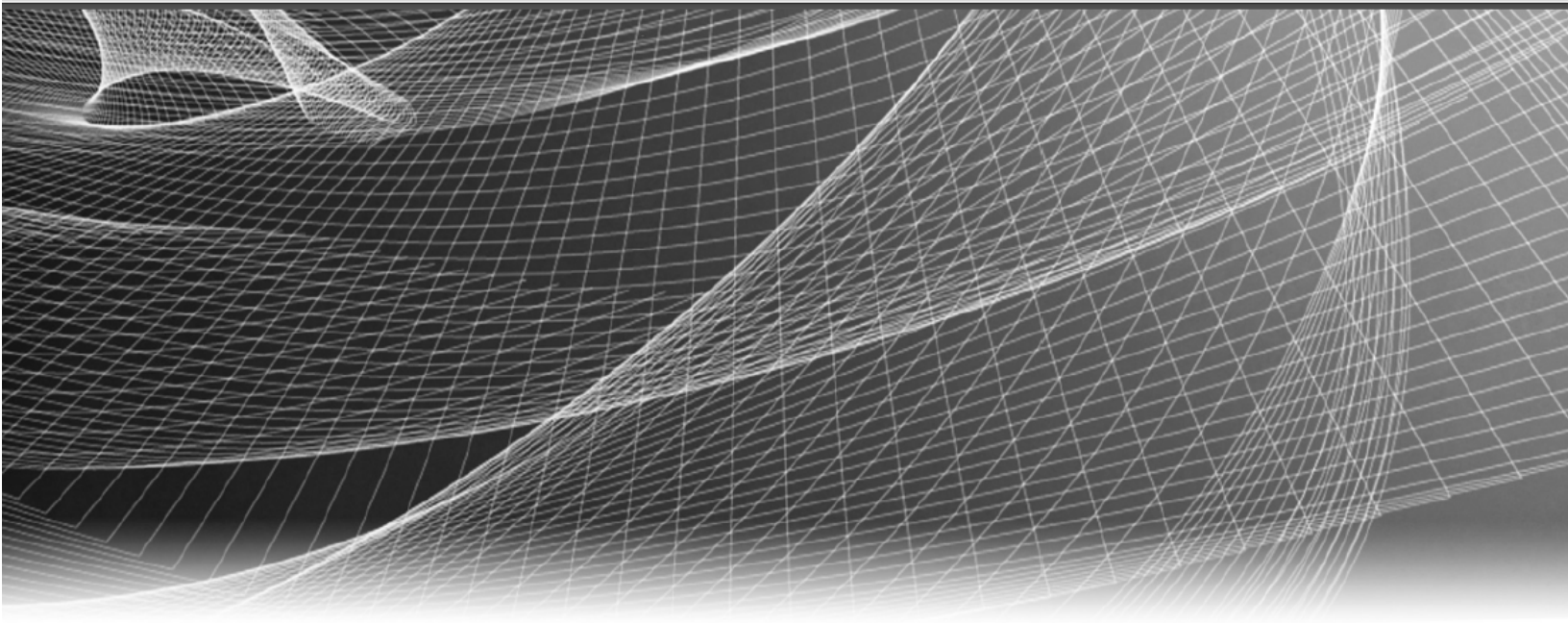

RSA Security Analytics

Release Notes

for Version 10.6.5

RSA

EMC²

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

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

Dell 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 what's new and changed in RSA® Security Analytics, as well as workarounds for known issues. Read this document before deploying or updating RSA Security Analytics.

RSA Security Analytics 10.6.6.0 is a service pack for Security Analytics 10.6.0.0.

Build Numbers

The following table lists the build numbers for various components of RSA Security Analytics version 10.6.5.0.

Component	Version Number
Security Analytics Web Server	10.6.5.0-171122112933.5
Security Analytics Decoder	10.6.5.0-7206.5
Security Analytics Concentrator	10.6.5.0-7206.5
Security Analytics Broker	10.6.5.0-7206.5
Security Analytics Log Decoder	10.6.5.0-7206.5
Security Analytics Log Collector	10.6.5.0-14178.5
Security Analytics IPDB Extractor	10.6.5.0-17279.5
Security Analytics Incident Management	10.6.5.0-1056.5
Security Analytics Reporting Engine	10.6.5.0-5599.5

Security Analytics Warehouse Connector	10.6.5.0-1948.5
Security Analytics Archiver (Workbench)	10.6.5.0-7206.5
Security Analytics Event Stream Analysis	10.6.5.0-312.g9e1afaf.5
Security Analytics Malware Analysis	10.6.5.0-8296.5
Security Analytics Context Hub	10.6.5.0-604.5

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA Security Analytics 10.6.5.0 Online Help	https://community.rsa.com/community/products/netwitness/1065
RSA Security Analytics 10.6.5.0 Update Instructions	https://community.rsa.com/community/products/netwitness/1065
RSA Security Analytics 10.6.5.0 Update Checklist	https://community.rsa.com/community/products/netwitness/1065

What's New

RSA Security Analytics 10.6.5.0 is a service pack for Security Analytics 10.6.x.x. This release includes the following new features and enhancements.

