” aggregation rule Group By condition “Domain by Suspected C&amp;C” was not functioning as expected and had to be changed to “Domain” to aggregate alerts and enable incidents to be created for “Suspected C&amp;C.” The “Domain by Suspected C&amp;C” condition works correctly in 11.1 and should be used as the Group By condition for the “Suspected Command &amp; Control Communication By Domain” aggregation rule (known as incident rule in 11.1).</p> <p>If you changed the “Suspected Command &amp; Control Communication By Domain” aggregation rule Group By condition to “Domain” for 11.0, you will need to change it back to “Domain by Suspected C&amp;C” for 11.1. (To do this, go to CONFIGURE &gt; Incident Rules. In the Incident Rules list, locate the <b>Suspected Command &amp; Control Communication by Domain</b> rule and click the link in the <b>NAME</b> field to open it. In the Incident Rules Details view Grouping Options section, set the <b>Group By</b> field to <b>Domain for Suspected C&amp;C</b> and click <b>Save</b>.)</p>

## Event Stream Analysis and ESA Analytics

Tracking Number	Description
ASOC-39880	Trial rules become disabled despite low memory usage.
ASOC-45568	After upgrading to Security Analytics 10.5.1.1, ESA rules that leverage PostgreSQL database integration appear to no longer work.
ASOC-45569	When deploying an advanced rule with post-alert enrichment, if the advanced rule syntax does not contain @RSAAalert, rule deployment fails.



## Features Not Supported

The following tables provide information on features no longer supported in RSA NetWitness Suite 11.1 or Later Releases.

### Features Not Supported in 11.1.0.0 or later releases

No.	Feature	Notes
1	Malware Colo	Malware co-located is not supported in 11.1.0.0 and later releases. Malware Analysis is supported using a standalone Malware Analysis.
2	All-In-One (AIO) Deployment	All-in-one deployment is not supported. Fresh Install AIO has been removed.
3	Standalone Warehouse Connector	Standalone Warehouse Connector is not supported.
4	Administration Features	<ol style="list-style-type: none"> <li>1. Forgot my password.</li> <li>2. Email Notification to user when password expires.</li> <li>3. Changing the Login banner is not supported.</li> <li>4. Test/Search AD user.</li> </ol>
5.	Pivotal	Pivotal is not supported.
6.	ESA Cross-Site Correlation	The ESA Cross-Site Correlation configuration option (previously found by going to ADMIN > System > ESA) has been removed and will not be supported as part of the 11.1 release going forward. If a 10.6.5.x user that was using this feature upgrades to 11.1, a message will inform them that the feature is no longer available, but they will still be able to see and modify the correlation rules that had previously been used for Cross-Site Correlation.

### Features Available in Future Releases

The following features are not available in 11.1 and may be available in a future release.

No.	Feature	Notes
1	IPDB Reporting	IPDB Extractor service is not supported in 11.1.0.0 and will be available in later releases.
2	STIG	If you have a STIG hardened host, you cannot upgrade to 11.1.0.0 as the backup scripts do not support that.
3	Multiple Security Analytics Server (NetWitness Server) support	Multiple server deployment is not supported.
4	PKI Authentication	PKI Authentication feature is not available in 11.1.0.0
5	Warehouse Analytics	Warehouse Analytics is not supported for 11.1.0.0 and will be available in later releases.
6	Endpoint Analytics	Analytics, such as risk score or IOC calculation is not supported on the endpoint scan data
7	Endpoint Remediation	Response functionality (containment/blocking) is not supported.
8	Endpoint Tracking	Tracking network events is not supported.
9	Endpoint Kernel mode	Endpoint agent currently works in the User mode and does not support the Kernel mode detection
10	Endpoint File reputation	File reputation, such as OPSWAT, YARA, and Reversing Lab lookups are not supported and hence cannot whitelist or blacklist files.

## Known Issues

---

This section describes issues that remain unresolved in this release. Wherever a workaround is available, it is noted or referenced in detail.

### Known Issues During Upgrade to 11.1

The following known issues occur during upgrade from 10.6.5.x to 11.1 or update from 11..0.0.x to 11.1.

#### After offline update and reboot the UI still notifies to reboot host

**Tracking Number:** ASOC-50839

**Problem:** When you perform an offline update from 11.0.0.x to 11.1 and reboot through CLI, the UI still Notifies to reboot host.

**Workaround:** Reboot the host using the UI.

#### After upgrading to 11.1, there is Concentrator Initialization error if you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have the same fields indexed on the Concentrator

**Tracking Number:** ASOC-50702

**Problem:** This error occurs when you have done customized meta keys on your Log Decoder and Concentrator.

**Workaround:** If you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have those same fields indexed on the Concentrator, then you must change data type of these fields to IPv4 on both the Log Decoder and Concentrator.

#### Integration-server service is missing on the UI after update

**Tracking Number:** ASOC-50835

**Problem:** After upgrading 11.0.0.x to 11.1.0.0, the integration-server service is missing on the UI.

**Workaround:** None.

#### After upgrade from 10.6.5.x to 11.1.0.0, offline licenses are not retained.

**Tracking Number:** ASOC-41757

**Problem:** Even if you upload a new response bin file from Download Central, offline licenses still do not work. Though old files are restored in `/var/lib/fneserver`, the licenses still remain deactivated.

**Workaround:** Perform the following steps to restore the licenses:

1. Generate a new response bin file from Download Central.
2. SSH into a Netwitness Server host 11.1.0.0 (AdminServer).
3. Move ra\* files (3 files) out of `/var/lib/fneserver/`

4. Log in to RSA NetWitness 11.1.0.0 UI with admin user credentials and navigate to ADMIN > System > Licensing Overview tab.
5. Under Licensing actions, click Refresh licenses.
6. Upload the response file received from Download Central under ADMIN > System > Licensing > Settings Tab > Upload Response.

**Note:** Upgrade using Online mode (RSA NetWitness Suite 11.1.0.0 connected to the Internet) works successfully and all licenses are restored after upgrade to 11.1.0.0.

### **After you upgrade to 11.1.0.0, the logstash files are not updated in Logstash output configuration file**

**Tracking Number:** ASOC-49843

**Problem:** When you upgrade from 10.6.5 to 11.1.0.0 or 11.0.0.x to 11.1.0.0, logstash files are not updated in the Logstash output configuration file. This happens when they have a global audit setup.

**Workaround:** If global auditing is configured, you need to edit one of the syslog entries in the Global notifications servers and click Save to apply the latest Audit log configuration.

### **Configure Feed data from Endpoint via recurring feed not working after upgrade**

**Tracking Number:** ASOC-50601

**Problem:** After upgrade, the recurring feed configured from legacy NetWitness Endpoint does not work due to the change in Java version

**Workaround:** Import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store. For more information, see the 'Export the NetWitness Endpoint SSL Certificate' section in the *RSA NetWitness Endpoint Integration Guide*

### **Respond Notification Settings do not migrate from 10.6.5.x to 11.1**

**Tracking Number:** ASOC-49390

**Problem:** The Incident Management notification settings in NetWitness Suite 10.6.5.x are different from the Respond notification settings available in 11.1, so your existing 10.6.5.x settings will not migrate to 11.1.

