RSA NETWITNESS® PLATFORM

Release Notes

for Version 11.2

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

Contents

Introduction

This document lists enhancements and fixes in RSA NetWitness® Platform 11.2.0.0. Read this document before deploying or updating to RSA NetWitness® Platform 11.2.0.0.

- 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® Platform 11.2.0.0 release provides new features and enhancements for investigation on logs, packets, and endpoints. As part of this release, user and entity behavioral analytics is introduced to detect and investigate attacks and identity-based anomalies.

NetWitness User and Entity Behavior Analysis (UEBA)

RSA NetWitness® UEBA is now part of the RSA NetWitness® Platform. NetWitness UEBA provides comprehensive user and entity behavioral analytics to better detect, investigate, and respond to advanced internal attacks and identity-based anomalies.

NetWitness UEBA has the following features, UEBA:

- Leverages dynamic statistical outlier analytics for behavior baselining, behavior modeling and peer group analytics to uncover anomalous behavior, lateral movement, insider threats, and data exfiltration.
- Identifies suspicious behavior-based anomalies leveraging unsupervised machine learning algorithms.
- Generates an identity and alert risk scoring model to only raise severity and priority on high risk indicators, reducing alert fatigue and false positives.

NetWitness UEBA Service Deployment. NetWitness UEBA can be configured and deployed from the NetWitness Platform Admin Server. NetWitness UEBA Server captures Windows log data from NetWitness Platform services, processes the data, and displays results on the NetWitness GUI. If the NetWitness Insights Endpoint agent is deployed, Windows log data collected is also analyzed. For information on deploying UEBA, see the *Physical Host Installation Guide* and the *Virtual Host Installation Guide*.

In version 11.2, UEBA natively supports a variety of the following Windows log sources such as:

- Windows Active Directory
- Windows Logon and Authentication Activity
- Windows File Servers

Identity Behaviors Baselining. Machine learning models are applied on historical and real-time data for the creation of behavior baselines that help with identifying outliers and provides visibility into organizational and individual metrics. Standard modeling policy executes a 30 day-training period. If additional historical data is stored beyond that point, the training period can be modified to execute upon an earlier timeframe. Only abnormal behaviors to these baselines result in anomalies or indicators of compromise.

Investigation of Top Alerts and High Risk Users. Analysts can leverage a pre-defined Out-of-the-Box (OOTB) dashboard and reporting to investigate top alerts (Alerts triggered by a sequence of indicators within a round hour (that is, one full hour) and high-risk users (Users with a high risk score). Analysts can view users that require immediate attention, perform deeper investigation, and reduce risk scores.

NetWitness UEBA License. The NetWitness UEBA License is based on the total number of users in your organization. Users are individuals who have network access and login credentials. If the number of users exceeds five percent (5%) of the purchased license, you must procure new licenses. For more information, contact your RSA Account Manager. for more information on licensing, see the *Licensing Management Guide*.

For more information on UEBA, see the *NetWitness User Entity and Behavior Analytics User Guide* .

NetWitness Respond

Access Event Analysis directly from the Incident Details view. You can seamlessly access Event Analysis from the Investigate view from within the Indicators panel storyline of an incident. To further investigate an incident, you can click an event type hyperlink within an event in the storyline to open the Event Analysis view in Respond.

Added the ability to send incidents from within NetWitness Respond to RSA Archer. If RSA Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response. When configured, you will see a Send to Archer button and Sent to Archer status in NetWitness Respond. You will also have the option to filter the incidents list for incidents sent to Archer. When you send an incident to Archer, the system automatically creates an entry in the journal for the incident.

Pivot to RSA Archer from Incidents. You can pivot to RSA Archer for device details and other information in RSA Archer® Cyber Incident & Breach Response for specific entities. These entities are IP address, host, and Mac address. In the Context Lookup panel, you can view the attributes for the underlined entity such as business unit values, device name, device type, and so on. For more information, see the *NetWitness Respond User Guide*.

Improved manual incident creation from the Alerts List view. You can add a priority, an assignee, and categories when you create an incident manually from alerts.