Reporting Engine

Map Charting Capability - The geo map on dashlet is plotted based on the information from the MaxMind database. If data is not available for any of the IP, you can plot the geo map on another grid with adjacent to map. For more information, see "Create a Custom dashboard" topic in the *Security Analytics Getting Started Guide*.

Decoder and Log Decoder

- **Top Parsers in Memory Consumption and Callback Counts** - You can analyze memory, meta callback, token callback, and meta count usage stats of the top parsers during a drop window, this helps you to troubleshoot the Decoder Service. The REST-based Decoder service `sdk/app/packetdrops` is updated to display the top five parsers in memory consumption and callback counts (`meta.callback.counts` and `token.callback.counts`) for packet drop instances. You can access this service in a browser on the Decoder REST port, for example: `http://<decoder>:50104/sdk/app/packetdrops`.
- **Support for CsvFileFeed Parsing** - The CsvFileFeed parsing type using CSV Grammar and escape definition is supported in Security Analytics. To provide additional checks during parsing. For more information, see the "Create and Deploy Custom Feeds Using a Wizard" topic in the *Decoder and Log Decoder Configuration Guide.*
- **Enhancements to the Log Tokenizer** - The log tokenizer is enhanced to parse the scan for a subset of recognizable tokens. For information, see the "Log Decoder Service Configuration" topic in the *Hosts and Services Getting Started Guide.*
- **Improved CEF Parser Toggling Settings** - CEF Parser toggling settings persist when parser settings are changed in the UI and have been improved in the following ways:
  a. If there is no `ipdevice` mapping list, the CEF parser will take effect.
  b. If an `ipdevice` mapping is defined, it will have higher priority than the CEF parser. It is no longer required to define CEF in `devices.disabled`.

Investigation

Endpoint Data Visibility - When Security Analytics is configured to consume data from RSA Security Analytics Endpoint, analysts can view the endpoint data in Investigate. With this enhancement, three types of events (network, log, and endpoint) are exposed in Investigate, and all events can be investigated in the same way. For more information, see *Investigate and Malware Analysis User Guide*.

Log Collector

- **Ability to configure device.ip for ODBC data sources** - In the Log Collector REST interface, you can choose to have the ODBC collector populate the device.ip option with either the event source IP address or the actual source IP on which logs are being collected. You can configure this field in the following location:
  http://<LC_IP_Address>:50101/logcollection/odbc/eventsources/<eventsource_type>/<eventsource_name>/use_eventsource_address
  The options are:

a. False = Actual source IP will be used

b. True = Event source IP will be used
   The Default value for this is False.

- **Syslog collection on Remote Log Collectors processes raw syslog data** - Syslog collection on Remote Log Collectors now processes raw syslog data that does not contain a valid priority (<PRI>) field.

Security Analytics Server

Defragmentation to Address H2 Database Size - The H2 database can become so large that it affects Jetty performance. To address this issue, there is a new option to defragment the H2 database at shutdown, which helps to reduce the size of the H2 database. To enable this option, in /etc/default/jetty, set DB_DEFRAG_ALWAYS set the value to true. (The default value for this option is false.)

Supported Browsers

RSA Security Analytics 10.6.5.0 supports the following browser versions and their build numbers.

Browser	Version Number	Build Numbers
Google Chrome	62.0	3202.62
Mozilla Firefox	57.0	0.1

Update Notes

The following update paths are supported for Security Analytics 10.6.5.0:

- Security Analytics 10.5.1.0 to 10.6.5.0
- Security Analytics 10.5.1.1 to 10.6.5.0
- Security Analytics 10.5.1.2 to 10.6.5.0
- Security Analytics 10.5.2.0 to 10.6.5.0
- Security Analytics 10.5.2.1 to 10.6.5.0
- Security Analytics 10.5.3.0 to 10.6.5.0
- Security Analytics 10.5.4.0 to 10.6.5.0
- Security Analytics 10.5.5.0 to 10.6.5.0
- Security Analytics 10.6.0.0 to 10.6.5.0
- Security Analytics 10.6.0.1 to 10.6.5.0
- Security Analytics 10.6.0.2 to 10.6.5.0
- Security Analytics 10.6.1.0 to 10.6.5.0
- Security Analytics 10.6.1.1 to 10.6.5.0
- Security Analytics 10.6.2.0 to 10.6.5.0
- Security Analytics 10.6.2.1 to 10.6.5.0
- Security Analytics 10.6.2.2 to 10.6.5.0
- Security Analytics 10.6.3.0 to 10.6.5.0
- Security Analytics 10.6.3.1 to 10.6.5.0
- Security Analytics 10.6.3.2 to 10.6.5.0
- Security Analytics 10.6.4.0 to 10.6.5.0
- Security Analytics 10.6.4.1 to 10.6.5.0
- Security Analytics 10.6.4.2 to 10.6.5.0

Note: The update paths supported are for 10.5.1.x (or later) and 10.6.x.x patches released on or before the 10.6.5.0 release.