**Workaround:** Manually update the Respond Notification Settings in 11.1. To do this, go to CONFIGURE > Respond Notifications and set the notification settings. You will need to add the list of SOC Manager email addresses. See the “Configure Respond Email Notification Settings” procedure in the *NetWitness Respond Configuration Guide*.

Notification Servers from previous releases will not display in the Email Server drop-down list. The email servers settings must be edited and saved in the Global Notification Servers (ADMIN > System > Global Notifications > Server tab).

Custom Incident Management notification templates cannot be migrated to 11.1. No custom templates are supported in 11.1.

To access these settings, you will need additional permissions. See “Respond Notification Settings Permissions” in the *NetWitness Respond Configuration Guide*. For detailed information about user permissions, see the *System Security and User Management Guide*

### Unable to select Domain for Suspected C&C and Domain in the rule builder

**Tracking Number:** ASOC-46834

**Problem:** When adding a condition to an Incident Rule, there is no option to select **Domain for Suspected C&C** from the match conditions drop-down list. Also, after upgrade to 11.1, for some incident rules, the **Domain** and **Domain for Suspected C&C** fields are blank.

**Workaround:** Use **Domain** in the Match Conditions drop-down list for both **Domain** and **Domain for Suspected C&C**. Pre-upgrade, make note of the rules that contain the Domain and Domain for Suspected C&C match conditions including the operators and values. After upgrade, manually add the conditions to 11.1 using only **Domain** in the Match Conditions.

1. Go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.
2. In the **Match Conditions** section, select **Domain** in the drop-down list (instead of Domain for Suspected C&C) and enter the rest of the condition.
3. Enter the remaining information for your rule and click **Save**. For more information about incident rules, see the *NetWitness Respond Configuration Guide*.

### Respond – Missing Group By field in Aggregate Alert will not fire

**Tracking Number:** ASOC-49820

**Problem:** In 10.6.5.x, you do not require incident rules to use the **Group By** field. If you have any rules that do not use the Group By field in 10.6.5, then after upgrade you will need to manually add a value to the Group By field as it is a required field in 11.1. Without a Group By field value, the rules will not work and they will not create incidents.

**Workaround:** Add a Group By field value to the rules that do not use the Group By field. For each incident rule:

1. Go to **CONFIGURE > Incident Rules** and click the link in the **Name** column for the rule that you want to update.
2. In the **Group By** field, verify that a Group By value is selected. If not, select a Group By value.
3. Click **Save** to update the rule.

For more information about incident rules, see the *NetWitness Respond Configuration Guide*.

### Aggregation Stops after Reconnection to Mongo

**Tracking Number:** ASOC-50911

**Problem:** After configuring the Mongo database and rebooting the ESA server, incidents are not being created. The ESA primary server acts the database host for NetWitness Respond application data. The NetWitness Server acts as the database host for NetWitness Respond control data. After the application database is configured on the ESA server and restarted, you must also restart the Respond service on the NetWitness Server..

**Workaround:** After configuring the Mongo database and rebooting the ESA server, restart the respond-server service..

From the command line:

```
systemctl restart rsa-nw-respond-server
```

Or from NetWitness suite:

Go to **ADMIN > services**, select the Respond Server service, and then select   > Restart.

### FIPS is disabled by default for the Log Collector Service

**Tracking Number:** ASOC-41841

**Problem:** FIPS is disabled by default for the Log Collector service, even if FIPS was enabled in 10.6.5.x.

**Note:** Even if FIPS is enabled in 10.6.5.x, it becomes disabled post-migration.

**Workaround:** To enable FIPS on the Log collector service, perform the following steps:

1. Stop the Log Collector service.
2. Open the `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` file.
3. Change the value of the following variable to **off** as described here:
 

```
Environment="OWB_ALLOW_NON_FIPS=on"
to
Environment="OWB_ALLOW_NON_FIPS=off"
```
4. Reload the system daemon by running `systemctl daemon-reload` command.
5. Restart the Log Collector service.
6. Set the FIPS mode for the Log Collector service on the UI:

**Note:** This step is not required in case of upgrade, if FIPS was enabled on 10.6.5.x.

- a. Go to ADMIN > Services.
- b. Select the Log Collector service and go to View > Config.
- c. In SSL FIPS Mode, select the checkbox under Config Value and click **Apply**.

**Note:** To enable Log Decoder and Packet Decoder, in `/sys/config` set `ssl.fips` to ON and restart the service.

### The investigation links are disabled for static charts during 10.6.5.x to 11.1 post-upgrade

**Tracking Number:** ASOC-42136

**Problem:** The investigation link is disabled for the static chart (the result of the report is in chart format) which has the datasource as NetWitness Suite-Broker (This service is available by default).

**Workaround:** There are two workarounds for this issue:

- The rules that have the result in a static chart can be viewed in Tabular format and the investigation works as expected.
- Or you can perform the following steps to fix the issue:
  1. Delete and add the NetWitness Suite-Broker again as the datasource to Reporting Engine with the same name.
  2. If the reports with a static chart are scheduled reports, then in the next run, the investigation link will work as expected.
  3. If the report is an Adhoc report, then re-run the report for getting the investigation links.

### Post upgrade from 10.6.5.x to 11.1.0.0, Warehouse Connector is not installed on Decoders

**Problem:** The Warehouse Connector is not installed on the Decoders by default.

**Workaround:** If, after an upgrade there is a need to re-establish a Warehouse connection, a utility is provided to reinstall the service. The utility is deployed during the bootstrap phase. To install Warehouse Connector, you must run the following command and specify the host by ID (`--host-id`), name (`--host-name`), or address (`--host-addr`). The latest available version will be installed by default unless a specific version is specified with `--version`. To install the Warehouse Connector on a host, run the following command on the Admin server:

```
[root]warehouse-installer --host-id <uuid of the host>
```

Details about the command:

Location: `/usr/bin`

Utility Name: `warehouse-installer`

Usage:

```
[root@nw11pds5 bin]# warehouse-installer --help
```

Warehouse Connector Installer

```
warehouse-installer [options]
```

Install options:

`--host-id <id>` Specify host to install (by ID)

`--host-name <name>` Specify host to install (by name)

--host-addr <address> Specify host to install (by address)

--version <#.#.#.#> Install version (defaults to latest)

General options:

-v, --verbose Enable verbose output

### **Post upgrade from 10.6.5.x to 11.0.0.x, duplicate dashboards for threat indicators**

**Tracking Number:** ASOC-41701

**Problem:** The dashboard, Threat-Indicators, was updated to report against new Hunting meta keys and renamed to Threat-Malware Indicators. On upgrade, both will appear in the UI instead of the old being replaced.

**Workaround:** Enable the Threat-Malware Indicators report charts and dashboard and disable the old Threat-Indicators dashboard.

### **On upgrade, the Health and Wellness custom policies for Context Hub Server are not available.**

**Tracking Number:** ASOC-41826

**Problem:** When you upgrade to Netwitness Suite 11.1.0.0, the Health and Wellness custom policies configured for 10.6.5.x Context Hub server will not be available.