Added the ability to hide node types in the nodal graph. To further study the interactions between the entities on the nodal graph, you can select the node types that you would like to include in the nodal graph. This can be especially helpful if a nodal graph contains over 100 nodes.

Adjusted the incidents filter for assigned and unassigned incidents. In the Incidents List Filters panel, you can no longer filter for assignees and unassigned incidents at the same time. If you select “Show only unassigned incidents”, the Assignee filter drop-down list is now disabled. If you select an Assignee from the drop-down list, the “Show only unassigned incidents” option is now disabled.

Improved the user experience with sorting the Incident List. You can click anywhere on the column header in the list to toggle the sort. You no longer have to click the up or down arrows to sort the list.

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

NetWitness Investigate

Contextual information for a meta value in the Event Analysis view. The Context Lookup panel, which was previously available in the Navigate view and the Events view, has been added to the Event Analysis view. The Context Lookup panel shows details about elements associated with an event (IP Address, User, Host, Domain, MAC Address, Filename, File hash) in the Context Hub. You can interact with the meta values of an event to get further insight such as related incidents, alerts, custom lists, RSA Archer assets, Active Directory details, and NetWitness Endpoint Thick Client. For more information, see "View Additional Context for a Data Point" in the *NetWitness Investigate User Guide*.

Pivot to Archer from meta values in Event Analysis view. You can now pivot to RSA Archer from these underlined entities - IP address, Mac and host in Event Analysis for viewing device details.

Free-Form queries in the Event Analysis view. Free-Form mode is an alternative to the basic query (Guided) mode available in earlier versions. In Free-Form mode, analysts can enter complex text queries, and switch between Free-Form and Guided mode. For more information, see "Filter Results in the Event Analysis View" in the *NetWitness Investigate User Guide*.

Profile enhancements include profile groups, new and updated profiles, and including the preQuery for a profile in the breadcrumb. For more information, see "Use Profiles to Encapsulate Custom Views" in the *NetWitness Investigate User Guide*.

- Profile groups allow you to organize profiles into logical groups, for example, different profile groups for different use cases, or for different users. You can move existing and new profiles into profile groups.
- A new out-of-the-box profile called RSA Endpoint Analysis uses a preQuery of `device.type=nwendpoint` and the RSA Endpoint Analysis meta group and column groups.
- In the RSA Threat Analysis profile, the following three meta keys are replaced:
`risk.warning` is now `behavior of compromise (boc)`
`risk.suspicious` is now `indicator of compromise (ioc)`
`risk.informational` is now `enabler of compromise (eoc)`
- When a profile is selected in the Navigate View or Events View, the PreQuery for the profile is displayed in the breadcrumb.

Improved search option configuration. The menu for setting search options has been reorganized to make it easy to understand and choose. For more information, see "Configure the Navigate View and Events View" in the *NetWitness Investigate User Guide*.

Improvements to the Text Analysis panel. In the Event Analysis view, several improvements address usability in viewing data.

- New pagination controls allow more flexibility in paging through a list of events.
- If a reconstructed event in the Text Analysis panel has a request or response that exceeds the maximum number of bytes limit, the header indicates that the message has been truncated. This provides as much data as possible when viewing the Text Analysis of an event that is too large to render.

Event Source Management

Identify Idle Event Sources. This new attribute displays the number of days since a log was last received from each event source. You can use this attribute to group event sources that have been idle for a specified time (for example, 90 days), for review or bulk removal.

Context Hub

Option to Import or Export Attributes. The attributes in Context Lookup panel can now be managed to help users view the attributes intended for RSA Archer device details. You can configure the attribute of interest from the device application of RSA Archer and view these attributes in the context panel. To perform this, you can export the existing attributes, add the new attribute and import the updated set of attributes. These attributes are reflected in the order imported in the Context Lookup panel when you view the context for an incident or an event on Event Analysis view. For more information, see the *Context Hub Configuration Guide*.

Services Implemented with the NetWitness Server

New Content Service. The new **Content** service manages the RSA provided and user created parser rules. You can now add parser rules in the UI. The Content service is used in the Log Parser Rules tab, which is described in Log Parsing section later in this document.