For more information on updating to 10.6.5.0, see the Update Instructions in the Product Documentation section.

Fixed Issues

This section lists issues fixed since the last Security Analytics release.

Security Fixes

Tracking Number	Description
ASOC-40692	Open SSH Security Update: https://access.redhat.com/errata/RHSA-2017:2029.html
ASOC-41842	Samba Security Update: https://access.redhat.com/errata/RHSA-2017:2790.html
ASOC-42353	NSS Security Update: https://access.redhat.com/errata/RHSA-2017:2832.html
ASOC-42260	Kernel Security Update: https://access.redhat.com/errata/RHSA-2017:2793.html

Server Fixes

Tracking Number	Description
SACE-7935	The current time in **Administration > Event Sources > Alarms > Alarmed Time** field is always changing.
SACE-7815	SMS cast error in Health and Wellness metric for Event Stream Analysis.
SACE-7634	Unable to export logs with pre-query.
SACE-7614	The drop-down menu to select templates is not working for Japanese language.
SACE-7330	Multiple core service account management issues
SACE-6395	Security Analytics feeds disables the custom live feeds with the same content instead of pausing the feeds.
SACE-7862/ASOC-40612	Unable to open Event Stream Analysis Explorer view, IndexOutOfBound error is displayed.
SACE-7504/ASOC-32649	Investigation returns data outside the specified timeframe.

SACE-7060	Alerts are not generated if the Warehouse Connector crashes.
SACE-6444	Archiver configuration details were misleading.
SACE-7795	In Archiver, the scheduler created in the Explore mode was incorrect and caused an exception in Archiver configuration.
SACE-7792	Custom recurring feeds failed on successive recurrences.

Health&Wellness Fixes

Tracking Number	Description
SACE-7275	Issue with SMS service and Rabbitmq which causes the Jettysrv to fail.

Investigation Fixes

Tracking Number	Description
SACE-8098	When you export PCAP or Logs from Events view using a non-default profile, the No Sessions Found error is displayed.
ASOC-39600	In the Navigate View, the CSV option for a meta key now includes line breaks for the meta key data in the Showing Values in CSV Format dialog and in Excel.
ASOC-39584	In the Navigate View, in the menu that is displayed when users right-click on data, items in the menu that are no longer valid have been removed.

Administration Fixes

Tracking Number	Description
SACE-7637	Issue when you add referrer URL in the CEF template.

Reporting Fixes

Tracking Number	Description
SACE-7355	Export CSV and PDF from Dashboard and Report does not display Thai characters.

Log Collector Fixes

Tracking Number	Description
SACE-7545/ASOC-40913	With regards to Checkpoint event collection, Virtual Log Collectors are not able to consume data at an optimum speed.
SACE-8112/ASOC-40317	The new fields added in the tvmfieldlist of chkpntevent.xml are not displayed.
SACE-6915	Log Collector crashes when the ODBC collection service runs into network connection issues while closing connections to event sources.
SACE-7855	The ODBC test connection audit log message is not correctly formatted.
ASOC-38739	When Security Analytics is updated from 10.6.3.0 to 10.6.3.1 nwlogcollector service crashes.
SACE-8226	ODBC Collection does not work when nwlogcollector service is restarted.

Event Stream Analysis Fixes

Tracking Number	Description
SACE-5005/ASOC-28229	Rules that are mapped to an external database as enrichment sources fail due to missing database driver path

Core Fixes

Security Analytics Core Services include Broker, Concentrator, Decoder, and Log Decoder.

Tracking Number	Description
SACE-8176	lc.ctime.meta disappears after reloading parser.
SACE-8035	The domain functions are broken due to parsers limitations.

ASOC-24080	CEF Parser toggling settings were cleared when parser settings were changed in the UI. This issue is fixed in the following ways: 1. If there is no ipdevice mapping list, the CEF parser will take effect. 2. If an ipdevice mapping is defined, it will have higher priority than the CEF parser. It is no longer required to define CEF in devices.disabled.
SACE-7994/ASOC-38891	The ucount/unique operator is not functional for rules.
SACE-8195	In ACK scans, the source and destination IP addresses are reversed.
SACE-8221	When you update CEF parsers, the escape characters from any meta value are handled automatically in the following way: • If the escape character "\=" is in the middle of the message it is replaced with "=" • If the escape character "\r" and "\n" is in the middle of the message it is replaced with a space. • If the escape character "\r" and "\n" occurs at the end of the message it is removed automatically.

