



RSA | Security Analytics

Alerting Using ESA
for Version 10.6.5

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.

October 2017

Contents

Getting Started with ESA	9
Best Practices	9
Understand Event Stream Analysis Rule Types	9
Best Practices for Writing Rules	11
Best Practices for Working with RSA Live Rules	12
Best Practices for Deploying Rules	13
Best Practices for System Health	13
Troubleshoot ESA	14
Troubleshoot ESA Services	14
Troubleshoot ESA Database Issues	16
Troubleshoot RSA Live Rules for ESA	16
Troubleshoot Deployments	17
Troubleshoot Rules	18
Steps to Troubleshoot Memory Issues with an ESA Service Offline	18
View Memory Metrics for Rules	24
Prerequisites	25
Procedures	25
How ESA Generates Alerts	29
Sensitive Data	29
How ESA Treats Sensitive Data from Security Analytics Core	29
Advanced EPL Rule	30
Enrichment Source	30
ESA Rule Types	31
Starter Pack Rules	31
Trial Rules Mode	31
Role Permissions	31
Practice with Starter Pack Rules	32
Rule Library	33
Procedure	34

Work with Trial Rules	37
Deploy Rules as Trial Rules	37
Procedure	38
View Memory Metrics for Rules Using Trial Mode	39
Prerequisites	40
Procedures	40
Add Rules to the Rule Library	43
Download Configurable RSA Live ESA Rules	43
Prerequisites	44
Procedure	44
Customize an RSA Live ESA Rule	45
Add a Rule Builder Rule	46
Step 1. Name and Describe the Rule	47
Step 2. Build a Rule Statement	48
To Add a Whitelist	50
To Add a Blacklist	51
Example: Blacklist	51
Example: Ignoring Case, Strict Pattern Matching, and Using The Is Not Null Operator	52
Example Results	56
Example: Grouping the Rule Results	58
Example: Working with Numeric Operators	59
Step 3. Add Conditions to a Rule Statement	60
Add an Advanced EPL Rule	63
Prerequisites	63
Procedure	63
Event Processing Language (EPL)	65
ESA Annotations	66
Sample Advanced EPL Rules	68
EPL #1:	68
EPL #2:	69

EPL #3:	69
EPL #4: Using NamedWindows and match recognize	70
EPL #5: Using Every @RSAAAlert(oneInSeconds=0, identifiers={"user_src"})	71
EPL #6: @RSAAAlert(oneInSeconds=0, identifiers={"ip_src"})	71
EPL #7: @RSAAAlert(oneInSeconds=0, identifiers={"ip_src"})	72
EPL #8: using groupwin , time_length_batch and unique	73
EPL #9: using groupwin , time_length_batch and unique	74
EPL #10: using groupwin , time_length_batch and unique	74
EPL #11: @RSAAAlert(oneInSeconds=0)	75
Working with Rules	76
Edit, Duplicate or Delete a Rule	76
Edit a Rule	76
Duplicate a Rule	76
Delete a Rule	77
Filter or Search for Rules	78
Filter	78
Search	78
Import or Export Rules	79
Import ESA Rules	80
Export	81
Choose How to be Notified of Alerts	83
Notification Methods	84
Add Notification Method to a Rule	85
Prerequisites	86
Procedure	86
Add a Data Enrichment Source	89
Sample Rule with Enrichment	90
Configure a Database Connection	92

Procedure	93
Enrichment Sources	95
Configure a Database as Enrichment Source	95
Configure In-Memory Table as Enrichment Source	97
Configure an Adhoc In-Memory Table	98
Add a Recurring in-Memory Table	101
Configure Warehouse Analytics as an Enrichment Source	103
Add an Enrichment to a Rule	105
Procedure	105
Deploy Rules to Run on ESA	107
How Deployment Works	107
Deployment Steps	108
Step 1. Add a Deployment	108
Step 2. Add an ESA Service	109
Step 3. Add and Deploy Rules	111
Additional Deployment Procedures	112
Delete ESA Service in a Deployment	112
Edit or Delete Rule in a Deployment	113
Edit a Rule	113
Delete a Rule	113
Edit or Delete a Deployment	113
Show Updates to a Deployment	115
View ESA Stats and Alerts	117
View Stats for ESA Service	117
Procedures	117
View a Summary of Alerts	118
Procedure	118
Behavior Analytics Automated Threat Detection	123
Understanding Behavior Analytics Automated Threat Detection	123
Workflow	124
Behavior Analytics Automated Threat Detection on Packets vs. Web Proxy Logs	125
Configure Behavior Analytics Automated Threat Detection	126

Prerequisites	126
Procedure: Configuring Behavior Analytics Automated Threat Detection	127
Result	140
Next Steps	141
Work with Behavior Analytics Automated Threat Detection Results	141
Understand Threat Detection Results	141
What to Do Next	143
	146
Troubleshoot Behavior Analytics Automated Threat Detection	146
Possible Issues	147
References	149
New Advanced EPL Rule Tab	149
Features	150
Alerts Summary View	152
Features	153
Build a Statement Dialog	156
Features	157
Deploy ESA Rules Dialog	160
Features	161
Deploy ESA Services Dialog	161
Features	162
Rule Builder Tab	162
Features	163
Rules Tab	168
Features	169
Options Panel	169
Rules Section	170
Deployments Section	170
Rule Library Panel	170
Rule Library Toolbar	172
Rule Library List	172
Deployment Panel	174
ESA Services	174

ESA Rules	175
Rule Syntax Dialog	176
Features	177
Select an ESA Service Dialog	178
Features	178
Services Tab	179
Features	179
Deployed Rule Stats Panel	181
	181
Settings Tab	182
Features	183
Database Connections	184
Updates to the Deployment Dialog	185
Features	186

Getting Started with ESA

This topic covers quick start topics for Event Stream Analysis (ESA) to help you get started in using ESA. The following topics are designed to help enable you to work with ESA.

- This topic helps you to understand how to best set up, deploy, and create rules. See [Best Practices](#)
- This topic helps you to troubleshoot different aspects of ESA, including rule writing and deployment: [Troubleshoot ESA](#)
- This topic helps you to work with memory metrics to understand memory usage for ESA services. See [View Memory Metrics for Rules](#)

Best Practices

Best practices provide guidelines to help you write and manage rules, deploy rules, and maintain system health for your ESA services.

Understand Event Stream Analysis Rule Types

The Security Analytics Event Stream Analysis (ESA) service provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators. However, when working with Event Stream Analysis, you should be aware of the factors that affect resource usage in order to create effective rules.

Each event that is received by ESA is evaluated to determine if it may trigger a rule. There are three types of rules that can be deployed in order to determine what the ESA engine should do with the incoming event. Each of these rule types have different impacts on system resource utilization. All three rule types may be created via the Rule Builder, Advanced EPL rules, or downloaded via RSA Live. The table below lists the rule type and the impact this rule may have on system resources.

Rule Type	Description
Simple Filter Rule	<p>This rule has no correlation to other events. At ingestion time, this rule is evaluated against a set of conditions, and if those conditions are met an alert is generated. If no conditions match, the event is quickly released by the engine to free up memory usage. These rules do not take up memory since the events are not retained beyond the initial evaluation. The memory resource usage does not increase as more simple filter rules are deployed. However, if the filter condition is too generic, it is possible that this rule can generate too many alerts, which will strain the system resources for the storage and retrieval of these alerts.</p> <p>For example, you might write a rule to generate an alert when HTTP network activity arrives over a non-standard HTTP port.</p>
Event Window Rule	<p>This rule evaluates a set of events over a time period for specific conditions. At ingestion time, the rule is evaluated against a set of conditions. If those conditions are met, the event is retained in memory for a specific amount of time. After the specified time passes, the events are removed from the time window if the number of events collected does not meet the threshold to trigger an alert. The memory consumption of such rules are highly dependent on the incoming event rate (traffic), the amount of data per event, and the time length specified in the event window. Each matching event is retained in memory until the time window has passed, so the longer the time window, the greater the potential volume. For example, you might write a rule that generates an alert if a user fails to log into any system five times within a ten minute time frame.</p>

Rule Type	Description
Followed By Rule	<p>This rule evaluates a chain of incoming events to determine if the sequence of events matches a particular condition. At ingestion time, the rule is evaluated against a set of conditions. If the conditions are met, one of two actions occurs:</p> <ul style="list-style-type: none"> • If this is first event of the sequence, a new event thread is started, and the event is retained as the head of the sequence. • If the event belongs to an existing event thread, it is added to that sequence. <p>In both cases, the event is retained in memory. The amount of resource usage is particularly sensitive to the customer environment for this type of rule. If the filter condition generates many event threads, resources are consumed for for each new thread (in addition to the event). Additionally, if the end of the event thread is never met (i.e. an alert is never generated), then the entire event is saved in memory indefinitely. For example, you might write a rule to generate an alert when a user fails to log into a server, then performs a successful login, and then creates a new account.</p>

In addition to the memory usage discussed above, alert generation also consumes system resources. Each alert that is generated must be stored for retrieval and must also be processed by Incident Management. This process uses disk space for storage, requires database memory to be consumed, and increases CPU utilization running queries.

When writing and deploying rules, you should be aware that each of these actions “cost” you system resources. The sections below are designed to help you keep your usage at a healthy level and monitor for problems if systems are becoming overloaded.

Best Practices for Writing Rules

These are general guidelines for writing rules.

- **Create alerts for actionable events.** The purpose of an alert should be to notify you of an event that requires immediate and specific action. For events that do not require action, or only require you to have awareness of the event, you can create a report. This helps to prevent you from overloading the database that stores alerts.
- **Configure new rules as trial rules so you can observe how they react in your environment.** If you deploy new rules as trial rules, they will be disabled if the configured

memory threshold is exceeded. You can also use the memory snapshot feature to see how much memory was being used when a trial rule was disabled. For more details, see [Work with Trial Rules](#).

- **Configure Alert notifications only after your rule testing and tuning is complete.** This can help ensure you do not get flooded with notifications if a rule behaves differently than you expect.
- **Rules need to be specific so that you limit resource usage.** Use the following guidelines to limit usage:
 - Make the filters on the rule exclude all but the necessary events for the rule to fire accurately.
 - Make the size of your windows (window time for correlation) as small as possible.
 - Limit the events that you include in the window: For example, if you only want to see IDS events, ensure that you only include those events in your time window.
- **Rules need to be tuned to an alert level that is manageable.** If you are flooded with alerts, then the purpose and utility of an alert is lost. In addition, it's possible to flood the database that stores alerts, which can slow or prevent your system from processing alerts. For example, maybe you want to know about encrypted traffic to other countries. But, you could limit the list to countries that are known risks. This limits the volume of alerts to a level you can manage.

Best Practices for Working with RSA Live Rules

These are guidelines for RSA Live Rules.

- **Deploy RSA Live rules in small batches.** Not every rule is suited to every environment. The best way to ensure your RSA Live rules are successful is to deploy them in small batches so you can test them in your environment. If you deploy small batches, it's much easier to tell if a particular rule has an issue.
- **Read the rule descriptions provided with RSA Live rules.** ESA rules are not “one size fits all.” Not all rules will work in your environment. The rule descriptions tell you which parameters you will need to modify to successfully deploy a rule in your environment.
- **Set your parameters.** RSA Live rules have parameters that need to be modified. If you do not modify your parameters, the rule may not work or it may exhaust your memory.

- **Deploy new rules as trial rules so you can observe how they react in your environment.** If you deploy new rules as trial rules, they will be disabled if the configured memory threshold is exceeded. For more details, see [Work with Trial Rules](#).

Best Practices for Deploying Rules

These are general guidelines for deploying rules.

- **Deploy rules in small batches so you can observe how they react in your environment.** Not all environments are the same, and a rule will need to be tuned for memory usage, alert volume, and effective detection of events.
- **Test rules before you configure alert notifications.** Configure Alert notifications only after your rule testing and tuning is complete. This can help ensure you do not get flooded with alerts if a rule behaves differently than you expect.
- **Monitor system health as a part of your deployment process.** When you deploy rules, monitor your system's health as a part of your deployment process. You can view total memory utilization for your ESA in the Health and Wellness tab. For more information, see "Viewing Health and Wellness statistics" in [Troubleshoot ESA](#).

Best Practices for System Health

These are general guidelines for system health.


- **Configure the alerts database to maintain a healthy level of alerts.** ESA uses MongoDB to store alerts. If the MongoDB becomes flooded with alerts, it can slow or stop the database. To ensure your database maintains a healthy level of alerts, configure settings to clear out alerts regularly. To do this, see "Configure ESA Storage" in the **Event Stream Analysis (ESA) Configuration Guide**.
- **Set up new rules as trial rules.** A common issue is that new rules may cause memory issues. To prevent this, you can set up new rules as trial rules. If the configured memory threshold is met, all trial rules are disabled to prevent the system from running out of memory. For more information about trial rules, see [Work with Trial Rules](#).
- **Set up thresholds in the Health & Wellness module to alert you if memory usage is too high.** There are metrics in the Health & Wellness module that track memory usage. You can set up alerts and notifications to send you an email if those thresholds are crossed. For more information about the memory statistics you can view, see "Viewing Health and Wellness statistics" in [Troubleshoot ESA](#).

- **Monitor memory metrics for each rule in the Health & Wellness module.** For each rule, you can view the estimated memory usage in the Health & Wellness module. You can use this information to ensure that rules do not use too much memory. For more information about the memory statistics you can view, see "Viewing Health and Wellness statistics" in [Troubleshoot ESA](#).

Troubleshoot ESA

This section describes common issues that may occur while using ESA, and it suggests common solutions to these problems.

Troubleshoot ESA Services

Problem	Possible Causes	Solutions
<p>On the Security Analytics Dashboard, the ESA service displays in red to indicate it is offline.</p> <p>On the Alerts > Configure page, the following message displays: "The Service is either offline or not reachable."</p>	<p>Several</p>	<p>When an ESA service is offline, there are many possible causes. However, a common issue is that you have created a rule that uses excessive memory and causes the ESA service to fail. To troubleshoot this problem, see "Steps to Troubleshoot Memory Issues with an ESA Service Offline."</p> <p>Other common causes might be that your firewall is blocking the connection between the ESA and Security Analytics, or the ESA service machine may be down.</p>
		<p>To bring up ESA Services:</p> <p>From Administration > Services, select the actions icon  for your ESA service, and choose start.</p> <p>If your ESA service is stopping and restarting in a loop, you may need to call Customer Support to get the services to start.</p>



Problem	Possible Causes	Solutions
<p>After a recent upgrade, the ESA service displays in red on the Security Analytics Dashboard to indicate it is offline.</p> <p>On the Alerts > Configure page, the following message displays: "The Service is either offline or not reachable."</p>	Configuration issues	<p>If your system has been recently upgraded, you may have made a configuration error. Under Administration > Services, select your ESA service, and click on Edit Service. On the Edit Service field, click Test Connection. If the connections fails, you likely have a configuration error. Attempt to fix your configuration error, and try again.</p>
The ESA appears to be running slowly.	Configuration issues	<p>You may be able to improve performance by modifying the buffer (the default value is <i>1048576 bytes</i>), or setting the TCP setting to <code>TCPNoDelay</code> to prevent a delay in receiving TPC Acks. You can modify these settings (<i>readBufferSize</i> and <i>tcpNoDelay</i>) by going to <i>Explorer /Workflow/Source/nextgenAggregation</i> .</p>

Troubleshoot ESA Database Issues

Problem	Possible Causes	Solutions
My ESA Dashboard doesn't load.	The database that stores alerts	You may need to configure Alert database settings so that the database clears old alerts on a timely basis. For information on configuring these settings, see "Configure ESA Storage" in the Event Stream Analysis (ESA) Configuration Guide .
<ul style="list-style-type: none"> • Or, there is an error getting data. • Or, it loads very slowly. 	has grown too large.	Once the database has become too large, you need to clear the alerts. Contact Customer Support to do this.

Troubleshoot RSA Live Rules for ESA

Problem	Possible Causes	Solutions
I imported a group of rules from RSA Live, and now my ESA service is crashing. Why?	You may not have configured the parameters for the RSA Live rule to tune it for your environment.	Each rule in RSA Live has a description that includes the parameters you must configure and prerequisites for your environment. Review this description to see if the rule is appropriate for your environment. To ensure that you deploy rules safely in your environment, configure new rules as trial rules to test them in your environment. Trial rules add a safeguard for testing new rules. For details on this, see Deploy Rules as Trial Rules .

Problem	Possible Causes	Solutions
I imported a group of rules from RSA Live, and while the rules deployed without errors, they were later disabled.	Not all RSA Live rules are meant for every environment. You may not have the correct meta in your ESA for the rule to run.	<p>You can verify that a rule was disabled by going to Alerts > Services > Deployed Rule Stats. If the rule is disabled, the green icon does not display next to the rule.</p> <p>If a rule deployed correctly but was disabled, check the logs for exceptions related to the rule. Specifically, check to see if the rules were disabled due to missing meta. To do this, go to Administration > Services, select your ESA service and then   > View > Logs.</p> <p>Then, search for a message similar to the following:</p> <p>"Property named '<meta_name>' is not valid in any stream"</p> <p>For example, you might see:</p> <pre>Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream</pre> <p>If a similar message displays, you may need to add a custom meta key to the Log Decoder or Concentrator. To do this, follow these instructions: "Create Custom Meta Keys Using Custom Feed " in the Decoder and Log Decoder Configuration Guide.</p>

Troubleshoot Deployments

Problem	Possible Causes	Solutions
I created a rule, and I checked the syntax. The rule looked fine. When I went to deploy the rule, I got an error. Why?	You may not have the correct meta to deploy the rule.	Check the Meta key references. You may not have the correct meta to deploy the rule.

Troubleshoot Rules

Problem	Possible Causes	Solutions
I created a custom rule (via the Rule Builder or Advanced EPL), and my rule is not firing. Why?	You may have connectivity issues.	<p>Check the 'Offered Rate' statistic on the Alerts > Configure > Services tab.</p> <p>If the offered rate is zero, then the ESA service is not receiving data from Concentrators. Validate the Concentrator connectivity. Go to Administration > Services, select your ESA and click on View > Config. Ensure the concentrator is enabled. Select the concentrator and click on test connection.</p> <p>If the offered rate is not zero, the meta key name and type used in the rule likely doesn't match the meta key present in events. Check to see if the meta key name and type used in the rule is valid by searching for the meta key name in Alerts > Configure > Settings tab (Meta key references search).</p>
	There may be a problem with the rule.	<p>If a specific rule is not firing, go to Alert > Configure > Services to see if the rule was disabled. In the Deployed Rule Stats section, a rule that is disabled displays a clear enabled button (instead of the green enabled button).</p> <p>You can also check Events Matched field. Go to Alerts > Configure > Services. From there, you can see the number of events that were matched in the Events Matched column.</p> <p>If no events matched, check the logic of your rule for errors. For example, check the syntax for uppercase and lowercase errors, and check the time window. If the rule still doesn't fire, consider simplifying the logic of the rule to see if it fires when there is less complexity.</p>

Steps to Troubleshoot Memory Issues with an ESA Service Offline

Step 1: Verify that your Host is Running

The first step to troubleshooting is to ensure that your host is running. To do this, go to **Administration > Hosts**. If the host is down, the system parameters will not display (updating host information can sometimes be delayed), the **Services** displays in red, and the **Updates** field displays an error message.

Name	Host	Services	Total Memory	CPU	OS	Uptime	Updates	Actions
231	10.101.59.231	1	94.56 GB	3.38%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 52 se...	Up-to-Date	[Refresh] [Stop]
232	10.101.59.232	1	94.56 GB	0.35%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 51 se...	Up-to-Date	[Refresh] [Stop]
233	10.101.59.233	3	94.56 GB	0.45%	Linux 2.6.32-431.2...	3 weeks 2 days 23 hours 9 minutes 52 sec...	Up-to-Date	[Refresh] [Stop]
234	10.101.59.234	2	94.56 GB	0.23%	Linux 2.6.32-431.2...	3 weeks 2 days 23 hours 9 minutes 35 sec...	Up-to-Date	[Refresh] [Stop]
235	10.101.59.235	5	94.56 GB	4.65%	Linux 2.6.32-431.2...	3 weeks 2 days 23 hours 9 minutes 23 sec...	Up-to-Date	[Refresh] [Stop]
236	10.101.59.236	1	94.56 GB	0.34%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 48 se...	Up-to-Date	[Refresh] [Stop] [Error]
237	10.101.59.237	2	94.56 GB	0.42%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 49 se...	Up-to-Date	[Refresh] [Stop]
238	10.101.59.238	2	94.56 GB	0.43%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 49 se...	Up-to-Date	[Refresh] [Stop]
239	10.101.59.239	2	94.56 GB	3.26%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 47 se...	Up-to-Date	[Refresh] [Stop]
240	10.101.59.240	1	94.56 GB	0.21%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 47 se...	Up-to-Date	[Refresh] [Stop]
241	10.101.59.241	1	94.56 GB	0.22%	Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 48 se...	Up-to-Date	[Refresh] [Stop]
242	10.101.59.242	1	94.56 GB		Linux 2.6.32-431.2...	2 weeks 2 days 21 hours 44 minutes 48 se...	Up-to-Date	[Refresh] [Stop]

If your host is down, contact your SA Administrator to restart it. Otherwise, go to Step 2.

Step 2: View Detailed Statistics in Health & Wellness

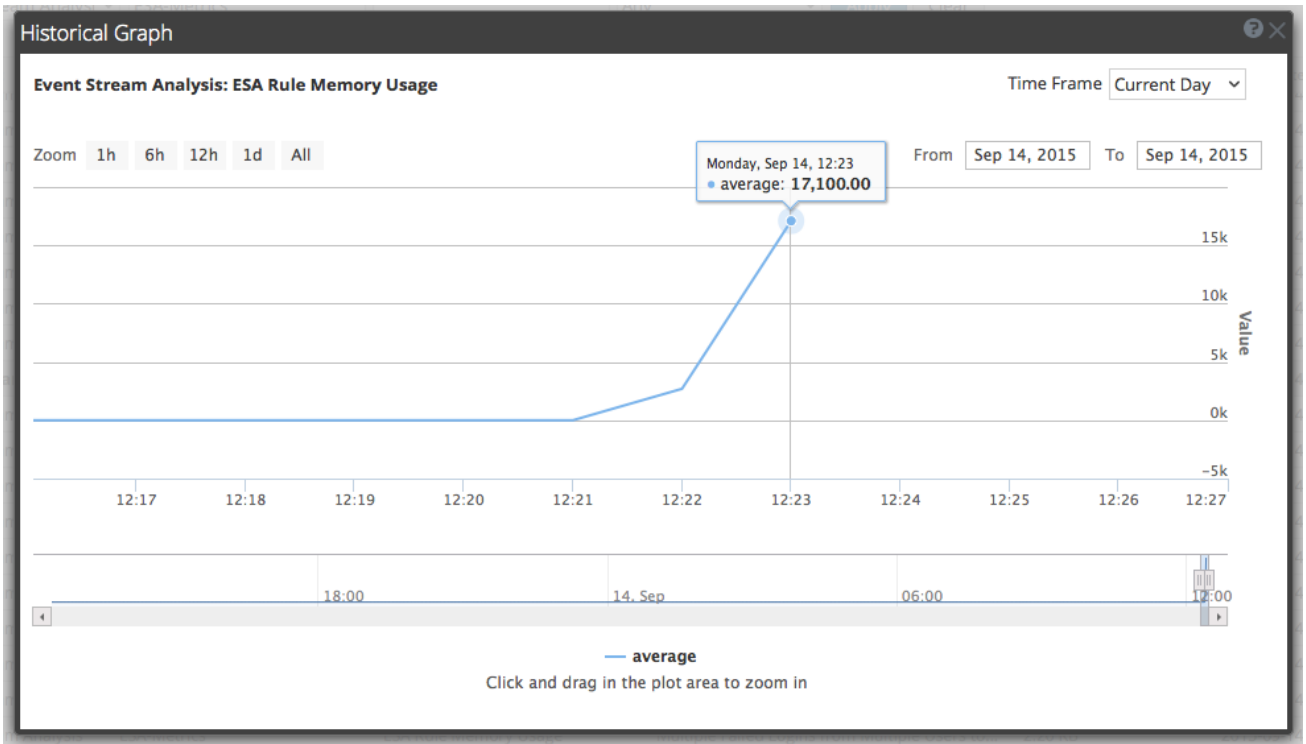
Once you are sure your ESA service is down, you can go to Health & Wellness to see where potential issues are occurring. The most common problem is that your ESA service is exceeding memory thresholds which causes it to stop or fail.

- Go to **Health & Wellness > Alarms** to see if the ESA triggered any alarms. Look for the following alarms:
 - ESA Overall Memory Utilization > 85%
 - ESA Overall Memory Utilization > 95%
 - ESA Service Stopped
- Go to **Health & Wellness > System Stats Browser** to see the memory metrics for each rule's performance. To view the metrics, enter the following:

Host	Component	Category
<your host>	Event Stream Analysis	esa-metrics

Host	Component	Category	Statistic	Order By	Value	Last Update	Historical Graph
New York, Paris	Event Stream Analysis	esa-metrics		Any			
				Ascending			
New York	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		0.15%	2015-09-24 09:01:23 P...	
New York	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-09-24 09:00:14 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Forwarder	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Cross-site Correlation ...	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Cross-site Correlation ...	184 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Cross-site Correlation ...	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Cross-site Correlation ...	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Forwarder	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Cross-site Correlation ...	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Forwarder	0 bytes	2015-09-24 08:23:47 P...	

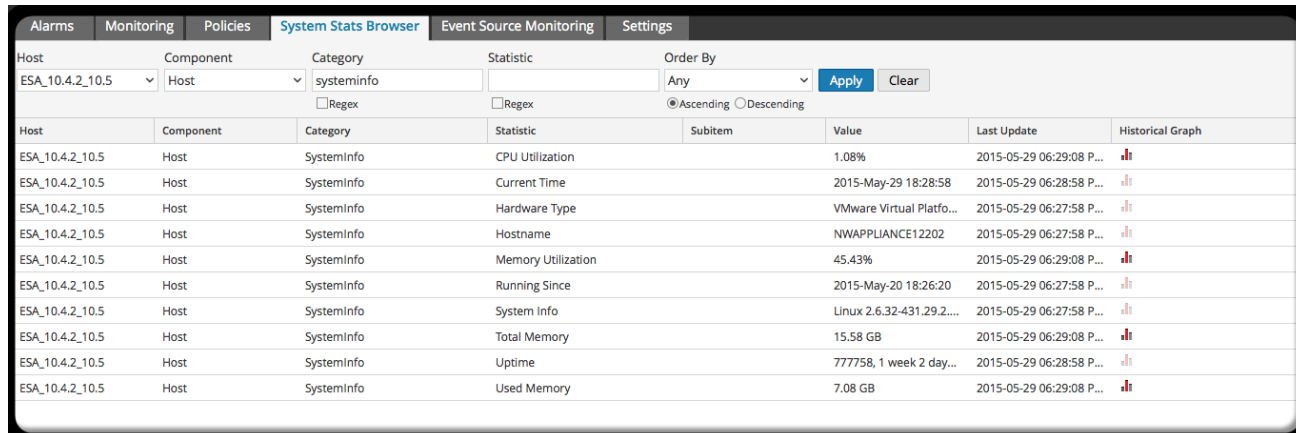
The memory for each rule is displayed in the **Value** column, and the value is displayed in bytes. You can view a historical view of memory usage in the **Historical Graph** column.



- Go to **Health & Wellness > System Stats Browser** to see details of your ESA performance. Select your host, and use the following filters to view the following statistics:


Host	Component	Category	Statistic	Example
<your host>	Host	SystemInfo	CPU Utilization	1.08%

Host	Component	Category	Statistic	Example
<your host>	Host	SystemInfo	Memory Utilization	45.43%
<your host>	Host	SystemInfo	Used Memory	7.08 GB
<your host>	Host	SystemInfo	Total Memory	15.58 GB
<your host>	Host	SystemInfo	Uptime	77758, 1 week, 2 day...
<your host>	Event Stream Analysis	ProcessInfo	Memory Utilization	7.07 GB
<your host>	Event Stream Analysis	ProcessInfo	CPU Utilization	0.2%
<your host>	Event Stream Analysis	JVM.Memory	all	Committed Heap Memory Usage 8.0 GB
<your host>	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %	4.64%



If you are having a problem with memory or CPU utilization, continue to step 3.

Step 3: Bring up your ESA Services

1. From **Administration** > **Services**, select the actions icon  for your ESA service and choose **start**.
2. Return to the ESA Service to troubleshoot which rules have created memory issues.

If your ESA service is stopping and restarting in a loop, you may need to call Customer Support to get the services to start.

If you are able to start your ESA service without a shutdown, continue to step 4.

Step 4: Check the Alerts and Events Volume

Once you are able to restart your ESA service without an immediate shutdown, you can review the stats for your rules to see which rules are consuming too many resources. Sometimes, ESA services fail because a rule is generating too many alerts or a rule is matching too many events. Check for both of these issues if you have determined that memory usage is causing your ESA service to shut down.

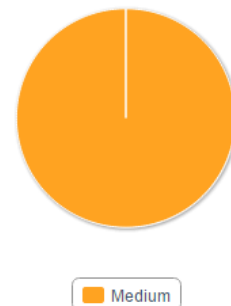
View Alert Summaries

Rules that generate a high volume of alerts can overwhelm the system and cause it to fail or restart. To view the alert summaries, go to **Dashboard** > **Alerts** > **Summary**. On the lower half of the screen, you can see the number of alerts generated for each rule in the **Count** field. If the number is significantly high for a particular rule, you need to disable the rule and rewrite it to be more efficient.

Alerts

Name	Count	Severity	Last Detected
epl_module_no_18	5123	Medium	2015-05-19T00:39:57
epl_module_no_21	12454	Medium	2015-05-19T00:39:57
epl_module_no_48	12454	Medium	2015-05-19T00:39:57
epl_module_no_12	12454	Medium	2015-05-19T00:39:57
epl_module_no_22	12454	Medium	2015-05-19T00:39:57
epl_module_no_49	12454	Medium	2015-05-19T00:39:57
epl_module_no_42	12454	Medium	2015-05-19T00:39:57
epl_module_no_27	12454	Medium	2015-05-19T00:39:57

Alerts by Severity



View Events Matched

Sometimes a rule matches too many events which can use up excessive memory. This typically occurs if you create a large event window where a great number of events accumulates without triggering an alert. These are a problem because each event is stored in memory while the rule waits for the alert to trigger. To check for this issue, go to **Dashboard > Alerts > Services**. From there, you can see the number of events that were matched in the **Events Matched** column. If there was a high number of events matched for a given rule, you can investigate the rule further to see if you can make it more efficient.

The screenshot shows the 'Services' tab in the ESA interface. The main content area displays '231 - Event Stream Analysis' with 'Local ESA' selected. It includes three summary sections: Engine Stats, Rule Stats, and Alert Stats. Below these is the 'Deployed Rule Stats' section, which contains a table of active rules. The 'Events Matched' column for the first rule, 'epl_module_no_43', is circled in red, showing a value of 70555. Other rules in the table have 12454 events matched. The interface also shows navigation controls at the bottom, including 'Page 1 of 3' and 'Page Size 25'.

Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	epl_module_no_43	Yes	2015-05-19 00:39:57	70555
<input type="checkbox"/>	epl_module_no_9	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_19	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_50	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_12	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_3	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_13	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_4	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_1	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_10	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_11	Yes	2015-05-19 00:39:57	12454


Step 5: Disable and Repair the Rule that Caused Issues

Once you have determined the rules that need to be rewritten, disable them and rewrite rules so that they don't generate such a high volume of alerts or events. For pointers on how to write more efficient rules, see [Best Practices](#).

Disable Rules

1. To disable rules, go to **Alerts > Services**, and select the rules you want to disable in the **Deployed Rules Stats** field.
2. Select **Disable** to disable the rules.


Edit Rules

1. To repair the rules, go to **Alerts > Rules > Rule Library**. Select the rule to edit, and click the actions icon .
2. Select **Edit**.
3. Edit the rule to be more efficient. For instructions on creating rules, see [Add Rules to the Rule Library](#)
4. Once you are satisfied with your rule, you can save the rule as a trial rule to ensure that any memory issues do not affect ESA services performance. To do this, follow the steps listed in [Work with Trial Rules](#).

Enable Rules

1. To enable rules, go to **Alerts > Services**, and select the rules you want to enable in the **Deployed Rules Stats** field.
2. Select **Enable** to enable the rules.

(Optional) Check the ESA Log Files for More Information

Once you verify that your services are down and some potential causes for the system going down, check to see if the service is stopping and restarting in a loop. To do this, go to the ESA logs. From the **Administration > Services** module, select your ESA service and click the actions icon  and select **View > Logs**.

If you cannot access the ESA logs from the Security Analytics interface, you can SSH into the system and go to: `opt/rsa/esa/logs/esa.log`.

View Memory Metrics for Rules

This topic tells ESA rule writers how to view memory metrics for rules. You can see estimated memory usage for each rule running on a server, and you can use this information to modify your rule statements and conditions if they use too much memory.

Rules can sometimes consume more memory than you expect, causing your ESA to slow down or stop. To see approximately how much memory a rule is using, you can configure memory metrics. Memory metrics allow you to view an estimated memory usage for each rule in the Health & Well System Stats browser (so you will need permissions to access this module). You can use this information to modify your rules to be more efficient.

At a high level, you will need to complete the following steps to use the memory metrics to troubleshoot memory usage for rules:

1. Ensure that the memory metrics feature is enabled (via Explorer > CEP > Metrics > EnableStats). The Memory Metrics feature is enabled by default.
2. Ensure you have the correct permissions to view the Health & Wellness module. For information on roles and permissions, see [Role Permissions](#).
3. View the memory statistics in Health & Wellness.
4. (Recommended) Configure Health & Wellness ESA policies to send an email if memory thresholds are exceeded. See "Manage Policies" in the **System Maintenance Guide** for instructions on sending email notifications.
5. Use the memory metrics data to modify rules to be more efficient, if necessary.

Prerequisites

The following are requirements for using memory metrics:

- Memory Metrics feature is enabled (via **Explorer > CEP > Metrics > EnableStats**).
- The user must have the appropriate permissions to view Health & Wellness statistics.
- (Recommended) Configure the ESA Health & Wellness policy to send an email when memory thresholds are exceeded.

Procedures

View Memory Metrics in the Health & Wellness System Monitoring Module

1. In the **Security Analytics** menu, go to **Administration > Health & Wellness > ESA > System Monitoring**
2. View the details for your ESA service.
3. Select **Rules**.
4. You can view the average memory usage for each rule for the previous hour.

Alerting Using ESA

Name	Event Stream Engine	Total Estimated Memory (last hr)
Rule with MatchRecognize	Local ESA (Default)	<1% 7.32 KB / 64.00 GB
Failed Logins Followed By Successful Login Password Change	Local ESA (Default)	<1% 336 bytes / 64.00 GB
Rule with Pattern	Local ESA (Default)	<1% 150 bytes / 64.00 GB
Brute Force Login To Same Destination	Local ESA (Default)	<1% 53 bytes / 64.00 GB
Brute Force Login From Same Source	Local ESA (Default)	<1% 45 bytes / 64.00 GB
Logins across Multiple Servers	Local ESA (Default)	<1% 45 bytes / 64.00 GB
Multiple Failed Logins from Multiple Diff Sources to Same Dest	Local ESA (Default)	<1% 45 bytes / 64.00 GB

View Memory Metrics in the Health & Wellness System Stats Browser

1. In the **Security Analytics** menu, go to **Administration > Health & Wellness > System Stats Browser**.
2. For component, select **Event Stream Analysis**. For category, enter **ESA-Metrics**.

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

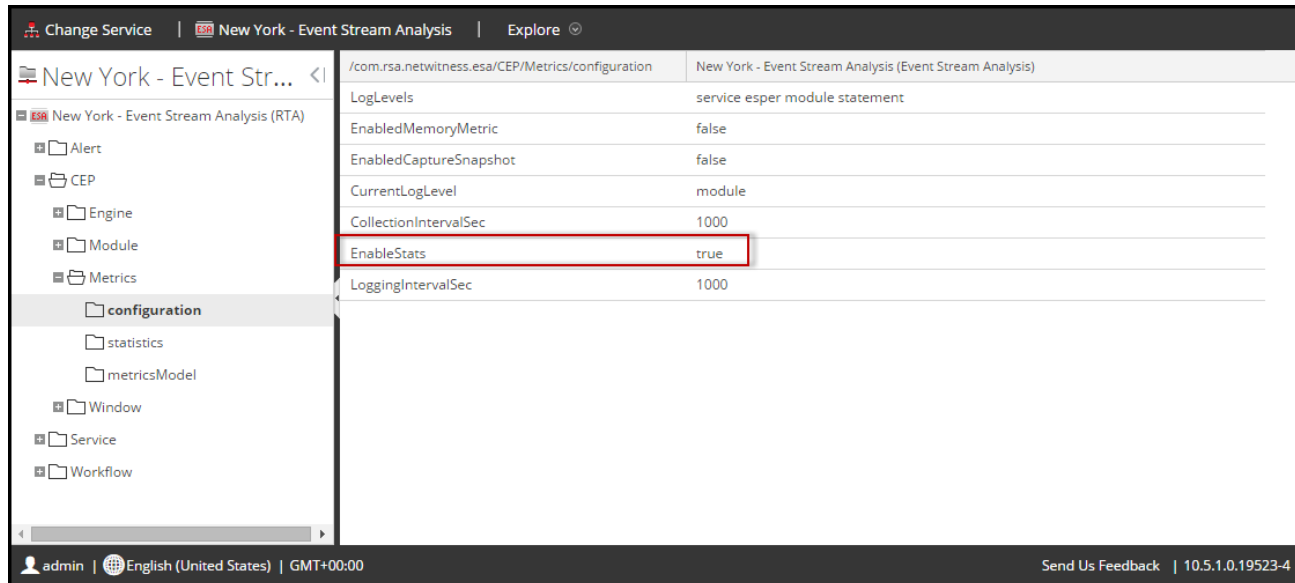
The name of the rule is displayed in the **Subitem** field, and the memory usage is displayed in the **Value** column.

3. To view the historical memory usage for the rule, click on the **Historical Graph** icon.

Note: The **Last Update** field reflects when Health & Wellness polls ESA. However, the Memory Metrics is not synchronized with the Health & Wellness polling. For example, if the memory threshold is exceeded on 10/10/15 at 12 p.m., but Health & Wellness polls at 10/10/15 at 12:10 p.m., the **Last Update** field will display a timestamp of 10/10/15 12:10 p.m.

Enable or Disable the Memory Metrics Feature

1. In the **Security Analytics** menu, go to **Administration > Services** and select your ESA.
2. Once you've selected your ESA, click on **Actions > View > Explore**, and navigate to **CEP Metrics > Configuration** as shown below.



3. Change the field **EnabledStats** to **true** or **false** depending on whether you want to enable or disable the memory metrics feature.

How ESA Generates Alerts

This topic provides a brief description of how an Event Stream Analysis (ESA) service runs rules to generate alerts. The Security Analytics Event Stream Analysis (ESA) service runs rules that specify criteria for problem behavior or threatening events in your network. When ESA detects an incident that matches rule criteria, it generates an alert.

To generate alerts, ESA performs the following functions:

1. Gathers data
2. Runs ESA rules against the data
3. Captures events that meet rule criteria
4. Generates alerts for those captured events

You can use the Alerts module to gain visibility into your network and to detect problems in it.

Sensitive Data

This topic explains how ESA treats sensitive data, such as usernames or IP address, that it receives from Security Analytics core. The Data Privacy Officer (DPO) role can identify meta keys that contain sensitive data and should display obfuscated data. ESA will not display or store sensitive meta. Consequently, ESA will not pass sensitive data to Incident Management.

Optionally, ESA can add an obfuscated version of the sensitive data to an event. For example, the DPO identifies `user_dst` as sensitive. ESA can add an obfuscated version, such as `user_dst_hash`, to an event. The obfuscated meta is not sensitive, so ESA will display and store it the same way as any other non-sensitive meta.

For more information on the strategy and benefits of obfuscating data, see the **Security Analytics Data Privacy Management Guide**.