**Workaround:** You must define these custom policies in 11.0.0.x.

### **On upgrade to 11.0.0.x, collections created from a 10.4 or later Workbench display blank Date Range and Date Created values**

**Tracking Number:** ASOC-9035

**Problem:** Any collections created from a 10.4 or later Workbench displays blank Date Range and Date Created values after upgrading to 11.0.0.x.

**Workaround:** None.

### **On upgrade from 10.6.5.x to 11.1, the Geo-map dashlet cannot be created using a pre-configured (OOTB) chart.**

**Tracking Number:** ASOC-41896

**Problem:** When you upgrade to Netwitness Suite 11.1.0.0, the Geo-map dashlet cannot be created using a preconfigured chart. This happens if a custom dashboard uses a Geo-map dashlet, which is created using a preconfigured chart.

**Workaround:** The data source must be manually updated for that preconfigured chart that is required to be used in the dashlet with Geo-map. Or, create a new chart using the same preconfigured rule and use the new chart in the dashlet with Geo-map.


### **On upgrade from 11.0 to 11.1, if you have been using the Entropy Parser and indexing payload, you will need to add the bucket flag to the index file so that the Entropy Parser can use index buckets.**

**Tracking Number:** ASOC-45721



**Problem:** When you upgrade to NetWitness Suite 11.1.0.0, if you have been using the Entropy Parser on the Decoder (packets only) and are indexing payload, you must add the bucket flag to your index file to take advantage of the new index buckets feature.

**Workaround:** Add bucket flag to index file so Entropy Parser can use index buckets, as follows:

1. In the NetWitness Suite menu, select **ADMIN > Services**.  
The Services view is displayed.
2. Select each Concentrator service that is aggregating traffic from the decoders.
3. Under  (actions), select **View > Config** and select the **Files** tab.
4. Select the `index-concentrator.xml` file and set the bucket flag to `true` for `payload.req` and `payload.res`. For example:

```
<key description="Payload Size Request" format="UInt 32"
level="IndexNone" bucket="true" name="payload.req"
valueMax="500000"/>
```

```
<key description="Payload Size Response" format=UInt32"
level="IndexNone" bucket="true" name="payload.res"
valueMaz="500000"/>
```

5. Click Apply.
6. For changes in the `index-concentrator.xml` file to take effect, you must restart the jetty service on the NW Server:  

```
systemctl restart jetty.service
```

## Context Hub

### OutOfMemory Error in the Context Hub service when large number of TAXII feeds are configured

**Tracking Number:** ASOC-41664, ASOC-42002

**Problem:** The Context Hub service runs into OutOfMemoryError and becomes unresponsive, if a large number of TAXII feeds are configured to fetch data.

**Workaround:** Restart the Context Hub service and make sure that the time range you select to fetch TAXII feeds from the TAXII server is not more than 6 months. If the issue persists even after updating the time range, see the Troubleshooting topic in the *Live Services Management Guide*.

**Single-column and multi-column lists added from the Data Source tab are not supported for Add to a list and Remove from list.**

**Tracking Number:** ASOC-37998

**Problem:** When you do a lookup on a specific context meta in the Investigation, Events, or Respond view, the list names displayed are the ones which have matching values.

When you right-click on a specific meta value and select the Add or Remove list option, the single-column and multi-column list names added from the data source tab will not be displayed. It will only display the lists added from the UI using the Lists tab.

**Workaround:** You need to manually add the values that were added from the Data Source tab to the specific CSV file. So that, next time when the scheduler runs, the values from the updated CSV file will be available in the specific lists.

### Empty list is imported when list has values with missing quotes

**Tracking Number:** ASOC-34187

**Problem:** When you import a list with missing quotes such as “172.16.0.0, the list is saved without any data. This is because of the Apache bug (CSV-141), which does not parse the CSV file with incorrect format.

**Workaround:** Import a list with correct quotes. For example, “172.16.0.0”, “host.mycompany.com” and so on.

### SSL handshake with RSA Archer certificate fails while adding it as a data source

**Tracking Number:** ASOC-32654

**Problem:** When you try to add RSA Archer as a data source using valid credentials, the test connection fails (ARCHER-37085). This happens when the 'Trust all Certificates' option is unchecked and you try to upload an RSA Archer trust certificate.

**Workaround:** Select the 'Trust All Certificates' checkbox and do not upload a certificate.

## General Application Issues

### The System Logs Off Idle Users in Respond and Some Investigate Views

**Tracking Number:** ASOC-46483

**Problem:** In the Respond view and some Investigate views (Event Analysis, Hosts, and Files), if a user is not actively querying data, the system logs off the user after the Idle Period is reached. The default Idle Period is 600 seconds (10 minutes). This can cause the work of an Analyst to be interrupted.

**Workaround:** If this becomes an issue with the Analysts, in the global security settings (ADMIN > Security), consider increasing the values of the **Session Timeout** and the **Idle Period**.

## Endpoint

### Unable to export files list to a CSV file

**Tracking Number:** ASOC-47549

**Problem:** While exporting data to a CSV file, database query takes a longer time when the database is under heavy load, and the UI request times-out.

**Workaround:** Apply appropriate filters and use at least one indexed field with an **Equals** operator to reduce the files for export. For more information on Filtering Hosts and Files, see *NetWitness Investigate User Guide*.

### Sorting on Agent Scan Status and Agent Last Seen fields are not accurate

**Tracking Number:** ASOC-50057

**Problem:** In the **Investigate > Hosts** view, sorting on Agent Scan Status and Agent Last Seen fields do not display the correct order.

**Workaround:** None

### Unable to generate Agent Packager if the auto uninstall is set in seconds

**Tracking Number:** ASOC-49324

**Problem:** In the **Auto Uninstall** field, if the seconds value is more than 9, for example, 02/12/2018 12:00:10 PM, then click **Generate Agent** fails to generate the packager.

**Workaround:** Enter a value below 10 seconds in the Auto Uninstall field.

### Sorting on columns should not be case-sensitive

**Tracking Number:** ASOC-32595

**Problem:** Sorting on columns in the Hosts and Files view is case-sensitive. It sorts the number first, uppercase, and then the lowercase.

**Workaround:** None.

### No message is displayed when filtering the values takes more than 60 seconds.

**Tracking Number:** ASOC-50197

**Problem:** In the Hosts and Files view, while filtering the values, if it takes more than 60 seconds, the UI does not display any message or results.

**Workaround:** None.

### Generate and copy \*nwelcfg file, does not update the timestamp

**Tracking Number:** ASOC-49847

**Problem:** After installing the Endpoint Insights Agent, if the Administrator wants to update a new Log Collection configuration and the endpoint agent

After installing the Endpoint agent, if the administrator wants to update a new Log collection config via any of the copy methods or third party endpoint management tool, the config file timestamp remains as that of the Endpoint server time and not the agent time. As a result, if the endpoint agent is on a different timezone from the endpoint server, the timestamp does not get updated properly.

**Workaround:** After copying the file, run the command on the Endpoint Agent: `copy /b <filename.nwelcfg> +,,` from the folder `%programdata%\NWEAgent\` where the `nwelcfg` file is there.