Warehouse Connector

Tracking Number	Description
SACE-6773/ASOC-39277	Warehouse Connector fails to send matching AVRO (Logs & Sessions) files.

Known Issues

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

Installation and Update

Incorrect version is displayed when you update from 10.5.2.0 to 10.6.0.1 or later

Tracking Number: ASOC-17443

Problem: When you update Security Analytics from 10.5.2.0 to 10.6.0.1 or later, update dialog displays incorrect message 'Update to 10.5.2.0'. This happens when you update Security Analytics server through UI.

Workaround: Ignore the message and continue with the update.

Security Analytics UI displays an error when you click Move to Repo

Tracking Number: ASOC-17654

Problem: During 10.6.0.1 or later update, an error message ' Failed to Apply Files to repository' is displayed on Security Analytics UI. This occurs when you upload all the zip files and click Move to Repo.

Workaround: You must refresh the page.

Issue with All-in-One Logs setup during an update from 10.5.2.0 or 10.6.0.0 to 10.6.4.0

Tracking Number: ASOC-21194

Problem: When you update from 10.5.2.0 or 10.6.0.0 to 10.6.4.0 in All-in-One Logs setup from Security Analytics UI, the puppet and RabbitMQ services are stopped. The update happens with an error and it takes a long time to complete.

Workaround: You must perform the following:

1. Start the puppet service using the following command:
   ```
   service puppet start
   ```
2. On Security Analytics UI, check if update is successful and click **Reboot**.
3. After Security Analytics is up, check the updates on the **Host** view and click **Update**.
4. Click **Reboot**.

Issue with All-in-One setup during Security Analytics 10.6.0.0 to 10.6.4.0 update

Tracking Number: ASOC-23344

Problem: When you update Security Analytics from 10.6.0.0 to 10.6.4.0, Security Analytics does not come up due to an issue with All-in-One setup.

Workaround: Execute the following command once you initiate an update:

```
puppet agent -t
```

Few RPMs are not installed when you update Security Analytics from 10.5.2.1 to 10.6.4.0

Tracking Number: ASOC-25944

Problem: When you update Security Analytics from 10.5.2.1 to 10.6.4.0, libpcap and tcpdump RPMs are not installed but Security Analytics UI displays Up-to-Date.

Workaround: Ensure all the rpms are installed using the following command:

```
yum update
```

sa.repo file gets modified during an update from 10.5.2.0 or 10.5.2.1 to 10.6.4.0 through RSA Link

Tracking Number: ASOC-25943

Problem: When you update Security Analytics from 10.5.2.0 or 10.5.2.1 to 10.6.4.0 through RSA Link, sa.repo file is set to enabled.

Workaround: You must disable the sa.repo file. Perform the following:

```
sed -i -e 's/enabled=1/enabled=0/g' /etc/yum.repos.d/sa.repo
```

Update from 10.6.3.0 to 10.6.4.0 changes the PAM server config file

Tracking Number: ASOC-33289

Problem: When you update from 10.6.3.0 to 10.6.4.0 using the **pam_radius_auth** RPM update, a new server configuration file in the **/etc/raddb** directory is created with the old server configuration file.

Workaround: You must update the new server configuration file (**/etc/raddb/server**) with the old server configuration file details after the RPM update.

Security Issues

Issue with alias name in the Security Analytics Server certificate

Tracking Number: SACE-7700

Problem: When you create custom Security Analytics server certificates, the alias name of the certificate cannot contain the following characters: [ ] { } ( ) < > or the characters & ! or |.

Workaround: Avoid using these characters in the alias name for the Server Certificate. Refer to the Step 5. (Optional) Use Custom Server Certificate topic in the *System Security and User Management guide*.

General Application Issues

Page Not Displayed error during log in using IE 10 Browser

Tracking Number: ASOC-9225

Problem: When logging on to Security Analytics from an Internet Explorer 10 browser window, the following error may be displayed:

The page can't be displayed.

Workaround: In addition to your other protocols, enable the TLS 1.2 protocol in your browser as follows:

1. Navigate to **Internet options > Advanced > Settings > Security**.
2. Ensure that TLS 1.2 protocol is enabled.

3. Click **Apply** and reload the page.

General Platform Issues

No Cancel option available for Warehouse Analytics jobs

Tracking Number: SAENG-4706

Problem: Once the Warehouse Analytics job is started, there is no option to cancel the job.