This topic explains the following:

- How ESA treats sensitive data it receives from Security Analytics core
- How to prevent sensitive data leaks in an Advanced EPL rule

How ESA Treats Sensitive Data from Security Analytics Core

When ESA receives sensitive data from Security Analytics core, ESA passes on only the obfuscated version of the data. ESA does not store or show sensitive data.

The following features are impacted:

- Outputs – ESA does not forward sensitive data to outputs, which include alerts, notifications and MongoDB storage.
- Advanced EPL rules – If an EPL statement creates an alias for a sensitive meta key, sensitive data will leak. This topic illustrates how this happens so you can avoid it.
- Enrichments – If a sensitive meta key is used in the join condition, sensitive data will leak. This topic illustrates how this happens so you can avoid it.

Advanced EPL Rule

If an EPL query statement renames a sensitive meta key, the data will not be protected.

ESA identifies a sensitive meta key by the name:

- ip_src is the sensitive meta key.
- ip_src_hash is the non-sensitive, obfuscated version.

To support data privacy, the sensitive meta key must not be renamed in an EPL query. If a sensitive meta key is renamed, the data will no longer be protected.

For example, in a rule such as select ip_src as ip_alias..., ip_alias contains the sensitive data but it is not protected because ESA only knows about ip_src, not ip_alias. In this case, IP addresses would not be obfuscated. Real values would be displayed.

Enrichment Source

When a sensitive meta key is used in a join condition, sensitive data can be displayed.

The enrichment database, which is the other part of the join condition, has one column that matches the sensitive meta key. This cross reference is to actual values not obscured values. Consequently, actual values are displayed.

In the following example, both parts of the join condition are highlighted.



Enrichments		ESA Event Stream Meta	Enrichment Source Column Name
<input type="checkbox"/>	GeolIP	ip_src	ipv4

- ip_src contains sensitive data.
- ipv4 will be added to the alert and exposed as non-sensitive data

Because the ipv4 value is the same as the ip_src value, ipv4 contains and displays sensitive data.

ESA Rule Types

This topic describes each type of ESA rule, when to use them and the permissions each role has with them. The following table lists each type, describes it and explains when to use it.

Rule Type	Description	When to Use
Rule Builder	In the rule builder, you define rule criteria in an easy-to-use interface.	Use the rule builder to create your first rules. You choose many of the rule conditions from lists.
Advanced EPL	With the Event Processing Language (EPL), you define rule criteria by writing a query.	Use advanced EPL rules to define rule criteria for in the EPL syntax.
RSA Live ESA	RSA Live has a catalog of ESA rules that you can download and modify to run in your network.	Download RSA Live ESA rules to leverage rules that are already built. Modify the configurable parameters to customize to meet your requirements.

Starter Pack Rules

A few sample Rule Builder rules come with Security Analytics and appear in the Rule Library. Use starter pack rules to get comfortable working with rules before creating your own. You can safely edit and deploy these sample rules.

Trial Rules Mode

For any type of rule, you can select the Trial Rule setting as an additional safeguard. Trial rules get disabled if they exceed a memory threshold the administrator sets. Run a rule in trial mode to monitor memory usage and to disable the rule automatically if it uses more memory than the threshold allows.

Role Permissions

This topic lists all ESA permissions and shows which permissions are assigned to each pre-configured Security Analytics role. User access is restricted based on roles and permissions assigned to roles.

- Administrators
- Operators
- Analyst
- Security Operations Center (SOC) Managers
- Malware Analysts (MA)
- Data Privacy Officer

There are four permissions for ESA:

1. Access Alerting Module – Is required for any permission
2. View Rules – Allows view-only permission for rules in the Rule Library
3. View Alerts – Allows view-only permission for alerts ESA generates
4. Manage Rules – Allows you to view, create, edit and delete rules

The following table lists permissions for ESA and the roles to which they are assigned. Use this table to see how each role can work with rules and alerts.

Permission	Administrators	Operators	Analysts	SOC Mgrs	MA's	DPOs
Access Alerting Module	Yes	Yes	Yes	Yes		Yes
View Rules	Yes	Yes		Yes		Yes
View Alerts	Yes		Yes	Yes		Yes
Manage Rules	Yes	Yes		Yes		Yes

For more information on roles and permissions, see the **System Security and User Management Guide**.

Practice with Starter Pack Rules

Security Analytics comes with two starter pack rules so analysts can become familiar with how rules look before you create your own rules. Use the starter pack rules to become familiar with the Rule Builder and to practice editing and deploying a rule.

Starter pack rules are installed in the Rule Library, which will contain every rule you download or create. The following figure shows the Rule Library after installation.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Alerts', 'Summary', and 'Configure'. The main content area is titled 'Rule Library' and contains a table of rules. The table has columns for 'Rule Name', 'Description', 'Trial Rule', 'Type', and 'Actions'. Two rules are listed:

Rule Name	Description	Trial Rule	Type	Actions
SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Monitors for non-SMTP traffic on TCP destination port 25 co...	Yes	Rule Builder	[Settings]
SAMPLE - P2P Software as Detected by an Intrusion Detection Device	P2P software as detected by an intrusion detection device (L...	Yes	Rule Builder	[Settings]

The interface also shows a sidebar with 'Rules', 'Services', and 'Settings' tabs, and a footer with user information (admin), language (English (United States)), and time (GMT+00:00).

These are the available starter pack rules:

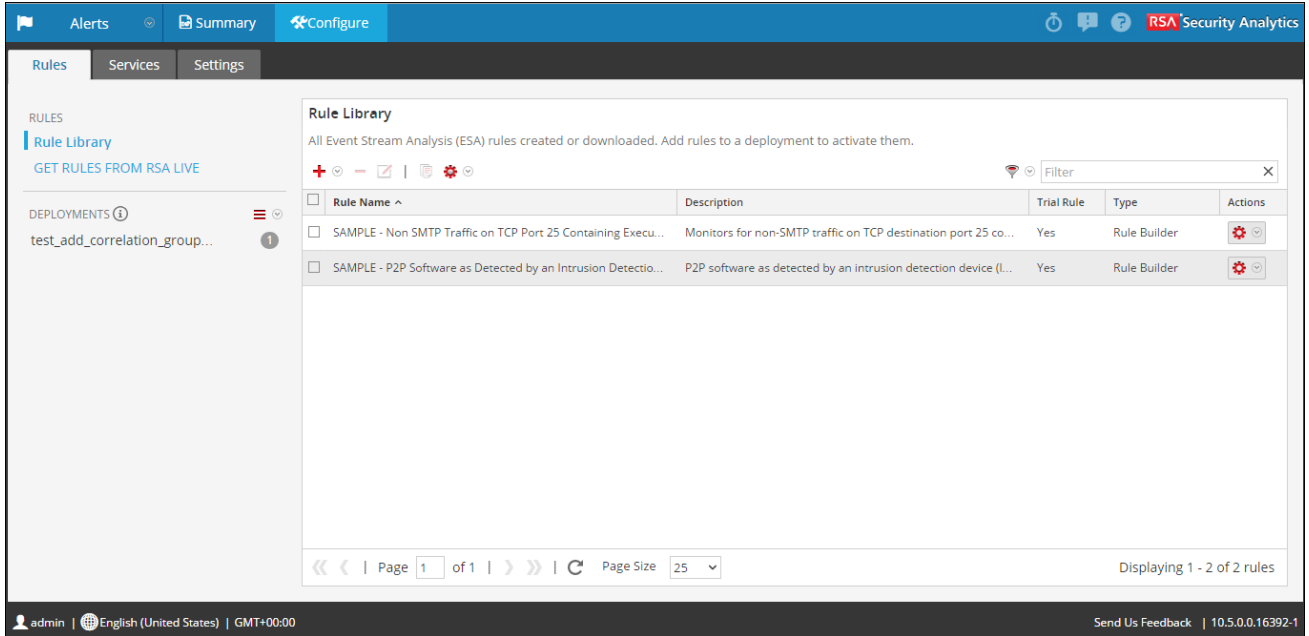
- SAMPLE: P2P Software as Detected by an Intrusion Detection Device
- SAMPLE: Non SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: Whitelist - From outside of Germany, P2P Software as Detected by an Intrusion Detection Device.
- SAMPLE: Blacklist - From inside countries that are not the US, Non-SMTP Traffic on TCP Port 25 Containing Executable
- SAMPLE: User Added to Admin Group Same User su Sudo

Each name begins with SAMPLE to distinguish the rules that are installed with Security Analytics from the rules you download and create.


Rule Library

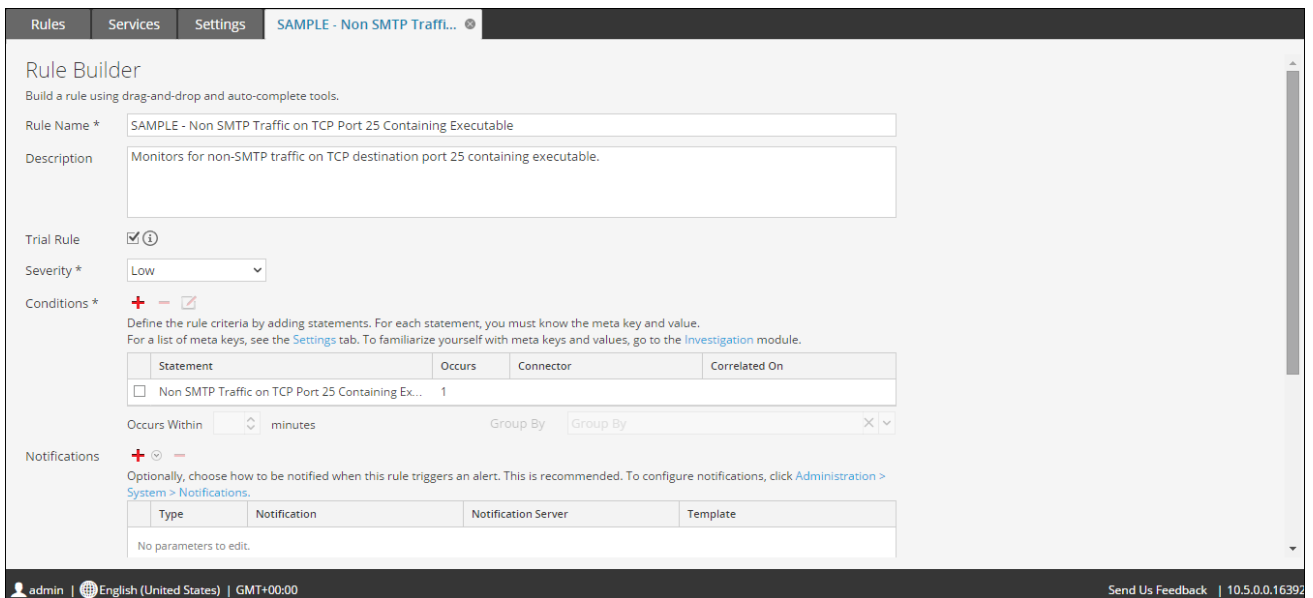
The Rule Library shows the following information for a rule:

- **Name** summarizes the data or events the rule collects.
- **Description** explains the rule in more detail, although only the beginning shows in the Rule Library.
- **Trial Rule** indicates if trial mode is enabled or disabled for the rule.
- **Type** shows the origin of the rule, built in Rule Builder or Advanced EPL or downloaded from RSA Live.



Procedure

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Configure view is displayed with the Rules tab open.
2. In the **Rule Library**, select a sample rule and click , or double-click a rule.
The rule is opened in Rule Builder.



3. To practice with a starter pack rule, refer to the following topics for detailed descriptions and procedures:
 - To familiarize yourself with the Rule Builder user interface, see [Rule Builder Tab](#) for a description of each field.
 - To learn how to edit a rule, see [Add a Rule Builder Rule](#) for a step-by-step procedure.
 - To deploy a starter pack rule, see [Deploy Rules to Run on ESA](#) to learn how to associate the rule with an ESA service.

After you practice with starter pack rules, you will be able to download, create and deploy your own rules.

Work with Trial Rules

When rules use too much memory, your ESA service can become slow or unresponsive. To ensure rules do not use excessive memory, you can enable trial rules for any type of rule. By default, new rules you create and RSA Live rules you import are configured to be trial rules. RSA recommends you disable the trial rule setting only after testing the new rule in your environment during normal and peak network traffic. When you create a trial rule, you set a global threshold of the percentage of memory that rules may use. If that configured memory threshold is exceeded, all trial rules are disabled.

The Security Analytics Event Stream Analysis (ESA) service is capable of processing large volumes of disparate event data from Concentrators. However, when working with Event Stream Analysis, it is possible to create rules that use excessive memory. This can slow your ESA service or even cause it to shut down unexpectedly. To ensure that this doesn't happen, you can configure your rule as a trial rule. When you configure a trial rule, you also set global threshold of the percentage of memory that rules may use. If that configured memory threshold is exceeded, all trial rules are disabled automatically.

For suggestions on creating more efficient rules, see "Best Practices for Writing Rules" in [Best Practices](#)

By default, new rules and RSA Live rules are configured as trial rules. As a best practice, when you edit an existing rule, select the Trial Rule option, which allows you to:

- Deploy the rule with an added safeguard.
- Optionally, view a snapshot of memory utilization to understand if the rule creates memory issues.
- Know if you must modify the rule criteria to improve performance.

Note: Run a rule as a trial rule long enough to assess the performance during normal and peak network traffic.

Deploy Rules as Trial Rules

This topic explains to administrators how to enable trial rules when creating new rules or editing rules. Trial rules are automatically disabled if a specified total JVM memory utilization threshold is exceeded.

Procedure

To deploy rules as trial rules:

1. In the **Security Analytics** menu, go to **Alerts > Configure**.
The Configure view is displayed with the Rules tab open.
2. From the Rule Library, choose to add or edit a rule. The rule builder is displayed in a new Security Analytics tab.

Rule Builder

Build a rule using drag-and-drop and auto-complete tools.

Rule Name *

Description

Trial Rule

Severity * *

Conditions * Investigation

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> 5 Failed Logons	5	followed by	
<input type="checkbox"/> Successful Logon	1		

Occurs Within minutes Group By

Notifications Global Notifications

Output	Notification	Notification Server	Template
No parameters to edit.			

Output Suppression of every minutes

Enrichments Settings

Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
No parameters to edit.			

Debug

* = required field

admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.17881-1

3. To make a new or existing rule a trial rule, select **Trial Rule** .
4. Add the rule conditions or modify the rule as needed. For instructions on editing rules, see [Add Rules to the Rule Library](#).
5. Click **Save**.
6. Ensure that trial rules are enabled for your ESA and that you are satisfied with the thresholds configured for trial rules.
The memory threshold is set in the configuration file. To configure it, see "Change Memory Threshold for Trial Rules" in the **ESA Configuration Guide**.

The threshold is configured per ESA and is a percentage of Java Virtual Memory.

The configuration parameter, `MemoryThresholdforTrialRules` default is 85.

7. Optionally, you can set up the policies in Health and Wellness to send you an email notification if the total JVM memory utilization threshold is exceeded.

The next time you deploy the rule, it runs in trial rule mode.

Note: If a trial rule is disabled, you will need to go to the **Alerts > Configure > Services** tab to re-enable the trial rules. For more instructions on re-enabling trial rules on a service, see [View ESA Stats and Alerts](#).

View Memory Metrics for Rules Using Trial Mode

This topic tells ESA rule writers how to view memory metrics when the memory threshold configured for trial rules is exceeded. If the memory threshold is exceeded, you can configure a snapshot to be taken of the memory usage for ESA rules at the time that trial rules are disabled, allowing you to investigate memory usage and edit the rules to be more efficient.

When you configure trial rules and enable the Memory Snapshot feature, if the memory threshold is exceeded, all trial rules are disabled and a snapshot of the memory usage for all ESA rules is taken at the time of disablement. This allows you to see how much memory was used so that you can modify your ESA rules to be more efficient. The memory snapshot can be viewed in the Health & Wellness System Stats browser, so you will need permissions to access this module. Once you view the details in the System Stats browser, you can modify the trial rule syntax and re-enable the trial rules.

At a high level, you will need to complete the following steps to use the Memory Snapshot to troubleshoot memory usage for rules:

1. Enable trial rules for any new rules you deploy. See [Deploy Rules as Trial Rules](#).
2. Ensure that you have configured Health & Wellness ESA policies to send an email if memory thresholds are exceeded.
3. Ensure you have the correct permissions to view the Health & Wellness module. For information on roles and permissions, see [Role Permissions](#).
4. Ensure that the Memory Snapshot feature is enabled (via the `EnabledCaptureSnapshot` parameter via SA Explorer). The Memory Snapshot feature is disabled by default. See "Enabling and Disabling the Memory Snapshot Feature" below. RSA recommends you disable the feature once you have completed testing new rules.

5. View the memory threshold statistics in Health & Wellness if the memory threshold is triggered for trial rules.
6. Modify the rule or rules that triggered the alarm. For best practices for rule writing, see [Best Practices](#).
7. Re-enable the trial rules that were disabled when the memory threshold was triggered. For instructions on re-enabling trial rules on a service, see [View ESA Stats and Alerts](#).
8. Continue to test the trial rules.

Note: Like any Debug tool, there can be exceptional overhead associated with using the Memory Snapshot feature. When actively taking a snapshot, the Memory Snapshot feature can add delays to your ESA services. The ESA service stops generating alerts while taking a snapshot. RSA recommends you disable the feature once you have completed testing new rules. If you disable the Memory Snapshot feature, trial rules will still be disabled when memory usage exceeds configured thresholds, but the memory snapshot will not be taken, and the statistics will not appear in the Health & Wellness System Stats browser.

Prerequisites

These are the requirements for viewing memory metrics:

- One or more ESA rules must be configured as a trial rule.
- Memory Snapshot must be enabled (via the EnabledCaptureSnapshot parameter via SA Explorer).
- The user must have the appropriate permissions to view Health & Wellness statistics.
- The user must have configured the ESA Health & Wellness policy to send an email when memory thresholds are exceeded.

Procedures

View Memory Metrics

1. In the **Security Analytics** menu, go to **Administration > Health & Wellness > System Stats Browser**.
2. For component, select **Event Stream Analysis**. For category, enter **ESA-Metrics**.

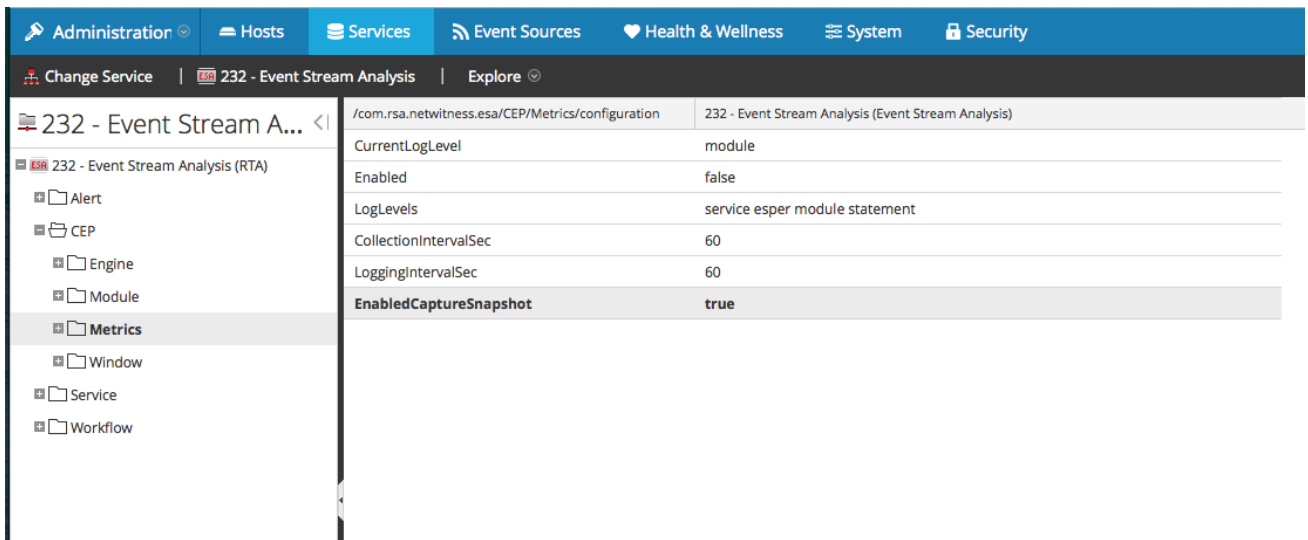
Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

The name of the rule is displayed in the **Subitem** field, and the memory usage is displayed in the **Value** column.

Note: The **Last Update** field reflects when Health & Wellness polls ESA. However, the Memory Snapshot only occurs when memory thresholds are exceeded, so this field does not reflect when the snapshot was taken or updated. The snapshot remains static until the memory threshold is exceeded again. For example, if the memory threshold is exceeded on 10/10/15 at 12 p.m., but Health & Wellness polls at 10/10/15 at 3 p.m., the **Last Update** field will display a date of 10/10/15 3 p.m.

Enable or Disable the Memory Snapshot Feature

1. In the **Security Analytics** menu, go to **Administration > Services** and select your ESA.
2. Once you've selected your ESA, click on **Actions > View > Explore**, and navigate to CEP Metrics as shown below.



3. Change the field `EnabledCaptureSnapshot` to **true** or **false** depending on whether you want to enable or disable the Memory Snapshot feature.

Add Rules to the Rule Library

This topic explains how to add each type of rule to the rule library. You must add a rule to the Rule Library before you can deploy it. Permission to manage rules is required for all tasks in this section. To add rules, you can download them from ESA Live, create a rule via the Rule Builder, or write advanced EPL rules.

For more details on each of these procedures, see:

- [Download Configurable RSA Live ESA Rules](#)
- [Add a Rule Builder Rule](#)
- [Add an Advanced EPL Rule](#)

In addition to deploying a rule, you can edit, duplicate, import, export, and remove a rule in the Rule Library. For details on these procedures, see [Working with Rules](#)

Download Configurable RSA Live ESA Rules

This topic explains how to download configurable rules from the Security Analytics Live Content Management System so you can customize them to meet your needs.

RSA Live contains a catalog of rules. Each rule has configurable parameters so you can customize the rule for your environment. If RSA Live has a rule to detect events that you want to detect in your network, download the rule to save time. You can edit the configurable parameters and save the rule in your Rule Library.

This is a sample of how each RSA Live ESA rule is described on RSA Live:

Rule Name	Description
Logins across Multiple Servers	<p>Detects logins from the same user across 3 or more separate servers within 5 minutes.</p> <p>The time window and number of unique destinations are configurable.</p>

As the name shows, the rule looks for logins across multiple servers. The description explains the rule criteria in more detail and specifies which parameters you modify.

Note: When a rule description includes a configurable parameter, the default setting for the parameter is used. In the sample rule, the description states 5 minutes. However, the time window is configurable so 5 is the default number of minutes.

Prerequisites

These are the prerequisites for downloading configurable RSA Live ESA rules;

- Have permission to manage rules
- Create a Live Account. See the **Live Services Management Guide** for details.
- Set up Live on Security Analytics. See the **Live Services Management Guide** for details.

Procedure

To download configurable RSA Live ESA rules:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed.
2. In the options panel, click **Get Rules from RSA Live**.
The Search tab is displayed.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Live', 'Search', 'Configure', and 'Feeds'. The 'Search' tab is active. The interface is divided into two main sections: 'Search Criteria' on the left and 'Matching Resources' on the right.

Search Criteria:

- Keywords: logins
- Resource Types: RSA Event Stream Analysis Rule
- Tags: (empty)
- Required Meta Keys: (empty)
- Generated Meta Values: (empty)
- Resource Created Date: Start Date and End Date (calendar icons)
- Resource Modified Date: Start Date and End Date (calendar icons)
- Buttons: Search, Cancel

Matching Resources:

Buttons: Show Results, Details, Deploy, Subscribe, Package

Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	Multiple Successful Logins from Mu...	2013-12-24 11:25 AM	2015-03-20 4:45 PM	RSA Event Stream...	Alert when log events contain multiple successfu
<input type="checkbox"/>	Multiple Failed logins Followed By S...	2013-12-24 11:20 AM	2015-02-14 8:20 AM	RSA Event Stream...	Multiple failed logins followed by a successful lo
<input type="checkbox"/>	Multiple Failed Logins from Multipl...	2013-12-24 11:26 AM	2015-03-20 4:45 PM	RSA Event Stream...	Alert when log events contain multiple failed logi
<input type="checkbox"/>	Multiple Failed Logins to Single Hos...	2014-02-27 11:23 AM	2015-03-20 4:45 PM	RSA Event Stream...	Alert when log events contain multiple failed logi
<input type="checkbox"/>	Logins across multiple servers	2014-10-16 5:39 PM	2014-10-16 5:39 PM	RSA Event Stream...	Detects logins from the same user across 3 or m
<input type="checkbox"/>	Multiple Failed Logins from Multipl...	2013-12-24 11:25 AM	2015-03-20 4:45 PM	RSA Event Stream...	Alert when log events contain multiple failed logi
<input type="checkbox"/>	Multiple Successful Logins from Mu...	2013-12-24 11:26 AM	2015-03-20 4:46 PM	RSA Event Stream...	Alert when log events contain multiple successfu
<input type="checkbox"/>	Multiple Failed logins Followed By S...	2013-12-24 11:21 AM	2013-12-24 11:22 AM	RSA Event Stream...	Five or more failed logins for a user followed by .
<input type="checkbox"/>	Multiple failed logins from same us...	2014-09-17 4:38 PM	2014-09-17 4:38 PM	RSA Event Stream...	Multiple failed logins from same user originating
<input type="checkbox"/>	Logins by same user to multiple ser...	2015-01-20 3:17 PM	2015-01-20 3:17 PM	RSA Event Stream...	Identifies a user that attempts to log in to multip
<input type="checkbox"/>	Consecutive Login without Logout	2014-10-16 5:39 PM	2015-02-14 8:25 AM	RSA Event Stream...	Detects consecutive logins by the same user to t
<input type="checkbox"/>	User Added to Admin Group Same ...	2013-12-24 11:24 AM	2015-03-20 4:44 PM	RSA Event Stream...	Alert when user is upgraded to one of admin gro
<input type="checkbox"/>	Attempted Identity abuse via exces...	2014-09-17 4:38 PM	2014-09-17 4:38 PM	RSA Event Stream...	Identity abuse is detected by multiple failed logi
<input type="checkbox"/>	Multiple Login Failures from Same ...	2014-03-14 10:44 AM	2014-03-14 10:44 AM	RSA Event Stream...	Detects when log events that contain multiple fa
<input type="checkbox"/>	Multiple login failures from same s...	2013-12-24 11:25 AM	2013-12-24 11:25 AM	RSA Event Stream...	Alert when log events contain multiple login failu

15 Matching Resources

Footer: admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.5.0.0.16457-1

3. In **Search Criteria**, for **Resource Type** select **RSA Event Stream Analysis Rule**.
4. Specify any of the following criteria to find a rule to configure for your environment.
For a detailed description of the search criteria, see "The Live Search View" in the **Live Services Management Guide**.

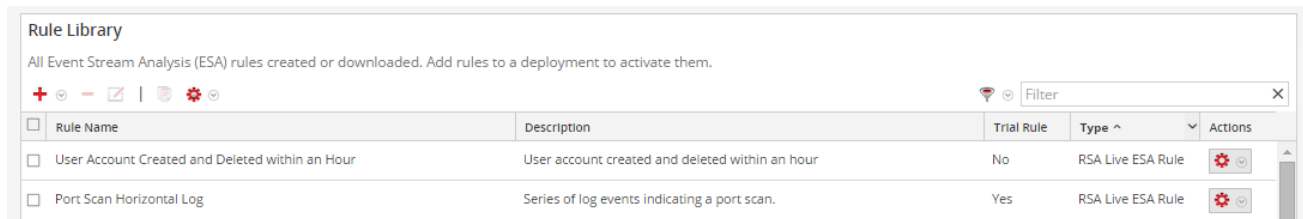
- a. Keywords
 - b. Tags
 - c. Required Meta Keys
 - d. Generated Meta Values
 - e. Resource Created Date
 - f. Resource Modified Date
5. Click **Search**. Rules that match the search criteria are displayed in Matching Resources.
 6. Select each rule to download and click **Deploy**.
The Deployment Wizard is displayed
 7. Follow the steps in the wizard. If you need more information, see "Deploy Resources in Live" in the **Live Services Management Guide**.

When you finish the steps in the wizard, the selected rules are displayed in the Rule Library.

Customize an RSA Live ESA Rule

This topic explains how to configure parameters in an RSA Live ESA rule. When you download an RSA Live ESA rule, the rule appears in the Rule Library which includes the following columns:

- Name
- Description
- Trial Rule
- Type



The screenshot shows the 'Rule Library' interface. At the top, it says 'All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.' Below this is a toolbar with icons for adding, deleting, and refreshing rules, and a search filter box. The main part of the interface is a table with the following columns: Rule Name, Description, Trial Rule, Type, and Actions. Two rules are listed:

Rule Name	Description	Trial Rule	Type	Actions
<input type="checkbox"/> User Account Created and Deleted within an Hour	User account created and deleted within an hour	No	RSA Live ESA Rule	
<input type="checkbox"/> Port.Scan Horizontal Log	Series of log events indicating a port scan.	Yes	RSA Live ESA Rule	


The type is RSA Live ESA Rule.

Prerequisites

- Administrator, Operator, SOC Manager or DPO role permissions are required.
- Rules must be downloaded to the Rule Library.

Procedure

To customize an RSA Live ESA rule:

1. In the **Security Analytics** menu, select **Alerts > Configure > Rule**.
2. In the **Rule Library**, select an RSA Live ESA Rule and click .

The RSA Live ESA Rule tab is displayed.
3. (Optional) Change the following fields:
 - Rule Name
 - Description
 - Trial Rule (Enabled by default. RSA recommends you run a rule as a trial rule long enough to assess the performance during normal and peak network traffic.)
 - Severity
4. To configure the rule for your environment, in the **Parameters** section replace the default in the **Value** Column.

Parameters	Name ^	Value
	With this number of events	200
	Within this number of seconds	60

5. Click **Save**

Add a Rule Builder Rule

This topic introduces a set of end-to-end procedures for adding a Rule Builder type rule.

Each ESA rule is designed to detect something in your network and to generate an alert for it:

- User activity that is not allowed, such as attempting to download software that is not sanctioned
- Suspicious behavior, such as mass audit clearing
- Known malicious threats, such as worm propagation or a password-cracking tool

There are two methods to design a rule in ESA:

- Rule Builder is an easy-to-use interface. You provide a meta key and value, then select choices from lists to complete the criteria.

- Advanced EPL allows you to write queries in the Event Processing Language. You must know EPL syntax.

If you know EPL, you can use either method. If you do not know EPL, you must use Rule Builder. These topics explain the Rule Builder.

Step 1. Name and Describe the Rule



This topic provides instructions to identify a rule, indicate if it is a trial rule and assign a severity level. When you add a new rule, the first information to provide is a unique name and description of what the rule detects. After you save the rule, this information is displayed in the Rule Library.

Prerequisites

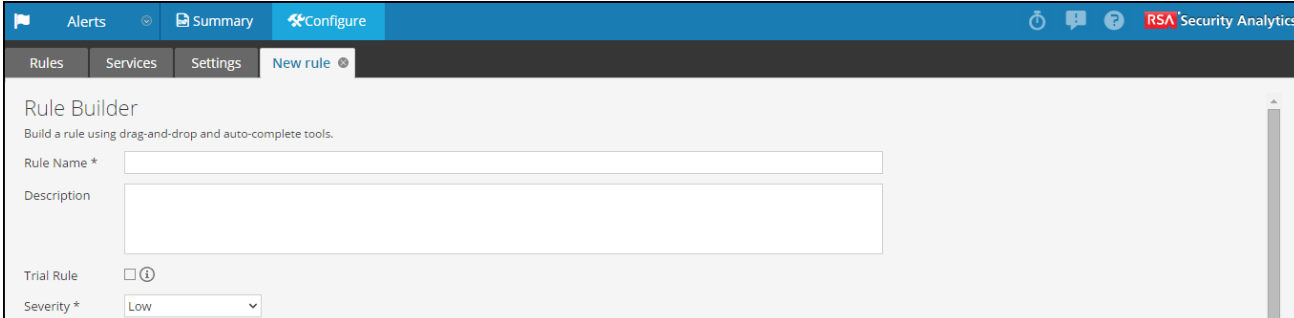
You must have permission to manage rules. See [Role Permissions](#).

Procedure

To name and describe a rule:

1. In the **Security Analytics** menu, select **Alerts > Configure > Rule**
2. In the **Rule Library**, select   > **Rule Builder**.

The New Rule tab is displayed.



3. Type a unique, descriptive name in the **Rule Name** field.
This name will appear in the Rule Library so be specific enough to distinguish the rule from others.
4. In the **Description** field, explain which events the rule detects.
The beginning of this description will appear in the Rule Library
5. By default, new rules are configured as a Trial Rule. A trial rule automatically disables the rule if all trial rules collectively exceed the memory threshold. If you are editing an existing rule, you can select **Trial Rule** to safely test the rule edits.

Use trial rule mode as a safeguard to see if a rule runs efficiently and to prevent downtime caused by running out of memory. For more information, see [Work with Trial Rules](#).

- For **Severity**, classify the rule as Low, Medium, High or Critical.

Step 2. Build a Rule Statement

This topic provides instructions to define rule criteria in Rule Builder by adding statements. A statement is a logical grouping of rule criteria in the Rule Builder. You add statements to define what a rule detects.

Example

The following graphic shows an example of a Rule Builder statement.

Every statement contains a key and value. Then, you build logic around the pair by selecting an option in each other field.

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met

Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/> event.medium	is	32	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> event.device_class	is	IDS, Firewall, IPS, Intrusion, Vuln...	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Prerequisites

To build a rule statement, you must know the meta key and the meta value.



For a complete list of meta keys, go to **Alerts > Configure > Settings > Meta Key References**.

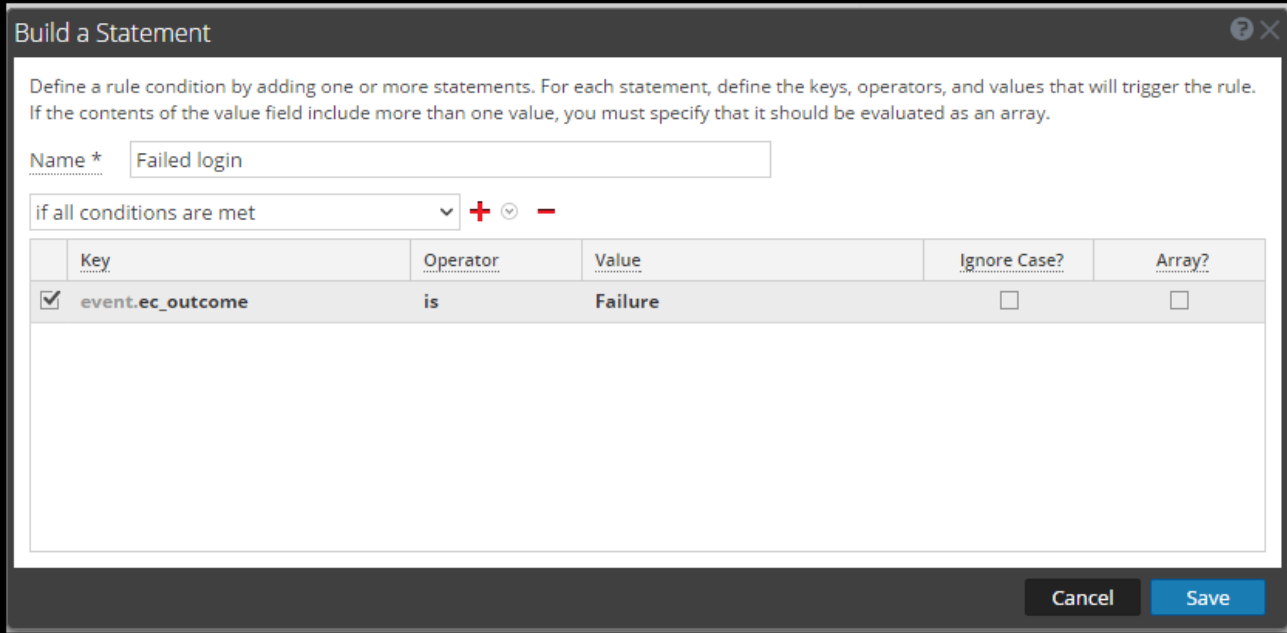
Procedure

To build a rule statement:

- In the **Security Analytics** menu, select **Alerts > Configure**.

The Rules tab is displayed by default.



2. In the **Rule Library**, click  > **Rule Builder** or edit an existing Rule Builder rule.
The Rule Builder view is displayed.
3. In the **Conditions** section, click  .
The Build Statement dialog is displayed.



Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met  

	Key	Operator	Value	Ignore Case?	Array?
<input checked="" type="checkbox"/>	event.ec_outcome	is	Failure	<input type="checkbox"/>	<input type="checkbox"/>

4. **Name** the statement. Be clear and specific. The statement name will appear in the Rule Builder.
5. From the drop-down list, select which circumstances the rule requires:
 - if **all conditions** are met
 - if **one of these conditions** are met
6. Specify the criteria for the statement:
 - a. For **Key**, type the name of the **Meta Key**.
 - b. For **Operator** specify the relationship between the meta key and the value you will provide for it.
The choices are: is, is not, is not null, is greater than (>), is greater than or equal to (>=), is less than (<), is less than or equal to (<=), contains, not contains, begins with, ends with
 - c. Type the **Value** for the meta key.
Do not add quotes around a value. Separate multiple values with a comma.

- d. The **Ignore Case?** field is designed for use with string and string array values. By choosing the **Ignore Case** field, the query will treat all string text as a lowercase value. This ensures that a rule that searches for the user named Johnson would trigger if the event contains "johnson," "JOHNSON," or "JoHnSoN."
- e. The **Array?**field indicates if the contents of the Value field represent one or more than one value.

Select the Array checkbox if you entered multiple, comma-separated values in the **Value** field. For example, "ec_activity is Logon, Logoff" requires you to select the Array checkbox.

7. To use another meta key in the statement, click **+**, select **Add Meta Condition** and repeat step 6.
8. To add a whitelist, click **+** and select **Add Whitelist Condition**.
9. To add a blacklist, click **+** and select **Add a Blacklist Condition**.
10. To save the statement, click **Save**.

To Add a Whitelist

You use a whitelist to ensure that specified events are excluded from triggering the rule. Whitelists can be based on geographic location or by customer-defined enrichment CSV sources. For example, if you want to create a rule that only triggers for IP addresses outside of the US, you can create a whitelist of US IP addresses.

1. After you add a meta condition, click **+** and select **Add Whitelist Condition**.
2. In the **EnterWhitelist Name** field, select an enrichment source. Any enrichment source loaded from a CSV or a named window in Esper can be used as source for a whitelist.
3. If you used a GeoIP source for the whitelist, ipv4 is automatically entered for the subcondition. Enter the meta value for the corresponding value field. For example, enter *ipv4 is ip_src* to ensure the GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database. In addition, if you used a GeoIP source for the whitelist, you might want to add a subcondition to specify the geographic region to exclude from the rule results. For example, to specify that the country code must be USA, enter "*CountryCode is US*".

To Add a Blacklist

You use a blacklist to ensure that specified events trigger the rule. Blacklists can be based on geographic location or by customer-defined enrichment CSV sources. For example, you can specify that the rule only includes results from Germany.

1. After you add a meta condition, click **+** and select **Add Blacklist Condition**.
2. In the **Enter Blacklist Name** field, select an enrichment source. Any enrichment source loaded from a CSV or a named window in Esper can be used as source for a blacklist.
3. If you used a GeoIP source for the blacklist, ipv4 is automatically entered for the subcondition. Enter the meta value for the corresponding value field. For example, enter ipv4 is ip_src to ensure the GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database. In addition, if you used a GeoIP source for the blacklist, you might want to add a subcondition to specify the geographic region to include in the rule results. For example, to specify that the rule only includes results for Germany, enter "*CountryCode is DE*".

Example: Blacklist

The following statement shows a blacklist statement for a rule that monitors for non-SMTP traffic on TCP destination port 25 containing an executable from countries that are outside of the United States.