### Disable log collection in Windows Endpoint Agent is not supported

**Tracking Number:** ASOC-49846

**Problem:** Once an Endpoint Agent is installed with the windows log collection feature enabled, the user is unable to disable windows log collection.

**Workaround:** Run the uninstall command provided in the "Uninstall Agents" section in the *Endpoint Agent Install guide*. Reinstall an agent with windows log collection disabled.

### Endpoint Agent - Account for Unresponsive UDP

**Tracking Number:** ASOC-40844

**Problem:** When the Primary Log Decoder/Remote Log Collector is not reachable and the Endpoint agent is configured to use UDP, the Secondary Log Decoder/Remote Log Collector is not used - this can lead to event loss.

**Workaround:** None.

### Secondary LD/VLC cannot be unselected

**Tracking Number:** ASOC-48755

**Problem:** When an option is selected in the secondary channel for LD/VLC, then it cannot be unselected.


**Workaround:** Primary LD/VLC is a required field and it always needs a destination. Secondary option is an optional field. You can click **Reset** in the Packager UI and start again or refresh the page.

## Respond

### Related Links URL created for Malware Events is invalid

**Tracking Number:** ASOC-48392

**Problem:** In the Respond Alert Details and Incident Details views, the URL link for a Malware Analysis alert is invalid. To view the URL link in the Alert Details view, go to RESPOND > Alerts and in the Alerts list, click the link in the NAME column for a Malware Analysis alert. In the Event Details, you can see the URL for the Malware Analysis alert.

To view the URL link in the Incident Details view, go to RESPOND > Incidents and in the Incidents list, click the link in the ID or NAME column for a Malware Analysis incident. In the Incident Details view, click the View Datasheet icon () to view the event details. If there are multiple events listed, click an event to view the event details. In the Event Details, you can see the URL for the Malware Analysis alert.

**Workaround:** None

### Overlapping Relationship Data in the Nodal Graph for Certain Data

**Tracking Number:** ASOC-48034

**Problem:** In the Respond Incident Details view nodal graph, when there are multiple relationships within an incident, the text can overlap on the arrows between the nodes, which is difficult to read. This issue appears in an incident when the source IP of the alert is also the destination IP of another alert and the destination IP of the first alert is the source IP of the second.

**Workaround:** None

### **Respond Administrator cannot query Investigate or view Live dashlets in the Dashboard**

**Tracking Number:** ASOC-40749

**Problem:** The Respond\_Administrator role does not have permission to query Investigate. This is necessary so that the Respond Administrator can pivot to Investigate or create incidents from events. The Respond\_Administrator Role also does not have the Live: Access Live Module permission, which is required to view Live dashlets in the dashboard.

**Workaround:**

1. Manually create the Respond\_Administrator role on the Core services. To do this, go to ADMIN > Services, select a Core service, and then in the Actions drop-down list, select View > Security > Roles Tab. Click + to add the Respond\_Administrator role. Add the following permissions to the Respond\_Administrator role:
  - sdk.content
  - sdk.meta
  - sdk.packets
  - storedproc.execute

Replicate the Respond\_Administrator role to other Core services that may be used by the users.

2. In the ADMIN > Security > Role tab, add the Live: Access Live Module permission to the Respond\_Administrator role.

### **Malware event File name with Korean characters is not shown properly in the Respond view**

**Tracking Number:** ASOC-40159

**Problem:** If there are Korean characters in an alert that is received from Malware Analysis, they will not be displayed correctly in the Respond view.

**Workaround:** None.

### **Unable to query domain in source/destination.device.geolocation**

**Tracking Number:** ASOC-39938

**Problem:** Geo-location that comes from ESA Correlation Rules is not available in the Incident Details view Related Indicators panel. (To access the Related Indicators panel, Go to RESPOND > Incidents and in the Incidents List, click the ID or NAME link of the incident. In the Incident Details view toolbar, click the Journal, Task, and Related icon. The Journal is displayed on the right. Click the RELATED tab.)

**Workaround:** None. This is a new functionality, so it is just data that is not searchable.

### **Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is not valid in NetWitness Suite 11.1.0.0**

**Tracking Number:** ASOC-41891

**Problem:** NetWitness Suite 11.1.0.0 will only work with NetWitness SecOps Manager 1.3.1.2. However, the Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is navigating to the legacy Security Analytics Incident Management page, which is not valid in NetWitness Suite 11.1.0.0.

**Workaround:** None.

### **ESA Rules with severity as High or Low are not populated in the RSA Archer UI**

**Tracking Number:** ARCHER-47101

**Problem:** When ESA alerts with severity High or Low are forwarded to RSA Archer, the Security Alert Priority field is not populated in the RSA Archer UI.

**Workaround:** None.

### **ESA Command and Control Aggregate Scores details are not populated in the RSA Archer UI.**

**Tracking Number:** ASOC-50183

**Problem:** When ESA Command and Control Aggregate Scores details are forwarded from NetWitness Suite to RSA Archer UI, fields such as Beaconsing Behavior, Rare Domains, Rare User Agents, Missing Referrers, and Suspicious Domains Aggregate Score do not get populated.

**Workaround:** None.

### **Incidents and Tasks are still available when RSA NetWitness SecOps Manager integration is enabled**

**Tracking Number:** ASOC-39886

**Problem:** After enabling NetWitness SecOps Manager integration in the Respond Server service, all incidents are managed in NetWitness SecOps Manager. In previous versions, when SecOps was enabled, incidents and remediation tasks were hidden. In NetWitness Suite 11.0.0.x, users are still able to access incidents and tasks in the Respond view (RESPOND > Incidents and RESPOND > Tasks). They are also not prevented from creating incidents in NetWitness Suite. If they create incidents from the Respond Alert List view (RESPOND > Alerts) or from Investigate, those incidents will not go to NetWitness SecOps Manager.

**Workaround:** If you enabled SecOps Manager integration in the Respond Server service, do not use the following in the Respond view: Incidents List view, Incident Details view, and Tasks List view. Also, do not create incidents from the Respond Alerts List view or from Investigate.

### **For migrated incidents, the event count always shows as 0 in the Overview panel**

**Tracking Number:** ASOC-38026

**Problem:** In the Incidents Overview panel Catalysts field, the number of events for migrated incidents always shows as 0 (zero). This is expected behavior in NetWitness Suite 11.0.0.x (To access the Overview panel, go to Respond > Incidents. If you click an incident in the Incidents List, the Overview panel appears to the right. If you click a link in the ID or NAME field in the Incidents List, the Incident Details view opens with the Overview panel on the left.)

**Workaround:** None.

### **Unable to Pivot to Investigate on all username, filename, and domain values when multiple values are present**

**Tracking Number:** ASOC-37997

**Problem:** If username fields contain commas that do not represent delimiters between values, you may not be able to pivot to Investigate on certain meta if there is more than one value in the field.

**Workaround:** You can query or pivot on other data, or manually investigate the meta. You can still access the meta through Investigate.