Workaround: You must kill the job manually. Following are the steps to kill the job:

For MapR:job

1. Get the Jobid from logs.
2. Login to jobtracker UI and search for Jobid to kill under "Running Jobs".
   Sample URL: http://<job-tracker-host>:50030/jobtracker.jsp
3. Kill the Jobid:
   - Select Jobid under "Running Jobs" and click **Kill Selected Jobs**.
     (or)
   - Click on Jobid link, scroll down and click **Kill this job** link.

For Pivotal:

1. Get the Jobid from job logs.
2. Kill the Jobid.
   For Example:
   ```
   mapred job -list
   mapred job -kill job_1406294496331_03
   ```
   (or)
   ```
   yarn application -list
   yarn application -kill application_1406294496331_0385
   ```

Administration

Identity feed is not working

Tracking Number: SACE-6600

Problem: Identity feed is not working due to certificate validation failure.

Workaround: Perform the following:

1. SSH to the Security Analytics server appliance.
2. Navigate to `/etc/hosts/` and map nodeID of the host to the appliance IP.
3. In the **Security Analytics** UI, select **Live** > **Feeds**.

4. In the **Feeds** view, click **Add**.
5. In the **Setup Feed** dialog, select **Identity Feed** and click **Next**.
6. In the **Define Feed** tab, select **Recurring**.
7. In the **URL** field, enter the nodeID of the host as the hostname. For example, use <nodeID> `1n702df2-5891-4e9g-9323-4f492a8556fd` instead of <ip_address> `10.63.21.244`.
8. In the **Select Services** form, select the Services on which feed is to be deployed and click **Next**.
9. In the **Review** form, review feed information and if correct, click **Finish**.

Unable to connect to Event Stream Analysis, Incident Management, or Context Hub service

Tracking Number: ASOC-38029

Problem: Unable to connect to Event Stream Analysis, Incident Management or Context Hub service, when you modify enableProtocols value.

Workaround: You must restart the jetty server using the following command:

```
restart jettysrv
```

Entitlements

Metered license does not flip back to in compliance immediately when there are no services attached to that Metered license

Tracking Number: ASOC-9078

Problem: As an example, if there is a Metered license available for a Log Decoder and you have one Log Decoder listed under it, the following conditions may occur:

- You are over your entitled usage and marked as out of compliance.
- You decide to move the Log Decoder into an available service-based license.
- Your Metered license has no service under it.
- Your Metered license flips back to an in-compliance state after seven days.

Workaround: None.

Aggregate usage report gets generated whenever one service is attached to a license and "All" is selected while exporting usage stats

Tracking Number: ASOC-10079

Problem: For any license type (All/Metered/Service-based), the aggregate PDF/CSV file should get generated only when there is more than one service listed under any license type.

Workaround: None.

Log Collector

Repeated error messages are shown if the domain name is not resolvable from the LWCS box

Tracking Number: SAENG-2476

Problem: While trying to access Windows logs from machine-A in a domain/workgroup which is in another domain and if the domain name for machine-A is not resolved by LWCS, then for every event collected, an error message is displayed.

Workaround: Add the domain entry into the host file of legacy box which is not resolvable.

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 5.

Tracking Number: ASOC-16717

Problem: Bandwidth throttling configuration changes to control the rate that the Remote Collector sends event data to a Local Collector do not persist after a reboot.

The `set-shoveltransfer-limit.sh` script is used to set the bandwidth throttle for event data transferred from a remote collector to local collector. The script uses both iptables rules and linux kernel traffic shaping filters to control the upload bandwidth used by the RabbitMQ port on transfers to an upstream collector. The script works correctly when executed, but fails to persist the traffic shaping filter values once the appliance is rebooted.

Workaround: Add the script execution to the `/etc/rc.local` on the remote collector, as shown in the following example:
`"/opt/netwitness/bin/set-shovel-transfer-limit.sh -s -r 4096kbit"`

Cloudtrail event source test connection fails with an error

Tracking Number: ASOC-37288

Problem: When you edit cloudtrail event source configured with proxy, the test connection fails with an error.

Workaround: Perform the following:

1. Re-enter the **Proxy Password** and **Secret key**.
2. Click **Test Connection**.
   The test connection is successful.
3. Click **Save**.
   The event source configuration is save successfully.

Checkpoint events collection fails with an error

Tracking Number: ASOC-42016

Problem: During the checkpoint events collection, NwCheckpointprocess displays error message related to /dev/random file, which increase "Processing Error Count" for every execution.

Workaround: You must SSH to the appliance and execute the following command:

```
"mv /dev/random /root && ln -s /dev/urandom /dev/random"
```

Server

Data retention scheduler page uses incorrect time zone

Tracking Number: ASOC-24566

Problem: On the Data Retention Scheduler page for a Packet Decoder and Concentrator, if a date threshold is set, Security Analytics uses the incorrect time zone to set the time in the backend and local time is converted to UTC time.