Build a Statement ? X

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

+ **⊖** **-**

<input type="checkbox"/>	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.service	is not	25	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.tcp_dstport	is	25	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.extension	is	exe,com,vb,vbs,vbe,cmd,bat,ws,ws...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	blacklist.GeoIpLookup				
<input type="checkbox"/>	ipv4	is	event.ip_src	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	countryCode	is not	US	<input type="checkbox"/>	<input type="checkbox"/>

Blacklist conditions can be added to include only those items defined in an enrichment list. Map a list column to an event meta key to join the list to the incoming data stream.

Statement	Description
service is not 25	The traffic is not SMTP traffic.
tcp_dstport is 25	The traffic is running on TCP port 25.
extension is exe, com,vb,vb-s,vbe,cmd,bat,ws,wsf,src,sh	The file extension is an executable.
GeoIpLookup	The blacklist is based on a GeoIPLookup source.
ipv4 is ip_src	The GeoIP records are selected based upon the ip_src being found in the GeoIP lookup database.
countryCode is not US	When looking up the IP address Event.ip_src in the GeoIP database, the record it returns does not contain "US" in the countryCode field.

Example: Ignoring Case, Strict Pattern Matching, and Using The *Is Not Null* Operator

The following example uses the ability to ignore case, exclude null values, and create a strict pattern match to ensure that it returns the expected rule results. The following conditions make up the rule:

Trial Rule

Severity * Low

Conditions * + - ✎ Investigation

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input type="checkbox"/> Failure	5	followed by			
<input checked="" type="checkbox"/> Success	1	AND			
<input type="checkbox"/> Modify Password	1				

Group By device_class user_dst

Occurs Within 5 minutes Event Sequence Strict Loose

Rule Condition	Description
Failures	This condition searches for five failed logins with a "followed by" connector, meaning that the condition (Failures) must be followed by the next condition (Success).
Success	This condition searches for one successful login.
ModifyPassword	This condition searches for an instance where the password is modified.
GroupBy: user_dst, device class	The GroupBy field ensures that all the previous conditions are grouped by the user_dst meta (the user destination account) and device class. This is important to the construction of the rule because the rule attempts to find a case where a user has attempted to log into the same destination account multiple times, finally logged in successfully, and then changed the password. Grouping by device class ensures that the user logged in from the same machine attempted to log into an account multiple times. The rule may give unexpected results if you do not group the results.
Occurs within 5 minutes	The time window for the events to occur is five minutes. If the events occur outside of this time window, the rule does not trigger.
Event Sequence: Strict	<p>The event sequence is configured for a strict pattern match. This means that the pattern must match exactly as it is specified with no intervening events.</p> <p>Strict pattern matching allows you to ensure that the Esper engine only generates alerts for rules that exactly match the pattern you want to find. For example, a common rule might be to search for five failed logins followed by a successful login. If you select a loose pattern match, this rule will trigger if there are any number of successful logins between the failed logins. Since the point of the rule is to find frequent <i>and</i> sequential login attempts, a strict match is required to ensure that you get the results you expect.</p>

Note: Each of these conditions is explained in further detail in the sections below.

For each condition, a statement is built in the Rule Builder. The following statement makes up the Failures condition:

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name * Failures

if all conditions are met

Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/> event.ec_activity	is	Logon	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.ec_outcome	is	Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Rule Statement	Description
ec-activity is Logon (ignore case)	Identifies activity that attempts to log on to a system. The Ignore Case field is designed for use with string and string array values. By choosing the Ignore Case field, the query will treat all string text as a lowercase value. You may want to use this field if you are unsure what case may be used when logging a particular event. Because the case is ignored, the rule can trigger if the activity is logged as Logon, logon, or LoGoN.
ec_outcome is Failure (ignore case)	Identifies activity outcome logged as "failure." Because the case is ignored, the rule can trigger if the activity is logged as "failure", "Failure," or "FaiLuRe."
user_dst is not null	Ensures that the condition is only true if user_dst is populated. The is not null operator allows you to ensure that a field returns a value. You may want to use this field when a rule depends on a particular field returning a value. For example, you want to create a rule that identifies the same user attempting to log into the same destination account multiple times (potentially a password-guessing attack). If the field that represents the user destination account is empty, you don't want the rule to trigger. To ensure the field contains a value, you use the is not null operator.

The following statement makes up the Success condition:

Build a Statement ? ✕

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met + -

	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.ec_activity	is	Logon	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.ec_outcome	is	Success	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>

Rule Statement	Description
ec_activity is Logon	Identifies logon activity.
ec_outcome is Success	Identifies a logon that is successful.
user_dst is not null	Ensures that user destination account field must be populated for the condition to be true.

The following statement makes up the ModifyPassword condition:

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met + -

Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/> event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.ec_subject	is	Password	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.ec_activity	is	Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Rule Statement	Description
user_dst is not null	Ensures the user destination account field must be populated for the condition to be true.
ec_subject is Password	Identifies a subject of Password.
ec_activity is Modify	Identifies activity where the password was modified.

Example Results

When the alert fires for the example rule, you can see that the rule triggered for seven events, and that each event contains a user. You can also see that the events follow a strict pattern: five failed login events, followed by a successful login event, followed by a modification to the account.

5Fails1Success1Config change - Strict Pattern

Description: 5 failures followed by 1 success and 1 config change
Strict Match Recognise

Time: 2015-11-18T21:05:59

Severity: Medium

Of Events: 7

Event Meta | Events

	Date	Source	Destination	Username	Alias Host
+	2015-11-18T21:05:34			AAA	09:50:11,
+	2015-11-18T21:05:34			AAA	09:50:12,
+	2015-11-18T21:05:34			AAA	09:50:11,
+	2015-11-18T21:05:34			AAA	09:50:10,
+	2015-11-18T21:05:34			AAA	09:50:10,
+	2015-11-18T21:05:46			AAA	09:50:16,
+	2015-11-18T21:05:55			AAA	09:50:16

Drilling down into the Investigation module by clicking on the source for one of the events, you can see the case for each of the string values. Because you used **Ignore Case**, the rule would trigger if the string values were upper or lower case.

Event Reconstruction

service	id	type	service type	service class	event source	event type	event time
	3213375	Log	winevent_snare	Windows Hosts	Security	Failure Audit	2007-11-16 09:50:08.000

View Meta | View Log | Export Logs

- event.type = "Failure Audit"
- event.computer = "RET7W001"
- category = "Logon/Logoff"
- event.desc = "Logon"
- user.dst = "AAA"
- logon.type = "10"
- process = "User32"
- alias.host = "LNOHPOLBYKDP71"
- ip.src = 10.129.66.126
- parse.error = "Convert Fail: ip.srcport: 0,6325212"
- ec.theme = "Authentication"
- ec.subject = "User"
- ec.activity = "Logon"
- ec.outcome = "Failure"

Example: Grouping the Rule Results

The **Group By** field allows you to group and filter rule results. For example, suppose that there are three user accounts; Joe, Jane, and John and you use the **Group By** meta, `user_dst`. The result will show events grouped under the accounts for Joe, Jane, and John.

You can also group by multiple keys, which can further filter rule results. For example, you might want to group by user destination account and machine to see if a user logged into the same destination account from the same machine attempts to log into an account multiple times. To do this, you might group by `device_class` and `user_dst`.

The following example shows a rule grouped by `device_class` and `user_dst`.

Rule Builder

Build a rule using drag-and-drop and auto-complete tools.

Rule Name *

Description

Trial Rule

Severity *

Conditions * Investigation

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Failed Logins	5	followed by	
<input type="checkbox"/> Successful Login	1		

Group By

Occurs Within minutes Event Sequence Strict Loose

Rule Condition	Description
Failed Logins	Identifies five failed login attempts (must be followed by the next condition; i.e., the five failed logins must be followed by a successful login).
Successful Login	Identifies one successful login.

Rule Condition	Description
Group By: user_dst and device_class	Groups the rule results by user_dst (user destination account) and device_class (type of machine the user is logging in from). This allows the rule to look for a user logged in from the same machine to the same destination account, resulting in a much more targeted rule result.
Occurs within 5 minutes with a strict pattern match	The events must occur within five minutes, and the pattern matching is strict, meaning it must follow the pattern exactly for the rule to trigger.

Example: Working with Numeric Operators

Numeric operators allow you to write rules against numeric values, such as specifying that a value is greater than, less than, or equal to a specific value. This is useful particularly for cases where you might want to specify a numeric threshold, i.e., *payload is greater than 7000*.

The following example attempts to identify a data transfer to a particular destination through the common ports where the transfer size is high and the payload is in a suspicious range.

Build a Statement ?

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met + -

	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.ip_dst	is	10.10.10.1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.ip_dstport	is less than or equal	1024	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.size	is greater than or equal	10000	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.payload	is greater than	7000	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.payload	is less than	8000	<input type="checkbox"/>	<input type="checkbox"/>

Rule Statement	Description
ip_dst is 10.10.10.1	The destination port is 10.10.10.1.
ip_dstport is greater than or equal to 1024	The destination port is in a commonly used port range, 1024 or greater.
size is greater than or equal to 10000	The size of the transfer is 10000 or greater, which is a suspiciously large transfer.
payload is greater than 7000	The payload is between 7000 and 8000, which is a suspiciously large payload.
payload is less than 8000	The payload is between 7000 and 8000, which is a suspiciously large payload.

Step 3. Add Conditions to a Rule Statement

This topic provides instructions to add conditions, such as specifying a certain time frame, to a rule statement. When you build a statement, you specify what a rule detects. You add conditions to make further stipulations, such as how many times or when the criteria must occur.

Example

The following graphic shows an example of the conditions for Rule Builder statements. Combined, the statements and conditions comprise the rule criteria.

The screenshot shows the configuration for a rule named "Trial Rule". The severity is set to "Low". The rule is configured with the following conditions:

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input type="checkbox"/> Failure	5	followed by			
<input checked="" type="checkbox"/> Success	1	AND			
<input type="checkbox"/> Modify Password	1				


Additional settings include "Group By" set to "device_class" and "user_dst", and "Occurs Within" set to "5 minutes" with "Event Sequence" selected and "Strict" correlation type chosen.

This rule detects 5 failed logon attempts followed by one successful logon, which could be the sign that someone has hacked into user account. This is the criteria for the rule:

- A. 5 failed logons are required.
- B. 1 successful logon must follow the failures
- C. A password was changed.
- D. All events must occur within 5 minutes.
- E. Group alerts by user (user_dst), because steps A and B must be performed on the same user destination account. Also, group by machine (device_class) to ensure that the user logged in from the same machine attempts to log into an account multiple times.
- F. The match is a strict pattern, meaning that the pattern must match exactly with no intervening events.

Procedure

To add conditions to a rule statement:

1. In the **Conditions** section, select a statement and click .
2. For **Occurs**, enter a value to specify how many occurrences are required to meet the rule criteria.
3. If you have multiple statements, in the **Connector** field select a logical operator to join one statement to another:
 - followed by
 - not followed by
 - AND
 - OR
4. **Correlation Type** applies only to **followed by** and **not followed by**. If you choose a correlation type of SAME, select one meta to correlate on, and if you choose a correlation type of JOIN, select two meta to correlate on. You may want to use JOIN if you are trying to correlate on meta from two different data sources. For example, say you want to correlate an AV alert with an IDS alert. See the examples below for a use case where two meta from different sources are joined.
5. If events must happen within a specific timeframe, enter a number of minutes in the **Occurs Within** field.
6. Choose whether the pattern must follow a **Strict** match or a **Loose** match. If you specify a strict match, this means that the pattern must occur in the exact sequence you specified with no additional events occurring in between. For example, if the sequence specifies five failed logins (F) followed by a successful login (S), this pattern will only match if the user executes

the following sequence: F,F,F,F,F,S. If you specify a loose match, this means that other events may occur within the sequence, but the rule will still trigger if all of the specified events also occur. For example, five failed login attempts (F), followed by any number of intervening successful login attempts (S), followed by a successful login attempt might create the following pattern: F,S,F,S,F,S,F,S,F,S which would trigger the rule despite the intervening successful logins.

- Choose the fields to group by from the dropdown list. The **Group by** field allows you to group and evaluate the incoming events. For example, in the rule that detects 5 failed logon attempts followed by 1 successful attempt, the user must be the same, so user_dst is the **Group By** meta key. You can also group by multiple keys. Using the previous example, you might want to group by user and machine to ensure that the same user logged in from the same machine attempts to log into an account multiple times. To do this, you might group by device_class and user_dst.

Example

The following graphic shows an example of the conditions for a rule that allow you to evaluate the same entities across multiple devices so you can accomplish complex use cases. For example, you can create a rule that triggers if an IDS (Intrusion Detection System) alert is followed by an AV(Anti-virus) alert for the same workstation. The work station key is not the same between the two (IDS & AV) sources, so you can perform a JOIN in order to evaluate the different entities.

In the IDS alert, the workstation is identified by the source IP address from the IDS alert, and would be compared to the destination IP address from the AV alert.

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input type="checkbox"/> IDS Check	1	followed by	JOIN	ip_src	ip_dst
<input type="checkbox"/> Antivirus Check	1				

Group By:

Occurs Within: 10 minutes

This is the criteria for the rule:

- An IDS alert occurs.
- The destination IP address from the AV alert and source IP address for the workstation from the IDS alert are joined to allow you to view the same entities across different sources.
- An Antivirus alert follows the IDS alert.

Add an Advanced EPL Rule

This topic provides instructions to define rule criteria by writing an EPL query. EPL is a declarative language for handling high-frequency time-based event data. It is used to express filtering, aggregation, and joins over possibly sliding windows of multiple event streams. EPL also includes pattern semantics to express complex temporal causality among events.

Write an advanced EPL rule when rule criteria is more complex than what you can specify in Rule Builder.

It is outside the scope of this guide to explain EPL syntax.

- For EPL Documentation, see <http://www.espertech.com/esper/documentation.php>.
- For the EPL Online Tool, see <http://esper-epl-tryout.appspot.com/epltryout/mainform.htm>



Prerequisites

The following are prerequisites for adding an advanced rule:

- You must know Event Processing Language (EPL).
- You must understand ESA Annotations to mark which EPL statements are linked to generating alerts.

Procedure

To add an Advanced EPL rule:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
2. In the **Rule Library**, select   > **Advanced EPL**.

The screenshot shows the 'New Advanced EPL Rule' configuration interface. It includes a navigation bar with 'Alerts', 'Summary', and 'Configure' tabs. Below this, there are sub-tabs for 'Rules', 'Services', 'Settings', and 'New Advanced EPL Rule'. The main form area is titled 'Advanced EPL' and contains the following fields and options:

- Rule Name ***: A text input field.
- Description**: A large text area for describing the rule.
- Trial Rule**: A checkbox option.
- Severity ***: A dropdown menu currently set to 'Low'.
- Query ***: A large text area for writing the EPL query.
- Notifications**: A section with a table for 'Global Notifications' and an 'Output Suppression' checkbox.

3. Type a unique, descriptive name in the **Rule Name** field.
This name will appear in the Rule Library so be specific enough to distinguish the rule from others.
4. In the **Description** field, explain which events the rule detects.
The beginning of this description will appear in the Rule Library
5. Select **Trial Rule** to automatically disable the rule if all trial rules collectively exceed the memory threshold.
Use trial rule mode as a safeguard to see if a rule runs efficiently and to prevent downtime caused by running out of memory. For more information, see [Work with Trial Rules](#).
6. For **Severity**, classify the rule as Low, Medium, High or Critical.
7. To define rule criteria, write a **Query** in EPL.

Note: For all meta key names, use an underscore not a period. For example, `ec_outcome` is correct but `ec.outcome` is not.

8. For dynamic statement name generation in ESA, you must enclose the meta keys in curly brackets and include this annotation in the syntax:

```
@Name("RIG {ip_src} {alias_host} {ec_activity}")
```

where,

- RIG is the static part of the statement name
- {ip_src}, {alias_host}, {ec_activity} is the dynamic part of the statement name

Note: If any of the metas in the dynamic part of the statement name has a null value, it is displayed as a static text.

If you want to view the meta along with the curly braces, for instance, {meta}, you can use the "\\" character. For example, @Name("static text \\{ip_src\\}")

If a rule should generate an alert, include this ESA annotation in the syntax:

```
@RSAAAlert
```

For more information on ESA Annotations, see [ESA Annotations](#).

Event Processing Language (EPL)

This topic describes Event Processing Language (EPL), a declarative language for dealing with high frequency time-based event data. ESA uses Event Processing Language (EPL), a declarative language for dealing with high frequency time-based event data. It is used for express filtering, aggregation, and joins over possibly sliding windows of multiple event streams. EPL also includes pattern semantics to express complex temporal causality among events. It can perform, but is not limited to, the following functions:

- Filter Event
- Alert Suppression
- Compute percentages or ratios
- Average, count, min and max for a given time window
- Correlate events arriving in multiple stream
- Correlate events that arrive out of order
- On-Off Windows
- Followed-by and Not Followed-by support
- Regex filter support

Databases require explicit querying to return meaningful data and are not suited to push data as it changes. The developer must implement the temporal and aggregation logic himself. By contrast, the EPL engine provides a higher abstraction and intelligence and can be thought of as a database turned upside-down. Instead of storing the data and running queries against stored data, EPL allows applications to store queries and continuously run the data through. Response from the EPL engine is real-time when conditions occur that match user defined queries.

For the purposes of online help, basic statements are used to illustrate how to set up ESA; however, for more information about writing EPL statements, the <http://www.espertech.com> site provides tutorials and examples.

Note: ESA supports Esper version 5.3.0.

ESA Annotations

This topic describes two annotations that Security Analytics provides to use in advanced EPL rules.

@RSAAAlert Annotation

The @RSAAAlert annotation is used to mark which EPL statements are linked to generating alerts. The @RSAAAlert is optional in advanced rules and is useful only with statements that are expected to generate ESA alerts.

Note: This annotation is not needed in all EPL statements, like those that create named windows

For example, consider the following sequence of simplified events:

@RSAPersist Annotation

The @RSAPersist annotation is used to mark a named window as a ESA managed window for persistence. By marking the named window as a ESA managed window, ESA periodically writes the contents of the window to disk and restores them back if the window is un-deployed and re-deployed. The systems take a snapshot just before the module is un-deployed and the window is removed. Conversely, it restores the window contents from the snapshot just after the module is re-deployed. This ensures that the contents of the window are not lost if the module state is altered or if the ESA service goes down.

For example, consider a named window, `DHCPTracker` that holds a mapping from IP addresses to each assigned hostname. You can annotate the statement with the @RSAPersist annotation as:

```
@RSAPersist
create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

Note: All windows definitions are not suitable for persistence. `@RSAPersist` annotation must be used with care. If the window has timed-records or if it depends on time based constraints it is very likely that the reverted snapshots will not restore it to the correct state. Also, any changes to the window definition will invalidate the snapshots and reset the window to a blank state. The system does not do any semantic analysis to determine if the changes to the window definition are conflicting or not. Note that other parts of a module (i.e. other than the particular `CREATE WINDOW` call that defines the window) may change, without invalidating the snapshots.

@UsesEnrichment (10.6.1.1 and later)

The `@UsesEnrichment` can be used in advanced EPL rules to reference enrichments. In order to synchronize enrichments with ESA, all enrichment dependencies in EPL rules must be referenced with the `@UsesEnrichment` annotation.

The `@UsesEnrichment` annotation uses the following format:

```
@UsesEnrichment(name= '<enrichment_name>')
```

For example, the following EPL references a whitelist enrichment:

```
@UsesEnrichment(name = 'Whitelist')
@RSAAAlert
SELECT * FROM Event(ip_src NOT IN (SELECT ip_address FROM
Whitelist))
```

@Name

The `@Name` is the statement name defined in ESA advanced rules. It is used to dynamically generate statement names in ESA alerts. The statement name of only an alert triggering statement is displayed. This annotation has meta keys enclosed in curly brackets.

The `@Name` annotation uses the following format:

```
@Name("<static_part_of_statement_name> {meta_key1} {meta_
key2}...")
```

For example, the following EPL references meta keys `ip_src` and `user_name` whose values will be dynamically generated.

```
@Name("Login Event to {ip_src} by {user_name}")
```

Note: You can specify any number of meta keys in the statement for dynamic statement name generation.

The length of individual meta key is limited to 64, after which the value is truncated and appended with "...".

The length of the dynamic generation of statement name is limited to 128, after which the value is truncated to 128 and appended with "...". All the remaining values post truncation will be treated as static values.

Sample Advanced EPL Rules

Following are the examples of Advanced ESA rules. Each example has multiple ways of implementing the same use-case.

Example #1:

Create an user account and delete the same user account in 300s. User information is stored in user_src meta.

EPL #1:

Rule Name	CreateuseraccountFollowedByDeletionof Useraccount1
Rule Description	Create a user account followed by an action to delete the same user account in 300 seconds.
Rule Code	<pre>SELECT * FROM Event(ec_subject='User' AND ec_outcome='Success' AND user_src is NOT NULL AND ec_activity IN ('Create', 'Delete')).win:time(300 seconds) match_recognize (partition by user_src measures C as c, D as d pattern (C D) define C as C.ec_activity='Create' , D as D.ec_activity='Delete');</pre>
Note	<ul style="list-style-type: none"> • Filter events needed for pattern in given time frame. Filter conditions should be such that only required events are passed to match recognize function. In this case, they are create and delete user account Events. i.e. Event(ec_subject='User' AND ec_outcome='Success' AND user_src is NOT NULL AND ec_activity IN ('Create', 'Delete')) • Partition by creates buckets. In this case, esper creates buckets per value of user_src. And hence value of user_src is common between both events. • Define pattern you want. Right now it is set to Create Followed by Delete. You can do multiple creates followed by delete (C+ D). Pattern is very similar to regular expression. • Most efficient use case.

EPL #2:

Rule Name	CreateuseraccountFollowedByDeletionof Useraccount2
Rule Description	Create a user account followed by an action to delete the same user account in 300 seconds.
Rule Code	<pre>SELECT * from pattern[every (a= Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_ activity IN ('Create')) -> (Event(ec_subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create') AND user_src = a.user_src)))where timer:within(300 Sec)];</pre>
Note	<ul style="list-style-type: none"> • Lets say same user is created twice and deleted once in that order. Then the above pattern will fire 2 alerts. • A thread is created for every User creation. • There is no way to control threads. It is important to have time bonds and preferably small intervals.

Example #2:

Detect pattern where user created followed by login by same user and user is deleted in end. In case of windows logs user info is stored in either user_dst or user_src depending on event.

user_src(create) = user_dst(Login) = user_src(Delete)

EPL #3:

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.
Rule Code	<pre>SELECT * FROM Event(ec_subject='User' and ec_activity in ('Create','Logon','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success').win:time(300 seconds) match_recognize (measures C as c, L as l, D as d</pre>

Note	<pre> pattern (C L D) define C as C.ec_activity = 'Create', L as L.ec_activity = 'Logon' AND L.user_dst = C.user_src, D as D.ec_activity = 'Delete' AND D.user_src = C.user_src); </pre>
	<ul style="list-style-type: none"> • Since user_src/user_dst is not common across all events we can't use partition. It will be 1 single bucket running 1 pattern at a time. For example, for user 1 and 2 if the stream of events are C1C2L1D1, C1L1C2D1, there will be no alert because C1 thread got reset by C2. Alert will be fired only if C1L1D1 are in order and no other event either from same user or other user falls in between. • Another solution would be to use Named Window and merge user_dst and user_src into single column and then run match recognize. (EPL #3). • Pattern can also be used. You might get more alerts than expected. (EPL #4).

EPL #4: Using NamedWindows and match recognize

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.
Rule Code	<pre> @Name('NormalizedWindow')create window FilteredEvents.win:time(300 sec) (user String, eactivity string, sessionid Long); @Name('UsersrcEvents') Insert into FilteredEvents select user_src as user, ec_activity as eactivity, sessionid from Event(ec_subject='User' and ec_activity in ('Create','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_src is not null); @Name('UsrdstEvents') Insert into FilteredEvents select user_dst as user, ec_activity as eactivity, sessionid from Event(ec_subject='User' and ec_activity in (Logon') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_dst is not null); </pre>

```

@Name('Pattern')
@RSAAAlert(oneInSeconds=0, identifiers={"user"})

select * from FilteredEvents
    match_recognize (
partition by user
measures C as c, L as l, D as d
pattern (C L+D)
define C as C.ecactivity= 'Create',
L as L.ecactivity= 'Logon',
D as D.ecactivity='Delete'
);

```

EPL #5: Using Every @RSAAAlert(oneInSeconds=0, identifiers={"user_src"})

```

SELECT a.time as time,a.ip_src as ip_src,a.user_dst as user_dst,a.ip_dst as ip_dst,a.alias_host
as alias_host from pattern[every (a=Event (ec_subject='User' and ec_activity='Create'
and ec_theme='UserGroup' and ec_outcome='Success') -> (Event(ec_subject='User' and
ec_activity='Logon' and ec_theme='Authentication' and user_src=a.user_dst) -> b=Event
(ec_subject='User' and ec_activity='Delete' and ec_theme='UserGroup' and user_
dst=a.user_dst))) where timer:within(300 sec)];

```

Rule Name	CreateUserLoginandDeleteUser
Rule Description	Detect a pattern where a user creates a User account followed by login by the same user followed by deletion of the User account.

Example #3:

Excessive login failures from same sourceIP

EPL #6: @RSAAAlert(oneInSeconds=0, identifiers={"ip_src"})

Rule Name	ExcessLoginFailure
Rule Description	The same user tried logging in from the same Source IP and faced login failures
Rule Code	<pre> SELECT * FROM Event (ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure').std:groupwin(ip_ src).win:time_length_batch(300 sec, 10) GROUP BY ip_ src HAVING COUNT(*) = 10; </pre>

Note

- Creates window per ip_src
- Uses time_length_batch: Looks at events in batches(tumbling window). Every event will be part of only 1 window. Window releases events either when time elapses or count is reached.
- One of issues with tumbling windows that events occurring towards end of batch might not lead to an alert.

In below sequence of events at t=301 even though 10 login failures occurred for same login in last 300 secs there will be no alert because batch of events was dropped at t=300

Time t	Login Failures for Specific Users	Alert	Time Batch
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3
850	3	0	3
900	1	1	3 ends and 4 begins

- Above problem can be resolved using win:time windows (EPL#7)instead of win:time_length_batch windows.
- Outer group by is to control events when time elapses. Say you have 9 events at end of 60 secs, esper engine will push those 9 events to listener. Group by and count will restrict it since count is not equal to 10.
- Time and count can be modified as needed.

EPL #7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Rule Name	ExcessLoginFailure
Rule Description	The same user tried logging in from the same Source IP and faced login failures

Rule Code	<pre>SELECT * FROM Event (ip_src IS NOT NULL AND ec_activity='Logon' AND ec_ outcome = 'Failure').std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_ src HAVING COUNT(*) = 10</pre>
Note	<ul style="list-style-type: none"> • This is sliding window and hence once alert is fired for a set of events they can be used for another alert as well till time has passed. • If 10 events were involved in causing alert only last event will appear • If < or > are used then you might see more than 1 alert. You should use alert suppression accordingly.

Example #4:

Multiple failed logins from multiple different users from same source to same destination, a single user from multiple different sources to same destination.

EPL #8: using groupwin , time_length_batch and unique

Rule Name	MultiplefailedLogins
Rule Description	<p>There are multiple failed logins for the following cases:</p> <ul style="list-style-type: none"> - From multiple users from same source to same destination. - Single user from multiple sources to the same destination.
Rule Code	<pre>SELECT * FROM Event(ec_activity='Logon' AND ec_outcome='Failure' AND ip_src IS NOT NULL AND ip_dst IS NOT NULL AND user_dst IS NOT NULL).std:groupwin(ip_src,ip_ dst).win:time_length_batch(300 seconds, 5}).std:unique (user_dst) group by ip_src,ip_dst having count(*) = 5;</pre>
Note	<ul style="list-style-type: none"> • ip.dst and ip.src are common across all events. • user_dst is unique for all events. • Alert is fired when there are atleast 5 different users try to login from same ip.src and ip.dst combination.

Example #5:

No Log traffic from a device in a given timeframe.

EPL #9: using groupwin , time_length_batch and unique

Rule Name	NoLogTraffic
Rule Description	There is no log traffic observed from a device in a given time frame.
Rule Code	<pre>SELECT * FROM pattern [every a = Event(device_ip IN ('10.0.0.0', '10.0.0.1') AND medium = 32) -> (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND device_type = a.device_type AND medium = 32))];</pre>
Note	<ul style="list-style-type: none"> • Rule only detects sudden loss of traffic. It won't alert if there is no traffic to begin with. You need at least 1 event for rule to alert. • List of device ip address or device hostnames as input. Only these systems will be tracked. • Time input is required. Alert is fired when time interval between events exceeds input time.

Example #6:

Multiple Failed Logins NOT followed by a Lockout event by the same user.

EPL #10: using groupwin , time_length_batch and unique

Rule Name	FailedloginswoLockout
Rule Description	There are multiple failed logins that are not followed by Lockout event by the same user.
Rule Code	<pre>SELECT * FROM pattern [every-distinct(a.user_dst, a.device_ip, 1 msec) (a= Event(ec_activity='Logon' and ec_outcome='Failure' and user_dst IS NOT NULL)-> [2](Event(device_ip =a.device_ip and ec_activity='Logon' and ec_outcome='Failure' and user_dst=a.user_dst) AND NOT Event((ec_activity='Logon' and ec_outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst)))) where timer:within(60 seconds) -> (timer:interval(30 seconds) and not Event(device_ip=a.device_ip and</pre>

Note	<pre>user_dst=a.user_dst and ec_activity='Lockout'))];</pre>
	<ul style="list-style-type: none"> • Above query detects the absence of a Lockout Event after the occurrence of 2 failed logins from same user. • The occurrence of the multiple failed logins are timed and are assumed to occur within a certain period of time. Also, in-practice the Lockout event is assumed to occur within a short time after the occurrence of the last failed login event because the threshold value of Failed logins per user is set in a given domain. • In current query, every distinct will suppress new thread for combination of user and device for 1 millisecc. • Time allowed for 3 failed logins is 60 secs since 1st failed attempt. Wait period for lockout event to occur is 30 secs

Example #7:

Custom functions to perform LIKE and REGEX operations for ARRAY elements.

EPL #11: @RSAAlert(oneInSeconds=0)

Rule Name	MatchLikeRegex
Rule Description	There are custom functions to perform LIKE and REGEX comparisons of array meta keys.
Rule Code	<pre>SELECT * FROM pattern[e1=Event(matchLike(alias_host, "10.0.0.%")) AND e2=Event(matchRegex(alias_host, "10\.0\.0\.1[0-9] [0-9]")) where timer:within(5 Minutes)];</pre>

Note:

1. "." in meta keys should be replaced with ("_").
2. All patterns should be time bound.
3. Use of appropriate tags in front of statements
 - a) @RSAPersist:
 - b) @RSAAlert:

For additional details you can refer to:

- EPL Documentation: <http://www.espertech.com/esper/documentation.php>
- EPL Online Tool: <http://esper-epl-tryout.appspot.com/epltryout/mainform.html>

Working with Rules

This topic discusses additional procedures you can perform on rules. You may want to perform any of the following procedures:


- [Edit, Duplicate or Delete a Rule](#)
- [Filter or Search for Rules](#)
- [Import or Export Rules](#)

Edit, Duplicate or Delete a Rule

This topic provides instructions to edit, duplicate, or delete an Event Stream Analysis (ESA) rule. When you edit a rule, ESA applies the updated criteria going forward. No changes are made to previously generated alerts.

Procedures

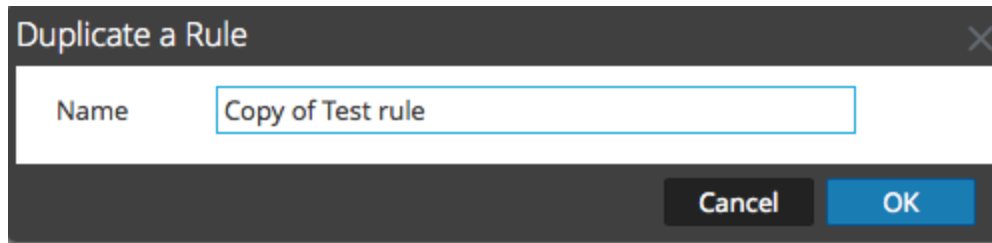
Edit a Rule

1. In the **Security Analytics** menu, select **Alerts > Configure > Rules**.
The Rules tab is displayed.
2. In the **Rule Library**, select the rule you want to edit and click .
Depending on the rule type, the respective rule tab is displayed.
3. Modify the required parameters.
4. Click **Save**.

Duplicate a Rule

1. In the **Rule Library**, select the rule you want to duplicate and click .

- The Duplicate a Rule dialog is displayed. The system adds **Copy of** in front of the rule name.



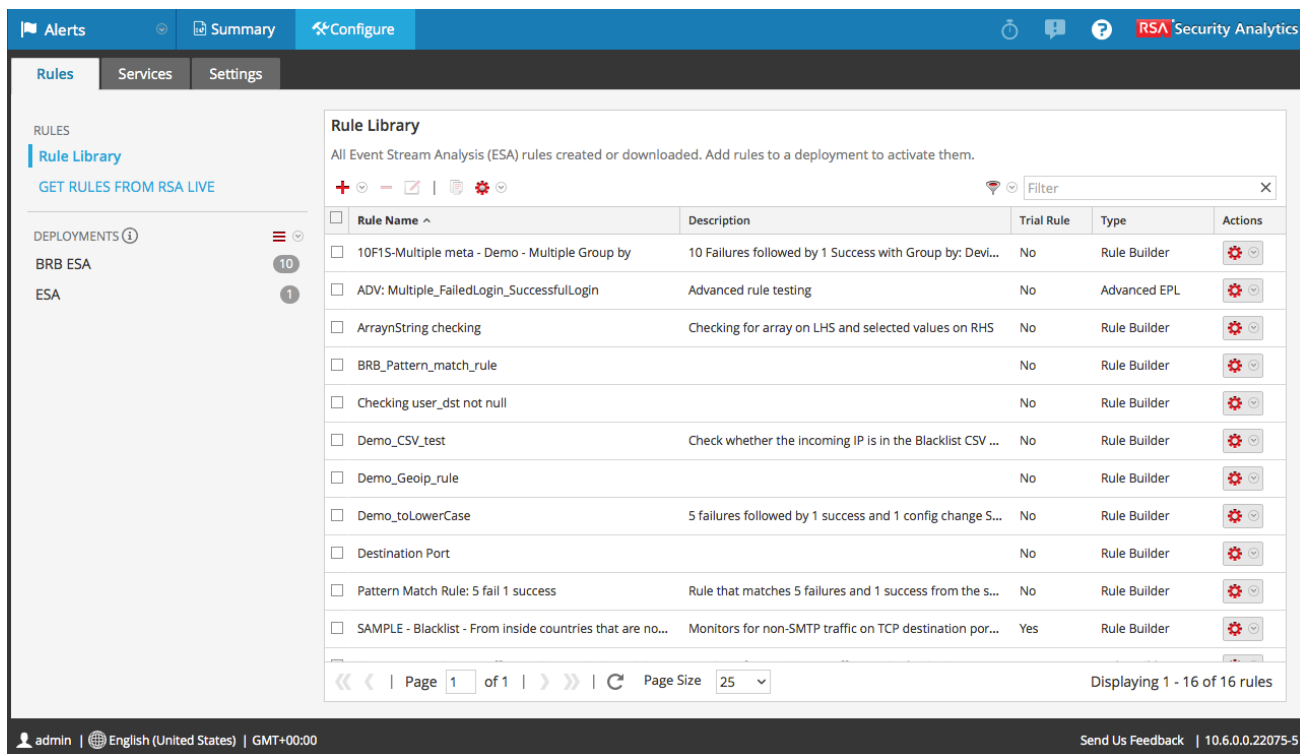
- In the **Name** field, type a unique name for the duplicate rule and click **OK**.

A duplicate rule with the new name is added to the Rule Library.

Delete a Rule

- In the **Security Analytics** menu, select **Alerts > Configure > Rules**.

The Rules tab is displayed.



- In the Rule Library, select one or more rules and click **⊖**.

A warning dialog is displayed.

- Click **Yes**.

A confirmation message that the rule is deleted successfully is displayed and the selected rule is deleted from the Rule Library.

Filter or Search for Rules


This topic shows analysts how to specify the type of rules that display in the Rule Library.

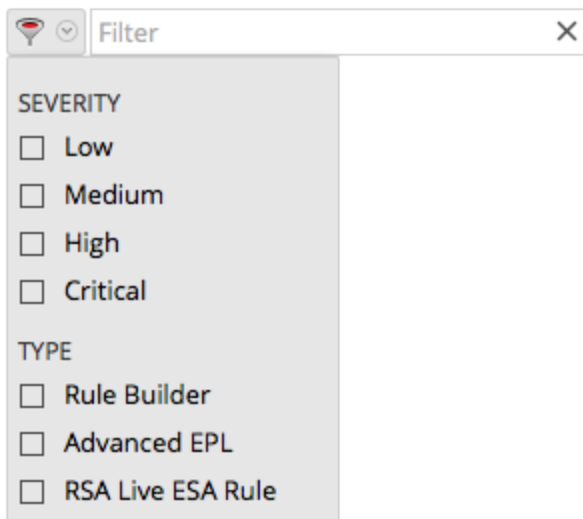
Prerequisites

Make sure that you understand the Rule Library view components. For more information, see [Rule Library Panel](#).

Procedures

Filter

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed by default.
2. In the **Rule Library** panel toolbar, click  and select the severity and type of rules that you would like to appear in the Rule Library list. The following figure shows the Filter drop-down list.



The selected rule types appear in the list.

Search

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed by default.
2. In the **Rule Library** panel toolbar, type a rule name in the Filter field.
The Rule Library panel lists the rules that match the names entered in the Filter field.

Import or Export Rules

The topic provides instructions to import ESA rules from a Security Analytics instance and to export ESA rules to your hard drive so you can keep a local copy.

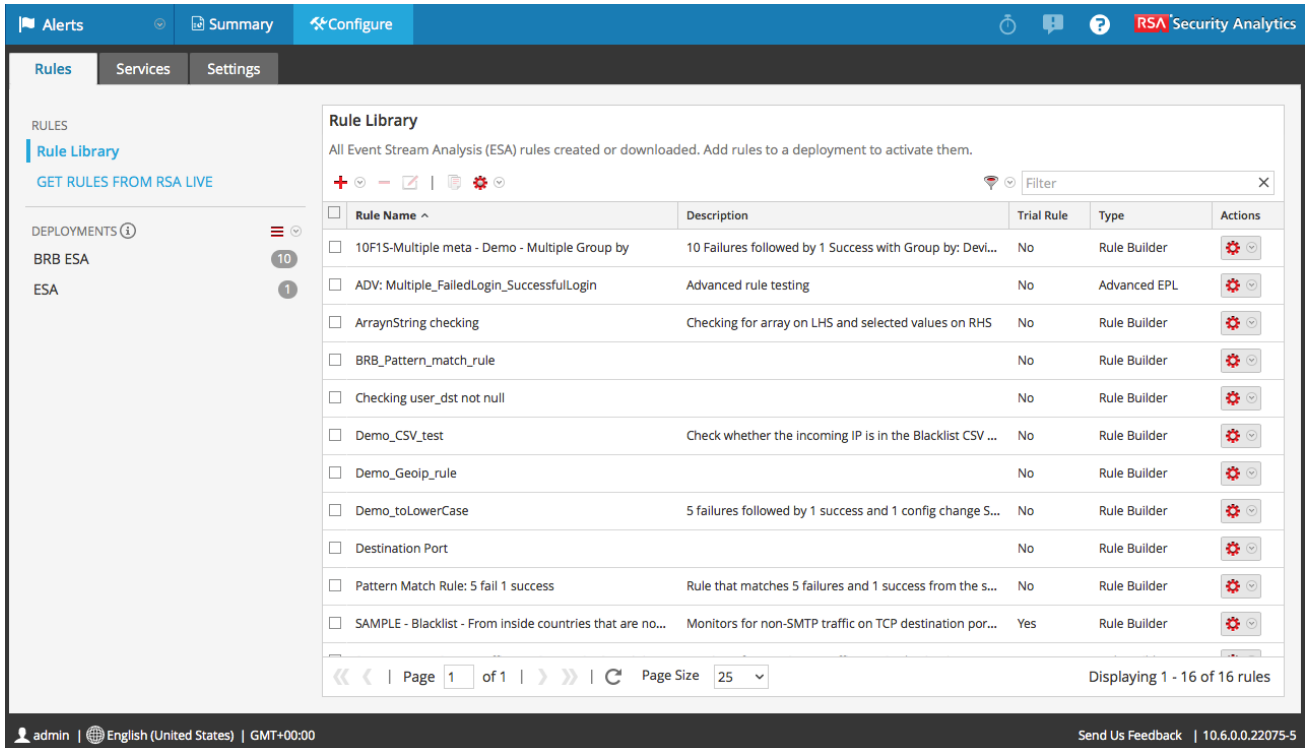
If you exported a rule in an earlier version of Security Analytics, the following conditions apply when you import the rule in version 10.5 or later:


- Exported in version 10.3 – You cannot import rules to version 10.5.
- Exported in version 10.4 – Rule behavior depends if cross-correlation is disabled, which is the default, or enabled:
 - Disabled – You can import rules to version 10.5.
 - Enabled – You must restart Security Analytics or make a minor change to the rule, save, remove the minor change and save again. Either procedure generates the forwarding rule that the 10.5 cross-site correlation feature requires.

Procedures

Import ESA Rules

1. In the **Security Analytics** menu, select **Alerts > Configure > Rules**.
The Rules tab is displayed.





2. In the **Rules Library** toolbar, click  > **Import**.
The Import ESA Rules dialog is displayed.



3. Click **Browse** to browse and select the file containing the ESA rules.
4. Click **Import**.

Export

1. Select an ESA rule or multiple rules and click   > **Export** in the Rule Library toolbar.
A warning dialog is displayed.
2. Click **Yes**.
The Export Rules dialog is displayed.
3. In the **Enter File Name** field, type a filename for the file with the ESA rules and click **Export**.
The file is exported as a binary file to your machine.

Note: The binary file cannot be edited.

Choose How to be Notified of Alerts

This topic explains the different notification methods and how to add a notification method to a rule. Administrator, SOC Manager or DPO role permissions are required for all tasks in this section.

When a rule triggers an alert, ESA can send a notification in the following ways:

- Email
- SNMP
- Syslog
- Script

To configure a notification, you configure these components:

- Notification server – After you configure a notification server, you can add it to a rule. When the rule triggers an alert, the rule will use that server to send alert notifications.
- Notifications – These are the outputs, which can be email, script, SNMP, and Syslog. When you design a rule, you can specify the notification for an alert.
- Templates – The format of an alert notification is defined in a template.

Alert suppression and alert rate regulation are two features that Event Stream Analysis provides. Alert suppression ensures that multiple emails are not sent out for the same alert. For example, consider a rule to detect failed user logins. If you set the alert suppression to three minutes, you will see only the alerts generated in that time frame. This is fewer than the number of alerts you would see without alert suppression. Some alerts can be duplicates. With alert suppression, emails are not sent for duplicate alerts. This ensures the inbox is not flooded with redundant alert notifications.

Alert rate regulation is a preventive measure to ensure that alerts from misconstrued rules do not flood the system. This ensures that ESA does not send more than the configured limit of emails within one minute.

Notification servers, notifications, and templates are configured in the Administration System view. For more information, see "Configure Notification Servers", "Configure Notification Outputs", and "Configure Templates for Notifications" in the **System Configuration Guide**.

Notification Methods

When a rule triggers an alert, ESA can send a notification in the following ways:

- Email
- SNMP
- Syslog
- Script

Email Notifications

Event Stream Analysis can send notifications to users through email about various system events.

To configure these email notifications, you need to:

- Configure the SMTP email server as an output provider. For instructions, see "Configure the Email Settings as Notification Server" in the **System Configuration Guide**.
- Set up an email account to receive notifications. For instructions, see "Configure Email as a Notification" in the **System Configuration Guide**.
- Configure a template for email notification. For instructions, see "Configure a Template" in the **System Configuration Guide**.

SNMP

Event Stream Analysis can send events as an SNMP trap to a configured SNMP trap host.

Note:

The MIB file **NETWITNESS-MIB.txt** is located on the ESA RPM at the following location */usr/share/snmp/mibs*. With the MIB file, you will be able to identify the SNMP alerts triggered from ESA. And, the Trap OID value for ESA is 20.

To configure these SNMP notifications, you need to:

- Configure SNMP trap host settings as an output provider. For instructions, see "Configure the SNMP Settings as Notification Server" in the **System Configuration Guide**.
- Configure SNMP trap settings as an output action. For instructions, see "Configure SNMP as a Notification" in the **System Configuration Guide**.
- Configure a template for SNMP. For instructions, see "Configure a Template" in the **System Configuration Guide**.

Syslog

Event Stream Analysis can send events and consolidate logs in Syslog format to a Syslog server. To configure these Syslog notifications, you need to:

- Configure Syslog server settings as an output provider. For instructions, see "Configure the Syslog Settings as Notification Server" in the **System Configuration Guide**.
- Configure Syslog message format as an output action. For instructions, see "Configure Syslog as a Notification" in the **System Configuration Guide**.
- Configure a template for Syslog. For instructions, see "Configure a Template" in the **System Configuration Guide**.

Script Alerter

Apart from the alert notifications ESA allows users to run scripts in response to ESA alerts.

Scripts enable you to do custom integration with applications that exist in your environment. For example, if you want to open an incident ticket from an application when a specific alert is triggered, Script Alerter lets you write a script that calls the application API and have ESA invoke it when the specific ESA rule is triggered. You can configure a FreeMarker template to define what details you want to extract from the output of the ESA rule and pass it as command line arguments to the script.

To use the Script Alert, you need to:

- Configure the user identity and other details that are required to execute the script. For instructions, see "Configure Script as a Notification Server" in the **System Configuration Guide**.
- Define the Script. For instructions, see "Configure Script as a Notification" in the **System Configuration Guide**.
- Configure a template for the script. For instructions, see "Configure a Template" in the **System Configuration Guide**.

Add Notification Method to a Rule

This topic tells administrators how to add a notification, such as email, to a rule. ESA uses the notification method when it generates an alert for an event that meets rule criteria.

You add a notification to a rule so ESA can let you know when a rule triggers an alert. Although the notification fields are not required, it is a best practice to add a notification to a rule.

When you add a notification method to a rule, you select the following information:


- Output
- Notification
- Notification Server
- Template

Prerequisites

- Your role must have permission to manage rules.
- The rule must exist.
- The notification method must be configured with a supported server and template:
 - Click **Administration > System > Global Notifications**.
 - For detailed procedures, see the **System Configuration Guide**.

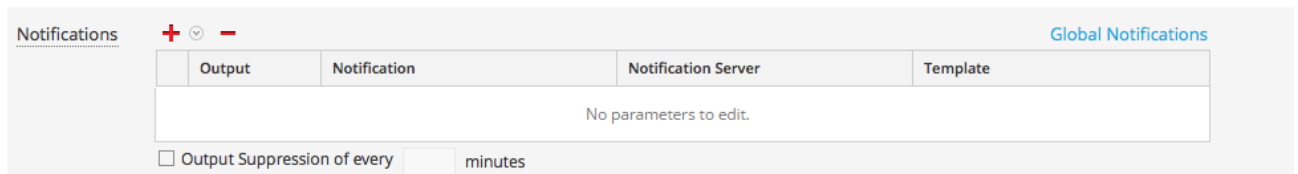
Procedure

To add a notification method to a rule:

1. In the **Security Analytics** menu, select **Alerts > Configure > Rules**.
2. In the **Rule Library**, click   to add a new rule or select an existing rule and click .



Depending on the rule type, the Rule Builder or Advanced EPL tab is displayed.

The Notifications section is the same for both tabs.



Output	Notification	Notification Server	Template
No parameters to edit.			

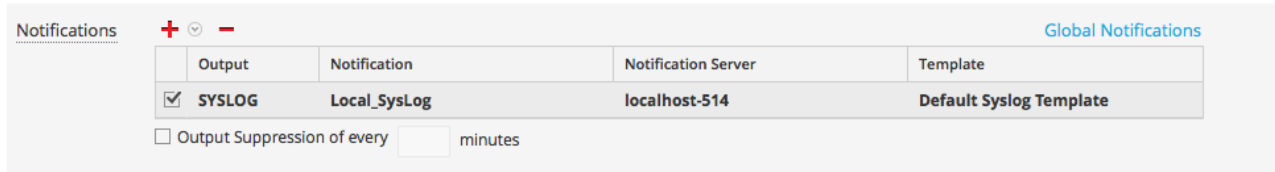
Output Suppression of every minutes

3. Click   and select the **Output** for the alert:
 - Email
 - SNMP
 - Syslog
 - Script
4. Double-click the **Notification** field and select the name of a previously configured output.
For example, Level 1 Analyst could be the name of an email notification that goes to the L1-

Analysts email distribution group.

5. Double-click the **Notification Server** field and select the server that sends the notification.
6. Double-click the **Template** field and select a format for the alert.

The following figure shows the settings for a Syslog notification.



Output	Notification	Notification Server	Template
<input checked="" type="checkbox"/> SYSLOG	Local_SysLog	localhost-514	Default Syslog Template

Output Suppression of every minutes

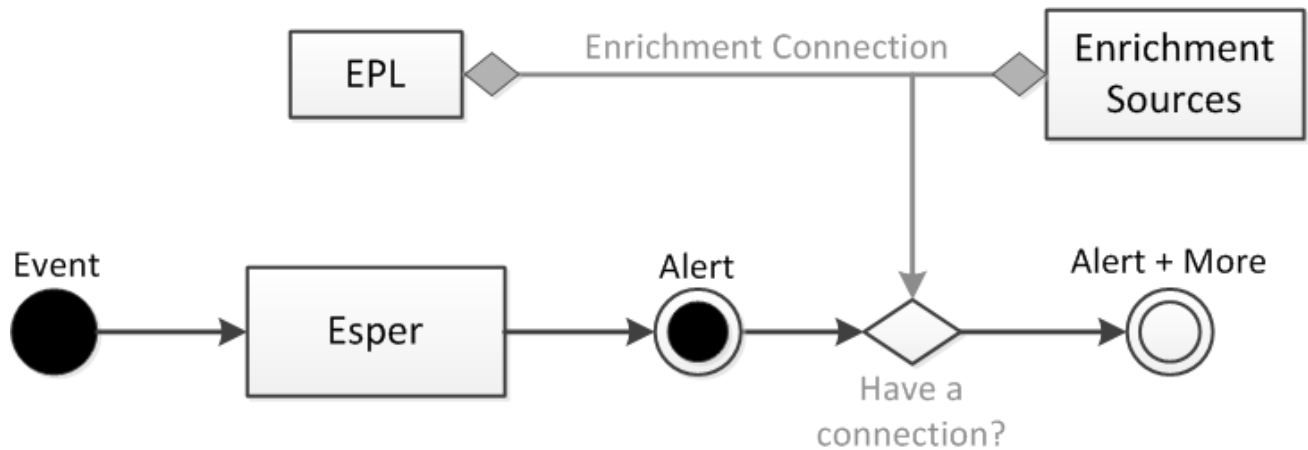
7. If you want to specify frequency, select **Output Suppression**, then enter the number of **minutes**.
8. If you want to add another notification, repeat steps 3-7.
9. Click **Save**.

When ESA generates an alert for an event that matches the rule criteria, you will be notified of the alert via each notification method added to the rule.

Add a Data Enrichment Source

This topic tells how to add a previously configured enrichment source to a rule. When ESA creates an alert, information from the source gets included in it.

Enrichments provide the ability to include contextual information into correlation logic and alert output. Without enrichments, all information included in an ESA alert is from a Security Analytics core service. With enrichments, you can request for look ups into a variety of sources and include the results into the outgoing alerts. The following figure illustrates the enrichment feature.



Enrichment configuration is made up of two logical units:

- Enrichment Sources – These are data stores of contextual information.
- Enrichment Connections – These act as connectors between alert meta and source columns.

ESA allows you to make connections between Event Processing Language (EPL) statements and enrichment sources. Once the connections are established, the system joins the selected fields from the alert output with the information in the sources and uses the matching data to enrich the alert that is sent out. ESA can connect with the following sources:

- Esper Named Windows
- Relational Database tables
- MaxMindGeoIP Database
- RSA Warehouse Analytics Watchlists

Note: The geoIP enrichment source can neither be created nor deleted. It is provided out of the box to the user.

Sample Rule with Enrichment

The following sample rule illustrates the enrichment feature provided by ESA:

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login Failure')
```