Log and Network Decoder

Support for standard pcapng files. To provide a more open database format, the Network Decoder can now write standard pcapng files. This capability is enabled by default if you install 11.2 directly. If you upgrade from a previous version to 11.2, you must enable pcapng-formatted database files manually, which can result in an approximate 4% decrease in disk space (as the pcapng files require more space than the nwdb files). You can also use the pcapng format with 10 Gbps capture, which does not decrease performance significantly (< 1%).

To enable the new configuration node:
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

New GeoIP2 Parser. The new GeoIP2 Parser converts IP addresses into geographic locations, provides the latest Maxmind GeoIP package, and supports IPv6 addresses as well as IPv4. The GeoIP2 Parser reads from `ip.src`, `ip.dst`, `ipv6.src` and `ipv6.dst` to generate GeoIP information, and is enabled in the Decoder by default. For more information, see “GeoIP2 and GeoIP Parsers” in the *Decoder and Log Decoder Configuration Guide*.

GeoIP Lookups on IPv4 IPv6 Metadata. You can now perform GeoIP lookups on any IPv4 or IPv6 metadata so that you can understand geographic information in scenarios when `ip.src` and `ip.dst` are not the focus for analysis.

- There is a new Lua API that provides Lua parsers with complete access to any GeoIP2 information. The Lua API returns the requested information from the GeoIP2 database. The parser is then free to use this information to create meta or to perform its own analysis.
- You can configure the native GeoIP2 parser to generate GeoIP2 metadata on any IPv4 or IPv6 key using the `config` node `parsers.options`.

For more information, see “GeoIP2 and GeoIP Parsers” in the *Decoder and Log Decoder Configuration Guide*.

TLS Certificate Hashing. The Network Decoder can produce hashes of certificates that are seen in the packet stream. These hashes are the SHA-1 value of any DER-encoded certificate encountered during a TLS handshake. The hashed data is written to the `cert.checksum` key. The hashes produced can be used to compare network traffic with hashes from public SSL blacklists. For more information, see “TLS Certificate Hashing” in the *Decoder and Log Decoder Configuration Guide*.

User Interface

Log Parser Rules tab has moved. The Log Parser Rules tab, located in ADMIN > Event Sources for version 11.1, has been moved to CONFIGURE for version 11.2.

Added additional language support. In the User Preferences, there is a new Language option, which enables you to select another available language. The selected language alters the text across the NetWitness Platform. For more information, see the *NetWitness Platform Getting Started Guide*.

NetWitness Rebranding. The NetWitness 11.2 product has been rebranded throughout the user interface, documentation, and other relevant occurrences as follows:

1. RSA NetWitness® Suite to RSA NetWitness® Platform
2. RSA NetWitness® Packets to RSA NetWitness® Network
3. RSA NetWitness® Logs and Packets to RSA NetWitness® Logs & Network
4. Packet Hybrid host type to Network Hybrid host type
5. Packet Decoder host type to Network Decoder host type
6. RSA NetWitness® SecOps Manager to RSA Archer® Cyber Incident & Breach Response

Administration

Configurable Context Menu Actions in Investigate. Right-click actions available in Investigate can now be configured using the Context Menu Actions UI by using different fields and groups. You can create new context menu actions and manage them using Context Menu Actions available under ADMIN > System. The Context Menu Actions configured using the UI can be viewed as a right-click action on meta keys in Investigation tab under - Navigate, Events, and Event Analysis views. In Event analysis, right-click actions are supported on meta keys as well.

Improved Login Banner available. The login banner now features fully customizable text and increased security measures.

Log Parsing

Log Parser Rules tab has been enhanced. RSA has added the ability to extend existing log parsers, add custom log parsers, and update log parser rules for your log parsers. Log parser rules change the way meta information is extracted from the event source logs. You can add log parser rules that extend existing log parsers in your system, as well as to the default log parser, which extracts meta from messages that might otherwise be listed as unknown. For more details, see the *Log Parser Customization Guide* available in RSA Link. For 11.1, the log parser rules were read-only.

