NetWitness® Platform XDR

Version 12.0

Reporting User Guide

NETWITNESS

Platform XDR

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

July, 2022

Contents

Reporting Overview

Reporting is a collection of data as a result of monitoring the network traffic, which can be used for further analysis. In NetWitness you can run a report against NetWitness Database core services to identify the network activities. For example, if you want to identify the Top Source Countries and Destination Countries, or top Threat and Risk trends that help monitor any changes to the normal categories or monitor the users and services that may potentially have malicious activities etc.

The reporting typically consist of: Reports and Charts. You can report on the log, packet and endpoint data collected, and customize the reports and charts to enhance the visual appearance. You can create real-time reports for historical data. You can create charts and dashlets, that can be added in the real-time chart dashlets as well.

Reporting Engine

Reporting relies on the Reporting Engine to provide data for the reports, alerts and charts. Hence, you must configure the Reporting Engine as a service to NetWitness before you can generate the reports. You must also specify the data source in the Reporting Engine from which the data is extracted.

The data that you can report or alert depends on the configuration of Reporting Engine and the data sources that you specify as part of the rule definition.

Note: Make sure you have access to the components in the Reporting.

Note: Reporting is accessible based on the role based access, defined for the user.

Report

A report is a combination of rules and other formatting objects such as headers and HTML-formatted notes that describe and identify data pertaining to a particular area of interest. Reports are defined and managed in the Build Report page and can be scheduled to run on an adhoc or timely basis. Once a report is run, results are stored centrally and can be automatically sent over email, SFTP, URL, and NFS to users, viewed via the NetWitness web interface, downloaded as PDF and CSV files.

A report consists of the following:

Property	Description	Example
Report Name **Note:** For **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.	Used to identify the report to schedule them at a later time.	Report1
Text	Pre-defined text fields used within a report to make the report more meaningful to the user.	Header1, Comment
Rules	The rules (queries) used to create a report.	select user.dst where ip.src = 10.10.10.1

Note: In the Reporting user interface, the displayed date or time is always according to the user-selected time zone profile.

Rule

A rule is the basic and essential building block in the Reporting. You must create a rule which can be used in a Report, Chart or Alert.

A rule represents a unique query that detects and summarizes the requested information within a collection of network data.

The rule syntax is very similar to that of Standard Query Language (SQL) where you can use the select clause, where clause, sort and group options and limits for the result set. A rule consists of the following:

Property	Description	Example
Name	The name of the rule.	Windows System Account Activity
Select	List of meta types that are returned in the result set. The list of meta types is provided in the Meta Library. Meta Library in the Rule Builder is continually synchronized with the index configuration of the NetWitness host to which NetWitness is connected. The number of meta types that this property can represent depends on how the rule is to be sorted. If the Sort by property is 'None' or Custom, a rule can have more than one select field, for example, for each match, include the ip.src, ip.dst, size, time in the rule result. If a rule is set to be sorted, either by session count, session size, or packet size, then there can only be one field on which to select.	
Where	A clause that is the base query for the rule.	alert='cleartext_ftp_password'
Then (Rule Actions)	A series of functions that manipulate the original result set of a rule in order to make the output in a report more meaningful or add additional functionality other than querying and displaying data.	lookup_and_add ('username','ip.src',10);
Sort By	Determines how the data in the result set is sorted. The various possibilities are: • Total • Value • Column Name	Total
Limit	Designates how large a result set can be for the given rule. Users must note that if a result set is sorted by count or size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.	20

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

Rule Types

There are different rule types in the Reporting. Rule types designate the source of data for the report rule. Following are the rule types:

Rule Type	Description
NetWitness Database (**NetWitness DB**)	The NetWitness database extracts the meta from a Reporting Engine configured to use a Concentrator, Broker and Archiver as the data sources and provides the meta for rules.
Warehouse Database (**Warehouse DB**)	The Warehouse database, also referred to as the NetWitness Warehouse, warehouses large volumes of data. The Warehouse is designed so that you can retrieve large volumes of data easily and efficiently. The Warehouse also extracts the meta from the Reporting Engine.
Respond Database (**Respond DB**)	The Respond database contain alerts and incidents generated from different services and you can create a report on those alerts and incidents.
Unused Rules	The Unused Rules is an option that helps in listing out the rules that are not used by any chart, alert and, report. For more information, see Filter Unused Rules.

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

List

A list is a variable that refers to a series of comma-separated values (CSV). You can insert a list into a rule or use it as an argument to a rule action. Lists can act as placeholders for other values, which you can populate and update as needed.

You can create, manage and view lists that can be used to define rules for Reporting and Alerting. You can also filter and delete the unused lists.

Lists cannot be empty or have duplicate or blank values.

Note: If you are defining a report with a rule which has lookup_and_add in the **Then** clause and direct the report output to a list, the list is not populated with the result.
For example, if you create a rule with ip.src in the **Select** clause and lookup_and_add ('ip.dst','ip.src', 10) in the **Then** clause, the report displays the result, but if you have redirected the output to a list, the list will be empty

Chart

Chart is a tabular or grid representation of data. It consists of the following:

Property	Description	Example
Chart Name	Identifies the chart.	Chart1
Rule Basis	Identifies the rule path chosen from the folder hierarchy.	

Any NetWitness DB rule in the Reporting Engine system which is not sorted by none can be used to instantly create a chart. In NetWitness, the chart interval can be adjusted from the chart definition panel itself. Each time a chart runs, it stores its result data locally in the Reporting Engine, so that it can be reviewed in either the Dashboard View or Chart View without any performance considerations. You can also filter the unused charts from Chart View.

Note: In the Reporting user interface, the output for the field where Date and Time are displayed is always according to the user-selected time zone profile.

Note: The Reporting Engine (RE) will automatically check for the available disk space before you execute a Test Rule, Report, Chart and Alert. If the RE disk space (in percentage) is less than the minimum disk space threshold (default value is 5), the RE will stop the current execution and an error message 'Available disk space of Reporting engine home is <5%, please clean up the space to proceed further' is displayed. Additionally, you may also configure the minimum disk space threshold by using the following path: **RE>Config>General>System Configuration>Mini disk space threshold in %.**

Reporting Guidelines

This section lists recommended guidelines to enhance the execution time of your reporting entities such as rules, reports, alerts, charts, and lists. The guidelines are provided for the following:

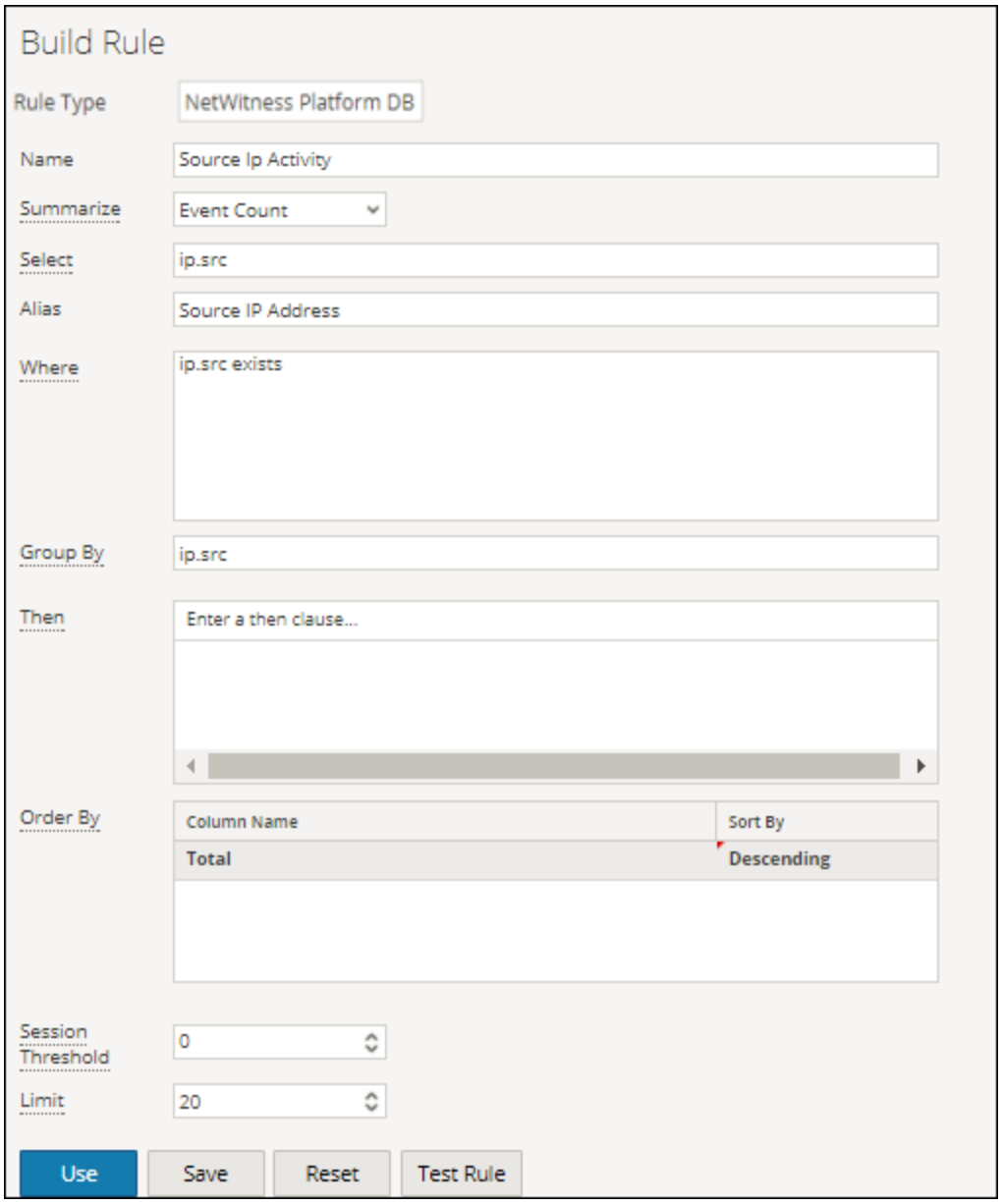
- NWDB Rules
- Timeout Configuration for NWDB Rules
- Lookup and Add rule action
- List value Reports

NWDB Rules

If the reporting entities such as report, alert, or chart contain NWDB rules (in most cases where the query contains Group By) takes a long time to execute, you may do the following:

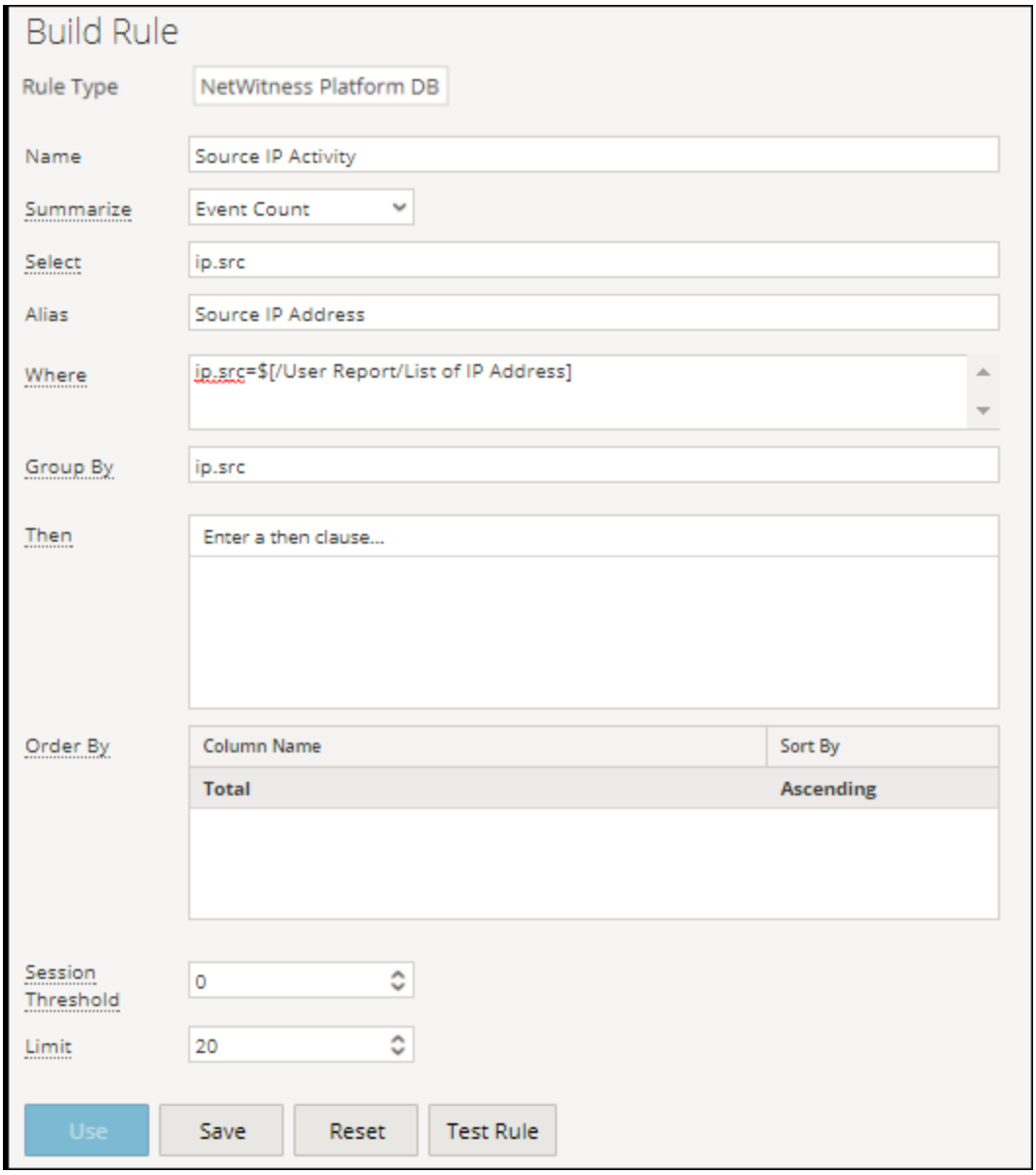
1. Refine the Where clause:

   You may limit the number of sessions scanned by using or refining the Where clause (especially when you use the Group By option). For example, consider the following rule.



If you use a Where clause as mentioned above, the number of sessions aggregated is huge. To avoid this, you can filter only required sessions by specifying the list of IP addresses or creating a List (list of IP Address) that contains relevant IP addresses.

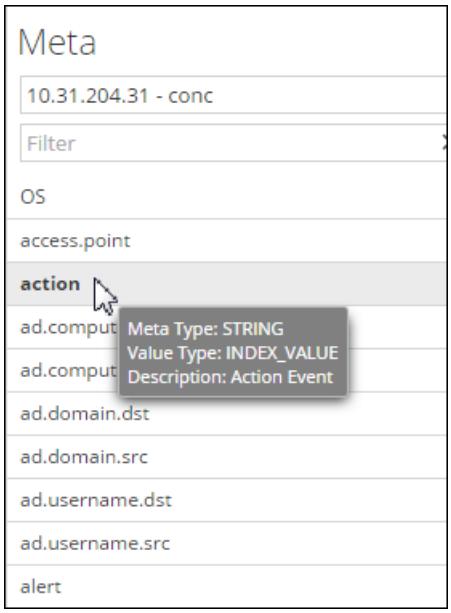
Note: The NWDB rule where clause is appropriately quoted if the syntax has an invalid quote. For example, in case of an invalid meta, or missing separator, the status and the error message is updated appropriately.



2. Using indexed Meta keys in the Where clause:

   To understand if the Meta is indexed or not, mouse hover the Meta List present on the right panel. If the Value Type is INDEX_VALUE, then the Meta is indexed. The Value Type is INDEX_KEY or INDEX_NONE if the Meta is not indexed.

   Below is a snapshot of a Meta key that is indexed.



3. Configure the Timeout option:

   If the query is taking a long time and fails due to timeout issues, you can configure the timeout for the NWDB rule executions. For more information, see below section "Timeout Configuration for NWDB Rules".

4. Schedule the queries to run at different times:

   If multiple query aggregates are concurrently executed and timeout occurs, you may schedule the queries to run at different times without much overlap.

Timeout Configuration for NWDB Rules

Note: It is a good practice to check the statistics of the Reporting Engine and the NWDB data sources before you make any changes to the configuration. For more information, see the "Monitor Service Details" topic for Reporting Engine and "Monitor System Statistics" topic in the *System Maintenance Guide*.

If NWDB rule execution fails due to timeout, you may get the following errors on the View a Report panel:

- Reporting Engine timeout error

  “Data source ‘`10.31.x.x Concentrator`' did not respond within the configured time `30` minutes for the ‘`/sdk/values`' request.”

- NWDB timeout error

  "Error occurred while fetching data from source '`10.31.x.x Concentrator`'. `{Timeout message from NWDB}`”

In such cases, you need do the following:

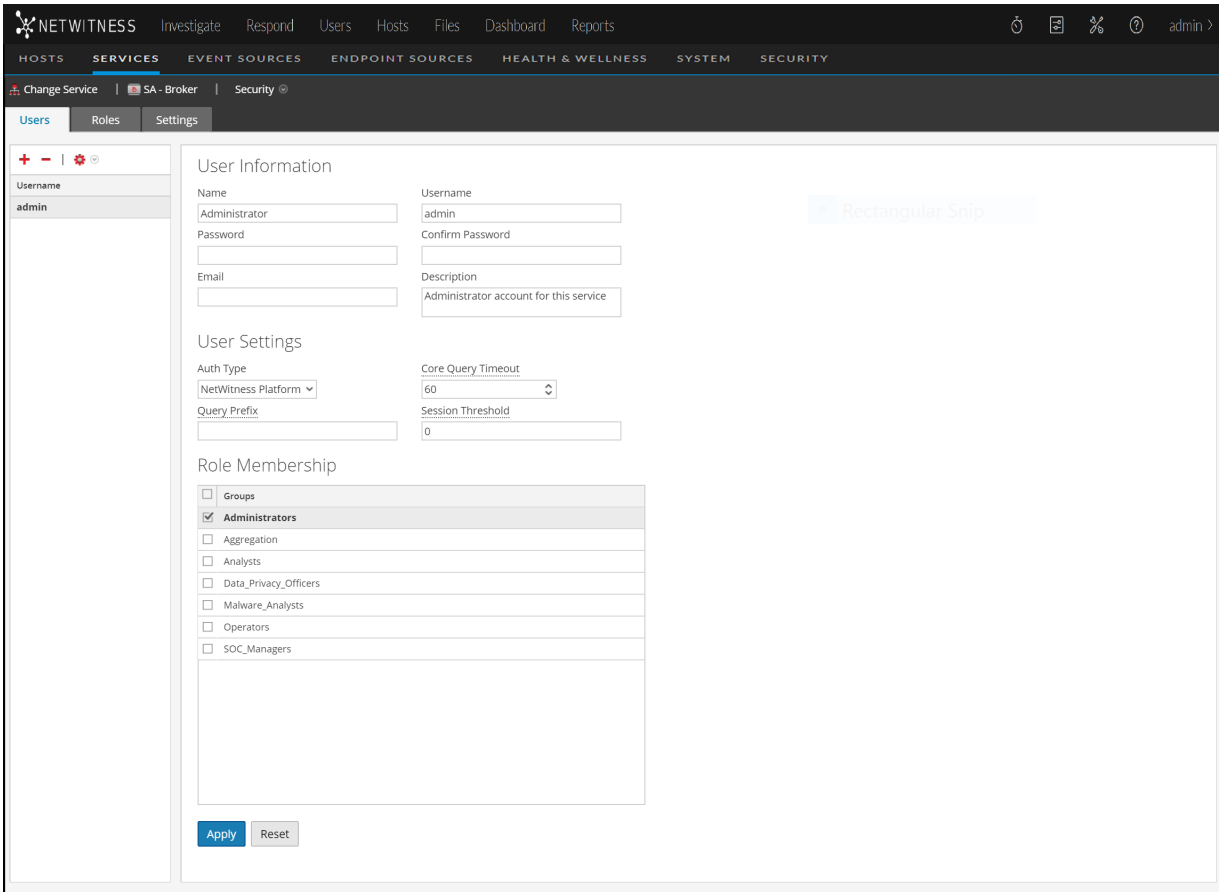
- Reporting Engine timeout

  In case of Reporting Engine timeout, you may set the timeout to a longer duration so the long running queries can be executed. For more information on setting the `NWDB Queries Time Out` and `NWDB Info Queries Time Out` option for the Reporting Engine, see "Step 2. Configure Reporting Engine Settings" topic in the *Reporting Engine Configuration Guide*. RSA recommends you set the `NWDB Query Time Out` to zero minutes (implies no timeout) and `NWDB Info Queries Time Out` to 60 minutes.

- NWDB timeout

  In case of NWDB timeout, you may need to configure the `query.level.timeout` and `max.concurrent.queries` parameters for the NWDB data source based on the recommendations in the *Core Database Tuning Guide* to fine tune the queries.

  The following figure is an example of Explorer view where you can set the parameters for NWDB data source.



- Schedule Reports at different times

  If the NWDB core devices are heavily utilized, you may schedule the reports to run at different times without overlap.

- Split the Report

If you have many rules in a Report, split the report into multiple reports with each report containing logical set of rules. If you have multiple rules, all rules will begin to execute at the same time based on available threads, therefore you may group the rules logically into separate reports.

Lookup_and_Add Rule Action

If a rule that consists of single or multiple `lookup_and_add` rule actions, takes a long time to execute the report, it is because each of the rule action triggers multiple lookup queries on the NWDB data source resulting in longer execution time.

To improve the report execution time, you may do the following:

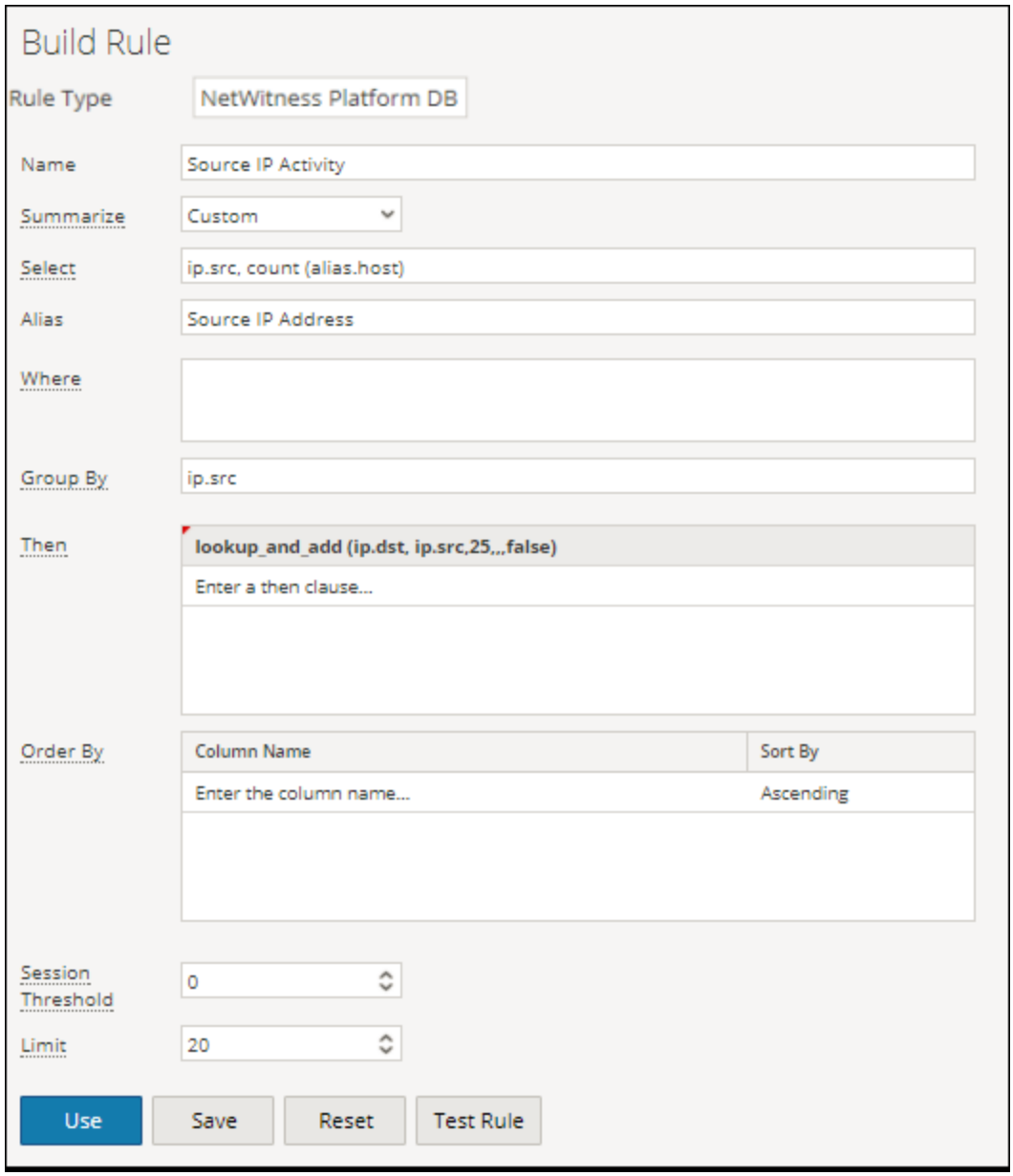
- Refine the Where clause in the following:
  - Rule that contains the `lookup_and_add` rule action
  - `lookup_and_add` rule action
- Set Limits

  You must set appropriate limits for the rule and rule actions. If the limit is high it will result in many queries being triggered and hence the report will take a long time to execute.
- Set the boolean aggregate parameter

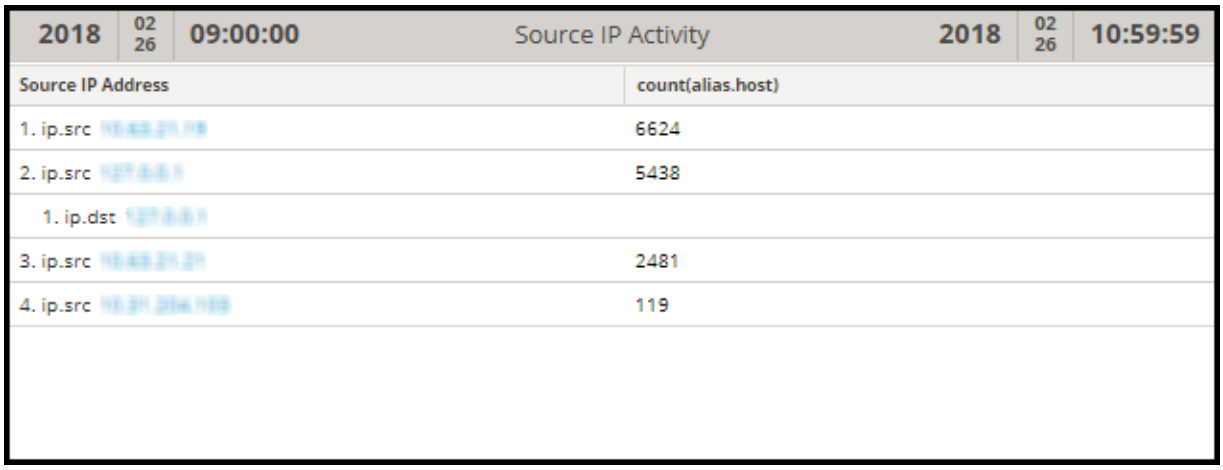
  If you do not want the aggregate value such as `sum(meta), count(meta)` etc. for the lookup values, set the boolean aggregate parameter to false in the `lookup_and_add` rule action. For more information, see the "NWDB Rule Syntax" section in Rule Syntax.

  ```
  lookup_and_add(string select, string field, int limit, boolean inherit,
  string extraWhere, boolean aggregate)
  ```

  Consider the rule with lookup_and_add rule action:



The output is displayed:

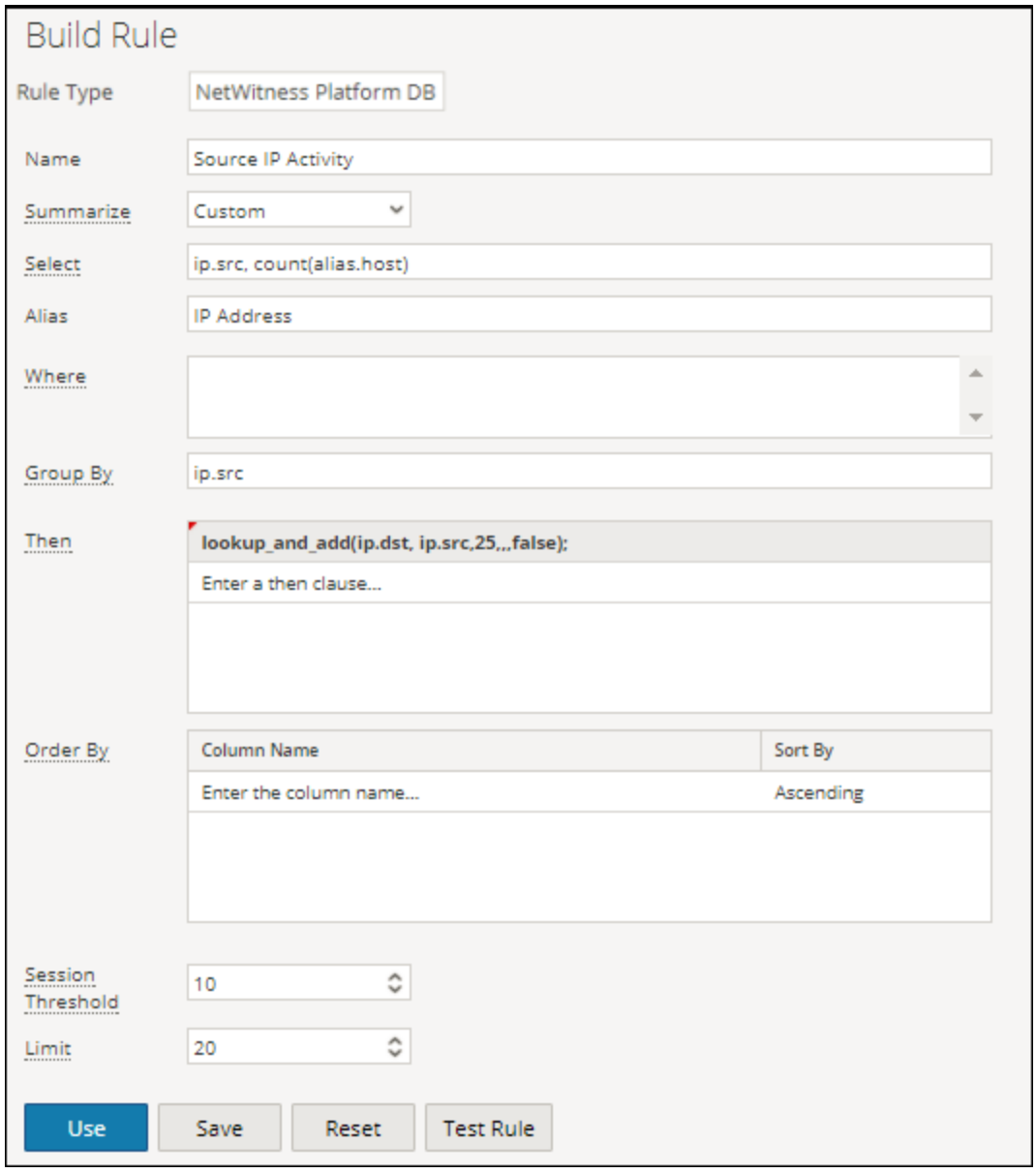


- Each `lookup_and_add` rule action triggers by default two concurrent lookup queries on the data source. NetWitness recommends that you retain the default setting, however if you want to increase the value you may want to ensure the value of `Max # of Concurrent LookupAndAdd Queries` parameter in Reporting Engine is less than the `Max Concurrent Queries` value in the NWDB data source configuration.

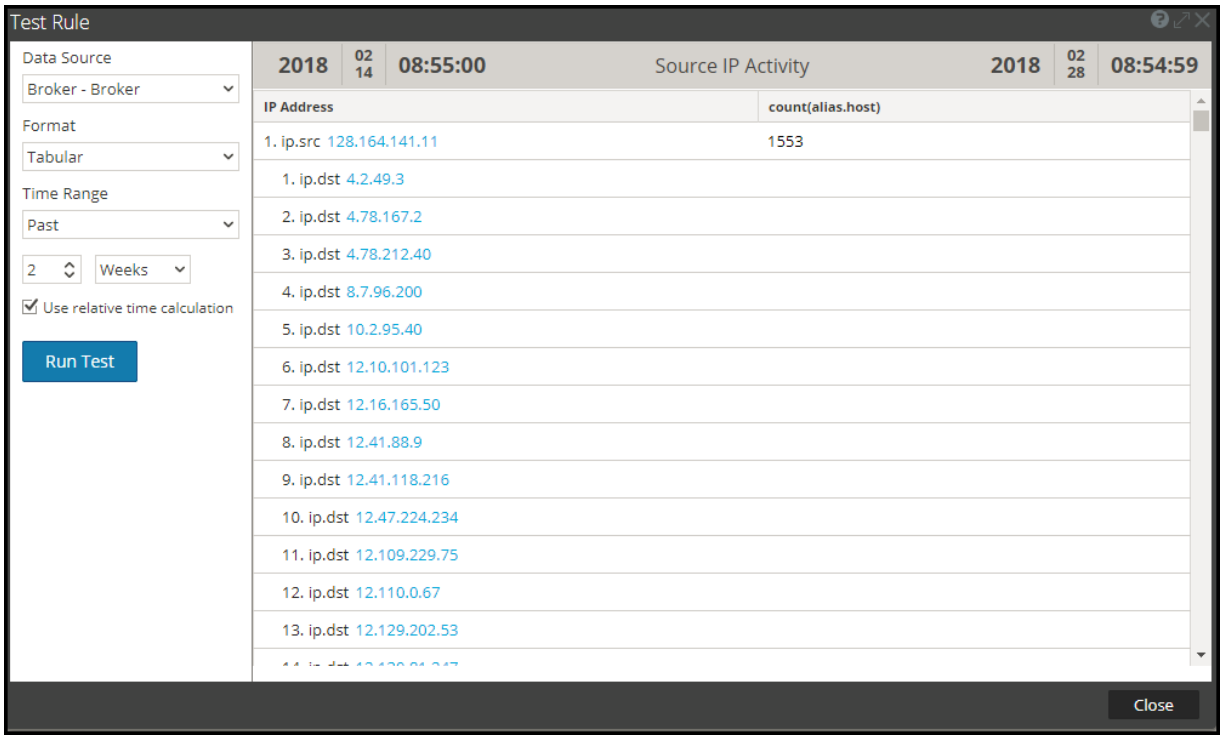
  If the NWDB data source is shared across other services, then you may retain a low value for the `Max # of Concurrent LookupAndAdd Queries` parameter in Reporting Engine as increasing it will impact the queries from other services. For more information, see "Reporting Engine General Tab" topic in *Reporting Engine Configuration Guide*.

- If you are interested only in unique values and not accurate aggregates, then set the `Session Threshold` to a non-zero value for the NWDB rule. For more information, see "Create a Rule Using NetWitness Data Source" section in Configure a Rule. The higher the value, the longer is the rule execution. If the value is set to zero it will take a longer time but will provide accurate aggregates.

  Consider a rule with lookup_and_add rule action and Session Threshold set to 10.



The output is displayed:



List Value Reports

Use a Refined List:

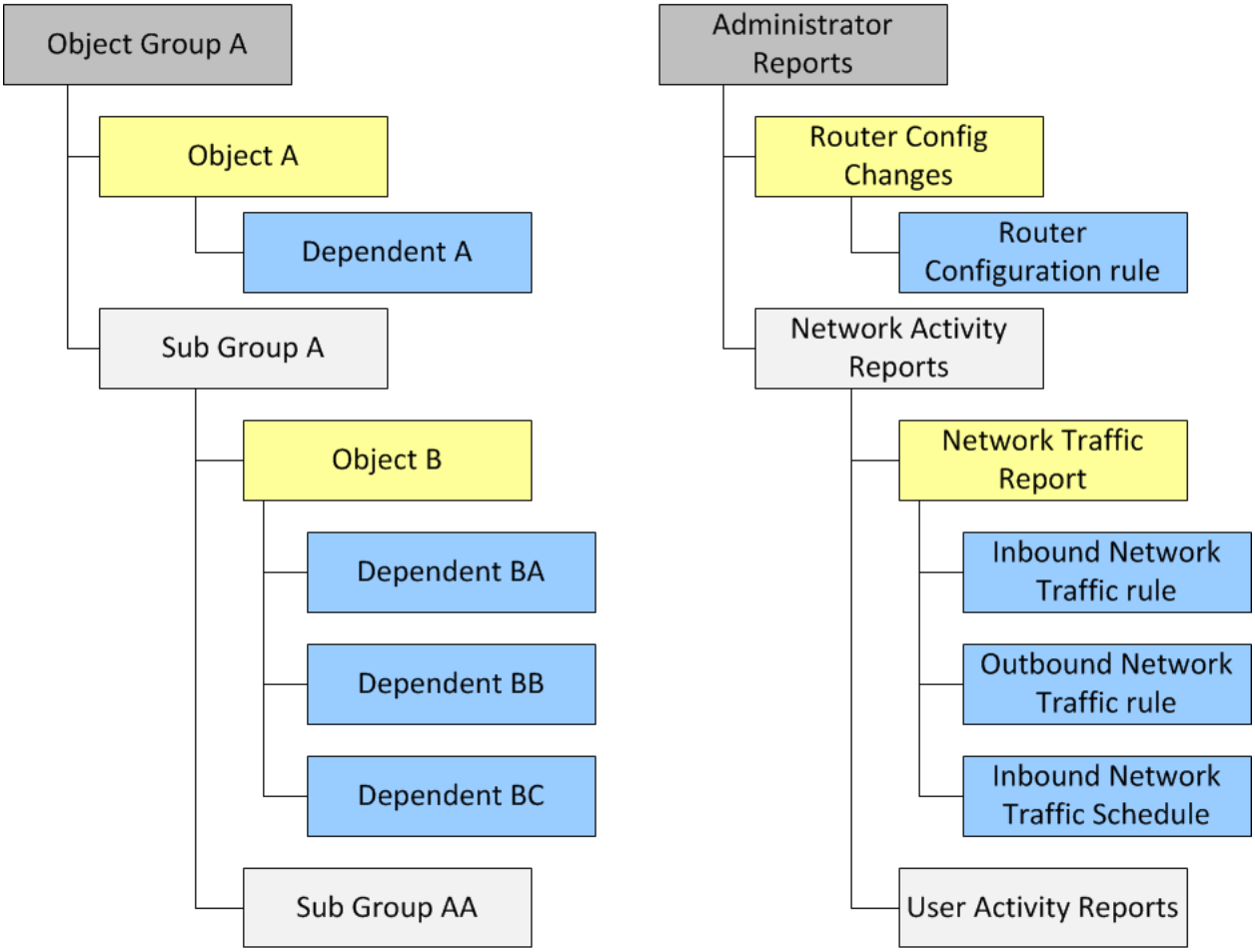
In case of List value reports (for any data source type), individual reports will be generated for each value in the list. Therefore, more the number of values in the list the longer the reports will take to execute. Hence, you must use a refined list to generate such reports.

Access Control for Reporting

Reporting Module provides you the option to set up access control for all the components in the module. In NetWitness, you can define different roles and specify the access control for each of the role from the System Security module. You can define the access control to be provided for the Reporting module for each role. For more information, see "Step 1: Review the Pre-Configured NetWitness Platform Roles" and "Step 2: (Optional) Add a Role and Assign Permission" topics in the *System Security and User Management Guide*.

In the Reports module, you can modify the role permissions or access to the following Reporting objects:

The Following is an example of the hierarchy of the object groups, objects and dependents. This is an illustration of the Report Groups and Reports hierarchy.



Report Groups and Reports Hierarchy

Permission for Object Groups

- You must have the Read & Write permission to set the permissions for the Object Group, Objects, or Dependents. The dependents with “No Access” permission are grayed out and dependents with “Read-Only” permission are indicated with an icon.
- When you set the permission for the Object Group, the Objects and Dependents in the Object Group do not inherit the permission automatically. You must select the "Apply these permissions to sub-groups and <Objects> in this group" option to achieve this. For example, if you do not want Operators roles to access reports in Report Group A, then you must set the permission on Group A to No access for the Operator role and select the "Apply these permissions to sub-groups and Reports in this group" option.
- When you set the permissions for the Object Group and select the "Apply these permissions to sub-groups and <Objects> in this group" option, the dependents such as rules or schedules in the objects do not inherit the permissions automatically. You must use the "Apply Read-only permission to Rules in the <Object>" option to apply the permission to the rules.

- When you set the permissions for the Objects, you must ensure that the Objects in hierarchy should always have a permission that is less than or equal to the one above in the hierarchy for the permission to be applied. For example, if the reports in a Report Group have Read & Write permission and you apply a Read-Only or No Access permission at the Report Group level and select the "Apply these permissions to sub-groups and Reports in this group" option, then the permission on the rules will remain unchanged.
- The permissions are cascaded from top to down in the hierarchy and not vice-versa. For example, if you apply a permission to a rule, it does not change the permission of the Report that contains the rule.

Permission for Objects or Dependents

- You must have the Read & Write permission to set the permissions for the Objects or Dependents.
- You can specify the permission for multiple objects at once instead of setting the permission for each object.
- When you set the permission for the Object, the dependents in the Object do not inherit the permission automatically. You must select the "Apply Read-only permission to Rules in the <Object>" option to achieve this.

When you apply the permission to dependents the permission is applied based on the existing permission for the role. For example, consider an Analyst and a Operator with the following permissions for the different dependents (Report A object has Rule AA, Rule AB, and Rule AC as dependents).

Object or Dependent	Analyst	Operator
Report A	Read & Write	No Access
Rule AA	Read & Write	No Access
Rule AB	Read and Write	Read and Write
Rule AC	Read-only	No Access

When the Analyst applies a Read & Write permission for the Operator role and selects the option "Apply Read-only permission to Rules in the <Object>", the permissions is set for the different dependents as follows:

Modify the Permissions

- **Group Level:** Set the permissions at the Object Group level and for all the object and entities in the Group. For example, if you have 80 reports in the Administrators Reports group and you do not want anyone except the Administrator to add or modify these reports, you can set the permission for all the other roles at the group level to Read-Only and select the option to apply it to all the reports and sub-groups in the report group.
- **Multiple Objects:**Select multiple objects and specify the access for all the selected objects. For example, if you have 10 reports in the Network Traffic sub group with sensitive information that you

do not want anyone to access, select the 10 reports and then set the permission for all the roles as "No Access".

- **Single Object:** Select only the object and specify the permission. For example, select the Network Traffic Report and specify the Read-Write permission for the Security Analyst role or select the Login Failure Alert and specify the Read-Write permission for a Security Analyst role.

Object or Dependent	Operator (Before Permission is applied)	Operator (After Permission is applied)
Report A	No Access	Read & Write
Rule AA	No Access	Read-only
Rule AB	Read and Write	Read & Write
Rule AC	No Access	Read-only

Roles and Permissions for Reporting Module

Although NetWitness has five pre-configured roles, you can add custom roles. For example, in addition to the pre-configured Analysts role, you can add custom roles for AnalystsEurope and AnalystsAsia.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to data
Analysts	Access to data but not to configurations
SOC_Managers	Same access as Analysts and an additional permission to handle incidents
Malware_Analysts	Access to malware events only

Depending on the user role, you can set the following access permissions to access the Reporting module components (Rules, Reports, Charts, Alerts, Lists):

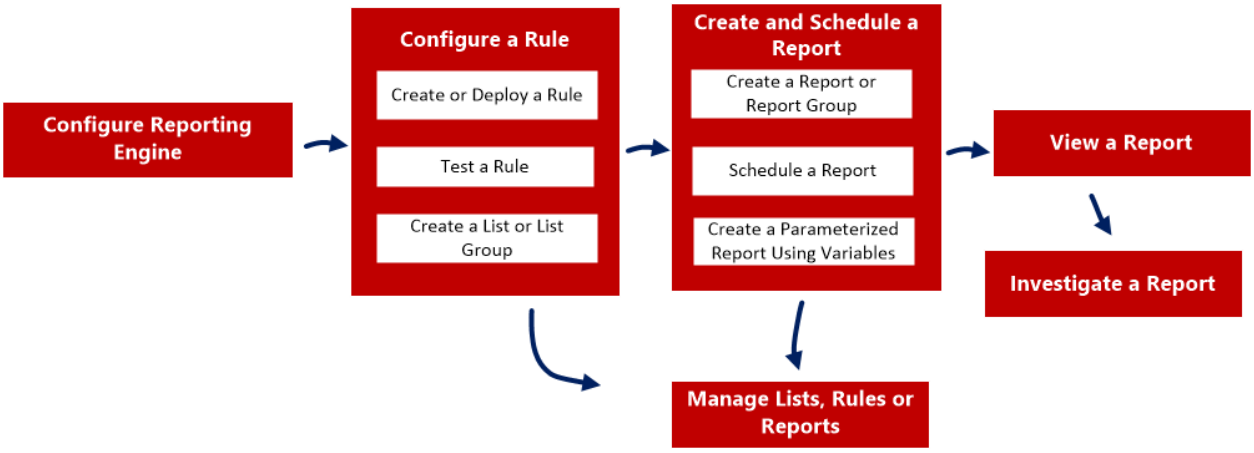
- Create
- Delete
- Export
- Manage
- View

Note: You must enable all these permissions for a user role to be able to define, delete, manage and view each of the Reporting modules. You must also have appropriate permissions for the data source to be listed, while defining the reports, charts, or alerts. For more information, see "Configure Data sources Permissions" topic in the *Reporting Engine Configuration Guide*.

For a detailed list of permissions and how to add a role and assign permissions, see "Role Permissions" and "Step 2. (Optional) Add a Role and Assign Permissions" topics in the *System Security and User Management Guide*.

Configure and Generate a Report

This figure is an overview of the entire process of configuring and generating a report.



To configure and generate a report, perform the following tasks:

1. Configure Reporting Engine - You must configure the Reporting Engine before you can configure and generate a report. You must also specify the data source in the Reporting Engine from which the data is extracted. For more information on how to configure Reporting Engine, see "Configure Reporting Engine" topic in the *Reporting Configuration Guide*.
2. Configure a Rule
3. Create and Schedule a Report
4. View a Report
5. Investigate a Report
6. Manage Lists, Rules or Reports

Configure a Rule

You can create a new rule or deploy an existing rule from the Live Services which can be used in a report. You can use different conditions to refine the data or information in the data sources such as:

- Select clause
- Where clause
- Group By
- Order By and so on

For example, you can write a rule to view the top 20 web addresses that the users visit daily.

You can create different type of rules using different data sources. Based on your requirements you can select any of the following options to create a rule:

- Create a Rule Using NetWitness Data Source
- Create a Rule Using Warehouse Data Source
- Create a Rule Using Respond Data Source

You can also use a list in a rule to refine a search result from the data source. Once a rule is created you can test a rule to see the results returned by the rule.

Create a Rule Group

To create a rule group or rule sub-group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Do one of the following.
   - To define a rule group:
     a. In the **Rules Groups** Panel, click  .
     The new rule group is added to the Rule Groups panel.
     b. Enter the name for the rule group and press ENTER.
   - To add a rule sub-group:
     a. In the **Rules Groups** panel, select the rule group to which you want to add a sub-group.
     b. Click  .
     The new rule sub-group is added to the rule group.
     c. Enter the name for the rule sub-group and press **ENTER**.

Create a Rule Using NetWitness Data Source

You can create a rule to fetch data or events from a NetWitness data source. The same procedure is used to define a rule to fetch data or events from an Archiver data source.

The Archiver data source can be added in the Services Config View of the Reporting Engine. For more information, see "(Optional) Add Archiver as a Data Source to Reporting Engine" topic in the *Archiver Configuration Guide*.

Prerequisites

Make sure that you understand how custom meta keys are created using custom feeds. For more information, see "Create Custom Meta Keys using Custom Feed" topic in the *Decoder and Log Decoder Configuration Guide*.