The rule generates an alert for every logon failure and thus if the following (simplified) event stream is received at ESA:

sessionid	ec_theme	username	ip_src	ip_dst	host_dst
1	Login Success	dshrute	23.xx.23x.16		
2	Login Failure	jhalpert	23.xx.23x.16	31.1x.x9.1x8	www.facebook.com

An alert with the following constituent events might be generated in response to the second session:

```
{
  "events": [
    {
      "username": "jhalpert",
      "host_dst": "www.facebook.com",
      "ip_dst": "31.1x.x9.1x8",
      "sessionid": 2,
      "ec_theme": "Login Failure",
      "esa_time": 1406148964130,
      "ip_src": "23.xx.23x.16"
    }
  ]
}
```

The JSON output shows all the information available for inclusion into an ESA notification using an appropriate FreeMarker template. For instance, the template expression `${events[0].username}` would evaluate to `jhalpert`.

With enrichments, the same module, with the same event stream, can generate the alert shown below. The system

can make multiple enrichment connections and pull contextual data to make the alert more meaningful.

For example:

`${events[0]["RSADataScienceLookup"][0].score}` gives the “**risk**” score of the destination domain computed by the RSA Warehouse Analytics module while `${events[0]["orgchart"][0].supervisor}` gives the name of the supervisor of the employee that the alert pertains to (pulled from an HR database) and `${events[0]["LoginRegister"][0].username}` gives the name of the user with the last successful logon from the same `ip_src` (using a stream based Named Window).

```
{"events": [
  {
    "username": "jhalpert",
    "host_dst": "www.facebook.com",
    "GeoIpLookup": [
      {
        "city": "Cambridge",
        "longitude": -71,
        "countryCode": "US",
        "areaCode": 617,
        "metroCode": 506,
        "region": "MA",
        "dmaCode": 506,
        "ipv4Obj": "/23.62.236.16",
        "countryName": "United States",
        "postalCode": "02142",
        "ipv4": "23.62.236.16",
        "latitude": 42,
        "organization": "Verizon Business"
      }
    ],
    "RSADataScienceLookup": [
      {
        "model_id": "suspiciousDomains_1",
        "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
        "score": 10,
        "key": "www.facebook.com"
      }
    ],
    "orgchart": [
      {
        "supervisor": "mscott",
        "name": "James Halpert",
        "extension": 3692,
        "location": "Scranton",

```

```
        "department": "Sales",
        "id": "jhalpert"
    }
],
"ip_dst": "31.13.69.128",
"sessionid": 2,
"LoginRegister": [
    {
        "username": "dshrute",
        "ip_src": "23.62.236.16"
    }
],
"ec_theme": "Login Failure",
"esa_time": 1406155218912,
"ip_src": "23.62.236.16"
}
]}
```

Configure a Database Connection

This topic provides information to configure a connection to an external database that can provide additional information in alerts. You configure a database connection so you can then configure the database as an enrichment source, to add further details to alerts. There are three steps in the process:

1. Configure a connection to a database.
2. Configure the external database as an enrichment source.
3. Add the enrichment source to a rule

This topic explains Step 1.

Example

This example illustrates how adding a database as an enrichment source adds value to alerts.

A rule detects users that attempt to sign up for a stealth email service. Twenty-five users match the rule criteria. Without the enrichment, the alert contains 25 User IDs. With the enrichment, the alert also includes the following information for each User ID:

- Name
- Title
- Department
- Office Location

Dependencies

When you configure a database, the following conditions apply:

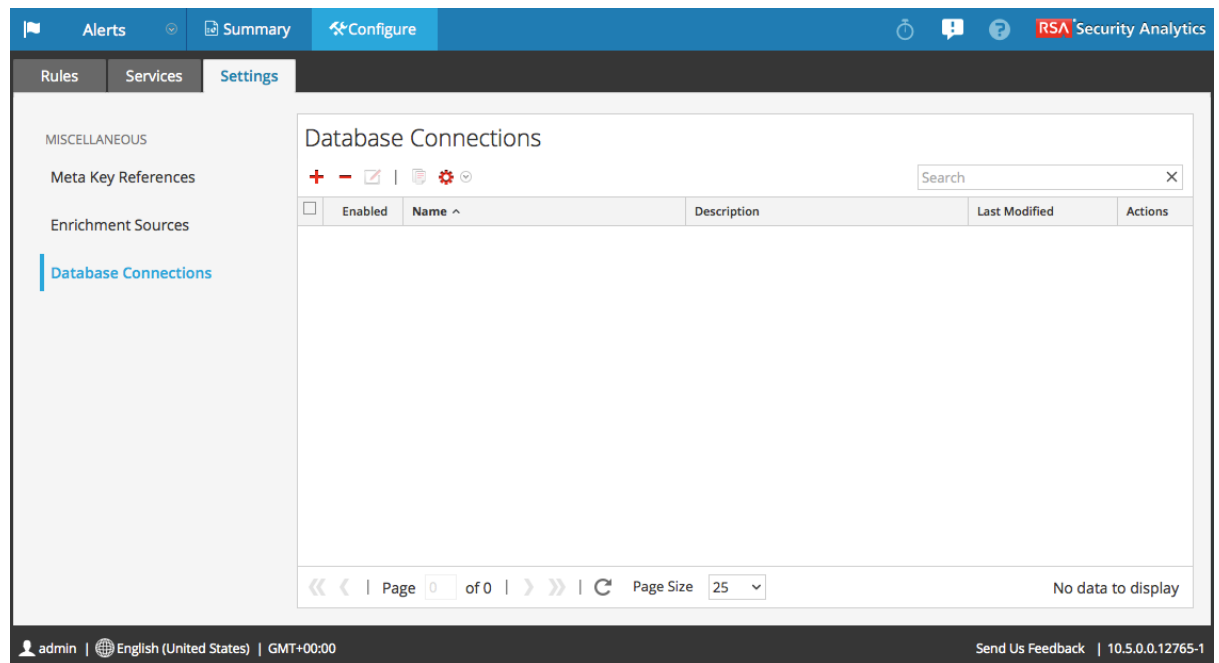
- A reference to the database is deployed on every ESA, even if the ESA does not deploy rules that use the database as an enrichment source.
- If the server that hosts the database goes down, it impacts a deployment.
 - An active deployment will continue to gather data and run rules but enrichments will not appear in alerts.
 - A new deployment will fail until you restart the host.

Procedure

To configure a database connection:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
2. Click the **Settings** tab.
3. In the options panel, select **Database Connections**.

The Database Connections panel is displayed.



4. Click **+** to add a database connection.

The screenshot shows a 'Database Connection' dialog box with the following fields and controls:

- Enable:** A checked checkbox.
- Connection Name *:** A text input field.
- Description:** A text input field.
- Driver Class *:** A dropdown menu with an 'Upload' button to its right.
- Database URL/IP *:** A text input field.
- Username *:** A text input field.
- Password *:** A text input field with masked characters (asterisks).
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

5. In the **Database Connection** dialog, provide the following information.

Field	Description
Enable	Select Enable to enrich the alert with additional data. By default, Enable is selected. Deselect Enable to exclude additional data from the alert.
Connection Name	Type a name to identify the connection. When you add a database as an enrichment source, this name appears in the list of Database Connections.
Description	(Optional) Type a brief description about the database connection.
Driver Class	<p>Select an appropriate driver class for the database.</p> <p>Two drivers come with Security Analytics, MongoDB and Postgres. To import a new driver, click Upload.</p> <p>The screenshot shows an 'Import Driver Class' dialog box with the following fields and controls:</p> <ul style="list-style-type: none"> Driver Class File: A text input field with a 'Browse' button to its right. Buttons: 'Cancel' and 'Import' buttons at the bottom right. <p>In the Import Driver Class dialog, click Browse, select a new driver, and click Import.</p>
Database URL or IP address	Type the URL or the IP address of the database to configure.

Field	Description
Username	Type the username to access the Database.
Password	Type the password to access the Database.

6. Click **Save**.

For related information, see [Settings Tab](#)

Enrichment Sources

This topic explains options for adding an external data source to provide additional information in alerts. Enrichment sources provide additional information in alerts. For example, a database can provide a name, department, and office location if a user matches rule criteria. There are three types of enrichment sources:

- External DB Reference
- In-Memory Table
- Warehouse Analytics

Configure a Database as Enrichment Source

You can configure a database as an enrichment source so you can add it to a rule. Then the Esper engine that analyzes events can access the information in the database to provide additional information in the alert.

For example, a rule detects users that attempt to sign up for a stealth email service. Twenty-five users match the rule criteria. The alert contains 25 User IDs. An external database would enhance the alert by providing the following additional information for each User ID:

- Name
- Title
- Department
- Office Location
- Reports To

You can edit, duplicate, import or export a database connection.

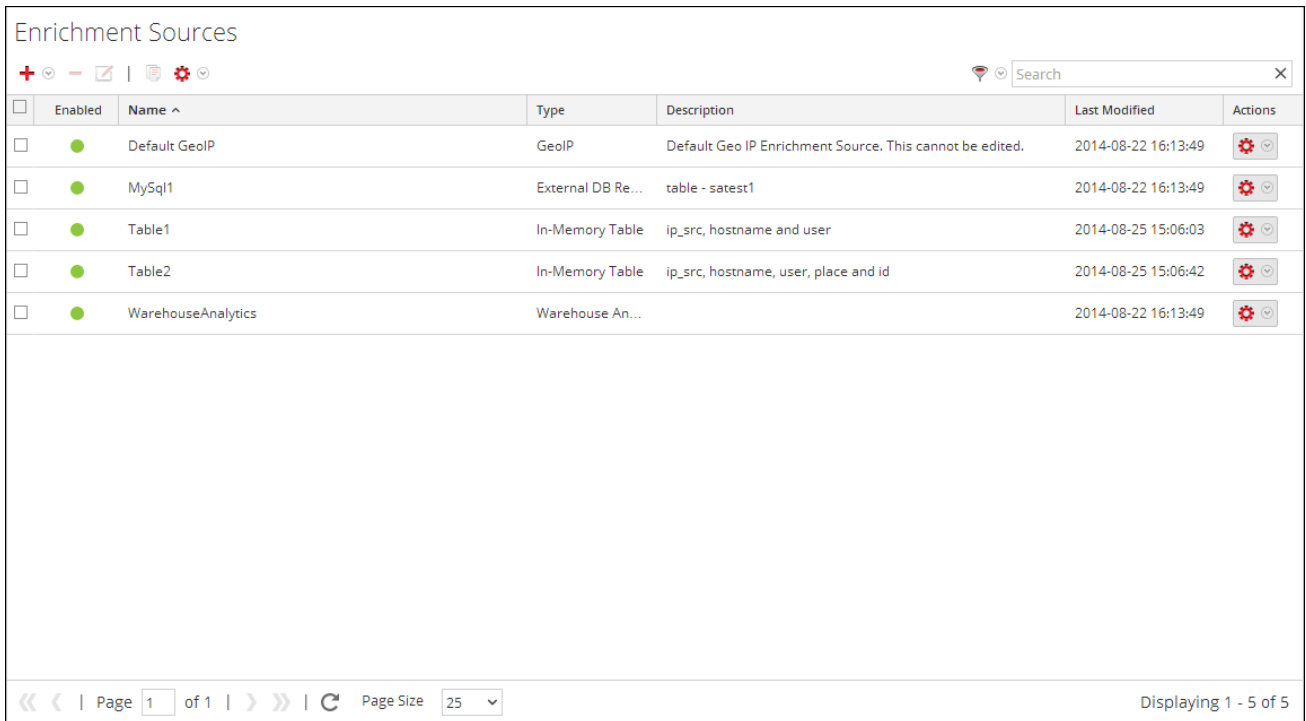
Prerequisites






You must configure a database connection. For more information, see [Configure a Database Connection](#).

Procedure

To configure database as an enrichment source:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
2. Click the **Settings** tab.
The Settings tab is displayed.
3. In the options panel, select **Enrichment Sources**.
The Enrichment Sources panel is displayed.



<input type="checkbox"/>	Enabled	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	●	Default GeolP	GeolP	Default Geo IP Enrichment Source. This cannot be edited.	2014-08-22 16:13:49	
<input type="checkbox"/>	●	MySQL1	External DB Re...	table - satetest1	2014-08-22 16:13:49	
<input type="checkbox"/>	●	Table1	In-Memory Table	ip_src, hostname and user	2014-08-25 15:06:03	
<input type="checkbox"/>	●	Table2	In-Memory Table	ip_src, hostname, user, place and id	2014-08-25 15:06:42	
<input type="checkbox"/>	●	WarehouseAnalytics	Warehouse An...		2014-08-22 16:13:49	

Page 1 of 1 | Page Size 25 | Displaying 1 - 5 of 5

4. From the  drop-down menu, select **External DB Reference**. You have to add a DB reference in order for the DB to be listed.

The External DB Reference dialog is displayed.

The screenshot shows a dialog box titled "External DB Reference". It contains the following fields and values:

- Enable:** A checkbox that is checked.
- User-Defined Table Name *:** A text input field containing "MySql1".
- Description:** A text input field containing "table - satest1".
- Database Connection *:** A dropdown menu with "MySQL1" selected.
- Table Name *:** A text input field containing "satest1".

At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

5. Select **Enable** to enrich alert with additional data. This is selected by default. If disabled, the alert will not be enriched with additional data.
6. In the **User-Defined Table Name** field, type a name to identify or label the database configuration.
7. In the **Description** field, type a brief description about the database configuration.
8. In the **Database Connection** drop-down menu, select the database connections defined.
9. In the **Table Name** field, enter database table name.
10. Click **Save**.

For details on parameters and their descriptions, see [Settings Tab](#).

Configure In-Memory Table as Enrichment Source

This topic provides instructions on how to configure an in-memory table. When you configure an in-memory table, you upload a .CSV file as an input to the table. You can associate this table with a rule as an enrichment source. When the associated rule generates an alert, ESA will enrich the alert with relevant information from the in-memory table.

For example, a rule could be configured to detect when a user tries to download freeware and to identify the person by user ID in the alert. The alert could be enriched with additional information from an in-memory table that contains details such as full name, title, office location and employee number.

An in-memory table is ideal for handling lightweight data. It is easy to set up and requires less maintenance than a database. For example, the AllTech Company is a small organization so the system administrator can maintain employee information in a .CSV file. If AllTech grows into a very large company, the administrator would have to configure an external database reference as an enrichment and associate the database with a rule.

Prerequisites

The column name in the .CSV file cannot have whitespace characters.

The first line of the .CSV file must be formatted this way for each column:

```
name_of_column_1 type_of_column_1
```

For example, these three columns are formatted correctly:

```
Last_Name string
```




```
First_Name string
```

```
Phone integer
```

Procedures

Configure an Adhoc In-Memory Table

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Configure view is displayed with the Rules tab open.
2. Click the **Settings** tab.
3. In the options panel, select **Enrichment Sources**.

Enrichment Sources						
Enabled	Name ^	Type	Description	Last Modified	Actions	
<input type="checkbox"/>	Default GeoIP	GeoIP	Default Geo IP Enrichment Source. This cannot be edited.	2015-05-13 10:11:34		
<input type="checkbox"/>	HrOrgChart	External DB Reference	Engineering organization in NE region	2015-05-13 10:11:34		
<input type="checkbox"/>	hrcsv	In-Memory Table	Employee information as of end of Q2	2015-05-13 10:13:58		

Page 1 of 1 | Page Size 25 | Displaying 1 - 3 of 3

4. In the **Enrichment Sources** section, click   > **In-Memory Table**.

In-Memory Table ✕

Upload Type: Adhoc Recurring

Enable

User-Defined Table Name*

Description

Import Data

Expert Mode

Table Columns + -

	Name	Type
<input type="checkbox"/>		

Key

Max Rows

Persist Stored File Format: Object JSON

[For information on how to define and use an In-Memory Table, see the documentation](#)

5. Describe the in-memory table:
- a. Select **Adhoc**.
 - b. By default, **Enable** is selected. When you add the in-memory table to a rule, alerts will be enriched with data from it.
If you add an in-memory table to a rule but do not want alerts to be enriched, deselect the checkbox.
 - c. In the **User-Defined Table Name** field, type a name, such as Student Information, for the in-memory table configuration.

- d. If you want to explain what the enrichment adds to an alert, type a **Description** such as:
When an alert is grouped by Rollno, this enrichment adds student information, such as name and marks.
6. In the **Import Data** field, select the .CSV file that will feed data to the in-memory table.
7. If you want to write an EPL query to define an advanced in-memory table configuration, select **Expert Mode**.
The Table Columns are replaced by a **Query** field.
8. In the **Table Columns** section, click **+** to add columns to the in-memory table.
9. If a valid file is selected in the Import Data field, the columns populate automatically.

Note: If you selected Expert mode, a Query field is displayed instead of Table Columns.

11. In the **Key** drop-down menu, select the field to use as the default key to join incoming events with the in-memory table when using a CSV-based in-memory table as an enrichment. By default, the first column is selected. You can also later modify the key when you open the in-memory table in enrichment sources.
12. In **Max Rows** drop-down menu, select the number of maximum number of rows that can reside in the in-memory table at a particular instance.
13. Select **Persist** to preserve the in-memory table on disk when the ESA service stops and to re-populate the table when the service restarts.
14. In **Stored File Format** field, do one of the following:
 - Select **Object**, if you want to store the file in a binary format.
 - Select **JSON**, if you want to store the file in a text format.By default, **Object** is selected.
15. Click **Save**.
The adhoc in-memory table is configured. You can add it to rule as an enrichment or part of the rule condition. See Add an Enrichment to a Rule.

When you add an in-memory table, you can add it to a rule as an enrichment or as a part of the rule condition. For example, the following rule uses an in-memory table as a part of the rule condition to create a whitelist, and it also uses an in-memory table of details in the user_dst file to enrich the alert that is displayed.

The rule shows the in-memory table as a whitelist rule condition:

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met + -

<input type="checkbox"/>	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	whitelist.User_list				
<input type="checkbox"/>	Username	is	event.user_dst	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Whitelist conditions can be added to exclude only those items defined in an enrichment list. Map a list column to an event meta key to join the list to the incoming data stream.

Next, the alert is enriched with the User_list in-memory table:

<input type="checkbox"/>	Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/>	In-Memory Table	User_list	user_dst	Username

Therefore, the user_dst in-memory table is used to create a whitelist, and it is also used to enrich the data in the alert if the alert is triggered.

Add a Recurring in-Memory Table

- In the **Security Analytics** menu, select **Alerts > Configure**.
The Configure view is displayed with the Rules tab open.
- Click the **Settings** tab.
- In the options panel, select **Enrichment Sources**.
- Click **+ > In-Memory Table**.
- Describe the in-memory table:
 - Click **Recurring**.
 - By default, **Enable** is selected. When you add the in-memory table to a rule, alerts will be enriched with data from it.
If you add an in-memory table to a rule but do not want alerts to be enriched, deselect the checkbox.

- c. In the **User-Defined Table Name** field, type a name, such as Student Information, for the in-memory table configuration.
 - d. If you want to explain what the enrichment adds to an alert, type a **Description** such as: When an alert is grouped by Rollno, this enrichment adds student information, such as name and marks.
6. Type the URL of the .CSV file that will feed data to the in-memory table. Click Verify to validate the link and populate the columns in the .CSV file. You can add or remove columns using the plus or minus button.
 7. If the server is configured behind another server, select **Use Proxy**.
 8. If the server requires logon credentials, select **Authenticated**
 9. For **Recur Every**, indicate how frequently ESA must check for the most recent .CSV:
 - a. Select Minute(s), Hour(s), Day(s), or Week.
 - b. If you select Week, select a day of the week.
 - c. Click **Date Range** to select a **Start Date** and **End Date** for the recurring schedule.

The image shows a user interface for selecting a date range. It features a 'Date Range' label with a small upward-pointing arrow icon to its left. Below this label are two input fields: 'Start Date' and 'End Date'. Each input field contains a calendar icon, indicating that a date picker is used for selection.

10. In the **Key** drop-down menu, select the field to use as the default key to join incoming events with the in-memory table when using a CSV-based in-memory table as an enrichment. By default, the first column is selected. You can also later modify the key when you open the in-memory table in enrichment sources.
11. In **Max Rows** drop-down menu, select the number of rows that can reside in the in-memory table at a particular instance.
12. Select **Persist** to preserve the in-memory table on disk when the ESA service stops and to re-populate the table when the service restarts.
13. In **Stored File Format** field, do one of the following:
 - Select **Object**, if you want to store the file in a binary format.
 - Select **JSON**, if you want to store the file in a text format.
By default, **Object** is selected.
14. Click **Save**.
The recurring in-memory table is configured. You can add it to rule as an enrichment or part of the rule condition. See [Add an Enrichment to a Rule](#).

Configure Warehouse Analytics as an Enrichment Source

This topic provides instructions on how to configure RSA Warehouse Analytics as an enrichment source for ESA. Data analysts can leverage RSA Analytics Warehouse data to analyze session and log data.

To configure Warehouse Analytics as an enrichment source:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
2. Click the **Settings** tab.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Alerts', 'Summary', and 'Configure'. The 'Configure' tab is active, and the 'Settings' sub-tab is selected. The left sidebar shows 'Miscellaneous' with 'Meta Key References' highlighted. The main content area displays a table titled 'Meta Key References' with a search bar and a refresh icon. The table lists various meta keys and their types. At the bottom of the table, it indicates 'Page 1 of 7' and 'Page Size 25'. The footer shows the user 'admin', language 'English (United States)', and time zone 'GMT+00:00'.

Name ^	Type
OS	string
access_point	string
accesses	string
action	string[]
ad_computer_dst	string
ad_computer_src	string
ad_domain_dst	string
ad_domain_src	string
ad_username_dst	string
ad_username_src	string
alert	string
alert_id	string

3. In the options panel, select **Enrichment Sources**.

The Enrichment Sources panel is displayed.

Enrichment Sources						
Enabled	Name ^	Type	Description	Last Modified	Actions	
<input type="checkbox"/>	Default GeolP	GeolP	Default Geo IP Enrichment Source. This cannot be edited.	2014-08-22 16:13:49		
<input type="checkbox"/>	MySQL1	External DB Re...	table - satest1	2014-08-22 16:13:49		
<input type="checkbox"/>	Table1	In-Memory Table	ip_src, hostname and user	2014-08-25 15:06:03		
<input type="checkbox"/>	Table2	In-Memory Table	ip_src, hostname, user, place and id	2014-08-25 15:06:42		
<input type="checkbox"/>	WarehouseAnalytics	Warehouse An...		2014-08-22 16:13:49		

Page 1 of 1 | Page Size 25 | Displaying 1 - 5 of 5

4. From the drop-down menu, select **Warehouse Analytics**.

Warehouse Analytics

Enable

Name *

Description

Warehouse Analytics Database URL *

Username

Password

5. Select **Enable** to enrich alerts with additional data. This is selected by default. If disabled, the alerts will not be enriched with additional data.
6. In the **Name** field, type a name to identify or label the Warehouse Analytics configuration.

7. In the **Description** field, type a brief description about the Warehouse Analytics configuration.
8. In the **Warehouse Analytics Database URL** field, type the MongoDB URL to the Warehouse Analytics database.
9. In the **Username** field, type the username to access the MongoDB.
10. In the **Password** field, type the password to access the MongoDB.
11. Click **Save**.

For more information, see [Settings Tab](#).



Add an Enrichment to a Rule

This topic tells how to add a previously configured enrichment source to a rule. When ESA creates an alert, information from the source gets included in it.

Adding an enrichment to a rule allows you to request for look ups into a variety of sources and include the results in the outgoing alerts, giving you a more detailed alert. This procedure requires role permissions for Administrator, DPO, and SOC Manager.

Procedure

To add an enrichment to a rule:

1. In the **Security Analytics** drop-down menu, select **Alerts > Configure**.
2. In the **Rule Library** view, do one of the following:
 - Double-click a rule.
 - Select a rule and click  in the **Rule Library** toolbar. The Rule Builder panel is displayed in a new Security Analytics tab.
3. In the **Enrichments** section, click  and select any of the following enrichment types:
 - In-Memory Table
 - External DB Reference
 - Warehouse Analytics
 - GeoIP

Note: If you use a GeoIP source, ipv4 is automatically populated, and is not editable.

The enrichment types that you have selected are displayed in the table.

4. For the added enrichment type, perform the following:
 - In the **Output** column, select the type that you have configured.
 - In the **Enrichment Source** drop-down list, select the enrichment source defined.
 - In the **ESA Event Stream Meta** field, type the event stream meta key whose value will be used as one operand of join condition.

Enrichments					Settings
	Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name	
<input checked="" type="checkbox"/>	In-Memory Table	Select Enrichment Source	Enter Meta	Enter Column Name	
<input type="checkbox"/>	External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name	
<input type="checkbox"/>	Warehouse Analytics	Select Enrichment Source	Enter Meta	key	
<input type="checkbox"/>	GeoIP	Select Enrichment Source	Enter Meta	ipv4	

- In the **Enrichment Source Column Name** field, type the enrichment source column name whose value will be used as another operand of the join condition.
5. Select **Debug**. This will add a `@Audit('stream')` annotation to the rule. This is useful when debugging the esper rules.
 6. Click **Show Syntax** to test if the defined ESA rule is valid.
 7. Click **Save**.

For details on parameters and their descriptions, see [Rule Builder Tab](#).

Deploy Rules to Run on ESA

This topic explains how to select an ESA and the rules to run on it. Administrator, SOC Manager or DPO role permissions are required for all tasks in this section.

To create a deployment, you need to perform the steps described in [Deployment Steps](#)

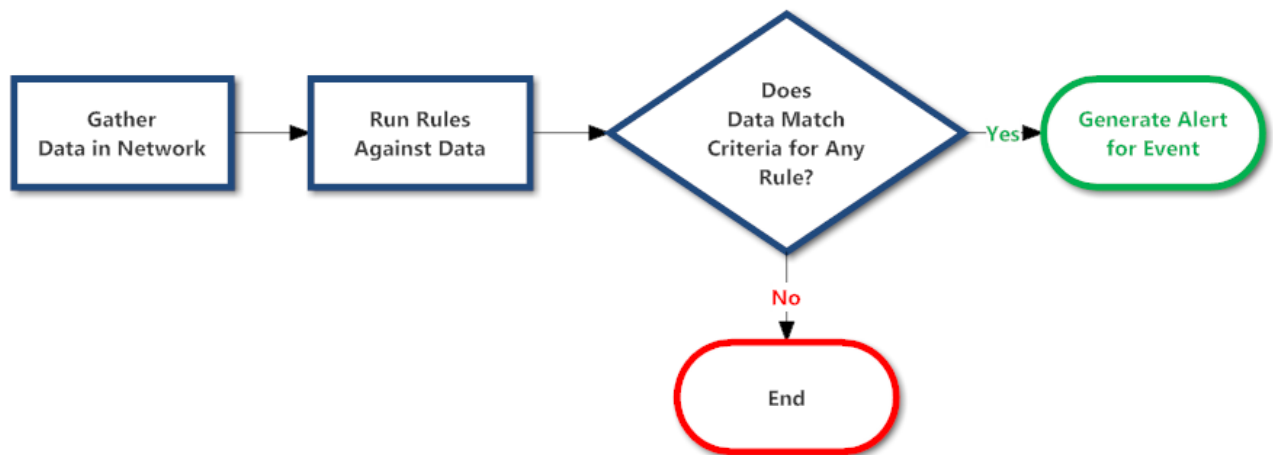
How Deployment Works

A deployment consists of an ESA service and a set of ESA rules. When you deploy rules, the ESA service runs them to detect suspicious or undesirable activity in your network. Each ESA rule detects a different event, such as when a user account is created and deleted within one hour.