Workaround: Use local time to set the date threshold. For example if you want data retention to be scheduled for 11 AM UTC, you need to set the time for 7:00 AM EDT.

Tracking Number: ASOC-22667

Problem: SNMP v3 trap logs are not working for Event Stream Analysis.

Workaround: None

Custom feeds with CSV content are not matching meta values, and quotes are not displayed correctly

Tracking Number: SACE-7121/ASOC-30636

Problem: Because custom feeds are case-sensitive, the feed will not tag the meta properly if the meta is in a different case than specified in the CSV file. Also, when a feed file with more than one set of double quotes is deployed, Adhoc feeds fail to deploy and recurring feeds deploy but do not make a match.

Workaround: To make the custom feed case-insensitive, the `ignorecase` Boolean value must be set to true within the MetaCallback tag in the XML file, for example:
`<MetaCallback name="device" valuetype="Text" ignorecase="true">`
Follow the steps that are documented in the KB Article 000029517 (https://community.rsa.com/docs/DOC-47865) entitled “Custom feed is not being applied to all meta data in RSA Security Analytics” . Also, when a feed file that contains double quotes is deployed and double quotes are incorrectly displayed on the Security Analytics UI, you can view the feed file in a text editor to check which string is actually going to be matched against strings in the log file. For example, if you have string “abc” that you want to match from a log file, then when you view the feed file in a text editor, it should also have “abc”. However, the SA User Interface will display these quotes as truncated for this given string in the custom feed.

Investigation

Incidents are not flagged when you manually add the alerts to existing incidents

Tracking Number: ASOC-16640

Problem: Investigation values are not highlighted when alerts in Incident Management are manually added to an incident. Alerts that are dynamically added to an incident will get highlighted.

Workaround: None.

Parallel Coordinate visualization is not displaying special characters correctly

Tracking Number: ASOC-9346

Problem: When configuring 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.

Investigation failed on Dashboard and Reports.

Tracking Number: ASOC-44853

Problem: Investigation is not working on Dashboard and Scheduled reports.

Workaround: You must disable the touch feature available on Chrome and Firefox browsers. This can be done using the following steps:

On Chrome:

1) Navigate to "chrome://flags/".

2) Select the "Disable" option for "Touch Events API" flag.

The touch events on the browser is disabled.

3) Reload the browser.

On Firefox:

1) Navigate to "about:config".

2) Click "I accept the risk".

3) Search for the "Preference Name" with the value "dom.w3c_touch_events.enabled".

4) Edit the "Value" column to 0.

The touch events on the browser is disabled.

5) Reload the browser.

Workbench

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.

Restoration collections created from the Explorer view will have a blank Date Range in the Collections Tab in UI

Tracking Number: ASOC-9087

Problem: A restoration collection that is not created through the Security Analytics User Interface will display an empty Date Range for that collection in the User Interface.

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.

On upgrade to 10.5.0.0 or later, collections created from a 10.4.0.0 Workbench display blank Date Range and Date Created values

Tracking Number: ASOC-9035

Problem: Any collections created from a 10.4.0.0 Workbench displays blank Date Range and Date Created values after upgrading to 10.5.0.0 or later.

Workaround: None.

Malware Analysis

Users with Analyst role are not able to run the on-demand 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.

Upload Scan Job does not get submitted to Colo Malware if stand alone Malware is also present in Security Analytics

Tracking Number: ASOC-9821

Problem: When both Colocated and Stand-Alone Malware Analysis exist in a Security Analytics environment, file scan commands will be submitted to the Stand-Alone Malware Analysis and not the Colocated Malware Analysis.

Workaround: None

Incident Management

View Original Event returns stack trace when no Concentrator is available

Tracking Number: ASOC-14266

Problem: When a user does not have the Concentrator online that was listed in the alert, and clicks on the sprocket of an event under alert details in the Incident Management service, then chooses "View Original Event", the user is given a stack trace. This is because the Concentrator is not currently functioning.

Workaround: None.

Out-of-the-box Aggregation Rules in Incident Management are duplicated after Update to 10.6.0.0

Tracking Number: ASOC-15031

Problem: After updating to Security Analytics 10.6.0.0, there are two sets of the same out-of-the-box aggregation rules for Incident Management. This can lead to ambiguity if you enable both sets of these rules.

Workaround: When enabling rules, be careful not to enable duplicate out-of-the-box Incident Management aggregation rules.

Incident Management (IM) service becomes unresponsive while loading large number of alerts

Tracking Number: ASOC-16900

Problem: IM service becomes unresponsive while loading large number of alerts. This happens when you select the time range for "All Data" on the Incidents window.