Upgrade Instructions

The following upgrade paths are supported for RSA NetWitness® Platform 11.2.0.0:

- RSA NetWitness® Platform 10.6.6.x to 11.2.0.0
- RSA NetWitness® Platform 11.0.x or 11.1.x to 11.2.0.0

For more information on upgrading to 11.2.0.0, see the upgrade instructions in the Installation & Upgrade section.

Fixed Issues

This section lists issues fixed since the last major release.

Security

Tracking Number	Description
ASOC-58379	Moderate CentOS 7 glibc security update https://access.redhat.com/errata/RHSA-2018:0805
ASOC-58373	CentOS 7 kernel security update https://access.redhat.com/errata/RHSA-2018:1629
ASOC-58376	dhcp Security Update: https://access.redhat.com/errata/RHSA-2018:1453
ASOC-58374	procps-ng Security Update https://access.redhat.com/errata/RHSA-2018:1700
ASOC-58381	ntp Security Update https://access.redhat.com/errata/RHSA-2018:0855
ASOC-58384	gcc Security Update https://access.redhat.com/errata/RHSA-2018:0849
ASOC-58380	krb5 Security Update https://access.redhat.com/errata/RHSA-2018:0666
ASOC-50151	openssh Security Update https://access.redhat.com/errata/RHSA-2018:0980
ASOC-58367	openjdk Security Update https://access.redhat.com/errata/RHSA-2018:1649
ASOC-58377	libvorbis Security Update https://access.redhat.com/errata/RHSA-2018:1058
ASOC-52448	Authconfig Security Update https://access.redhat.com/errata/RHSA-2017:2285
ASOC-52439	Libx11 Security Update https://access.redhat.com/errata/RHSA-2017:1865
ASOC-52443	NetworkManager Security Update https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52444	Bash Security Update https://access.redhat.com/errata/RHSA-2017:2299

Tracking Number	Description
ASOC-52445	Openldap Security Update https://access.redhat.com/errata/RHSA-2017:1852
ASOC-49815	Systemd Security Update https://access.redhat.com/errata/RHSA-2018:0260

General Application Issues

Tracking Number	Description
ASOC-46483	The system logs off idle users in Respond and some Investigate Views

Investigate

Tracking Number	Description
ASOC-51011	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.
ASOC-50702	After upgrading to 11.1, there are mismatched data types between the Log Decoder (table-map.xml) and Concentrator (index-concentrator.xml) definitions.
ASOC-50924	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.
ASOC-50771	If you go to Event Analysis from 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.
ASOC-49854	The Service selector spinner keeps loading infinitely.
ASOC-50712	Cannot add meta entities to a custom column group in the Events view when the Optimize Investigation Page Loads option is disabled.
ASOC-50349	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	Description
ASOC-50041	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.
ASOC-45198	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.
ASOC-48945	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.
ASOC-48710	When investigating in the Event Analysis view, the following error message is returned: “An Unexpected error has occurred.”

Respond

Tracking Number	Description
ASOC-40749	Respond Administrator cannot query Investigate or view Live dashlets in the Dashboard.
ASOC-41891	Security Analytics Incident Management link in the NetWitness SecOps Manager 1.3.1.2 is not valid in NetWitness Suite 11.1.0.0.
ASOC-46834	Unable to select Domain for Suspected C & C and Domain in the rule builder
ASOC-50911	Aggregation Stops after Reconnection to Mongo
ASOC-51480	Endpoint events with a detector IP are not being aggregated by the Endpoint incident rule and do not create incidents with the current default incident rule’s match condition. See the “Set Up and Verify Default Incident Rules” topic in the *NetWitness Respond Configuration Guide*.

Event Stream Analysis (ESA)

Tracking Number	Description
ASOC-50201	When you deploy new ESA rules in the Health and Wellness view and create a new policy under Event Stream Analytics using the statistic ESA Rule Memory usage, all ESA rules deployed were not listed.

Features Not Supported

The following tables provide information on features no longer supported in RSA NetWitness® Platform 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	1. Forgot my password. 2. Email Notification to user when password expires. 3. Test/Search AD user.
5.	Pivotal	Pivotal is not supported.
6.	Warehouse Analytics	Warehouse Analytics is not supported.

Features Available in Future Releases

The following features are not available in 11.2 and may be available in a future release.