The ESA service performs the following functions:

1. Gathers **data** in your network
2. Runs ESA **rules** against the data
3. Applies rule **criteria** to data
4. Generates an **alert** for the captured event

The following graphic shows this workflow:



In addition, you may want to perform other steps on your deployment, such as deleting an ESA service in your deployment, editing or deleting a rule from your deployment, editing or deleting a deployment, or showing updates to a deployment. For descriptions of these procedures, see [Additional Deployment Procedures](#)

Deployment Steps

This topic explains how to add a deployment, which includes an ESA service and a set of ESA rules. You can add a deployment to organize and manage ESA services and rules. Think of the deployment as a container for both components:

1. An ESA service
2. A set of ESA rules

For example, if you add a Spam Activity deployment it could include ESA London and a set of ESA rules to detect suspicious email activity.

To add a deployment, you need to complete the following procedures:

- [Step 1. Add a Deployment](#)
- [Step 2. Add an ESA Service](#)
- [Step 3. Add and Deploy Rules](#)

Step 1. Add a Deployment

Prerequisites

The following are required to add a deployment:

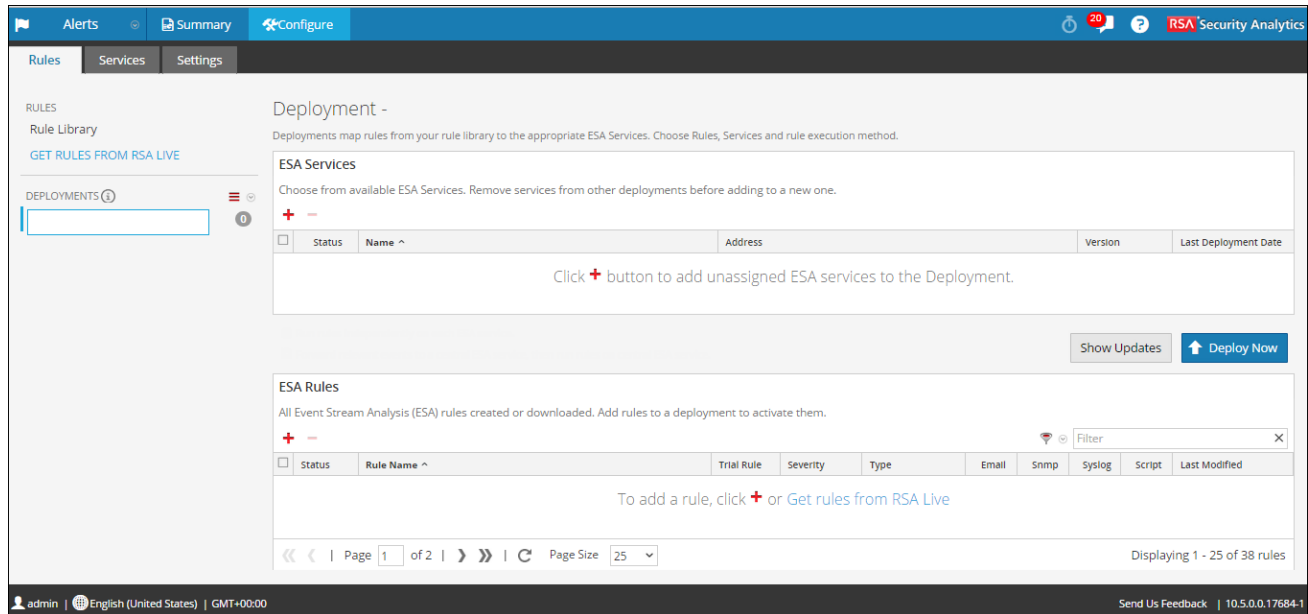
- The ESA service must be configured on the host. See "Configure ESA" in the **Event Stream Analysis (ESA) Configuration Guide**.
- Rules must be in the Rule Library. See [Add Rules to the Rule Library](#).

Procedure

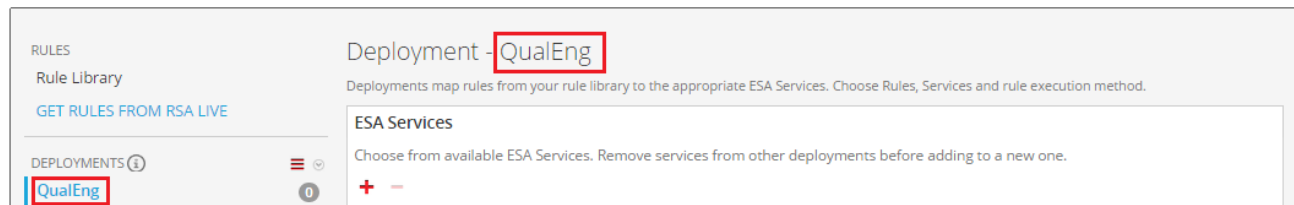
To add a deployment:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed.

2. In the options panel, next to Deployments, select  > **Add**.
The Deployment view is displayed on the right.



3. Type a **name** for the deployment. The naming convention is up to you.
For example, it could indicate the purpose or identify an owner.
4. Press **Enter**.
The deployment is added.



Step 2. Add an ESA Service

The ESA service in a deployment gathers data in your network and runs ESA rules against the data. The goal is to capture events that match rule criteria, then generate an alert for the captured event.

You can add the same ESA to multiple deployments. For example, ESA London could be in the these deployments simultaneously:

- Deployment EUR, which includes one set of ESA rules
- Deployment CORP, which includes another set of ESA rules

When you remove an ESA from a deployment, the rules are also removed from the ESA. For example, Deployment EUR could include ESA London and a set of 25 rules. If you remove ESA London from Deployment EUR, the 25 rules are also removed from ESA London. Consequently, if an ESA is not part of any deployment the ESA does not have any rules.

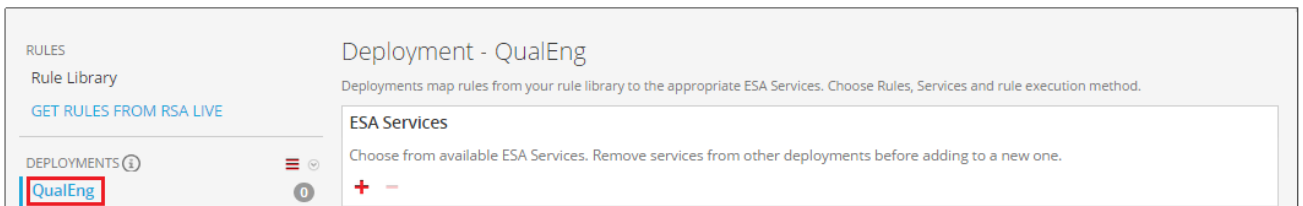
Procedure

To add an ESA service:

1. In the **Security Analytics** menu, select **Alerts > Configure**.

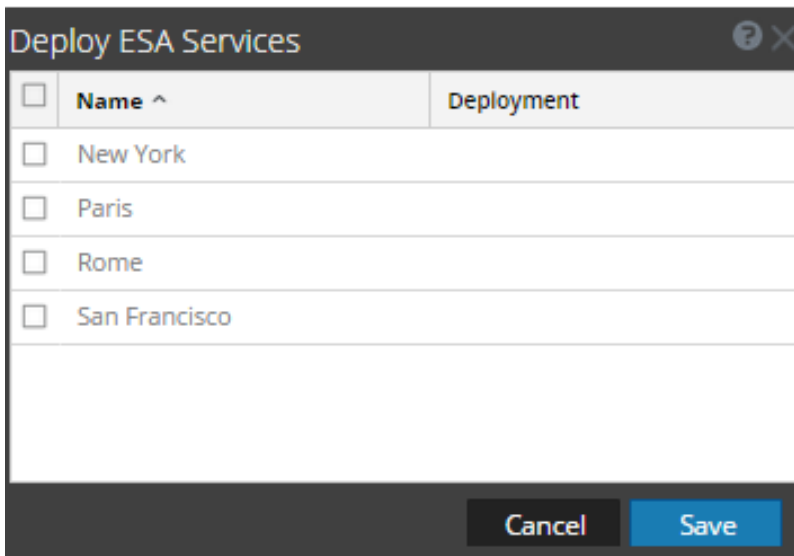
The Rules tab is displayed.

2. In the options panel, select a **deployment**:



3. In the **Deployment** view, click **+** in **ESA Services**.

The Deploy ESA Services dialog lists each configured ESA.



4. Select an ESA and click **Save**.

The Deployment view is displayed. The ESA is listed in the **ESA Services** section, with the status Added.

Step 3. Add and Deploy Rules

This topic explains how to add ESA rules to a deployment and then deploy the rules on ESA. Each ESA rule has unique criteria. The ESA rules in a deployment determine which events ESA captures, which in turn determine the alerts you receive.

For example, Deployment A includes ESA Paris and, among others, a rule to detect file transfer using a non-standard port. When ESA Paris detects a file transfer that matches the rule criteria, it captures the event and generates an alert for it. If you remove this rule from Deployment A, ESA will no longer generate an alert for such an occurrence.

Procedure

To add and deploy rules:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed.
2. In the options panel, select a deployment.
3. In the **Deployment** view, click **+** in **ESA Rules**.


The Deploy ESA Rules dialog is displayed and shows each rule in your Rule Library:

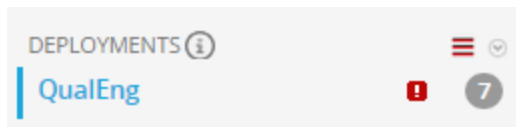
<input type="checkbox"/>	Rule Name ^	Description	Trial Rule	Type
<input type="checkbox"/>	ADActivity	User with admin rights performing high number of pri...	No	Advanced EPL
<input type="checkbox"/>	File Transfer Using Non Standard Port (Starter Pack)	File transferred using non-standard TCP destination po...	No	Rule Builder
<input type="checkbox"/>	Non DNS Traffic on TCP or UDP Port 53 Containing Exe...	Non DNS traffic on TCP or UDP port 53 containing exec...	No	Rule Builder
<input type="checkbox"/>	Non HTTP Traffic on TCP Port 80 Containing Executabl...	Non HTTP traffic on TCP port 80 containing executable...	No	Rule Builder
<input type="checkbox"/>	Non SMTP Traffic on TCP Port 25 Containing Executabl...	Non SMTP traffic on TCP port 25 containing executable...	No	Rule Builder
<input type="checkbox"/>	P2P software as detected by an Intrusion detection de...	P2P software as detected by an Intrusion detection de...	No	Rule Builder
<input type="checkbox"/>	User login from multiple geos over VPN within N secon...	Auto-generated from rule User login from multiple geo...	No	Advanced EPL
<input type="checkbox"/>	Windows Audit Log Cleared (Starter Pack)	Alert is fired when windows audit log(security log) is cl...	No	Rule Builder

Page 1 of 1 | Page Size 25 | Displaying 1 - 16 of 16 rules

Cancel Save

4. Select rules and click **Save**.
The Deployment view is displayed.
5. The rules are listed in the ESA Rules section.

- In the Status column, **Added** is next to each new rule.
- In the Deployments section,  indicates there are updates to the deployment.
- The total number of rules in the deployment is on the right.



6. Click **Deploy Now**.

The ESA service runs the rule set.

Additional Deployment Procedures

In addition to deploying an ESA service and rules, you may want to perform other steps on your deployment, such as deleting an ESA service in your deployment, editing or deleting a rule from your deployment, editing or deleting a deployment, or showing updates to a deployment.

To perform these procedures, go to:

- [Delete ESA Service in a Deployment](#)
- [Edit or Delete Rule in a Deployment](#)
- [Edit or Delete a Deployment](#)
- [Show Updates to a Deployment](#)


Delete ESA Service in a Deployment

This topic provides instructions to delete an ESA service in a deployment. On a deployment with a service, you can edit the rules which are applied to the service and delete the service from the deployment.

Each of the following procedures starts in the Rules tab.

Procedure

To delete an ESA service:

1. In the **Security Analytics** menu, select **Alerts > Configure > Rules**.
The Rules tab is displayed.
2. In the options panel, under **Deployments**, select a deployment.
3. In the **ESA Services** panel, select a service and click  in the toolbar.
A confirmation dialog is displayed.

4. Click **Yes**.

The service is deleted.

Edit or Delete Rule in a Deployment


On a deployment with rules, you can edit and delete rules to customize the deployment. Each of the following procedures starts in the Rules tab.

Procedures

Edit a Rule

1. In the Security Analytics menu, select Alerts > Configure > Rules.
The Rules tab is displayed.
2. In the options panel, under Deployments, select a deployment.
3. In the **ESA Rules** panel, double-click a rule to open it in a new Security Analytics tab.
4. Modify the rule, then click **Apply**.
The rule is saved.

Delete a Rule

1. In the **Security Analytics** menu, select **Alerts > Configure > Rules**.
The Rules tab is displayed.
2. In the options panel, under **Deployments**, select a deployment.
3. In the **ESA Rules** panel, select a rule and click  in the toolbar.
A confirmation dialog is displayed.
4. Click **Yes**.
The rule is deleted.

Edit or Delete a Deployment

This topic explains how Security Analytics forwards a correlation rule to each ESA service in a correlation group. In a correlation group, each ESA service must run the same set of rules. When you add a rule to a correlation group, Security Analytics forwards the rule to each ESA in the group.

To access the deployments:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Configure view is displayed with the Rules tab open.

- In the options panel, under **Deployments**, select a deployment.

The Deployment view is displayed.

The screenshot shows the 'Deployment - New' configuration page in the RSA Security Analytics interface. The page is divided into several sections:

- Navigation:** Alerts, Summary, Configure (active), and a user profile icon.
- Left Panel:** Rules, Services, Settings. Under 'RULES', there is a 'Rule Library' section with a link 'GET RULES FROM RSA LIVE >>'. Under 'DEPLOYMENTS', there is a 'new' button and a notification icon with the number '1'.
- Main Content Area:**
 - Deployment - New:** A heading followed by the instruction: 'Deployments map rules from your rule library to the appropriate ESA Services. Choose Rules, Services and rule execution method.'
 - ESA Services:** A section with the instruction: 'Choose from available ESA Services. Remove services from other deployments before adding to a new one.' It features a '+ -' button and a table with columns: Status, Name, Address, Version, Last Deployment Date. Below the table is a message: 'Click + button to add unassigned ESA services to the Deployment.'
 - Buttons:** 'Show 1 Updates' and 'Deploy Now'.
 - Rule Library:** A section with the instruction: 'All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.' It features a '+ -' button, a search filter, and a table with columns: Status, Rule Name, Trial Rule, Severity, Type, Email, Snmp, Syslog, Script, Last Modified. One rule is listed with status 'Added', name '<img ...', trial rule 'No', severity 'Low', type 'Advanced EPL', and last modified '2015-04-06 09:30:58'.
 - Footer:** Navigation arrows, 'Page 1 of 1', 'Page Size 25', and 'Displaying 1 - 1 of 1 rules'.

Edit a Deployment

- In the options panel, under **Deployments**, select a deployment.

The Deployment view is displayed.


- Select  > **Edit**.

The deployment name is made available for editing.

Delete a Deployment

- In the options panel, under **Deployments**, select a deployment.

The Deployment view is displayed.

- Select  > **Delete**.


A confirmation dialog is displayed.

- Click **Yes**.

The deployment is deleted.

Show Updates to a Deployment

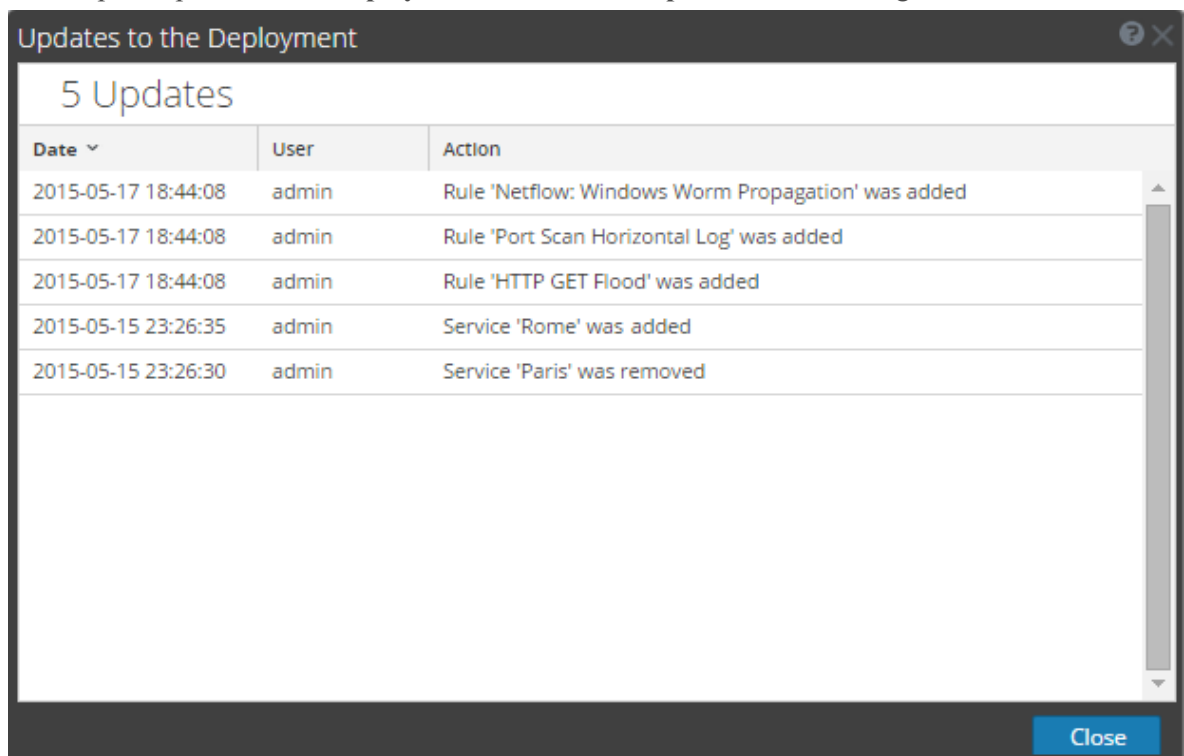
This topic explains how to show updates, such as adding or deleting rules, to a deployment.

When you make a change to a deployment, the update icon () appears next to the name of the deployment.

Procedure

To show the updates to a deployment:

1. In the Security Analytics menu, select Alerts > Configure.
The Rules tab is displayed.
2. In the options panel, under **Deployments** click **Show Updates** on the far right.



3. Click **Close**.

View ESA Stats and Alerts

When the ESA generates alerts, you can view details about how the rules performed, such as statistics on the engine, rule, and alert, and you can also view information on which rules are enabled or disabled. For instructions on viewing ESA stats, see [View Stats for ESA Service](#)

When your ESA generates alerts, you can view the results in the Alerts Summary page. This enables you to see trends and understand both the volume and frequency of alerts. For instructions on viewing alerts, see [View a Summary of Alerts](#)

View Stats for ESA Service

This topic describes how to view the deployment stats for an ESA service. This procedure is useful when you are attempting to determine the effectiveness of a rule or troubleshoot a deployment.

Procedures

View ESA Stats

1. In the **Security Analytics** menu, select **Alerts > Configure > Services**.
2. From the **ESA Services** list on the left, select a service.

The deployment stats for the selected service are displayed.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Alerts', 'Summary', and 'Configure'. The left sidebar shows 'ESA SERVICES' with a list: New York, Paris, Rome, and San Francisco (selected). The main content area is titled 'San Francisco' and contains the following sections:

- Engine Stats:**
 - Esper Version: 5.1.0
 - Time: 2015-05-17T23:05:29
 - Events Offered: 0
 - Offered Rate: 0 per second / 0 max
- Rule Stats:**
 - Rules Enabled: 7
 - Rules Disabled: 0
 - Events Matched: 0
- Alert Stats:**
 - Email: 0
 - SNMP: 0
 - Syslog: 0
 - Script: 0
 - Storage: 0
 - Message Bus: 0
- Deployed Rule Stats:**

Enable Disable See [Health & Wellness](#) to monitor rule memory usage.

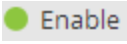

<input type="checkbox"/>	Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - P2P Software as Detected by an Intrusion Detection Device	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	ECAT alert with audit log cleared	No		0
<input type="checkbox"/>	<input checked="" type="radio"/>	HTTP GET Flood	Yes		0

Page 1 of 1 | Page Size 25 | Displaying 1 - 7 of 7

Footer: admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.5.0.0.17881-1

3. Review the following sections of ESA stats.
For a complete description of each statistic in each section, see [Services Tab](#).
 - **Engine Stats**
 - **Rule Stats**
 - **Alert Stats**
4. In the Deployed Rule Stats, review details about the rules deployed on the ESA.
For a complete description of each column in each section, see [Services Tab](#).
 - If the rule is enabled or disabled
 - What the rule name is
 - If the rule is running in Trial Rule mode
 - Last detected
 - Events matched
5. To get a snapshot of the rule memory, click **Health & Wellness**.


Enable or Disable Rules

1. In the **Deployed Rule Stats** panel, select a rule from the grid.
2. Click  to enable the rule, or click  to disable the rule.

The Services tab is refreshed to show the changes, which take effect immediately.

Refresh the Statistics

The Services tab does not update statistics automatically unless you enable or disable a rule. To ensure you view current statistics:

1. Click  in the upper right corner to refresh the information.
2. View the updated information.

View a Summary of Alerts

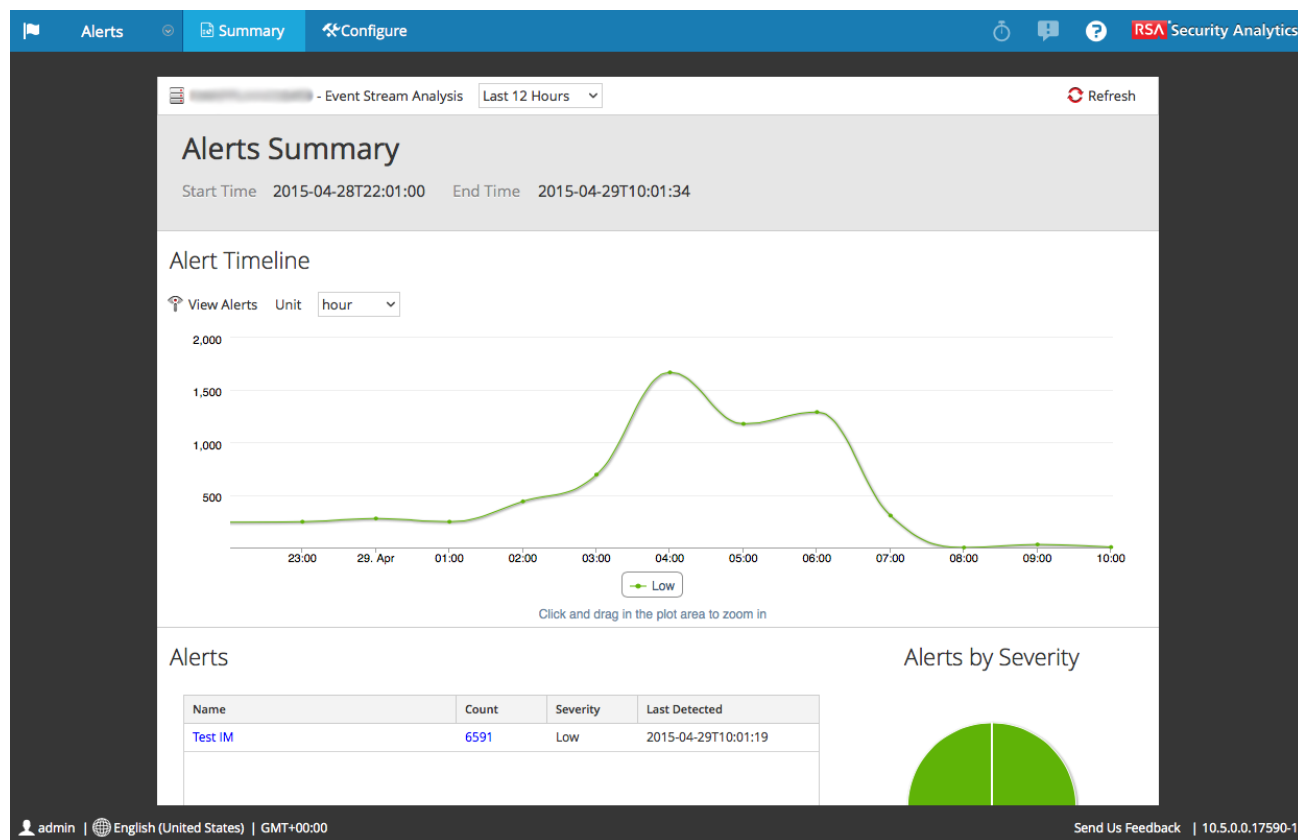
This topic describes how to view a summary of alerts. You can see a consolidated view of alerts generated in a specified time range.

Procedure


To view a summary of alerts:

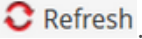
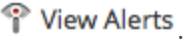
1. In the **Security Analytics** menu, select **Alerts > Summary**.

If there is a default ESA service, the Summary view is displayed with the information for that service.



If no default service has been selected, the Select an ESA Service dialog is displayed.

2. In the **Select an ESA Service** dialog, select a service and click **Select**.
The Summary view is displayed.
3. To choose a new service to view:
 - a. Click .
The Select an ESA Service dialog is displayed.
 - b. Select a service from the list and click **Select**.
The Summary view is displayed with the information for the chosen service.
4. To choose the timeframe of the summary, open the **Time Range** drop-down menu and select a time range.
The Start Time and End Time fields reflect the new range.
5. To choose the timeline, open the **Unit** drop-down menu and select a unit of time.

6. To refresh the information in the Summary view, click .
7. To view alerts in a list, click .
8. In the list view, you can see more details about each alert.

← Back to Summary					
Date	Name	Severity	# of Events	Alert Id	Statement
2017-06-21T04:15:52	Adv_ESA_rule	Low	1	0ea66d53-75aa-427a-ab75-02b8b...	RIG ip=6.4.2.2 LNOHPOLBYKDP71...
2017-06-21T04:11:30	Adv_ESA_rule	Low	1	5c52a73d-06f7-44ed-9a62-231ff02d...	RIG ip=6.4.2.2 LNOHPOLBYKDP71,0...
2017-06-21T03:18:44	Adv_ESA_rule	Low	1	d14dcbd7-e363-43da-9979-03903f...	RIG ip=6.4.2.2 LNOHPOLBYKDP71,0...
2017-06-21T03:17:25	Adv_ESA_rule	Low	1	018d5912-d3e5-43e5-b429-f80183...	RIG ip=6.4.2.2 LNOHPOLBYKDP71,0...
2017-06-21T03:01:33	Adv_ESA_rule	Low	1	9996d9dd-659b-49de-85f2-2f85536...	RIG ip=6.4.2.2 activity=Logon
2017-06-21T02:47:57	Adv_ESA_rule	Low	1	613039b3-eedf-44a9-b9de-021f72a...	RIG ip=6.4.2.2 activity=Logon
2017-06-21T02:46:11	Adv_ESA_rule	Low	1	2e1fdaff-ba8a-4541-9780-73fdc7ac...	RIG ip=6.4.2.2 domain=LNOHPOLB...
2017-06-21T02:44:25	Adv_ESA_rule	Low	1	454e3d06-ce73-40d8-b81f-b80d42...	RIG (ip_src3) LNOHPOLBYKDP71,09...
2017-06-20T13:07:38	Adv_ESA_rule	Low	1	64c8bb54-bf9b-4de3-bd14-899d14...	RIG (ip_src2) LNOHPOLBYKDP71,09...
2017-06-20T13:06:16	Adv_ESA_rule	Low	1	e44ad184-9383-4684-8b06-35e698...	RIG (ip_src2) LNOHPOLBYKDP71,09...
2017-06-20T13:06:00	Adv_ESA_rule	Low	1	af5d2c85-e4ab-49ce-839b-b28a46b...	RIG (ip_src2) LNOHPOLBYKDP71,09...
2017-06-20T13:02:56	Adv_ESA_rule	Low	1	215452df-cb1c-4feb-9854-bf43432...	RIG (ip_src2) LNOHPOLBYKDP71,09...
2017-06-20T13:02:44	Adv_ESA_rule	Low	1	85a52135-3ee6-4e77-b85c-e59259f...	RIG (ip_src2) LNOHPOLBYKDP71,09...
2017-06-20T12:55:47	Adv_ESA_rule	Low	1	10b4402b-1bf2-4f1a-9fda-818c711f...	RIG LNOHPOLBYKDP71,09:50:16 Lo...
2017-06-20T12:48:49	Adv_ESA_rule	Low	1	33a8351d-230d-4581-83dc-cdcd77...	RIG LNOHPOLBYKDP71,09:50:16 Lo...
2017-06-20T12:43:15	Adv_ESA_rule	Low	1	5ebeddc5-5a6d-4955-874b-3514ef0...	RIG LNOHPOLBYKDP71,09:50:16 Lo...
2017-06-20T12:41:03	Adv_ESA_rule	Low	1	0064b47b-ec5a-4ad7-ad20-48d064...	RIG LNOHPOLBYKDP71,09:50:16 Lo...
2017-06-20T12:39:54	Adv_ESA_rule	Low	1	2ca1ba24-abb0-4684-82d2-8acc0b...	RIG 6.4.2.2 LNOHPOLBYKDP71,09:5...
2017-06-20T12:07:18	Adv_ESA_rule	Low	1	085f14eb-aba9-4880-a582-2a28dd...	RIG 6.4.2.2 LNOHPOLBYKDP71,09:5...
2017-06-20T12:06:53	Adv_ESA_rule	Low	1	78691a4b-2740-4b75-b2eb-99c705...	RIG 6.4.2.2 LNOHPOLBYKDP71,09:5...
2017-06-20T12:06:07	Adv_ESA_rule	Low	1	7a2d6d6b-3c3c-47c5-b123-c239b75...	RIG 6.4.2.2 {alias_host} LogonUser...
2017-06-20T11:59:13	Adv_ESA_rule	Low	1	52052386-9376-405c-bbbf-b88e807...	RIG 6.4.2.2 {alias_host} LogonUser...
2017-06-20T11:59:00	Adv_ESA_rule	Low	1	2530bbd7-e652-412f-8446-d16310...	RIG 6.4.2.2 {alias_host} LogonUser...

Page 1 of 2 | 25 | Displaying 1 - 25 of 47

- Date-- date the alert was generated.
- Name--name of the alert.
- Severity-- severity of the alert. (low, medium, or high).
- # of Events-- the number of events associated with the alert.
- Alert ID-- unique ID for each alert.
- Statement - dynamically generated statement name.

Also, you can view a detailed summary of each alert generated by clicking an alert. The following figure shows more details about the alert generated.

Adv_ESA_rule

Description

Statement RIG ip=6.4.2.2 LNOHPOLBYKDP71,09:50:16 activity=Logon

Time 2017-06-21T04:15:52

Severity Low

Event Meta Events

Export Logs

Date	Id	Raw Content
2017-06-21T04:15:39	26678131	<4> Nov 16 09:50:16 ret7w001.ad.bankone.net MSWinEventLog,1,Security,6325213,Fri Nov 16 09:50:12 2007,528,Security,SYSTEM,User,Success Audit,DEVTERRM,Logon/Logoff,,Successful Logon: User Name: U408798 Domain: LNOHPOLBYKDP71 Logon ID: (0x0 0x1085AD0) Logon Type: 10 Logon Process: User32 Authentication Package: Negotiate Workstation Name: LNOHPOLBYKDP71 Logon GUID: {1830d565-61a2-0635-5082-c56634df7d6b} Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 6.4.2.2 Source Port: 0 ,6325212

Close

- Description - description of the alert.
- Statement - dynamically generated statement name.
- Time - time the alert was generated as per the timezone set on Security Analytics UI.
- Severity - severity of the alert (low, medium, high).
- Date- date the event was executed .
- ID- event ID.
- Raw Content - detailed information of the event.

For more information, see [Alerts Summary View](#).

Behavior Analytics Automated Threat Detection

This topic discusses how to configure and use Behavior Analytics Automated Threat Detection. Behavior Analytics Automated Threat Detection is a service you deploy on your ESA installation that examines your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

For details on how to work with Behavior Analytics Automated Threat Detection, see the following topics:

- [Configure Behavior Analytics Automated Threat Detection](#)
- [Work with Behavior Analytics Automated Threat Detection Results](#)
- [Troubleshoot Behavior Analytics Automated Threat Detection](#)

Understanding Behavior Analytics Automated Threat Detection

This topic provides an overview of Behavior Analytics Automated Threat Detection. Behavior Analytics Automated Threat Detection is a service you deploy on your ESA. The Behavior Analytics: Suspicious Domains module examines your HTTP traffic to detect domains likely to be malware command and control servers connecting to your environment. Once Behavior Analytics Automated Threat Detection examines your HTTP traffic, it generates scores based on various aspects of your traffic behavior (such as the frequency and regularity with which a given domain is contacted). If these scores reach a set threshold, an ESA alert is generated. This ESA alert also triggers an alert in the Incident Manager. The alert in the Incident Manager is enriched with data that helps you to interpret the scores to determine what mitigation steps to take.

This version of Behavior Analytics Automated Threat Detection provides scoring to detect Command and Control communications. Command and control communications occur when malware has compromised a system and is sending data back to a source. Often, Command and Control malware can be detected via beaconing behavior. Beaconing occurs when the malware regularly sends communications back to the Command and Control server to notify it that a machine has been compromised and the malware is awaiting further instructions. The ability to catch the malware at this stage of compromise can prevent any further harm from occurring to the compromised machine and is considered a critical stage in the "kill chain."

This feature solves several common problems that occur when searching for malware:

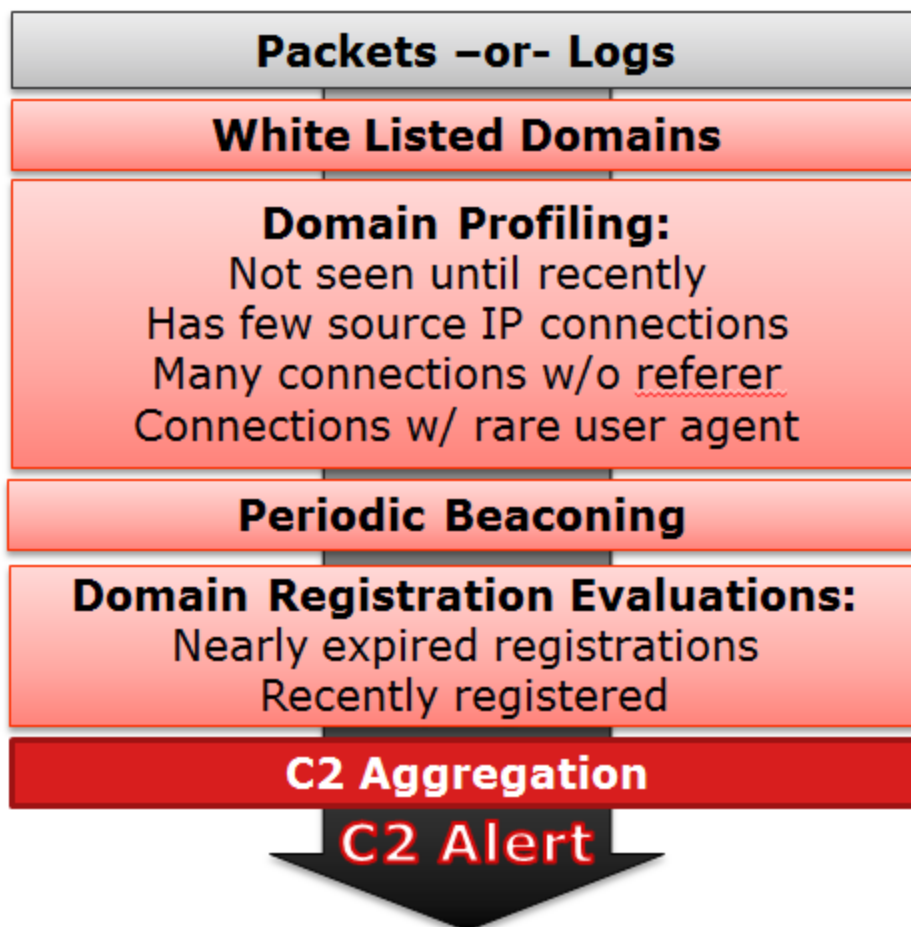
- **Ability to use algorithms rather than signatures.** Because many malware creators have begun using polymorphic or encrypted code segments which are very difficult to create a signature for, this approach can sometimes miss malware. Because Behavior Analytics Automated Threat Detection uses a behavior-based algorithm, it is able to detect malware

more quickly and effectively.

- **Ability to automate hunting.** Hunting through data manually is an effective but extremely time-consuming method of finding malware. Automating this process allows an analyst to use his or her time more effectively.
- **Ability to find an attack quickly.** Instead of batching and then analyzing the data, Behavior Analytics Automated Threat Detection analyzes data as it is ingested by Security Analytics, allowing for the attacks to be found in near real-time.

Workflow

Behavior Analytics Automated Threat Detection works much like a filtering system. It checks to see if certain behavior occurs (or certain conditions exist), and if that behavior or condition occurs, it moves to the next step in the process. This helps to make the system efficient, and frees up resources so that events which are determined to be non-threatening are not held in memory. The following diagram provides a simplified version of the workflow.



- 1.) **Packets or Logs are routed to the ESA.** The HTTP packets or logs are parsed by the Decoder or Log Decoder and sent to the ESA device.
- 2.) **Whitelist is checked.** If you created a whitelist via the Context Hub, the ESA checks this list to rule out domains. If a domain in the event is whitelisted, the event is ignored.
- 3.) **The domain profile is checked.** Behavior Analytics Automated Threat Detection checks to see if the domain is newly seen (approximately three days), has few source IP connections, has many connections without a referer, or has connections with a rare user agent. If one or several of these conditions is true, the domain is next checked for periodic beaconing. For a detailed description of these domain profile scores, see "Work with Behavior Analytics Automated Threat Detection Scores".
- 4.) **The domain is checked for periodic beaconing.** Beaconing occurs when the malware regularly sends communications back to the command and control server to notify it that a machine has been compromised and the malware is awaiting further instructions. If the site displays beaconing behavior, then the domain registration information is checked.
- 5.) **Domain registration information is checked.** The Whois service is used to see if the domain is recently registered or nearly expired. Domains that have a very short lifespan are often hallmarks of malware.
- 6.) **Command and control (C2) aggregates scores.** Each of the above factors generates a separate score which is weighted to denote various levels of importance. The weighted scores determine if an alert should be generated. If an alert is generated, the aggregated alerts appear in the Incident Manager and can then be investigated further from there. Once the alerts begin to appear in the Incident Manager, they continue to aggregate under the associated incident. This makes it easier to sort through volumes of alerts that can be generated for a command and control incident.

If you are an analyst, you can view the alerts generated in the Alerts Summary module, or in the Incident Manager module. If you use SecOps, you can view alerts in SecOps versions 1.2 and 1.3.

Behavior Analytics Automated Threat Detection on Packets vs. Web Proxy Logs

RSA Security Analytics provides you with the ability to perform Behavior Analytics Automated Threat Detection using either packets or Web Proxy Logs. While packet data can be streamed directly off of the wire into the Security Analytics installation and analyzed directly, if you have the ability to use a web proxy in your installation there may be benefits to doing so. Because some installations use network translation or SSL encryption, the true source IP of an outgoing connection may be masked if you are observing it at the packet level. By using a web proxy you gain the benefit of its ability to accelerate and decrypt SSL traffic as well as its ability to track the true source IP addresses of traffic it monitors.

Using Behavior Analytics Automated Threat Detection for Security Analytics 10.6.2 or later, you can use only one detection method: packets or logs, but not both for the same ESA instance. Multiple ESA instances may be used to aggregate data from both packet and web proxy log sources, however.

Configure Behavior Analytics Automated Threat Detection

This topic tells administrators and analysts how to configure and work with Behavior Analytics Automated Threat Detection.

This procedure provides the steps needed to configure Behavior Analytics Automated Threat Detection on your ESA. However, before you enable Behavior Analytics Automated Threat Detection, it is important to note that there are many potential installation configurations which may be installed on the ESA, including: Behavior Analytics Automated Threat Detection, ESA Rules, and the Context Hub. Each of these may take up resources, so it is important to have considered sizing before enabling this feature on your ESA.