Workaround: You must reset the time range on IM to avoid this timeout. Perform the following:

1. Verify if the IM service is running using the following command:
   ```
   service rsa-im status
   ```
   If the service is not running, manually start the service using the following command:
   ```
   service rsa-im start
   ```

2. Log in to the Security Analytics UI.
3. In the main menu, select **Dashboard**.
4. In the **Default Dashboard** view, click + drop-down list.
5. Click **Add Dashlet**.
6. In **Type** field, select **Incidents Queue Activity**.
7. In the **Time Range** field, limit the time range to a small value, for example, Last 1 Hour.
8. Click **Add**.
9. Verify if the Incident Queue Activity dashlet is loaded, for example, Total # of Alerts, Total # of Incidents and Total # Remediation in the Last Hour is loaded on Incident Queue Activity.
10. Click **Total # of Alerts**, **Total # of Incidents**, or **Total # of Remediation** count to load the Incidents window with the limited amount of data.

Event Stream Analysis

Deployment (called Synchronization in 10.4.0.0 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 10.4.0.0 setup and do the synchronization. The issue is observed if you update your system from a pre-10.4.0.0 where the rules are deployed from Live with incorrect Module IDs.

Workaround: Delete the rules with incorrect Module ID's 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.

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 data base 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.

Alert pane fails to load when the size of MongoDB is too large

Tracking number: ASOC-9026

Problem: In Security Analytics 10.4.0.0, the alert pane fails to load when the size of MongoDB is too large.

Workaround: You must enable automated ESA storage maintenance to reduce the size of MongoDB.

Forwarding rule name is not updated when advanced rule name changes

Tracking number: ASOC-9585

Problem: For a cross-site deployment, when you change the name of an advanced rule, the forwarding rule does not change along with the name change for the advanced rule. This can result in an orphaned rule which can continue to forward events.

Workaround: To rename a cross-site advance rule, create a new rule and delete the old one.

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 10.5.0.0, 10.5.0.1, and 10.6.0.0, you will need to modify the EPL to use the above workaround.

Query-Based Aggregation EPS rate drops when native aggregation is triggered in parallel

Tracking Number: ASOC-20026

Problem: When query-based aggregation is targeting a Concentrator and Native aggregation is started from a different appliance targeting the same Concentrator, the Query-based aggregation performance drops significantly.

Workaround: None.

Warm-up Duration is Retained When Changing from Packet to Log Automated Threat Detection and vice-versa

Tracking Number: ASOC-22226

Problem: The warm-up duration period is retained when switching between packet and log Automated Threat Detection modules.

Workaround: Manually reset the value for the warm-up duration.

When you switch from Automated Threat Detection for Logs (Using Query-Based Aggregation) to Packets, the mechanism does not change

Tracking Number: ASOC-23874

Problem: When you switch from Automated Threat Detection for Logs (Using Query-Based Aggregation) to Packets, the mechanism does not change.

Workaround: Manually change the value. To change the value, go to **Administration > Services**, select your Event Stream Analysis service and then **View > Explore**. From there, select **Source > nextgenAggregationSource** and change the Mechanism field from "QUERY" to "AGGREGATION".

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.

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.

Reporting Engine

Some compliance reports cannot be deployed from Live

Tracking Number: SAENG-1334

Problem: If the dependencies of certain compliance reports in Live are not deployed prior to the reports themselves, deployment of those fails.

Workaround: Retry the deployment. If the problem persists, try to deploy the rule or list dependencies first and then deploy the reports.

Some Reporting Alerts can fail or be delayed if the RabbitMQ connection is blocked

Tracking Number: SAENG-5329

Problem: If the **Forward Alerts to IM** option is enabled and RabbitMQ connections to the Incident Management are blocked, some of the Reporting Engine threads can be blocked.

Workaround: Disable the **Forward Alerts to IM** option until the RabbitMQ broker in the Security Analytics server at the Incident Management, has started and can accept the connections.

Updates to connection parameters on the Service page do not reflect on the Reporting Data sources

Tracking Number: ASOC-8149

Problem: If there are any changes or updates to service names, ports or parameters on the service page, they are not propagated to the corresponding data sources added in the Reporting Engine.

Workaround: Add data sources with modified service and use them. Additionally, if the names of the existing services are modified, the corresponding schedules must be updated in Reporting.

Cannot Navigate to Investigation from the NWDB reports if the connection parameters on the Service page are updated

Tracking Number: ASOC-8575

Problem: The Investigation link for the meta values of the executed reports is not displayed on the NWDB results page.

Workaround: None. To be fixed in the future release.

Direction meta is not available when the data source is added

Tracking Number: ASOC-24061

Problem: In the OOTB Dashboard, the Investigation Query does not contain quotes for the values when you click on investigate for "Traffic Flow Direction chart" that is available in the "Overview" Dashboard.

Workaround: Restart the Reporting Engine or add data source again or wait for 24 hours to update the schema cache. Restart the jetty that is required to reflect in the dashlet query as a hyperlink of investigation query created during dashlet creation. When you update the RE schema cache, the dashlet is not updated.