No.	Feature	Notes
1	IPDB Reporting	IPDB Extractor service is not supported in 11.2.0.0 and will be available in later releases.
2	STIG	If you have a STIG hardened host, you cannot upgrade to 11.2.0.0 as the backup scripts do not support that.

No.	Feature	Notes
3	Multiple Security Analytics Server (NetWitness Server) support	Multiple server deployment is not supported.
4	PKI Authentication	The PKI Authentication feature is not available in 11.2.0.0.
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	The Endpoint agent currently works in User mode and does not support Kernel mode detection.
10	Endpoint File reputation	File reputation, such as OPSWAT, YARA, and Reversing Lab lookups, are not supported and thus 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 11.2

The following known issues occur during upgrade from 10.6.6 to 11.2 or update from 11.1 or 11.1.x to 11.2.

STIX recurring feed fails on upgrade from 10.6.6 to 11.2

Tracking Number: ASOC-61227

Problem: When you upgrade Security Analytics 10.6.6 to NetWitness Platform 11.2, the STIX Recurring feed you created using HTTPS URL fails to work. This is because, in 10.6.x, by default, all the certificates are trusted. However, this is not the case in 11.2. In 11.2, the Trust All certificates option is provided and is disabled by default.

Workaround: Navigate to Configure > Custom Feeds and edit the failed feed. Either enable the Trust all option, or upload a valid SSL certificate to resolve the issue. In case of any further queries, contact the RSA Customer Support.

On upgrade to NetWitness Platform 11.2, license details are not retained on AWS cloud

Tracking Number: ASOC-61614

Problem: When you upgrade from Security Analytics 10.6.6 to NetWitness Platform 11.2, the license server id is not retained. Admin server is thus unable to obtain the license server details from the external back-end system, due to which the services cannot be licensed.

Workaround: Follow the steps provided in "Access Download Central" and "Register the Server (Online)" topics in the *Licensing Management Guide* to obtain the license details from the external back-end system and register the new license server ID.

After upgrade from 10.6.6 to 11.2.0.0, offline licenses are not retained

Tracking Number: ASOC-41757

Problem: Even if you upload a new response bin file from Download Central, offline licenses do not work. Though old files are restored in `/var/lib/fneserver`, the licenses 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 11.2.0.0 (AdminServer).
3. Move ra* files (3 files) out of `/var/lib/fneserver/`

4. Log in to the RSA NetWitness 11.2.0.0 UI with admin user credentials and go to **ADMIN** > **System** > **License Details**tab.
5. Click **Refresh Licenses**.
6. Upload the response file received from Download Central. Go to **ADMIN** > **System** > **Licensing** > **Settings** tab
7. Click **Upload Response**.

Note: Upgrade using Online mode (RSA Netwitness Suite 11.2.0.0 connected to the Internet) works successfully and all licenses are restored after upgrade to 11.2.0.0.

The investigation links are disabled for static charts during 10.6.6 to 11.2 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 to restore the investigation links.

On upgrade from 10.6.6 to 11.2, the Geo-map dashlet cannot be created using a pre-configured (OOTB) chart.

Tracking Number: ASOC-41896

Problem: When you upgrade to Netwitness Suite 11.2.0.0, 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.x to 11.2, 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 from Version 11.0 to Version 11.2, 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.

> **Note:** If you are upgrading from Version 11.1 or later to Version 11.2, you do not need to make this change.

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-custom.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-custom.xml` file to take effect, you must restart the concentrator service:

   ```
   systemctl restart nwconcentrator
   ```

UEBA

When the proxy is configured, and in case of updates, the license details do not get refreshed automatically

Tracking Number: ASOC-52366

Problem: When the proxy is configured, and in case of updates the license details do not get refreshed automatically or even after clicking the Refresh button in the License Details view. This is because the communication to the license server is not established.

Workaround: The Administrator has to manually download the license details using the offline mode and upload latest license details through the NetWitness Platform UI. For more information, see the *Licensing Management Guide*.

Endpoint

Nginx rejects post requests exceeding request size 1 MB

Tracking Number: ASOC-56236

Problem: The Nginx server is upgraded and the default payload size is set to 1 MB. This causes any data post request exceeding 1 MB to fail.