Prerequisites

- If you are using Packet data, you must have configured a Decoder for HTTP packet data, and you must have configured an HTTP Lua or Flex parser.
- If you are using web proxy log data, you must have configured the appropriate Log Decoder with the correct parser for your web proxy.
- If you are using web proxy log data, you must have updated to the latest log parsers. The following parsers are supported Blue Coat ProxySG SGOS (cacheflowelff), and Cisco IronPort WSA (ciscoipportwsa) and Zscaler (zscalernss).
- You can use one mode per ESA appliance (either packets or logs, but not both).
- If you are using web proxy log data, for best results you should configure all web proxies the same way (set to the same time zone, and use the same collection method--syslog or batch, and if you use batch use the same batching cadence).
- You must have correctly configured the Incident Manager database.
- A connection from ESA appliance to the Whois service (same location as RSA Live cms:netwitness.com:443) must be opened on port 443. Verify with your System Administrator that this is completed.
- To whitelist a domain you need to enable the Context Hub service.
- You must have configured your Incident Manager database correctly. If you are unsure whether the Incident Manager database is configured correctly, review "Step 2. Configure a

Database for the Incident Management Service" in the "Incident Management Configuration Guide"

Important: Behavior Analytics Automated Threat Detection requires a "warm-up" period that acclimates the scoring algorithm to the traffic in your network. You should plan to configure Behavior Analytics Automated Threat Detection so that the warm-up period can be run during normal traffic. For example, starting Behavior Analytics Automated Threat Detection on a Tuesday at 8:00 am in the timezone which contains the majority of your users allows the module to accurately analyze a day of normal traffic.

Procedure: Configuring Behavior Analytics Automated Threat Detection

This procedure provides the steps needed to configure Behavior Analytics Automated Threat Detection.

The basic steps required are:

1. **Configure Log Settings (for Log Customers only)** Before you can use Behavior Analytics Automated Threat Detection for Logs, you must configure several settings. *Skip this step if you plan to use Behavior Analytics Automated Threat Detection for Packets.*
2. **Create a whitelist (optional) using the Context Hub service.** Creating a whitelist allows you to ensure that commonly accessed websites are excluded from any Behavior Analytics Automated Threat Detection scoring.
3. **Enable Behavior Analytics Automated Threat Detection for your specified ESA.** You need to enable Behavior Analytics Automated Threat Detection for each ESA where you want the service to run.
4. **Configure WhoIs settings.** The Whois Service allows you to get accurate data about domains that you connect to. In order to ensure effective scoring, it is important that you configure the Whois service settings.
5. **Verify that the Whois Service is reachable from your environment.** For Behavior Analytics Automated Threat Detection to perform correctly, it is essential that the Whois service is reachable. Once Behavior Analytics Automated Threat Detection is running, you can verify the service is connecting.
6. **Verify the C2 Incident Manager rule is enabled and monitor for activity.** When using Behavior Analytics Automated Threat Detection, a period of time is required for the scoring algorithm to warm-up. After the warm-up period, verify the C2 rule is enabled on Incident Manager and monitor to see if the rule is triggered.



7. **Verify that the Rule in the Incident Manager is configured correctly.** When you view incidents in the Incident Manager, it's helpful if the incidents are grouped by the Suspected C&C domain.

Step 1: (For Log Customers Only) Configure Log Settings

To configure Behavior Analytics Automated Threat Detection for Logs, you need to complete a few extra configuration steps:

- Verify that the supported parsers are enabled for your Log Decoder.
- You must get the latest versions of the appropriate web proxy parser from RSA Live.
- Update the mapping on the Envision config file. This file is required to update the Log Decoder to work with the new meta available via the parsers.
- Verify that the *table-map.xml* file got updated correctly.
- Verify that the indexes have been updated correctly.

To verify your parsers are running on your Log Decoder:

1. Go to **Administration > Services >** and select your Log Decoder.
2. Select your Log Decoder, then   **> View > Config.**
3. In the Service Parsers Configuration pane is a list of enabled parsers.
4. Verify that the appropriate web proxy parser is enabled.

The screenshot displays the RSA Security Analytics configuration interface. The top navigation bar includes tabs for Administration, Hosts, Services, Event Sources, Health & Wellness, System, and Security. The current view is the 'Config' section, with sub-tabs for General, Files, Data Retention Scheduler, App Rules, Correlation Rules, Feeds, Parsers, Parser Mappings, and Data Privacy. The 'Parsers' tab is active, showing three configuration panels:

- System Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56002
Stat Update Interval	1000
Threads	20
- Log Decoder Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
Adapter	
Berkeley Packet Filter	
Capture Interface Selected	log_events, Log Events
Cache	
Cache Directory	/var/netwitness/cache
Cache Size	4 GB
Capture Settings	
Assembler Maximum Size	32 MB
Assembler Minimum Size	0
Assembler Session Flush	1
Assembler Session Pool	50000
Assembler Timeout Packets	60
Assembler Timeout Session	60
Capture Autostart	<input checked="" type="checkbox"/>
Capture Buffer Size	32 MB
Parse Maximum Bytes	128 KB
- Parsers Configuration:** A table with columns 'Name' and 'Config Value'.

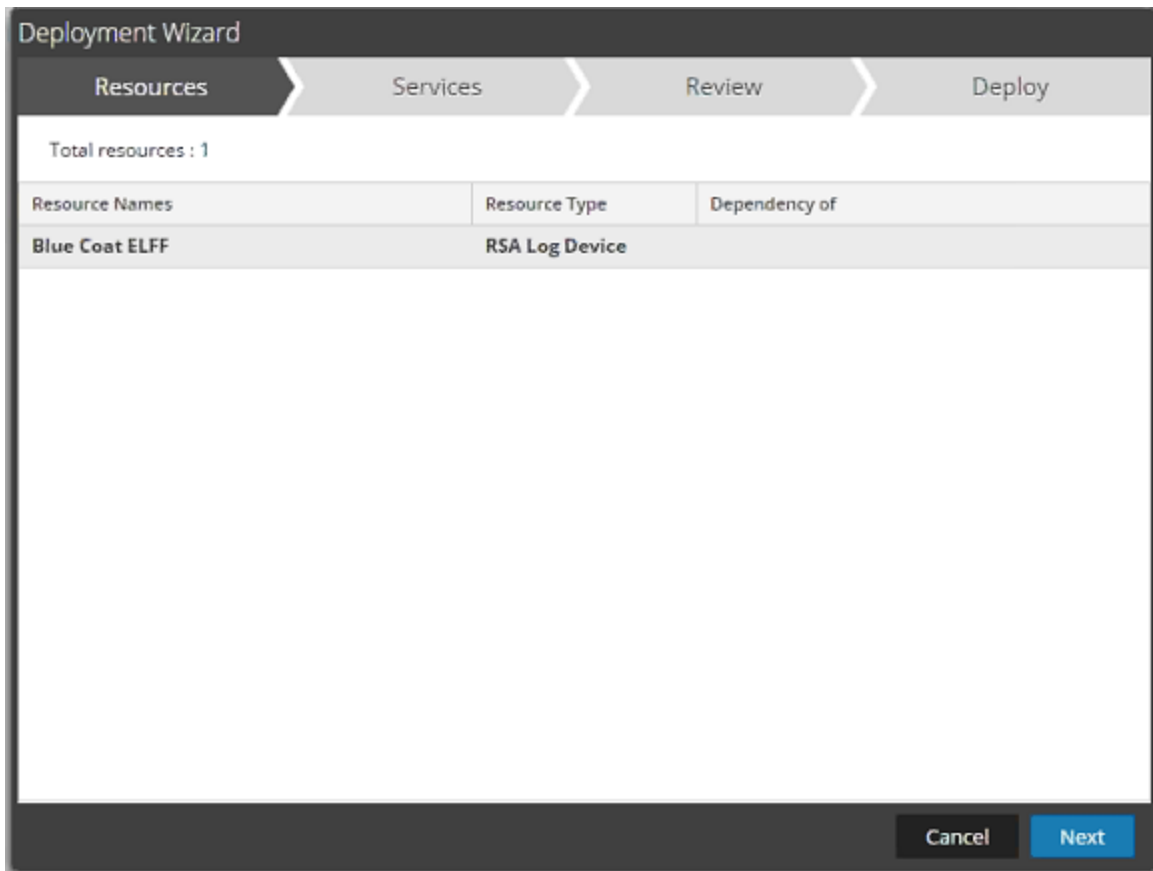
Name	Config Value
<input checked="" type="checkbox"/> ALERTS	Enabled
<input checked="" type="checkbox"/> FeedParser	Enabled
<input checked="" type="checkbox"/> GeoIP	Disabled
<input checked="" type="checkbox"/> Log Parser	Enabled
<input checked="" type="checkbox"/> LogTokens	Enabled
<input checked="" type="checkbox"/> NETWORK	Enabled
- Service Parsers Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
ciscoidsxml	<input checked="" type="checkbox"/>
ciscoportesa	<input checked="" type="checkbox"/>
ciscoportwsa	<input checked="" type="checkbox"/>
ciscolms	<input checked="" type="checkbox"/>
ciscomars	<input checked="" type="checkbox"/>
ciscomeraki	<input checked="" type="checkbox"/>
ciscomse	<input checked="" type="checkbox"/>
cisconac	<input checked="" type="checkbox"/>
cisconcm	<input checked="" type="checkbox"/>
cisconxos	<input checked="" type="checkbox"/>
ciscopix	<input checked="" type="checkbox"/>
ciscorouter	<input checked="" type="checkbox"/>

An 'Apply' button is located at the bottom center of the configuration area. The footer of the interface shows 'RSA Security Analytics', user 'admin', last login 'Thursday, August 25, 2016 6:02:52 PM UTC', language 'English (United States)', time zone 'GMT+00:00', and version '10.6.1.0'.

To get the latest parsers from RSA Live:

1. Go to **Live > Search**.
2. Enter a search term for one of the supported web proxy parsers.
3. Select the appropriate web proxy parser (for example, the Blue Coat ProxySG SGOS (cacheflowelff) parser). Note: you should have taken steps to correctly configure logging to occur on your web proxy parser correctly.
4. Click **Deploy**. The Deployment Wizard opens.



- 5.
6. Under **Services**, select the Log Decoder as the Service.
7. Click **Deploy** to deploy the parser to your Log Decoder.

To Get the Latest Envision Config File:

1. Go to **Live > Search**.
2. Enter **envision** as the key word for the search.

3. Select the latest Envision Config file, and click **Deploy**, and the Deployment Wizard opens.

The screenshot shows the RSA Live interface with the 'Matching Resources' table. The table has columns for 'Subscribed', 'Name', 'Created', 'Updated', 'Type', and 'Description'. The 'Envision Config File' resource is selected, and the 'Deploy' button is highlighted.

Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	Envision Content File	2012-02-09 4:44 PM	2016-07-25 8:21 AM	RSA Log Device	This file is used to update the content file for NWFL, Event So
<input checked="" type="checkbox"/>	Envision Config File	2014-03-07 4:50 PM	2016-08-02 5:42 PM	RSA Log Device	This file is used to update the Log Device base config files
<input type="checkbox"/>	Cisco Secure IDS.XML	2014-02-14 3:24 AM	2015-12-01 9:31 PM	RSA Log Device	Log device content for event source Cisco Secure IDS.XML - c
<input type="checkbox"/>	Snort/Sourcefire	2014-02-14 3:49 AM	2016-07-19 12:11 PM	RSA Log Device	Log device content for event source Snort/Sourcefire - snort,
<input type="checkbox"/>	Blue Coat ELFF	2014-02-14 3:23 AM	2016-07-29 4:00 PM	RSA Log Device	Log device content for event source Blue Coat ELFF - cachello
<input type="checkbox"/>	Fortinet FortiGate	2014-02-14 3:32 AM	2016-08-17 2:09 PM	RSA Log Device	Log device content for event source Fortinet FortiGate - fortir
<input type="checkbox"/>	Windows Events (NIC)	2014-02-14 3:55 AM	2016-08-17 8:12 PM	RSA Log Device	Log device content for event source Windows Events (NIC) - v
<input type="checkbox"/>	Tipping Point	2014-02-14 3:52 AM	2015-04-15 7:53 PM	RSA Log Device	Log device content for event source Tipping Point - tippingpo
<input type="checkbox"/>	Dragon IDS	2014-02-14 3:29 AM	2015-12-01 9:31 PM	RSA Log Device	Log device content for event source Dragon IDS - dragonids, I
<input type="checkbox"/>	Symantec AntiVirus/Endpoi...	2014-02-14 3:51 AM	2016-07-04 10:34 AM	RSA Log Device	Log device content for event source Symantec AntiVirus/Endf
<input type="checkbox"/>	Linux	2014-02-14 3:46 AM	2016-07-07 9:31 AM	RSA Log Device	Log device content for event source Linux - rhlinux, Parser Ve
<input type="checkbox"/>	Cisco Secure ACS Appliance	2014-02-14 3:26 AM	2016-08-02 11:16 AM	RSA Log Device	Log device content for event source Cisco Secure ACS Appliar
<input type="checkbox"/>	Microsoft Exchange	2014-02-14 3:41 AM	2016-08-05 10:02 AM	RSA Log Device	Log device content for event source Microsoft Exchange - ms
<input type="checkbox"/>	McAfee ePolicy Orchestrator	2014-02-14 3:31 AM	2016-08-16 1:01 PM	RSA Log Device	Log device content for event source McAfee ePolicy Orchestr
<input type="checkbox"/>	Cisco ASA	2014-02-14 3:24 AM	2016-08-17 2:09 PM	RSA Log Device	Log device content for event source Cisco ASA - ciscoasa, Par
<input type="checkbox"/>	IntruShield	2014-02-14 3:36 AM	2015-11-23 9:50 AM	RSA Log Device	Log device content for event source IntruShield - intrushield,
<input type="checkbox"/>	ISS Realsecure	2014-02-14 3:37 AM	2015-12-01 9:31 PM	RSA Log Device	Log device content for event source ISS Realsecure - iss, Pars
<input type="checkbox"/>	Netscreen IDP	2014-05-06 5:01 PM	2015-12-01 9:32 PM	RSA Log Device	Log device content for event source Netscreen IDP - netscree
<input type="checkbox"/>	iSeries	2014-02-14 3:36 AM	2015-12-10 9:25 AM	RSA Log Device	Log device content for event source iSeries - iseries, Parser V
<input type="checkbox"/>	Infoblox NIOS	2014-02-14 3:36 AM	2016-05-03 11:59 AM	RSA Log Device	Log device content for event source Infoblox NIOS - infoblox
<input type="checkbox"/>	IBM WebSphere	2014-02-14 3:35 AM	2016-06-14 10:31 AM	RSA Log Device	Log device content for event source IBM WebSphere - ibmw



4. Under **Services**, select your Log Decoder.
5. Click **Deploy** to deploy the Envision configuration file to the Log Decoder.

To Verify the Envision Configuration File was Updated Correctly:

1. Under **Administration > Services > Log Decoder**, Files, you can see the table-map.xml file. This file is modified when you update the Envision Configuration file.
2. Search for the term, *event.time*. The field should now read, "*event.time*" flags = "*None*". This means the event.time meta is now included in the mapping. Similarly, the fqdn flag should be set to "*None*".

To Verify the Indices for the index-concentrator.xml File is Updated:

You will need to verify that the index-concentrator.xml file includes both the event.time and fqdn meta.

1. Go to **Administration > Services** and select your Concentrator.
2. Select your Concentrator, then   > **View > Config**.
3. In the Files directory, search for the index-concentrator.xml file.
4. Verify that the following entry exists in your index-concentrator.xml file. If not, you'll need to ensure your Concentrator is upgraded to the correct version:

```
<key description="FQDN" level="IndexValues" name="fqdn"
format="Text" valueMax="100000" defaultAction="Open"/><key
description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="0" />
```

The screenshot shows the configuration interface for the 'Files' tab. The configuration is for 'index-concentrator.xml' on a 'Concentrator'. The XML code is displayed in a text area, and the 'FQDN' and 'Event Time' keys are highlighted with a red circle. The code includes several key descriptions, with the 'FQDN' and 'Event Time' keys highlighted by a red circle.

```
<!-- Additional Elements -->
<key description="Network Name" level="IndexValues" name="netname" format="Text" valueMax="10000"/>
<key description="Traffic Flow Direction" level="IndexValues" name="direction" format="Text" valueMax="10000"/>
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/>
<key description="Event Time" format="TimeT" level="IndexValues" name="event.time" valueMax="0" />

<!-- Additional Elements -->
<key description="Investigation Category" level="IndexValues" name="inv.category" format="Text" valueMax="10000"/>
<key description="Investigation Context" level="IndexValues" name="inv.context" format="Text" valueMax="10000"/>

<!-- Additional Elements -->
<key description="Session Analysis" level="IndexValues" name="analysis.session" format="Text" valueMax="10000"/>
<key description="Service Analysis" level="IndexValues" name="analysis.service" format="Text" valueMax="10000"/>
<key description="File Analysis" level="IndexValues" name="analysis.file" format="Text" valueMax="10000"/>
<key description="Indicators of Compromise" level="IndexValues" name="ioc" format="Text" valueMax="10000"/>
<key description="Behaviors of Compromise" level="IndexValues" name="boc" format="Text" valueMax="10000"/>
<key description="Enablers of Compromise" level="IndexValues" name="eoc" format="Text" valueMax="10000"/>

</language>
```




An 'Apply' button is visible at the bottom right of the configuration area.

Step 2: Create a Domains Whitelist (Optional)

Note: This step is optional: if you use the Incident Manager to manage these incidents, you can also create a whitelist by closing an incident as false-positive.


This procedure is used when working with Behavior Analytics Automated Threat Detection to ensure that certain domains do not trigger a threat score. Sometimes, a domain you access regularly may trigger an Behavior Analytics Automated Threat Detection score. For example, a weather service might have similar beaconing behavior as a Command and Control communication, thus triggering an unwarranted negative score. When this happens, it's called a false positive. To prevent triggering a false positive with a specific domain you can add the domain to a whitelist. Most domains do not need to be whitelisted because the solution only alerts on very suspect behaviors. The domains you may want to whitelist are valid automated services which few hosts connect to.

Note: You can have only one Context Hub service instance enabled in your Security Analytics deployment. If your Context Hub service is running on a different ESA, you need to configure it to connect to the ESA that runs the Context Hub service. For instructions, see "Configure an ESA to Connect to the Context Hub on Another ESA" in the **Event Stream Analysis Configuration Guide**.

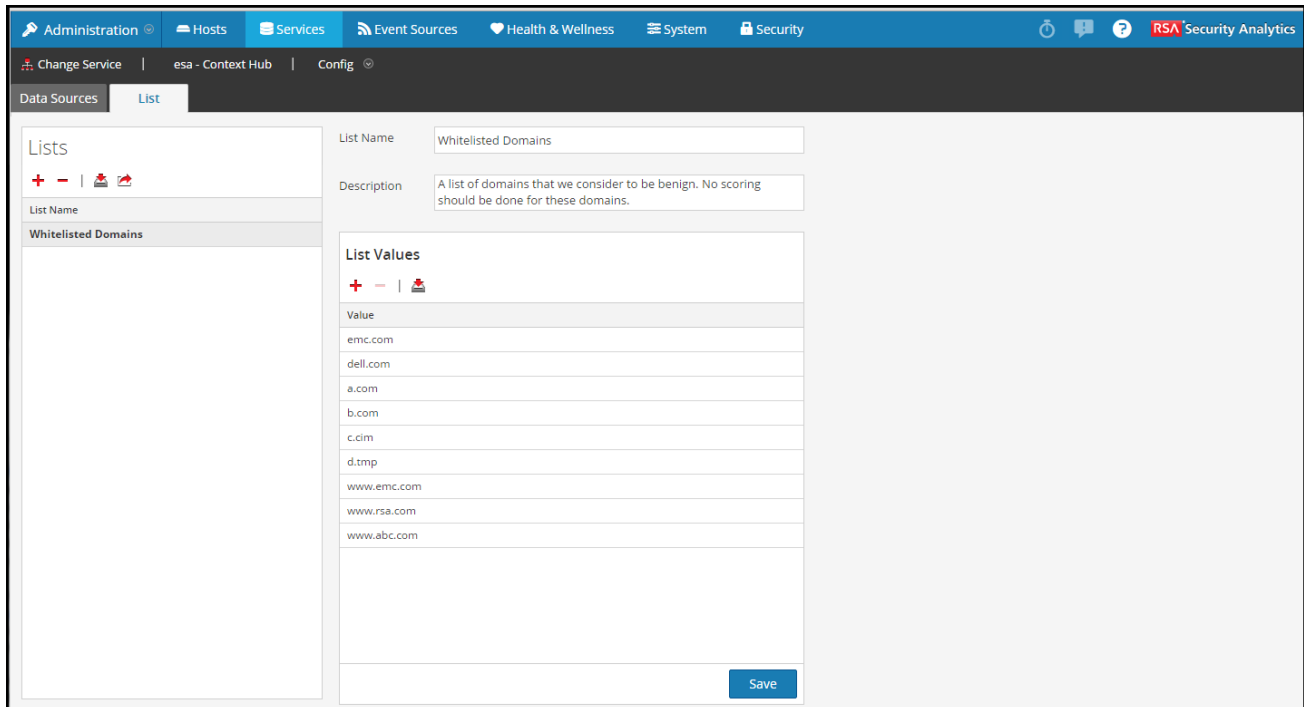
1. From the Context Hub Service, you can create a list and manually add domains, or you can upload a .CSV file containing a list of domains.
 - a. From **Administration > Services**, select the Context Hub.
 - b. Select the Context Hub, then  > **View > Config**.
 - c. Select the **List** tab to open the Lists for editing.
 - d. In the left pane, click  to add a list. Enter a name for the list and then manually add domains by clicking  in the right pane.




You can enter full domains, or you can use a wild card to include all sub-domains for a given domain. For example, you can enter *.gov to whitelist all government IP addresses. However, you cannot use other regex functions, such as [a-z]*.gov. This is because using *.gov replaces an entire string, such as www.irs.gov.

Caution: The whitelist must be named *Whitelisted Domains*. Otherwise, the Context Hub will not be able to process the list as a whitelist.


- e. Or, to import a .CSV file, click , and in the Import File dialog box, navigate to the .CSV file. Note that the file must be named *Whitelisted Domains*. Choose from the following delimiters: Comma, LF (Line Feed), and CR (Carriage Return) depending on how you have separated the values in your file. Then click **Upload**.
- f. From the Context Hub Service, you can also modify an existing whitelist to add or remove a domain.

- g. In the right pane, **List** displays your existing domain whitelist.
- h. Click **Whitelisted Domains**. The values for the whitelist display in the right pane.



- i. To add a domain, click  and enter the domain name.
- j. To remove a domain, select the domain and click .
- k. To import a .CSV file, click , and in the Import File dialog box, navigate to the .CSV file. Choose from the following delimiters: Comma, LF (Line Feed), and CR (Carriage Return) depending on how you have separated the values in your file. Then click **Upload**.

Step 3: Enable Behavior Analytics Automated Threat Detection and Enable the Whois Lookup Service

1. From Administration > Services, select your ESA service and then  > View > Config.
2. Click on the Advanced tab, and select **Enable Automated Threat Detection**, then choose either Automated Threat Detection for Packets or Automated Threat Detection for Logs (if

you want to perform C2 Detection on web proxy logs).

Data Sources **Advanced**

Alert Engine

Max Constituent Events

Forward Alerts On Message Bus

Debug Rules?

Apply

Event Stream Engine

Max Pattern Subexpressions

Apply

Automated Threat Detection

IMPORTANT: Depending on traffic volumes Automated Threat Detection can require significant memory and computation resources. Before enabling Automated Threat Detection please read the [product documentation](#) to fully understand the benefits and requirements. RSA recommends deploying Automated Threat Detection on dedicated hardware for best performance.

Enable Automated Threat Detection

Configuration Automated Threat Detection for Packets
 Automated Threat Detection for Logs

A warm-up period is required to allow Automated Threat Detection to acclimate to your traffic. During this time, alerting for Automated Threat Detection is suppressed. To stop an existing warm-up period, enter a warm-up duration of 0 and click Apply.

Warm-Up Duration (HH)

Warm-Up Time Remaining (HH:mm)

Apply

Whois Lookup Service configuration

IMPORTANT: Whois service connectivity is required for C2 threat detection. C2 threat detection accuracy will be dramatically reduced without whois service connectivity. Live credentials are used, hence make sure to configure live before enabling this

Enable Whois Lookup Service

Apply

1. Set a warm-up duration. A warm-up period is required to allow Behavior Analytics Automated Threat Detection to acclimate to your traffic. During this time, alerting is suppressed. Set the warm-up duration in hours. RSA recommends a warm-up period of 24 hours. After this warm-up period, alerts can be viewed. If the ESA restarts, this warm-up period starts over, so the time is reset. To stop an existing warm-up, enter 0 for the Warm-up Duration value, and click **Apply**.

Note: When you set the warm-up period, it should be run when typical traffic is running. This enables Behavior Analytics Automated Threat Detection to create a scoring model based on typical behavior in your network. For example, if you set the warm-up period to run over a weekend, the Behavior Analytics Automated Threat Detection creates a model based on traffic that is both lower than and different from typical weekday traffic. A better solution would be to run the warm-up period on a weekday starting at 8 a.m. to ensure the model reflects normal traffic.

2. Click Enable Live Whois Lookup to enable the Whois service for your ESA. This allows your ESA service to obtain detailed information about the domain that triggers the Behavior Analytics Automated Threat Detection score. By default, the Whois service uses the same User ID and password as your RSA Live User ID and password. If you have not configured an RSA Live account, you will need to do so prior to enabling the Whois service.



Behavior Analytics Automated Threat Detection and Whois Live Lookup are now enabled on your selected ESA. Once you enable the Whois Live Lookup, you can specify other Whois Lookup settings from the Explorer by following the instructions in Step 3: Configure the Whois Service Settings for your ESA.

Note: A rule is added to perform C2 detection. However, this rule "Suspect C&C" ESA rule," is not visible in the User Interface for editing. The rule is not editable, and to prevent accidental deletion or modification, the rule is hidden from view. You can view the associated Incident Manager rule and results in the Incident Manager, however.

Step 4: Configure Advanced Whois Service Settings for your ESA

If you did not configure the Whois Lookup service in the previous step or if you want to configure advanced settings, you can do so now.

Warning: The Whois service is critical for accurate Behavior Analytics Automated Threat Detection scoring. If you do not configure the Whois service, excessive alerting can occur.

1. From **Administration > Services**, select your ESA service and then   > **View > Explore**.
2. In the Explorer, click **Service > Whois > whoisClient**.

3. Configure the following settings (note that only the first two parameters require modification. RSA recommends you use the default settings for other parameters):

Parameter	Description
whoisUserId	<p>Required only if you did not already enable the Whois service. Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live User ID. If you have not configured an RSA Live account, you will need to do so.</p> <p>The default value is "whois".</p>
whoisPassword	<p>Required only if you did already enable the Whois service. Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live password. If you have not configured an RSA Live account, you will need to do so.</p> <p>The default value is null.</p>
whoisUrl	<p>Optional: Enter the URL to obtain Whois data from the RSA Whois Service. Note that the trailing slash ("/") is required. Otherwise, requests will fail.</p> <p>The default value is: "https://cms.netwitness.com/whois/query/"</p>
whoisAuthUrl	<p>Optional: Enter the URL to obtain authentication tokens from the RSA Whois Service.</p> <p>The default value is: " https://cms.netwitness.com/authlive/authenticate/WHOIS"</p>
whoisAuthTokenLifespanSeconds	<p>Optional: Enter the time, in seconds, after which an authentication token should be renewed.</p> <p>The default value is 3300.</p>
whoisHttpsProxy	<p>Optional: If HTTP requests require a proxy, set this to the same value as is used for the RSA Live service. Only use this parameter when insecureConnection is set to true.</p> <p>The default value is false.</p> <p>(Requires an ESA restart to take effect.)</p>

Parameter	Description
insecureConnection	<p>Optional: Set this parameter to true to allow the HTTP request to the RSA Whois Service ignore SSL certs.</p> <div data-bbox="634 373 1323 470" style="border: 1px solid green; padding: 5px;"> <p>Note: If the RSA Whois Service is accessed via a proxy, this parameter should be set to true.</p> </div> <p>The default value is false. (Requires an ESA restart to take effect.)</p>
allowedRequests	<p>Optional: Enter how many queries you want to allow before you start throttling the Whois service. This parameter works with <code>allowedRequestsIntervalSeconds</code>, where you set the interval for queries. For example, if you set allowedRequests to 100 and allowedRequestsIntervalSeconds to 60, you are allowed 100 requests in any 60 second interval.</p> <p>The default value is 100. (Requires an ESA restart to take effect.)</p>
allowedRequestsIntervalSeconds	<p>Optional: If you set the allowedRequests parameter, you need to also configure this setting to determine the interval. This value should be tuned for your environment.</p> <p>The default setting is 60 seconds. (Requires an ESA restart to take effect.)</p>
queueMaxSize	<p>Optional: Specify the maximum size of the queue of the domains whose information will be requested of the RSA WhoisService.</p> <p>The default is 100,000.</p>
cacheMaxSize	<p>Optional: Specify the maximum number of cached Whois entries. Once this limit is reached, the least recently used entry will be removed to accommodate a new entry.</p> <p>The default is 50,000. (Requires an ESA restart to take effect.)</p>

Parameter	Description
refreshIntervalSeconds	<p>Optional: Specify the number of seconds for the refresh interval. If requested Whois information is found in the cache, and the cache entry has been there for more than the specified number of seconds, the entry is removed from the cache and the domain returned to the queue to be looked up. (The cache entry is returned for the request that identified it as stale.)</p> <p>The default setting is 2,592,000 seconds (30 days).</p>
waitForHTTPRequest	<p>Optional: Requires that the ESA wait for the Whois service to respond before it can complete running the EPL. This ensures that the Whois data is always included in the results, but it can negatively impact performance as the ESA pauses up to 30 seconds to wait for the Whois service response.</p> <p>If you do not configure this setting, and the response time is slow, the ESA completes running the analysis for a given event without the Whois data, and calculates the score without the data.</p> <p>The default setting is true.</p>

Step 5: Verify the Whois Service is Reachable from your Environment

After starting Behavior Analytics Automated Threat Detection, test that the WhoIs service is reachable from your environment, and that the account information configured is valid. You can see the count incrementing for the WhoIs calls in the Explorer.

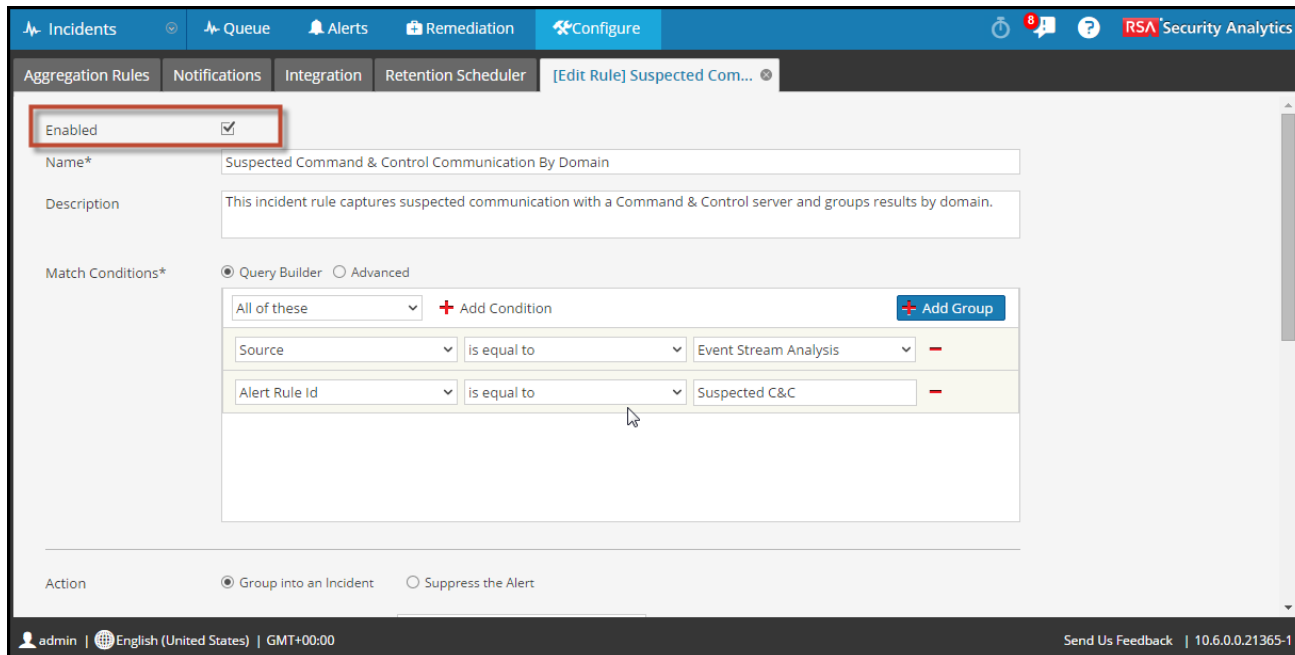
To verify the Whois lookups are successful, go to **ESA > Explore > Service > Whois > whoisClient** and confirm that the *ServiceRequestCount* and *Response200ValidData* parameters are incrementing.

Step 6: Verify the Suspected Command & Control By Domain Rule is Enabled and Monitor the Rule

Verify the Suspected Command & Command Control by Domain rule on the **Incident Manager**.

Note: You must have configured the Incident Manager database for the Suspected Command & Control by Domain rule to display in the Incident Manager. If it does not display, follow the steps to configure the database in Configure Incident Manager in the *Incident Management Configuration Guide*.

1. From **Incidents > Configure**, select **Aggregation Rules**.
2. Select the **Suspected Command & Control Communication by Domain** Rule, and double-click to open it.



3. Verify that **Enabled** is selected.

The Rule displays a green Enabled button when it is enabled.

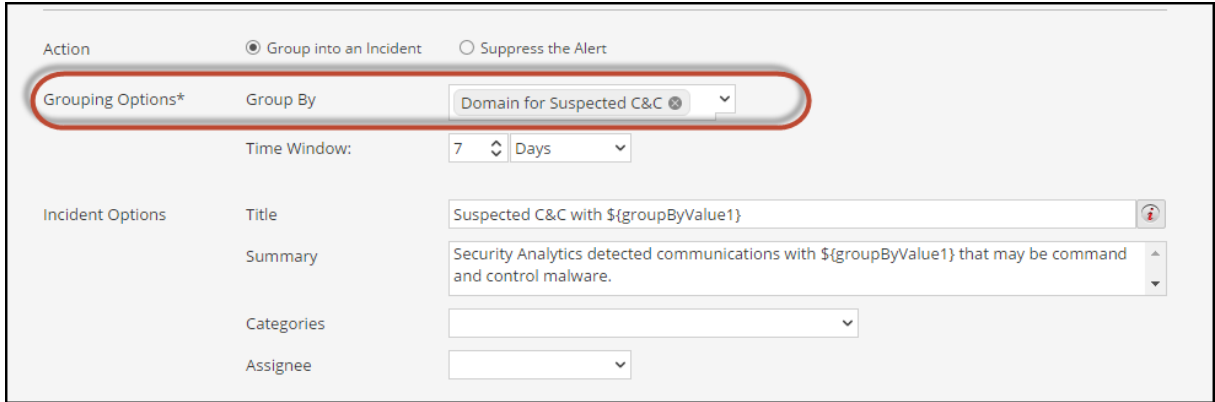
Result

Once you have enabled Behavior Analytics Automated Threat Detection, your ESA will begin to perform analytics on the HTTP traffic. You can view detailed information for each incident in the Incident Management queue.

Step 7: Verify the Incident is grouped by the Suspected C & C Domain

In order to group incidents correctly, the Incident Manager should group the incidents by the C&C Domain.

1. From **Incidents > Configure**, select **Aggregation Rules**.
2. Select the **Suspected Command & Control Communication by Domain** Rule, and double-click to open it.
3. Verify that the **Group By** field is set to *Domain for Suspected C&C*.



Action: Group into an Incident Suppress the Alert

Grouping Options*
 Group By: Domain for Suspected C&C
 Time Window: 7 Days

Incident Options
 Title: Suspected C&C with \${groupByValue1}
 Summary: Security Analytics detected communications with \${groupByValue1} that may be command and control malware.
 Categories:
 Assignee:

Next Steps

Monitor the Incident Manager to see if the rule is triggered. If the rule is triggered, follow the steps in the following section to investigate the domain associated with the triggered rule.

[Work with Behavior Analytics Automated Threat Detection Results](#)

Work with Behavior Analytics Automated Threat Detection Results

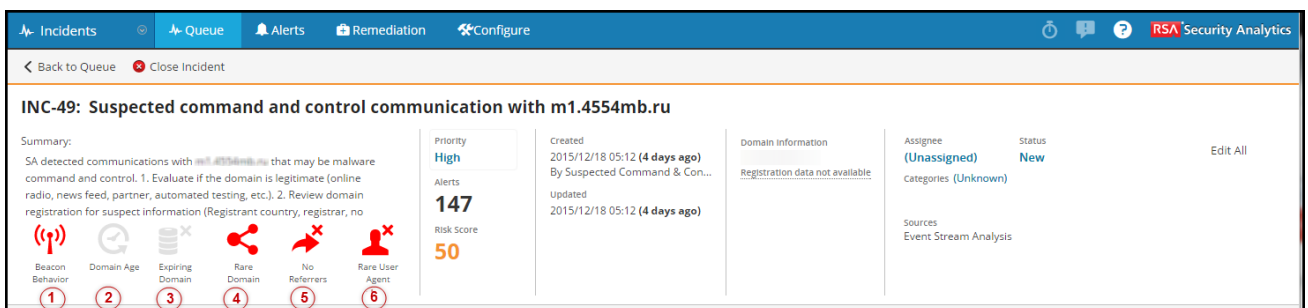
This topic explains how to interpret and work with Behavior Analytics Automated Threat Detection results.

When you view the Behavior Analytics Automated Threat Detection results in the Incident Manager, there are a number of different factors that are used to determine the overall score. This section is designed to help you understand how these scores are generated and what they mean.

Understand Threat Detection Results

When you work with Behavior Analytics Automated Threat Detection, several scores are aggregated together to make up the Command and Control Detection score. To better understand how this score is triggered, it's a good idea to understand the elements that make up the final score.

When you receive a Command & Control Detection alert, you can view the following detailed alert summary in the Incident Management module:



Incidents Queue Alerts Remediation Configure

Back to Queue Close Incident

INC-49: Suspected command and control communication with m1.4554mb.ru

Summary:
 SA detected communications with [m1.4554mb.ru](#) that may be malware command and control. 1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.). 2. Review domain registration for suspect information (Registrant country, registrar, no

Priority: **High**
 Alerts: **147**
 Risk Score: **50**

Created: 2015/12/18 05:12 (4 days ago)
 By Suspected Command & Con...
 Updated: 2015/12/18 05:12 (4 days ago)

Domain information
 Registration data not available

Assignee: (Unassigned)
 Status: New
 categories (Unknown)

Sources
 Event Stream Analysis

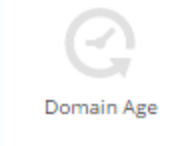
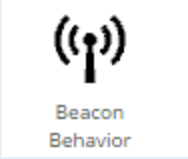
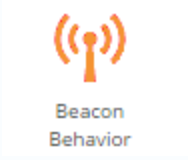
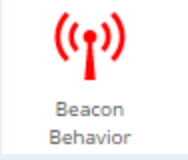
Beacon Behavior (1) Domain Age (2) Expiring Domain (3) Rare Domain (4) No Referrers (5) Rare User Agent (6)

Each icon represents a different score that makes up the total risk calculated. Note that the scores are weighted, so each score represents a different proportion of the final score. For example, The beacon behavior score might be 20% of the final score, while the domain age might be 5%:

1. **Beacon Behavior.** Command and control detection seeks to find highly regular periodic connections with a suspicious domain, so beaconing behavior has to do with how regularly the source IP is connecting to the domain server. A high score means that connections between this source IP and the domain are highly regular.
2. **Domain Age.** Often, a Command and Control Server uses a new domain to create connections, so if a domain is new to the network, it means it is more likely to be a command and control domain. A high score indicates that this domain is relatively new on this network. This score is derived from the Whois service. If your Whois service is not working, or if ESA cannot connect with it, the icon displays in gray. If there is an issue with connectivity or the Whois service returns a null value or a value in an unexpected format, then a default value is used to estimate this score. This ensures that the overall scoring is more accurate.
3. **Expiring Domain.** Often a Command and Control server uses an expiring domain to create connections, so if a domain is soon to be expired, it is more likely to be a Command and Control domain. This score is derived from the Whois service. If your Whois service is not working, or if ESA cannot connect with it, the icon displays in gray. If there is an issue with connectivity or the Whois service returns a null value or a value in an unexpected format, then a default value is used to estimate this score. This ensures that the overall scoring is more accurate.
4. **Rare Domain.** A rare domain is one that that relatively few source IPs have been connected to on a given network in the most recent week. If a domain is rarely used, the possibility of it being a Command and Control domain is higher than if it is a commonly used legitimate domain such as *Google.com*.
5. **No Referers.** A referer is an HTTP field that identifies the address of the web page that linked to the resource being requested. For example, if I access my bank website from my work website, the work website would appear as the referer. Because people frequently link to a site via a referer, a high score (meaning a low percentage of IPs connecting to this domain have used referers) indicates that a Command and Control communication is more likely.
6. **Rare User Agent.** User agents identifies the client software originating the request. A high score indicates that user agent associated with the IP address is not commonly used. Like the

Rare Domain score, an uncommon user agent has a greater likelihood of being associated with a Command and Control domain.