### **In memory table enrichment info is not displayed for ESA alerts**

**Tracking Number:** ASOC-37533

**Problem:** You cannot view custom enrichments for ESA Correlation Rules in the Respond Alerts view.

**Workaround:** None.

### **DOMAIN and HOST metas do not display correctly in the Respond view**

**Tracking Number:** ASOC-37232

**Problem:** Domain and Host metas may be incorrectly labeled in the Respond Incidents Details view when alias.host contains different types of data. The Domain field behavior is inconsistent and it may be populated with hostnames.

**Workaround:** None. Multiple types of information will continue to exist in the Domain field.

### **After upgrade, unable to filter incidents using the Assignee field**

**Tracking Number:** ASOC-36973

**Problem:** After upgrading incidents from 10.6.5.x to 11.0.0.x, Analysts are not able to filter the migrated incidents using the Assignee field (RESPOND > Incidents - Filter panel).

**Workaround:** None.

### **Respond - Create Incidents from Alerts in the Respond Alert List view**

**Tracking Number:** ASOC-35811

**Problem:** When you manually create an incident from alerts in the Respond Alert List view (RESPOND > Alerts) in 11.0.0.x, you just have the minimum functionality to create an incident from alerts. You can only provide a name for the incident and the priority defaults to Low. When manually creating an incident, you do not have additional options, such as adding a Priority, Assignee, or Category.

**Workaround:** You can update additional fields by manually editing the incident after you create it, such as changing the priority from Low to High. However, you cannot add a category to an incident.

### **Whitelist Domains while closing Incidents as False Positive**

**Tracking Number:** ASOC-25135

**Problem:** In 10.6.5.x, if a Suspected C&C Incident was marked as "Closed - False Positive" , an entry was made to the "Whitelisted Domains" list from context hub. There should be a similar functionality in the Respond view.

**Workaround:** Analysts can manually add domains to a whitelist in the Respond view. The *NetWitness Respond User Guide* provides procedures.

### **Integration Settings for SecOps Manager should be exposed in the User Interface**

**Tracking Number:** ASOC-25127

**Problem:** The Integration settings for sending all incidents to RSA NetWitness SecOps Manager should be exposed in the user interface.

**Workaround:** The user interface for partial RSA NetWitness SecOps Manager integration was removed in 11.0.0.x. Administrators can complete the integration from the Explorer view for the Respond Server service.

### **Incidents are not flagged when a user manually adds alerts to an existing incident**

**Tracking Number:** ASOC-16640

**Problem:** Investigation values are not highlighted when alerts in Respond have manually been added to an incident. Alerts that are dynamically added to an incident will get highlighted.

**Workaround:** None.



## Log Collector

### The vsftpd service has been changed to support only TLSv1.2

**Tracking Number:** ASOC-42497

**Problem:** For compliance reasons, the **vsftpd** service configuration on Log Collector and Virtual Log Collector nodes has been changed to support only TLSv1.2 and high encryption ciphers. TLSv1.0, 3DES and NULL encryption will no longer be accepted by default. This will break uploading of log files by FTPS protocol from event sources that do not support higher encryption.

**Workaround:** Use the following procedures to restore collection.

If you have event sources requiring TLSv1.0, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_tlsv1=NO` to `ssl_tlsv1=YES`
2. Restart **vsftpd** service by running this command:

```
systemctl restart vsftpd
```

If you have event sources requiring 3DES and/or NULL encryption, use the below steps:

1. Edit `/etc/vsftpd/vsftpd.conf` and change the line `ssl_ciphers=HIGH:-3DES:-aNULL` to `ssl_ciphers=HIGH`
2. Restart **vsftpd** service by running this command:

```
systemctl restart vsftpd
```

### DPO Role missing on Log Collector

**Tracking Number:** ASOC-7937

**Problem:** The new Data Privacy Officer role does not exist on the Log Collector.

**Workaround:** None.

### Checkpoint collection not working with error "peer ended the session"

**Tracking Number:** ASOC-8351

**Problem:** The checkpoint collection is not working and the logs show the error: **peer ended the session**

**Workaround:** To resolve this issue:

1. Make a backup and then remove the checkpoint position file (`/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_Security.xml`).
2. Restart the service to regenerate the file.
3. (Optional) If the **Max Idle Time Poll** is set to 0, set it to 20.

**Note:** By removing the position file, your Log Collector may re-collect a substantial amount of log data.

## Investigate

**Three new meta groups for 11.0 and the same column groups for 11.1 are not created when you upgrade from 10.6.5 to 11.x: RSA Endpoint Analysis, RSA Outbound HTTP, RSA Outbound SSL/TLS.**

**Tracking Number:** ASOC-51011

**Problem:** When you upgrade from Version 10.6.5 to 11.x, three out-of-the-box meta groups (RSA Endpoint Analysis, RSA Outbound HTTP, and RSA Outbound SSL/TLS) are not created due to a conflict with a column group added in Version 11.0. When you upgrade from Version 10.6.5 to 11.1, three out-of-the-box column groups (RSA Endpoint Analysis, RSA Outbound HTTP, and RSA Outbound SSL/TLS) are not created. These meta groups should appear in the Manage Meta Groups dialog and the Manage Column Groups dialog.

**Workaround:** None.

**After upgrading to 11.1, there are mismatched data types between the Log Decoder (table-map.xml) and Concentrator (index-concentrator.xml) definitions.**

**Tracking Number:** ASOC-50702

**Problem:** This error occurs when you have done customized meta keys on your Log Decoder and Concentrator.

**Workaround:** If you have 'stransaddr' and 'dtransaddr' enabled on the Log Decoder and you have those same fields indexed on the Concentrator, then you must change data type of these fields to IPv4 on both the Log Decoder and Concentrator.

**If the URL for a drill point is very long and you use the query in the Event Analysis view, an error (414 Request error) is returned.**

**Tracking Number:** ASOC-50196

**Problem:** Several situations create a very long query that the browser cannot handle, especially if you are using Internet Explorer, which has a much lower character limit than most browsers. Pivoting to Event Analysis from Reporting can result in a very long query, and a number of pivots in the Navigate view can create a very long query.

**Workaround:** Continue to work in the Navigate view or Events view when the URL becomes too long to render in the Event Analysis view.

**Attempting a direct query, or query via link, that uses an IPV6 meta value with unsupported special characters generates an error in the Event Analysis view and the Navigate view.**

**Tracking Number:** ASOC-50924

**Problem:** Literal ipv6 addresses with a percent (%) sign and also UNC Path Names such as 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net are not supported. The error in the Event Analysis view is Internal Server Error. The Navigate page shows a syntax error.

**Workaround:** None.

**If you got to Event Analysis by way of the Events view, either by clicking the Event Analysis link or by right-clicking one of the events, the right-click options on meta values do not work.**

**Tracking Number:** ASOC-50771

**Problem:** If you clicked Event Analysis in the Detail View of the Events view, the Event Analysis view opens as usual. However, the right-click options on a meta value in the Event Meta panel do not work.

**Workaround:** If you go through **Navigate > Event Analysis**, or if you go through Events and a reconstruction of an event, the right-click options function in Event Analysis.