Workaround: Add the following setting to the Nginx configuration file (`/etc/nginx/conf.d/nginx.conf`) and restart the Nginx server.

```
client_max_body_size 100M
```

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 through any of the copy methods or third party Endpoint management tool, the configuration file timestamp remains to be 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 configuration file, run the command on the Endpoint Agent: `copy /b <filename.nwelcfg> +,,` from the folder %programdata%\NWEAgent\ where the nwelcfg file is there.

Respond

When all alerts are deleted for an alert rule, the filter for the rule is not properly removed

Tracking Number: ASOC-59243

Problem: In the Alerts List view (Respond > Alerts), you can filter alerts by Alert Name and then delete all of the alerts that have that name. If you do not remove the alert name filter after deleting the alerts, the next time the Alerts List view loads, the filter will still be in place, but it will no longer be visible as a checkbox in the Filters panel because all alerts with that name have been deleted. You will continue to see zero results when visiting the Alerts List view.

Workaround: Before you refresh or reload the Alerts List view, you can remove the filter by clearing the checkbox by the alert name. If you already refreshed or reloaded the Alerts List view, the only way to remove the hidden filter is to press the **Reset Filters** button, which removes all filters, including the hidden alert name filter.

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

Tracking Number: ASOC-52428

Problem: Meta values in hover over values are not highlighted when alerts in Respond have manually been added to an incident. While alerts that are automatically or dynamically added to an incident are shown in hover over.

Workaround: None.

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.

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.

Incidents and Tasks are still available when RSA Archer Cyber Incident & Breach Response integration is enabled

Tracking Number: ASOC-39886

Problem: After enabling Archer Cyber Incident & Breach Response (NetWitness SecOps Manager) integration in the Respond Server service, all incidents are managed in Archer Cyber Incident & Breach Response. In previous versions, when SecOps was enabled, incidents and remediation tasks were hidden. In NetWitness Platform 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 Platform. If they create incidents from the Respond Alerts List view (RESPOND > Alerts) or from Investigate, those incidents will not go to Archer Cyber Incident & Breach Response.

Workaround: If you enabled Archer Cyber Incident & Breach Response (NetWitness 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 Platform 11.0.0.x and later. (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.

In memory table enrichment information 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.

Integration Settings for Archer Cyber Incident & Breach Response should be exposed in the User Interface

Tracking Number: ASOC-25127

Problem: The Integration settings for sending all incidents to Archer Cyber Incident & Breach Response (NetWitness SecOps Manager) should be exposed in the user interface.

Workaround: The user interface for partial Archer Cyber Incident & Breach Response (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.

Log Collector

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 11.2.0.0.

> **Note:** Even if FIPS is enabled in 11.2.0.0, 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 11.2.0.0.

   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.

Investigate

Imported Investigate profiles are not displayed in the Profiles drop-down menu

Tracking Number: ASOC-61230

Problem: When you import Profiles to the Navigate view or the Events view using the Manage Profiles dialog, the newly imported profiles are not added to the Profiles drop-down menu.

Workaround: Refresh the browser window to see the recently added profiles.

In the Event Analysis view, log and network events are not interleaved

Tracking Number: ASOC-60941

Problem: Network and log events are interleaved and sorted in time order in the Events view, but in the Event Analysis view, events are sorted differently. In the Event Analysis view, the events are not interleaved as they should be; instead all log events sorted in time order are displayed before all network events sorted in time order.

Workaround: Use the Events view to see interleaved network and log events.

When a large PCAP is extracted from the Events view, if it times out after 5 minutes, the query time is displayed as 8 hours in the Jobs tray error message

Tracking Number: ASOC-60464

Problem: When exporting a PCAP with ~100000 sessions from the Events view using Export > Export All PCAP, the download may fail due to the 5-minute packets call timeout. If the call times out, the error message in the Jobs tray incorrectly displays the timeout as 8 hours (28800000 ms).

Workaround: None.