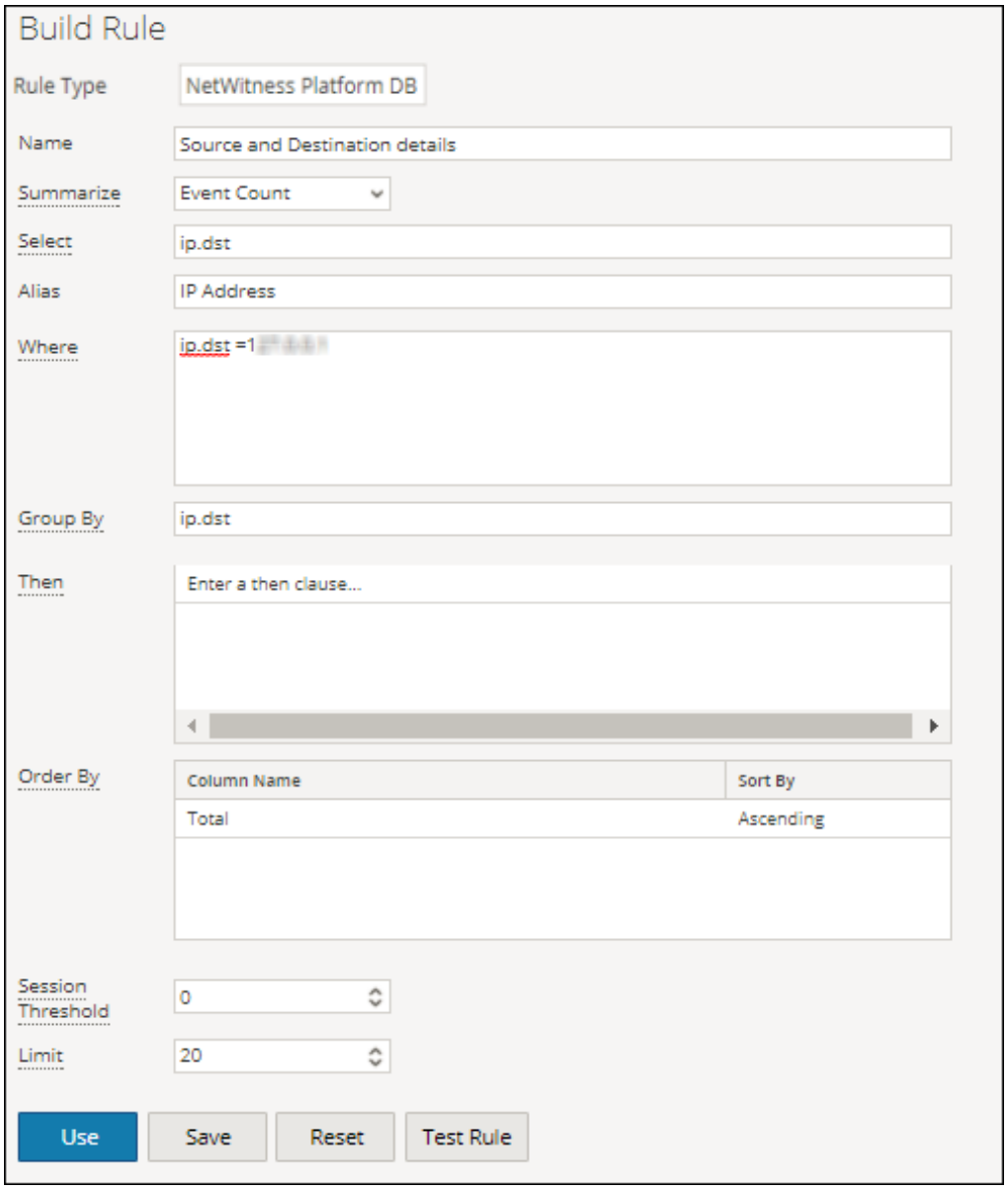
To create a rule to fetch data or events from a NetWitness Data Source, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** toolbar, click + > **NetWitness Platform DB**.

   The Build Rule view tab is displayed.



3. In the **Rule Type** field, **NetWitness Platform DB** is selected by default.
4. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.
5. The **Summarize** field determines the type of summarization or aggregation for the rule. Based on the type of rule to be defined, you must select one of the following:
   - To define a **Non-Aggregate** rule without any grouping, select: **None**
   - To define an **Aggregate** rule with special aggregation like the collection (sessions/events/packets) related aggregates, select one of the following:
     - Event Count
     - Packet Count
     - Session Size

- To define an **Aggregate** rule with meta values and custom aggregates like sum(), count(), and so on, select: **Custom**

  Choosing 'Custom' in the **Summarize** field enables you to define aggregate function of your choice in the *Select* clause. For example, select ip.src, countdistinct(ip.dst), distinct(ip.dst). The supported aggregate functions are:

  - sum (<meta>)
  - count(<meta>)
  - countdistinct(<meta>)
  - min(<meta>)
  - max(<meta>)
  - avg(<meta>)
  - first(<meta>)
  - last(<meta>)
  - len(<meta>)
  - distinct(<meta>)

  For more detailed information about Aggregate and Non-aggregate rule, see "NWDB Rule Syntax section" in Rule Syntax.

6. In the **Select** field, enter a meta or select a meta from the list of available meta types provided in the Meta Library. For more information, see "Meta Panel" in Build Rule View. The meta name to fetch raw log is raw. raw can only be used in the **Select** field. It cannot be used in the **Where** and **Then** fields. Multiple aggregate functions are supported for Custom aggregate rule in the **Select** field. For example, Select: *ip.src, username, service, distinct(country.src), sum(payload).*
7. In the **Alias** field, enter the alias name for columns used in the Select clause.
8. In the **Where** field, enter a meta or select a meta from the list of available meta types and use the operators to construct the Where clause for the base query criteria.
9. The **Group By** field is a read-only field which gets populated with meta that are defined in the Select clause. For a Non-Aggregate function, this field is not visible. A maximum of six meta are supported in the **Group By** field.

   Note: In earlier versions of NetWitness, only one meta was supported for Custom aggregate rule in the **Group By** clause. From now, a maximum of six meta are supported in the **Group By** clause.

10. In the **Then** field, enter the rule actions that manipulate the original result set of a rule in order to make the output in a report more concrete or add additional functionality other than querying data and displaying it, for example, creating a feed from the results. For a complete list of available rule actions, see "NWDB Rule Syntax" in Rule Syntax.

    Note: When a rule is executed for an Archiver data source, it is recommended not to use query intensive rule actions such as lookup_and_add() and show_whats_new().

11. In the **Order By** field, perform the following:

a. In the **Column Name** column, enter the name of the columns by which you want to sort the results. By default, the value is empty. The value gets populated based on the value selected in the **Summarize** field.

- For Summarize 'None', if no **Order By** is selected, then by default it is ordered by session or collection time.
- For other Summarize values, the default sorting is based on the first 'group by' meta selected when no 'order by' is defined. For Event Count, Packet Count, and Session size, the accepted values are Total and Value.

b. In the **Sort by** column, select one of the following ways to sort the results:

- Ascending Order
- Descending Order

12. In the **Session Threshold** field, enter the optimization setting to stop scanning the matching sessions for each possible unique value for the selected meta. The threshold is an integer between 0 (default) and 2147483647.

Note: This is applicable to only NWDB Aggregate rules. If the default value is specified, all the matching sessions will be scanned and the accurate value will be returned. A higher session threshold allows accurate counts for a value. However, this causes longer rule execution time. For example, consider you set the Session Threshold as 1000 for ip.src. If there are 5000 matching sessions then for a particular ip.src value which is present in more than 1000 sessions, NWDB stops the scan after 1000 sessions and returns the extrapolated aggregate value. This optimizes the query execution time. If the value is present in less than 1000 sessions, then the actual value is returned.

13. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by event count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.
14. Click **Save**.

Note: Unlike parsed meta, raw logs are fetched from decoders. When both raw log and parsed meta are queried in a single rule, due to different retention periods, parsed meta might be available and raw logs missing in the same session. So the result will have parsed meta values and empty raw value for those sessions. For example, for the rule Select **ip.src**, **ip.dst**, **service**, **username**, **raw**, the parsed meta might be populated and the **raw** meta remains empty for a few sessions.

Create a Rule Using Warehouse Data Source

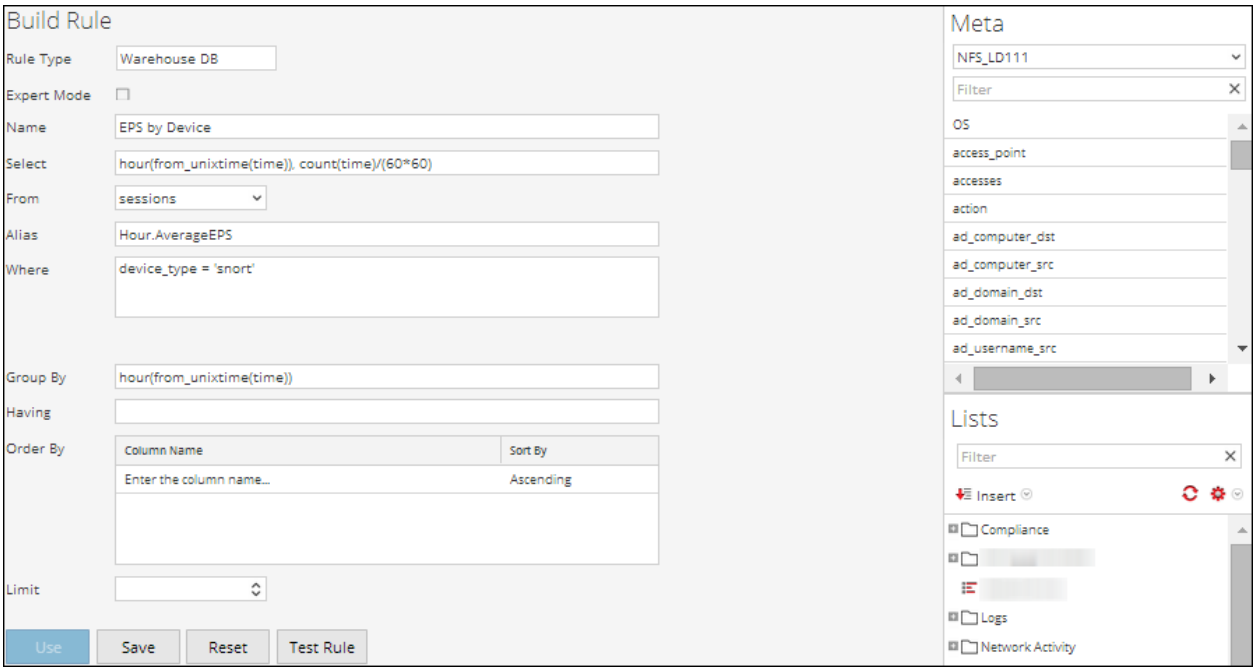
You can create a rule to fetch data or events from a Warehouse event source. You can define the rules in two modes:

- Default Mode
- Expert Mode

Default Mode

In Default Mode, you can create rules containing simple SQL like HIVE queries that contain clauses like Select, Where, Group By, and Having. By default, you can create rules to query sessions or raw logs. For more information on "Simple query syntax and examples", see Warehouse DB Simple Rules Syntax.

The following figure is an example of the **Build Rule view** that displays when you select **Warehouse DB** for **Rule Type** without the Expert Mode selected.

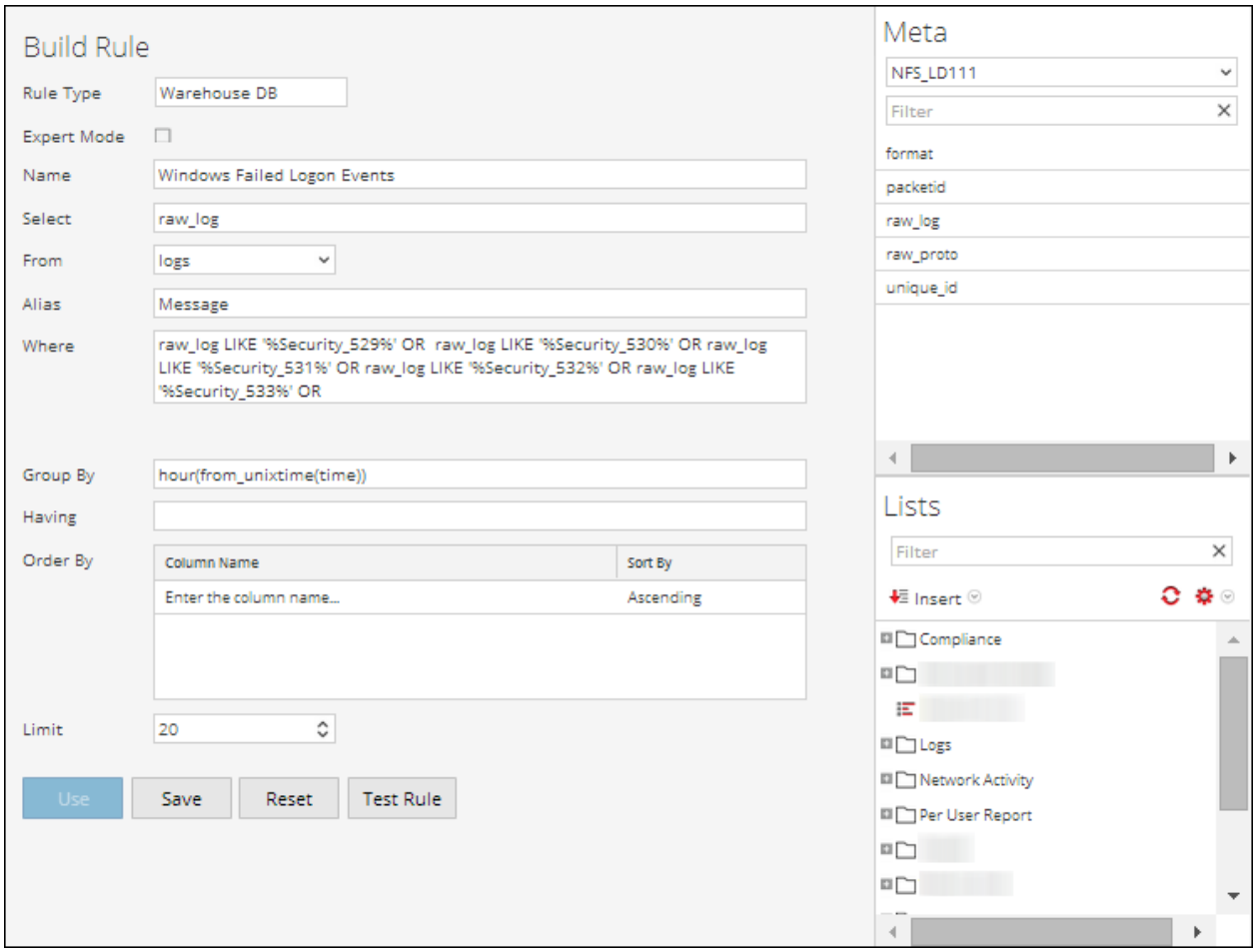


Querying Raw Logs

The raw log format is used in the select or where clause to query for raw logs.

Note: The time range that you can specify in your query is a day (24 hours). If you have specified a time range less than a day in your query, the result set contains data of at least a day (24 hours).

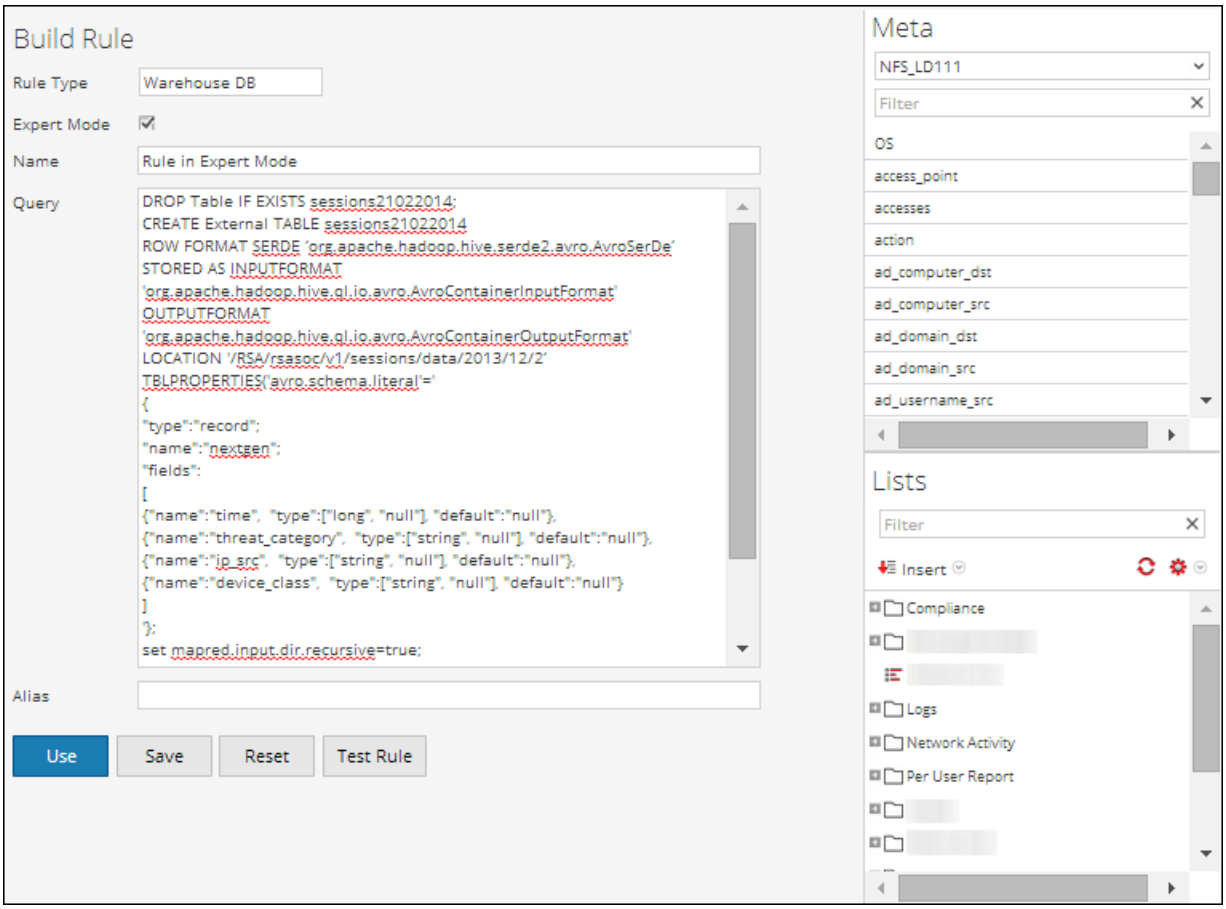
The following figure is an example of the **Build Rule view** that displays when you select **Warehouse DB** for **Rule Type** and create a rule for querying raw logs.



Expert Mode

Advanced rules are defined using complex HIVE queries created using the clauses DROP, CREATE, and so on. Unlike simple rules, we always insert the results into a table. For more information on "Advanced HIVE query language", see *HIVE language manual*.

The following figure is an example of the Build Rule view that is displayed when you select **Warehouse DB** for **Rule Type** with Expert Mode selected.



If you want to generate a report for a specific time range, you need to manually define the time range in the query using the following two variables:

- ${report_starttime} - The starting time of the range in seconds.
- ${report_endtime} - The ending time of the range in seconds.

For example, **`SELECT col1, col2 FROM custom_table WHERE timecol >= ${report_starttime} AND timecol <= ${report_endtime};`**

Note: By default, Reporting Engine treats `${keyword}` as a variable. If you want to specify HIVE variables, you must mention the complete syntax of a variable. For example, `${hiveconf:hive.exec.scratchdir}`.

Prerequisites

Make sure that you understand how custom meta keys are created using custom feeds. For more information, see "Create Custom Meta Keys using Custom Feed" topic in the *Host and Services Configuration Guide*.

To create a rule to fetch data or events from a Warehouse data source, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** toolbar, click  > **Warehouse DB**.

   The Build Rule view is displayed.

3. In the **Rule Type** field, **Warehouse DB** is selected by default.

   If you are defining the rule in Default mode, perform the following:

   a. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.

   b. In the **Select** field, enter a meta or select the meta from the drop-down or select a meta from the list of available meta types provided in the Meta Panel. For more information, see " Meta Panel" in Build Rule View.

   c. In the **From** drop-down menu, select one of the following:

      - Session
      - Logs

   d. In the **Alias** field, enter the alias name for columns used in the Select clause.

   e. In the **Where** field, enter a meta or select a meta from the list of available meta types provided in the Meta Panel. The Where clause provides the base query criteria for the rule.

   f. In the **Group By** field, enter the meta selected in the Select clause, so that the result set is grouped based on the meta.

   g. In the **Having** field, enter the criteria to filter the result set for aggregated queries.

   h. In the **Order By** field, perform the following:

      1. In the **Column Name** column, enter the name of the columns by which you want to group the results.
      2. In the **Sort by** column, select one of the following ways to sort the results:

         - Ascending Order
         - Descending Order

   i. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by session count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.

   j. Click **Save**.

4. If you are defining the rule in Expert mode, select the **Expert Mode** checkbox and perform the following:

   a. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and reports.

   b. In the **Query** field, enter the Hive query statement to query the data source.

   c. In the **Alias** field, enter the alias name for columns used in the Select clause.

   d. Click **Save**.

Create a Rule Using Respond Data Source

You can create a rule to fetch incidents or alerts from a Respond data source.

Prerequisites

Make sure that you:

- Ensure Reporting Engine service is up and running.
- Ensure the Incident Management service is up and running. For more information, see "Configure a Database for the Respond Server Service" topic in the *NetWitness Respond Configuration Guide*.
- (Optional) Ensure the Event Stream Analysis service is up and running. For more information, see "Step 2. Configure Advanced Settings for an ESA Service" topic in the *ESA Configuration Guide*.
- (Optional) Ensure the Malware Analysis service is up and running. For more information, see " (Optional) Configure Auditing on Malware Analysis Host" topic in the *Malware Configuration Guide*.

Note: You need to configure any one of the services (Event Stream Analysis, Reporting Engine, Malware Analysis, or Endpoint) based on your requirement and the type of alerts or incidents you want to generate.

To create a rule to fetch data or events from a Respond Data Source, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** toolbar, click  > **Respond DB**.

   The Build Rule view tab is displayed.

3. In the **Rule Type** field, Respond is selected by default.
4. In the **Name** field, enter a name that is used to Identify or label the rule in alerts and incident reports.
5. The **Summarize** field determines the type of summarization or aggregation for the rule. Based on the type of rule to be defined, you must select one of the following:
   - To define a **Non-Aggregate** rule without any grouping, select **None**
   - To define an **Aggregate** rule with meta values and custom aggregates select **Custom**

     Choosing 'Custom' in the **Summarize** field enables you to define aggregate function of your choice in the *Select* clause based on the report type you have selected.

     For more detailed information about Aggregate and Non-aggregate rule, see Rule Syntax.
6. In the **From** field, based on the type of report output to be displayed, you must select one of the following:
   - Alert
   - Incident

- incidentStats
- incidentUserStats

7. In the **Select**field, enter a meta or select a meta from the list of available meta types provided in the Meta Library. For more information, see "Meta Panel" in Build Rule View. It cannot be used in the **Where** field. Only one aggregate function is supported at a time in a query.

   For example, the supported metas for alert are:

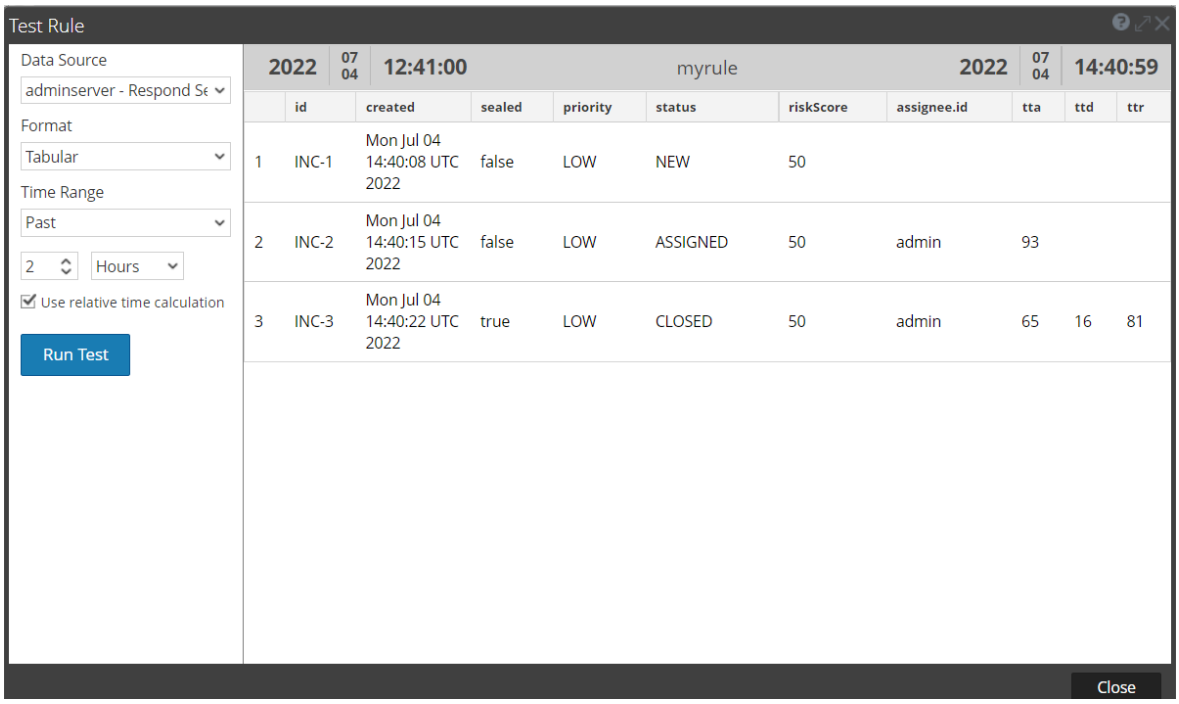
   - alert_host_summary
   - alert.name
   - alert.numEvents
   - alert.severity
   - alert.source
   - alert.timestamp
   - incidentCreated
   - incidentId
   - receivedTime

   For example, the supported metas for incident are:

   - categories
   - created
   - priority
   - riskScore
   - sealed
   - status
   - assignee.id
   - tta (for more information on this meta, see **View Basic Summary Information about the Incident** topic in the *Respond User Guide.*)
   - ttd (for more information on this meta, see **View Basic Summary Information about the Incident** topic in the *Respond User Guide.*)
   - ttr (for more information on this meta, see **View Basic Summary Information about the Incident** topic in the *Respond User Guide.*)

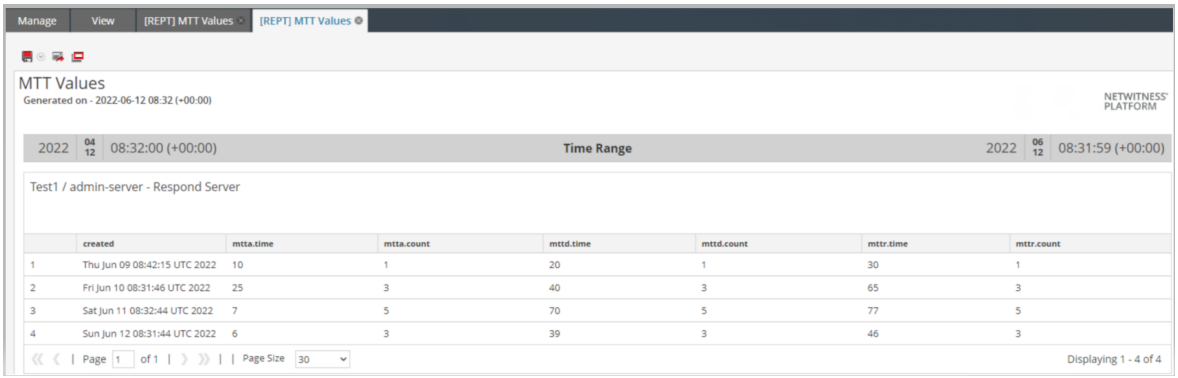
   Note: When an incident is assigned, tta and assignee.id metas are populated. Similarly, when the task assigned is completed and the incident is closed, ttd and ttr metas are populated. Refer to

the following figure.



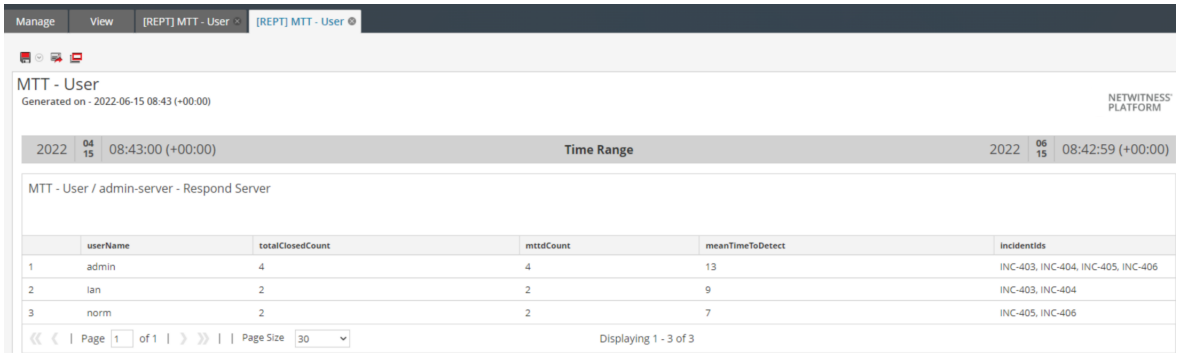
For example, the supported metas for incidentStats are:

- created
- mtta.time - This meta displays the average time taken to acknowledge the incidents in a single day.
- mtta.count - This meta displays the number of incidents acknowledged in a single day.
- mttd.time - This meta displays the average time taken to detect the incidents in a single day.
- mttd.count - This meta displays the number of incidents detected in a single day.
- mttr.time - This meta displays the average time taken to resolve the incidents in a single day.
- mttr.count - This meta displays the number of incidents resolved in a single day.



For example, the supported metas for incidentUserStats are:

- userName - This meta displays the assignee's or the user's ID for the associated user stats.
- totalClosedCount - This meta displays the total number of Incidents closed by the assignee till date.
- meanTimeToDetect - This meta displays the average time taken by the user to detect the incidents in the time range selected.
- mttdCount - This meta displays the count of incidents contributing to the MTTD value computed.
- incidentIds - This meta displays the list of incident IDs closed by the user during the time range selected.



For more detailed information, see "Aggregate and Non-aggregate rule" topic in the Rule Syntax.

8. In the **Alias** field, enter the alias name for columns used in the Select clause.
9. In the **Where** field, enter a meta or select a meta from the list of available meta types and use the operators to construct the Where clause for the base query criteria.
10. The **Group By** field is a read-only field which gets populated with meta that are defined in the Select clause. For a Non-Aggregate function, this field is not visible. A maximum of six meta are supported in the **Group By** field.
11. In the **Order By** field, perform the following:
    a. In the **Column Name** column, enter the name of the columns by which you want to sort the results.

    Note: by default the first meta in the select clause will be dispalyed.

    b. In the **Sort by** column, select one of the following ways to sort the results:
    - Ascending Order
    - Descending Order
12. In the **Limit** field, enter the limit to be put on the query while fetching data from the database. If a result set is sorted by the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.
13. Click **Save**.

Deploy a Rule

In NetWitness you can deploy the selected rules on the service (for example, Reporting Engine), using the Deployment Wizard.

Prerequisites

Make sure that:

- The services on which you deploy a rule is up and running.
- The Live Services is configured.

To deploy a rule, perform the following:

1. Go to  **(Configure) > LIVE CONTENT**.
2. In the **Search Criteria** panel, search Live resources (for example, search for the **Application Rule** resource Type).
3. In the **Matching Resources** panel, select **Show Results > Grid**.
4. Select the checkbox to the left or the rules that you want to deploy.
5. In the **Matching Resources** toolbar, click  .
6. Click **Next**.
7. Select the service on which you to deploy a rule (For example, Reporting Engine) and click **Next**.
8. Click **Deploy**.
   The rule is deployed successfully.

Use Meta Aliases for Reporting

When you refer to meta data in Reports and Charts, you can only view aliases for the meta names. These aliases makes them more understandable to a broader audience.

You cannot provide alias values for any meta in the WHERE clause because NetWitness uses the WHERE clause to fetch data from the data source (for example, in the Concentrator) and data sources do not support aliases. In other words, you cannot provide the alias value **HTTP** for the HTTP port # 80.

Note: * You cannot create aliases for meta other than the ones that have existing aliases by Reporting Engine. Also, the format of the aliases cannot be changed.
* Aliases are not supported for Alerts and CSV reports.

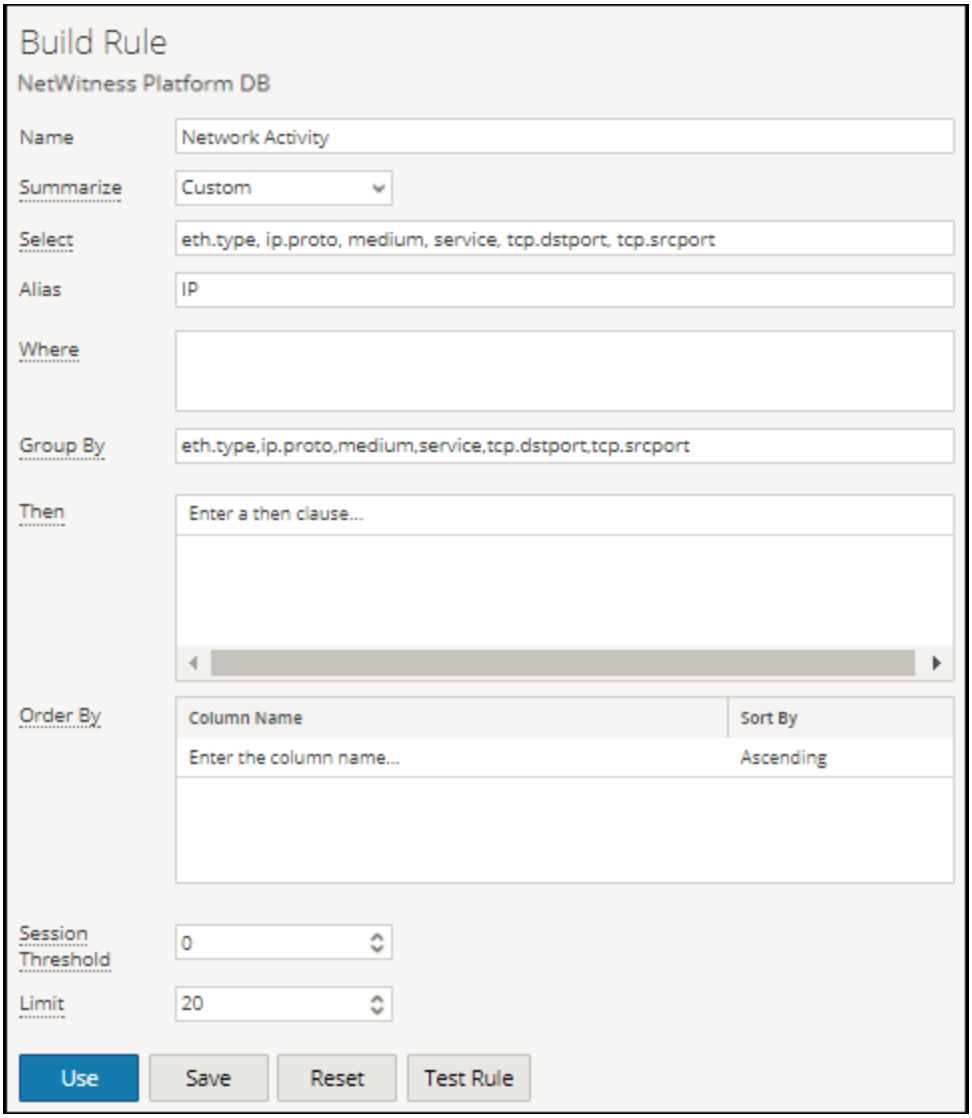
To use alias in a rule, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. In the **Rules** panel, do one of the following:

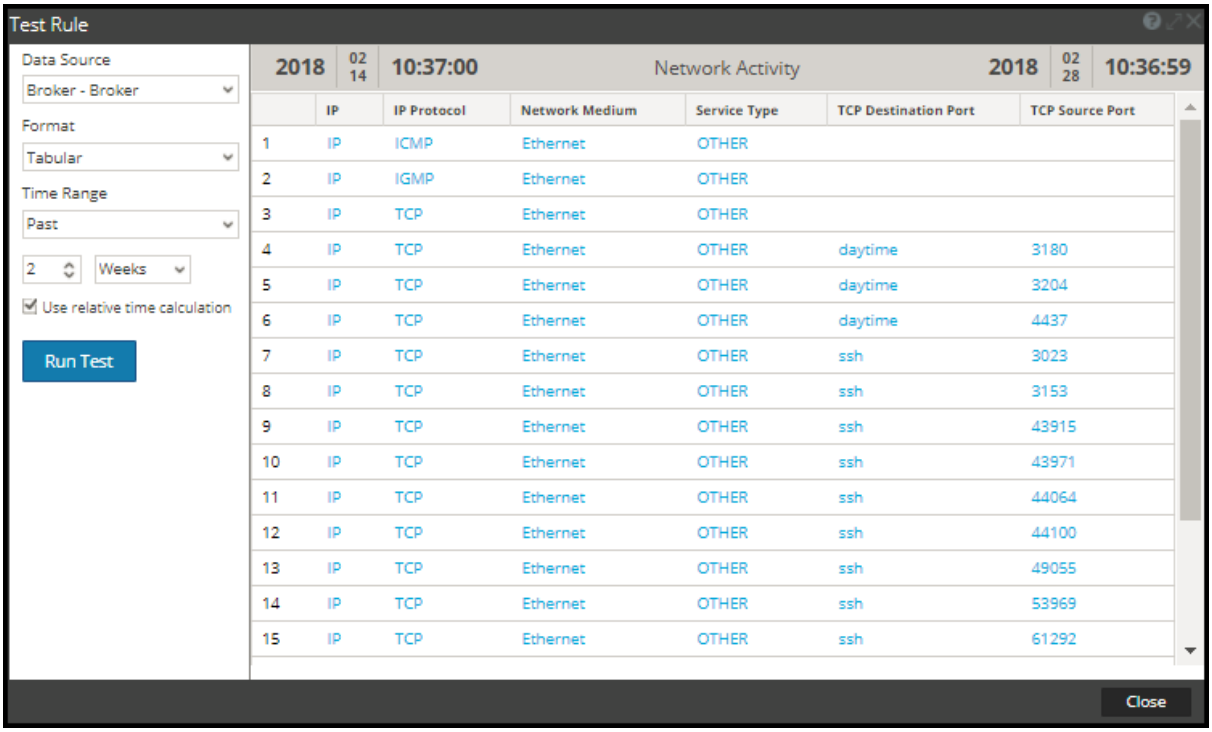
- Select a rule and click in the Rules toolbar.
- Click > **Edit**.

3. Specify the meta key with aliases in the **Select** field.

The following example specifies the **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport**, and **tcp.srcport** meta in the Select field.



4. Click **Test Rule**.
   The following example displays the results under the **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport**, and **tcp.srcport** alias columns that were specified in the **Select** field of the rule.



	IP	IP Protocol	Network Medium	Service Type	TCP Destination Port	TCP Source Port
1	IP	ICMP	Ethernet	OTHER		
2	IP	IGMP	Ethernet	OTHER		
3	IP	TCP	Ethernet	OTHER		
4	IP	TCP	Ethernet	OTHER	daytime	3180
5	IP	TCP	Ethernet	OTHER	daytime	3204
6	IP	TCP	Ethernet	OTHER	daytime	4437
7	IP	TCP	Ethernet	OTHER	ssh	3023
8	IP	TCP	Ethernet	OTHER	ssh	3153
9	IP	TCP	Ethernet	OTHER	ssh	43915
10	IP	TCP	Ethernet	OTHER	ssh	43971
11	IP	TCP	Ethernet	OTHER	ssh	44064
12	IP	TCP	Ethernet	OTHER	ssh	44100
13	IP	TCP	Ethernet	OTHER	ssh	49055
14	IP	TCP	Ethernet	OTHER	ssh	53969
15	IP	TCP	Ethernet	OTHER	ssh	61292

Alias Definitions

The alias files in this section are examples only and are based on current alias definitions in the Reporting Engine. NetWitness cannot modify these definitions in the Reporting Engine depending on the changes in the concentrator xml file. Since any changes in the Concentrator xml file are not reflected in the Reporting Engine.

The details of different meta are explained in each of the **meta.aliases**.

eth.type

```
ALIAS_FORMAT=$alias
 0=802.3
 257=Experimental
 512=Xerox PUP
 513=Xerox PUP
 1024=Nixdorf
 1536=Xerox NS IDP
 1537=XNS Address Translation (3Mb only)
 2048=IP
 2049=X.75 Internet
 2050=NBS Internet
 2051=ECMA Internet
 2052=CHAOSnet
 2053=X.25 Level 3
 2054=ARP
 2055=XNS Compatibility
 2076=Symbolics Private
 2184=Xyplex
 2304=Ungermann-Bass network debugger
 2560=Xerox IEEE802.3 PUP
```

```
2561=Xerox IEEE802.3 PUP Address Translation
2989=Banyan Systems
2991=Banyon VINES Echo
4096=Berkeley Trailer negotiation
4097=Berkeley Trailer encapsulation for IP
4660=DCA - Multicast
5632=VALID system protocol
6537=Artificial Horizons
6549=Datapoint Corporation (RCL lan protocol)
15360=3Com NBP virtual circuit datagram (like XNS SPP) not registered
15361=3Com NBP System control datagram not registered
15362=3Com NBP Connect request (virtual cct) not registered
15363=3Com NBP Connect repsonse not registered
15364=3Com NBP Connect complete not registered
15365=3Com NBP Close request (virtual cct) not registered
15366=3Com NBP Close response not registered
15367=3Com NBP Datagram (like XNS IDP) not registered
15368=3Com NBP Datagram broadcast not registered
15369=3Com NBP Claim NetBIOS name not registered
15370=3Com NBP Delete Netbios name not registered
15371=3Com NBP Remote adaptor status request not registered
15372=3Com NBP Remote adaptor response not registered
15373=3Com NBP Reset not registered
16972=Information Modes Little Big LAN diagnostic
17185=THD - Diddle
19522=Information Modes Little Big LAN
21000=BBN Simnet Private
24576=DEC unassigned
24577=DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
24578=DEC Maintenance Operation Protocol (MOP) Remote Console
24579=DECNET Phase IV
24580=DEC Local Area Transport (LAT)
24581=DEC diagnostic protocol (at interface initialization?)
24582=DEC customer protocol
24583=DEC Local Area VAX Cluster (LAVC)
24584=DEC AMBER
24585=DEC MUMPS
24592=3Com Corporation
28672=Ungermann-Bass download
28673=Ungermann-Bass NIUs
28674=Ungermann-Bass diagnostic/loopback
28675=Ungermann-Bass ??? (NMC to/from UB Bridge)
28677=Ungermann-Bass Bridge Spanning Tree
28679=OS/9 Microware
28681=OS/9 Net?
28704=LRT (England) (now Sintrom)
28720=Racal-Interlan
28721=Prime NTS (Network Terminal Service)
28724=Cabletron
32771=Cronus VLN
32772=Cronus Direct
32773=HP Probe protocol
32774=Nestar
32776=AT&amp;amp;T/Stanford Univ.
32784=Excelan
32787=Silicon Graphics diagnostic
32788=Silicon Graphics network games
32789=Silicon Graphics reserved
32790=Silicon Graphics XNS NameServer
32793=Apollo DOMAIN
32814=Tymshare
```

```
32815=Tigan
32821=Reverse Address Resolution Protocol (RARP)
32822=Aeonic Systems
32823=IPX (Novell Netware?)
32824=DEC LanBridge Management
32825=DEC DSM/DDP
32826=DEC Argonaut Console
32827=DEC VAXELN
32828=DEC DNS Naming Service
32829=DEC Ethernet CSMA/CD Encryption Protocol
32830=DEC Distributed Time Service
32831=DEC LAN Traffic Monitor Protocol
32832=DEC PATHWORKS DECnet NETBIOS Emulation
32833=DEC Local Area System Transport
32834=DEC unassigned
32836=Planning Research Corp.
32838=AT&amp;amp;T
32839=AT&amp;amp;T
32840=DEC Availability Manager for Distributed Systems DECamds
32841=ExperData
32859=VMTP
32860=Stanford V Kernel
32861=Evans &amp;amp; Sutherland
32864=Little Machines
32866=Counterpoint Computers
32869=University of Mass. at Amherst
32870=University of Mass. at Amherst
32871=Veeco Integrated Automation
32872=General Dynamics
32873=AT&amp;amp;T
32874=Autophon
32876=ComDesign
32877=Compugraphic Corporation
32878=Landmark Graphics Corporation
32890=Matra
32891=Dansk Data Elektronik
32892=Merit Internodal
32893=Vitalink Communications
32896=Vitalink TransLAN III Management
32897=Counterpoint Computers
32904=Xyplex
32923=EtherTalk - AppleTalk over Ethernet
32924=Datability
32927=Spider Systems Ltd.
32931=Nixdorf Computers
32932=Siemens Gammasonics Inc.
32960=DCA Data Exchange Cluster
32966=Pacer Software
32967=Applitek Corporation
32968=Intergraph Corporation
32973=Harris Corporation
32975=Taylor Instrument
32979=Rosemount Corporation
32981=IBM SNA Services over Ethernet
32989=Varian Associates
32990=TRFS (Integrated Solutions Transparent Remote File System)
32992=Allen-Bradley
32996=Datability
33010=Retix
33011=AppleTalk Address Resolution Protocol (AARP)
33012=Kinetics
```

```
 33015=Apollo Computer
 33023=Wellfleet Communications
 33026=Wellfleet BOFL
 33027=Wellfleet Communications
 33031=Symbolics Private
 33067=Talaris
 33072=Waterloo Microsystems Inc.
 33073=VG Laboratory Systems
 33079=IPX
 33080=Novell Inc
 33081=KTI
 33087=M/MUMPS data sharing
 33093=Vrije Universiteit (NL)
 33094=Vrije Universiteit (NL)
 33095=Vrije Universiteit (NL)
 33100=SNMP
 33103=Technically Elite Concepts
 33169=PowerLAN
 33149=XTP
 33238=Artisoft Lantastic
 33239=Artisoft Lantastic
 33283=QNX Software Systems Ltd.
 33680=Accton Technologies (unregistered)
 34091=Talaris multicast
 34178=Kalpana
 34525=IPv6
 34617=Control Technology Inc.
 34618=Control Technology Inc.
 34619=Control Technology Inc.
 34620=Control Technology Inc.
 34848=Hitachi Cable (Optoelectronic Systems Laboratory)
 34902=Axis Communications AB
 34952=HP LanProbe test?
 36864=Loopback (Configuration Test Protocol)
 36865=3Com XNS Systems Management
 36866=3Com TCP/IP Systems Management
 36867=3Com loopback detection
 43690=DECNET
 64245=Sonix Arpeggio
 65280=BBN VITAL-LanBridge cache wakeups
 34915=PPPoe
 34916=PPPoe
 2056=Frame Relay ARP
 16962=IEEE bridge spanning protocol
 25944=Bridged Ethernet/802.3 packet
 65278=ISO CLNP/ISO ES-IS DSAP/SSAP
```

ip.proto

```
ALIAS_FORMAT=$alias
 0=HOPOPT
 1=ICMP
 2=IGMP
 3=GGP
 4=IP
 5=ST
 6=TCP
 7=CBT
 8=EGP
 9=IGP
 10=BBN-RCC-M
 11=NVP-II
 12=PUP
```

```
13=ARGUS
14=EMCON
15=XNET
16=CHAOS
17=UDP
18=MUX
19=DCN-MEAS
20=HMP
21=PRM
22=XNS-IDP
23=TRUNK-1
24=TRUNK-2
25=LEAF-1
26=LEAF-2
27=RDP
28=IRTP
29=ISO-TP4
30=NETBLT
31=MFE-NSP
32=MERIT-INP
33=SEP
34=3PC
35=IDPR
36=XTP
37=DDP
38=IDPR-CMTP
39=TP++
40=IL
41=IPv6
42=SDRP
43=IPv6-Rout
44=IPv6-Frag
45=IDRP
46=RSVP
47=GRE
48=MHRP
49=BNA
50=ESP
51=AH
52=I-NLSP
53=SWIPE
54=NARP
55=MOBILE
56=TLSP
57=SKIP
58=IPv6-ICMP
59=IPv6-NoNx
60=IPv6-Opts
61=AnyHost
62=CFTP
63=AnyNetwork
64=SAT-EXPAK
65=KRYPTOLAN
66=RVD
67=IPPC
68=AnyFile
69=SAT-MON
70=VISA
71=IPCV
72=CPNX
73=CPHB
```

```
74=WSN
75=PVP
76=BR-SAT-MO
77=SUN-ND
78=WB-MON
79=WB-EXPAK
80=ISO-IP
81=VMTP
82=SECURE-VM
83=VINES
84=TTP
85=NSFNET-IG
86=DGP
87=TCF
88=EIGRP
89=OSPFIGP
90=Sprite-RP
91=LARP
92=MTP
93=AX.25
94=IPIP
95=MICP
96=SCC-SP
97=ETHERIP
98=ENCAP
99=AnyPrivate
100=GMTP
101=IFMP
102=PNNI
103=PIM
104=ARIS
105=SCPS
106=QNX
107=A/N
108=IPComp
109=SNP
110=Compaq-Pe
111=IPX-in-IP
112=VRRP
113=PGM
114=AnyHop
115=L2TP
116=DDX
117=IATP
118=STP
119=SRP
120=UTI
121=SMP
122=SM
123=PTP
124=ISIS
125=FIRE
126=CRTP
127=CRUDP
128=SSCOPMCE
129=IPLT
130=SPS
131=PIPE Pr
132=SCTP St
133=FC Fi
134=RSVP-E2E-
```

```
 255=Reserved
```

medium

```
ALIAS_FORMAT=$alias
 1=Ethernet
 2=Tokenring
 3=FDDI
 4=HDLC
 5=NetWitness
 6=802.11
 7=802.11 Radio
 8=802.11 AVS
 9=802.11 PPI
 10=802.11 PRISM
 11=802.11 Management
 12=802.11 Control
 13=DLT Raw
 32=Logs
```

service

```
ALIAS_FORMAT=$alias
 0=OTHER
 20=FTPD
 21=FTP
 22=SSH
 23=TELNET
 25=SMTP
 53=DNS
 67=DHCP
 69=TFTP
 80=HTTP
 110=POP3
 111=SUNRPC
 119=NNTP
 123=NTP
 135=RPC
 137=NETBIOS
 139=SMB
 143=IMAP
 161=SNMP
 179=BGP
 443=SSL
 502=MODBUS
 520=RIP
 1024=EXCHANGE
 1080=SOCKS
 1122=MSN IM
 1344=ICAP
 1352=NOTES
 1433=TDS
 1521=TNS
 1533=SAMETIME
 1719=H.323
 1720=RTP
 2000=SKINNY
 2040=SOULSEEK
 2049=NFS
 3270=TN3270
 3389=RDP
 3700=DB2
 5050=YAHOO IM
 5060=SIP
```

```
5190=AOL IM
5222=Google Talk
5900=VNC
6346=GNUTELLA
6667=IRC
6801=Net2Phone
6881=BITTORRENT
8000=QQ
8002=YCHAT
8019=WEBMAIL
8082=FIX
20000=DNP3
1000000=KERNEL
1000001=USER
1000003=SYSTEM
1000004=AUTH
1000005=LOGGER
1000006=LPD
1000008=UUCP
1000009=SCHEDULE
1000010=SECURITY
1000013=AUDIT
1000014=ALERT
1000015=CLOCK
```

tcp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
 464=kpasswd
 512=exec
 513=login
 514=cmd
 515=printer
 520=efs
 526=tempo
 530=courier
 531=conference
 532=netnews
 540=uucp
 543=klogin
 544=kshell
 556=remotefs
 636=ldaps
 749=kerberos-adm
 993=imaps
 995=pop3s
 1109=kpop
 1433=ms-sql-s
 1434=ms-sql-m
```