An error message is displayed in Reporting Engine, if you select the 'All Day' option for chart display

Reporting

Test Rule results with large data are not displayed in Internet Explorer 10

Tracking Number: SAENG-3926

Problem: When you click the **Test Rule** multiple times in quick succession, results with large input data may not displayed in Internet Explorer 10.

Workaround: If this issue occurs, try one of the following steps:

- Close the Test Rule window on Internet Explorer 10 and run the test again.
- Use other browsers like Chrome or Mozilla Firefox to test the rule execution.

Dynamic Lists cannot be added when editing a report schedule from View All Schedules page

Tracking Number: SAENG-5837

Problem: You cannot add a dynamic list from the Edit option on the 'View All Schedules' page to an existing schedule.

Workaround: Edit the schedule from the Report Schedule page to add a dynamic list.

Proper error message is expected for the rules running with Empty List

Tracking Number: ASOC-16271

Problem: When you execute a rule with empty list values for Numeric, IP address, and Mac address meta, the rule execution fails with the following ambiguous error message: Error occurred while fetching data from source.

Workaround: Create a valid list that contains values and use it for the rule. Using a valid list, the error is not displayed.

Administration

Configuration audit event captured by SA lacks context of which service was changed

Tracking Number: ASOC-8889

Problem: The Security Analytics server does not capture the applicable target service for configuration changes in audit events.

Workaround: None.

Excessive audit logs are logged when accessing SA UI pages/ importing/ exporting/ login/ logout from SA UI

Tracking Number: ASOC-8916

Problem: Security Analytics creates an excessive amount of audit logs when Security Analytics users log on, log out, import, export, and access pages from the Security Analytics user interface.

Workaround: None.

Audit Logs: SA_SERVER is not capturing the value for queryString

Tracking Number: ASOC-8994

Problem: When changing file contents of a Security Analytics service, the Security Analytics 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 Security Analytics server does not mention the name or URL of the Security Analytics server that sent the email. If there are multiple Security Analytics servers, the user may not know where to go to update their password.

Workaround: None.

Audit logs do not report the page (name) accessed when user tries to access SA pages where the user does not have permissions

Tracking Number: ASOC-9323

Problem: When a user tries to access Security Analytics user interface pages without the necessary permissions, the audit logs do not capture the page names accessed by the user.

Workaround: None.

Event Source Management

ESM Automatic Alarms do not work on an All-in-One (AIO) appliance

Tracking Number: ASOC-16588

Problem: Automatic monitoring does not work for data collected through the Log Decoder on an AIO. Policy alarms will continue to work correctly.

Workaround: None.

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

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 LogCollector or LogDecoder columns.

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

1. SSH to the Security Analytics appliance.
2. Restart the SMS service by running this command: service rsa-sms restart.
3. On the Security Analytics 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.

If you are collecting events from deleted event sources, then they are automatically added back to the Event Source Manage page with the new Log Collector or Log Decoder name.

Core Services

Security Analytics Core Services includes Broker, Concentrator, Decoder, and Log Decoder

Incorrect syntax in Concentrator custom index file causes initialization errors

Tracking Number: ASOC-4195

Problem: When starting a Broker, Concentrator, Decoder, or Log Decoder, an initialization error is displayed. This can occur due to the enforcement of XML syntax checking.

Workaround: The index-<SA Core component>-index.xml file now requires proper XML syntax. If you experience this error, add the proper XML header and footer to the XML file to correct the error.

An example of proper headers and footers are in the file as shown below.

Decoder or Log Decoder example:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto?>
<!-- *** Please insert your custom keys or modifications below this line *** -->
</language>
```

Concentrator or Broker example:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexValues" defaultAction="Auto?>
<!-- *** Please insert your custom keys or modifications below this line *** -->
</language>
```

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: Users 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.

Metacallback feeds do not support ranged indices (IP range or CIDR)

Tracking Number: SATCE-260, ASOC-18044

Problem: Security Analytics does not support CIDR when the Metacallback option is selected. Ranged indices are still required for feeds that only need ip.src or ip.dst, but not both.

Workaround: In this release, we provide support for Metacallback feeds for CIDR on Decoder and Log Decoder devices using the existing custom feed advanced configuration wizard. To access the wizard, go to **Live > Feeds, > Custom Feed > Advanced Configuration Wizard**, and use the xml feed definition file. You can also upload xml and feed binary files using the REST interface with **/decoder/parsers/upload**.

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.

Contacting Customer Care

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

RSA Link	https://community.rsa.com/
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email	support@rsa.com
Community	http://www.emc.com/security/security-analytics/security-analytics.htm
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.

Preparing to Contact 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 Security Analytics product or application you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
1.0		RTO