The icons display in different colors, and the colors help to visually indicate the level of risk. See the table below for details.

Icon	Meaning
Grey 	No score was generated because no data was available. This may occur if the Whois service is disabled or there is no data available to generate a given score.
Black 	The score indicator is weak.
Orange 	The score indicator is moderate.
Red 	The score indicator is high.

Note: Suspected Command and Control alerts from packets and logs from the same domain may be aggregated into the same incident.

What to Do Next

There are three possible paths you may want to follow once you have viewed threat scores:

- **Drill down for more details.** For each score, there are multiple factors that make up a score. You can view these details on the **Event Details** page.
- **Investigate the domain in the Investigation module.** You can go to the Investigations screen to get more details about the domain and related incidents.
- **Add domains to a whitelist.** If you look at the details and determine that the domain in question is not a threat, it's a good idea to add it a whitelist. This will ensure the domain no longer triggers a Threat Detection score, and it helps to tune the accuracy of scoring.

Drill Down Into the Scores for More Details

Each event score is enriched with data to help you determine whether the communication with the domain is malware and the severity of the attack if it is. For each of the scores listed above, there are more details that are included in the details for each event.

To access these details:

1. From the **Incidents** queue, double-click on an Incident to view the **Incident Details**.
2. From the **Alert Details** section, double-click on an alert.
3. The **Event Details** page opens.

From there, you can view details for the event, and for each detail, there is hover-over text to help you interpret the data. You can see details such as the score range, the number of occurrences for each time of score, the beaconing period, the information available from the Whois registration data, etc.


For example, you can see from the following event details that the Rare Domain score was 100 (the highest score), but that there was only one IP associated with this domain, and there were 24 occurrences in the previous week.

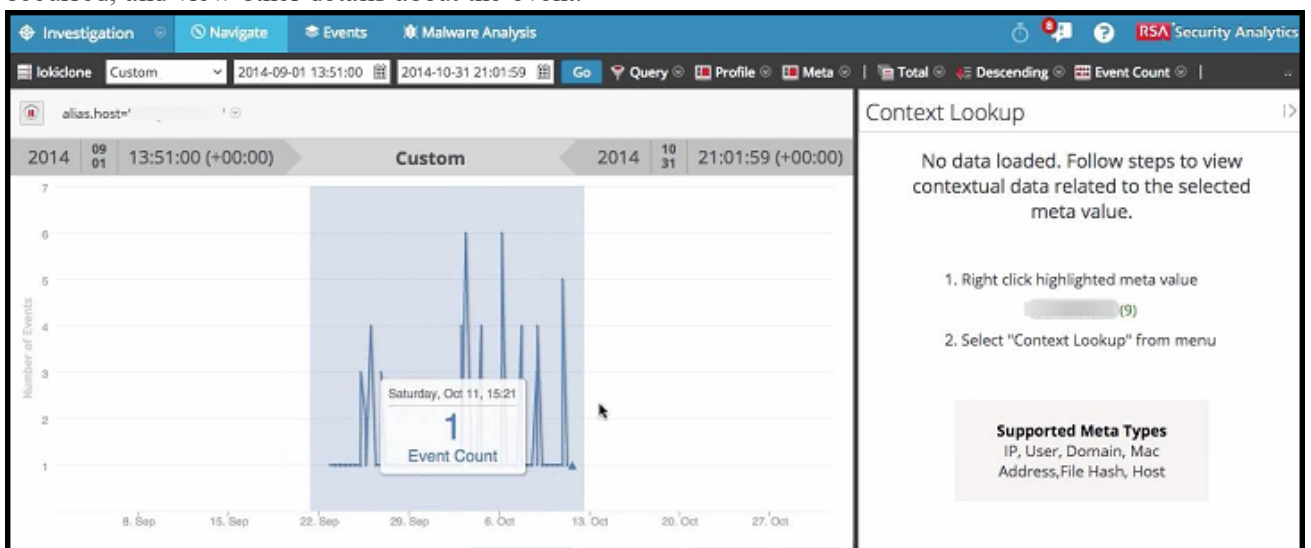
Event Details -- 2015/12/21 00:56

	<u>Contribution of No Domain Referrer Score:</u>	4
	<u>Contribution of Rare User Agent Score:</u>	4
Beacon Behavior Indicator	<u>Beaconing Score:</u>	97.93435439256842
	<u>Beaconing Period:</u>	35350
Domain Age Indicator	<u>Domain Age Score (This Network):</u>	100
	<u>Domain Age (This Network):</u>	564000
Expiring Domain Indicator	No domain registration data available	
Rare Domain Indicator	<u>Rare Domain Score (This Network):</u>	100
	<u>IPs Associated With The Domain:</u>	1
	<u>Occurrences in the last week:</u>	24
No Referers Indicator	<u>No Referers Score:</u>	100
	<u>IPs With No Referrer:</u>	1
	<u>Percentage of IPs With No Referrer:</u>	100
	<u>Occurrences in the last week:</u>	24
Rare User Agent Indicator	<u>Rare User Agent Score:</u>	100
	<u>IPs With Rare User Agent:</u>	1
	<u>Percentage of IPs With Rare User Agent:</u>	100
	<u>Occurrences in the last week:</u>	24

Close

Investigate the Domain from the Investigation Module

From the Alert Details, you can also open the Investigations module to drill down into the domain details. To do this, from the **Alert Details** click  > **Investigate Destination Domain**. From there, you can search the days surrounding the event to see what else may have occurred, and view other details about the event.





Reduce False Positives

Sometimes, a domain you access regularly may trigger an Behavior Analytics Automated Threat Detection score. For example, a weather service might have the same beaconing behavior as a Command and Control communication, thus triggering an unwarranted negative score. When this happens, it's called a false positive. If, after investigating the event, you discover it is a false-positive, you can mark it as a false-positive, which will add the domain to a whitelist. Once the domain is added to the whitelist, it will not trigger an Behavior Analytics Automated Threat Detection score.

Note: If you use SecOps or another ticketing solution, you can manually add domains to the white list using the Context Hub service. See "Step 2: Configure a Whitelist" in [Configure Behavior Analytics Automated Threat Detection](#).

Procedure

1. From the **Incidents Detail** page, you can mark a particular incident as a false-positive which will automatically add it to the whitelist.
 1. From the **Incident Manager**, select the incident which triggered a false-positive score. Click   > **Edit Incident**.
The **Edit Incident** dialog box displays.
 2. In the **Edit Incident** dialog box, click the **Status** field and select *Closed-False Positive*. This adds the domain to the whitelist and closes the incident. Once the domain is added to the whitelist, it is ignored when Behavior Analytics Automated Threat Detection scoring occurs.

Note: If you modify the status of an incident marked as *false-positive*, you can choose to remove it from the whitelist.


Troubleshoot Behavior Analytics Automated Threat Detection

Behavior Analytics Automated Threat Detection is an analytics engine that examines your HTTP data. It also makes use of other components, such as a WhoIs service and the Context Hub, which can add complexity to your installation. This topic provides suggestions to help you find issues if your Behavior Analytics Automated Threat Detection deployment does not provide the results you expect.

When you troubleshoot Behavior Analytics Automated Threat Detection, it is important to factor in the mode used. If mixed mode is used (Behavior Analytics Automated Threat Detection enabled on the same machine as ESA Rules, or Context Hub), you'll need to consider the memory usage and i/o of these applications when troubleshooting. Generally, when mixed mode installation is configured, Behavior Analytics Automated Threat Detection is enabled to use approximately fifty percent of the memory available, whereas ESA Rules memory usage is unbounded. Therefore, you may want to check your ESA Rules as a first step when troubleshooting in mixed mode.

If you are using mixed mode, you should also consider whether the ESA is configured for Memory Pool or Event Time Ordering. Memory Pool can impact performance, while Event time ordering can impact performance and memory usage.

Possible Issues

Problem	Possible Causes	Solutions
I'm seeing too many alerts (false positives).	Several	<p>One possible cause is that the Whois lookup is failing or is not configured. The Whois lookup is helpful in determining whether a URL is valid, and if the connection fails or is not properly configured, it can result in false positives.</p> <p>There are a number of counters for the Whois Lookup service you can view.</p> <ol style="list-style-type: none"> 1. From Administration > Services, select your ESA service and then  > View > Explore. 2. In the Explorer, click Service > Whois > whoisClient. <p>Below are a few useful counters to check:</p> <ul style="list-style-type: none"> • FailedLookupCount: Whenever a request to the RSA Whois Service for Whois data fails, this count is incremented. • LookupEnqueueFailureCount: This counts any failed attempts to add an entry to the cache. These failures will be due to errors internal to the cache. • Response401Count: This counts the requests to the RSA Whois Server that failed with a status code of 401. Requests with expired authentication tokens are included in this count. This count is included in FailedLookupCount.

Problem	Possible Causes	Solutions
		<p>You may need to whitelist URLs. Sometimes the legitimate behavior for a URL triggers an alert. One way to prevent this from occurring is to add the URL to the whitelist. For instructions on doing this, see "Reduce False Positives" in Work with Behavior Analytics Automated Threat Detection Results.</p>
<p>I'm not seeing any alerts.</p>	<p>The ESA requires a "warm-up" period when you enable Automated Threat Detection.</p>	<p>When you enable Behavior Analytics Automated Threat Detection, there is a "warm-up" period, during which no alerts are viewable. The default time period is 24 hours. After this 24 hour learning period, alerts can be viewed. If the ESA restarts, this learning period starts over, and you will need to wait the specified warm-up time to view alerts.</p>
<p>I'm seeing performance issues (more resource usage or a drop in throughput).</p>	<p>Several</p>	<p>If you are having performance issues on an ESA that is also running ESA rules, follow the troubleshooting steps for rules. ESA rules are unbounded, whereas Behavior Analytics Automated Threat Detection is configured to use a specified amount of resources (usually approximately 50%). For these troubleshooting steps, go to Troubleshoot ESA.</p>

References

In the Alerts module, you configure and deploy ESA rules to get alerted about potential network threats.

These topics explain the user interface in the Alerts module.

- [New Advanced EPL Rule Tab](#)
- [Alerts Summary View](#)
- [Build a Statement Dialog](#)
- [Deploy ESA Rules Dialog](#)
- [Deploy ESA Services Dialog](#)
- [Rule Builder Tab](#)
- [Rules Tab](#)
- [Rule Syntax Dialog](#)
- [Select an ESA Service Dialog](#)
- [Services Tab](#)
- [Settings Tab](#)
- [Updates to the Deployment Dialog](#)


New Advanced EPL Rule Tab

This topic describes the Advanced EPL Rule tab that you use to define rule criteria with an Event Processing Language (EPL) query.

To access the Advanced EPL Rule tab:

1. In the **Security Analytics** menu, select **Alerts > Configure**.

The Configure view is displayed with the Rules tab open by default.

2. In the **Rule Library** toolbar, select   > **Advanced EPL**.

The Advanced EPL Rule tab is displayed.

Below is a screen shot of the Advanced EPL Rule tab.

The screenshot shows the 'New Advanced EPL Rule' configuration page in the RSA Security Analytics interface. The page is titled 'Advanced EPL' and instructs the user to 'Write a rule in Event Processing Language.' The configuration fields are as follows:

- Rule Name ***: A text input field.
- Description**: A large text area for a summary of the rule.
- Trial Rule**: A checkbox that is currently unchecked.
- Severity ***: A dropdown menu set to 'Low'.
- Query ***: A large text area for the EPL query.
- Notifications**: A section with a table for configuring notifications. The table has columns for 'Output', 'Notification', 'Notification Server', and 'Template'. Below the table, it says 'No parameters to edit.' There is also a checkbox for 'Output Suppression of every' followed by a text input for 'minutes'.

The interface includes a top navigation bar with 'Alerts', 'Summary', and 'Configure' tabs, and a footer with user information (admin), language (English (United States)), time zone (GMT+00:00), and version (10.6.0.0.22075-5).

Features

The following table lists the parameters in the Advanced EPL Rule tab.

Parameters	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.
Query	EPL query that defines rule criteria.

Notifications

In the Notifications section, you can choose how to be notified when ESA generates an alert for the rule.

For more information on the alert notifications, see [Add Notification Method to a Rule](#).

The following figure shows the Notifications section.

Notifications				Global Notifications
Output	Notification	Notification Server	Template	
<input checked="" type="checkbox"/> SYSLOG	Local_SysLog	localhost-514	Default Syslog Template	
<input type="checkbox"/> Output Suppression of every <input type="text"/> minutes				

Parameter	Description
+	To add an alert notification type.
-	To delete the selected alert notification type.
Output	Alert notification type. Options are: <ul style="list-style-type: none"> • Email • SNMP • Syslog • Script
Notification	Name of previously configured output, such as an email distribution list.
Notification Server	Name of server that sends the output.
Template	Name of template for the alert notification.
Output Suppression of every	Option to specify alert frequency.
Minutes	Alert frequency in minutes.

Enrichments

In the Enrichments section, you can add a data enrichment source to a rule.

For more information on the enrichments, see [Add an Enrichment to a Rule](#).

The following figure shows the Enrichments section.

Enrichments Settings			
Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/> In-Memory Table	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> Warehouse Analytics	Select Enrichment Source	Enter Meta	key
<input type="checkbox"/> GeoIP	Select Enrichment Source	Enter Meta	ipv4

Parameter	Description
+	To add an enrichment.
-	To delete the selected enrichment.
Output	Enrichment source type. Options are: <ul style="list-style-type: none"> • In-Memory Table • External DB Reference • Warehouse Analytics • GeoIP
Enrichment Source	Name of previously configured enrichment source, such as a .CSV filename for an In-Memory Table.
ESA Event Stream Meta	ESA meta key whose value will be used as one operand of join condition.
Enrichment Source Column Name	Enrichment source column name whose value will be used as the other operand of the join condition.

Alerts Summary View

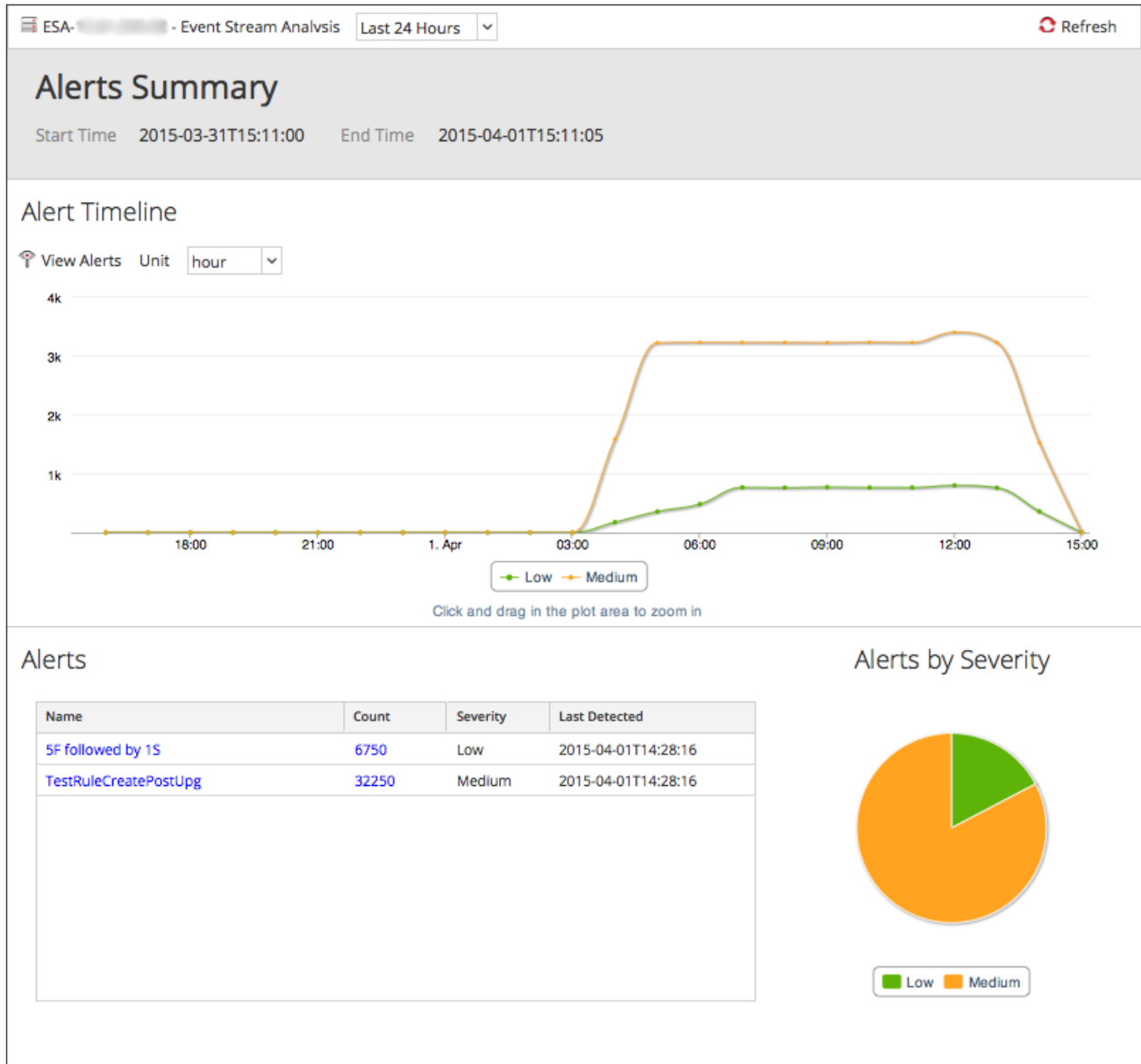
The Alerts Summary view provides a consolidated view of all the alerts generated in a particular time range. You can specify a time range and represent alerts as graphs and charts in tabular format. For example, if you want to view how many alerts of low, medium and high severity are generated in a particular time range, you can use a chart for better clarity. You can also view the number of alerts generated in a specific minute, hour or day.

On further drilling down, the view also provides event meta and event details on each alert generated.

Note: In the User Interface (UI), the date or time displayed depends on the time zone profile selected by the user.

In Security Analytics, the Alerts Summary view is displayed when you navigate to **Alerts > Summary** and select an ESA service.

The following figure shows the various components of the Alerts Summary view.



Features

The Alerts Summary view consists of the following sections:

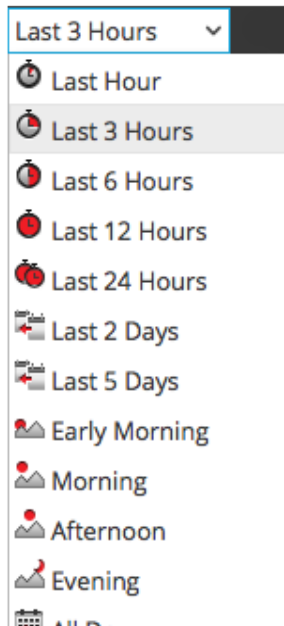
- Alerts Summary
- Alert Timeline
- Alerts
- Alerts by Severity

Alerts Summary

The Alerts Summary section displays the time period in which alerts are generated. The following figure displays the Alerts Summary section.



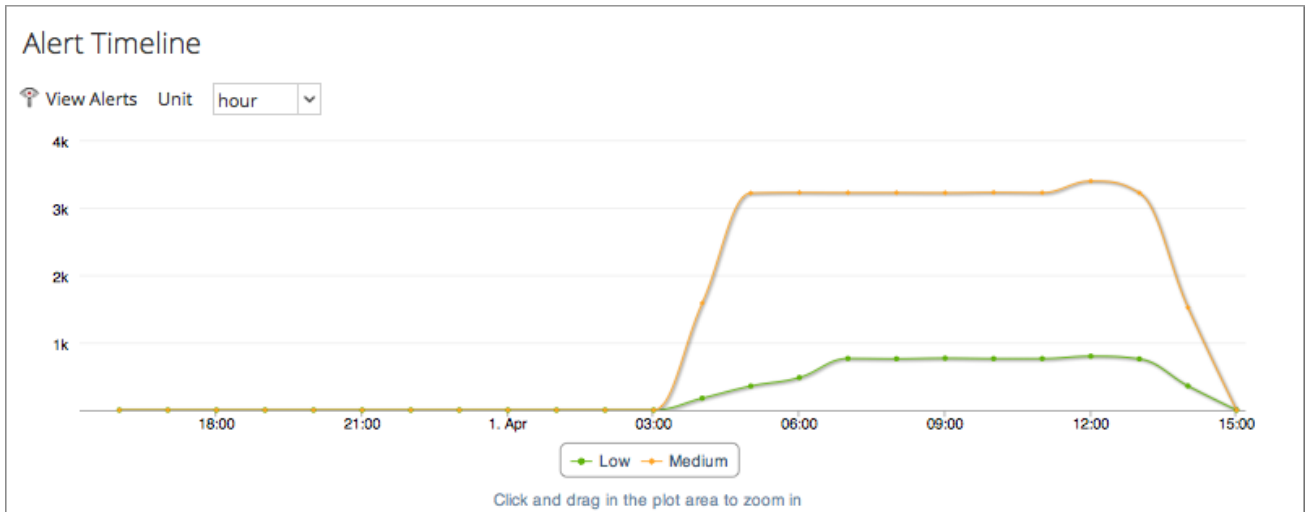
On the top left part of the section, the ESA service selected is displayed. You can select a time period based on which you want alerts to be displayed. Some of the options available are displayed in the following figure.



Based on the time period that you select, the start time and end time are displayed in the section.

Alert Timeline

The Alert Timeline section shows a graphical representation of the alerts generated during a particular time period. The following figure displays the Alert Timeline section.



You can perform the following using the Alert Timeline section:

- View alerts generated during a particular minute, hour or day by selecting the option from the drop-down list of **Unit**.
- View details about each alert generated by clicking **View Alerts**.
- View the number of alerts generated, severity level of the alerts and time they are generated by hovering the mouse over a specific point on the graph.

Note: You can click the legends provided in the Alert Timeline based on the **Severity**. Also, you can click and drag in the plot area to zoom in and view data.

Alerts

The Alerts section shows the alerts generated during a particular time period in tabular format. The following figure displays the Alerts section.

Name	Count	Severity	Last Detected
test	19057	Low	2015-03-31T13:05:49
User login from multiple geos over VPN wit...	5	Medium	2015-03-30T11:20:12
ADActivity	40	Low	2015-03-31T09:37:00
5F followed by 1S	10994	Low	2015-04-01T14:28:16
TestRuleCreatePostUpg	42544	Medium	2015-04-01T14:28:16

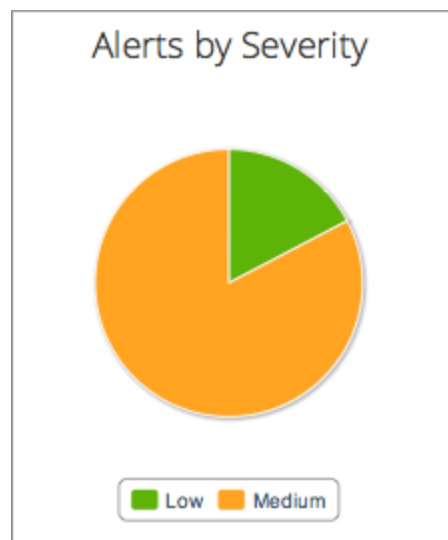
The following table lists the various columns in the Alerts section and their description.

Column	Description
Name	The name used to identify the alert.
Count	The number of times the alert occurred.
Severity	The severity level of the alert.
Last Detected	The last time the alert was detected.

You can view details on each alert generated by clicking an alert and also export the logs related to each event in the alert.

Alerts by Severity

The Alerts by Severity section shows a chart representation of the alerts based on the severity level. The following figure displays the Alerts by Severity section.



You can view details on the alerts generated by clicking in the chart.

Build a Statement Dialog

The Build a Statement dialog allows you to construct a condition statement when creating a new Rule Builder rule.

To access the Build a Statement dialog:

1. In the Security Analytics menu, select **Alerts > Configure**.

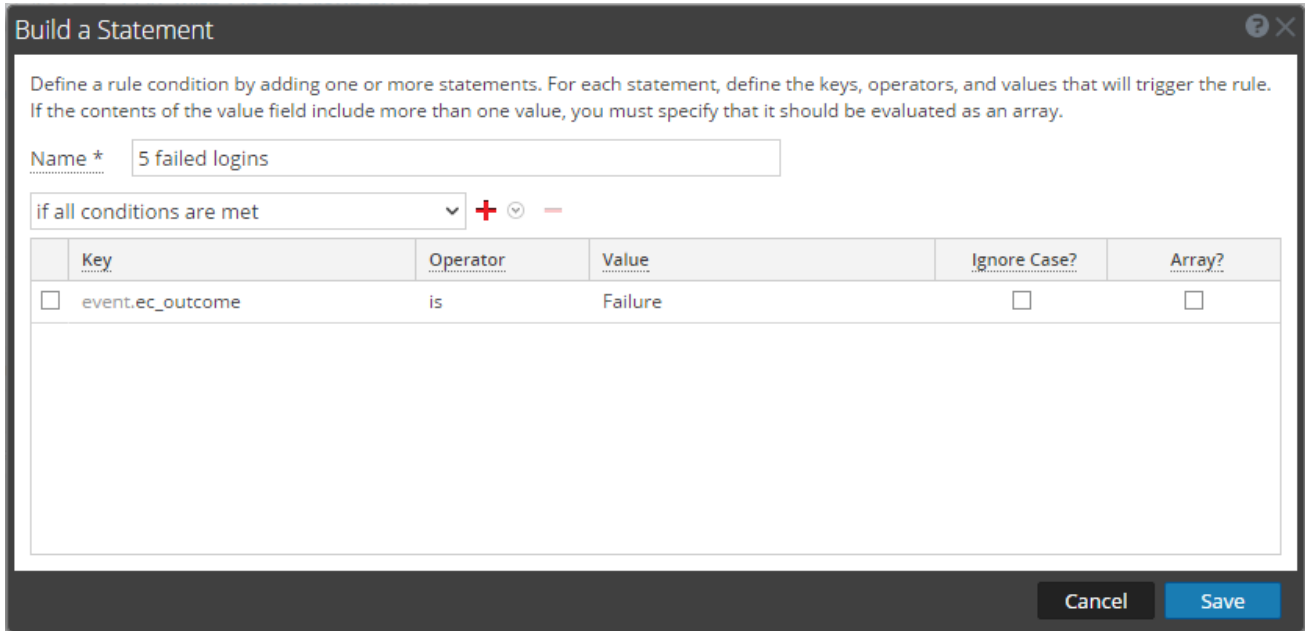
The Configure view is displayed with the Rules tab open.

2. In the **Rule Library** toolbar, select  > **Rule Builder**.

A New Rule tab is displayed in Security Analytics.

3. In the **Conditions** section, click .



The Build a Statement dialog is displayed.



Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name *

if all conditions are met  



	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.ec_outcome	is	Failure	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Features

The following table describes the parameters in the Build a Statement dialog.

Parameter	Description
Name	Purpose of the statement.
Select	Conditions the rule requires. There are two options: <ul style="list-style-type: none"> • If all conditions are met • If any of these conditions are met
Key	Key for ESA to check in the rule statement.

Parameter	Description
Evaluation Type	Relationship between the meta key and value for the key: <ul style="list-style-type: none"> • is • is not • is not null • is greater than (>) • is greater than or equal to (>=) • is less than (<) • is less than or equal to (<=) • contains • not contains • begins with • ends with
Value	Value for ESA to look for in the key.
Ignore Case?	This field is designed for use with string and array of string values. By choosing the Ignore Case field, the query will treat all string text as a lowercase value. This ensures that a rule that searches for the user named Johnson would trigger if the event contains "johnson," "JOHNSON," or "JoHnSoN."
Array?	Choice to indicate if contents of Value field represent one value or multiple values: <ul style="list-style-type: none"> • Select the box to indicate multiple values. • Clear the box to indicate one value.
	Add a statement. You can add a meta condition, whitelist condition, or blacklist condition.
	Delete selected statement.
Save	Add statement to the Conditions section of the Rule Builder tab.

The following table shows the operators you can use in the Rule Builder:

Operator	Required Value	Usage	Example	Meaning
is	Singular string value	The meta key is equal to the <i>value</i> field.	<i>user_dst</i> is John Doe.	<i>user_dst</i> is equal to the string "John Doe".
is	Array string value	The meta key is equal to one of the elements of the <i>value</i> field.	<i>user_dst</i> is John, Doe, Smith.	<i>user_dst</i> is equal either to the string "John" or to the string "Doe" or to the string "Smith" (Note, the spaces are stripped).
is not	Singular string value	The meta key is not equal to the <i>value</i> field.	<i>size</i> is not 200.	<i>size</i> is not equal to the number 200 (size is a numeric value).
is not	Array string value	The meta key is not equal to any of the elements of the <i>value</i> field.	<i>size</i> is not 200, 300, 400.	<i>size</i> is equal neither to 200 nor to 300 nor to 400.
is not null	N/A (looks for any value)	The meta key value is not null.	<i>user_dst</i> is not null.	<i>user_dst</i> is a meta that contains a value.
is greater than (>)	Number	The numeric value of the meta key is greater than the number in the <i>value</i> field.	<i>payload</i> is greater than 7000.	<i>payload</i> is a numeric value that is greater than 7000.
is greater than or equal to (>=)	Number	The numeric value of the meta key is greater than or equal to the number in the <i>value</i> field.	<i>payload</i> is greater than or equal to 7000.	<i>payload</i> is a numeric value that is greater than or equal to 7000.
is less than (<)	Number	The numeric value of the meta key is less than the number in the <i>value</i> field.	<i>ip_dstport</i> is less than 1024.	<i>ip_dstport</i> is a numeric value that is less than the numeric value 1024.
is less than or equal to (<=)	Number	The numeric value of the meta key is less than or equal to the number in the <i>value</i> field.	<i>ip_dstport</i> is less than or equal to 1024.	<i>ip_dstport</i> is a numeric value that is less than or equal to numeric value 1024.
contains	String	The <i>value</i> field is a substring of the meta key (This operator is only available for a string-valued meta key).	<i>ec_outcome</i> contains failure.	<i>ec_outcome</i> is a string that contains the substring "failure".
not contains	String	The <i>value</i> field is not a substring of the meta key (This operator is only available for a string-valued meta key).	<i>ec_outcome</i> not contains failure.	<i>ec_outcome</i> is a string that does not contain the substring "failure".



Operator	Required Value	Usage	Example	Meaning
begins with	String	The <i>value</i> field is the beginning of the meta key (This operator is only available for a string-valued meta key).	<i>ip_dst</i> begins with 127.0.	<i>ip_dst</i> is a string that starts with "127.0".
ends with	String	The <i>value</i> field is the end of the meta key (This operator is only available for a string-valued meta key).	<i>user_dst</i> ends with son.	<i>user_dst</i> is a string that ends in "son".

Note: Terms in ***bold italic*** are Meta that may not exist in all customer environments.

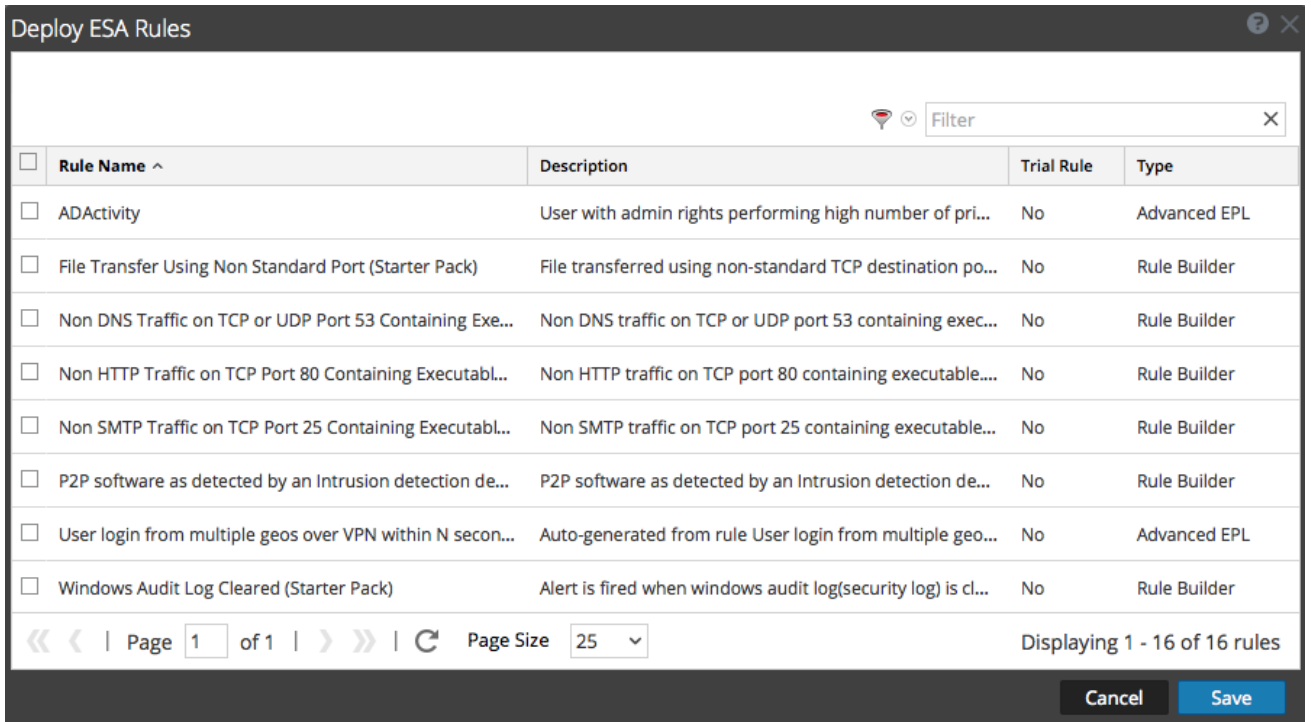
Deploy ESA Rules Dialog

The Deploy ESA Rules dialog allows you to filter and select rules to deploy to an ESA service.

To access this dialog:


1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed by default.
 2. In the options panel, under the **Deployment** section, select or add a new deployment by clicking  > **Add**.
 3. In the **ESA Rules** panel, click .
- The Deploy ESA Rules dialog is displayed.

The following figure is an example of this dialog.



Features

The following table describes the parameters of the Deploy ESA Rules dialog.

Parameters	Description
	Filters the list of rules based on severity and type. The text box beside this icon filters based on rule name.
Rule Name	Displays the name of the rule.
Description	Describes the rule.
Trial Rule	Indicates whether or not the rule is a trial rule.
Type	Indicates the type of rule: RSA Live ESA, Advanced EPL, or Rule Builder.

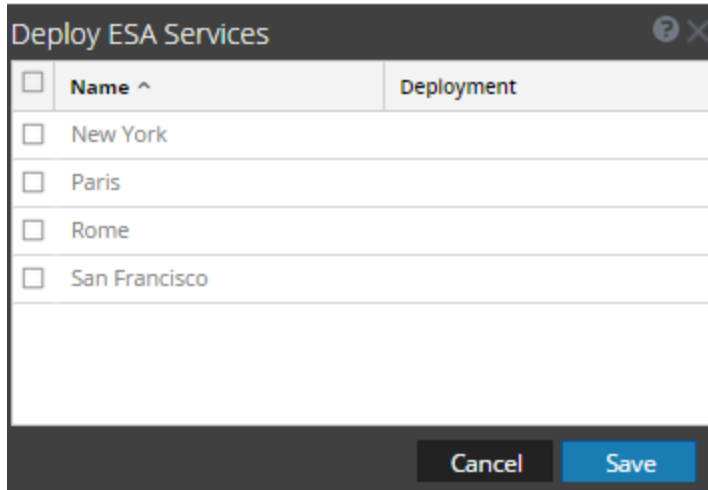
Deploy ESA Services Dialog

The Deploy ESA Services dialog displays all ESA services available to be added to a deployment.

To access this dialog:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed by default.
2. In the options panel, under the **Deployment** section, select or add a deployment.
3. In the **ESA Services** panel, click **+**.
The Deploy ESA Services dialog is displayed.

The following figure is an example of this dialog.



Features

The following table describes the parameters of the Deploy ESA Services dialog.


Parameters	Description
Name	Displays the name of configured ESA services.
Deployment	Displays the deployments to which the service has already been added.

Rule Builder Tab

The Rule Builder tab enables you to define a Rule Builder rule.

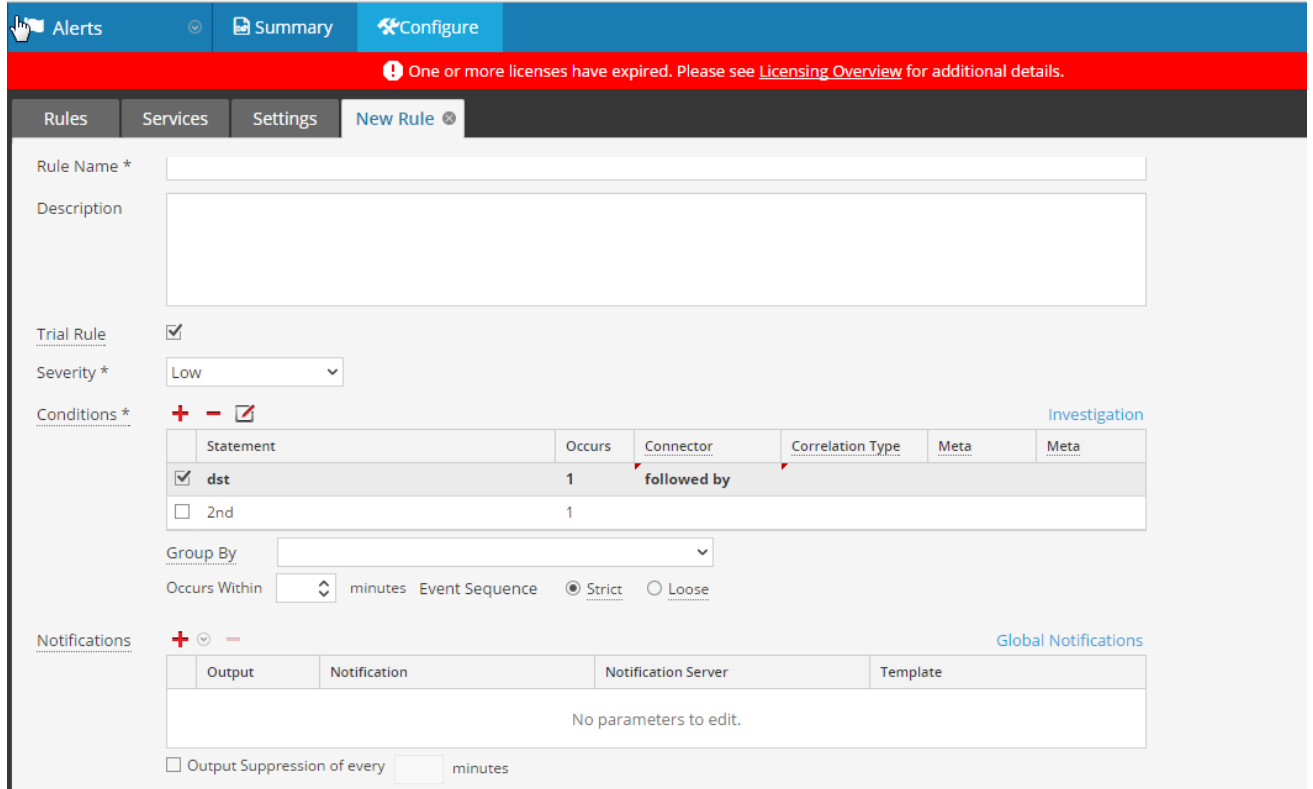
To access the Rule Builder tab:

1. In the Security Analytics menu, select **Alerts > Configure**.
The Configure view is displayed with the Rules tab open by default.