```
 1512=wins
 1524=ingreslock
 1723=pptp
 2053=knetd
 1122=msn im
 1352=notes
 1521=tns
 1533=sametime
 1718=h323
 1720=rtp
 1863=msn im
 2049=nfs
 3389=rdp
 5050=yahoo im
 5060=sip
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

tcp.srcport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
 110=pop3
 111=sunrpc
 113=auth
 117=uucp-path
 119=nntp
 135=epmap
 137=netbios-ns
 139=netbios-ssn
 143=imap
 158=pcmail-srv
 170=print-srv
 179=bgp
 194=irc
 389=ldap
 443=https
 445=cifs
```

```
 464=kpasswd
 512=exec
 513=login
 514=cmd
 515=printer
 520=efs
 526=tempo
 530=courier
 531=conference
 532=netnews
 540=uucp
 543=klogin
 544=kshell
 556=remotefs
 636=ldaps
 749=kerberos-adm
 993=imaps
 995=pop3s
 1109=kpop
 1433=ms-sql-s
 1434=ms-sql-m
 1512=wins
 1524=ingreslock
 1723=pptp
 2053=knetd
 1122=msn im
 1352=notes
 1521=tns
 1533=sametime
 1718=h323
 1720=rtp
 1863=msn im
 2049=nfs
 3389=rdp
 5050=yahoo im
 5060=sip
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

udp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 37=time
 39=rlp
 42=nameserver
 53=domain
 67=bootps
 68=bootpc
 69=tftp
 88=kerberos
 111=sunrpc
 123=ntp
 135=epmap
 137=netbios-ns
```