**The service keeps loading infinitely.**

**Tracking Number:** ASOC-49854

**Problem:** This sometimes occurs when you open Event Analysis from the Navigate view or the Event view, and when you refresh the Event Analysis view.

**Workaround:** Refresh the page in the browser.

**Cannot add meta entities to a custom column group in the Events view with the Optimize Investigation Page Loads option disabled.**

**Tracking Number:** ASOC-50712

**Problem:** Meta keys belonging to meta entities are not displayed in custom column groups. This issue is seen in the Events view when you disable Optimize Investigate Page Loads in the Events view settings and then refresh the page.

**Workaround:** If you want to use meta entities in a custom column group, ensure that the Optimize Investigation Page Loads option is enabled.

**Custom column groups that contain meta entities can be created in the Events view, but when the custom column group is used in the Event Analysis view, you cannot see the meta keys included in the meta entity in the results.**

**Tracking Number:** ASOC-50349

**Problem:** Custom column groups are not displaying meta keys that belong to meta entities. This issue is seen in the Events list in the Event Analysis view.

**Workaround:** Use a column group that does not contain meta entities. However, meta entities can still be queried and used in the query builder.

**When downloaded from the Event Reconstruction view, logs and metadata are always in text format irrespective of the format selected in the Events view.**

**Tracking Number:** ASOC-50091

**Problem:** When you download metadata or a log in the Event Reconstruction view, the format that you selected in the Events view is not used. The exported data is always in text format.

**Workaround:** Download metadata and logs from the Events view if you want to use a format other than text format.

**When you right-click on a meta value that contains a semicolon in the Event Analysis view and attempt to apply the drill in a new tab in the Navigate view, there is an error: Unable to build visualization****Tracking Number:** ASOC-50041**Problem:** The URL is correctly formed in the Event Analysis view, but when received in the Navigate view, only the part of the string before semicolon is queried, and everything after it is stripped off.**Workaround:** Enter the query, complete with the semicolon, directly in the Query dialog in the Navigate view or Events view.**The query builder in the Event Analysis view is unresponsive for filters that contain a space.****Tracking Number:** ASOC-49427**Problem:** When adding a filter, if you add an extra space before <meta key>, between <meta key> and <operator>, and after <operator>, the query builder becomes unresponsive and the Query Events button is disabled so that you cannot continue adding filters.**Workaround:** Click on an existing filter, and then click the query builder. If that does not work, refresh the page.**When you alter the URL and the new URL is for a restricted event, the reconstructed content for the previous query persists in the Event Analysis view and no error message is displayed.****Tracking Number:** ASOC-45198**Problem:** After viewing an event that you have access to, if you change the URL to an event you are restricted from viewing the content of the previous event is still displayed.**Workaround:** None.**When you enter a query to a session to which you do not have access in the Event Analysis view, no data is displayed and there is no error message.****Tracking Number:** ASOC-48945**Problem:** If you enter a query in the Event Analysis view query builder that would result in viewing an event you are restricted from viewing, no data is displayed and there is no error message.**Workaround:** You can check the URL in the Navigate view (**Navigate > Actions > Go to event in Event Analysis**), and the following message will be displayed: "Session is unavailable for viewing."**When investigating in the Event Analysis view, the following error message is returned: "An Unexpected error has occurred."****Tracking Number:** ASOC-48710**Problem:** This error is displayed when the session you are attempting to access has been removed, rolled out, or you have insufficient permission to view the session.**Workaround:** None.

**In a mixed-mode environment, an analyst with insufficient permissions can download PCAPs and logs from a 10.6.5.x service in the Investigate > Event Analysis View, but not files or payloads.****Tracking Number:** ASOC-49676, 41698

**Problem:** Role-Based Access Control (RBAC) on the 11.0.0.x and 11.1 NW Server is not applied uniformly to downloads when investigating 10.6.5.x services. If the `sdk.packets` setting has not been disabled, analysts with SDK Meta and roles permission in place to restrict viewing and reconstructing event content can download the PCAP and log of an event that has content restrictions. Other types of downloads appear to download, then generate errors due to insufficient permissions, and the data is still protected.

**Workaround:** Disable the `sdk.packets` setting on 10.6.5.x services to limit the analyst from downloading any PCAPs or logs during phased upgrade. When the upgrade of all services is complete, re-enable the `sdk.packets` setting in all services. The RBAC experience will be consistent across all services. See the “UpgradeTasks” section in the *Physical Host Upgrade Guide* for details.

**Issue with Interaction between Expand and Contract Icons in Investigate Event Analysis.****Tracking Number:** ASOC-47670

**Problem:** When you contract the left panel in the Event Analysis view, the right panel expands, but the expand/contract icon on right panel does not change to the contract icon. To contract the right panel using the expand/contract icon on the right panel you have to press it twice. The behavior should be that when you contract the left panel and the right panel expands, the expand/contract icon for right panel switches to contract and vice versa. There is a similar issue with the Show/Hide Events panel icon. If the Event panel is contracted and you click on the Show/Hide Events Panel icon, the left panel disappears and the right panel expands. The expand/contract icon on the right (and now only) panel remains in expanded form. When you click on the expand icon in this configuration, the left panel reappears and the right panel effectively contracts. The behavior should be: after you hide the left panel, the expand/contract icon on the right panel should take its contract form.

**Workaround:** When the expand/contract icon in the right panel or the Show/Hide Events panel icon in the toolbar has not changed to the correct state, click the icon twice.

**PCAP and payload download issues in Event Analysis view in a Mixed Mode Environment****Tracking Number:** ASOC-37309

**Problem:** The Event Analysis workflow requires all services to be running 11.0.0.x. If the NW Server, Broker, and Concentrator are running 11.0.0.x, and the Decoders are running 10.6.5.x, the admin user will not be able to download files, logs, PCAPs, and payloads.

**Workaround:** Download files from Event Reconstruction.

**Parallel Coordinate visualization is not displaying special characters correctly****Tracking Number:** ASOC-9346

**Problem:** When configuring the meta key content type as one of the meta for the axis, if the meta value contains any special characters, the values do not display correctly.

**Workaround:** None.

## Workbench

### Empty collection seen in Collections tab

**Tracking Number:** ASOC-6859

**Problem:** An empty collection is seen in the Collections tab if the workbench service stops or restarts during restoration process

**Workaround:** None.

### Data range is not displayed for collection if workbench service or Jettysrv is restarted while restoration is in process

**Tracking Number:** ASOC-6822

**Problem:** The date range is not displayed for a collection if the workbench service or Jettysrv is restarted while the restoration is in process.

**Workaround:** None.

## Custom Feeds

### RSA Archer Recurring Feeds failing in SSL mode

**Tracking Number:** ARCHER-41524

**Problem:** RSA Archer recurring feeds does not work in SSL mode.

**Workaround:** You must create the RSA Archer recurring feeds in non-SSL mode..

### The status of STIX feed progress bar is incomplete.

**Tracking Number:** ASOC-40642

**Problem:** Sometimes, the status of the progress bar for some of the STIX feeds are incomplete even if the feeds are successfully pushed to the Decoder(s).