2. In the **Rule Library** toolbar, select   > **Rule Builder**.

The Rule Builder tab is displayed.

The following figure shows the Rule Builder tab.



Alerts Summary Configure

One or more licenses have expired. Please see [Licensing Overview](#) for additional details.




Rules Services Settings **New Rule**

Rule Name *

Description

Trial Rule



Severity * Low

Conditions *    Investigation

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input checked="" type="checkbox"/> dst	1	followed by			
<input type="checkbox"/> 2nd	1				

Group By

Occurs Within minutes Event Sequence Strict Loose

Notifications   Global Notifications

Output	Notification	Notification Server	Template
No parameters to edit.			

Output Suppression of every minutes

Features

The following table lists the parameters in the Rule Builder tab.

Parameters	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.

The Rule Builder includes the following components:

- Conditions section
- Notifications section
- Enrichments section

Conditions Section

In the Conditions section of the Rule Builder tab, you define what the rule detects.

The following figure shows the Conditions section.

The screenshot displays the 'Conditions' section of a rule builder. At the top, there is a 'Trial Rule' checkbox which is checked. Below it, the 'Severity' is set to 'Low'. The 'Conditions' section contains a table with the following data:

Statement	Occurs	Connector	Correlation Type	Meta	Meta
<input type="checkbox"/> Failure	5	followed by			
<input checked="" type="checkbox"/> Success	1	AND			
<input type="checkbox"/> Modify Password	1				

Below the table, there are 'Group By' fields containing 'device_class' and 'user_dst'. At the bottom, the 'Occurs Within' is set to 5 minutes, 'Event Sequence' is selected, and the 'Strict' correlation type is chosen.

The following table lists the parameters of the Conditions section.

Parameter	Description
	Add a statement.
	Remove selected statement.
	Edit selected statement.
Statement	Logical group of conditions for one operation.
Occurs	Alert frequency if the condition is met. This specifies that there must be at least that many events that satisfy the criteria in order to trigger an alert. The time window in minutes binds the Occurs count.

Parameter	Description
Connector	<p>Options to specify relationship among the statements:</p> <ul style="list-style-type: none"> • followed by • not followed by • AND • OR <p>The Connector joins two statements with AND, OR, followed by, or not followed by. When followed by is used, it specifies that there is a sequencing of those events. AND and OR build one large criteria. The followed by creates distinct criteria that occurs in sequence.</p>
Correlation Type	<p>Correlation Type applies only to followed by and not followed by. If you choose a correlation type of SAME, select one meta to correlate on, and if you choose a correlation type of JOIN, select two meta to correlate on. You may want to use JOIN if you are trying to correlate on meta from two different data sources. For example, say you want to correlate an AV alert with an IDS alert.</p>
Meta	<p>Enter the meta condition if choosing a correlation type of SAME or JOIN (as described above).</p>
Meta	<p>Enter the second meta condition if choosing a correlation type of JOIN (as described above). For example, The destination IP address from the AV alert and source IP address for the workstation from the IDS alert are joined to allow you to view the same entities across different sources.</p>
occurs within minutes	<p>Time window within which the conditions must occur.</p>

Parameter	Description
Event Sequence	Choose whether the pattern must follow a <i>strict</i> match or a <i>loose</i> match. If you specify a strict match, this means that the pattern must occur in the <i>exact</i> sequence you specified with no additional events occurring in between. For example, if the sequence specifies five failed logins (F) followed by a successful login (S), this pattern will only match if the user executes the following sequence: F,F,F,F,F,S. If you specify a loose match, this means that other events may occur within the sequence, but the rule will still trigger if all of the specified events also occur. For example, five failed login attempts (F), followed by any number of intervening successful login attempts (S), followed by a successful login attempt might create the following pattern: F,S,F,S,F,S,F,S,F,S which would trigger the rule despite the intervening successful logins.
Group By	Select the meta key by which to group results from the dropdown list. For example, suppose that there are three users; Joe, Jane, and John and you use the Group By meta, user_dst (user_dst is the meta field for the user destination account). The result will show events grouped under the user destination accounts, Joe, Jane, and John. You can also group by multiple keys. For example, you might want to group by user and machine to see if a user logged in from the same machine attempts to log into an account multiple times. To do this, you might group by device_class and user_dst.

Notifications

In the Notifications section, you can choose how to be notified when ESA generates an alert for the rule.

For more information on the alert notifications, see [Add Notification Method to a Rule](#).

The following figure shows the Notifications section.

Notifications Global Notifications

Output	Notification	Notification Server	Template
<input checked="" type="checkbox"/> SYSLOG	Local_SysLog	localhost-514	Default Syslog Template

Output Suppression of every minutes

Parameter	Description
+	To add an alert notification type.
-	To delete the selected alert notification.

Parameter	Description
Output	Alert notification type. Options are: <ul style="list-style-type: none"> • Email • SNMP • Syslog • Script
Notification	Name of previously configured output, such as an email distribution list.
Notification Server	Name of server that sends the output.
Template	Name of template for the alert notification.
Output Suppression of every	Option to specify alert frequency.
Minutes	Alert frequency in minutes.



Enrichments

In the Enrichments section, you can add a data enrichment source to a rule.

For more information on the enrichments, see [Add an Enrichment to a Rule](#).

The following figure shows the Enrichments section.

Enrichments Settings			
Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/> In-Memory Table	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> Warehouse Analytics	Select Enrichment Source	Enter Meta	key
<input type="checkbox"/> GeolP	Select Enrichment Source	Enter Meta	ipv4

Parameter	Description
	To add an enrichment.
	To delete the selected enrichment.

Parameter	Description
Output	Enrichment source type. Options are: <ul style="list-style-type: none"> • In-Memory Table • External DB Reference • Warehouse Analytics • GeoIP
Enrichment Source	Name of previously configured enrichment source, such as a .CSV filename for an In-Memory Table.
ESA Event Stream Meta	ESA meta key whose value will be used as one operand of join condition.
Enrichment Source Column Name	Enrichment source column name whose value will be used as the other operand of the join condition. For an in-memory table, If you configured a key when creating a .CSV-based enrichment, this column automatically populates with the selected key. However, you can change it if you like. For a GeoIP enrichment source, ipv4 is automatically selected.

Rules Tab

This topic describes the Rules tab, which you use to manage ESA rules and deployments.

The Rules tab is displayed when you select **Alerts > Configure** in the Security Analytics menu.

The following figure shows the Rules tab.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Alerts', 'Summary', and 'Configure' tabs. The 'Rules' tab is selected, and the 'Rule Library' is displayed. The Rule Library contains a table of rules with the following columns: Rule Name, Description, Trial Rule, Type, and Actions. The table lists 16 rules, including '10F1S-Multiple meta - Demo - Multiple Group by', 'ADV: Multiple_FailedLogin_SuccessfulLogin', and 'SAMPLE - Blacklist - From inside countries that are no...'. The interface also shows deployment counts for BRB ESA (10) and ESA (1).

Rule Name	Description	Trial Rule	Type	Actions
10F1S-Multiple meta - Demo - Multiple Group by	10 Failures followed by 1 Success with Group by: Devi...	No	Rule Builder	[Settings]
ADV: Multiple_FailedLogin_SuccessfulLogin	Advanced rule testing	No	Advanced EPL	[Settings]
ArrayString checking	Checking for array on LHS and selected values on RHS	No	Rule Builder	[Settings]
BRB_Pattern_match_rule		No	Rule Builder	[Settings]
Checking user_dst not null		No	Rule Builder	[Settings]
Demo_CSV_test	Check whether the incoming IP is in the Blacklist CSV ...	No	Rule Builder	[Settings]
Demo_Geoip_rule		No	Rule Builder	[Settings]
Demo_toLowerCase	5 failures followed by 1 success and 1 config change S...	No	Rule Builder	[Settings]
Destination Port		No	Rule Builder	[Settings]
Pattern Match Rule: 5 fail 1 success	Rule that matches 5 failures and 1 success from the s...	No	Rule Builder	[Settings]
SAMPLE - Blacklist - From inside countries that are no...	Monitors for non-SMTP traffic on TCP destination por...	Yes	Rule Builder	[Settings]

Features

The Rules tab is divided into three sections:

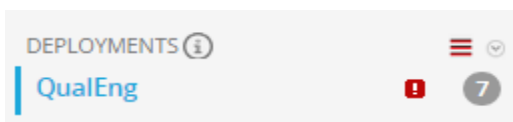
- [Options Panel](#)
- [Rule Library Panel](#)
- [Deployment Panel](#)

Options Panel

In the options panel of the **Rules** tab, you can perform the following:

- View ESA rules in the Rule Library
- Create deployments

The following figure shows the options panel in the **Rules** tab.



Features




There are two sections in the options panel: Rules and Deployments.

Rules Section

The Rules section contains two options. **Rule Library** is selected by default, and when it's selected, the Rule Library view is displayed within the tab. **Get Rules From RSA Live** navigates to the Live Search view, where you can search for rules.

Deployments Section

The Deployments section lists deployments and indicates whether there are updates to the deployments. From this section, deployments can be added, deleted, edited, and refreshed. Selecting a deployment from the list displays the Deployment panel within the tab. The following table describes the features of this section.

Feature	Description
	Displays a drop-down menu from which you can choose to add, edit, or delete a deployment. You can also refresh the list of deployments to see if there are any new updates to the list.
	Indicates whether there are any updates to the deployment.
	Indicates the number of rules in the deployment.

Rule Library Panel

This topic describes the components of the Rule Library panel. You can perform the following tasks using the Rule Library panel:

- Add an ESA rule
- Delete an ESA rule
- Edit an ESA rule

- Duplicate an ESA rule
- Import ESA rules
- Export an ESA rule
- Filter the ESA rules list

To access this view, in the Security Analytics menu, select **Alerts > Configure**. The Rules tab is displayed and the Rule Library panel is on the right.

Features

The following figure shows the Rule Library panel.

<input type="checkbox"/>	Rule Name ^	Description	Trial Rule	Type	Actions
<input type="checkbox"/>	5 Failed Login Attempts followed by Successful Login	The same user makes 5 failed login attempts. On the next try, the user lo...	Yes	Rule Builder	
<input type="checkbox"/>	Cross-site Correlation 5F+1S	xsite rule between NY & SF for % failures + 1 Success scenario	Yes	Rule Builder	
<input type="checkbox"/>	ECAT alert with audit log cleared	ECAT alert with audit log cleared	No	RSA Live ESA Rule	
<input type="checkbox"/>	Enrich Username with Org Access recurring csv	Each record we get that contains a username will get the data enriched f...	No	Advanced EPL	

Page 1 of 1 | Page Size 25 | Displaying 1 - 4 of 4 rules

The Rule Library panel includes the following components:

- Rule Library toolbar
- Rule Library list

Rule Library Toolbar

The Rule Library toolbar allows you to add, delete, edit, duplicate, filter, export, and import ESA rules. The following figure shows the icons for these actions.




Rule Library List

The following figure shows the Rule Library list.

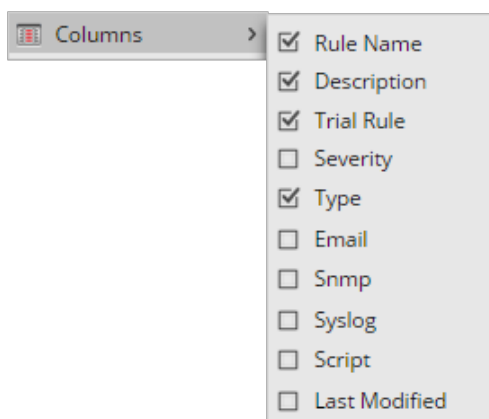


The Rule Library list shows all the ESA rules that have been downloaded from RSA Live or created in the Advanced EPL and Rule Builder tabs. The following table lists the columns in the Rule Library list and their description.

Column	Description
Rule Name	Purpose of the ESA rule.
Description	Summary of what the ESA rule detects.
Trial Rule	Deployment mode to see if the rule runs efficiently.

Column	Description
Type	The type of rule.
Actions ()	Menu to delete, edit, duplicate, or export the selected rule.
Severity	Threat level of alert triggered by the rule.
Email	Indicates whether an alert notification for the rule is sent by email. This column is not visible by default.
Snmp	Indicates whether an alert notification for the rule is sent using SNMP. This column is not visible by default.
Syslog	Indicates whether an alert notification for the rule is sent using Syslog. This column is not visible by default.
Script	Indicates whether an alert notification for the rule executes a script. This column is not visible by default.
Last Modified	The date and time when the ESA rule was last modified. This column is not visible by default.

To display columns which aren't visible by default, hover over the title of a column and click the v on the right. This opens a drop-down menu in which you can sort the contents of the column or choose which columns you want to see in the Rule Library list.

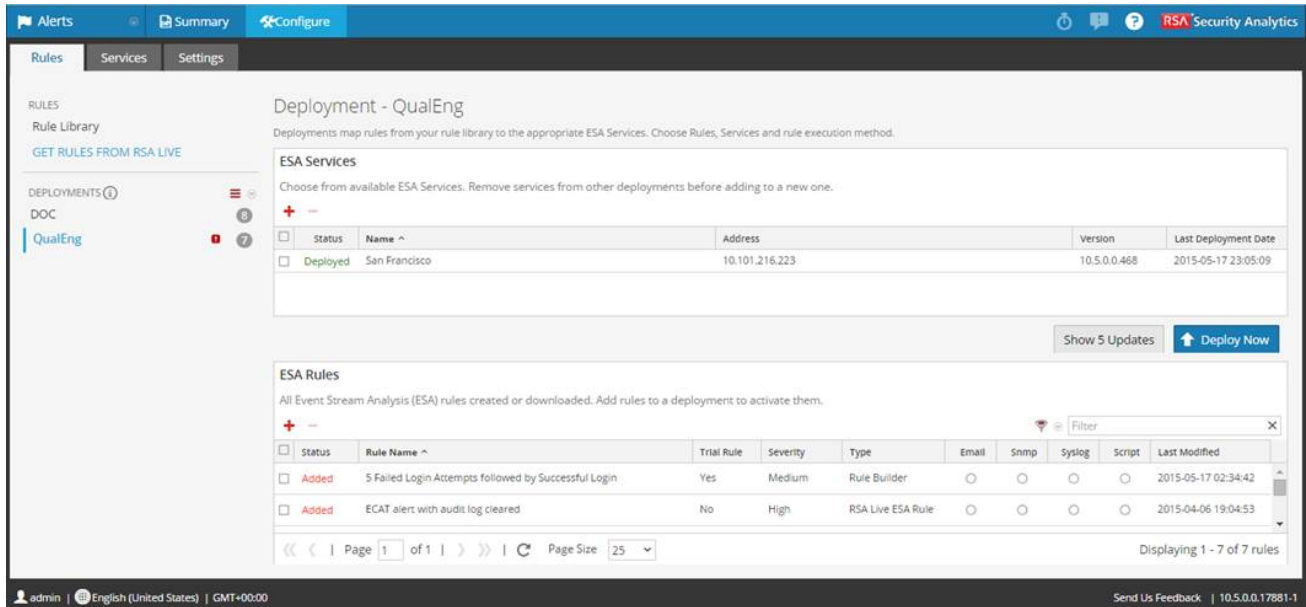


Deployment Panel

This topic provides an overview of the Deployment panel. The Deployment panel enables you to create and configure the deployments. The Deployment panel includes the following sections:

- ESA Services
- ESA Rules

The following figure shows the Deployment panel.





Features

ESA Services

Using the ESA Services section, you can manage each ESA service in the deployment.

In the ESA Services section, you can perform the following.

Task	Description
	Add an ESA service to the deployment.
	Remove the selected ESA service from the deployment.
Show Updates	Open the Updates to the Deployment dialog.
Deploy Now	Deploy current set of rules.





The following table lists the parameters of the ESA Services section.

Parameter	Description
Status	Indicates if the deployment status is Added , Deployed , Updated , or Failed .
Name	Name of the ESA service.
Address	IP address of the host where the ESA service is installed.
Version	Version of the ESA service.
Last Deployment Date	The date and time when the ESA service was last deployed.

ESA Rules

In the ESA Rules section, you manage rules in the deployment. This section lists all rules that are currently in the deployment.

In the **ESA Rules** section, you can perform the following.

Task	Description
	Open the Deploy ESA Rules dialog, where you can select a rule.
	Remove the selected ESA rules from the deployment.
	Filter the list of rules.
	Search for a rule.




The following table lists the parameters of the ESA Rules section.

Parameter	Description
Status	Indicates the rule status: <ul style="list-style-type: none"> • Deployed - the rule is deployed. • Updated - the rule has been updated since the last deployment. • Added - the rule has been added since the last deployment. • Failed - the deployment failed.
Rule Name	Purpose of the ESA rule.
Trial Rule	Deployment mode to see if the rule runs efficiently.
Severity	Threat level of alert triggered by the rule.
Output	The type of the ESA rule.
Email, SNMP, Syslog, Script	Indicates which notification types are used for alerts generated by the rules.
Last Modified	The date and time when the ESA rule was last modified.

Rule Syntax Dialog

This topic describes the features of the Rule Syntax dialog. The Rule Syntax dialog displays the EPL syntax of conditions, statements, and debugging parameters, and provides a warning when the syntax is invalid.

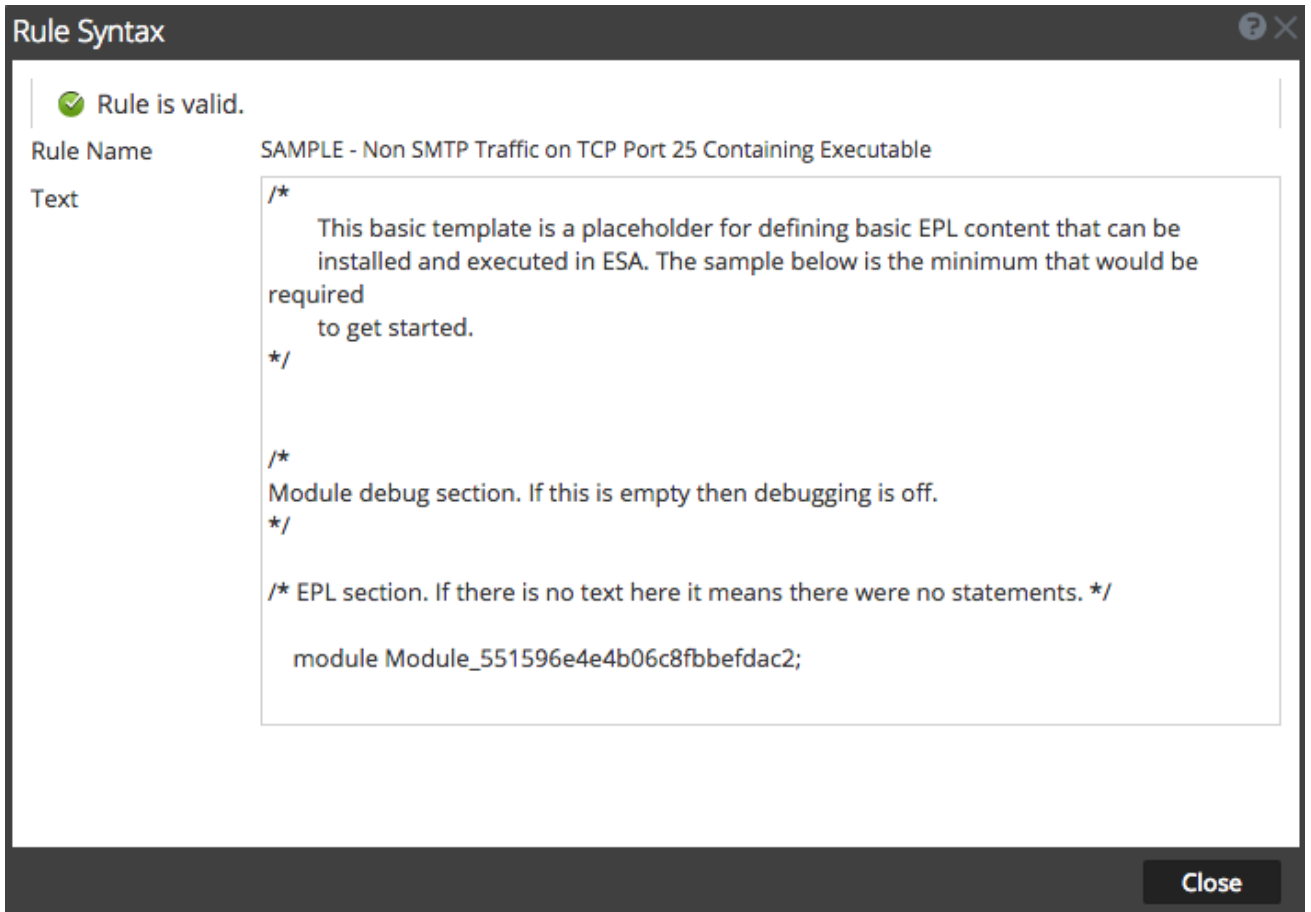
To access this dialog:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
2. In the **Rule Library** view, do one of the following:
 - a. Click  and select **Advanced EPL** or **Rule Builder**.
 - b. Double-click an existing rule.
 - c. Select an existing rule and click  in the **Rule Library** toolbar.
 - d. In the row of an existing rule, select  > **Edit**.

The new or existing rule is displayed in a new tab, available to edit.

3. Click **Show Syntax** at the bottom of the tab.

The following figure is an example of the Rule Syntax dialog.




Features

The following table describes the Rule Syntax dialog parameters.

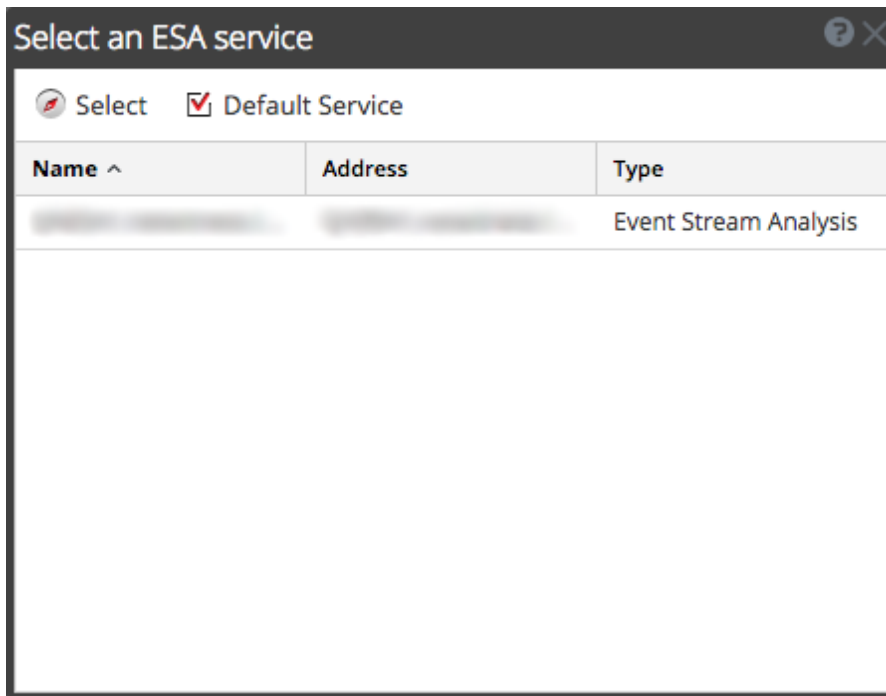
Parameters	Description
Rule is valid or Validation error in rule	Indicates whether the rule syntax is valid or needs to be changed.
Rule Name	Displays the name of the rule.
Text	Displays the EPL syntax of conditions, statements, and debugging parameters if the rule is valid.

Select an ESA Service Dialog

This topic describes the features of the Select an ESA Service Dialog. The Select an ESA Service dialog displays all available ESA services. Selecting a service allows you to view a summary of the service in the Summary view.

To access this dialog, in the Security Analytics menu, select **Alerts > Summary**. If the Select an ESA Service dialog is not displayed automatically, click .

The following figure is an example of this dialog.



Features

The following table describes the features of the Select an ESA Service dialog.

Parameters	Description
Select	Displays the Summary view for the selected service.
Default Service	Designates a default service. The Summary view will automatically display for the default service.
Name	Displays the name of the ESA service.
Address	Displays the address of the ESA service.

Parameters	Description
Type	Displays the type of service.

Services Tab

This topic provides an overview of the **Alerts > Configure > Services** tab. The Services tab provides details of the ESA services added to Security Analytics.

The following figure shows the Services tab:

The screenshot displays the 'Services' tab in the RSA Security Analytics interface. The main section is titled 'ESA - Event Stream Analysis'. It contains three summary panels: 'Engine Stats', 'Rule Stats', and 'Alert Stats'. Below these is a 'Deployed Rule Stats' table with columns for 'Enable', 'Name', 'Trial Rule', 'Last Detected', and 'Events Matched'. The interface also includes navigation tabs (Rules, Services, Settings), a top navigation bar (Alerts, Summary, Configure), and a footer with user information and version details.

Engine Stats		Rule Stats		Alert Stats	
Esper Version	5.3.0	Rules Enabled	11	Email	0
Time		Rules Disabled	0	SNMP	0
Events Offered	0	Events Matched	0	Syslog	0
Offered Rate	0 per second / 0 max			Script	0
				Storage	0
				Message Bus	0

Enable	Name	Trial Rule	Last Detected	Events Matched
<input checked="" type="checkbox"/>	Demo_toLowerCase	No		0
<input checked="" type="checkbox"/>	Pattern Match Rule: 5 fail 1 success	No		0
<input checked="" type="checkbox"/>	Destination Port	No		0
<input checked="" type="checkbox"/>	ArraynString checking	No		0
<input checked="" type="checkbox"/>	ADV: Multiple_FailedLogin_SuccessfullLogin	No		0
<input checked="" type="checkbox"/>	10F1S-Multiple meta - Demo - Multiple Group by	No		0

The Services tab has the following sections:

- ESA Services panel
- General Stats panel
- Deployed Rule Stats panel

Features

ESA Services Panel

The ESA Services panel lists the name of each ESA service added to Security Analytics.

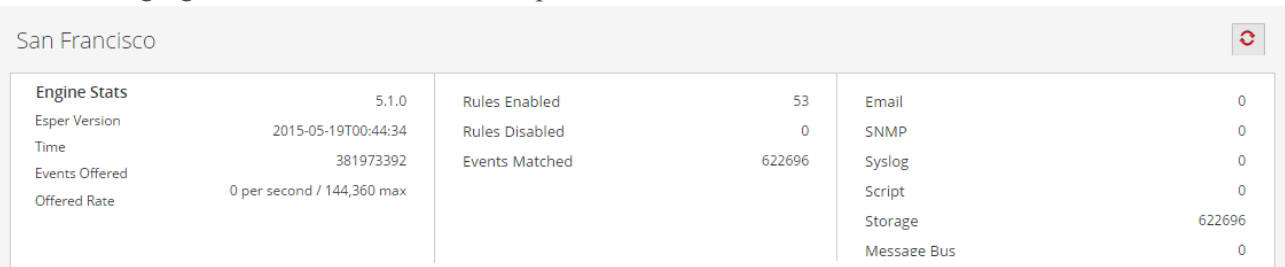
General Stats Panel

The General Stats panel provides information on the Esper engine, rules and alerts.

The General Stats panel contains the following sections:

- Engine Stats
- Rule Stats
- Alert Stats

The following figure shows the General Stats panel.



Engine Stats		Rule Stats		Alert Stats	
Esper Version	5.1.0	Rules Enabled	53	Email	0
Time	2015-05-19T00:44:34	Rules Disabled	0	SNMP	0
Events Offered	381973392	Events Matched	622696	Syslog	0
Offered Rate	0 per second / 144,360 max			Script	0
				Storage	622696
				Message Bus	0

The table lists and describes the parameters in each section.

Sections	Parameter	Description
Engine Stats	Esper Version	Esper version running on the ESA service
	Time	Time when the last event was sent to Esper Engine
	Events Offered	Number of events analyzed by the ESA service since the last service start
	Offered Rate	Current events offered rate on the ESA service
Rule Stats	Rules Enabled	Number of rules enabled.
	Rules Disabled	Number of the rules disabled
	Events Matched	Total number of events matched to all rules on the ESA service

Sections	Parameter	Description
Alert Stats	Email	Number of email notifications sent by the ESA service
	SNMP	Number of SNMP notifications sent by the ESA service
	Syslog	Number of Syslog notifications sent by the ESA service
	Script	Number of Script notifications sent by the ESA service
	Storage	Total number of alerts stored in database
	Message Bus	Total number of alerts sent to the message bus

Deployed Rule Stats Panel

The Deployed Rule Stats panel provides details on the rules that are deployed on the ESA service.

The following figure shows the Deployed Rule Stats panel.

Deployed Rule Stats					
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		See Health & Wellness to monitor rule memory usage.			
<input type="checkbox"/>	Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - P2P Software as Detected by an Intrusion Detection Device	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	ECAT alert with audit log cleared	No		0
<input type="checkbox"/>	<input checked="" type="radio"/>	HTTP GET Flood	Yes		0

Page 1 of 1 | Page Size 25 | Displaying 1 - 7 of 7

The table lists the various parameters in the view and their description.

Parameters	Description
<input checked="" type="radio"/>	Indicates the rule is enabled. Enables a rule that was disabled.
<input type="radio"/> Disable	Indicates the rule is disabled. Disables a rule that was enabled.
Health & Wellness	Displays a snapshot of memory usage when trial rules get disabled

Parameters	Description
Enable	Indicates whether the rule is enabled or disabled. Green icon indicates rule is enabled. White icon indicates rule is disabled.
Name	Name of the ESA rule.
Trial Rule	Indicates if the rule is running in trial rule mode.
Last Detected	The last time alert was triggered for the rule.
Events Matched	The total number of events that matched the rule.

Settings Tab

This topic describes the components of the Settingstab. In the Settingstab, you can perform the following tasks:

- View a list of meta keys
- Configure a data enrichment source
- Add a connection to an external database

The following figure shows the Meta Key References section in the Settings tab.

The screenshot shows the 'Meta Key References' section in the Settings tab of the RSA Security Analytics interface. The table below represents the data shown in the screenshot:

Name ^	Type
OS	string
access_point	string
accesses	string
action	string[]
ad_computer_dst	string
ad_computer_src	string
ad_domain_dst	string
ad_domain_src	string
ad_username_dst	string
ad_username_src	string
alert	string
alert_id	string
alias_host	string[]
alias_ip	string[]
alias_ipv6	string[]
alias_mac	string

At the bottom of the table, it indicates 'Page 1 of 7' and 'Page Size 25'. The status bar at the bottom shows 'Displaying 1 - 25 of 173 Meta Key References'.

Features

Meta Key References

The Meta Key References section lists each meta key and the type of value the key requires.

Enrichment Sources

In the Enrichment Sources section, you can configure the following external data sources:

- GeoIP
- External Database Reference
- In-Memory Table
- Warehouse Analytics

The following figure shows the Enrichment Sources section in the Settings tab.

The screenshot displays the RSA Security Analytics interface. At the top, there are navigation tabs for 'Alerts', 'Summary', and 'Configure'. Below this, a sub-menu shows 'Rules', 'Services', and 'Settings', with 'Settings' being the active tab. On the left side, a sidebar menu lists 'MISCELLANEOUS', 'Meta Key References', 'Enrichment Sources' (highlighted), and 'Database Connections'. The main content area is titled 'Enrichment Sources' and contains a table with the following data:

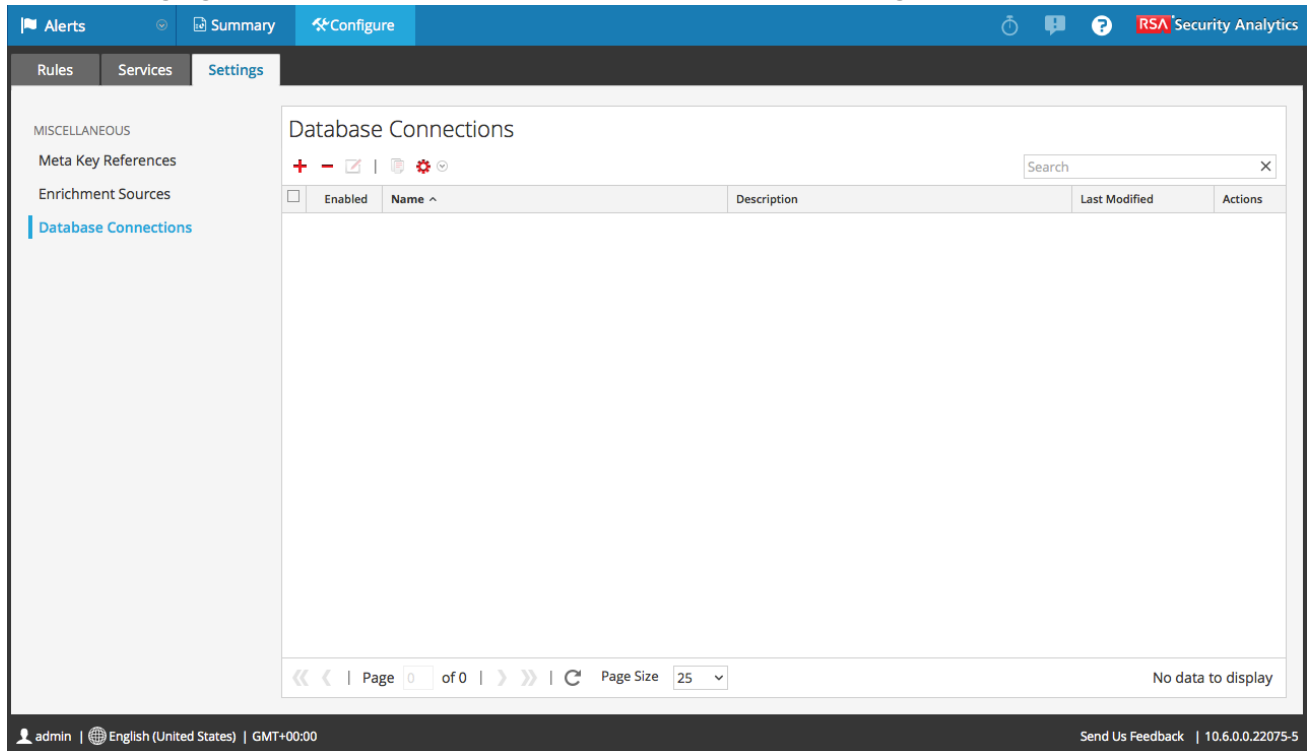
<input type="checkbox"/>	Enabled	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	●	Default GeolP	GeolP	Default Geo IP Enrichment Source. This canno...	2016-02-12 06:13:07	
<input type="checkbox"/>	●	Gold_CSV	In-Memory Table		2016-02-15 04:07:02	
<input type="checkbox"/>	●	Sunila_CSV	In-Memory Table		2016-02-16 07:06:05	

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and 'Page Size 25'. The footer of the interface includes the user 'admin', language 'English (United States)', time zone 'GMT+00:00', a 'Send Us Feedback' link, and the version number '10.6.0.0.22075-5'.

Database Connections

In the Database Connections section, you can configure a connection to an external database so ESA can access that data.


The following figure shows the Database Connections section in the Settings tab.



In the Database Connections section you can perform the following:

- Add a Database Connection
- Delete a Database Connection
- Edit a Database Connection
- Duplicate a Database Connection
- Import a Database Connection
- Export a Database Connection

Updates to the Deployment Dialog

The Updates to the Deployment dialog displays changes to the deployment, such as adding a rule or service. Deployment updates are indicated by the update icon () next to the name of the deployment in the Rules tab options panel.

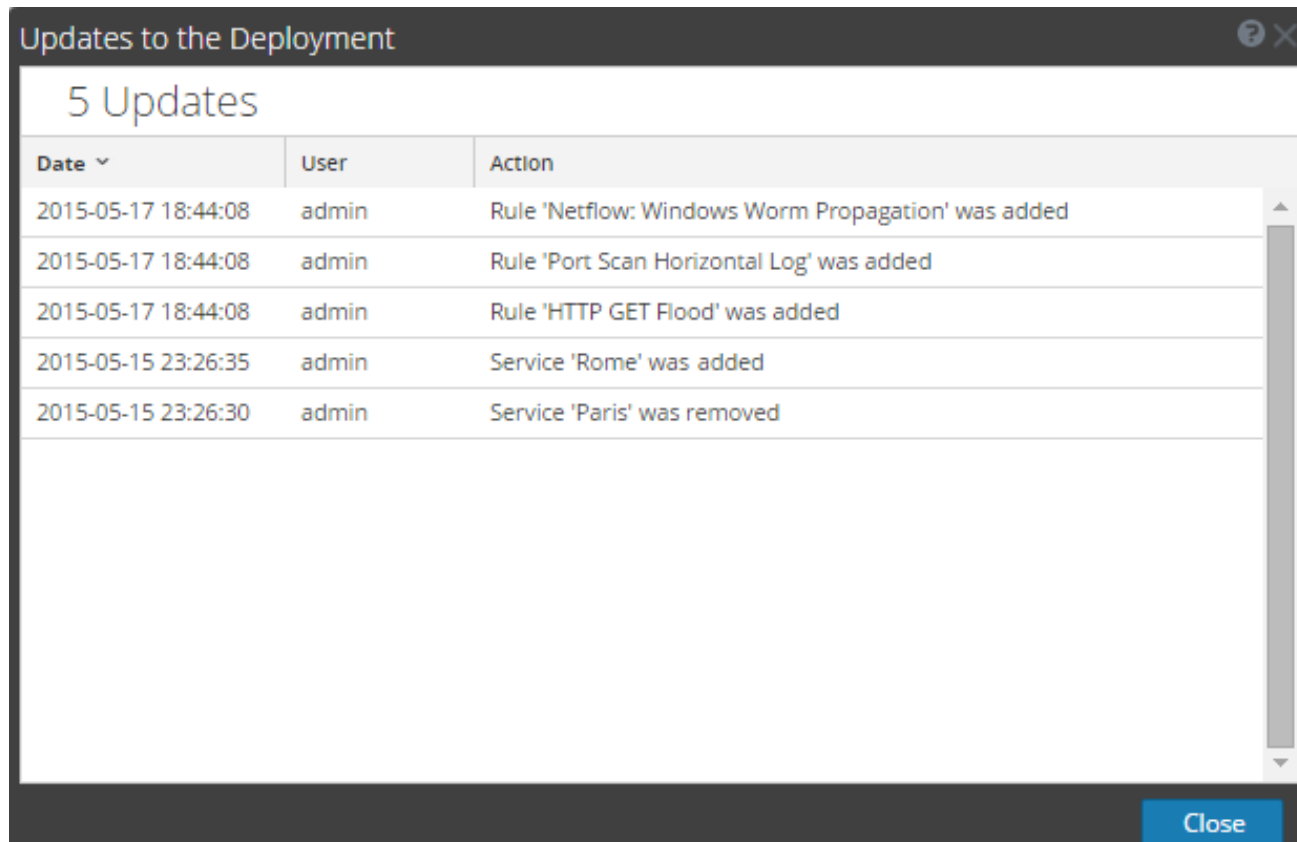
To access this dialog:

1. In the **Security Analytics** menu, select **Alerts > Configure**.
The Rules tab is displayed by default.
2. In the options panel, under the **Deployments** section, select or add a deployment.

- In the **Deployment** panel, click **Show Updates**.

The Updates to the Deployment dialog is displayed.

The following figure is an example of this dialog.



Features

The Updates to the Deployment dialog displays the number of updates at the top of the dialog. The following table describes the parameters of this dialog.

Parameters	Description
Date	Displays the day and time of the update.
User	Displays the user who made the update.
Action	Describes the update.