```
138=netbios-dgm
161=snmp
162=snmptrap
213=ipx
443=https
445=cifs
464=kpasswd
500=isakmp
512=biff
513=who
514=syslog
517=talk
518=ntalk
525=timed
533=netwall
550=new-rwho
560=rmonitor
561=monitor
749=kerberos-adm
1167=phone
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1701=l2tp
1812=radiusauth
1813=radacct
2049=nfsd
2504=nlbs
```

Test a Rule

You can test a rule based on the time range and the data source selected.

To test a rule, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. In the **Rules** panel, do one of the following:
   - Select a rule and click  in the Rules toolbar.
   - Click  > **Edit**.
     The Build Rule view tab is displayed.

3. Click **Test Rule**.
   The Test Rule view is displayed.

> **Note:** When you click **Test Rule**, the rule is not saved. You have to click **Save**in the Build Rule view to save the rule.

4. From the **Data Source** drop-down list, select a data source.
   You must select the appropriate data source for the rule defined.
5. From the **Format** drop-down list, select the format in which you want the result displayed.
6. From the **Time Range** drop-down list, select one of the following.
   - **Past** -To specify number of years, days, weeks, months, days or hours.
   - **Range** - To specify a date range and time period.

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

7. **X-Axis** and **Y-Axis** are used to specify the meta to be plotted in charts.
   In **X-Axis**, the Meta for the 'Group by' rule is displayed. In **Y-Axis**, the aggregate functions used in the rule are displayed.

> **Note:** Sum, Count, Countdistinct and Average are the supported aggregate functions for rule. By default, for Custom Rules with multiple 'Group by', you can select only the first meta in **X-Axis**.

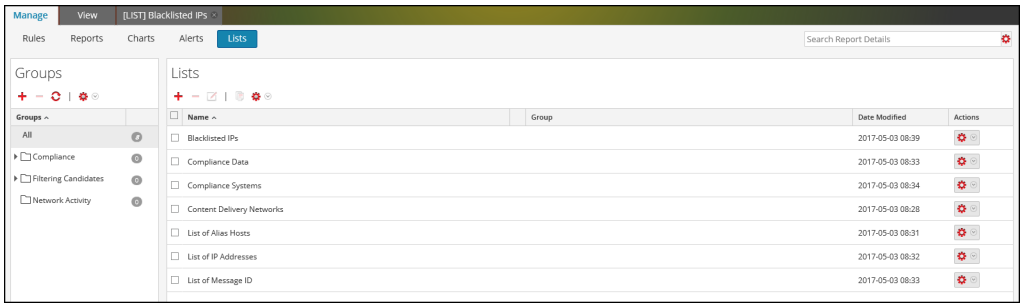
8. Click **Run Test** to execute the rule.
   The rule data (if any) for the selected time range is displayed.

Create a Lists or List Group

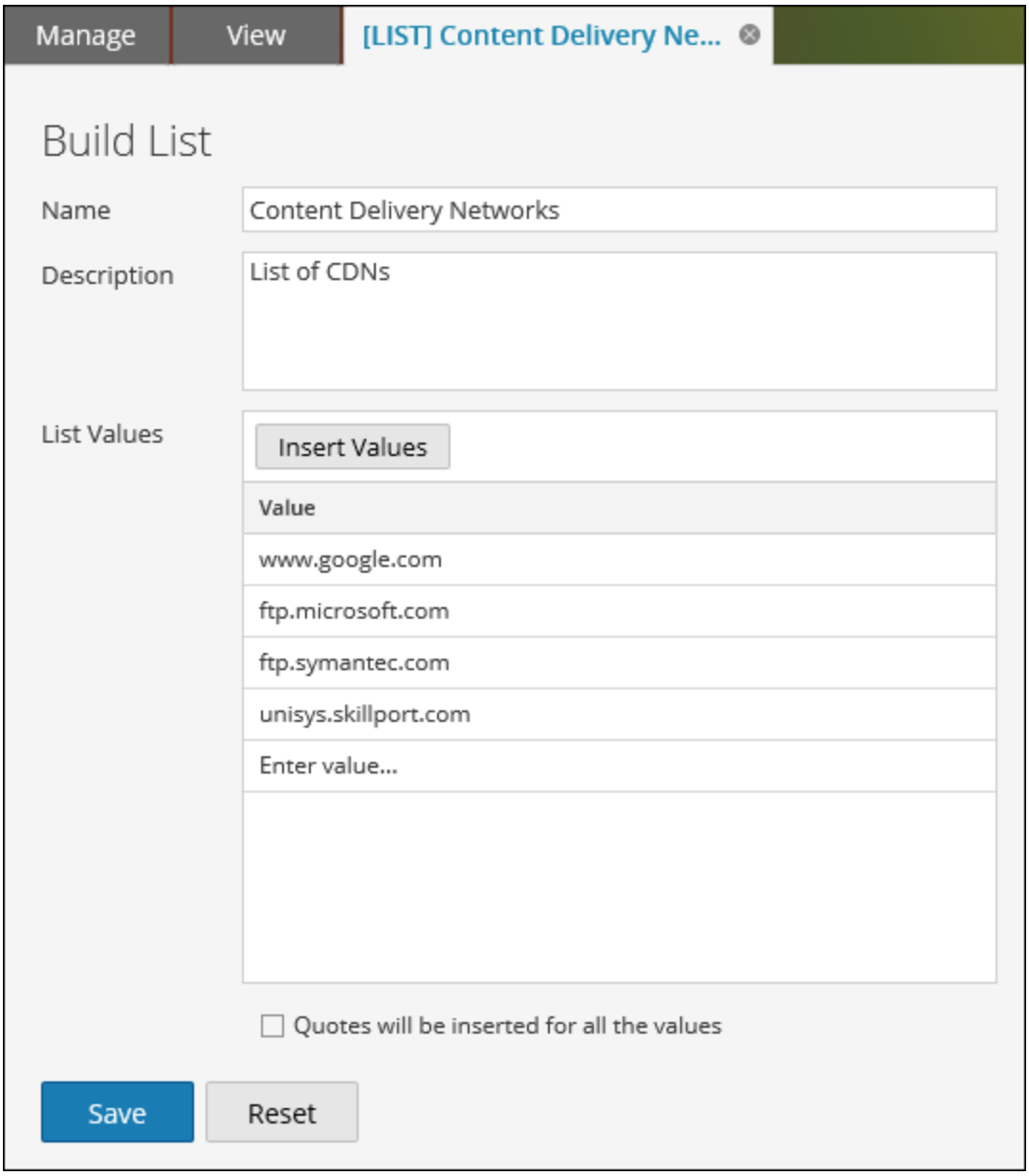
To create a list, perform the following:

Lists can be added within a group or in the root folder.

1. Go to **Reports**, and click **Lists**.
   The List view is displayed.



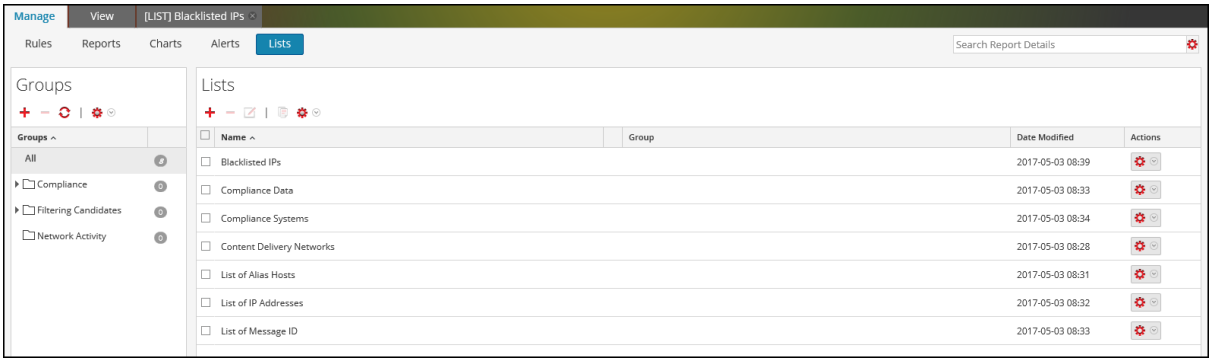
2. In the **Lists** toolbar, click  .
   The Build List view tab is displayed.



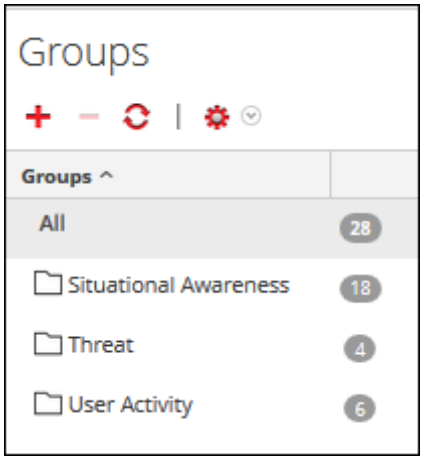
3. In the **Name** field, enter a unique name for the list.
4. In the **Description** field, enter a description for the list.
5. In the **List Values** field, do one of the following:
   - Click **Insert Values** and enter the values separated by commas. You can paste a list of values from a file or other lists.
   - In the **Value** column, enter the values.
6. If you want quotes to be inserted directly for the values at runtime, select **Quotes will be inserted for all the values**.
7. Click **Save**.

To create a list group, perform the following:

1. Go to **Reports**, and click **Lists**.
   The List view is displayed.



2. Do the following:
   - To create a list group:
     a. In the **Lists Groups** panel, click  .
        A new list group is added to the List Groups panel.



     b. Enter the name for the list group and press **ENTER**.
   - To create a list subgroup:
     1. In the **Lists** Groups panel, select the list group to which you want to add a subgroup.
     2. Click  .
        A new list subgroup is added to the list group.
     3. Enter the name for the list subgroup and press **ENTER**.

Create and Schedule a Report

You can create a simple or complex report and configure its execution properties by scheduling a report. A report can include multiple rules and you can schedule different time range to execute the same report. For example, depending on your requirement, you can schedule a report to run daily, weekly or monthly.

When you run a report, the results are stored in Reporting Engine.

After you generate a report, you can perform the following:

- Send the reports by email to other users by configuring the output actions. You can also configure the output actions before generating a report.
- Download the reports as PDF or Comma-Separated Values (CSV) format files.

Note: The cancel operation is not supported for Respond Reports.

Create a Report or Report Group

To create a report to a group or sub-group, perform the following:

1. Go to **Reports**.

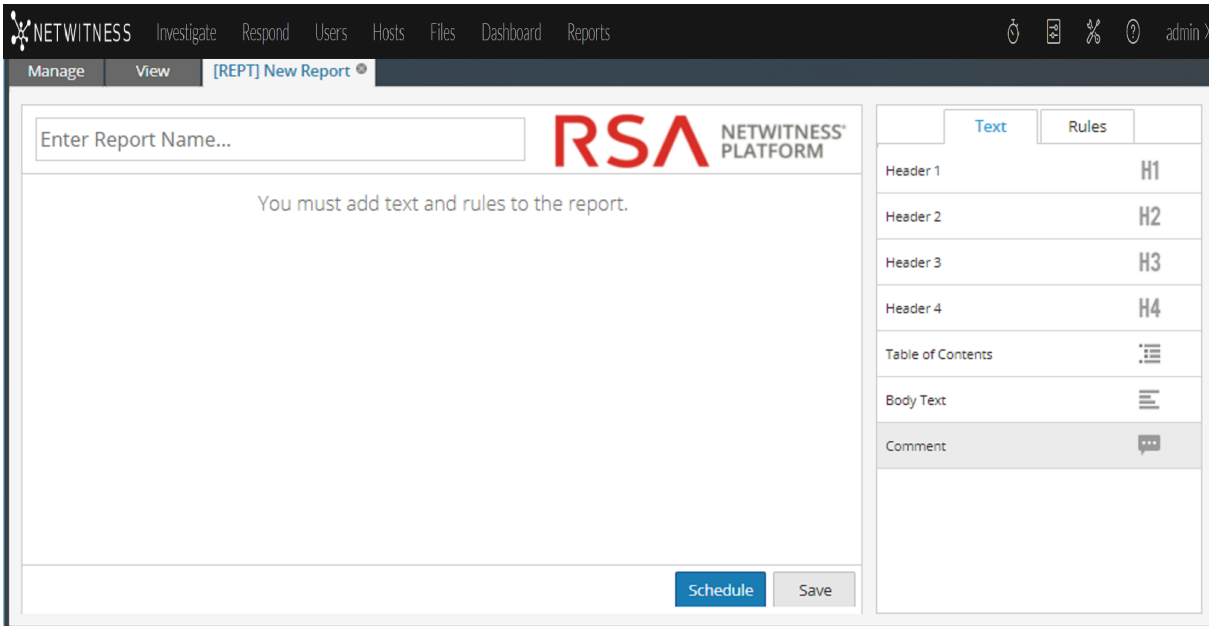
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** toolbar, click + .

   The Build Report tab is displayed.



4. Enter the name of the report.

5. Drag and drop the text and rules to the report.

   Note: The text entered is optional and you may need this option only when you want to display user-defined headers or content.

6. Click **Save**.

   A confirmation message that the report is saved successfully is displayed.

To create a group to the default folder or add sub-groups under a report group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports Groups** panel, click  .

   A default group is added in the Report Groups panel.

4. Enter the name of the new group.
5. Press **Enter**.

   The group is added to the Report Groups panel.

Schedule a Report

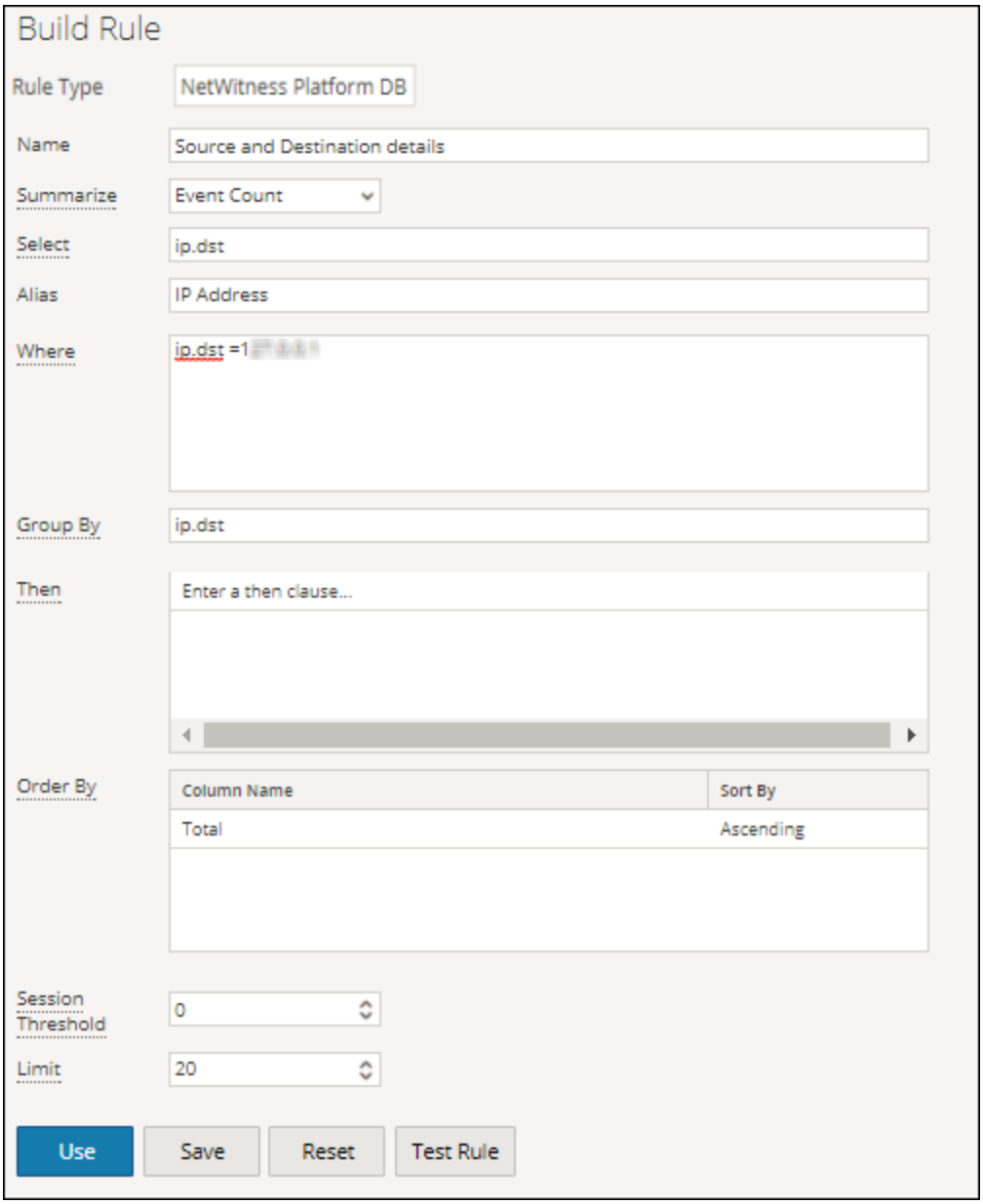
Note: When you schedule a Warehouse report, you can use a supported task scheduler to allocate specific resources in a cluster for the scheduled job. For more information on "supported task schedulers", see Task Scheduler for Warehouse Reporting.

To schedule a report, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** panel, click  to create a rule.
3. Click **Save**.
4. Click **Use**.



5. Go to **Reports**.

   The Manage tab is displayed.

6. Click **Reports**.

   The Report view is displayed.

7. On the **Reports** panel, click + to create a report.
8. Enter the Report Name in the field.
9. Add the rule by drag and drop which has the user defined variable from the Rules tab.
10. Click **Schedule**.

The Schedule Report view is displayed.

If you provide another user with access permissions to a report, you must also provide permissions for the report group, the rules used in the report, and the rule groups otherwise an error message is displayed.

11. To execute the reports as per the schedule, select the **Enable** checkbox.
12. In the **Schedule Name** field, enter a name for the schedule report configuration.
13. From the Data Source field, select the data source.

    Note: If the data source is not listed, then ensure you have **Read**permissions set for the data source. This is applicable for NWDB, Respond and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in *Reporting Engine Configuration Guide*.

14. (Optional) From the **Warehouse Resource Pool** drop-down, select the pools or queues available in the cluster to schedule the report to run on either the pool or queue. This drop-down list is available only if you select a Warehouse DB report.

    Note: All the queues or pools you specified in the Explore page for the Reporting Engine are listed. If no pools or queues are configured in the Explorer page, this drop-down is disabled and the jobs are submitted to the clusters without any a queue or pool name.

    Note: If the pool or queue configured in the report schedule is removed from the Cluster, then in the Capacity Scheduler, the queue name remains undefined. However, in the Fair Scheduler, the specified pool name will be created using the property mapred.fairscheduler.allow.undeclared.pool.

15. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format. This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
16. From the **Run** field, select the type of run schedule. (For example, Now or Hourly).

    Depending on the type of run schedule, choose one of the following:

    - If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
    - If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
    - If you select a **Daily** run schedule, you must enter a value in the **At** field.
    - If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

    Note: While scheduling a report, if you select **Past** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.

    For information on how to generate a report with variables, see Create a Parameterized Report Using Variable.

17. (Optional) In the **Output Actions** panel, do the following:

a. Enter the email address and subject.

b. Edit the body of the message for the report.

c. Select the format of the attachment.

d. Enter a value for the CSV and Multi-value delimiters.

e. (Optional) In the Other Options field, do the following:

i. Click + and select SFTP, URL, or Network Share output action.

A row gets added with the selected output action.

ii. Select the appropriate options to send the report in PDF or CSV format, or both to the RE configured SFTP, or URL, or Network Share output action.

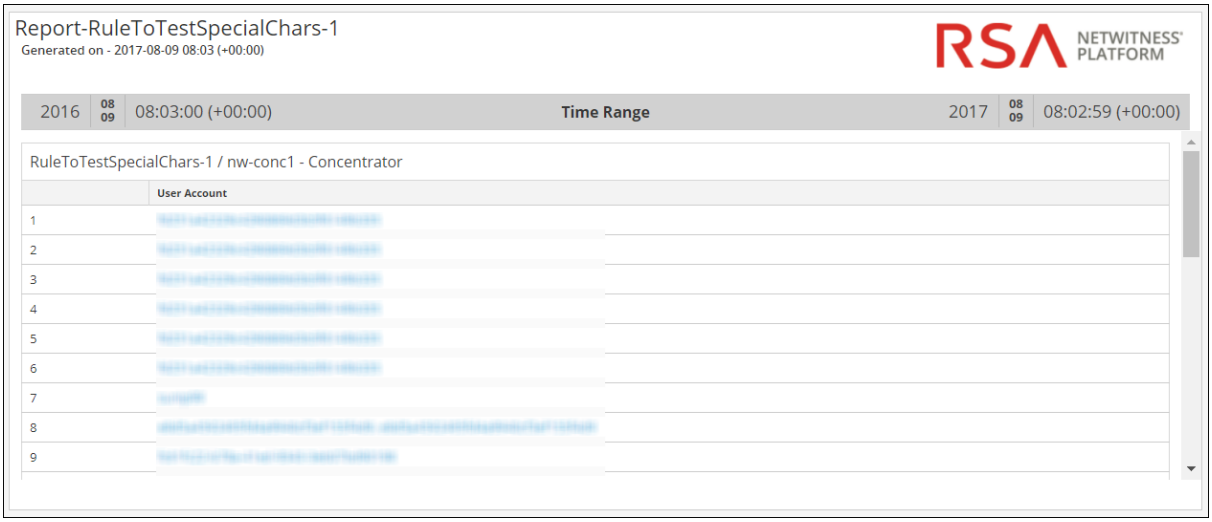
18. (Optional) To add a list in the Dynamic List panel, see Generate a List from the Scheduled Report.

19. (Optional) To choose a logo in the Logo panel, see "Manage and Select a Report Logo" section in Manage Lists, Rules or Reports.

Note: If you do not specify a logo, the default RSA logo will be used.

20. Click **Schedule**.

The scheduled report executes as scheduled and provides the configured outputs.



After you create and Schedule a report, you can perform any of the following tasks:

- You can notify the email recipient when the report execution completes and send reports in PDF and CSV formats as attachments in the email.
- You can generate a list based on the scheduled report and view them in the **Lists** module.
- You can send a scheduled report in PDF or CSV format, or both to the RE configured SFTP location, or URL, or Network Share.
- You can change the default logo and view them in the scheduled report.

- You can modify the NetWitness Reporting Engine config details, by navigating to the Reporting Engine General Tab. See the "Reporting Engine General Tab" topic in the *Reporting Engine Guide*.

Examples

When you schedule reports in the Schedule Report view, by default, the results for the **Past** option are presented based on the user specified time zone. The following examples provide a clear picture on what results to expect when you select **Hours**, **Days**, **Weeks**, **Months**, or **Years** for the **Past** option based on the absolute or relative duration.

Note: By default, the relative duration checkbox is de-selected. This implies that the results for the **Past** option are presented based on the absolute duration.

- **Based on Absolute duration** - Absolute Duration allows a report to be scheduled at an absolute time with respect to the current time, excluding the seconds and considering the time interval as a whole. For example, 12.00pm is the absolute time with respect to the current time (12.45 pm).
  - Hours - Suppose that you select Hours and specify one hour. If the current user specified time is 4.20PM, the report is generated for the time range, 3.00PM to 4.00PM.
  - Days - Suppose that you select Days and specify one day. If the current date is August 27, 2014 and the current user specified time is 10.15AM, the report is generated for the range: August 26, 2014, 12.00AM to August 27, 2014, 12.00AM.
  - Weeks - Suppose that you select Weeks and specify one week. If the current date is August 27, 2014 2.30PM and the day is Wednesday, the report is generated for the range: Saturday, August 16, 2014, 12.00AM to Saturday, August 23, 2014, 12.00AM.
  - Months - Suppose that you select Months and specify one month. If the current date is August 27, 2014 2.30PM, the report is generated for the range:
    July 01, 2014, 12.00AM to July 31, 2014, 12.00AM.
  - Years - Suppose that you select Years and specify one year.If the current date is August 27, 2014 2.30PM, the report is generated for the range:
    January 01, 2013, 12.00AM to December 31, 2013, 12.00AM.
- **Based on Relative duration** - Relative Duration allows a report to be scheduled at a time relative to the current time which might vary based on the current time. For example, 12.45 pm is the relative time with respect to the current time (12.45 pm).
  - Hours - Suppose that you select Hours and specify one hour. If the current user specified time is 4.20PM, the report is generated for the time range, 3.20PM to 4.20PM.
  - Days - Suppose that you select Days and specify one day. If the current date is August 27, 2014 and the current user specified time is 10.15AM, the report is generated for the range: August 26, 2014, 10.15AM to August 27, 2014, 10.15AM.
  - Weeks - Suppose that you select Weeks and specify one week. If the current date is August 27, 2014 12.30PM and the day is Wednesday, the report is generated for the range: Thursday, August 21, 2014 12.30PM to Wednesday, August 27, 2014 12.30PM.
  - Months - Suppose that you select Months and specify one month. If the current date is August 27, 2014, 2.30PM the report is generated for the range:
    July 27, 2014 2.30PM to August 27, 2014 2.30PM.

- Years - Suppose that you select Years and specify one year.If the current date is August 27, 2014 2.30PM, the report is generated for the range: August 27, 2013 2.30PM to August 27, 2014 2.30PM.

Generate a List from the Scheduled Report

You can generate a list from the output of the scheduled report. Make sure that your lists are created in NetWitness prior to generating a list to schedule a report.

To generate a list from the Build Report view, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Reports**.

   The Report view is displayed.
3. In the **Reports** panel, select a report and in Actions column, click  > **Schedule Report**.

   The Schedule Report view tab is displayed.
4. In the Output Actions section, in **Dynamic List** panel, click  .

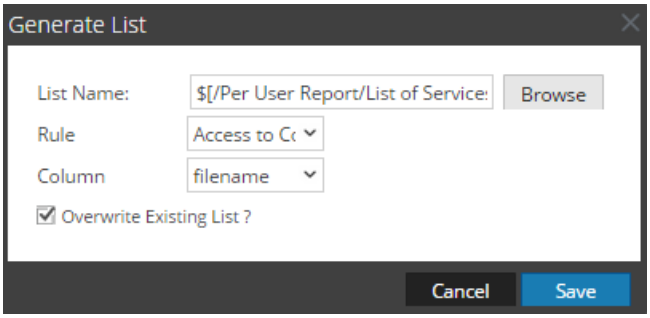
   The Generate List dialog box opens.
5. Click **Browse**.

   The List Selection panel is displayed.
6. Choose a list item and click **Select**.

   The list name gets populated in the List Name field.
7. Select a valid rule to filter the report results further based on the rule definition.
8. Select a value for the **Column** field.

   The column forms the values for the list that gets created.
9. If you want to overwrite the existing list, select the **Overwrite Existing List?** checkbox.
10. Click **Save**.

    The list name gets populated in the Generate List panel.



11. (Optional) Select a list from the Generate List panel and click to delete the selected list.
12. (Optional) Select a list from the Generate List panel and click to edit the list details.

Create a Parameterized Report Using Variable

You use variables for reporting in the NetWitness Reporting module. Parameterized reporting allows you to specify values dynamically at runtime without changing the rule definition so you can view the results based on a particular value. You can achieve parameterize reporting by using variables in the query or rule. For information on adding a rule, see Configure a Rule. At runtime, you can enter the value for the variable or select the value from the list based on which the result set is displayed.

The syntax to specify the variable is as follows:

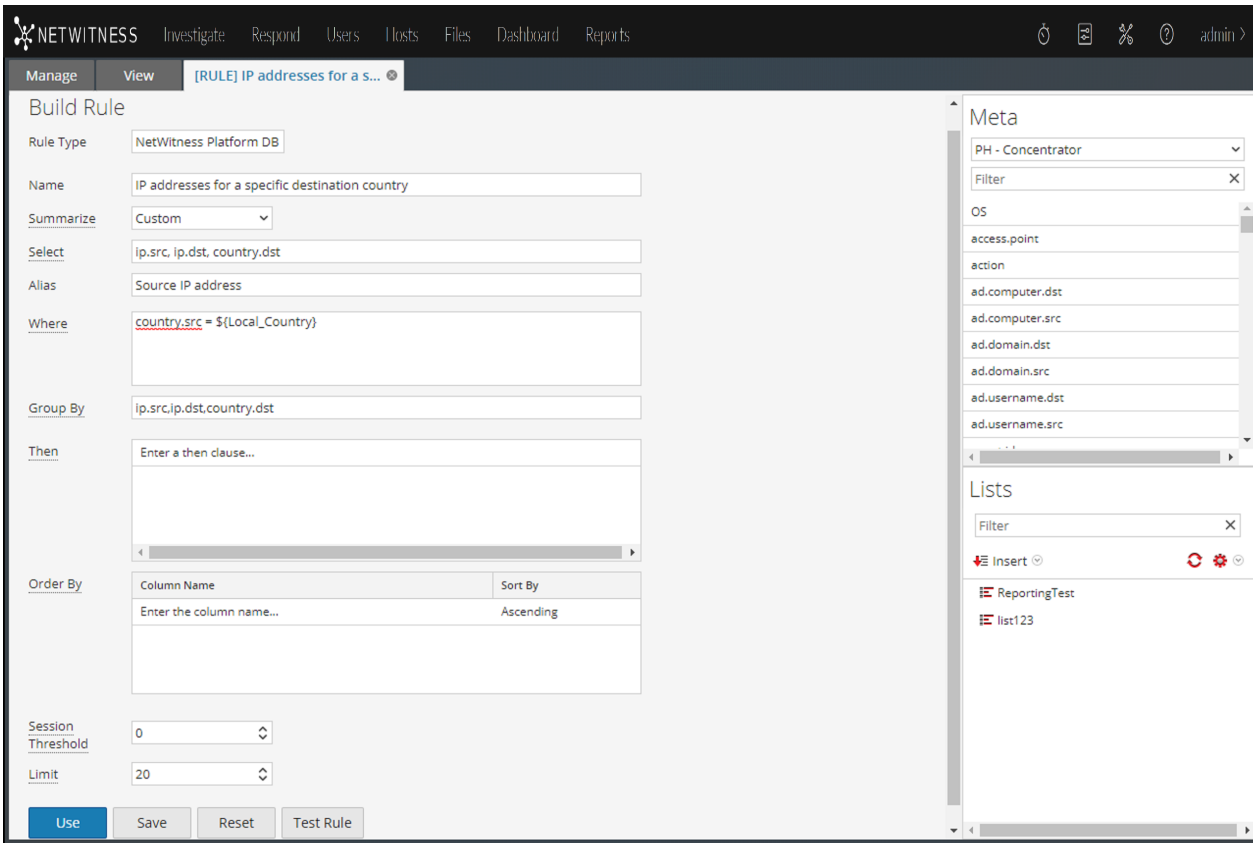
Description	Examples of Supported Syntax
Insert `$` before a variable. Enclose a variable within braces.	`columnname=${<variable>}`

The syntax to define the variable is the same for NetWitness DB and Warehouse DB data sources. When you assign the value of the variable in a Run Configuration, you must enclose the value within single quotes: `'<value>'`.

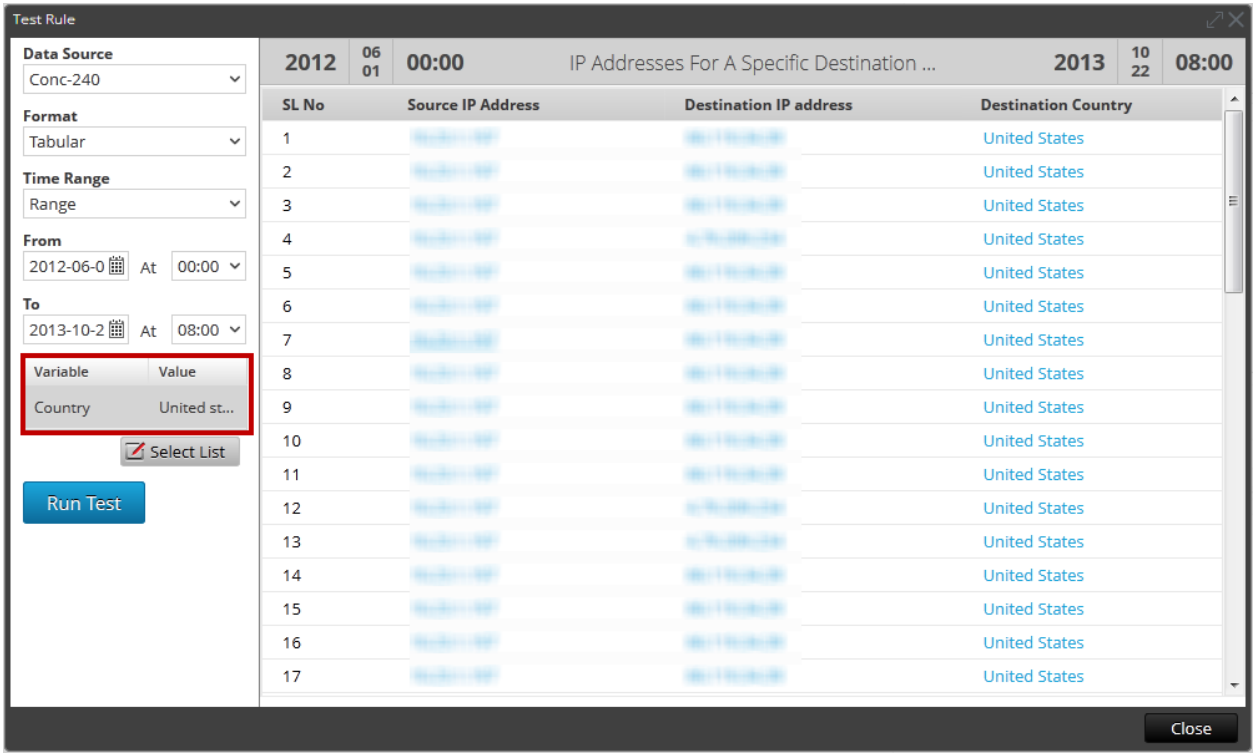
Some examples where a variable can be used are provided in this section.

View Source IP Addresses for a Specific Destination Country

The following is an example of a NetWitness DB rule to view the source and destination ip addresses for a specific destination country. Here the value for source country is defined as a variable `${local_country}`.



At runtime, you are prompted to enter the value for the variable. The figure below shows the `local_Country` variable where you can enter the value. If you enter the value as **United states**, all the source and destination ip addresses with destination country as United states are listed.



You can use the above rule to schedule a report. You can schedule two types of reports:

- Report with Dynamic Variables
- Iterative Report

Report with Dynamic Variables

Dynamic variables allows the user to specify the values for a variable defined in a rule while scheduling a report.

To schedule a report with Dynamic Variable, perform the following:

1. Go to **Reports**.

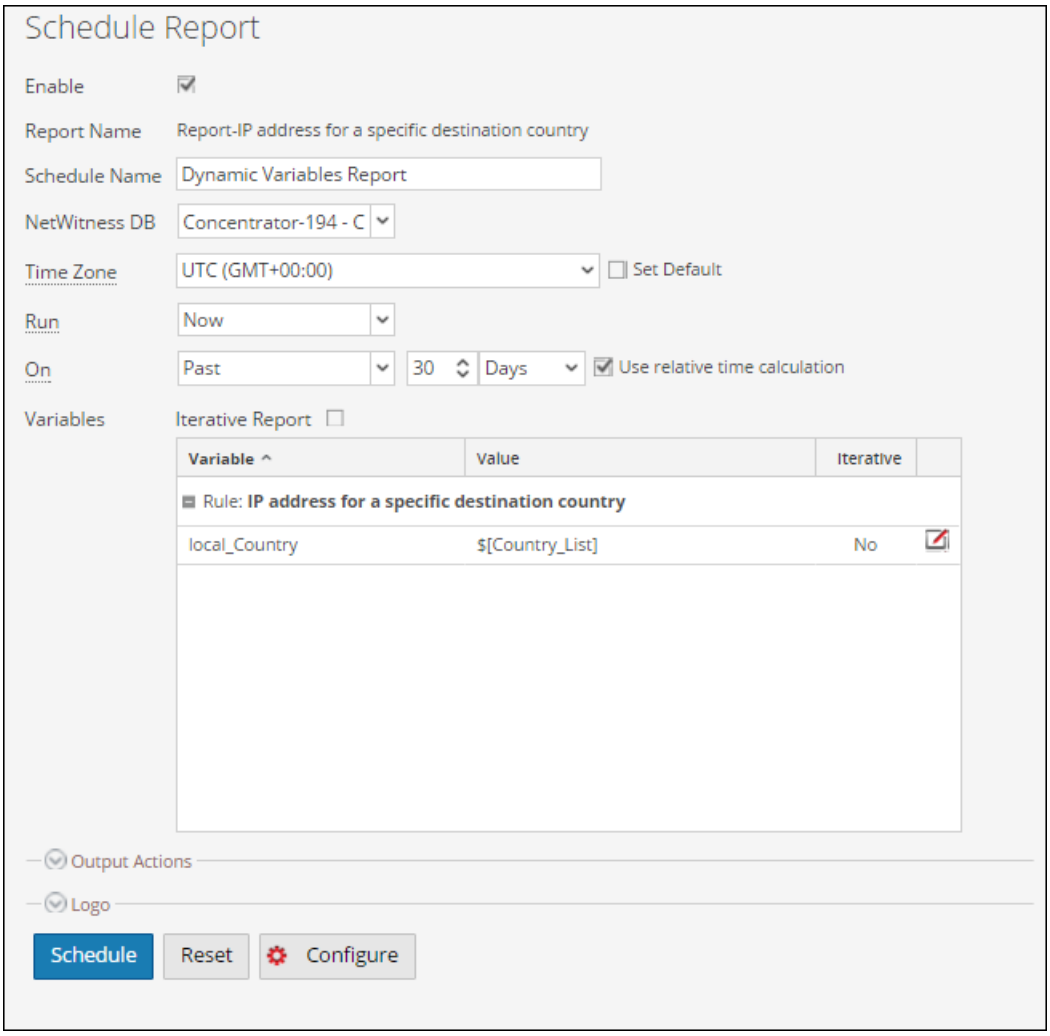
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. On the **Reports** panel, click + to create a report.
4. Enter the Report Name in the field.
5. Add the rule by drag and drop which has the user defined variable from the Rules tab.
6. Click **Schedule**.

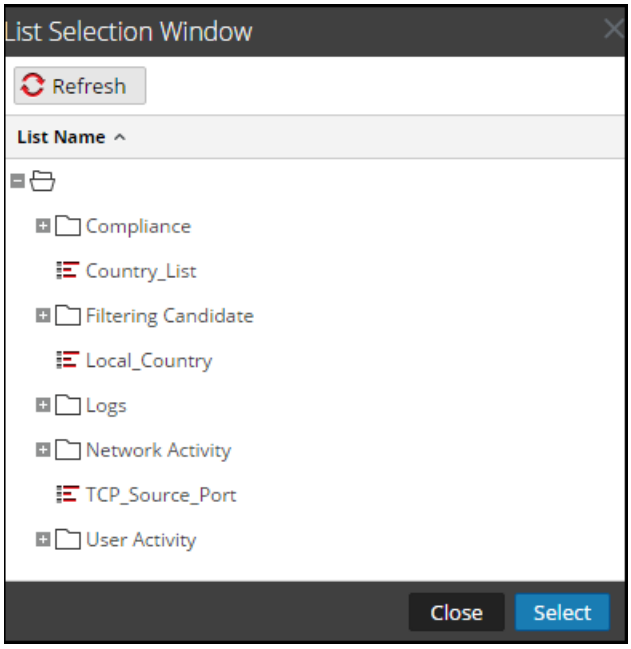
   The Schedule Report view tab is displayed.



7. To execute the reports as per the schedule, select the **Enable** checkbox.
8. In the **Schedule Name** field, enter a name for the schedule report configuration.
9. In the **NetWitness DB** drop-down, select the database.
10. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format.This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. From the **Run** field, select the type of run schedule. (For example, Now or Hourly). Depending on the type of run schedule, do either of the following:
    - If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
    - If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
    - If you select a **Daily** run schedule, you must enter a time value in the **At** field.
    - If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

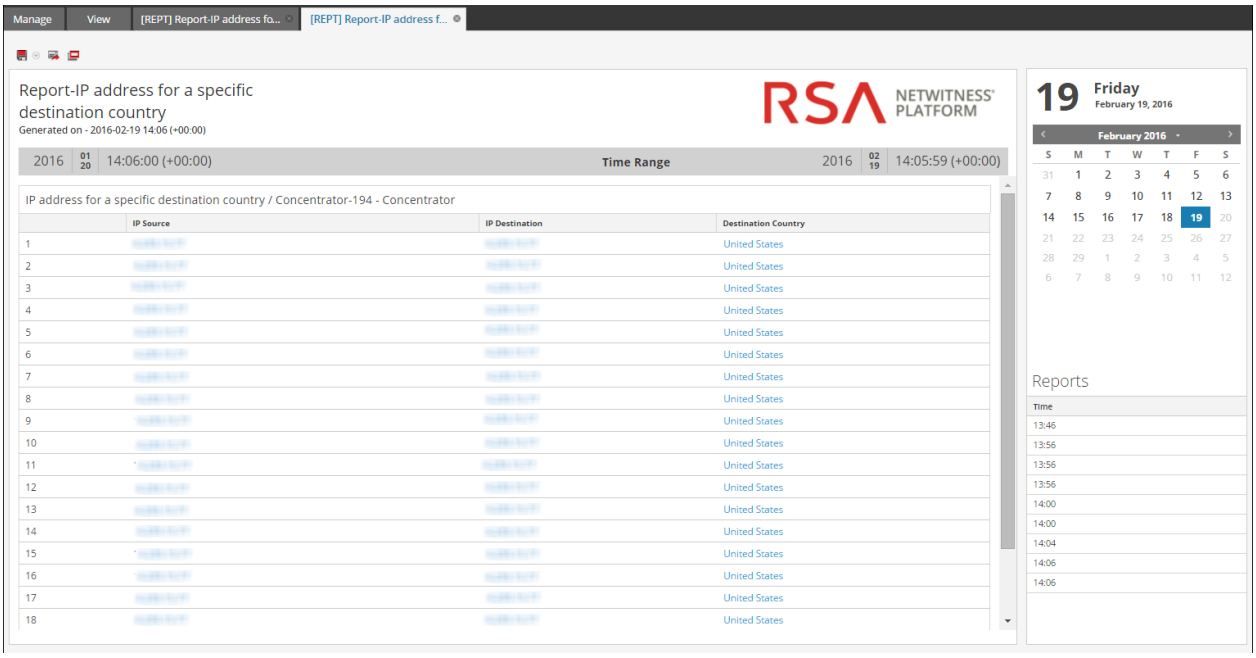
Note: While scheduling a report, if you select **Paste** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.

12. In the variables field, click  .
13. Do one of the following:
    - Enter the value for the variable, or
    - Choose the list value for the variable.



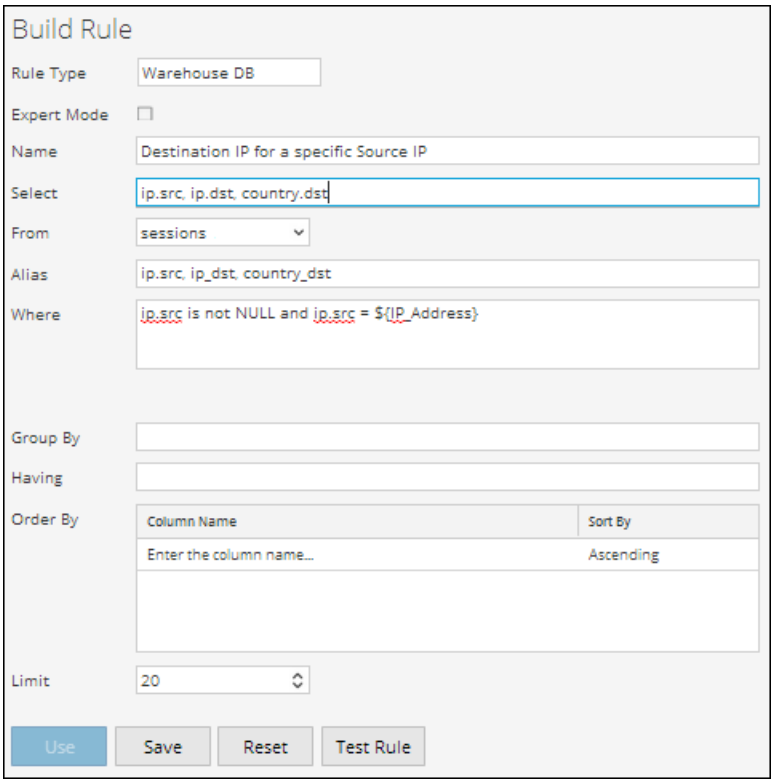
14. Click **Select**.
15. Click **Schedule**.

    The scheduled report executes as scheduled and provides the configured outputs.

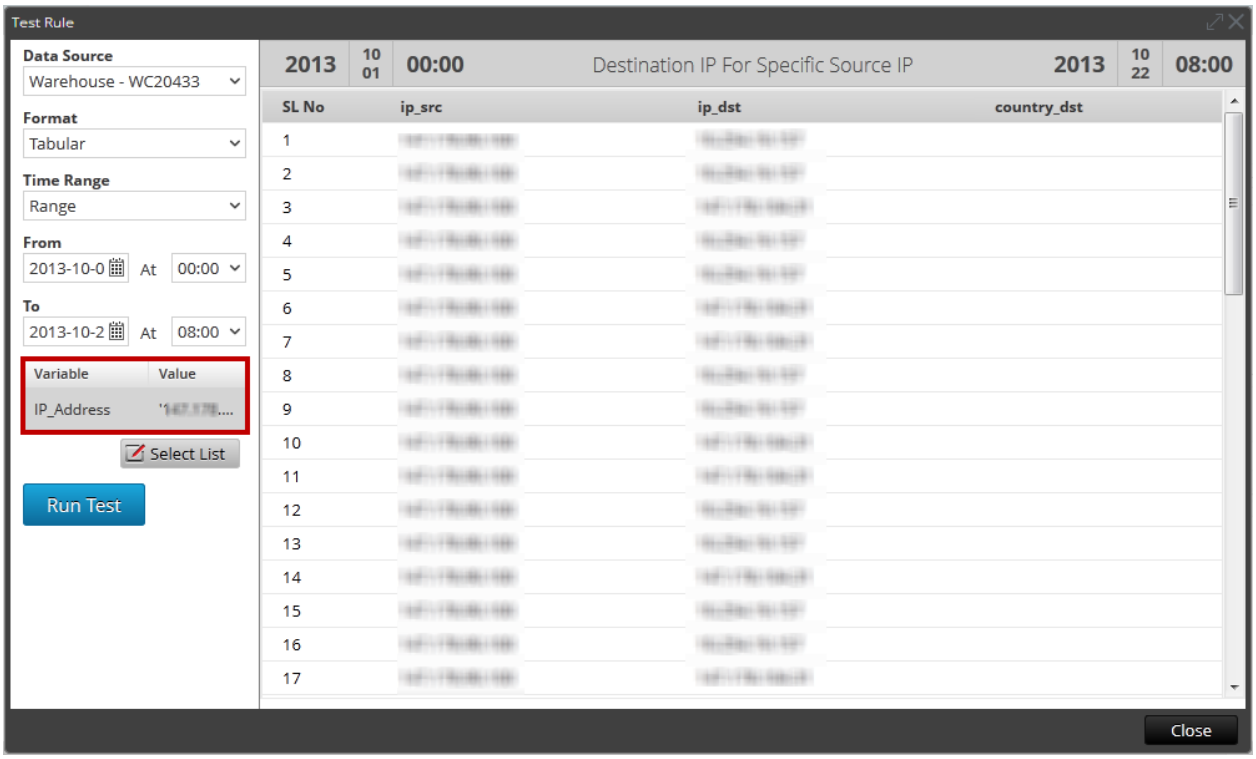


View All Destination IP Addresses for a Source IP Address

The following is an example of a Warehouse rule to view all the destination IP addresses for a specific source IP. The source IP address `ip_src` is defined as a variable `${IP_Address}`.

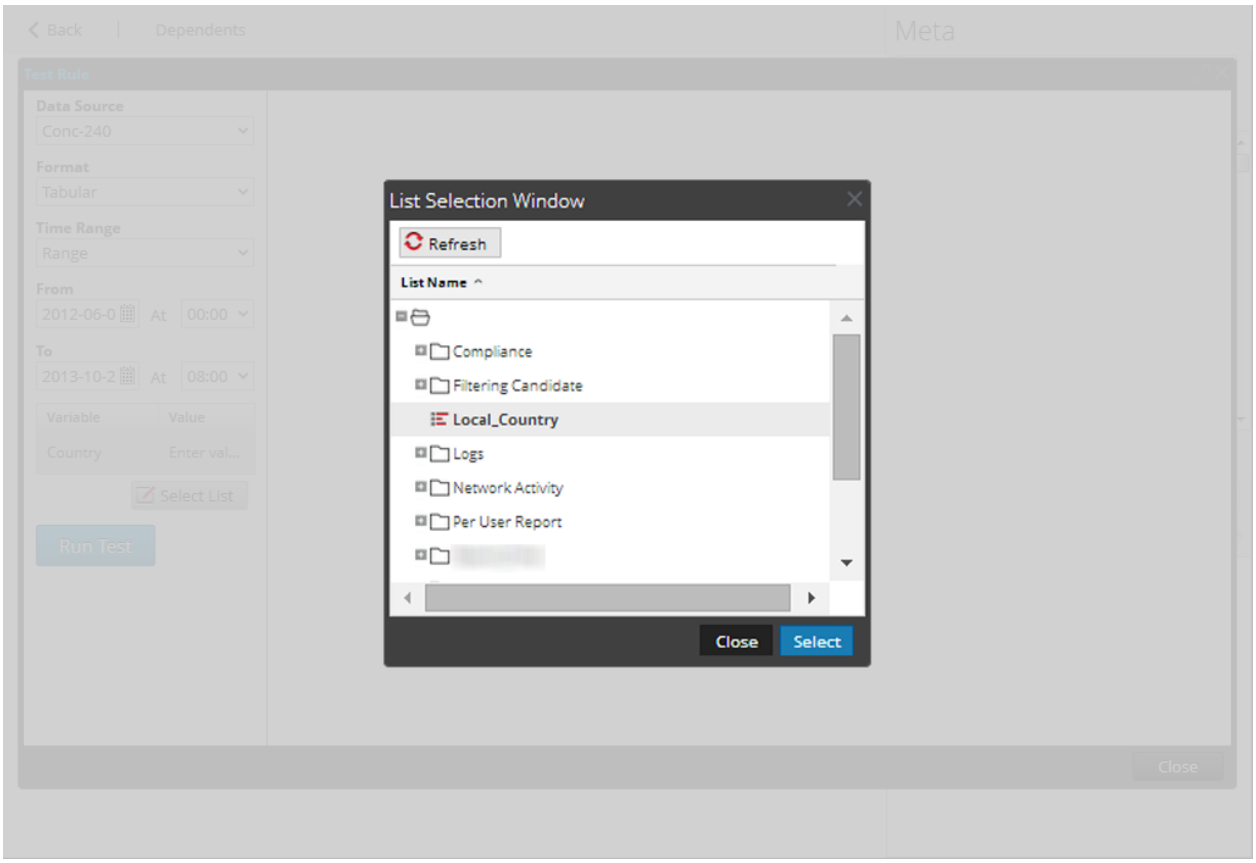


At runtime, you are prompted to enter the source IP address. The figure below shows the `IP_Address` variable, and you can enter a valid source IP address. All the destination IP addresses with the specified source IP are listed.



Associate a Variable to a List of Values

You can associate the variable to a list. For example, you can create a list called `Local_Country` and enter all the country names as values. You can select the list `Local_Country` as the value for the variable `Local_Country`. At Run Configuration, the `Local_Country` list is populated and you can select the country based on which results are displayed.



Iterative Report

An iterative report generates a report for every value in the list.

To schedule an iterative report, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

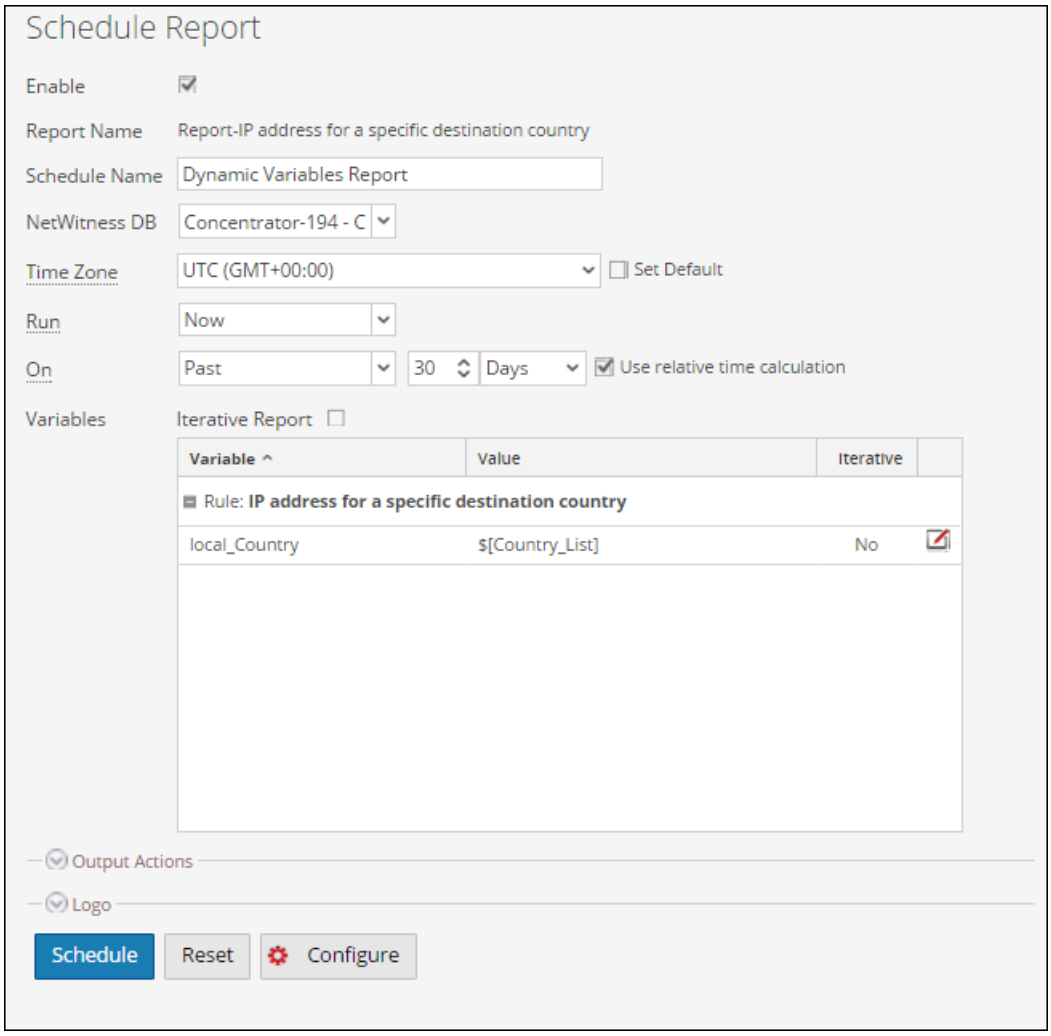
   The Report view is displayed.

3. On the **Reports** panel, click + to create a report.

4. Enter a Report name in the field.

5. Add the rule which has the user defined variable from the Rules tab.

6. Click **Schedule**.
   The Schedule Report view tab is displayed.



7. To execute the reports as per the schedule, select the **Enable** checkbox.
8. In the **Schedule Name** field, enter a name for the schedule report configuration.
9. From the **Data Source** field, select the data source.

> **Note:** If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in the *Reporting Engine Configuration Guide*.

10. (Optional) From the **Warehouse Resource Pool** drop-down, select the pools or queues available in the cluster to schedule the report to run on either the pool or queue. This drop-down list is available only if you select a Warehouse DB report.

> **Note:** All the queues or pools you specified in the Explore page for the Reporting Engine are listed. If no pools or queues are configured in the Explorer page, this drop-down is disabled and the jobs are submitted to the clusters without any a queue or pool name.

Note: If the pool or queue configured in the report schedule is removed from the Cluster, then in the Capacity Scheduler, the queue name remains undefined. However, in the Fair Scheduler, the specified pool name will be created using the property `mapred.fairscheduler.allow.undeclared.pool`.

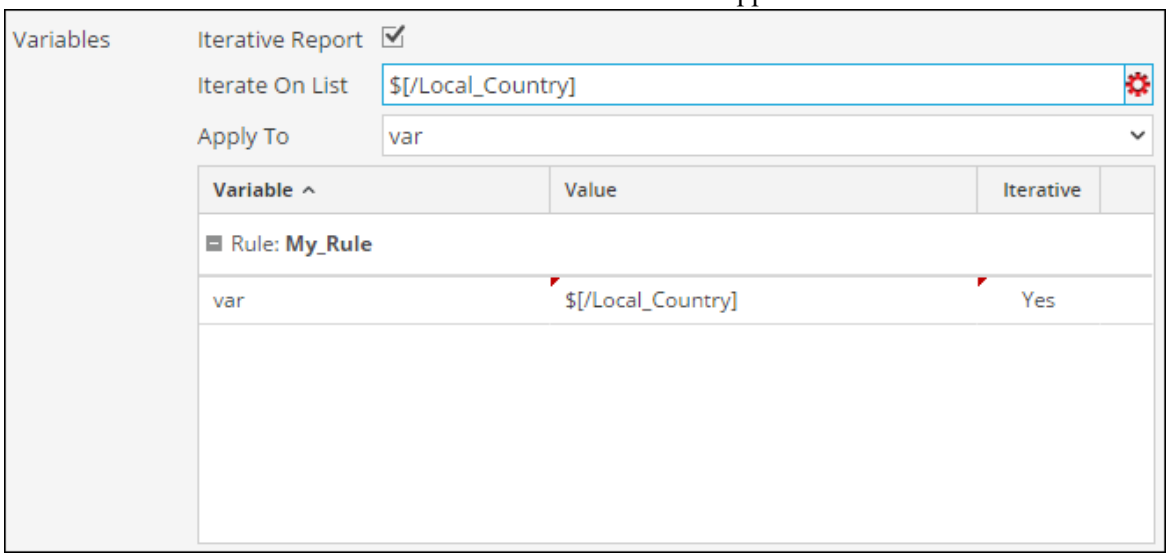
11. From the Time Zone drop-down, select a time zone to display all the time-related data in a report output in the specified format. This setting is configurable from the Reporting Engine Explore view (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
12. From the **Run** field, select the type of run schedule. (For example, Now or Hourly). Depending on the type of run schedule, do either of the following:
    - If you select a **Later** or **Monthly** run schedule, you must provide a value for the day and time in the respective field provided.
    - If you select an **Hourly** run schedule, you must specify the minutes in the **At Minute** field.
    - If you select a **Daily** run schedule, you must enter a time value in the **At** field.
    - If you select a **Weekly** run schedule, you must enter a value in the **At** field and also select the week days.

    Note: While scheduling a report, if you select **Paste** option or **Range (specific/generic)** option or an end time range very close to the current time, you must ensure that the aggregate data in the data source is returned. If there is an aggregation delay in the data source, the end time you choose must account for the delay, otherwise reports lose non-aggregate data for that time range.
13. In the variables field, do the following:
    a. To run iterative reports, select the **Iterative Report** checkbox.
    b. To Iterate on List value, click  .

       The List Selection Window opens.
    c. Choose a list and click **Select**.

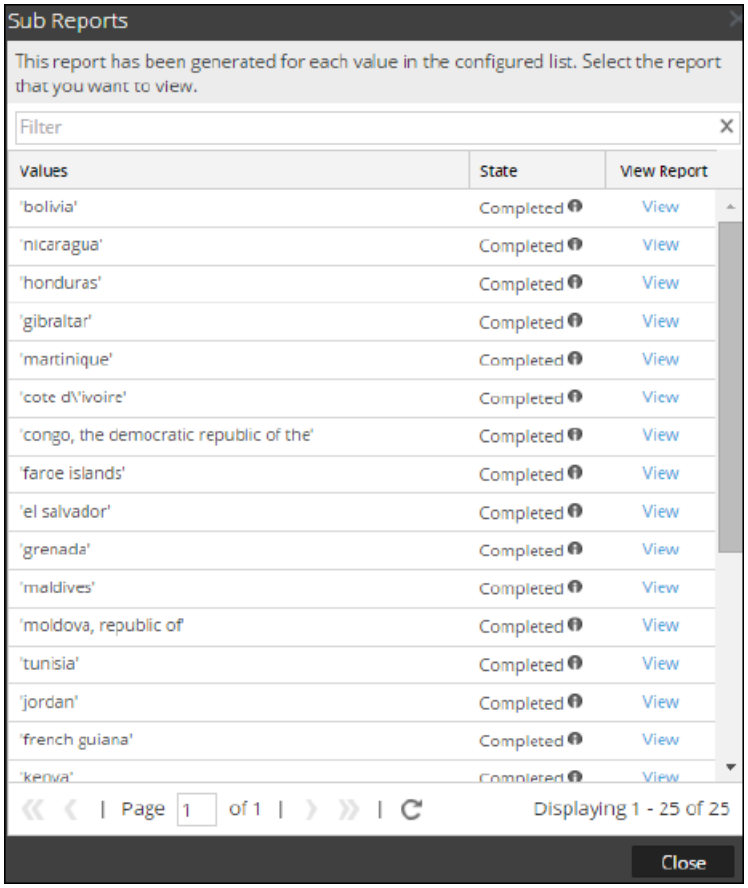
       The list item selected gets added to the **Iterate on List** field.

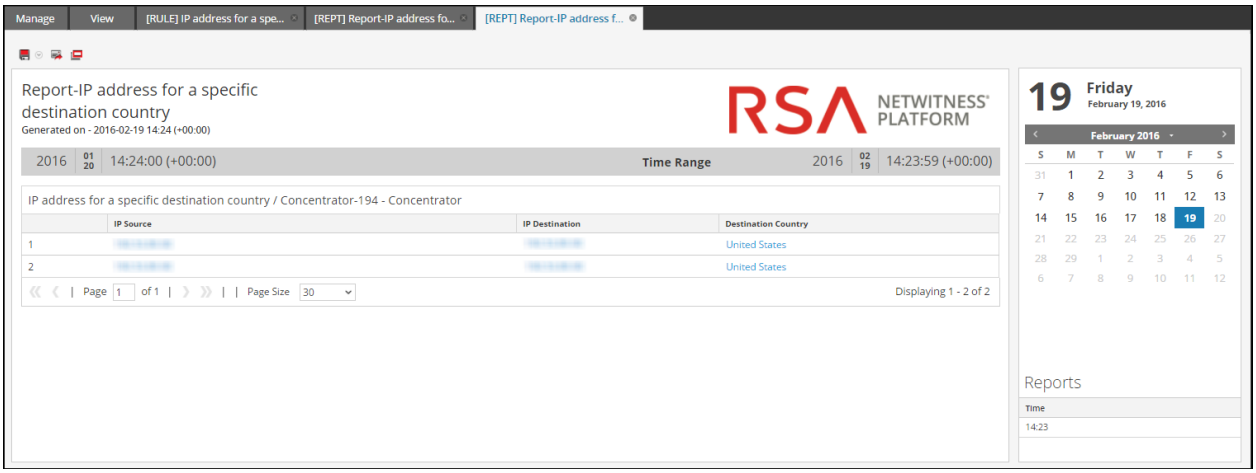
d. Select the variable on which the selected list value has to be applied.



14. Click **Schedule**.
    The scheduled report executes as scheduled and provides the configured outputs.

The following figure shows the Iterative Report view.





Create a Report Using a Rule

You can create a report using a rule. When you create a report using a rule, a default report is created with this single rule. You can further edit the report to add more rules.

To create a report using a rule, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Choose any of the following:

   - Create a report using a rule when you create or edit the rule:

     a. In the **Rules** view, select a rule and click  > **Use**> **Report**.

     The Use Rule dialog is displayed.

   - Select a rule in the Rules panel and click  in the Rule toolbar. From the drop-down menu, select **Use** > **Report**.

   - In the Rules panel click  > **Create Report**.

Note: Custom rules can be used to create a Report and If you select the view for the rule as "Area" or "Pie", a window pops up for **X-Axis** and **Y-Axis** inputs. By default, you can select only the first meta in **X-Axis**.

3. Select **New Report** or **Existing Report** based on your requirement.
4. Click **Select**.

View a Report

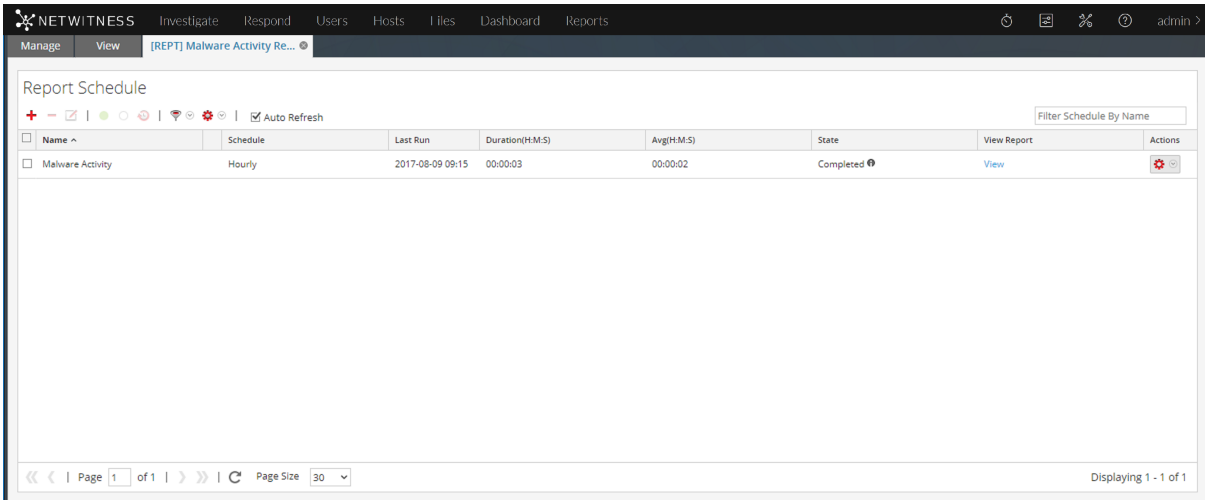
You can view a report or list of all reports. You can also view the scheduled reports to know the state of the scheduled report. If the scheduled report is in a stop or disable state, you can start or enable the scheduled report.

After you view a report, you can perform any of the following tasks:

1. You can print, save, email and view reports on full screen.
2. You can also select a date from the calendar to view a list of successfully run reports for the chosen date.

To view a report, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, select a report and in Actions column, click  > **View Scheduled Reports**.
4. Click the **#Schedules** column.
   The Schedule Reports view tab is displayed with the status of each of the scheduled report.



5. Select a scheduled report and click **View**.
   One of the following is displayed:
   - The selected report.
   - The Sub reports panel for a scheduled report having 'Iterative' selected.

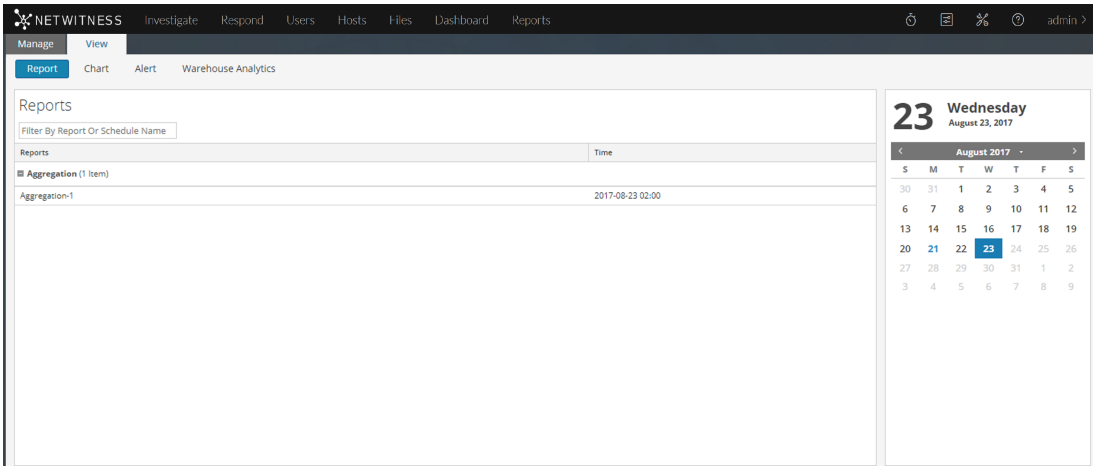
For each value in the configured list a report is displayed.

> **Note:** If the report status is partial or complete, the "last run timestamp" and the "last run (seconds)" are updated. However, the average time taken to run the report is updated only when the report status is complete and not when it is partial.

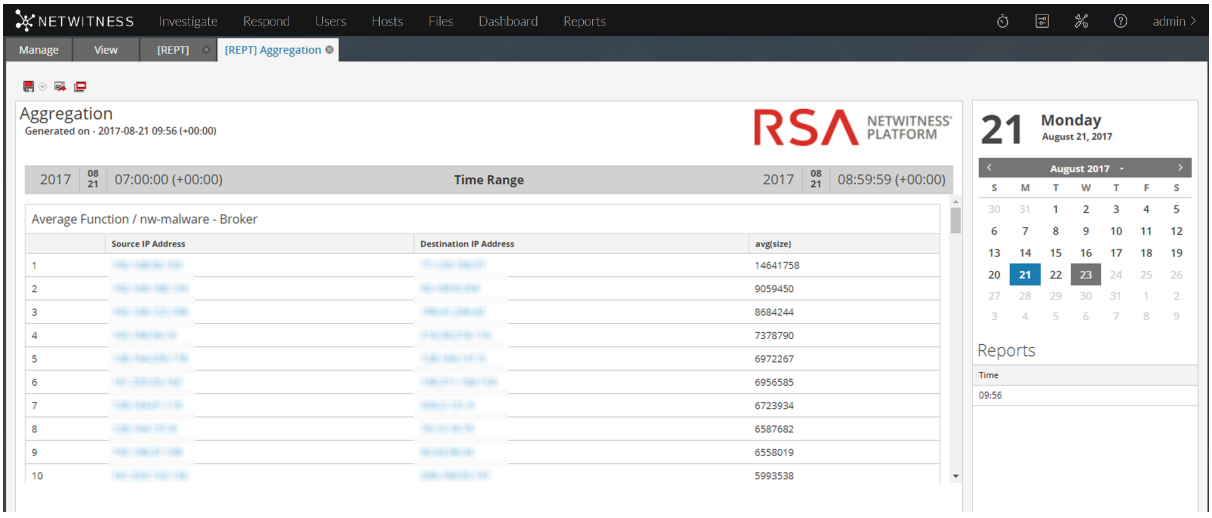
To view a list of all reports, perform the following:

1. Go to **Reports**.
   The **Manage** tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, click **View All Reports**.
   A list of reports along with their schedule name and time are displayed on the View tab.

> **Note:** If no list is displayed, select a date from the calendar to view a list of reports for that date.



4. Double-click on a report to view the details of the report.
5. You can select a scheduled report and print, save as PDF/CSV, send email notifications, or view it on full screen.



Investigate a Report

You can investigate a report by directly navigating to the Investigation View from the report. With the Investigate a report option, you can investigate each event mentioned in the report.

To investigate a report, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

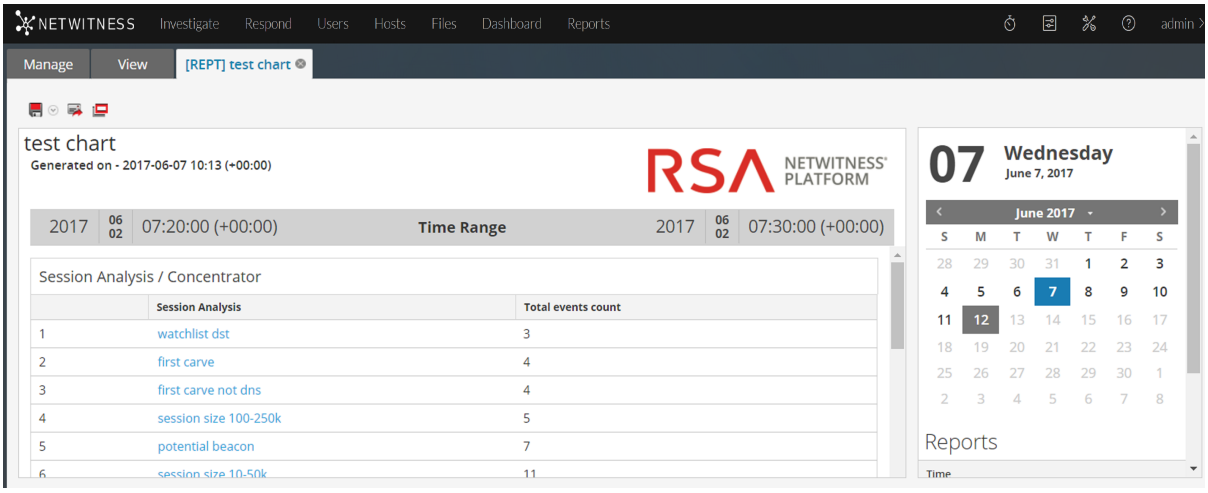
3. In the **Reports** toolbar, click **View All Reports**.

   The View All Reports tab is displayed.

   Note: If no reports are displayed in the View All Reports, select a date for which you want to display the reports.

4. Double-click the report name to view the report details.

   The Report details screen is displayed.



   You can click on the session analysis to investigate on the report.

Note: If you want to manually copy the result data and use it for investigation, make sure that the binary values are prefixed with 'hex:'.

Manage Lists, Rules or Reports

You can set access control, delete, edit, import, or export a list, rule or report.

Manage a List

You can perform the following procedures to manage a list.

- Access Control for a List and List Group
- Edit a List
- Delete a List or List Group
- Duplicate a List
- Export a List or List Group
- Import a List or List Group
- Filter Unused Lists

Access Control for a List and List Group

You can set up the access permissions for the user roles to manage lists or list groups. The Reporting provides access control at the list and list group level. Only a user who has the right set of permissions can perform the tasks in the Reporting. The access control is managed by the administrator from the  (Admin) > Security > Roles tab.

As an administrator, you must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

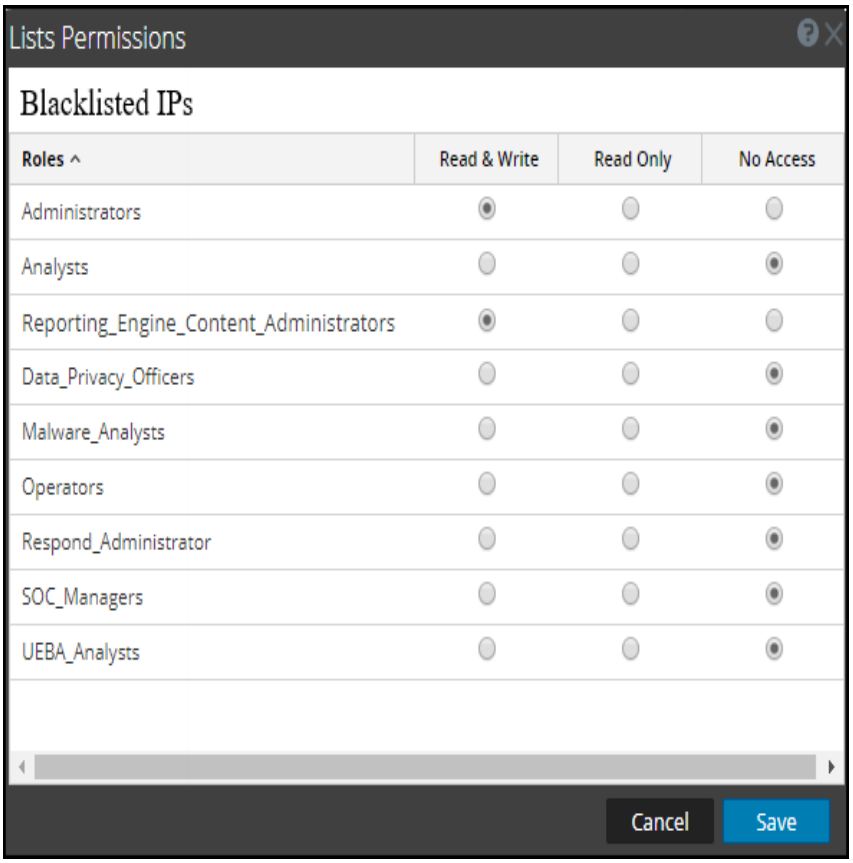
Lists or list groups can be assigned to a specific set of user roles. When users log into NetWitness, they can access only those lists to which they belong. Users who belong to a user role with the **Read & Write** access permission have full access rights on the lists. Further, the access can be strengthened so that lists are accessed only by those who have the **Read Only** access.

Note: You must have **Read Only** permission for a list group to view the lists within that group.

For example, if you want **Security Analysts** to have access to all the lists in a list group, you can set the permission **Read & Write** at the list group level. And, if you do not want the **Operator** role to have access to a specific set of lists in a list group, you can set the permission **No Access** at the list group level.

At the list or list group level, you can set the following access permissions for the user roles in NetWitness. For more information, see List View:

- Read & Write
- Read Only
- No Access



The following table lists the columns in the Lists Permissions panel:

Column	Description
Roles	Describes roles of the users logged into the NetWitness user interface.
Read & Write	Allows users to access, view, edit, delete, import, and export lists on the Lists view. Users can also change the permission on the rule.
Read Only	Allows users to only access and view the list on the lists view.
No Access	Doesn't allow users to access or view the lists.

Access Control for a List

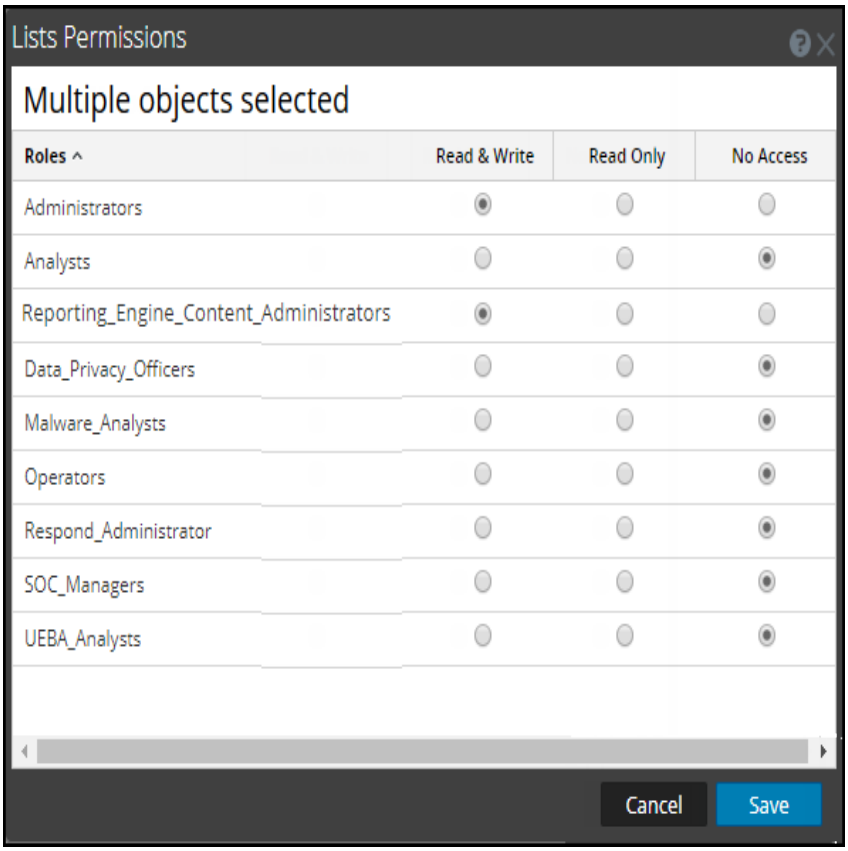
To change the list permissions, you must select a list and set access permissions using the List Permissions panel.

If you want to change the access permission for a specific user role, you must set it at the list level. Except for administrators (with full access in Reporting Engine service Config page) and reporting engine content administrators, the default permission set for all the user roles is **No Access** before applying job permissions.

Access Control Multiple Lists

You can select multiple lists at once and set access permissions using the Lists Permissions Panel. The access permission that you choose is applied to all the selected lists.

Note: The **"*"** beside the role name indicates that other permissions are available for the user role. If you want to change the access permission for the required user role, select the user role and change the access permission.



Note: If a user (other than ADMIN) creates a list, ADMIN cannot access that list.

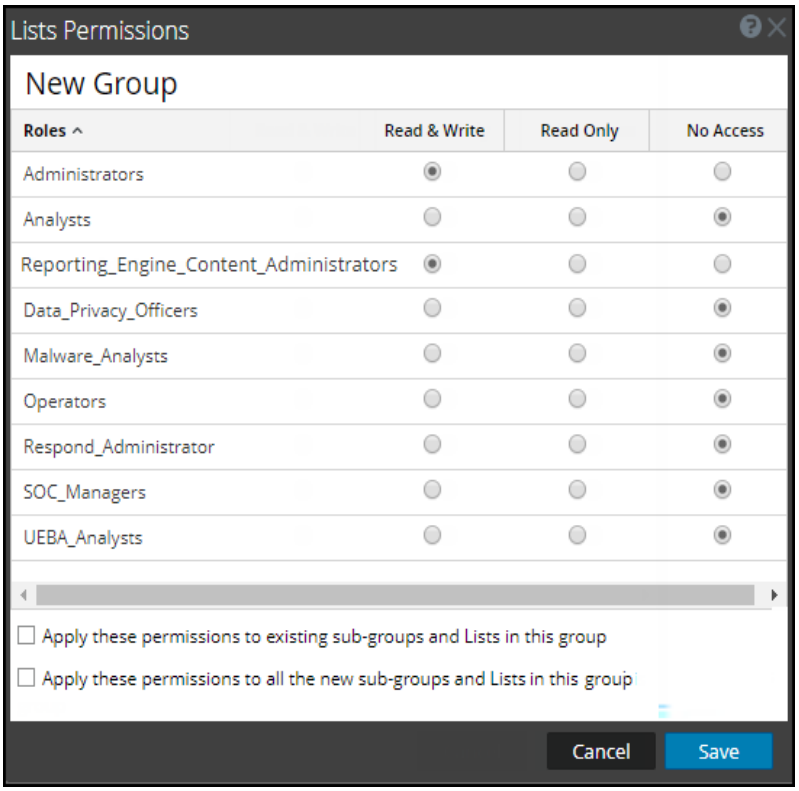
Access Control for a List Group

To change the list group permissions, you must select a list group and set access permissions using the Lists Permissions panel.

If you want to change the access permission for a specific user role, you must set it at the list group level. The default permission set for all the other user roles is **No Access** before applying job permissions.

You can also apply permissions to existing subgroups and lists in the group by selecting the appropriate checkbox.

You can also apply permissions to all the new subgroups and lists in the group by selecting the appropriate checkbox.



The following scenarios describe defining permissions for list groups or subgroups and lists in the groups:

- Scenario 1: Permissions applied to list group or subgroup based on the user role.

  Each of the levels will have a permission set depending on the user role. For example, if a list group is assigned the role of Security Analyst, permissions are set to Read & Write for the list group.

- Scenario 2: Permissions applied to subgroups and lists in the group.

  The access permissions that you set can be applied to subgroups and child objects of this group. Permission at the list group level will be inherited by the subgroups and lists in the group.

Role (Analysts)	Permissions applied to list group or subgroup based on the user role	Permissions applied to subgroup and lists in the group
Group	Read & Write	Read & Write
Subgroup	Read	Read & Write - Inherited
Lists	Read	Read & Write - Inherited

Access permission for a list or list group

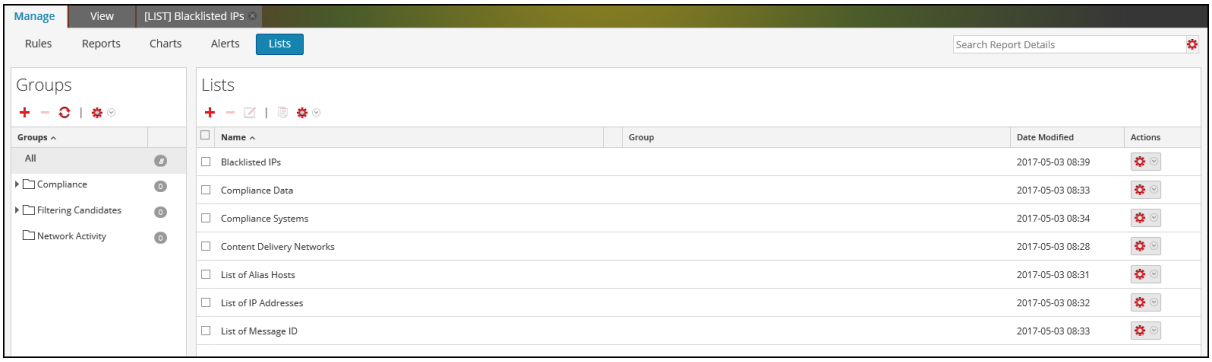
Ensure that you have at least **Read & Write** access permission so that you can set access permissions for lists or list groups.

To set access permission for a list, perform the following:

1. Go to **Reports**.

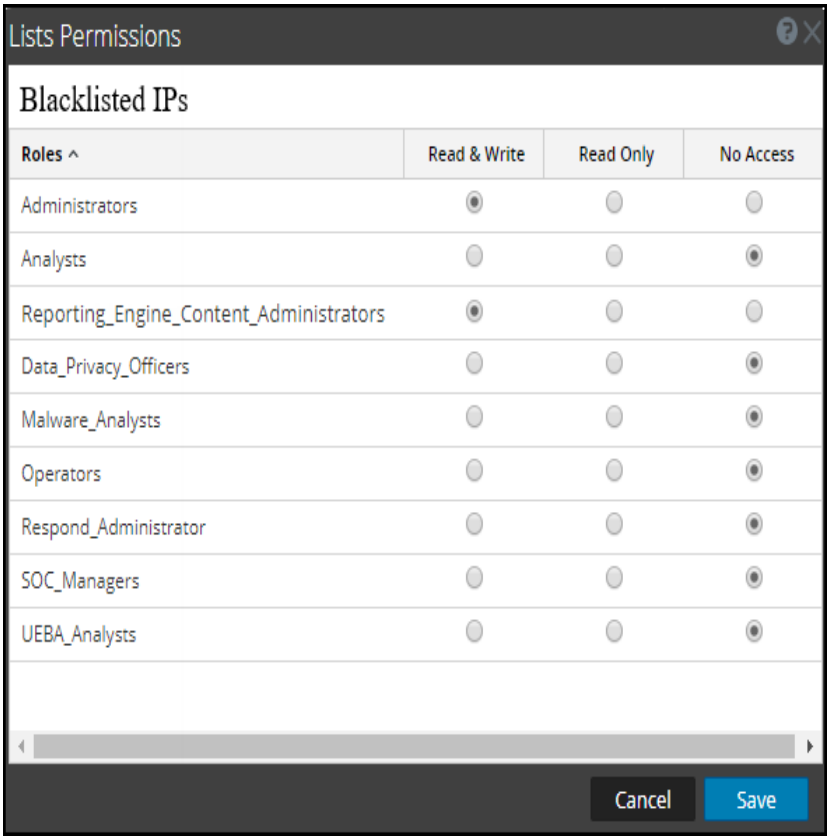
   The Manage tab is displayed.

2. Click **Lists**.
   The List view is displayed.



3. In the **Lists** panel, select a list.

4. Click  > **Permissions** in the List toolbar.
   The List Permissions dialog is displayed.



5. Select the appropriate access permission for each of the user roles and click **Save**.

   A confirmation message that the permission is successfully set for the selected list is displayed.

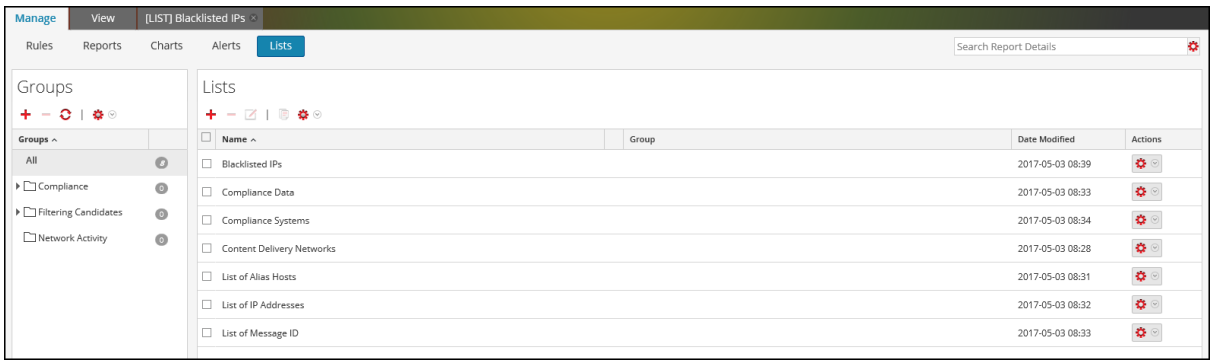
To set access control for a list group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

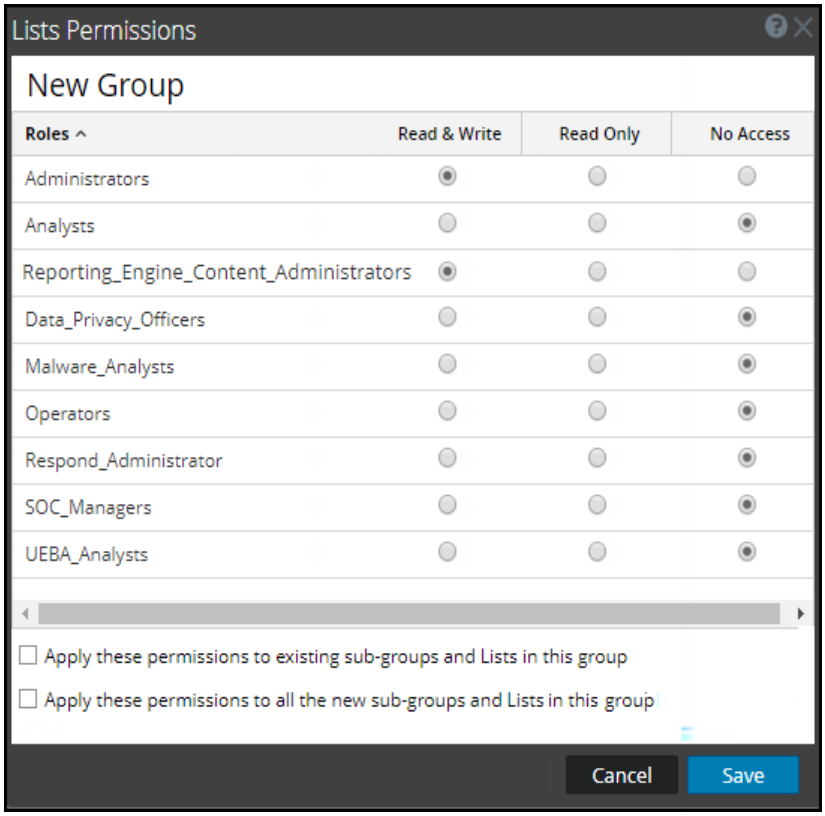
   The List view is displayed.



3. In the **Lists Groups** panel, select a list group.

4. Click  > **Permissions**.

   The List Permissions dialog is displayed.



5. (Optional) Select the appropriate checkbox to apply these permissions to existing subgroups and lists in this group.
6. (Optional) select the appropriate checkbox to apply these permissions to all the new subgroups and lists in this group.
7. Click **Save**.

   A confirmation message that the permission is successfully set for the selected list group is displayed.

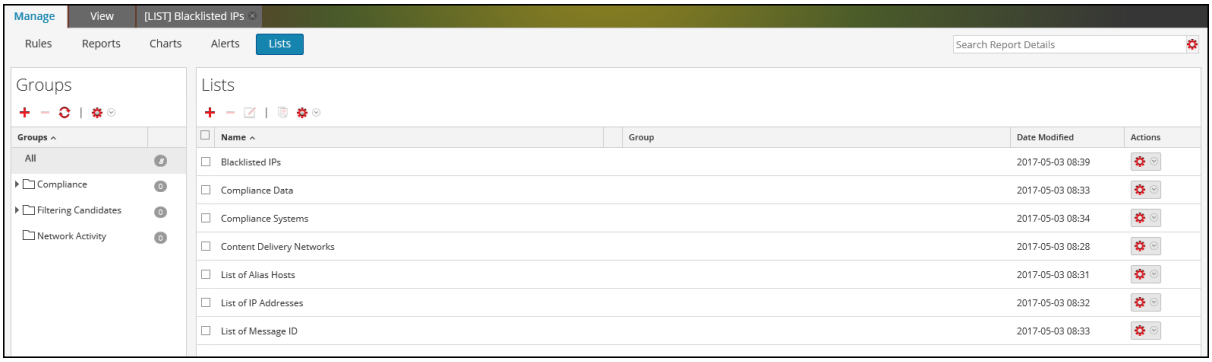
Edit a List

To edit a list, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Lists**.

   The List view is displayed.



3. In the **Lists** panel, select a list that you want to edit and do one of the following.
   - Click  in the **Lists** toolbar.
   - In the **Lists** panel, click  > **Edit**.

     Note: You can only edit one list at a time.
4. Modify the required fields and add new values to the list.
5. Click **Save**.

   A confirmation message that the list is saved successfully is displayed.

Delete a List or List Group

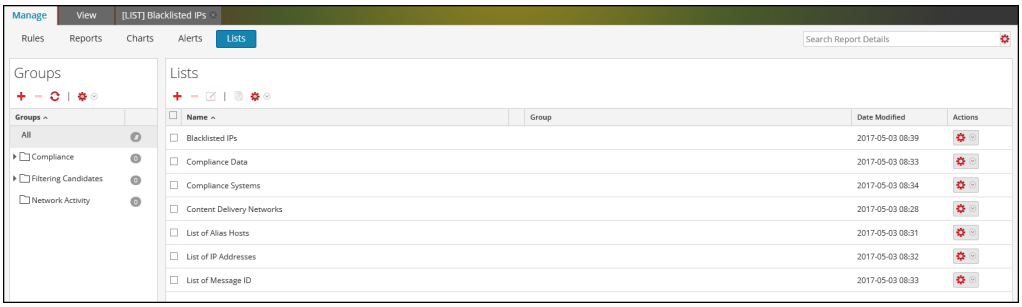
To delete a list, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The List view is displayed.



3. In the **Lists** panel, do one of the following:

   - Select a list or multiple lists that you want to delete and click in the **Lists** toolbar.
   - In the **Actions** column, click > **Delete**.

     Note: Before you delete a list, make sure that the list is not associated with any rule.

4. Click **Yes** to delete the list.

   A confirmation message that the list is deleted is displayed and the selected list is deleted from the List View panel.

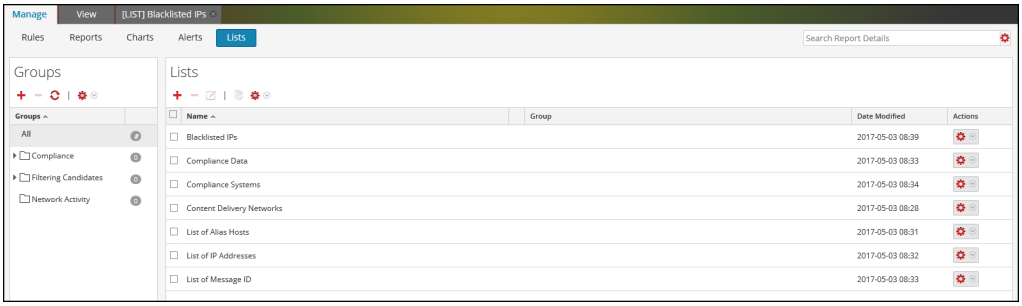
To delete a list group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

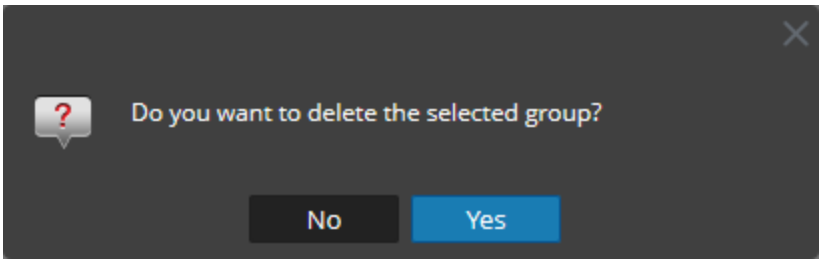
2. Click **Lists**.

   The List view is displayed.



3. In the **Lists Groups** panel, select the group and click .

   A confirmation dialog is displayed.



Caution: If you delete a group, all subgroups and lists in that group are deleted.

4. Click **Yes** to delete the selected group.

Note: If you try to delete a list group that has lists referenced in a rule or an alert, a warning message that **Lists are referenced in a rule** is displayed.

Duplicate a List

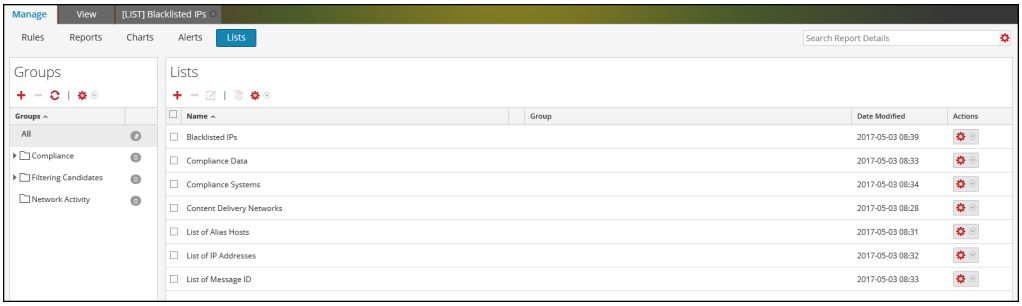
To duplicate a list, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The List view is displayed.



3. In the **Lists** panel, select a list that you want to duplicate.

   Note: You can only duplicate one list at a time.

4. In the **Lists** toolbar, click  .

Export a List or List Group

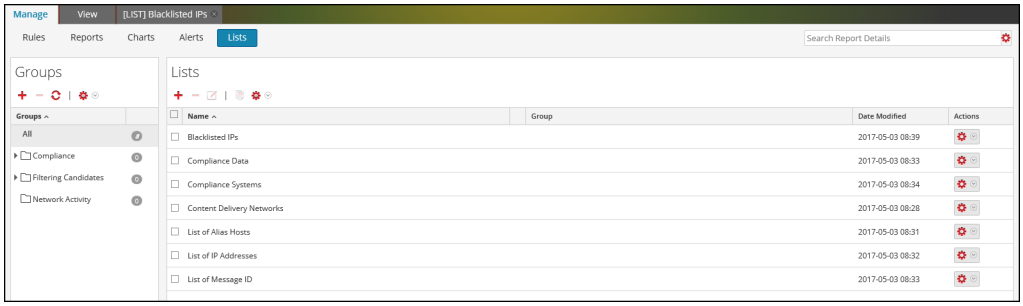
To export a list, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

The List view is displayed.



3. In the **Lists** panel, do one of the following:

   - Select a list and click  **> Export** in the List toolbar.
   - In **Actions** column, click  > **Export**

   You can export multiple lists at a time. To select multiple lists, select the checkbox of the lists to be exported. A browser-specific export dialog may be displayed allowing you to open or save the file.

To export a list group, perform the following:

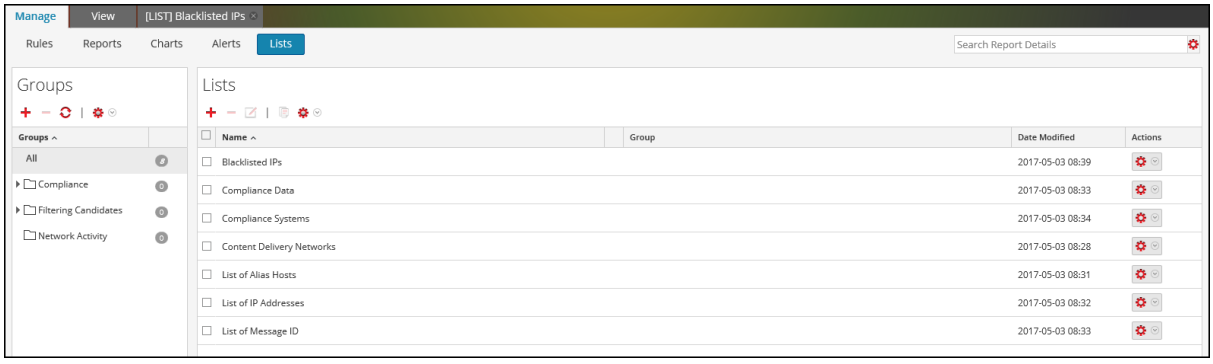
You can export selected list groups to an external file that can be later imported to NetWitness. If nothing is selected in the List Library panel, the entire list tree is exported. When you export, the result is a single export file in binary format.

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The List view is displayed.



3. In the **Lists Groups** panel, select the list group containing the lists which you want to export.

4. Click  > **Export**.

   You can export multiple list groups at a time. To select multiple list groups, press and hold the CTRL button and select the list groups to be exported. The exported file is saved to the local drive.

Import a List or List Group

To import a list, perform the following:

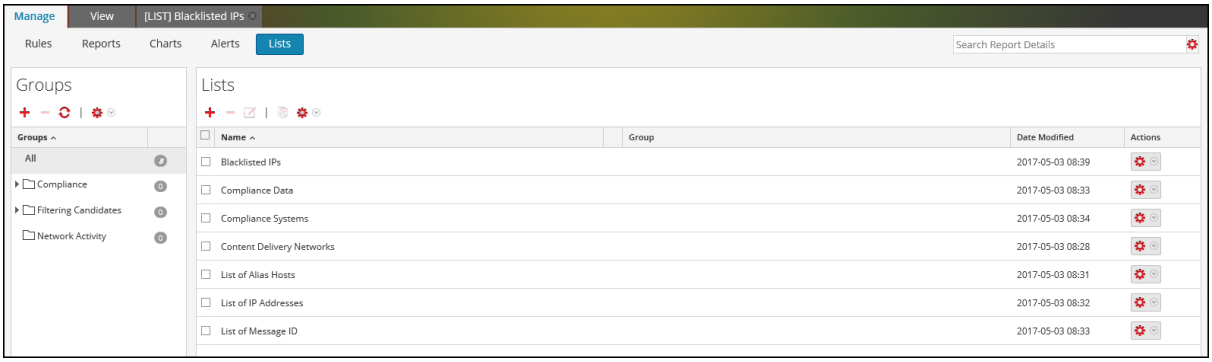
You can import lists from instances of NetWitness into the list tree in the List View panel. Lists must be in a valid binary file exported from a NetWitness instance.

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The List view is displayed.

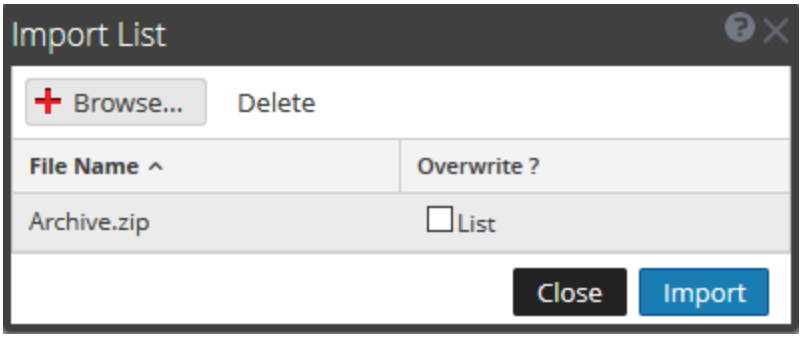


3. In the **Lists** toolbar, click  > **Import**.

   The Import List dialog is displayed.

   Note: You can import multiple lists at a time. To select multiple lists, press and hold the CTRL button and select the lists to be imported.

4. Click **Browse** and select archived file containing the lists.



5. Click **Import**.

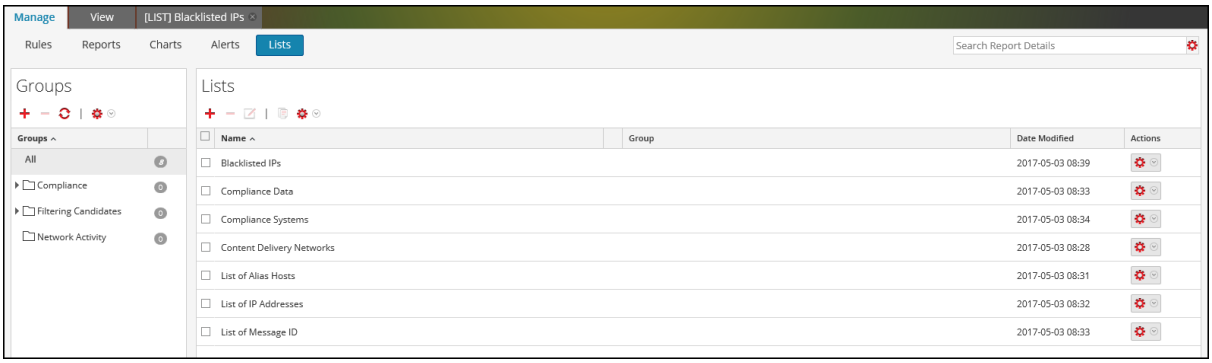
Note: During the import process, if a duplicate list exists and you do not select the overwrite option, the list is imported and no message about duplicate lists is displayed.

To import a list group, perform the following:

You can import list groups from instances of NetWitness into the list tree in the List Groups panel. Lists must be in a valid binary file exported from a NetWitness instance.

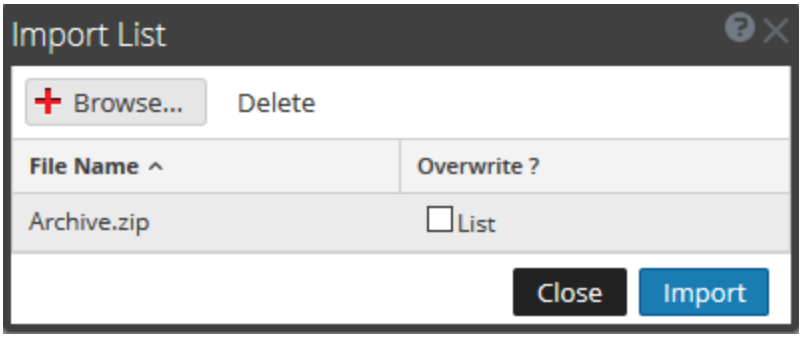
1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.

   The List view is displayed.



3. In the **Lists Groups** panel, click  > **Import**.

   The Import List dialog box is displayed.
4. Click **Browse** and select archived file containing the list groups.



   You can import multiple list groups at a time. To select multiple list groups, press and hold the CTRL button and select the list groups to be imported.
5. Click **Import**.

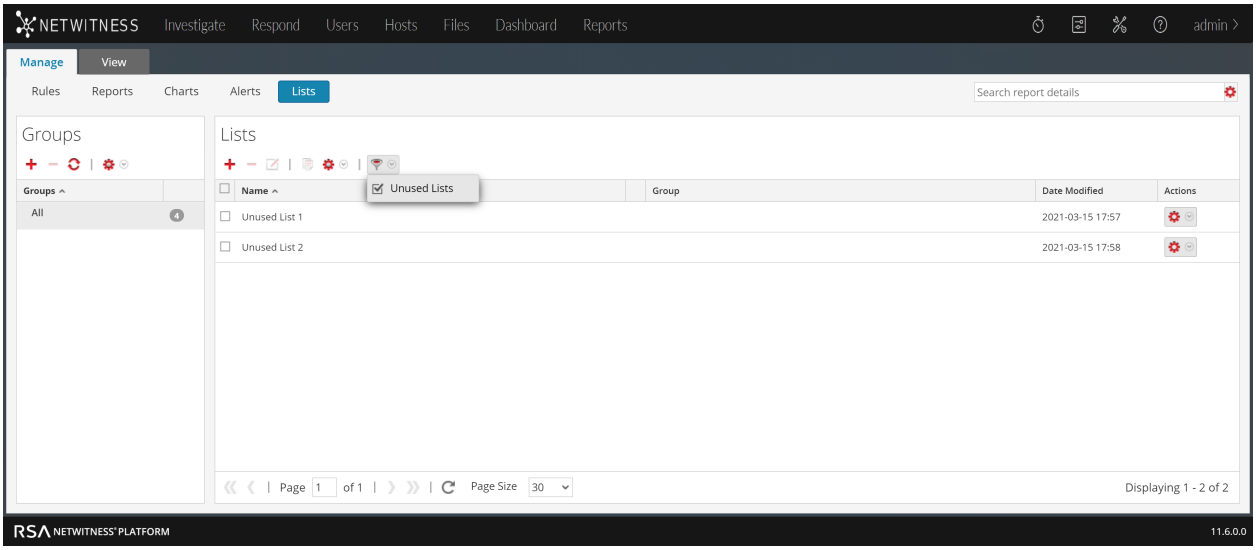
Note: During the import process, if a duplicate list group exists and you do not select the overwrite option, the list group is imported and no message about duplicate list group is displayed.

Filter Unused Lists

You can filter and delete the lists that are not used by any rule. To filter unused lists:

1. Go to **Reports**.
   The **Manage** tab is displayed.
2. In the **Lists** panel, click  and select **Unused Lists**.
   List of unused lists will get displayed.

3. [Optional] Delete the unused lists.
   For more information, see Delete a List or List Group.



Manage a Rule

You can perform the following procedures to manage a rule.

- Access Control for a Rule and Rule Group
- Delete a Rule or Rule Group
- Duplicate a Rule
- Edit a Rule
- View Dependents of a Rule
- Export a Rule or Rule Group
- Filter Unused Rules

Access Control for a Rule and Rule Group

To set access permissions the user will have depending on the user role to manage a rule or rule group. The Reporting provides access control at the rule and rule group level. Only a user who has the right set of permissions can perform the tasks in the Reporting. The access control is managed by the administrator from the **(Admin) > Security > Roles** tab.

When creating users and user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Rules or Rule Groups can be tied to a specific set of user roles so that when a user logs into NetWitness, the only rules they can access are rules accessible to the group to which the user belongs. Users that belong to a user role with the ‘Read & Write’ access permission have full access rights on the rule. Further, the access can be tightened so that rules are accessed only by those who have the ‘Read Only’ access.

Note: You must at least have ‘Read Only’ permission on a group to view the rules within that group.

At the rule level, you can set the following access permissions for the user roles:

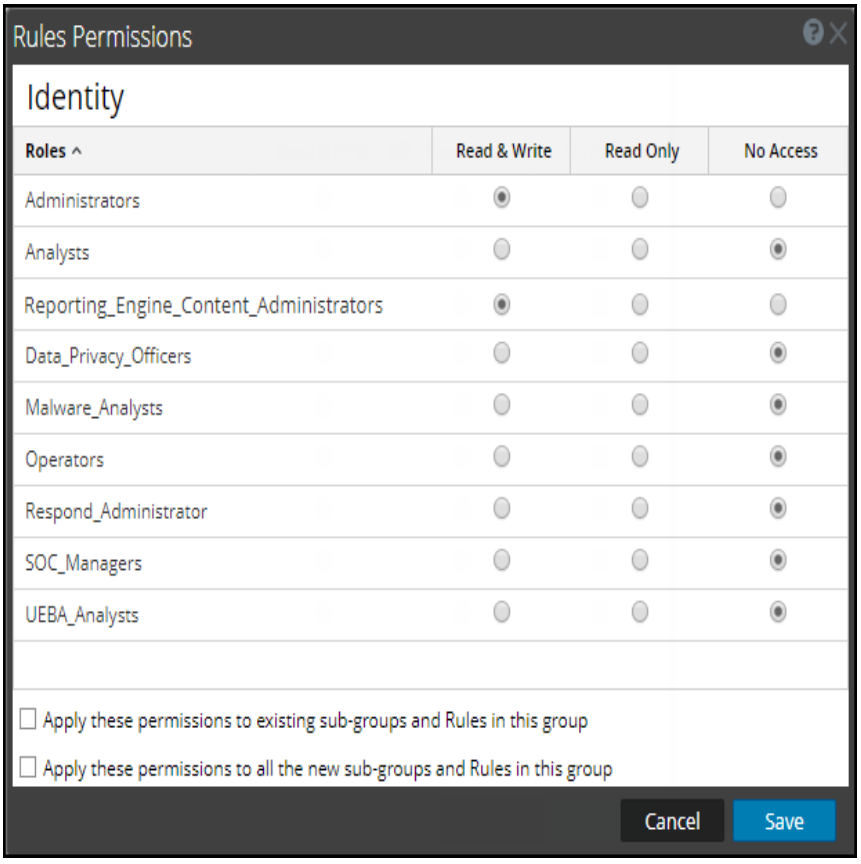
- Read & Write
- Read Only
- No Access

Suppose, you want the **Security Analysts** to have access to all the rules in a Rule Group, you can set the permission '**Read & Write**' at the Rule Group level. And, if you do not want the **Operator** role to have access to a specific set of rules in a rule group, you can set the permission '**No Access**' at the Rule Group level. The permission is set only for the rule group but not the rules or subgroups in the Rule Group.

Access Control for a Rule Group

When you want to change the rule group permissions, you must select a rule group and set access permissions using the Rule Permissions panel.

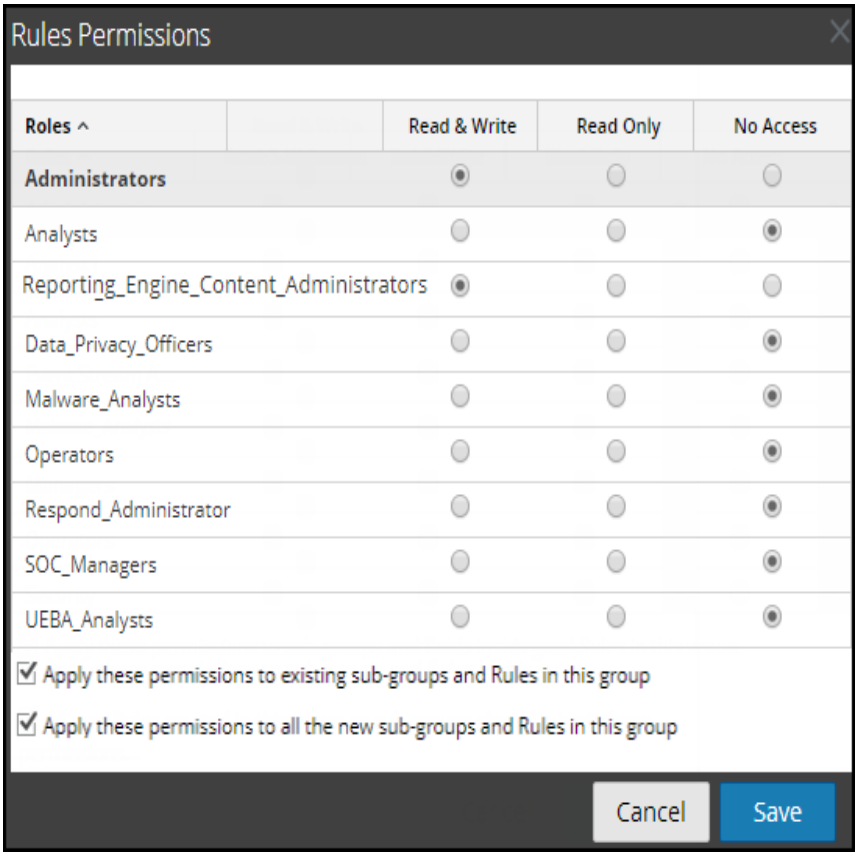
Before applying rule group permissions, the default permission set for all the user roles is 'No Access' permission, and the checkboxes are deselected.



If you want to change the access permission for a specific user role, you must set these at the rule group level, as shown in the figure. Suppose, you want the **Administrators** to have access to all the rules in a Rule Group, you can set the permission '**Read & Write**' in the Rule Group Permissions panel.

You can also apply permissions to existing subgroups and Rules in the group by selecting the appropriate checkbox.

You can also apply permissions to all the new subgroups and Rules in the group by selecting the appropriate checkbox.



You can also apply permissions to subgroups and rules in the group by selecting the checkbox.

The two scenarios are explained in brief:

- Scenario 1: Permissions applied to Rule Group/ Sub Group/ Rules based on the user role.
- Scenario 2: Permissions applied to Sub Group and Rules in the Group.

Role (Analysts)	Permissions applied to Rule Group/ Sub Group/ Rules based on the user role	Permissions applied to Sub group and Rules in the Group
Group	Read & Write	Read & Write
Sub Group	Read	Read & Write - Inherited
Rules	Read	Read & Write - Inherited

The access permissions that you set can be applied to subgroups and child objects of this group.

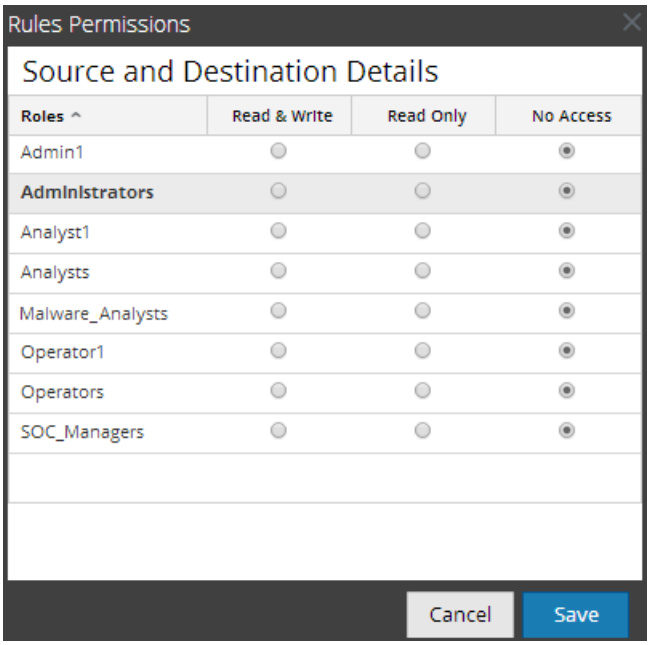
The Rule Group will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** rule group.

For scenario 1, each of the levels will have a permission set depending on the user role. For scenario 2, the permission at the Rule Group level will be inherited by the Sub Group and Rules in the Group.

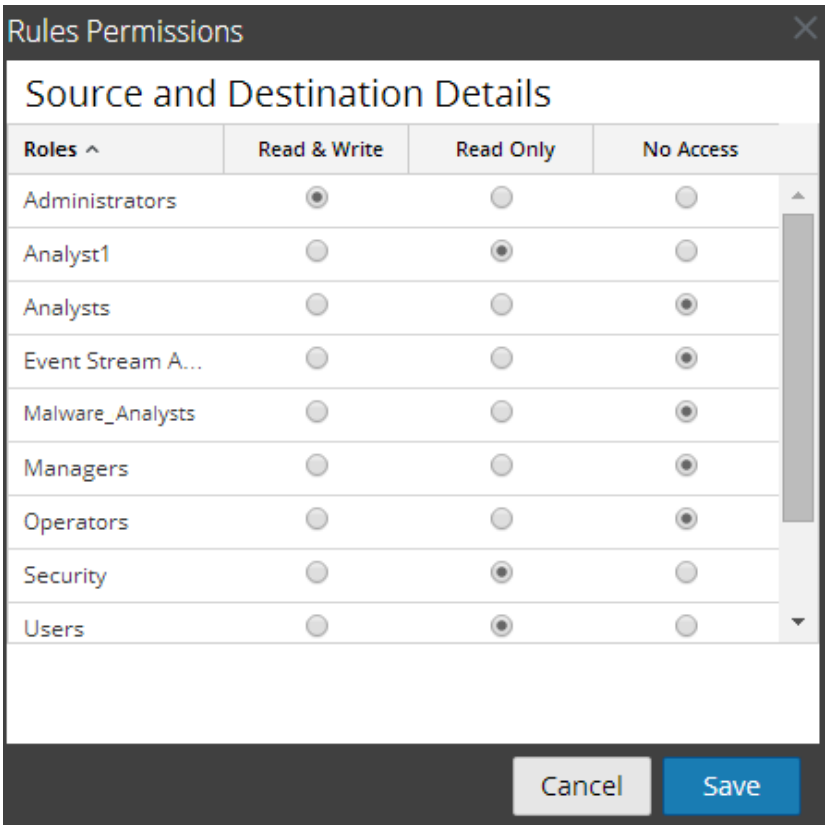
Access Control for a Rule

When you want to change the rule permissions, you must select a rule and set their access permissions using the Rule Permissions panel.

Before applying the Rule permissions, the default permission set for all the user roles is 'No Access' permission and the checkbox is deselected.



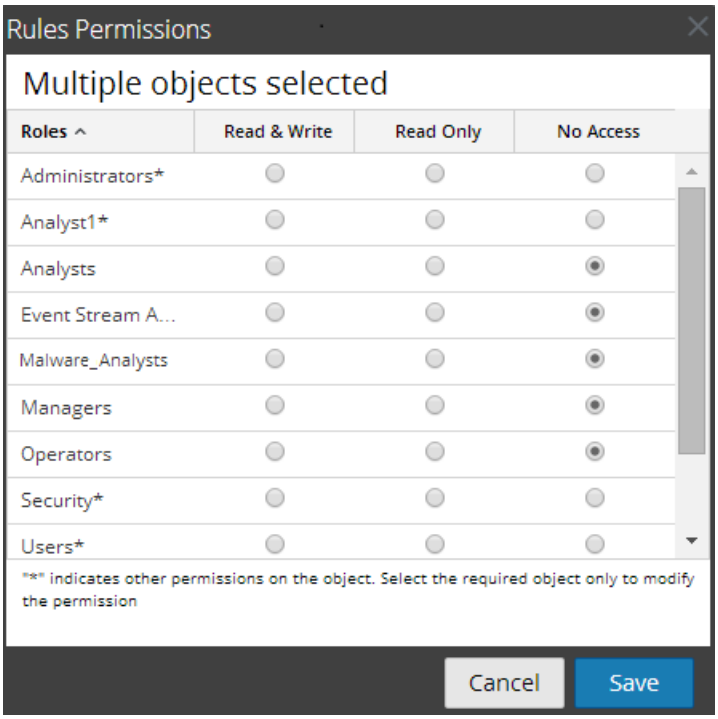
If you want to change the access permission for a specific user role, you must set these at the rule level, as shown in the figure. Suppose, you want the **Administrators** to have access to a specific rule, you can set the permission '**Read & Write**' in the Rule Permissions panel.



Access Control for a Rule When Multiple Rules are Selected

When you want to change permissions of multiple rules, you can select multiple rules at a time and set their access permissions using the Rules Permissions Panel. The access permission that you choose will be applied to all the selected rules.

Note: The '*' besides the role name indicates the other permissions available on the user role. If you want to change the access permission for the required user role, select the user role and change the access permission.



Log in as a specific user and view the access details

When you log in to the NetWitness UI as a user having 'Read access' permission, all the rules will be denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Rules panel.

When you log in to the NetWitness

UI as a user not having 'Read & Write' access permission on a Rule, all the rules will be denoted with the symbol ( ) and the rules appear grayed out on the Rules List panel.

The following figure shows the Rules panel when logged in with minimal 'Read & Write' access permission.

Name	Type	Group	Date Modified	Actions
*(raw_log)-RULE	Warehouse	Aggregate Function	2014-07-13 09:46	
[redacted]	Warehouse	Regular	2014-07-16 07:34	
Accounts Created	NetWitness DB	Identity Management	2014-07-14 10:56	
Accounts Created SAW	Warehouse	Compliance_old	2014-07-14 09:40	
Accounts Created SAW	Warehouse	Warehouse	2014-07-25 09:48	
Accounts Created SAW(1)	Warehouse	Warehouse	2014-07-25 09:54	
Accounts Deleted	NetWitness DB	Identity Management	2014-06-26 08:35	

Note: If a user (other than administrator) creates a rule, ADMIN cannot access that rule.

Tabular Listing

The following table lists the columns in the Rules Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness user interface.
Read & Write	The user can access, view, edit, delete, import, and export rules on the Rules view. The user can also change the permission on the rule.
Read Only	The user can only access and view the rule on the Rules view
No Access	The user cannot access or view the rule for which this permission is set.

Set Access Control for a Rule

You can set access control for a rule. The Reporting Engine provides access control at the rule level. Only a user who has the right set of permissions can perform tasks on the rule. The administrator when creating users and roles must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

At the rule level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write – View or edit the rules in the rule group.
- Read Only – View the rules in the rule group.
- No Access – Cannot view or edit the rules in the rule group.

Prerequisites

Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a rule.

To set access control for a rule, perform the following:

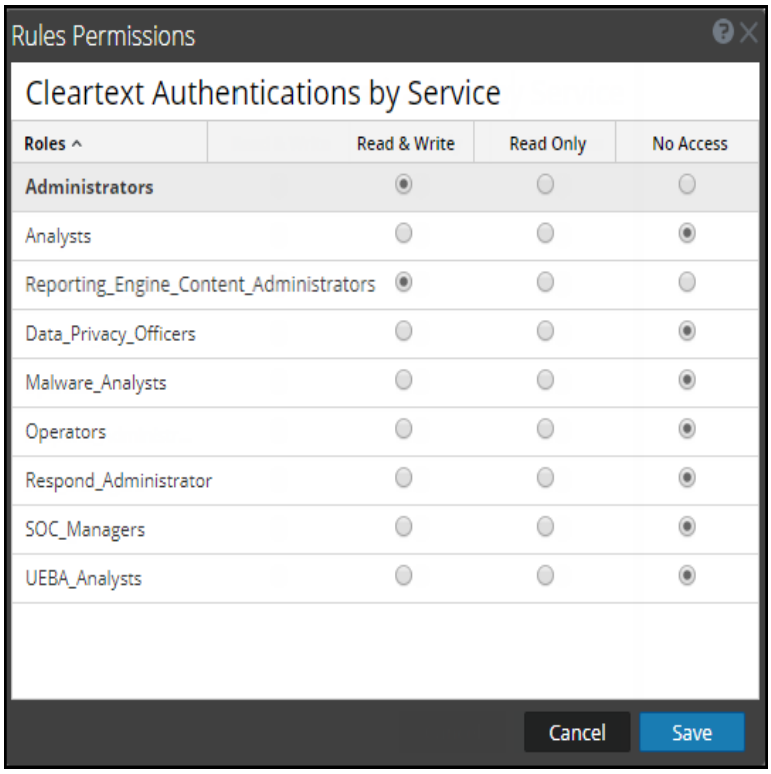
1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** panel, select the rule.

3. Click  > **Permissions** in the Rule toolbar.

   The **Rules Permissions** dialog is displayed.



4. Select the following appropriate access permission for the user role and click **Save**.
   - Read & Write
   - Read Only
   - No Access

Set Access Control for a Rule Group

You can set access control at the rule group level. Only a user who has the right set of permissions can perform the tasks on the rule. The administrator when creating users and roles must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

At the rule group level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write – View or edit the rules in the rule group.
- Read Only – View the rules in the rule group.
- No Access – Cannot view or edit the rule in the rule groups.

Prerequisites

Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a rule group.

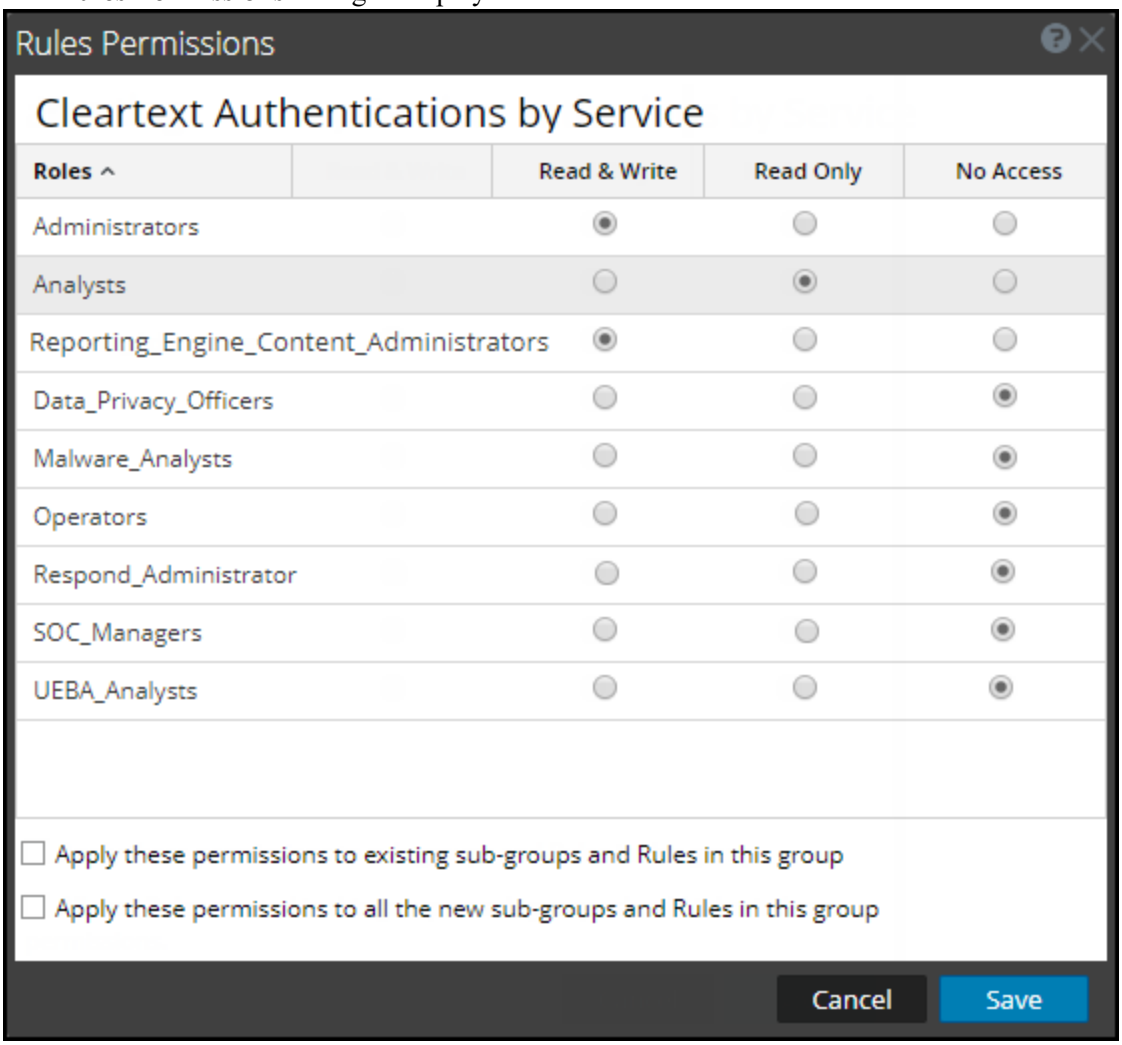
To set access control for a rule group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules Groups** panel, select the rule group and Click and select **Permissions**.

   The **Rules Permissions** dialog is displayed.



3. (Optional) Select the appropriate checkbox to apply these permissions to existing subgroups and Rules in this group.
4. (Optional) Select the appropriate checkbox to apply these permissions to all the new subgroups and Rules created in this group.
5. Click **Save**.

   A confirmation message that permission is successfully set for the selected rule group is displayed.

Delete a Rule or Rule Group

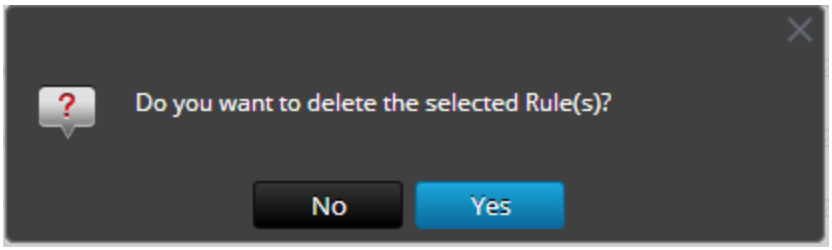
To delete a rule, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** panel, do one of the following.
   - Select a rule and click − in the Rule toolbar.
   - Click ⚙ > **Delete**.

     A confirmation dialog is displayed.



   Note: If a rule is being used in a report, a warning that the rule is in use and cannot be deleted is displayed.

3. Click **Yes** to delete the rule.

   A confirmation message that the rule is deleted successfully is displayed and the selected rule is deleted from the Rules panel.

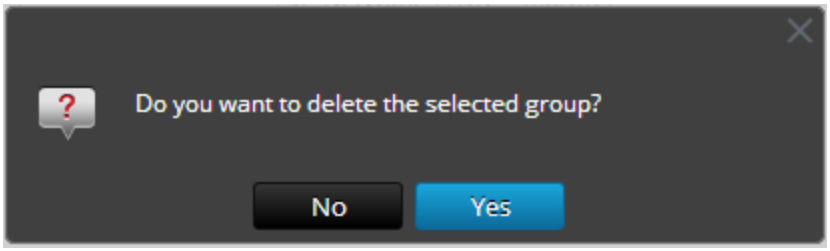
To delete a rule group, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules Groups** panel, select the rule group that you want to delete.
3. Click −.

   A confirmation dialog is displayed.



   Note: If any one of the rules in the group is being used in reports, a warning that the rule is in use and cannot be deleted is displayed.

4. Click **Yes** to delete the group.

   A confirmation message that the group is deleted successfully is displayed and the selected group is deleted from the Rule Groups panel.

Duplicate a Rule

To duplicate a rule, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** panel, select a rule that you want to duplicate.
3. In the Rule toolbar, click  .

Edit a Rule

To edit a rule, perform the following:

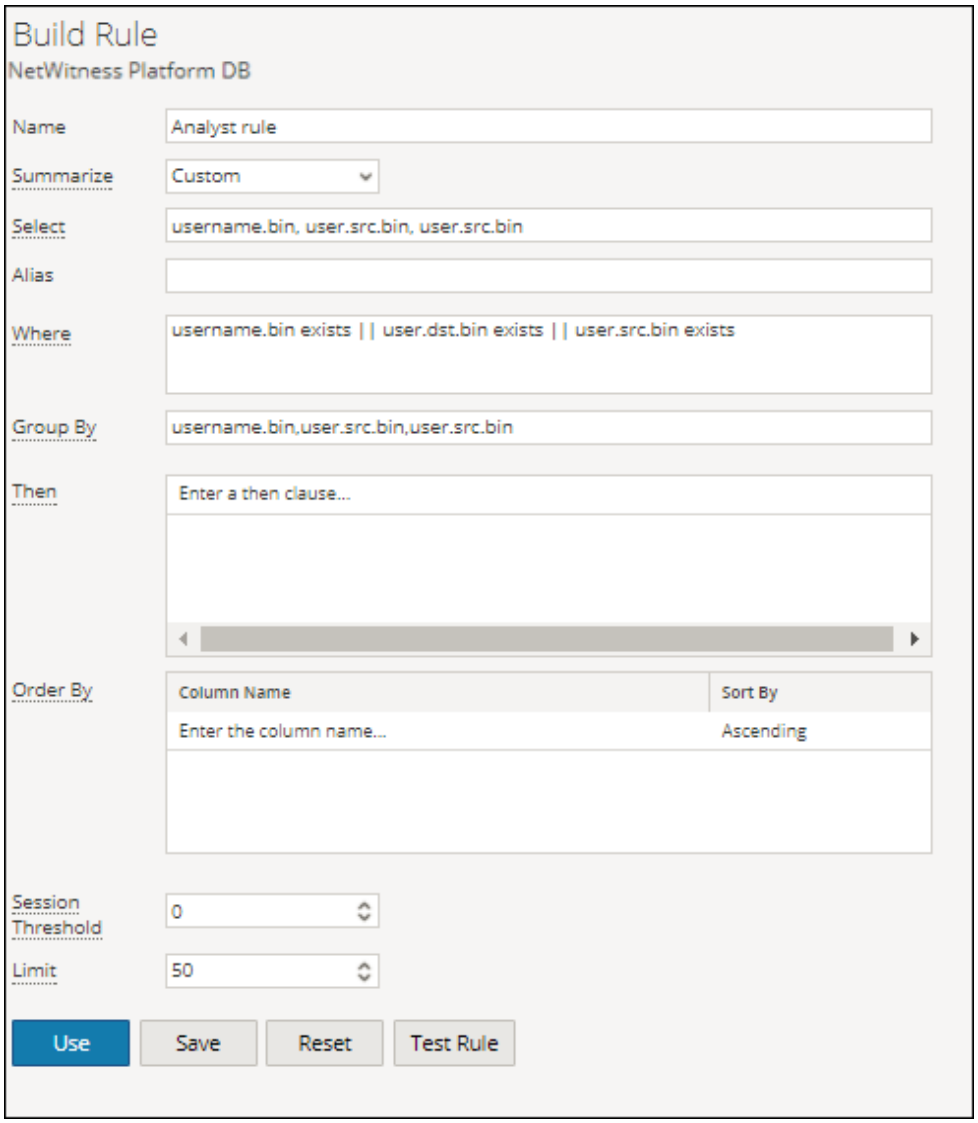
1. Go to **Reports**.

   The Manage tab is displayed.

2. In the **Rules** panel, do one of the following:

   - Select a rule and click  in the Rule toolbar.
   - Click  > **Edit**.

     The Build Rule view tab is displayed.



Note: If a rule is edited, the updated rule definition is applied to the Reports, Charts, and Alerts where the rule is included.

3. Modify the required fields.
4. Click **Save**.

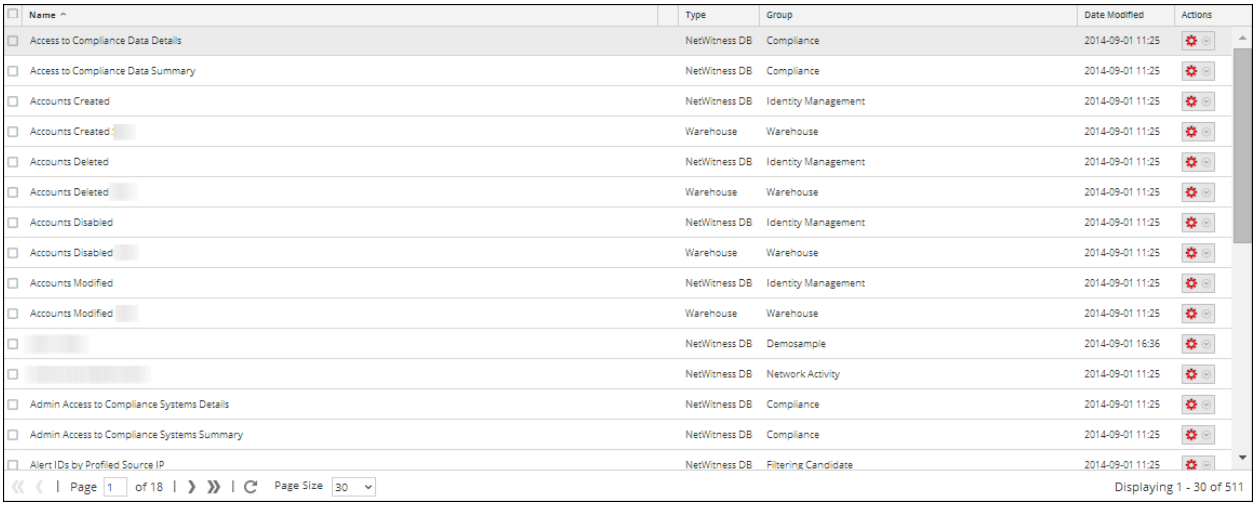
   A confirmation message that the rule is saved successfully is displayed.

When you edit a rule, ensure to re-select the Rule for which you want the Chart to be generated, so that the edited rule is applied. If you do not re-select the Rule and attempt to save or test the rule, the rule is saved and a warning message is displayed.

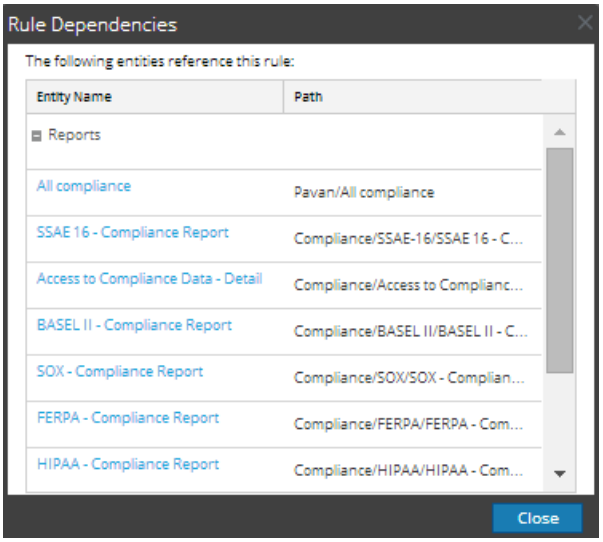
View Dependents of a Rule

You can view dependents of a rule. You must traverse a rule list, select a rule for which you want to identify the dependency over a report, chart, or alert.

The following figure shows the Rule View where you select the rule 'Access to Compliance Data Details'.



The following figure shows the dependency of the rule over alerts and reports.



The following table lists the various columns in the Rule Dependencies dialog and their description.

Column	Description
Entity Name	The name of the entity referencing the rule.
Path	The path where the entity is located in the user interface.

To view dependents of a rule, perform the following:

1. Go to **Reports**.

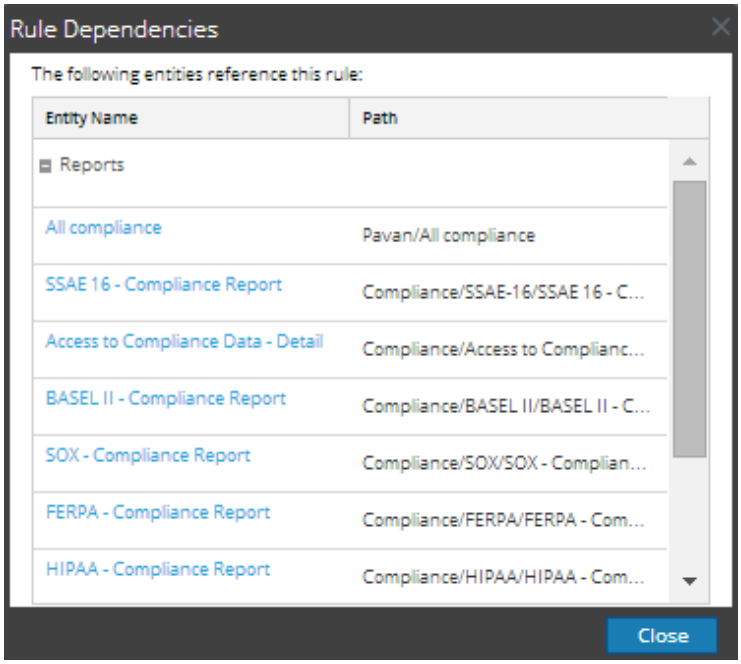
   The Manage tab is displayed.

2. Click **Rules**.

   The Rule view is displayed.

3. In the **Rules** panel, select a rule and in Actions column, click > **Dependents**.

   The Rule Dependencies dialog is displayed.



Export a Rule or Rule Group

Note: Make sure that you have rules in the rule group.

To export a rule, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

   In the **Rules** panel, do one of the following:

   - Select a rule and click > **Export** in the Rule toolbar.
   - Click > **Export**.

2. A browser-specific export dialog may be displayed, allowing you to open or save the file. You can export multiple rules at a time. To select multiple rule, press and hold the CTRL button and select the rules to be exported.

To export a rule group, perform the following :

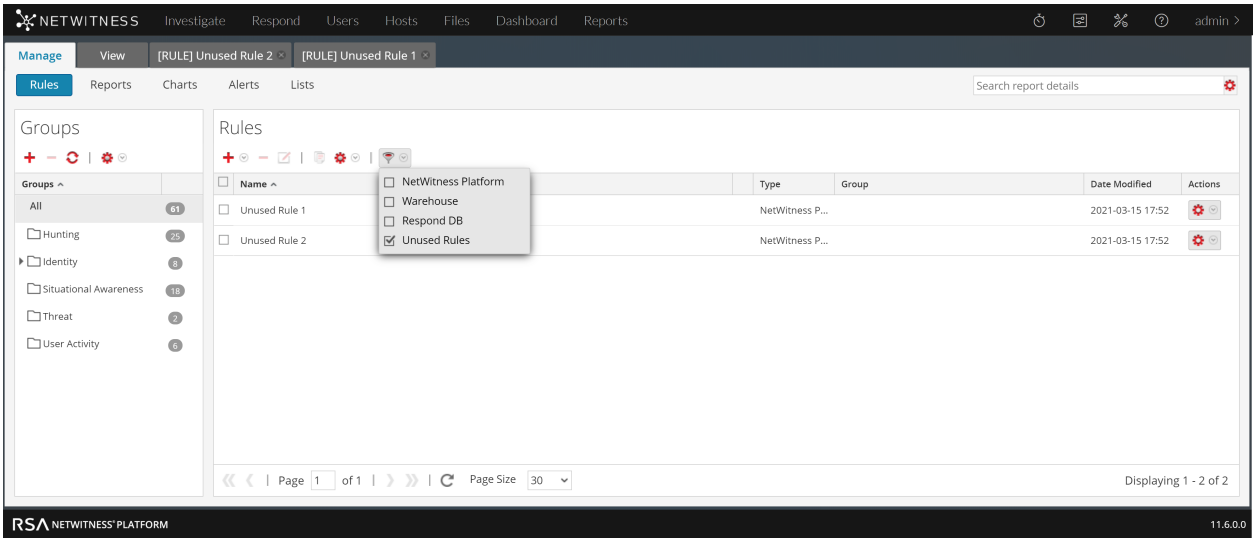
1. Go to **Reports**.
   The Manage tab is displayed.
2. In the **Rules Groups** panel, select the rule group containing the rules which you want to export. You can export multiple rules groups at a time. To select multiple rule groups, press and hold the CTRL button and select the rules groups to be exported.

3. Click  > **Export**.
   A browser-specific export dialog may be displayed allowing you to open or save the file.

Filter Unused Rules

You can filter and delete the rules that are not used by any group in charts, alerts, and reports. To filter unused rules:

1. Go to **Reports**.
   The **Manage** tab is displayed.
2. In the **Rules** panel, click  and select **Unused Rules**.
   List of unused rules is displayed.
3. [Optional] Delete the unused rules.
   For more information, see Delete a Rule or Rule Group.



Manage a Report

You can perform the following procedures to manage a report.

- Access Control for a Report or Report Group
- Delete a Report or Report Group
- Duplicate a Report
- Edit a Report
- Refresh a Report Group or Report List
- Edit a Scheduled Report
- Delete a Scheduled Report

- Export a Report
- Export a Report Group
- Import a Report or Report Group
- Enable or Disable a Scheduled Report
- Start or Stop a Scheduled Report
- View an Execution History of a Scheduled Report
- Manage and Select a Report Logo
- Search Reporting Details

Access Control for a Report or Report Group

This section covers the access permissions the user has depending on the user role to manage a report and report group. The Reporting provides access control at the report and report group level. The user who has the right set of permissions can only perform the tasks in reporting module. The access control is managed by the administrator from the **(Admin) > Security > Roles** tab.

When creating users and user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Reports and Report Groups can be tied to a specific set of user roles so that when a user logs into NetWitness, the reports with the access rights for the specific user role can be viewed. Users that belong to a user role with the ‘Read & Write’ access permission can define reports. Further, the access can be tightened so that reports are accessed only by those who have the ‘Read Only’ access.

Note: You must have ‘Read Only’ permission for a group to view the reports within that group.

At the report level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write
- Read Only
- No Access

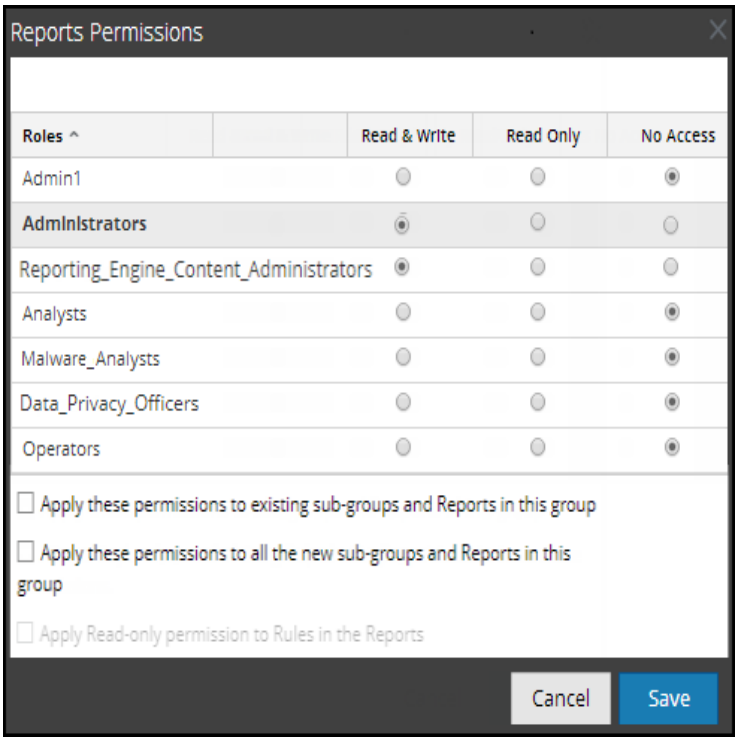
Suppose, you want the NetWitness to have access to all the reports in a Report Group, you can set the permission '**Read & Write**' at the Report Group level. And, if you do not want the **Operator** role to have access to a specific set of reports in a report group, you can set the permission '**No Access**' at the Report Group level.

The permission is set only for the report group but not the reports, rules, or subgroups in the Report Group.

Access Control for a Report Group

When you want to change the report group permissions, you must select a report group and set access permissions using the Reports Permissions panel.

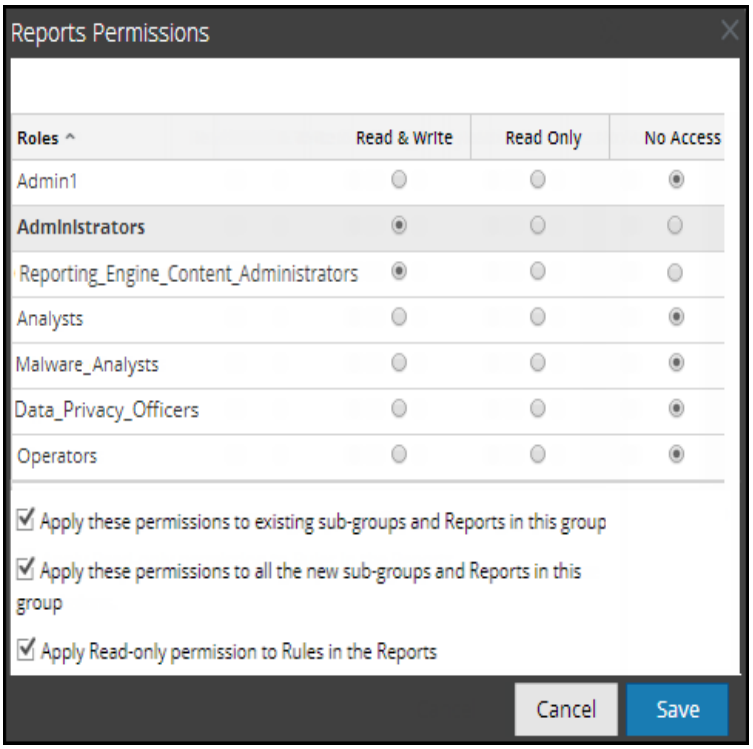
Before applying report group permissions, the default permission set for all the user roles is 'No Access' except for administrators (with full access in Reporting Engine service Config page) and reporting engine content administrators, as shown in the figure.



If you want to change the access permission for a specific user role, you must set these at the report group level, as shown in the figure. <suppose,>Administrators to have access to all the reports in a Report Group, you can set the permission '**Read & Write**' in the Report Group Permissions panel.

You can also apply permissions to existing subgroups and reports in the group, as well as apply read-only permission to rules in the reports by selecting the appropriate checkboxes, as shown in the figure.

You can also apply permissions to all the new subgroups and reports by selecting the appropriate checkbox.



The three scenarios are explained in brief:

- Scenario 1: Permissions applied to Report Group/ Sub Group/ Report based on the user role.
- Scenario 2: Permissions applied to Sub Group and Report in the Group.
- Scenario 3: Read-only permission applied to Rules in the Report.

	Role (Analyst)	Permissions applied to Report Group/ Sub Group/ Report based on the user role	Permissions applied to Sub group and Report in the Group	Permission (Read-only) applied to Rules in the Report
Group	Read & Write	Read & Write	Read & Write	Read & Write
Sub Group	Read	Read	Read & Write - Inherited	Read & Write
Report	Read	Read	Read & Write - Inherited	Read & Write
Rules	Read	Read	Read	Read

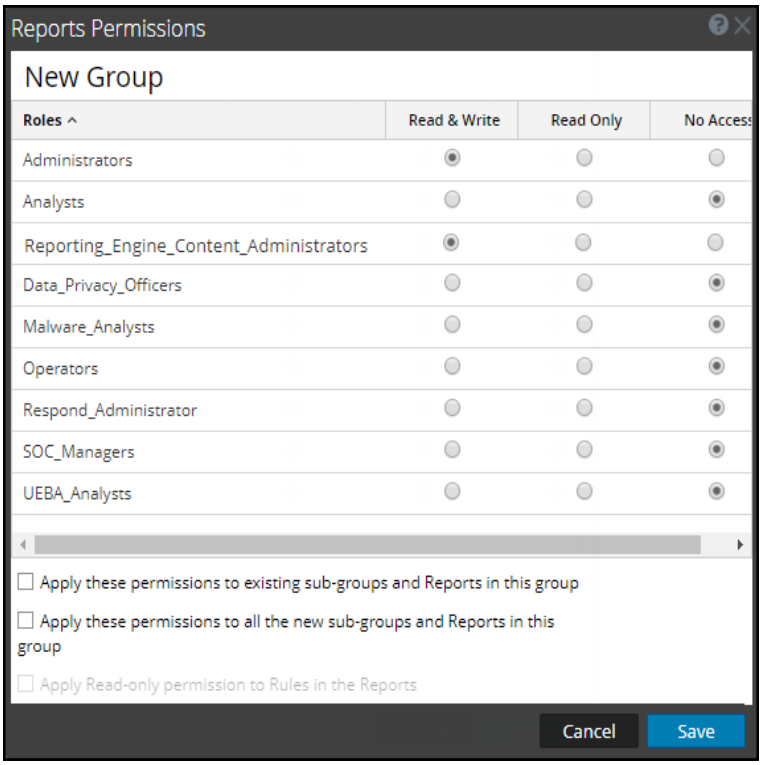
The Report Group will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** report group.

For scenario 1, each of the levels has a permission set depending on the user role. For scenario 2, the permission at the Report Group level (Read & Write) is inherited by the Sub Group and Reports in the Group. For scenario 3, the Read permission is set for the Rules except that the permission set for the rules cannot be higher than the permissions set for the Report Group.

Access Control for a Report

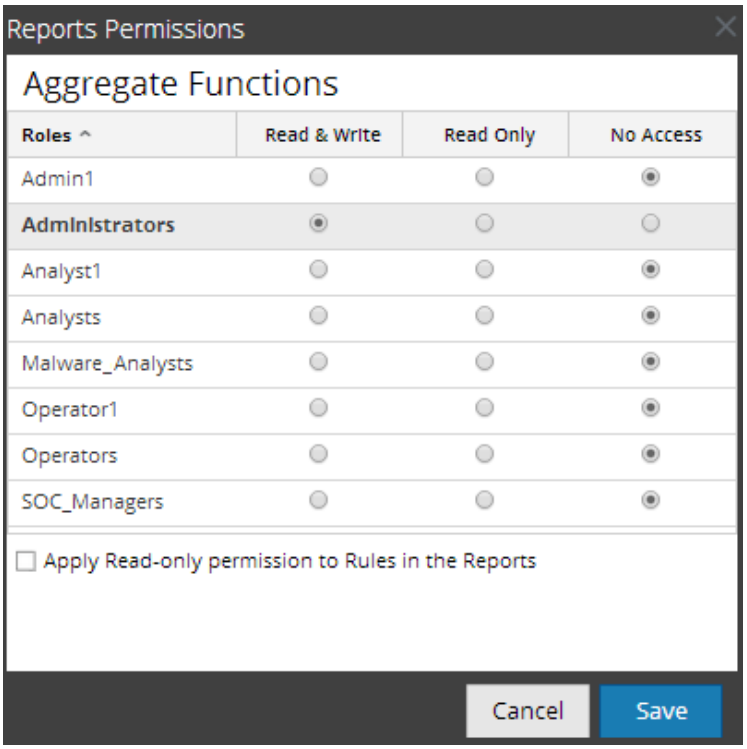
When you want to change the report permissions, you must select a report and set their access permissions using the Report Permissions panel.

Before applying the Report permissions, the default permission set for all the user roles is 'No Access' permission and the checkbox is unchecked, as shown in the figure.



If you want to change the access permission for a specific user role, you must set these at the report level, as shown in the figure. Suppose, you want the **Administrators** to have access to a specific report, you can set the permission '**Read & Write**' in the Report Permissions panel.

You can apply read-only permission to rules in the reports by selecting the checkbox, as shown in the figure.



The two scenarios are explained in brief:

- Scenario 1: Permissions applied to Report Group/ Sub Group/ Report/ Rules.
- Scenario 2: Read-only permission applied to Rules in the Report.

	Role (Analysts)	Permissions applied to Report Group/ Sub Group/ Report/ Rules based on the user role	Permission (Read-only) applied to Rules in the Report
Group	Read & Write	Read & Write	Read & Write
Sub Group	Read	Read	Read & Write
Report	Read	Read	Read & Write
Rules	Read	Read	Read

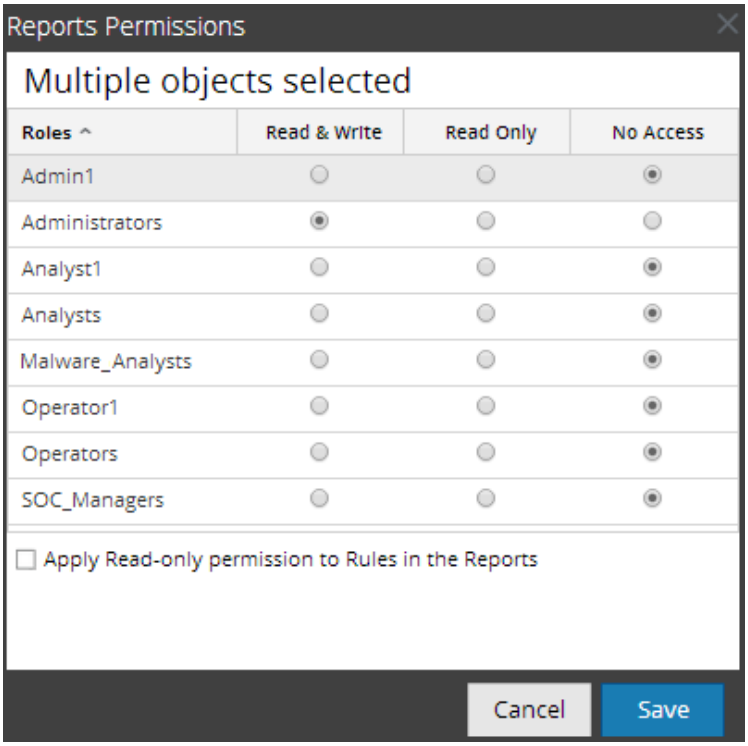
The Report will be assigned the role of a **Security Analyst** and permissions are set to **Read & Write** reports.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the Read permission is set for the Rules except that the permission for the rules cannot be higher than the permission for the Reports.

Note: If the permission for the rules is higher than the permission for the Reports then the permission is be applied only to the reports. For example, if you set the permissions for the Report Group as **No Access** and then specify the option *Apply Read-only permission to Rules in the Reports*, then the read-only permission is not set for the rules.

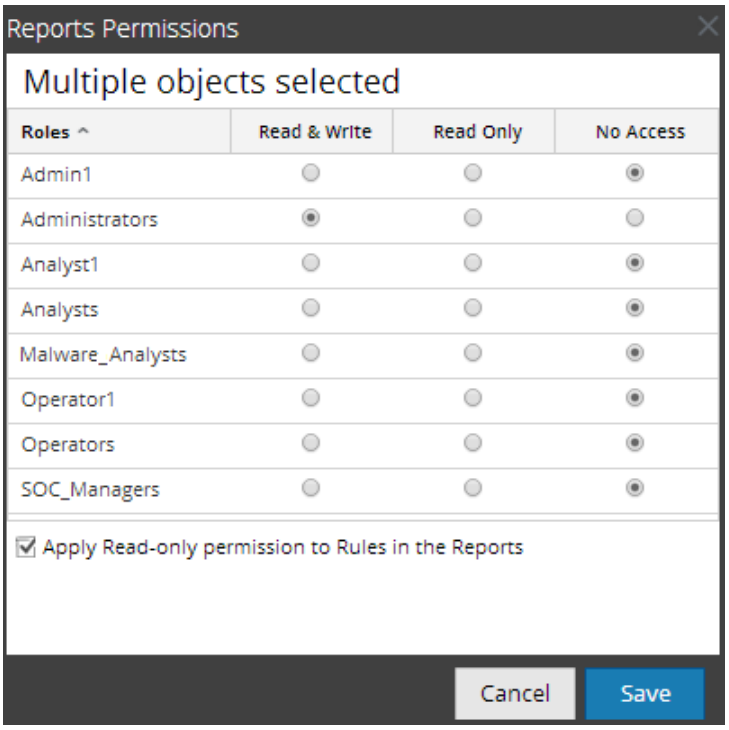
Access Control for a Report When Multiple Reports are Selected

When you want to change permissions of multiple reports, you must select several reports and set their access permissions using the Report Permissions panel. The access permission that you choose is applied to all the selected reports.



Access Control for a Report When Multiple Reports with several rules are Selected

When you want to change permissions when multiple reports with several rules are selected, you must select the checkbox in the Report Permissions panel, as shown in the figure. The read-only access permission is applied to all the rules of the selected reports, provided that the permission of the rules are lower than the permission of the reports.

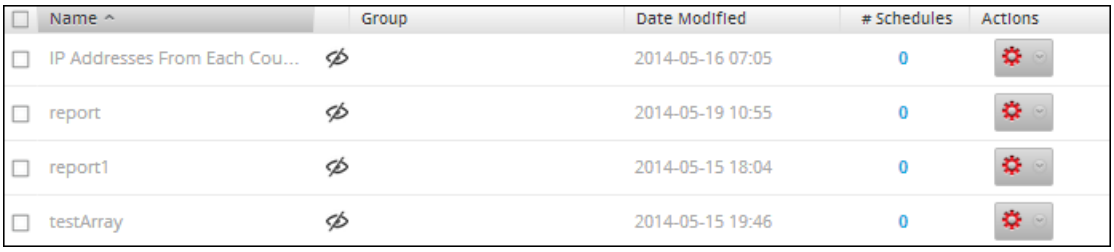


Log in as a Specific User and View the Access Details

When you log in to the NetWitness UI as a user having 'Read access' permission, all the reports is denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Reports panel.

When you log in to the NetWitness UI as a user not having 'Read & Write' access permission on a Report, all the reports are denoted with the symbol (⊘) and the reports appear grayed out on the Reports panel.

The following figure shows the Reports panel when logged in with minimal 'Read & Write' access permission.



Note: If a User (other than the super user) creates a report there will be no access to that report for the super user.

Tabular Listing

The following table lists the various columns in the Reports Permissions Panel:

Column	Description
Roles	The role of the user logged into the NetWitness UI.
Read & Write	The user can access, view, edit, import, export, and delete the report on the Reports view. The user can also change the permission on the report.
Read Only	The user can only access and view the report on the Reports view.
No Access	The user cannot access or view the report for which this permission is set.
Apply these permissions to existing subgroups and Reports in this group	Select the checkbox to apply the selected permissions to the existing subgroups in the group and reports in the group. **Note:** This checkbox is populated only when you set access permissions for a Report Group.
Apply these permissions to all new subgroups and Reports in this group	Select the checkbox to apply the selected permissions to the all new subgroups in the group and reports in the group. **Note:** This checkbox is populated only when you set access permissions for a Report Group.
Apply Read-only permission to Rules in the Reports	Select the checkbox to automatically apply permissions to the rules in the reports.

Set Access Control for a Report

Prerequisites

Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a report.

To set access permissions for a report, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

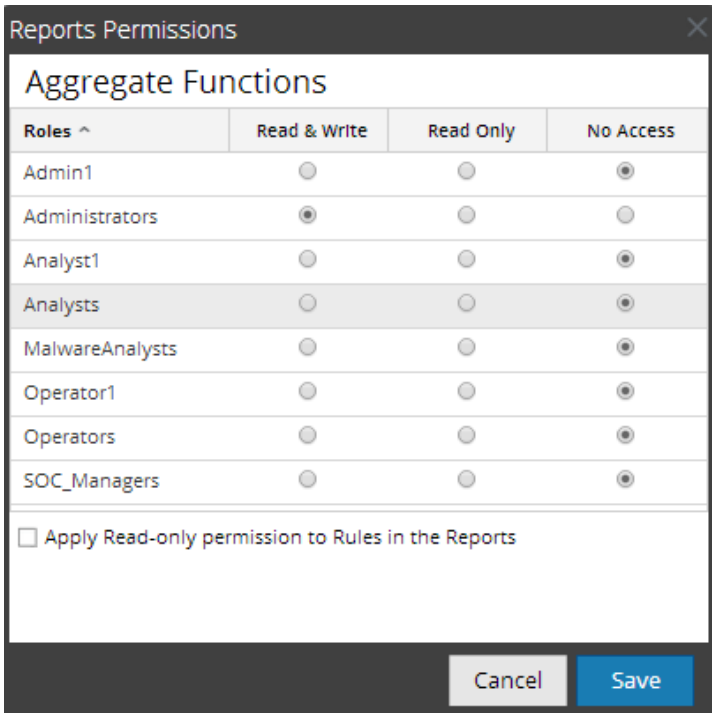
2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, select a report.

4. Click > **Permissions**.

   The Reports Permissions dialog is displayed.



5. Based on the user role, select the appropriate buttons.
6. (Optional) Select the checkbox, if you want to provide read access permission to rules in the reports.

   Note: On selecting the check box, all dependent rules are given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

7. Click **Save**.

   A confirmation message that the permission is set for the selected report is displayed.

Set Access Control for a Report Group

Prerequisites

Make sure that you have a minimal 'Read & Write' access permission to set access permissions for a report group.

To set access permissions for a Report Group, perform the following:

1. Go to **Reports**.

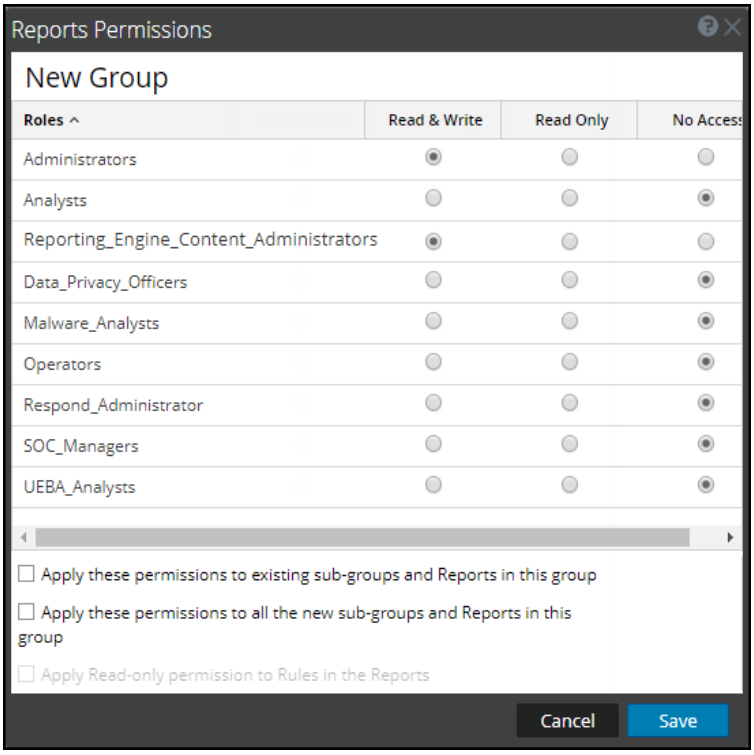
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports Groups** panel, select or right-click on a report group.
4. Click > **Permissions**.

The Reports Permissions dialog box is displayed.



4. Based on the user role, select the appropriate buttons.
5. (Optional) Select the appropriate checkbox to apply the selected permissions to subgroups and reports in the group.
6. (Optional) Select the appropriate checkbox to apply the selected permissions to all the new subgroups and reports in this group.
7. (Optional) Select the appropriate checkbox to provide read access permission to rules in the reports.

   Note: On selecting the check box, all dependent rules is given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

8. Click **Save**.

   A confirmation message that the permission is successfully set for the selected report group is displayed.

Delete a Report or Report Group

To delete reports in a group or subgroup from the Reports panel:

1. Go to **Reports**.

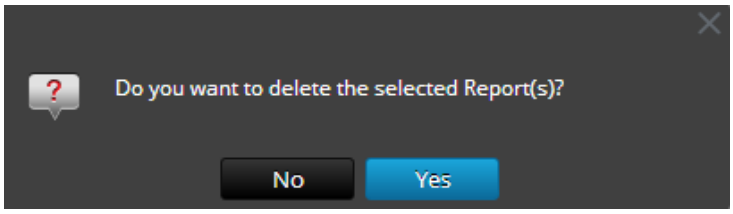
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, do one of the following:
   - Select the reports and click −.
   - Click ⚙ > **Delete**.

     A confirmation dialog is displayed.



4. Click **Yes** to delete the report.

   A confirmation message that the report is deleted successfully is displayed and the selected report is deleted from the Reports panel.

Delete a Report Group

Prerequisites

Make sure that you have no reports associated with the report group.

To delete report groups in the default folder or subgroups under a report group, perform the following:

1. Go to **Reports**.

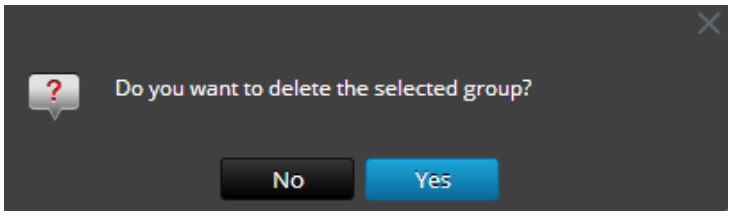
   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports Groups** panel, select the report group and click −.

   A confirmation dialog is displayed.



4. Click **Yes** to delete the group.

   A confirmation message that the group is deleted successfully is displayed and the selected group is deleted from the Report Groups panel.

Duplicate a Report

You can duplicate a report to schedule multiple report for the same report. The duplicated report is displayed in the Reports panel with suffixes. For example, Report (1).

Generally, the duplicate option is used in two scenarios:

- You want to make a copy of the report, to move the same report to another group.
- You want to retain most of the configuration settings for an object but modify few of these settings. For example, when you have a complex query in a rule or several rules in a report, it is very much appropriate to use the duplicate option.

To duplicate an existing report, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, select a report that you want to duplicate and click  .

   The report is saved successfully and added to the Report list.

You can move the duplicated report to another group.

Edit a Report

To edit reports in a group or subgroup from the Reports panel, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. Select a report and in Actions column, click  > **Edit**.
   The Build Report view tab is displayed.

4. Modify the text and add more rules to the report (if required).
5. Click **Save**.

   A confirmation message that the report is saved successfully is displayed.

Refresh a Report Group or Report List

You can refresh a report group or reports to view the re-arrangement of groups or reports.

To refresh a report group or reports, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. Do the following to move the group or reports to a new location:

   - In the **Reports Groups** panel, drag and drop the group.
   - In the **Reports** panel, drag and drop the reports to the desired group in the Report Groups panel.
     The report group or reports are moved to the new location.

4. Do the following to refresh a group or report list:

   - In the **Reports Groups** panel, click  .

     The report group gets refreshed.

   - In the **Reports** panel, click  .

     The Report list gets refreshed.

Edit a Scheduled Report

To edit a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

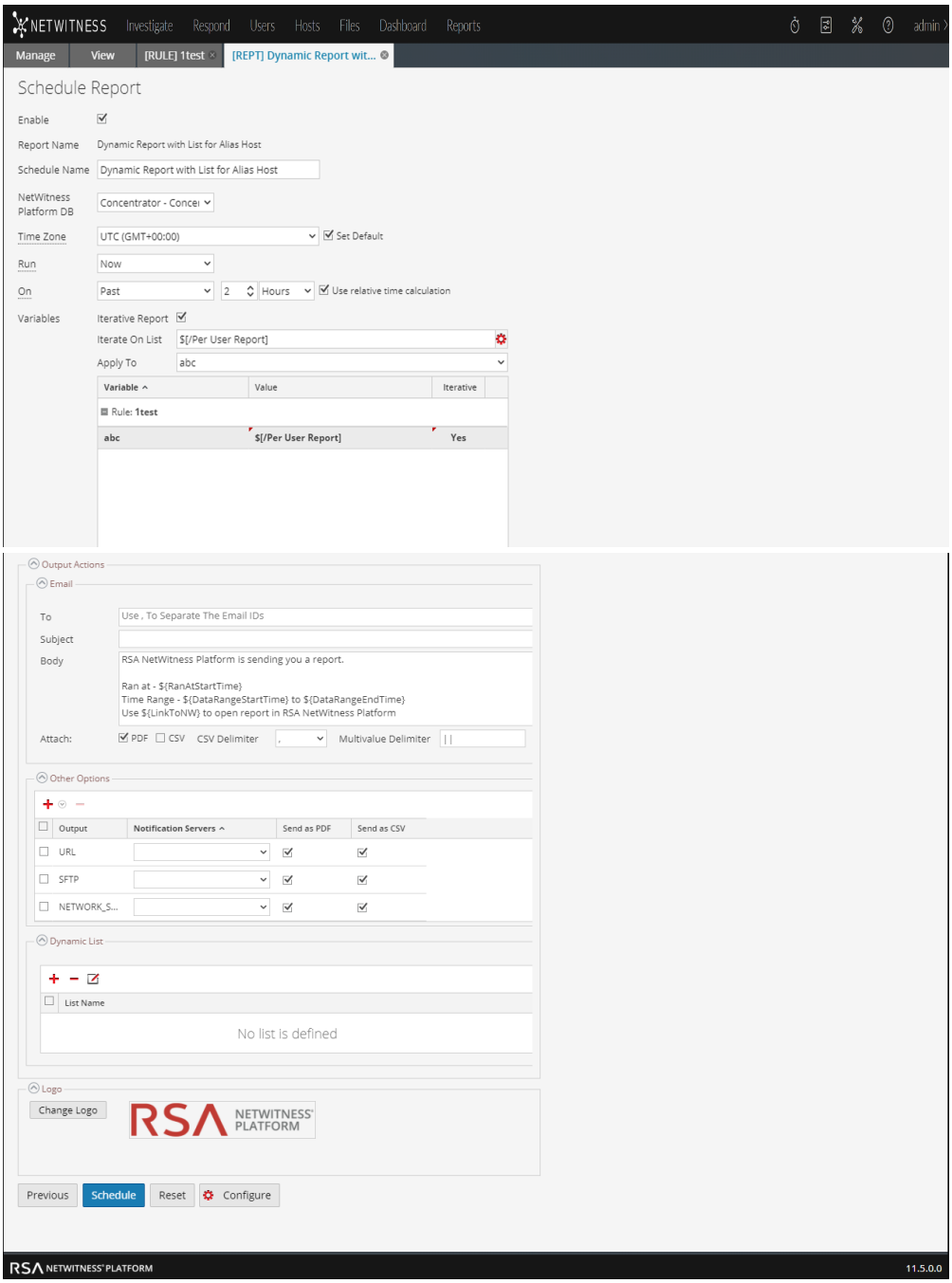
   The Report view is displayed.

3. In the **Reports** panel, select a report and in Actions column, click  > **View Scheduled Reports**.

   The Report Schedule tab is displayed.

4. In the **Report Schedule** panel, do one of the following:

   - Select a report and click  .
   - Select a report and click  > **Edit Schedule**.
     The Schedule Report tab is displayed.



5. In the Schedule Report tab, do the following:

   a. In the **Schedule Name** field, modify the name for the schedule report configuration.

   b. To execute the reports as per the schedule, select the **Enable** checkbox.

   c. From the **Data Source** field, select the datasource.

> **Note:** If the data source is not listed, ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see "Configure Data Source Permissions" topic in the *Reporting Engine Configuration Guide*.

6. (Optional) From the **Warehouse Resource Pool** drop-down, select the pool or queue for the report.

   Note: The **Warehouse Resource Pool** drop- down is displayed only if the Warehouse Rule is selected. If no pools or queues are entered for the Reporting Engine, this field is disabled.

7. From the **Run** field, select the type of run schedule. (For example, Now or Hourly).