**Workaround:** None.

## Malware Analysis

### Users with Analyst role are not able to run the on-deman malware scan

**Tracking Number:** ASOC-5425

**Problem:** A user who has the Analyst role has access to the Investigation and Malware Analysis modules. But when the user tries to run the on-demand Malware Analysis scan from the Investigation screen, it fails with an invalid username error. The job gets submitted but fails because of the credentials.

**Workaround:** None.

### **If the Core device is not configured with IP address, the View Network Session option is disabled for Malware Analysis events**

**Tracking Number:** ASOC-5571

**Problem:** Due to the new service ID and changes to the ASG, Malware Analysis is not showing the View Network Session option from the Malware Event Summary. It looks like the device ID is coming as null.

**Workaround:** None.

## **Event Stream Analysis**

### **ESA Rules deployed not listed while creating policy using statistics ESA Rule Memory Usage**

**Tracking Number:** ASOC-50201

**Problem:** When you deploy new ESA rules in the Health and Wellness page and create a new policy under Event Stream Analytics using the statistic ESA Rule Memory usage, all ESA rules deployed are not listed.

**Workaround:** Run the following restart command on NetWitness Server: `systemctl restart rsa-sms`.

### **Unable to deploy ESA rule with array meta in Enrichment**

**Tracking Number:** ASOC-47584

**Problem:** If a user configures an In-Memory table as an Enrichment Source in ESA where a table column has type as string, creates an ESA rule with a whitelist condition, and maps the string list column to a string array event meta key, when the rule is deployed, the rule is disabled as the datatype conversion from String[] to String is not allowed.

**Workaround:** None.

### **For ESA rules that use enrichment sources, the Ignore Case option does not work for first statement**

**Tracking Number:** ASOC-49906

**Problem:** When creating an ESA rule that uses any enrichment source, if the Ignore Case option is enabled on the first enrichment statement, no results are returned. Note that this issue does not apply to any statements after the first statement (that is, substatements).

**Workaround:** When creating a new rule, the Ignore Case option is now disabled. For existing rules that have the Ignore Case option enabled for an enrichment statement, the option is still enabled but users will be prompted to disable the option when opening the rule in ESA and then save the updated rule.

### **ESA rule with meta entity does not get triggered**

**Tracking Number:** ASOC-47522

**Problem:** When meta entities are configured for use in the Investigate interface, they are not available for use in the ESA Correlation Rule Builder. Customers are not able to build ESA correlation rules using meta entity information, and they must specify the exact pieces of metadata to use in the rules.

**Workaround:** None

**Deployment (called Synchronization in 10.4 and earlier) fails if you deploy this rule from RSA Live: No Log Traffic detected from device in given time frame**

**Tracking Number:** SAENG-5888

**Problem:** Deployment, formerly called synchronization, fails for rule "No Log Traffic detected from device in given time frame" deployed from Live. This issue is not observed if you deploy the rules from Live on a 10.4 setup and do the synchronization. The issue is observed if you update your system from a pre-10.4 where the rules are deployed from Live with incorrect Module IDs.

**Workaround:** Delete the rules with incorrect Module IDs and redeploy them from Live.

**Case-sensitive sorting is not working properly in ESA All Rules grid**

**Tracking Number:** SAENG-3605

**Problem:** When rule names begin with lower and upper case letters, the sort does not work properly in the Rule Name column of ESA All Rules grid. For example, "Rule 1" is not followed by "rule 2" when you sort by name.

**Workaround:** None.

**Cannot set ESA compression level as in other appliances**

**Tracking Number:** ASOC-26481

**Problem:** Administrators cannot set the compression level in ESA like they can with other appliances, even using the Explorer view.

**Workaround:** Delete the Concentrator source from ESA and add it again so that the compression level changes are reflected:

1. Remove the Concentrator data source from ESA. (Go to ADMIN > Services, select the Event Stream Analysis service, and from the actions menu select View > Config. On the Config view Data Sources tab, remove the Concentrator data source.)
2. Set compression level in ESA. (Go to the Explore view, and in the node list, navigate to Workflow/Source/nextgenAggregationSource and set the CompressionLevel.)
3. Add the Concentrator Data Source again to ESA. (Return to the Config view Data Sources tab and add the Concentrator data source.)

**Event Stream Analysis service becomes unresponsive when using Query-based aggregation for automated threat detection for Logs**

**Tracking Number:** ASOC-25174

**Problem:** Event Stream Analysis may become unresponsive due to heavy resource usage, and the configuration for the wrapper may need to be adjusted.

**Workaround:** You may need to change the ping time settings in the `wrapper.conf` file. Perform the following:



1. Go to **Administration > Services > Event Stream Analysis> Explorer** and navigate to the `/opt/rsa/esa/conf/` folder.
2. Change the settings to the following values:  
`wrapper.ping.timeout=300`
3. Add the following lines at the end of the file:  
`wrapper.restart.delay=40`  
`wrapper.ping.timeout.action=RESTART`
4. Restart the Event Stream Analysis service.

### ESA Displays Warning For Array Operators

**Tracking number:** ASOC-14157

**Problem:** When writing an advanced rule, array operators, such as `anyOf`, fails. For example:

```
SELECT * FROM
```

```
Event(
```

```
alias_host.anyOf(i => i.length()>50)
```

```
);
```

results in an error similar to the following:

```
Logger name: com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
```

```
Thread: pipeline-sessions-0
```

```
Level : WARN
```

```
Message : Expected array-type input from property 'alias_host' but received class java.util.Vector
```

**Workaround:** To do a fuzzy comparison, first convert the array to a string. For example:

```
SELECT * from Event (cast(alias_host, string)LIKE '%TESTHOST%');
```

**Note:** If you used array operators in EPL developed in versions 10.5, 10.5.0.1, and 10.6, you will need to modify the EPL to use the above workaround.

### Deployment fails if the server that hosts an external database goes down

**Tracking Number:** ASOC-9011

**Problem:** You configure a database connection to use the database as an enrichment source for a rule. A reference to the database is deployed on every ESA, even if the ESA does not deploy any rules that use the database. If the server that hosts the database goes down, any new deployment will fail.

**Workaround:** Restart the server that hosts the database.

### Trial rules configuration: Out-of-Bound Values are Capped

**Tracking Number:** ASOC-6633

**Problem:** When configuring parameters for trial rules, you can configure the following values:

- **MemoryCheckPeriod:** Defines the polling interval to check the ESA memory consumption.
- **MemoryThresholdForTrialRules:** Defines the threshold value; when reached, all trial rules will be disabled.

If you configure these parameters with out-of-bound values, the values are capped to the system's minimum or maximum values rather than the values defined in the parameters.

**Workaround:** None.

## Reporting

### Post-upgrade from 10.6.5.x to 11.1, Categories meta for incident collection is not supported.

**Tracking Number:** ASOC-40851

**Problem:** When using the Categories meta for incident collection, the results rendered are in an incorrect format. Hence this meta is not supported and you cannot use the categories meta in either select clause or where clause. Also, it is not available in the list of metas for selection in the Rule Builder page.