Users who have not been assigned investigate-server* permission do not get the proper error message explaining why they don’t have access to the Event Analysis view

Tracking Number: ASOC-60366

Problem: If the administrator has not assigned investigate-server* permission for a user, the user should see the permission denied error when attempting to view a session in the Event Analysis view. Instead, the internal server error is returned.

Workaround: None.

Active Directory meta values in the Event Analysis view, such as username, may have context data available, but the meta values are not underlined as an indicator

Tracking Number: ASOC-58853

Problem: Analysts working in the Event Analysis view will not see an indicator that active directory metadata has context enrichment; they must hover the mouse over an active directory meta value to determine if it has associated context and open the Context Lookup panel.

Workaround: Hover over or select a meta value and click the **View Context** button to determine if it has associated context for Active Directory.

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.

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.

Custom Feeds

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.

Event Stream Analysis (ESA)

ESA CH rules get disabled during upgrade or ESA host reboot

Tracking Number: ASOC-60511

Problem: If the ESA host restarts and Context Hub rules are deployed on ESA, the Context Hub rules may be disabled. This happens as a result of a race condition between the Context hub and Event Stream Analysis services startup order on the ESA host.

Workaround: To resolve this issue, do one of the following:

- Go to the **CONFIGURE > ESA Rules > Services** tab and enable the disabled rules that are dependent on Context Hub.
- Restart the Event Stream Analysis service.

ESA Rules with custom meta do not deploy on the ESA Server

Tracking Number: ASOC-60367

Problem: If you add new custom meta keys in 11.2, ESA rules using those meta keys may not deploy. This happens because the Event Stream Analysis service needs information from the Concentrator.

Workaround: To deploy an ESA Correlation Rule with custom meta, do the following:

1. Add the non-standard keys to the index-concentrator-custom.xml file (ADMIN > Services > Select a Concentrator and then select Actions > View > Config > Files tab).
2. Restart the Concentrator (ADMIN > Services > Select a Concentrator and then select Actions > Restart).
3. Ensure that the Concentrator is configured as a data source for the Event Stream Analysis service (ADMIN > Services > Select the Event Stream Analysis service and then select Actions > View > Config > Data Sources tab).
4. Restart the Event Stream Analysis service (Actions > Restart).
5. Ensure that the new meta keys are listed in the Meta Key References (CONFIGURE > ESA Rules > Settings tab > Meta Key References).
6. Deploy the ESA Rule with custom meta.

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.

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.

Reporting

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 "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.

Event Source Management

The Manage Parser Mappings window has an empty Display Name for Log Parsers if the Event Source was created manually

Tracking Number: ASOC-53914

Problem: When you open the Manage Parser Mappings window from the ADMIN > Event Sources > Discovery view, the display name for mapped event sources is empty for event sources that were created manually.

Workaround: Close the mapping window and re-open it.

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 the Event Source Discovery view, and before it no longer shows up as auto mapped.

Workaround: None.

SMS Service crashes with Out of Memory Error

Tracking Number: ASOC-62575

Problem: On systems with a large number of active event sources, when the system cannot keep up with the processing of log statistics messages, the SMS service can crash with a **java.lang.OutOfMemoryError: Java heap space** error.

Workaround: If you experience this issue, please contact RSA support for details on how to address the issue.

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 or later, the Broker, Concentrator, and Archiver are always FIPS enforced and the administrator does not have the option to toggle 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.

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

Tracking Number: ASOC-40867

Problem: NetWitness Platform does not support uploading feeds for the XMLs where there are more than one callback.

Workaround: The ad hoc Feed can be uploaded using NwConsole or the REST URL of the Decoder directly. This is not applicable for Recurring Feed.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.2 Online Documentation	https://community.rsa.com/community/products/netwitness/112
RSA NetWitness Platform 11.2 Upgrade Instructions	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D
RSA NetWitness Platform 11.2 Upgrade Checklists	Virtual Host Upgrade Checklist for Version 10.6.6.x to 11.2 Physical Host Upgrade Checklist for Version 10.6.6.x to 11.2
RSA NetWitness Platform Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides

Documentation	Location URL
RSA Content for RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

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 Platform product or application you are using.
- The type of hardware you are using.

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

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

Revision History

Revision	Date	Description
1.0	15-Aug-18	Release to Operations