8. Select the date range to run the query based on absolute duration or select the **Use relative time duration** checkbox to run the query based on relative duration.
9. (Optional) In the Output Actions panel, do the following:
   a. Type the email address and subject.
   b. Edit the body of the message for the report.
   c. Select the format of the attachment.
   d. Type a value for the CSV and Multivalue delimiters.
10. (Optional) In the Other Options field, do the following:
    a. Click  > **SFTP** or **URL** or **Network Share**. Based on the selected option, a row gets added in the Other options field.
    b. Select the appropriate options to send the report in PDF or CSV format to the configured SFTP, URL or Network Share.
11. (Optional) To add a list in the Dynamic List panel, see Generate a List from the Scheduled Report section in Create and Schedule a Report.
12. (Optional) To choose another logo in the Logo panel, see Manage and Select a Report Logo section.

    Note: If you do not specify a logo, the default RSA logo is used.

13. Click **Schedule**.

    The scheduled report executes as scheduled and provides the configured outputs.

Delete a Scheduled Report

To delete a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

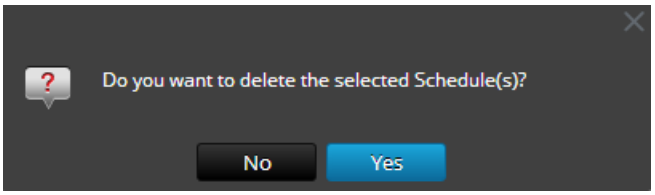
   The Report view is displayed.

3. In the **Reports** toolbar, click **View All Schedules**.

   View Report Schedule is displayed.

4. In the **Report Schedule** panel, select the report.
5. Click  >**Delete Schedule**.

   A confirmation dialog is displayed.



6. Click **Yes** to delete the scheduled report.

   A confirmation message that the scheduled report is deleted successfully is displayed and the selected schedule is deleted from the Scheduled Reports List panel.

Export a Report

You can export the selected reports to an external file that can be later imported to another NetWitness environment.

Prerequisites

Make sure that you have reports in the report group.

To export selected reports in the Report Groups panel to an external file, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

   In the **Reports** panel, do one of the following:

   - Select a report and click  > **Export**.
   - Click  > **Export**.

3. You can export multiple reports at a time. To select multiple reports, check the checkbox of the report to be exported. The exported file is saved to the local drive in an archived format.

Open CSV files with Unicode characters in MS Excel

To open downloaded CSV files containing Unicode characters in MS Excel, follow these steps:

1. Download and save the CSV file.
2. Open Microsoft Excel and navigate to the **Data** tab.
3. Click on **From Text** menu item; find the CSV file that you downloaded and click **Import**.
   The Text Import Wizard is displayed.
4. Select **Delimited** or **Fixed Width** data type from the **Original data type** radio button.
5. Click **File origin** drop down list and select **65001: Unicode (UTF-8)** and click **Next**.
6. Select the delimiter that was used in the file that you imported and click **Next**.
7. Select the data format for each column of data that you want to import and click **Finish**.
   The correct output is displayed in an MS Excel sheet.

Export a Report Group

You can export a selected report groups to an external file that can be later imported to another NetWitness environment.

Prerequisites

Make sure that you have reports in the Report Group.

To export selected report groups in the Report Groups panel to an external file, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports Groups** panel, select a report group and click  and select one of the following:

   - **Export** - This selection exports a report in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple report groups at a time. To select multiple report groups, press and hold the CTRL button and select the report groups to be exported. The exported file is saved to the local drive.

Import a Report or Report Group

You can import a group containing subgroups and reports from other instances of NetWitness into Report Groups panel. Reports must be in a valid binary file that was exported from another NetWitness instance.
During the import process, you select the binary file and specify whether existing reports with the same name must be overwritten or not by the reports contained in the binary import file.

- If you choose to overwrite, all duplicate rules, lists and reports are overwritten by the contents of the binary import file.
- If you choose not to overwrite, and a duplicate rule, list or report exists in the target folder, the import fails and display a message about duplicate reports.

You cannot import reports to a specific report group. The imported files are stored in the **All**root folder.

Prerequisites

Make sure that you have the reports or report groups exported from other instances of NetWitness.

To import groups containing subgroups and reports from other instances of NetWitness into Report Groups panel, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

The Report view is displayed.

3. In the **Reports Groups** panel, select a folder to import the file.
4. Do one of the following:
   - In the **Reports Groups** toolbar, click > **Import** to import a group.
   - In the **Reports** toolbar, click > **Import** to import a report.
     The Import Report dialog is displayed. You can import multiple reports and report groups at a time. To select multiple reports or report groups, press and hold the CTRL button and select the reports or report groups to be imported.
5. Click **Browse** to select the binary file.

   NetWitnessprovides a file system view of the files.
6. Locate the binary file and click **Open**.

   The file gets added to the Import Report list.
7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, check the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, check the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing report in the library with an identically named report in the binary file when importing, check the **Report** checkbox. If you do not select the Overwrite option, and an identical report is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Enable or Disable a Scheduled Report

To enable or disable a scheduled report from the Scheduled Reports List panel, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, select a report and click > **View Scheduled Reports**.
   View Report Schedule is displayed.
4. Select a report from the Report Schedule panel.
5. In the Actions column, click > **Enable**.
   The state of the report is changed to ‘Running’, if the report is scheduled to run immediately.

6. In the Actions column, click  > **Disable**.
   The state of the report is changed to 'Inactive'.

Start or Stop a Scheduled Report

To start or stop a scheduled report, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, select a report and click  > **View Scheduled Reports**.
   The Report Schedule view is displayed.
4. Select a report from the Scheduled Reports List panel.
5. In the Actions column, click  > **Start**.
   The state of the report is changed to 'Running', if the report is scheduled to run immediately.
6. In the Actions column, click  > **Stop**.
   The state of the report is changed to 'Completed'.

Note: If you have multiple executions running for a scheduled report and the state of the report is in Queued state, the STOP option is disabled till all the previous executions are completed and last execution is in running state. To stop the individual execution of a particular schedule, refer to Stop an Individual Execution of a Scheduled Report.

View an Execution History of a Scheduled Report

You can view the execution history of a scheduled report. You can view the history of a scheduled report that is run. You can view the history based on the following criteria:

- Number of past schedules executed
- Start date and end date for the date range

You can view the details such as how many times the scheduled report was executed, the time of execution (seconds), execution state. You can also view the report generated on a full screen.

To view the execution history of a scheduled report, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.

3. In the **Reports** panel, do one of the following:
   - Click  > **View Scheduled Reports**.
   - Click the **#Schedules** column.
     The Schedule Reports view tab is displayed with the status of each of the scheduled report.
4. Do one of the following:
   - Select a scheduled report and click  > **Execution History**.
   - Select a scheduled report and click  .
     The Execution History view is displayed.

   Note: By default, you can view 10 number of execution history of a scheduled report. The execution history shown depends on the Retain Report History Configuration set on the **General**tab of the  **(Admin) > Services > Reporting Engine Config** view.
   For example, if you set the Retain Report History Configuration to 100 days, the data displayed on the Execution History view. is the past 100 days execution history details considering the current date information.
5. From the **Get history by:** field, select the type of history to be fetched. (For example, Past or Range (Specific))
6. In the **Count** field, enter the number of executions to be displayed.
7. Click **Show History**.
   The execution history of the scheduled report is displayed.

Stop an Individual Execution of a Scheduled Report

If you have multiple executions running for a scheduled report, you can stop the individual execution of the scheduled report in **Execution History** panel.

To stop the individual execution of a scheduled report, perform the following:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, do one of the following:
   - Click  > **View Scheduled Reports**.
   - Click the **#Schedules** column.
     The Schedule Reports view tab is displayed with the status of each of the scheduled report.
4. Do one of the following:
   - Select a scheduled report and click  > **Execution History**.
   - Select a scheduled report and click  .
     The Execution History panel is displayed.

5. Select a schedule, in the **Actions** column, click .
   The state of the execution schedule is changed to 'Cancelled'.

Manage and Select a Report Logo

Prerequisites

Make sure that you have the Reporting Engine service defined prior to managing a logo.

Manage Report Logos

To manage logos, perform the following:

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. In the **Services** panel, select an Reporting Engine service and click **View** > **Config**.
   The services config view is displayed.
3. Select the **Manage Logos** tab.
   All the available logos are displayed.

Add a Logo

To add a logo, perform the following:

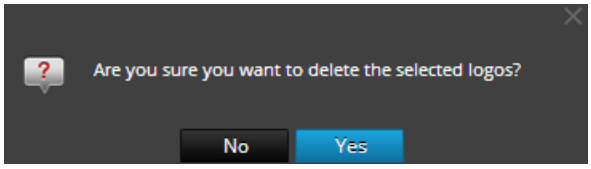
1. In the **Manage Logos** tab, click .
   A file browser opens where you can choose the file from the local drive.
2. Select the logo and click **Open**.
   The selected logo gets added to the Manage Logos section.

Delete a Logo

To delete a logo, perform the following:

1. In the **Manage Logos** tab, do one of the following:
   - Select the logo and click .
   - Perform (Ctrl+click) to select multiple logos and click .

   A confirmation dialog is displayed.



2. If you want to delete the logo, click **Yes**.
   The selected logo is deleted from the Manage Logos section.

Set Default Logo

To set a default logo, perform the following:

In the **Manage Logos** tab, select a logo and click Set default.
The chosen logo is set as the default logo for the RE service.

Select a Logo

To select a logo, perform the following:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, select a report.

4. Click > **View Scheduled Reports**.
   The View scheduled reports view tab is displayed.

5. Select a scheduled report and in Actions column, click > **Edit Schedule**.

   The Schedule Report view tab is displayed.

6. In the Logo panel, click **Change Logo**.

   The Change a Logo dialog box is displayed.

7. Do one of the following:

   - Click **Upload new logo** to upload another logo.
   - Select a logo from the list.

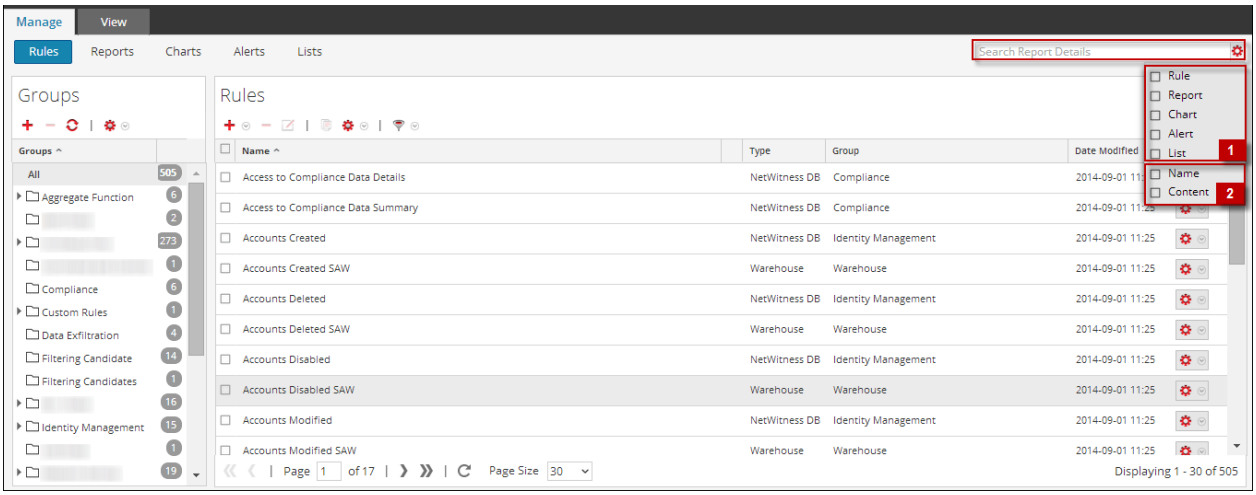
8. Click **Select**.
   The selected logo is available on the Logo panel.

Search Reporting Details

This section provides instructions on how to perform a keyword search on name and content for each of the Reporting components. You can perform a keyword search on name and content for each of the Reporting components (Rule/Report/Chart/Alert/List) on the Reporting UI.

Note: You cannot search based on date and numeric values.

The following figure shows the search parameters available in the Reporting Module:



The following are the search parameters available on the Reporting UI:

1. Search for entities (rule, report, chart, alert, list).
2. Search for the entities based on either the name or content.

Note: Searches are case insensitive. For example, Completed is equivalent to completed.

Prerequisites

In the Reporting Module, you can perform a keyword search based on the name and content (definition). In this context, content implies definition of each of the reporting components. For instance, the value defined in the rule, report, report schedule, chart, and alert panel. You can also prioritize your search by selecting either or all of the components: Rule, Report, Chart, Alert, or List.

Note: You cannot search based on the List values and list path stored in schedule definition panel.

For example, to search for the rule name (ExpertRule), you must select **Rule, Name, and Content** in the **filtering options** drop-down to view all the rule names that matched the search. You can similarly search for a report, chart, alert, or list definition.

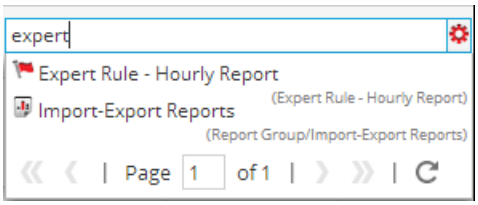
To search for reporting details from the Manage tab, perform the following:

1. Go to **Reports**.

   The **Manage** tab is displayed.

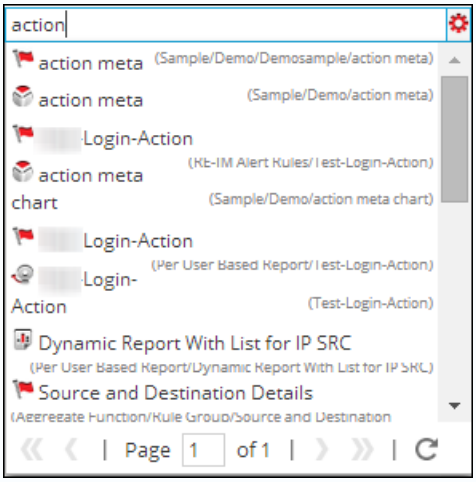
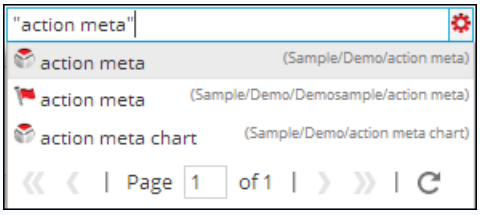
2. Click  and select the appropriate criteria to search.
3. In the **Search** field, enter the text to be searched.

   The search drop-down list is displayed:

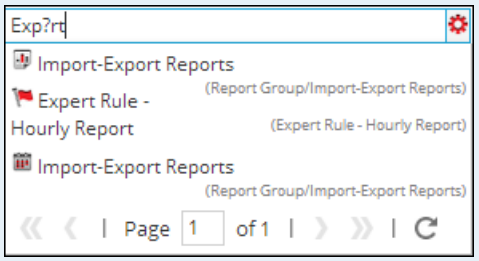
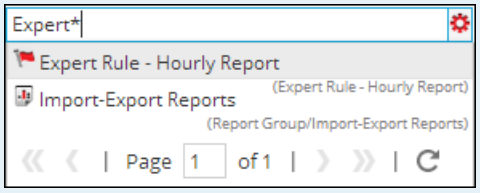
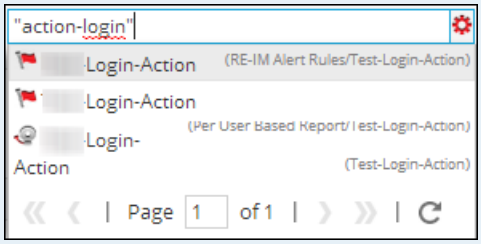


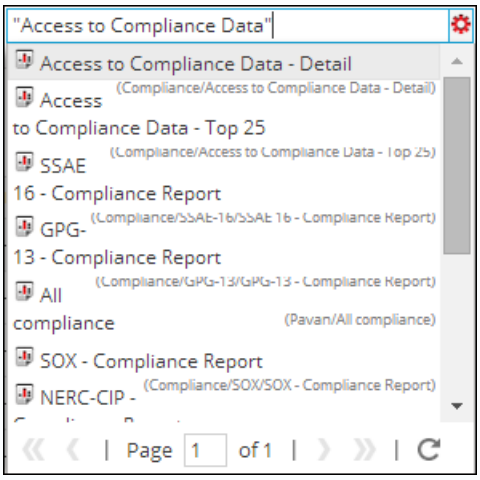
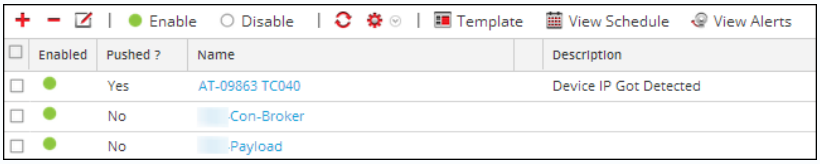
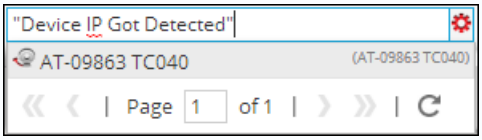
Search Syntax and Different Types of Search

The following table explains the search syntax and the possible searches that can be performed on the Reporting user interface.

Search Types	Description
Word or phrase based search	**Word Based Search:** To search for a word such as "action" or "meta", you must enter the word in the search box. The following figure shows the search results for the text **action**.  **Phrase based search:** A Phrase is a group of words surrounded by double quotes such as "action meta". To search for a phrase, you must enclose phrases in double-quotes in the search box. The following figure shows the search results for the phrase "action meta". 

Search Types	Description

Wildcard Search (Single/ Multiple/ Special Character Search)
 	
The question mark "**?**" symbol is used to perform a single character wild card search and asterisk "*" symbol is used to perform multiple character wildcard search.
	Single character search:
	The single character wildcard search looks for terms that match with the single character replaced. For example, to search for "Expert" or "Export" you can use the search syntax:
	`Exp?rt`
	The following figure shows the search results for the wildcard character **Exp?rt**.
	 
	Multiple character search:
	Multiple character wildcard search looks for 0 or more characters. For example, to search for Expert, or Experts, you can use the search syntax:
	`Expert*`
	The following figure shows the search results for the wildcard multiple character **Expert***.
	 
	Special character search:
	Certain punctuation and special characters are ignored during search (@#$%^&*(){}"~=+-[]\?|!:,.). For example, a search for action-login will be interpreted during search as "action" "login", that is, if rules exist with name "action-login" and "action@login" and search string is "action-login", the search result will return both the rules.
	 

Search Types	Description
Search based on name or content	**Search based on name:** When you want to search based on the name of a report, select **Report**and **Name**box from the filtering options drop-down. For example, to search for the report name "Report With Multiple Rules", you can use the search syntax: "Access to Compliance Data" **Note:** When you search for a report, it implies you can search for the report schedules as well. The search result will return the report containing the specific name.  **Search based on content:** When you want to search for the content within an alert, say alert description, select **Alert** and **Content** box from the filtering options drop-down. For example, to search for the alert description "Device IP Got Detected", you can use the search syntax: "Device IP Got Detected"  The search will return the result having the specific content. 

Working with Charts

The Reporting module user interface provides access to NetWitness charts. The following topics discuss charts:

- Configure and Generate a Chart
- Configure a Chart
- Schedule a Chart
- View a Chart
- Test a Chart
- Investigate a Chart
- Manage a Chart Group and Chart

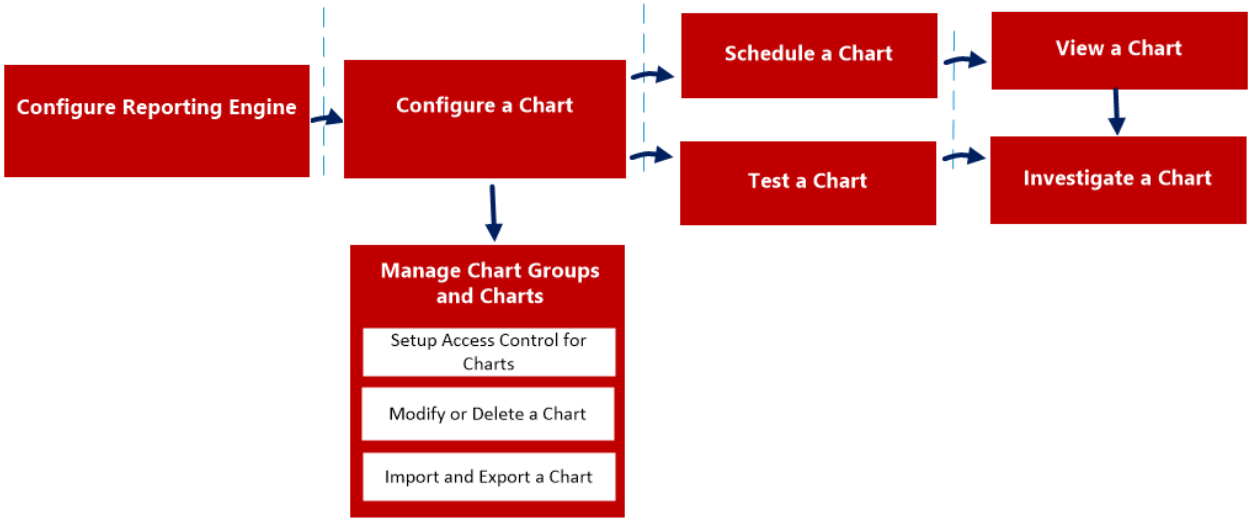
Configure and Generate a Chart

Chart is a graphical visualization of data. You can view different kinds of charts, including multiple types of plot, line, bar, and area charts.

Any NWDB rule in the Reporting Engine system which is not sorted by none can be used to instantly create a chart. For more information on "How to create an NWDB rule", see Configure a Rule.

The chart interval can be adjusted from the chart definition panel itself. Every time a chart is executed, it stores its result data locally in the Reporting Engine, so that it can be reviewed in either the Dashboard View or Chart View without any performance considerations.

The following is an overview of the entire process of configuring and generating a chart.



To configure and generate a chart, perform the following:

1. Configure Reporting Engine
2. Configure an NWDB rule
3. Configure a Chart

4. Schedule a Chart
5. View a Chart
6. Test a Chart
7. Investigate a Chart
8. Manage a Chart Group and Chart

Configure Reporting Engine

You must configure the Reporting Engine before you can configure and generate a chart. You must also specify the data source in the Reporting Engine from which the data is extracted. For more information on how to configure a Reporting Engine, see "Configure Reporting Engine" topic in *Reporting Engine Configuration Guide*.

Configure an NWDB Rule

The NetWitness rule which is not sorted by none is used to create a chart. The NetWitness database extracts the meta from the Reporting Engine and provides the meta for rules. These rules are an essential building block in managing a chart.

Note: If the rule contains the lookup_and_add, sum_count, or sum_values rule actions, the associated chart will not contain data. Do not use lookup_and_add function in a rule to create a chart or a report in a chart format as the output of the lookup_and_add function in a rule will not be displayed on the chart and may result in graphical representation of incorrect information. Also, the PDF for that chart created may show an empty chart or incorrect representation of data.

Configure a Chart

You can configure a chart using the NWDB rules.

Schedule a Chart

After a chart is defined with the required components, you can configure its execution properties by scheduling a chart. Here, you can quickly view, add, and edit the schedule details for a chart.

View a Chart

You can view the scheduled charts in the Chart View.

Test a Chart

You can run the test on a chart and view all the chart details based on the selected time range.

Access Control for a Chart

The Reporting Module provides access control at the chart level. Only a user who has the right set of permissions can perform the tasks in Reporting module. The access control is managed by the administrator from the  **(Admin) > Security > Roles** tab.

When you create users and user roles, ensure that the roles that you create for specific tasks have access to all the necessary permissions. This could require permissions at several levels of the role hierarchy.

Charts can be tied to a specific set of user roles so that when a user logs in NetWitness, the charts with the access rights for the specific user role can be viewed. Users that belong to a user role with the 'Read & Write' access permission can define charts. Further, the access can be tightened so that charts are accessed only by those who have the 'Read Only' access.

At the chart level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write
- Read Only
- No Access

To change the access permission for a specific user role, you must set the permission at the chart level. For example, for **Administrators** to have access to a specific chart, you could set the permission 'Read & Write' in the Charts Permissions dialog.

You can apply read-only permission to rules in the charts by selecting the checkbox.

Two scenarios that describe how to set access control are explained here:

- Scenario 1: Permissions applied to Chart Group/ Subgroup/ Chart/ Rules based on the user role.
- Scenario 2: Read-only permission applied to Rules in the Chart.

	Role (Analyst)	Permissions applied to chart group, subgroup, chart or rules based on the user role	Permissions (Read-only) applied to rules in the chart
Group	Read & Write	Read & Write	Read & Write
Subgroup	Read	Read	Read & Write
Chart	Read	Read	Read & Write
Rules	Read	Read	Read

The chart is assigned the role of a **Security Analyst** and permissions are set to 'Read & Write' charts.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the Read permission is set for the rules except that the permission for the rules cannot be higher than the permission for the charts.

Note: If the permission for the rules is higher than the permission for the chart, the permission is not applied. For example, if you set the permissions for the Report Group as **No Access** and specify the option *Apply Read-only permission to Rules in the Reports*, the read-only permission is not set for the rules.

Access Control for a Chart When Multiple Charts are Selected

To change permissions for multiple charts, you must select several charts and set their access permissions using the Charts Permissions panel. The access permission that you choose is applied to all the selected charts.

Access Control for a Chart When Multiple Charts with Several Rules are Selected

To change access permissions for a specific user role when multiple charts with several rules are selected, select the checkbox in the Charts Permissions panel.

The read-only access permission is applied to all the rules of the selected charts, provided that the permission of the rules are lower than the permission of the charts.

Note: If a user (other than the super user) creates a chart, the super user cannot access that chart.

Access Control for a Chart Group

To change chart group permissions, select a chart group and set the access permissions using the Charts Permissions panel. Before chart group permissions are applied, the default permission set for all the user roles is 'No Access'.

To change the access permission for a specific user role, set the permission at the chart group level. For example, for administrators to have access to all the charts in a Chart Group, set the permission 'Read & Write' in the Charts Group Permissions panel.

You can also apply permissions to subgroups and charts in the group, and apply read-only permission to rules in the charts by selecting the appropriate checkboxes.

Three scenarios that describe how to set access control are explained here:

- Scenario 1: Permissions applied to chart groups, subgroups, or charts based on user roles.
- Scenario 2: Permissions applied to subgroups and charts in the group.
- Scenario 3: Read-only permission applied to rules in the chart.

	Role (Analyst)	Permissions applied to chart groups, subgroups, or charts based on user roles	Permissions applied to subgroups and charts in the group	Permissions (Read-only) applied to rules in the chart
Group	Read & Write	Read & Write	Read & Write	Read & Write
Subgroup	Read	Read	Read & Write - Inherited	Read & Write
Chart	Read	Read	Read & Write - Inherited	Read & Write
Rules	Read	Read	Read	Read

The chart group is assigned the role of a **Security Analyst** and permissions are set to 'Read & Write'.

For scenario 1, each of the levels will have a permission set depending on the user role.

For scenario 2, the permission at the chart group level will be inherited by the subgroup and by charts in the group.

For scenario 3, the Read permission is set for the rules. However, the permission set for the rules cannot be higher than the permissions set for the chart group.

The following table lists the columns in the Charts Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness UI.
Read & Write	The user can access, view, edit, import, export, and delete the chart in the Charts view. The user can also change the permission for the chart.
Read Only	The user can only access and view charts on the Charts view.
No Access	The user cannot access or view charts for which this permission is set.
☐ Apply these permissions to existing sub-groups and Charts in this group	Select the checkbox to apply the selected permissions to the existing subgroups in the group and charts in the group. **Note:** This checkbox is populated only when you set access permissions for a Chart Group.
☐ Apply these permissions to all new sub-groups and Charts in this group	Select the checkbox to apply the selected permissions to the new subgroups in the group and charts in the group. **Note:** This checkbox is populated only when you set access permissions for a Chart Group.
☐ Apply Read-only permission to Rules in the Charts	Select the checkbox to automatically apply permissions to the rules in the charts.

Configure a Chart

After a chart is defined with the NetWitness rules with NWDB as the data source, you can configure its execution properties.

Create a Chart Group

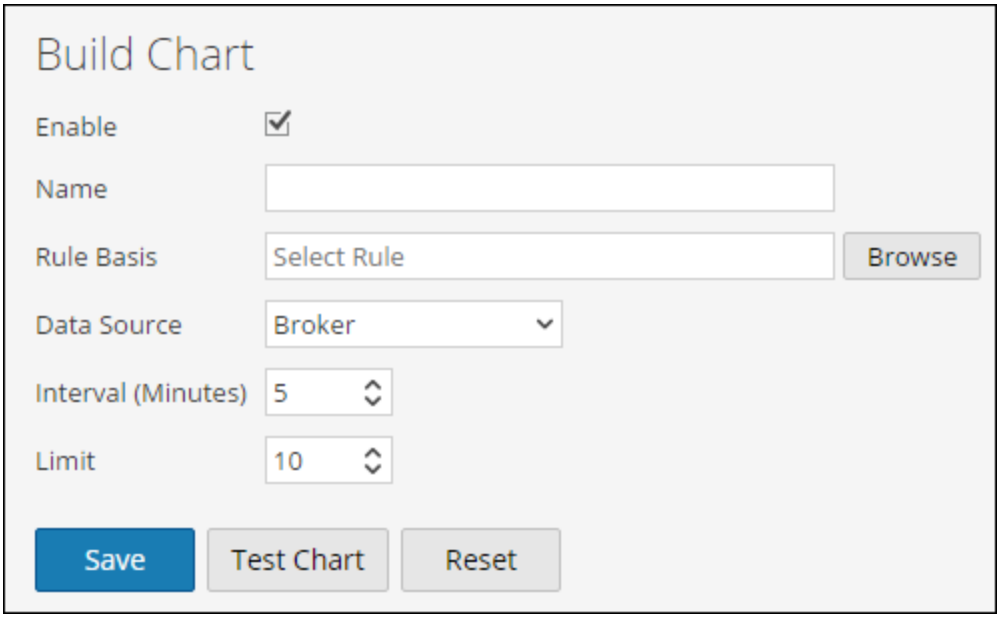
To add groups to the default folder or to add subgroups under a chart group:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Charts Groups** panel, click  .
   A default group is added in the Chart Groups panel.
4. Enter the name of the new group.
5. Press **Enter**.
   The group is added to the Chart Groups panel.

Create a Chart

To add charts to a group or subgroup:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Charts** to display the Chart view.
3. In the **Charts** toolbar, click  .
   The Build Chart tab is displayed.



4. Enter the name of the chart.
5. For the Reporting Engine to collect the data and generate chart results, select the **Enable** checkbox.
6. In the Rule Basis field, do the following:
   a. Click **Browse**. The Add Rule dialog box is displayed.
   b. Navigate the Rule tree and select a rule.
   c. Click **Select**.
7. The Rule appears in the **Rule Basis** field.
8. Select the data source from the **Data Source** drop-down list.

   Note: If the default data source is configured in the Reporting Engine, then the data source is displayed by default on the Build Chart page. If the data source is not displayed, ensure you have Read permissions set for the data source. This is applicable for NWDB and Warehouse data sources. For more information, see the "Configure Data Source Permissions" topic in the *Host and Services Configuration Guide*.

9. (Optional) To modify the Interval value, click the up or down arrow.
   The Interval value is the interval in minutes at which the rule which forms the basis of the chart is

run to collect data.

10. Select the **Limit** value to limit the number of records to be displayed.
11. **X-Axis** and **Y-Axis** are used to specify the meta to be plotted in charts.
    In the **X-Axis**, the meta for the 'Group by' rule is displayed. In the **Y-Axis**, the aggregate functions used in the rule are displayed.

    Note: Sum, Count, Countdistinct and Average are the supported aggregate functions for chart. By default, for Custom Rules with multiple 'Group by', you can select only the first meta in **X-Axis**.
12. Click **Save**.
    A confirmation message that the chart is saved successfully is displayed.

Schedule a Chart

You must schedule a chart to further investigate on the chart details.

By enabling a chart, the chart executes as scheduled and provides the configured output with the state of the chart changed to ‘Scheduled’.

To schedule a chart:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Charts** panel, select a chart or several charts that display ○ in the **Enabled** column.
4. Click  .
   A confirmation message indicates that the chart(s) state is changed successfully.

View a Chart

After you view a chart, you can perform the tasks:

- You can print, save, email and view charts on full screen.
- You can also select a date from the calendar to view a list of successfully run charts for the chosen date.

To view a chart:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, Select a chart and click  > **View**.

   The View Chart view tab is displayed.

4. In **Chart Options**, do the following:

   a. Select the **Time Range**.

   > **Note:** When you select the Time Range option, you can select a pre-set time range such as last hour, last 3 hours and the Last N Days...or you can customize the selection by choosing Last N Days or Custom. If you select Last N Days option, you can view the historical data for a maximum of 15 days. If you select the Custom option, you can select a start date and end date to view the data for the selected date range.

   b. Select the **Series**, either **Chart Values over Time** or **Chart with Totals**.
   When you select **Chart Values over Time**, the chart displays the change in values for the selected time. When you select **Chart with Totals**, the chart displays a total for each aggregate value for the selected time.

   c. Select **Items To Plot** to define the number of events to view on the chart.

   d. From the **Chart Type** drop-down list, select the chart type.

   e. Click **Reload** to reload the selected chart.
   If there is a delay in retrieving the historical data for the selected time range, a message is displayed.

After the chart is generated, a notification is displayed in the notification tray available in the NetWitness toolbar. For more information on the NetWitness toolbar, see the "Browser Window" topic in the *NetWitness Getting Started Guide*.

View all Charts List

To view a list of all the charts:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** toolbar, click **View All Charts**.

   All the executed charts for the selected date are displayed in a new tab.

   > **Note:**
   > * If no list is displayed, you can select a date from the calendar to view a list of charts.
   > * If you want to view a specific chart, enter the chart name in the search criteria.

4. Click the chart name to view the chart details for that date.

Test a Chart

You can test a chart in the **Test a Chart** view.

To test a chart:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. Do one of the following:

   - In the **Charts** toolbar, click  .
   - In the **Charts** panel, double-click a chart or select a chart and click  .
   - In the **Charts** panel, select a chart and in Actions column, click  > **Edit**.

   The Build Chart view tab is displayed.

4. Click **Test Chart** to view the chart.

   The View Chart view tab is displayed.

5. In the **Time Range** drop-down, select the hours range.
6. Select the **Series**, either **Chart Values over Time** or **Chart with Totals**.
7. In the **Items To Plot** field, select the number of items to plot.
8. From the **Chart Type** drop-down list, select the chart type.
9. Click **Run Test** to run the test.

The chart data (if any) for the selected time range is displayed.

Investigate a Chart

You can investigate the chart by navigating directly to the Investigation module from the chart.

To investigate a chart:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** toolbar, click **View All Charts**.

   All the executed charts for the selected date from the **Chart Options** panel are displayed on a new tab.

4. Double-click the chart name to view the chart details such as the time at which the chart is executed and the default data source used for the chart execution.
5. Do one of the following:

- Click a data point on the chart to investigate.
- In the toolbar, click **Investigate** to investigate for the entire time range.

Manage a Chart Group and Chart

You can manage chart groups and charts using the following procedures.

Manage a Chart Group

Depending on the access permissions set for the user role, you can modify or delete, import or export, drag and drop a chart, or refresh a chart group.

Modify a Chart Group

To modify a chart group in the default folder or subgroups under a chart group:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts Groups** panel, select the chart group to modify.

The selected chart group is modified and can be viewed on the **Charts Groups** panel.

Delete a Chart Group

To delete a chart group in the default folder or subgroups under a chart group:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts Groups** panel, select the group and click −.

   A confirmation dialog asks for confirmation that you want to delete the selected group.

4. Click **Yes** to delete the group.