**Workaround:** None.

### Incorrect data displayed for Charts

**Tracking Number:** ASOC-35523, ASOC-37958

**Problem:** When a chart is executed for defined time ranges, the results are inconsistent between test chart and a view chart.

**Workaround:** None.

### When querying on the Respond DB, empty rows are displayed.

**Tracking Number:** ASOC-37846

**Problem:** When querying on the Respond DB, and if the data is not available for the requested columns, then empty rows are displayed on the UI.

**Workaround:** None.

### Hide and Investigate options are not supported in Google Chrome and Mozilla Firefox browsers on Windows 10 operating system.

**Tracking Number:** ASOC-37590

**Problem:** If you are using Chrome or Firefox browsers on a Windows 10 operating system, and click on a chart data point, the hide and investigate options are not displayed. However, these options are available using the Internet Explorer browser.

**Workaround:** Disable the touch feature on Chrome and Firefox browsers. To disable this option in Chrome use the following procedure:

1. Navigate to - chrome://flags/ on Chrome or Firefox Browser.
2. Select the "Disable" option for "Touch Events API" flag.
3. Relaunch the browser.

To disable this option in Firefox, use the following procedure:

1. Navigate to - "about:config".
2. Click on "I accept the risk".
3. Search for the "Preference Name" - "dom.w3c\_touch\_events.enabled".
4. Update the "Value" column to 0.
5. Relaunch the browser.

## Administration

### Audit Logs: SA\_SERVER is not capturing the value for queryString

**Tracking Number:** ASOC-8994

**Problem:** When changing file contents of a NetWitness Suite service, the NetWitness Suite server audit logs do not indicate which file the user changed.

**Workaround:** None.

### Password expiry email lacks source information

**Tracking Number:** ASOC-9187

**Problem:** The password expiry email sent by the NetWitness Suite server does not mention the name or URL of the NetWitness Suite server that sent the email. If there are multiple NetWitness Suite servers, you may not know where to go to update your password.

**Workaround:** None.

## Event Source Management

### Renaming the Log Collector or Log Decoder hostname is not reflected in Event Source Manage View

**Tracking Number:** ASOC-9235

**Problem:** On the **Administration > Host** page, if you edit the Log Collector or Log Decoder appliance "name," then the change will not be reflected on the **Administration > Event Sources > Manage** page in the Log Collector or Log Decoder columns.

**Workaround:** Once you update a name from the Host page, perform the following steps:

1. SSH to the NetWitness Suite appliance.
2. Restart the SMS service by running this command:

```
systemctl restart rsa-sms
```
3. On the NetWitness Suite UI, wait for the **Event Source Manage** page to come back up, then delete the event sources with the old Log Collector or Log Decoder names.

### Not all types are displayed for auto-mapped addresses

**Tracking Number:** ASOC-48328

**Problem:** If a new application is added on an existing Event Source that is auto-mapped, there could be a delay in when that type shows in Event Source Discovery and is un-auto-mapped.

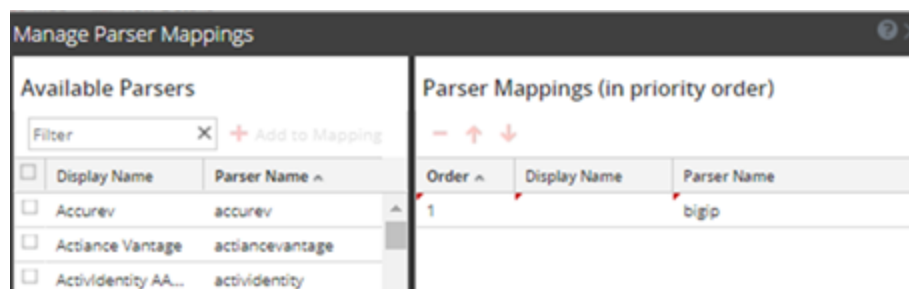
**Workaround:** None.

### Suggested mapping do not load when the Event Source is created manually.

**Tracking Number:** ASOC-49492

**Problem:** For an Event Source that is manually added without entering a value for Log Decoder, when the **Manage Parser Mappings** dialog is opened, suggested Parser Mappings may not have a Display Name.

**Workaround:** Close the **Manage Parser Mappings** dialog, then reopen it and the Display Name is displayed as shown in the following example.



## Core Services

**The SSL FIPS Mode checkbox in the Services Config view should be disabled for Brokers, Concentrators, and Archivers, because changing the checkbox value does not turn off FIPS enforcement for the service.**

**Tracking Number:** ASOC-41902

**Problem:** In 11.0.0.x, the Broker, Concentrator, and Archiver are always FIPS enforced and the administrator does not have the option to toggle between between FIPS and Non-FIPS. The admin can use the SSL FIPS Mode checkbox to toggle FIPS mode on and off on a Log Decoder, Packet Decoder, or Log Collector.

**Workaround:** None.

### **Broker System roles do not show the custom meta keys defined in Concentrator**

**Tracking Number:** ASOC-6749

**Problem:** If any custom meta keys are defined, the same meta keys should show up in the Broker, too. But the Broker system roles are not showing the custom meta.

**Workaround:** You can copy the Concentrator Language file and the custom index file (if it exists) to the Broker to add the SDK meta key roles to the system roles.

### **Custom Feed configuration- Advanced Option XML file invalid error for multi metacallback.**

**Tracking Number:** ASOC-40867

**Problem:** Netwitness Suite does not support uploading feeds for the xmls where there are more than one callback.

**Workaround:** The Adhoc Feed can be uploaded using NwConsole, or using the REST URL of the decoder directly. This is not applicable for Recurring Feed.

### **Ability to Create Source and Destination IP-Based Feeds Using CIDR or Range**

**Tracking Number:** SATCE-628

**Problem:** When creating a source and destination-based feed on a Log Decoder, it only populates the source meta key. You cannot use a range-based or CIDR feed. You must list every single IP address.

**Workaround:** Create two different feeds using IP addresses and you can use CIDR in these feeds.

## Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Suite 11.1.0.0 Online Documentation	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Suite 11.1.0.0 Upgrade Instructions	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Suite 11.1.0.0 Upgrade Checklist	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Suite Hardware Setup Guides	<a href="https://community.rsa.com/community/products/netwitness/hardware-setup-guides">https://community.rsa.com/community/products/netwitness/hardware-setup-guides</a>
RSA Content for RSA NetWitness Suite	<a href="https://community.rsa.com/community/products/netwitness/rsa-content">https://community.rsa.com/community/products/netwitness/rsa-content</a>

## Contacting Customer Care

---

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

- The version number of the RSA NetWitness Suite 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 SecurCare	<a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a>
Phone	1-800-995-5095, option 3
International Contacts	<a href="http://www.emc.com/support/rsa/contact/phone-numbers.htm">http://www.emc.com/support/rsa/contact/phone-numbers.htm</a>
Email	<a href="mailto:nwsupport@rsa.com">nwsupport@rsa.com</a>
Community	<a href="https://community.rsa.com/docs/DOC-1294">https://community.rsa.com/docs/DOC-1294</a>
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	7-Mar	Release Notes for RSA NetWitness Suite v11.1
1.1	31-May-18	Removed ASOC-49115 from Known Issues.