The selected group is deleted from the Chart Groups panel.

Import a Chart Group

To import chart groups from other instances of NetWitness:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. From the **Charts Groups** panel, select a folder to import the file.
4. Do one of the following:

   - In the Chart Groups panel, click  > **Import**.

     The **Import Chart** dialog box is displayed.

   - You can import multiple chart groups at the same time. To select multiple chart groups, press and hold the CTRL button and select the chart groups to be imported.

5. Click **Browse** to select the binary file.

   NetWitness provides a file system view of the files.

6. Locate the binary file and click **Open**.

   The file is added to the Import Chart list.

7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, select the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, select the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing chart in the library with an identically named chart in the binary file when importing, select the **Chart** checkbox. If you do not select the Overwrite option and an identical chart is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Export a Chart Group

To export selected chart groups:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts Groups** panel, select a chart group and click  and do one of the following:

   - **Export** - This selection exports a chart in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple chart groups at the same time. To select multiple chart groups, press and hold the CTRL button and select the chart groups to be exported. The exported file is saved to the local drive.

Drag and Drop Chart to a Group

To drag and drop a chart from the Charts panel to a group in the Charts Groups panel:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. Select a chart from the **Chart** panel and drag and drop the chart to a group in the **Chart Groups** panel.

The chart is copied to the group in the Chart Groups panel.

Refresh a Chart Group

To refresh chart groups:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts Groups** panel, drag and drop the group.

   The chart group is moved to the new location.

4. In the **Charts Groups** panel, Click  .

The chart group is refreshed.

Manage a Chart

Depending on the access permissions set for the user role, you can modify or delete, duplicate, import and export, enable or disable charts, search for existing charts, and refresh a chart list.

Access Control for a Chart

To set access permissions for a chart:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, select a chart.

4. Click  > **Permissions**.

   The Charts Permissions dialog box is displayed.

5. Based on the user role, select the appropriate buttons.

6. (Optional) Select the checkbox if you want to provide read access permission to dependent rules.

   Note: On selecting the check box, all dependent rules with No access permission are granted a READ access permission.

7. Click **Save**.

A confirmation message that the permission is successfully set for the selected chart is displayed.

Modify a Chart

To modify a chart in a group or subgroup:

1. Go to **Reports**.

   The Manage tab is displayed.

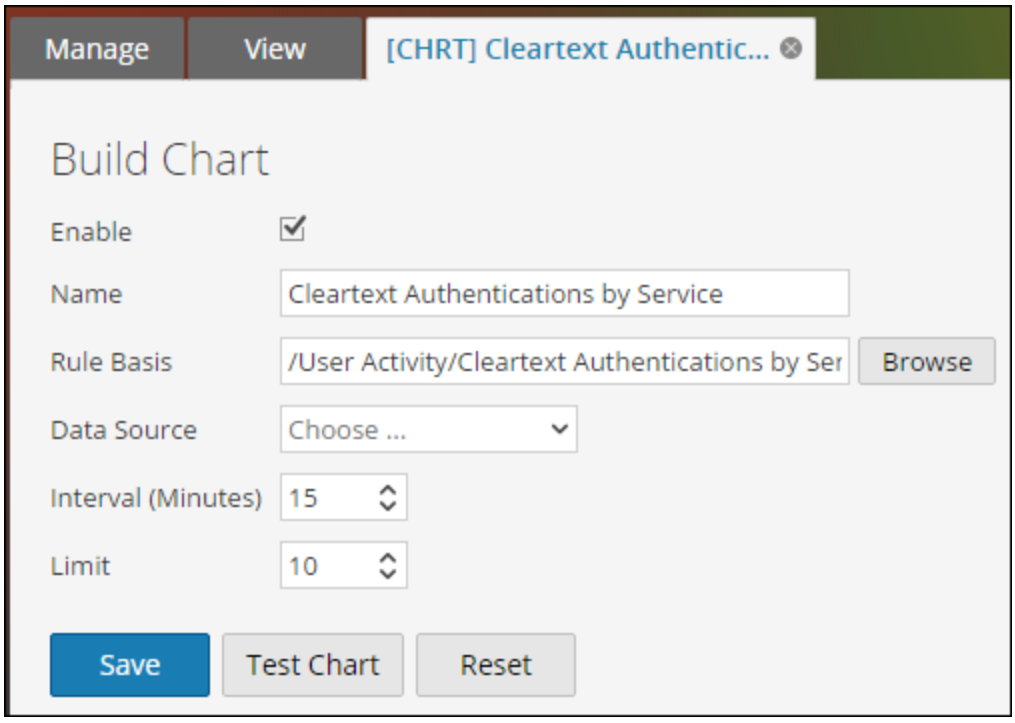
2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, do one of the following:

   - Double-click a chart or select a chart and click  .
   - Select a chart and click  > **Edit**.

     The Build Chart view tab is displayed.



4. Modify the name of the chart.
5. For the Reporting Engine to collect the data and generate chart results, select the **Enable** checkbox.
6. (Optional) In the **Rule Basis** field, do the following:

a. Click **Browse**.

The Add Rule dialog is displayed.

b. Navigate the Rule tree and select a rule.

c. Click **Select**.

The Rule appears in the Rule Basis field.

7. Select the data source from the **Data Source** drop-down list.

> **Note:** If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data sources. For more information, see the "Configure Data Source Permissions" topic in the *Host and Services Configuration Guide*.

8. (Optional) To modify the Interval value, click the up or down arrows.
9. Select the limit value to limit the number of records to be displayed.
10. Click **Save**.

A confirmation message that the chart is modified successfully is displayed.

Delete a Chart

To delete a chart in a group or subgroup:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Charts**.
   The Chart view is displayed.
3. In the **Charts** panel, do one of the following:
   - Select the charts and click .
   - Click  > **Delete**.
     A confirmation message asks if you want to delete the selected chart.
4. Click **Yes** to delete the chart.

A confirmation message that the chart is deleted successfully is displayed and the selected chart is deleted from the Charts panel.

Duplicate a Chart

To duplicate an existing chart:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Charts**.

   The Chart view is displayed.

3. From the **Charts** panel, select a chart to be duplicated.
4. In the **Charts** toolbar, click  .

The chart is duplicated and gets added to the Charts panel.

Import a Chart

To import charts from other instances of NetWitness:

1. Go to **Reports**.

   The Manage tab is displayed.
2. Click **Charts**.

   The Chart view is displayed.
3. From the **Charts Groups** panel, select a folder from which to import the file.
4. Do one of the following:

   - In the **Chart** toolbar, click  > **Import**.

     The **Import Chart** dialog box is displayed.
   - You can import multiple charts at the same time. To select multiple charts, press and hold the CTRL button and select the charts to be imported.
5. Click **Browse** to select the binary file.

   NetWitness provides a file system view of the files.
6. Locate the binary file and click **Open**.

   The file is added to the Import Chart list.
7. (Optional) To overwrite any existing rule in the library with an identically named rule in the binary file when importing, select the **Rule** checkbox. If you do not select the Overwrite option, and an identical rule is encountered in the binary file, the binary file is imported and no error message is displayed.
8. (Optional) To overwrite any existing list in the library with an identically named list in the binary file, select the **List** checkbox. If you do not select the Overwrite option, and an identical list is encountered in the binary file, the binary file is imported and no error message is displayed.
9. (Optional) To overwrite any existing chart in the library with an identically named chart in the binary file when importing, select the **Chart** checkbox. If you do not select the Overwrite option and an identical chart is encountered in the binary file, the binary file is imported and no error message is displayed.
10. Click **Import** to import the binary file.

Export a Chart

To export selected charts to an external file:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, select a chart and click  and do one of the following:

   - **Export** - This selection exports a chart in a .zip file.
   - **Export as Text** - This selection exports a chart from the Reporting Engine in a .zip file which contains the data in text format.

   You can export multiple charts at the same time. To select multiple charts, select the checkboxes of the charts to be exported. The exported file is saved to the local drive.

Enable a Chart

To enable a chart:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, select a chart or several charts that display ○ in the **Enabled** column.

4. Click ●.

A confirmation message indicates that the chart(s) state is changed successfully.

Disable a Chart

To disable a chart:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, select a chart or several charts that display ● in the **Enabled** column.

4. Click ○.

A confirmation message indicates that the chart(s) status is changed successfully.

Search an Existing Chart

To search for an existing chart:

1. Go to **Reports**.

   The Manage tab is displayed.

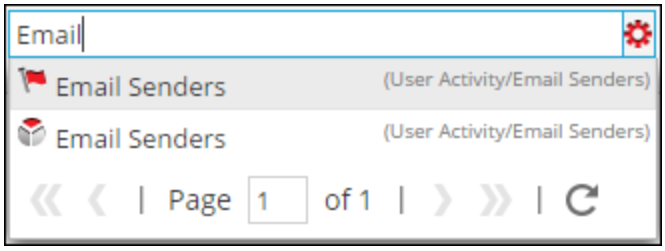
2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** toolbar, enter text in the Search text box.

4. Click > **Chart**.

All charts that match the search string are displayed in the search drop-down list.



Refresh a Chart

To refresh charts:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Charts**.

   The Chart view is displayed.

3. In the **Charts** panel, drag and drop the charts to the desired group in the **Charts Groups** panel.

   The charts are moved to the new location.

4. Do either of the following:

   - In the **Charts** panel, click .
   - In the **Charts** toolbar panel, select **Auto Refresh**.

   The Chart list is refreshed.

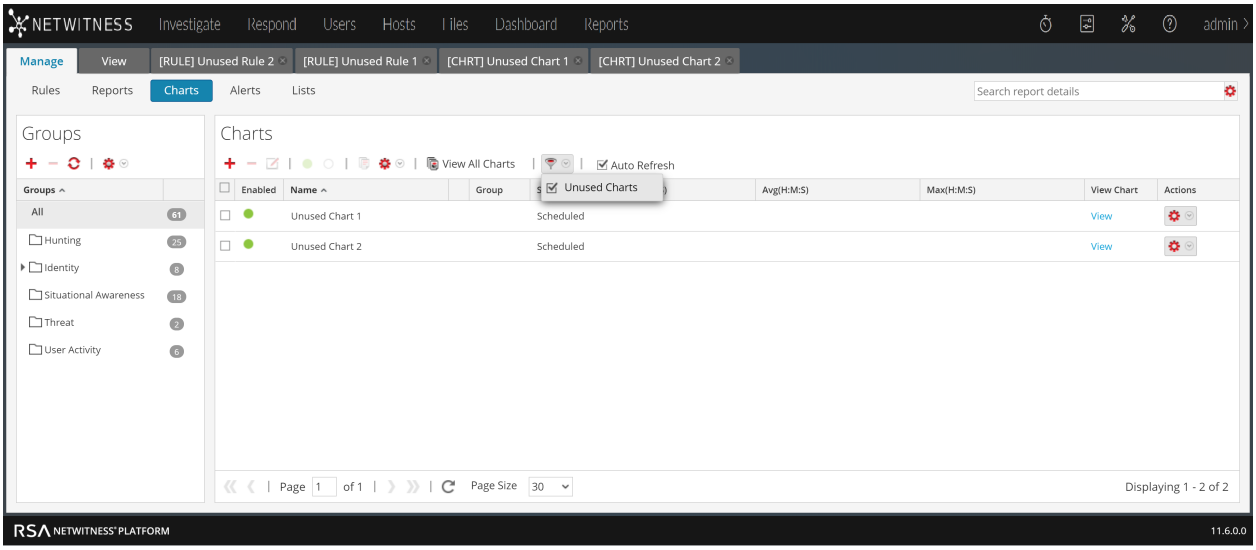
Filter Unused Charts

You can filter and delete the charts that are not used in any dashlet.

To filter unused charts:

1. Go to **Reports**.
   The **Manage** tab is displayed.

2. In the **Charts** panel, click  and select **Unused Charts**.
   List of unused charts will get displayed.
3. Delete the unused charts.
   For more information, see Delete a Chart.



Working with Alerts

The Alerting module user interface provides access to NetWitness alerts. The following topics discuss alerts:

- Alerting Overview
- Configure Reporting Engine
- Configure an Alert
- Schedule an Alert
- View an Alert
- Investigate an Alert
- Manage an Alert and Alert Template

Alerting Overview

Alerts can be used to generate timely insights about current security issues, vulnerabilities, and exploits. For example, when a malicious email is sent from a compromised account, you would need an alert that automatically notifies you when such an event occurs.

The following concepts of alerting will help you understand more about alert rules, conditions, notifications, and templates.

Alert Rules

Alert rules specify the logic for alert generation. Alert rules allow you to set up threshold limits and define how to be notified if these limits are exceeded. For example, you may set up a rule to be alerted if the CPU usage remains abnormally high for 5 minutes or more.

Alert Definitions

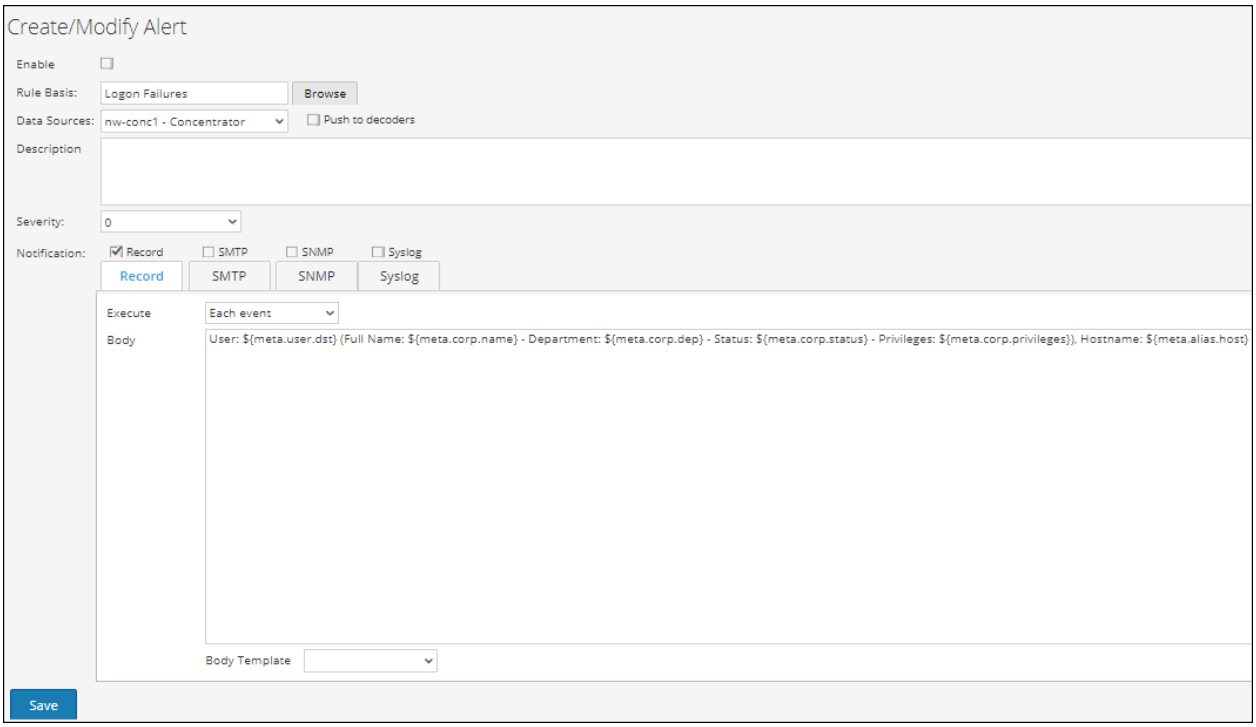
The alert definition is similar to defining rules for reports. These rules must be defined based on your use case. Alert definitions are made by selecting the alert rules you define in the Build Rule view. You select this rule while defining an alert.

Note: You can only alert using rules defined for NetWitness data source.

Once an alert is created, this data is collected from the Reporting Engine and displayed on the user interface.

Once an alert is defined, you can schedule the alert to run every minute (by default), or run at the present time, or run at the near future.

Note: In the NetWitness user interface, wherever Date and Time is displayed, it is always according to the user selected time zone profile.



Alert Notifications

The following are the components required to configure alert notifications:

- Notification server – Notification Server is used to send alert notifications. For example, SMTP mail server. Once 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 – Alert outputs, which can be email, SMTP, SNMP, and Syslog.
- Templates – The pre-defined format of an alert message.

When ever the rule condition is encountered, alerts get generated based on the severity level and notifies the user depending on the notification method set for that specific alert. The following are the various notification methods:

- Email/ SMTP: Simple Mail Transfer Protocol (SMTP) sends alert emails for system activity. Email alerts can be sent to their intended recipients by selecting SMTP as notification type.
- SNMP: Simple Network Management Protocol (SNMP) sends alerts to multiple computers for SNMP traps. SNMP alerts can be sent to other computers by selecting SNMP as notification type.
- Syslog: Syslog alerts generate notifications from Syslog messages. Syslog alerts can be sent by selecting Syslog as notification type.

Alerts can be configured to notify events that require attention, or as mechanisms to take automated actions based on conditions configured in an alert. An alert is sent when conditions within the entity have met the criteria selected for the alert. The notification criteria determines when and at what frequency the alert is generated.

Alert Templates

Alert templates are pre-defined format for an alert message. You can use these templates to create alerts.

Access Control for Alerting

Depending on the user role, the user is provided with specific set of access permissions in order to manage an alert. The Administrator manages the access rights provided to each user role from the **(Admin) > Security > Roles** tab. You can set access permissions for the user roles to manage an alert. The Reporting module provides access control at the alert level.

Note: Reporting Engine Alert permissions are prefixed with 'RE' to distinguish them from Event Streaming Analysis (ESA).

When you create users and user roles, ensure that the roles that you create for specific tasks have access to all the necessary permissions. This could require permissions at several levels of the role hierarchy.

Alerts can be combined with a specific set of user roles so that when a user logs into NetWitness, the only alerts they can access are alerts accessible by the role to which the user belongs. Users that belong to a user role with the '**Read & Write**' access permission can define alerts. The access can further be tightened so that the alerts are accessed only by those who have the '**Read Only**' access.

At the alert level, you can set the following access permissions for the user roles in NetWitness:

- Read & Write
- Read Only
- No Access

Note: Before applying the Alert permissions, the default permission set for all the user roles is '**No Access**' permission and the checkbox is unchecked.

If you want to change the access permission for a specific user role, you must set it at the alert level. Except for administrators, the default permission set for all the other user roles is '**No Access**' permission.

The two scenarios are explained in brief:

- Scenario 1: Permissions applied to alert/ rules based on the user role.
- Scenario 2: Read-only permission applied to rules in the Alert.

	Role (Analysts)	Permissions applied to Alert/ Rules based on the user role	Permission (Read-only) applied to Rules in the Alert
Alert	**Read & Write**	**Read & Write**	**Read & Write**
Rules	**Read**	**Read**	**Read**

The Alert is assigned the role of a Security Analyst and permissions are set to **Read & Write** alerts.

For scenario 1, each of the levels has a permission set based on the user role. For scenario 2, the **Read** permission is set for the Rules except that the permission for the rules must not be higher than the permission for the Alerts.

If the permission for the rules is higher than the permission for the Alerts, the permission is not applied. For example, if you set the permissions for the Alert as **No Access** and then specify the option *Apply Read-only permission to Rules in the Alerts*, the read-only permission is not set for the rules.

Access Control for an Alert When Multiple Alerts are Selected

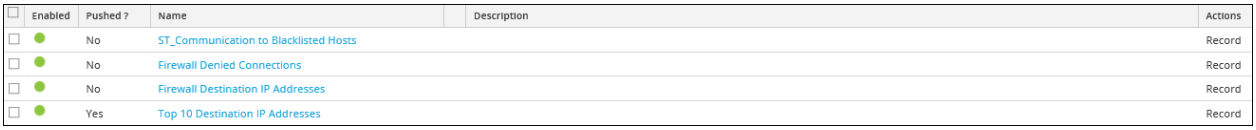
When you want to change permissions of multiple alerts, you must select several alerts and set their access permissions using the Alert Permissions panel. The access permission that you choose is applied to all the selected alerts.

Log in as a specific user and view the access details

When you log in to the NetWitness UI as a user having **Read** access permission, all the alerts will be denoted with the symbol (📖) and when you click on the symbol the 'Read Only' callout is displayed on the Alert panel.

When you log in to the NetWitness UI as a user not having **Read & Write** access permission on an Alert, all the alerts will be denoted with the symbol ( ) and the alerts appear grayed out on the Alert panel.

The following figure shows the Alert panel when logged in with minimal **Read & Write** access permission.

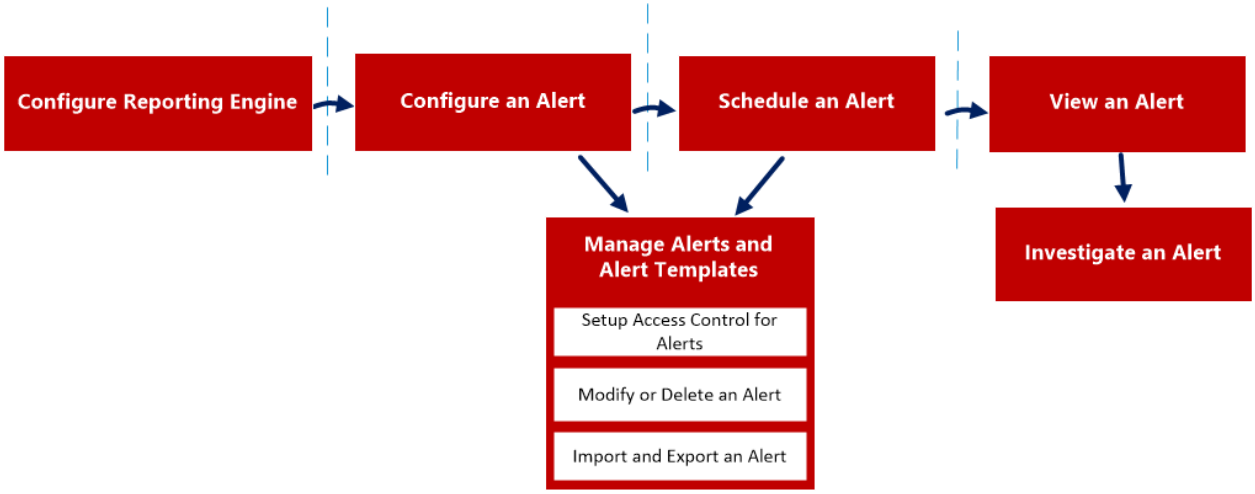


Note: If a user (other than ADMIN) creates an alert, ADMIN cannot access that alert.

The following table lists the various columns in the Alert Permissions panel:

Column	Description
Roles	The role of the user logged into the NetWitness user interface.
Read & Write	The user can access, view, edit, import, export, and delete the alert on the Alerts page. The user can also change the permission on the alert.
Read Only	The user can only access and view the alert on the Alerts page.
No Access	The user cannot access or view the alert for which this permission is set.
Apply Read-only permission to Rules in the Alerts	The user can automatically apply permissions to the rules in the alerts.

The following is an overview of the entire process of alerting:



To configure and generate an alert on Reporting Engine, perform the following:

1. Configure Reporting Engine
2. Configure an Alert
3. Schedule an Alert
4. View an Alert
5. Investigate an Alert
6. Manage an Alert and Alert Template

Configure Reporting Engine

Ensure that:

- You have Decoders that are connected to the Concentrator added to the Reporting Engine for the selected data source, before creating an alert rule.
- You have installed and configured a Syslog server that supports TCP/TLS in your environment. For example, WinSyslog. You can configure the Reporting Engine to send Syslog messages over TCP with Transport Layer Security (TLS) when an alert is triggered.

To configure the Reporting Engine to send Syslog alerts over TCP with Transport Layer Security (TLS):

1. Obtain the required certificates.
2. Append the CA certificate to the ca.pem file on the NetWitness server.
3. Configure the Syslog server to accept messages from client machines.
4. Configure the delivery of alert messages in the NetWitness UI.

Task 1: Obtain the required certificates

To generate certificates for configuring Reporting Engine to send Syslog messages over TCP with TLS:

1. Generate a Certifying Authority (CA) certificate. For more information, see http://www.rsyslog.com/doc/tls_cert_ca.html.

Note: You can ignore this step if you already have a CA running in your environment.

2. Generate a key pair for the Syslog server. For more information, see http://www.rsyslog.com/doc/tls_cert_machine.html.

Note: You can ignore this step if you have already configured security for the Syslog server using the key and certificates generated by the same CA.

Task 2: Append the CA certificate to the ca.pem file on the NetWitness Server

To append an existing CA certificate to the ca.pem file:

1. Manually append the contents of the CA certificate that you generated to the **/etc/pki/CA/certs/ca.pem** file.
2. Run the following command on the NetWitness server to have the certificate populate to the Truststore:
   ```
   keytool -import -file /etc/pki/CA/certs/ca.pem -keystore cacerts
   ```

Task 3: Configure the Syslog Server to accept messages from client machines

To configure the Syslog server to accept messages from client machines that have the same CA certificates:

1. Copy the following files to your secure TCP server target location:
   - ca_cert.pem
   - server_cert.pem
   - server_key.pem

   Where:

   ca_cert.pem - is the CA certificate

   server_cert.pem - is the server certificate

   server_key.pem - is the server key

   For more information, see the documentation specific to your Syslog server. If you are using rsyslog, refer to http://www.rsyslog.com/doc/tls_cert_server.html.

Task 4: Configure the delivery of alert messages in NetWitness

Configure Reporting Engine to send Syslog messages over TCP with Transport Layer Security (TLS) when an alert is triggered by enabling **SECURE_TCP** in the **Output Actions** tab for the Reporting Engine service in the Reporting Engine Services Config View. For more information, see the **"Reporting Engine Output Actions"** topic in the *Host and Services Configuration Guide*.

Configure an Alert

You can configure an alert by setting up alert notifications and adding a notification method to a rule.

Note: Only Administrators can set up these notifications.

To configure an alert:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Alerts**.

   The Alert view is displayed.

3. In the **Alert** toolbar, click  .

   The Create/Modify Alert panel is displayed.

4. Click **Enable** to enable the alert.
5. In the **Rule Basis** field:
   a. Click **Browse**.

      The Lookup Rule Basis dialog box is displayed.

   b. Navigate the Rule tree and select a rule.
   c. Click **OK**.

      The Rule name is displayed in the Rule Basis field.

6. From the **Data Sources** drop-down list, select a data source.

   Note: If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse Connector data sources. For more information, see **"Configure Data Source Permissions"** topic in the *Host and Services Configuration Guide*.

7. Select the **Push to decoders** checkbox for the Reporting Engine to send the rule to the Decoder.
8. (Optional) Enter an alert description in the **Description** field.
9. From the **Severity** drop-down list, select the severity level.
10. In the **Notification** field:
    a. Select the appropriate notification.
       The selected notification tab is displayed in the Create/Modify Alert dialog box.
    b. (Optional) Deselect the notification to disable the notification tab.
    c. Define an action in one of the **Notification** tabs:

i. In the **Record** tab field:

   a. From the **Execute** drop-down list, select the frequency for recording an alert.

   b. Enter the RECORD message. You can create a new message or select a template in the **Body Template** field and modify the template here.

   c. (Optional) If templates have been defined, select a template for the RECORD message that you can use as is or modify.

ii. In the **SMTP** tab field:

   a. From the **Execute** drop-down list, select a value to identify the number of times to send an email message for the alert.

   b. Enter an email address or comma-separated list of email addresses to send this alert.

   c. Enter the subject of the email message.

   d. Enter the body of the message. You can create a new message or select a template in the **Body Template** field and modify the template here.

iii. In the **SNMP** tab field:

   a. From the **Execute** drop-down list, select a value to identify the number of times that you want to send an SNMP message for the alert.

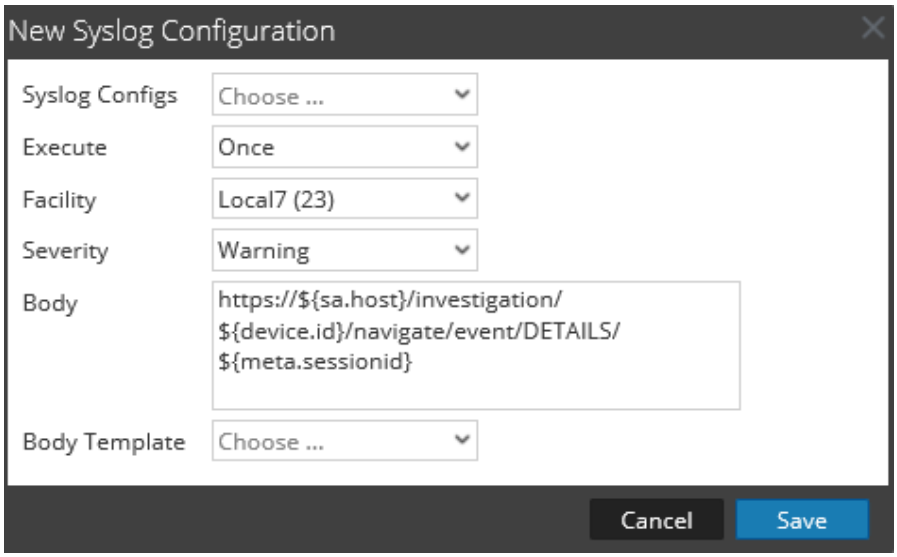
   b. Enter the SNMP message. You can create a new message or select a template in the **Body Template** field and modify the template here.

iv. In the **Syslog** tab field:

> **Note:** You can configure Multiple Syslog servers on the Syslog Configuration panel. For more information, see **"Reporting Engine Output Actions"** topic in the *Host and Services Configuration Guide*.

   a. Click .

   The New Syslog Configuration dialog box is displayed.



b. From the **Syslog Configs** drop-down list, select a value for the syslog configuration.

c. From the **Execute** drop-down list, select a value to identify the number of times to send a Syslog message for the alert.

d. From the **Facility** drop-down list, select the facility.

e. From the **Severity** drop-down list, select the severity level.

f. Enter the Syslog message. You can create a new message or select a template in the **Body Template** field and modify the template here.

> **Note:** If you want to add a metakey, specify the same in the format: ${meta.metakey}. For example, ${meta.ip.dst}.

g. Click **Save**.
The Syslog configuration gets added to the alert.

11. Click **Create**.

NetWitness creates an alert with a confirmation message that the alert is saved successfully. NetWitness generates the alert and executes the output actions every minute.

Schedule an Alert

You must schedule an alert to search for events on a regular schedule.

To schedule an alert:

1. Go to **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. Select an alert to schedule.
4. On the **Alert** toolbar, click **Enable**.
The selected alert is scheduled.

View an Alert

You can view an alert or a list of all alerts.

You can view the alerts triggered and investigate any alert in the Investigation module and customize these views to show alerts for a specific period of time, and set the maximum number of alerts displayed in a single page.

To view an alert:

1. Go to **Reports** to view the Manage tab.
2. Click **Alerts** to open the Alert view.
3. On the **Alert** toolbar, click **View Alerts**.
   The View Alerts view is displayed.

Investigate an Alert

You can investigate every alert that is triggered on the Alert View. For more detailed investigation on a particular alert, you can view the alert on the Investigation module.

To investigate an alert:

1. In the **Alert** section toolbar, click **View Alerts** to navigate to the View Alerts view.
2. Do one of the following:
   - Click the  button against the alert you want to investigate.
     The Investigation module displays the details of the first session that registered the match for the given alert for immediate analysis.
   - Click on the alert name of the alert you want to investigate.
     The Investigation module displays all matches for that particular alert for the hour surrounding the registered alert.

Manage an Alert and Alert Template

You can manage alerts, scheduled alerts, and alert templates using the following procedures.

Manage an Alert

Depending on the access permissions set for the user role, you can modify or delete, import and export, enable or disable alerts, view or refresh an alert list.

Access Control for an Alert When a Single Alert is Selected

To set access permissions for an alert:

1. Go to **Reports**.
   The Manage tab is displayed.

2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** panel, select an alert.
4. Click > **Permissions**.
   The Alert Permissions dialog box is displayed.
5. Based on the user role, select the appropriate options.
6. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.

Note: When the check box is selected, all dependent rules with the No access permission will be given the READ access permission.

7. Click **Save**.
   A confirmation message that the permission is successfully set for the selected alert is displayed.

Access Control for an Alert When Multiple Alerts are Selected

To change permissions of multiple alerts:

1. In the **Alerts** panel, select all the alerts whose permissions must be set.
2. Click > **Permissions**.
   The Alert Permissions dialog box is displayed.
3. Select the permission to set for the respective user role.
4. Click **Save**.
   A confirmation message that the permission is successfully set for all the selected alerts is displayed.

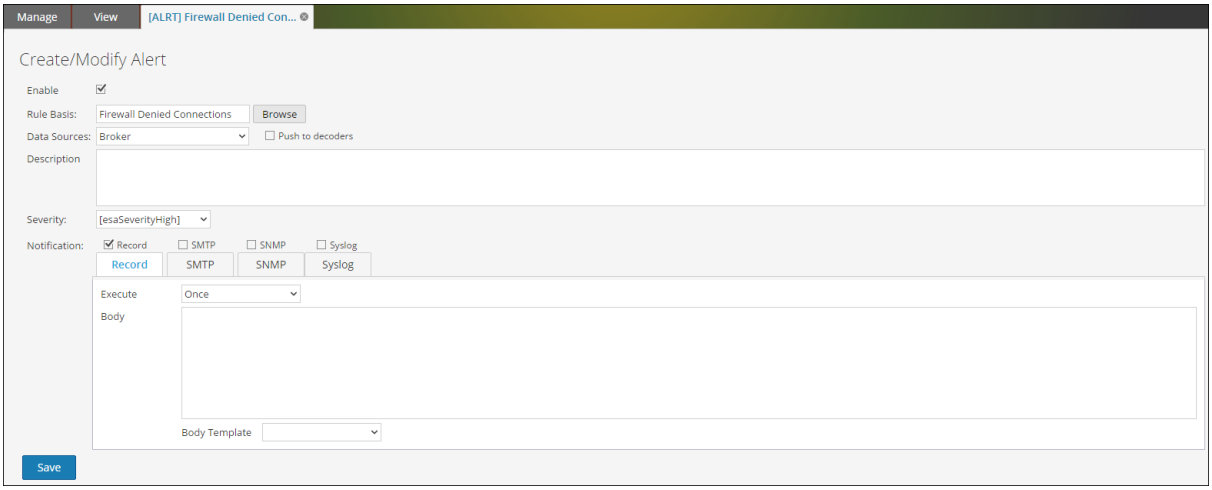
Edit an Alert

For example, if you want to be notified about the alert over an email on a different Email ID, you will have to modify the alert notification section with the new Email ID details to be reverted over an email when an alert is generated. Additionally, you can also modify the alert description and alert notification in the Create or Modify Alert panel.

To edit an alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.

3. In the **Alert** panel, select an alert and click .
   The Create or Modify Alert tab is displayed.



4. In the **Rule Basis** field, navigate the rule tree and select another rule.
   The Rule name is displayed in the Rule Basis field.
5. (Optional) Select a data source from the **Data Sources** drop-down list.

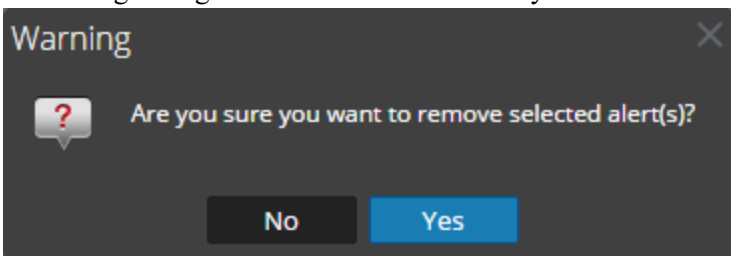
> **Note:** If the data source is not listed, then ensure you have **Read** permissions set for the data source. This is applicable for NWDB and Warehouse data source. For more information, see **"Configure Data Source Permissions"** topic in the *Host and Services Configuration Guide*.

6. (Optional) Modify the alert description in the **Description** field.
7. Modify the appropriate **Notification** tabs – **RECORD**, **SMTP**, **SNMP**, and **Syslog**.
8. Click **Save**.
   A confirmation message that the alert is modified successfully is displayed.

Delete an Alert

To delete an alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** panel, select the alert and click .
   A warning dialog asks for confirmation that you want to remove the selected alerts.



4. Click **Yes** to delete the alert.
   A confirmation message that the alert is deleted successfully is displayed and the selected alert is deleted from the Alert panel.

Import an Alert

To import an alert from other instances of NetWitness in the Alerts panel:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click > **Import**.
   The Import Alert dialog box is displayed.
4. Click **Browse** to select the binary file.
   NetWitness provides a file system view of the files. You can import multiple alerts at a time. To select multiple alerts, select the checkbox of the alert to be imported.
5. Locate the binary file, and click **Open**.
   The file is added to the Import Alert list.
6. (Optional) To overwrite any existing alert in the library with an identically named alert in the binary file when importing, select the Alert checkbox. If you do not select the Overwrite option, and an identical alert is encountered in the binary file, the binary file is imported and no error message is displayed.
7. Click **Import** to import the binary file.

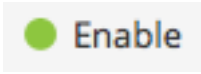
Export an Alert

To export an alert to an external file that can be later imported to NetWitness:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** panel, select an alert and click and do one of the following:
   - **Export** - This selection exports an alert in a .zip file.
   - **Export as Text** - This selection exports all the content from the Reporting Engine in a .zip file which contains the data in text format.
     You can export multiple alerts at a time. To select multiple alerts, check the checkbox of the alert to be exported.
4. Click > **Export**.
   The exported binary file is saved to the local drive.

Enable an Alert

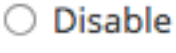
To enable an alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** panel, select the alert that displays ○ in the **Enabled** column.
4. Click 

.
   A confirmation message shows that the change to the alert(s) state was successful.

Disable an Alert

To disable an alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** panel, select the alert that displays ● in the **Enabled** column.
4. Click 

.
   A confirmation message shows that the alert(s) status is changed successfully.

View an Alert List

To view an alert list:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click **View Alerts**.
   The View Alerts view tab is displayed.
4. Select the last number of days from the drop-down list.
5. Enter a value for the **Max no of alerts**.
   The alerts list is displayed based on the chosen filter value.

Refresh an Alert List

To refresh the list of alerts:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. From the **Alert** toolbar, click  to refresh the alerts list.
   The Alert panel is refreshed.

Manage a Scheduled Alert

You can enable or disable a scheduled alert, and view all scheduled alerts.

Enable a Scheduled Alert

To enable a scheduled alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click View Schedule.
   The View Alerts Schedule view tab is displayed.
4. In the **Alerts Schedule List** panel, select the scheduled alert (s) to be enabled.
5. Click .
   A confirmation message indicates that the alert(s) status is changed successfully and the alert is now available in the Alert panel.

Disable a Scheduled Alert

To disable a scheduled alert:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click View Schedule.
   The View Alerts Schedule view tab is displayed.
4. In the **Alerts Schedule List** panel, select the scheduled alert (s) to be disabled.
5. Click .
   A confirmation message indicates that the alert(s) status is changed successfully and the alert is now available in the Alert panel.

View all Alerts Scheduled

To view all the alerts scheduled:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. In the **Alert** toolbar, click **View Schedule**.
   The View Alerts Schedule view is displayed with a list of all the scheduled alerts.

Manage an Alert Template

You can modify or delete an alert template, and view all alert templates.

Edit an Alert Template

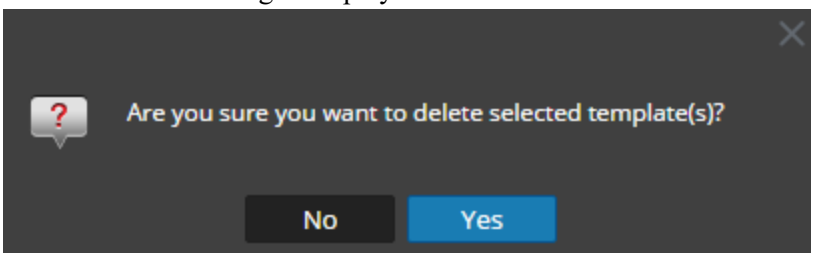
To edit an alert template:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click Template.
   The Alert Template view is displayed.
4. In the **Alert Template** panel, select a template and click .
   The Create/Modify Template dialog box is displayed.
5. Click **Save**.
   A confirmation message that the template is modified successfully is displayed.

Delete an Alert Template

To delete an alert template:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.
3. Click Template.
   The Template view tab is displayed.
4. In the **Alert Template** panel, select a template and click .
   A confirmation dialog is displayed.



5. Click **Yes** to delete the template.
   A confirmation message that the template is deleted successfully is displayed.

View all Alert Templates

To view all alert template messages:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Alerts**.
   The Alert view is displayed.

3. In the **Alert** toolbar, click **Template**.
   The Template view tab is displayed with a list of templates.

List of Available Variables

Below are the list of variables available on the Reporting Engine notification for Reporting Engine alerts.

```
Name: ${name}
Severity: ${severity}
alert count: ${count}
Start_session_id = ${sid1}
end_session_id = ${sid2}
data source id = ${device.id}
netwitness host = ${nw.host}
```

See below example for how to use metadata information on the notification template.

To use ip.src and ip.dst meta, use the format `${meta.<meta-name>}`.

```
ip.src meta = ${meta.ip.src}
ip.dst meta = ${meta.ip.dst}
```

Appendix

This section provides detailed information about the supported aggregate functions, rule syntax, advanced rules query syntax in Reporting and task scheduler for Warehouse Reporting.

Rule Syntax

This section describes the different rule syntax supported in the Reporting Engine.

NWDB Rule Syntax

The NWDB rule is one of the rule syntax supported in the Reporting Engine. To enhance the execution time of your reporting entities, see "Reporting Guidelines" section in Reporting Overview.

A Rule is a function that manipulates the result set of a rule in order to make the output in a report more meaningful or add additional functionality to a rule other than querying data and displaying it. Any combination of these rule actions can be used to create unique and interesting representations of the information collected by NetWitness.

The Reporting Engine supports the following categories of NWDB data source rule syntax:

- **select** clause
  - Non-Aggregate Rule
  - Aggregate Rule
- **alias**
- **where** clause
- **where** clause Operators
- **then** clause
- **Limit** field
- Rule Actions
- Rule Operators

Select Clause

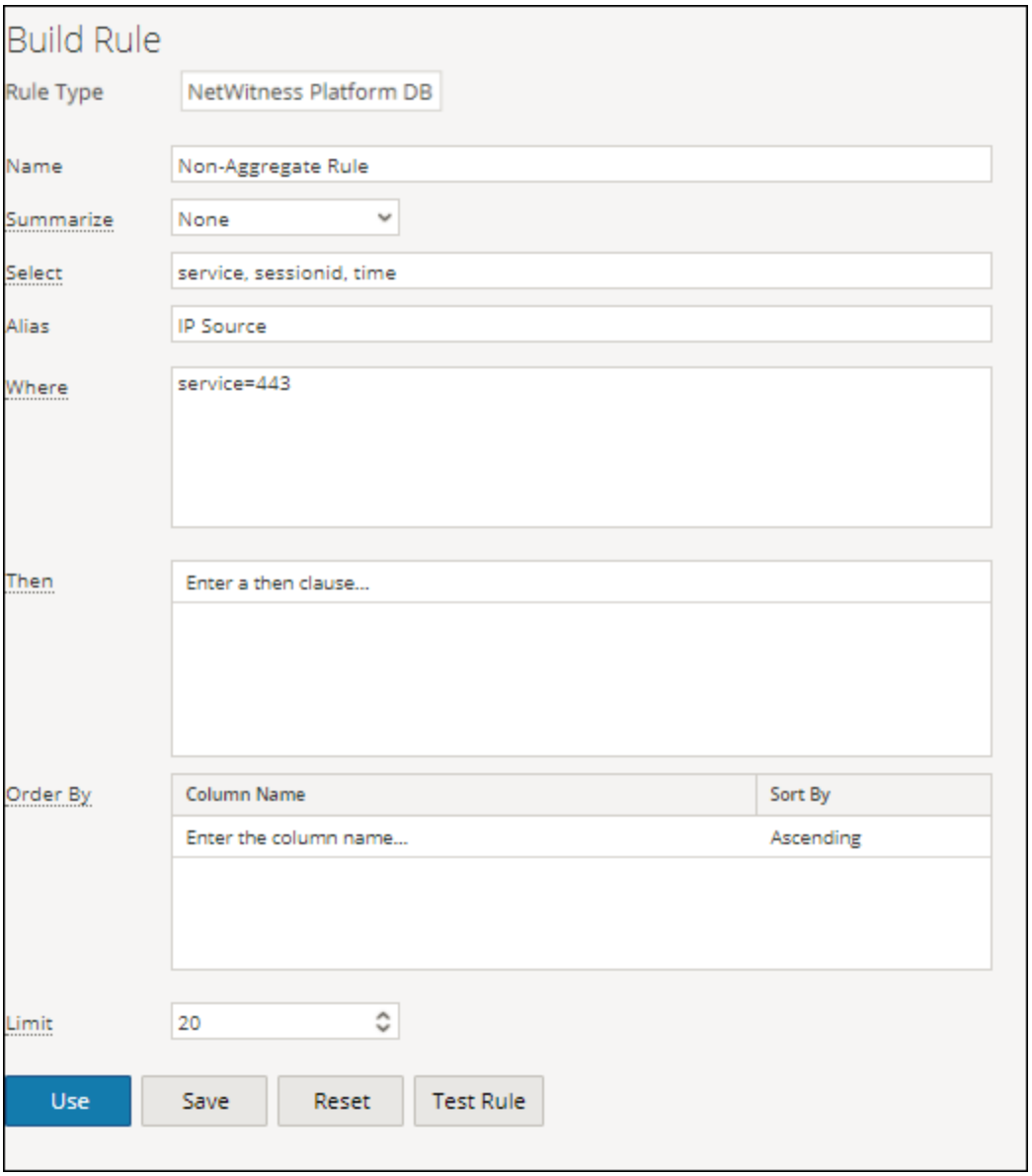
The select clause is a comma separated list of values. For example: select sessionid,time,service.

There are two types of select clause for NWDB Rule:

- Non-aggregate rule
- Aggregate rule

Non-Aggregate Rule

When you want to define a rule without any grouping, choose 'None' in the Summarize field. In a non-aggregate rule, you can select any number of metas in the *Select* clause. For example, select service, sessionid, time.

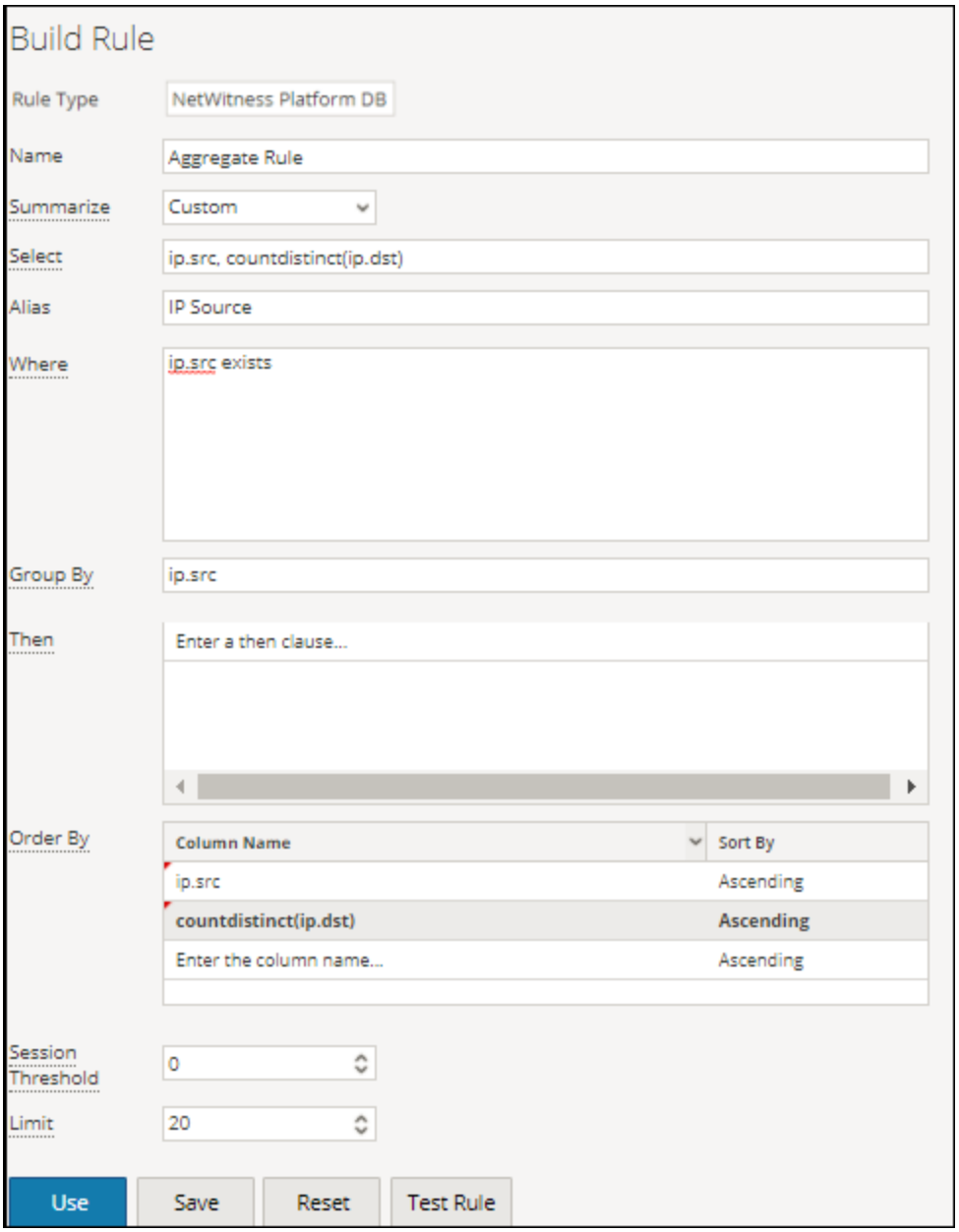


Aggregate Rule

When you want to query for a specific meta and its associated aggregate value then you must use the Aggregate rule. To get an aggregate, you must choose either of the three metas (Event Count, Packet Count, Session Size) or choose 'Custom' in the **Summarize** field to include an aggregate function in the *Select* clause. For example, select ip.src, sum (ip.dst). When Custom aggregate rule is enabled, the following fields are populated in the user interface:

- Group By
- Order By
- Session Threshold

The following figure shows the Build Rule view for Aggregate Rule.



There are two types of aggregate values that can be queried:

- Collection aggregation
- Meta aggregation

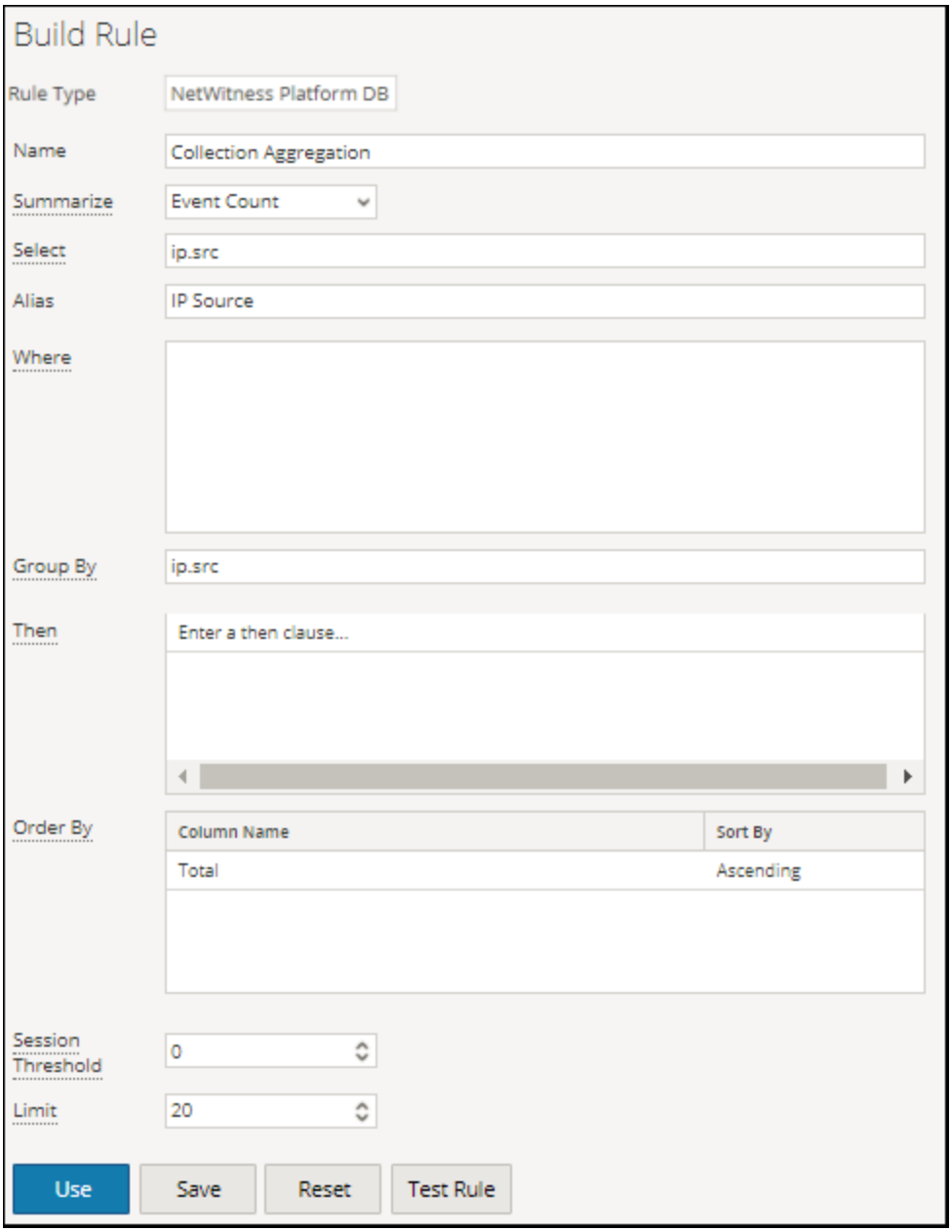
Collection Aggregation

With collection aggregation, you can get aggregates related to Event, Session or Packets. The following values can be queried in a collection aggregation:

- **Event Count**: The total count of events.
- **Packet Count**: The total count of packets.

- **Session Size**: The total session size.

These options are listed in 'Summarize' field and any one of them can be selected in a rule.
For example, choose any of the Collection aggregates (Event Count or Packet Count or Session Size) in the 'Summarize' field and select ip.src.



Meta aggregation

With meta aggregation, you can get aggregates of meta values. The following are the supported meta aggregate functions:

- sum(meta)
- count(meta)
- countdistinct(meta)
- min(meta)
- max(meta)
- avg(meta)
- first(meta)
- last(meta)
- len(meta)
- distinct(meta)

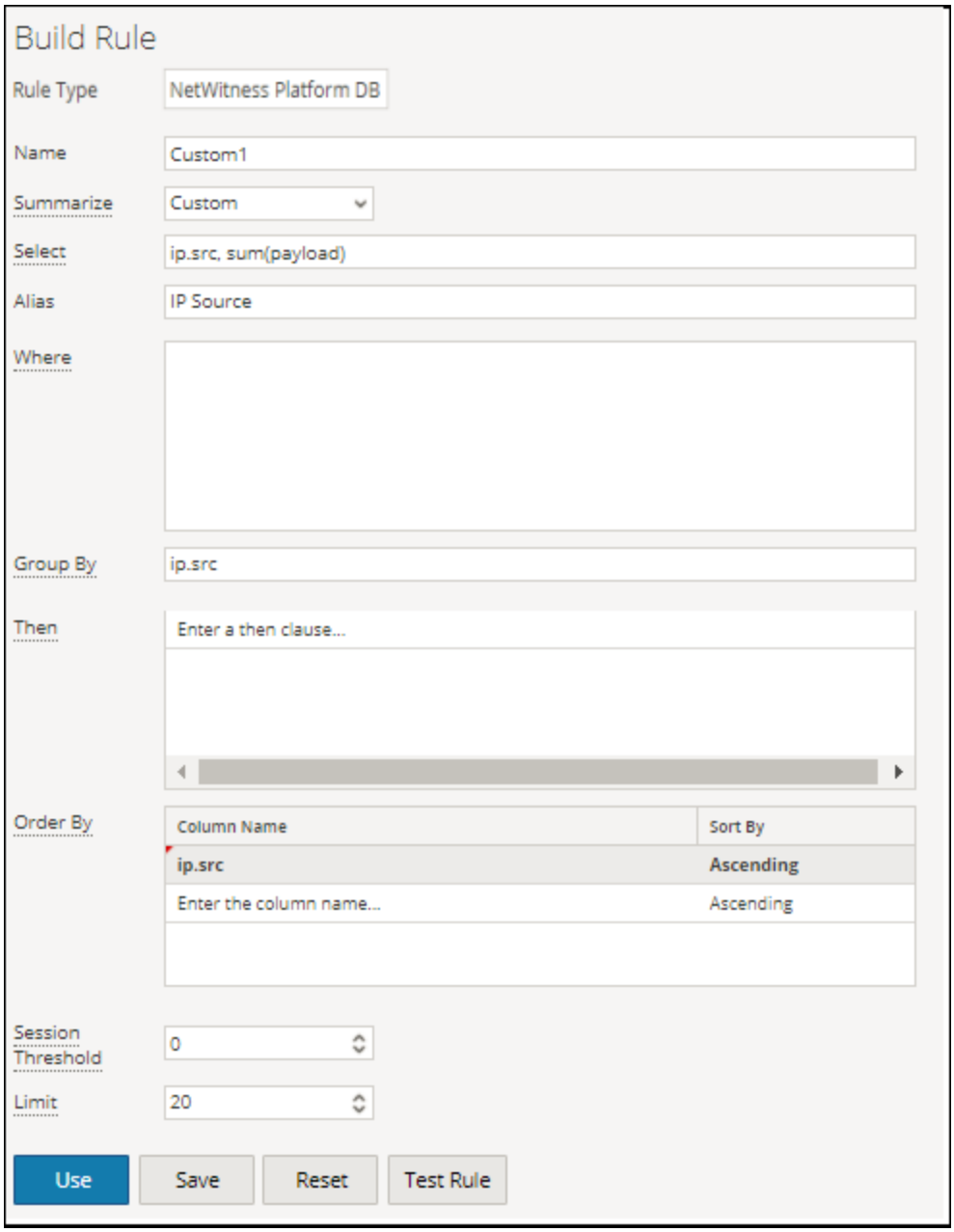
Supported Meta Aggregate Functions

The NWDB service supports the following meta aggregate functions and syntax in this release.

Syntax	Function
sum(<meta>)	The sum of all meta values. For example, if you provide the field sum(payload) in the select clause, the resultset is the sum of payload size. **Note:** The meta field chosen for the sum aggregate function must be of numeric data type.
count(<meta>)	The total number of meta fields that would be returned. For example, if you provide the field count(ip.dst) in the select clause, the resultset is the number of times an ip.dst value is returned.
countdistinct (<meta>)	The total number of distinct meta fields that would be returned. For example, if you provide the field countdistinct(ip.dst) in the select clause, the resultset is the number of times a distinct ip.dst value is returned.
min(<meta>)	The minimum of all meta values. For example, if you provide the field min(payload) in the select clause, the resultset is the min of payload size.
max(<meta>)	The maximum of all meta values. For example, if you provide the field max(payload) in the select clause, the resultset is the max of payload size.
avg(<meta>)	The average of all meta values. For example, if you provide the field avg(payload) in the select clause, the resultset is the avg of payload size. **Note:** The meta field chosen for the avg aggregate function must be of numeric data type.

Syntax	Function
first(<meta>)	The first occurrence of the meta value. For example, if you provide the field first(ip.src) in the select clause, the resultset is the first occurrence of ip.src for that group.
last(<meta>)	The last occurrence of the meta value. For example, if you provide the field last(ip.src) in the select clause, the resultset is the last occurrence of ip.src for that group.
len(<meta>)	Converts all field values to a UInt32 length instead of returning the actual value. This length is the number of bytes to store the actual value, not the length of the structure stored in the meta database. For instance, the meta value "NetWitness" returns a length of 10. All IPv4 fields, like ip.src, returns 4 bytes.
distinct (<meta>)	The distinct values of the meta. For example, if you provide the field distinct(ip.src) in the select clause, the resultset is all the distinct ip.src for that group.

You must select 'Custom' in 'Summarize' field and provide the meta and the meta aggregate functions in the select clause.



Note: Meta aggregate functions cannot be used in a WHERE clause and the rule actions like min_threshold/max_threshold can be used to filter aggregate functions. It is advised to use a more refined WHERE clause to get a better rule performance while using 'group by'.

Aggregate Query for Multiple Meta

To execute aggregate query for multiple Meta, follow these steps:

1. Go to **Reports**.

   The Manage tab is highlighted and the **Rules** view is displayed.

2. In the **Rules** toolbar, click + > **NetWitness Platform DB**.

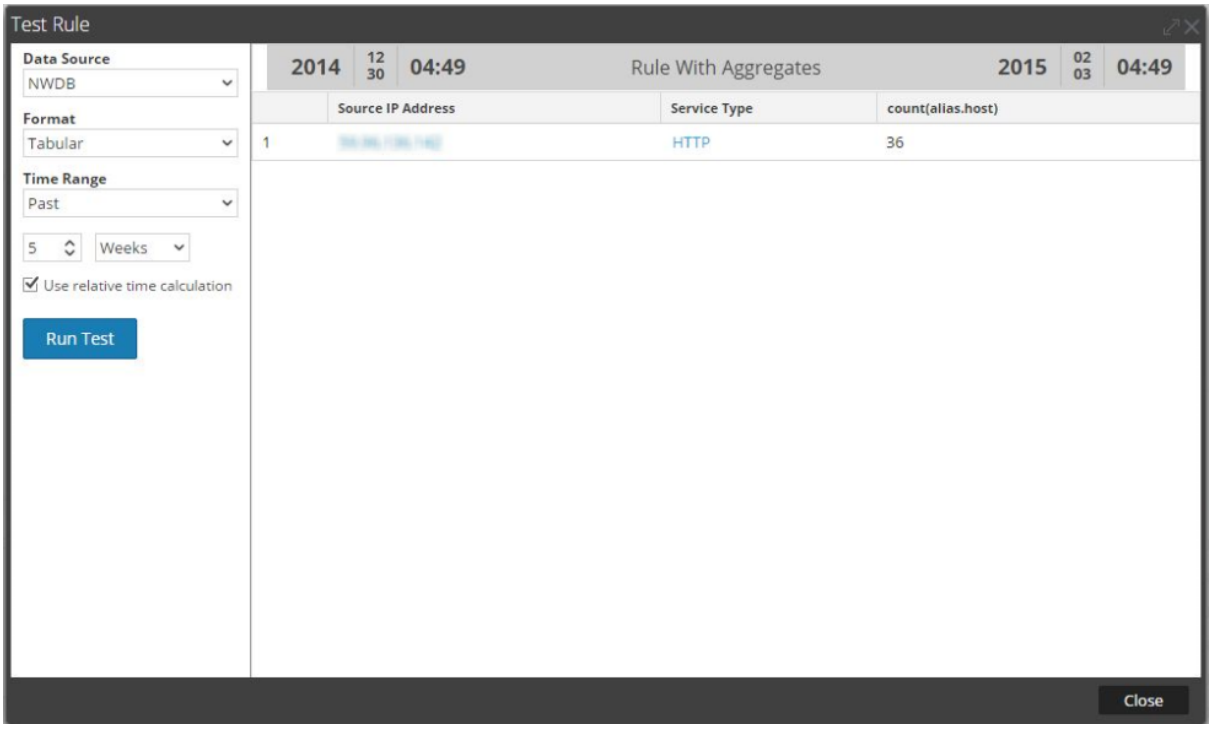
   For example, enter the following meta in the fields highlighted below:

   SELECT: ip.src, service, count(alias.host)
   ALIAS: Source IP Address, Service Type, count(alias.host)
   WHERE: ip.src = 59.96.136.142

   Note: In the alias field you can enter a name for columns used in the select clause. If you do not specify the alias for one of the field in the select clause, then the default description will be used. For example, if the select clause has Field1, Field2, Field3, Field4, and alias has only Field1, Field3, Field4, then for Field2 a default description is used.

3. Click the **Test Rule** button at the bottom of the screen.

   The Test Rule page is displayed.



Summarize

Summarize determines the type of summarization or aggregation for the rule.

Name	Config Value
Summarize	To query metas without any custom grouping, select: • **None**: The data is grouped by session in this case. To get collection (sessions/events/packets) related aggregates, select either of the following: • **EventCount**: The total count of events. • **Packet Count**: The total count of packets. • **Session size**: The total session size. To get meta based aggregates, select: • **Custom**: This indicates that expected meta aggregate function is defined in rule select clause.

Order By

Order By determines how to sort the result set.

Name	Configuration Value
Column Name	The **Column Name** is the name of the columns by which you want to sort the results. By default, the value is empty. When you click on a column, the value gets populated based on the Summarize field. • For 'None' and 'Custom', the value gets populated based on the entries made in the Select field. You can select from this list or add custom name. • For Event Count, Packet Count and Session size, accepted values are Total and Value. • Total - sort by aggregate value • Value - sort by group by meta
Sort By	**Sort By** determines the order in which you want to sort the results. The following are the values: • Ascending Order • Descending Order

Session Threshold

The session threshold is the optimization setting to stop scanning the matching sessions for each possible unique value for the selected meta. The threshold is an integer between 0 (default) and 2147483647. The threshold 0 scans for all matching sessions.

Note: If you provide a non-zero value (a value higher than zero), the aggregate results are inaccurate. This can be used only when you are interested in unique values and not aggregate values.

Supported where Clause

Syntax	Description
where <field1> [<field-operator>] < value1>,<value2>,<value3-value4> <logic-operator> <field2>,and so on	The where clause is a comma separated list of language field values and ranges that is used by NwValues function. In the where clause, string values have to be enclosed within single quotes. For example, where username = 'admin' && service = 22.
where <field1> [<field-operator>] <List1>	You can use a list in the where clause if you have multiple values to report on. For example, where ip.src exists && alias.host exists && alias.host contains $[User Reports/List of Alias Host]. When you use the list you must specify in the format $[<path>/<List name>].

In the where clause, make sure the syntax is correct based on the meta type.
For example,
For all text meta type use quotes for example, username = ‘user1’.
For all IP Addresses, Ethernet Addresses, and Numeric meta types do not use quotes for example, service = 80 && ip.src = 192.168.1.1.
For date and time meta types, if the date and time format is 'YYYY-MM-DD HH:MM:SS‘, use quotes.
If the date and time format is 1448034064 (number of seconds since EPOCH (Jan 1, 1970)), do no use quotes.

Note: If list is used in the rule, make sure that the list values are quoted or unquoted based on the type of the meta used. Checking the **Quotes will be inserted for all the values** checkbox in list definition page (for more information see, "Create Lists or List Groups" section in Configure a Rule) would quote all the list values.

Supported where Clause Operators

Syntax	Description
=	Returns results where the field is equal to any provided value. For example, tcp.dstport = 21-25,110 returns session with TCP destination ports of 21, 22, 23, 24, 25, or 110.
!=	Returns results for fields that do not match the values specified. For example, eth.type !=0x0800 returns sessions outside of hex value (decimal value of 2048) that is all non-IP based protocols.
begins	Checks for a value at the beginning of a text or binary field.
contains	Searches a text or binary value for a partial match.
ends	Checks for a value at the end of a text or binary field.
exists	If the field value exists, regardless of value, the operation evaluates to true.
!exists	If the field value does not exist, the operation evaluates to true.
length	Evaluates the length of the field. For example, username length 20-u returns any username that is 20 or more characters long.

Syntax	Description
regex	Performs a regular expression search against text or binary values.
not	Not operator is used to negate a clause or condition. For example, (not(user.dst ends "$")) will not display values for user destination.

Supported then Clause

Syntax	Description
then <rule action>	The then clause contains a rule action that manipulates the original result set of a rule in order to make the output in a report more concrete or add additional functionality other than querying data and displaying it. For example, dedup (filename).

Limit field

This indicates the limit to be put on the query while fetching data from the database. If a result set is sorted by event
count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not
sorted, the first N values are returned.

Rule Actions

The NWDB data source rule syntax supports the following rule actions:

- dedup
- filter_on
- filter_out
- lookup_and_add
- max_threshold
- min_threshold
- regex
- sum_count
- sum_values
- show_whats_new

dedup (string field)

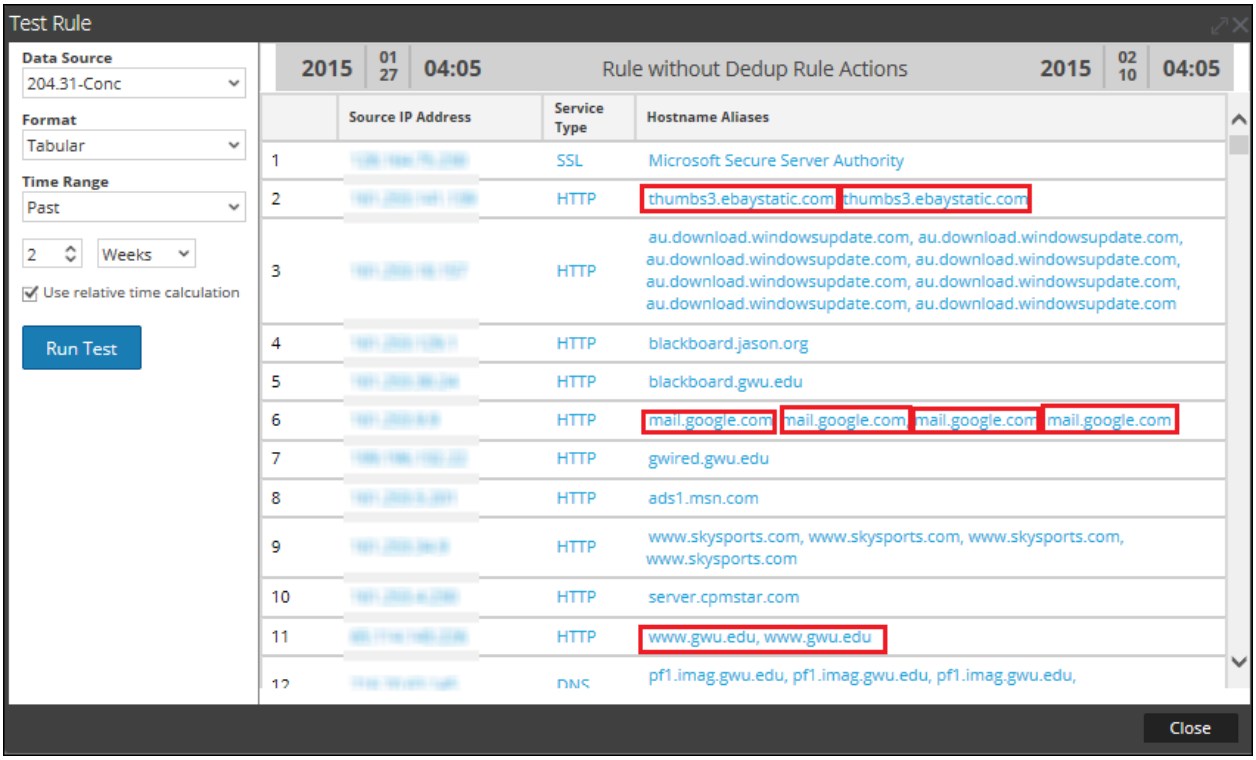
dedup removes the duplicate entries in an unsorted result set and displays only pertinent data.
The dedup rule action removes duplicate entries of a specific field in the report, so that only the first occurrence of that value is listed in the report.

Note: The dedup rule action cannot be used with an aggregate rule.

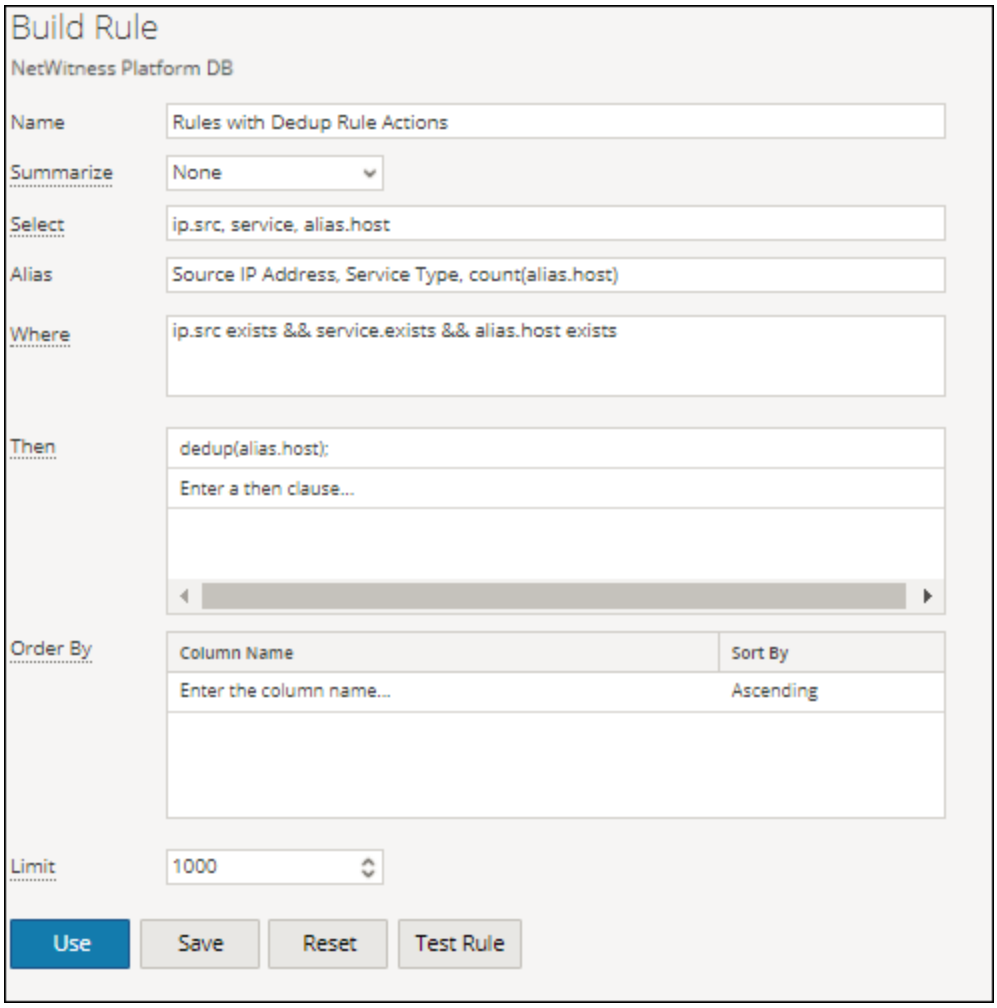
For example, the meta data generated by an individual session is often repetitive, especially when you have sessions with a lot of DNS lookups or web sessions that access the same host multiple times for various resources (such as, javascript, css). To remove the duplicate entries of the host, you can use the dedup rule action.

Example:

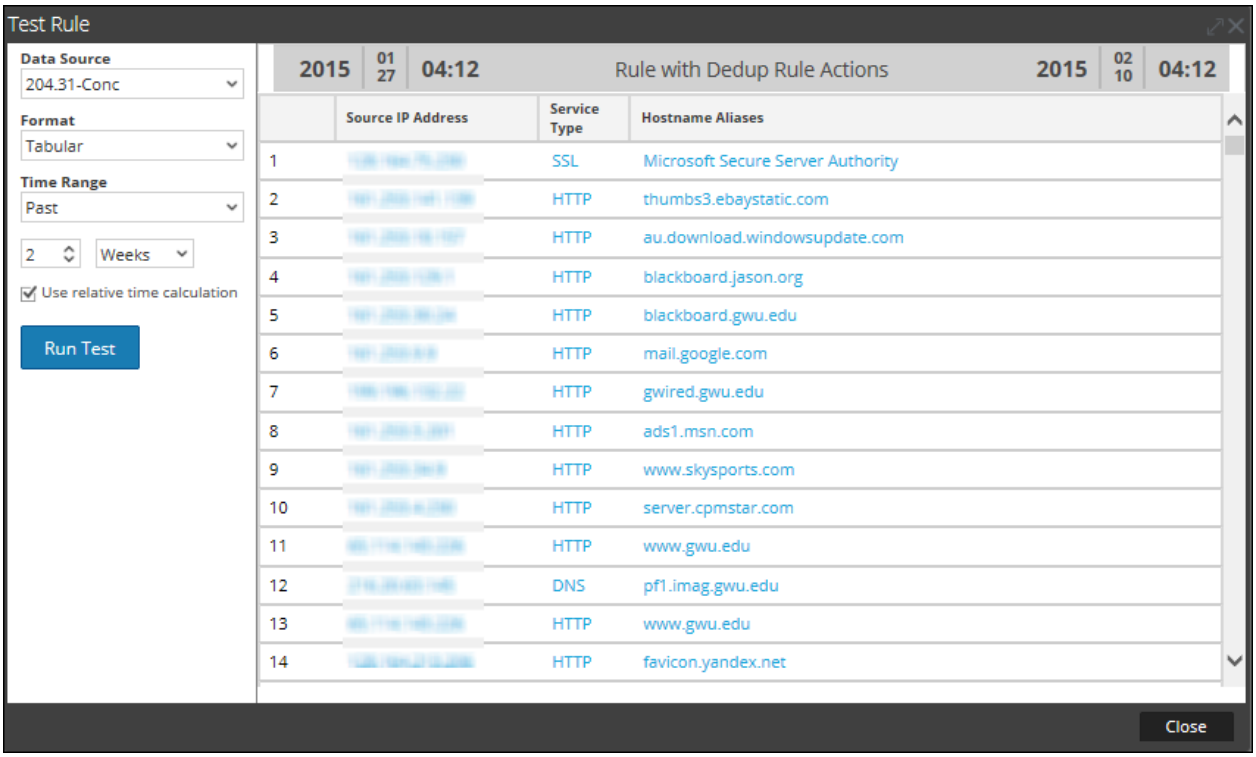
The following example is a lengthy result set that can be trimmed by removing the duplicate values in the same session.



The following figure shows the use of dedup rule action to remove the duplicate entries from the result set.



The duplicate value for each entry in the rule result set is reduced to one value.



filter_on (string filter, string field, bool matchExact)

`filter_on` removes values that do not contain the `filter` criteria from the result set. If the result set contains multiple fields, you must select a specific field to which the filter is applied. To add additional results to a single result set, include function such as lookup_and_add.

The matchExact parameter determines if the match is an exact match or contains a match.

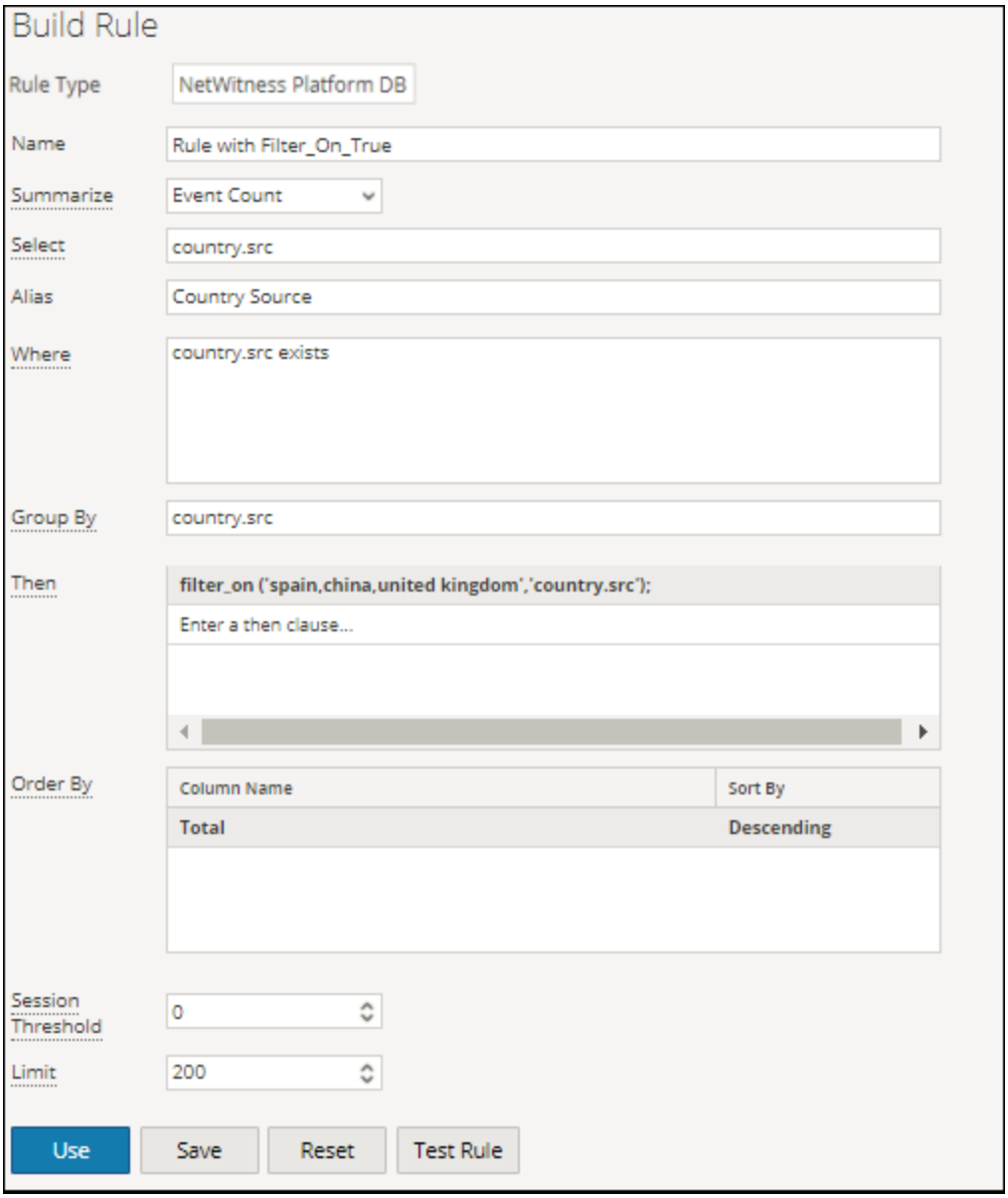
- If matchExact is set to `false`, any value that contains the filter text is considered a match.
- If matchExact is set to `true`, only values that match the provided filter text is included in the result set.

Note: Unless the matchExact parameter is specified, the default behavior of the rule action is to match exactly the text specified in the filter parameter. To specify that results containing the filter text must be kept in the result set, users must set the matchExact parameter to false.

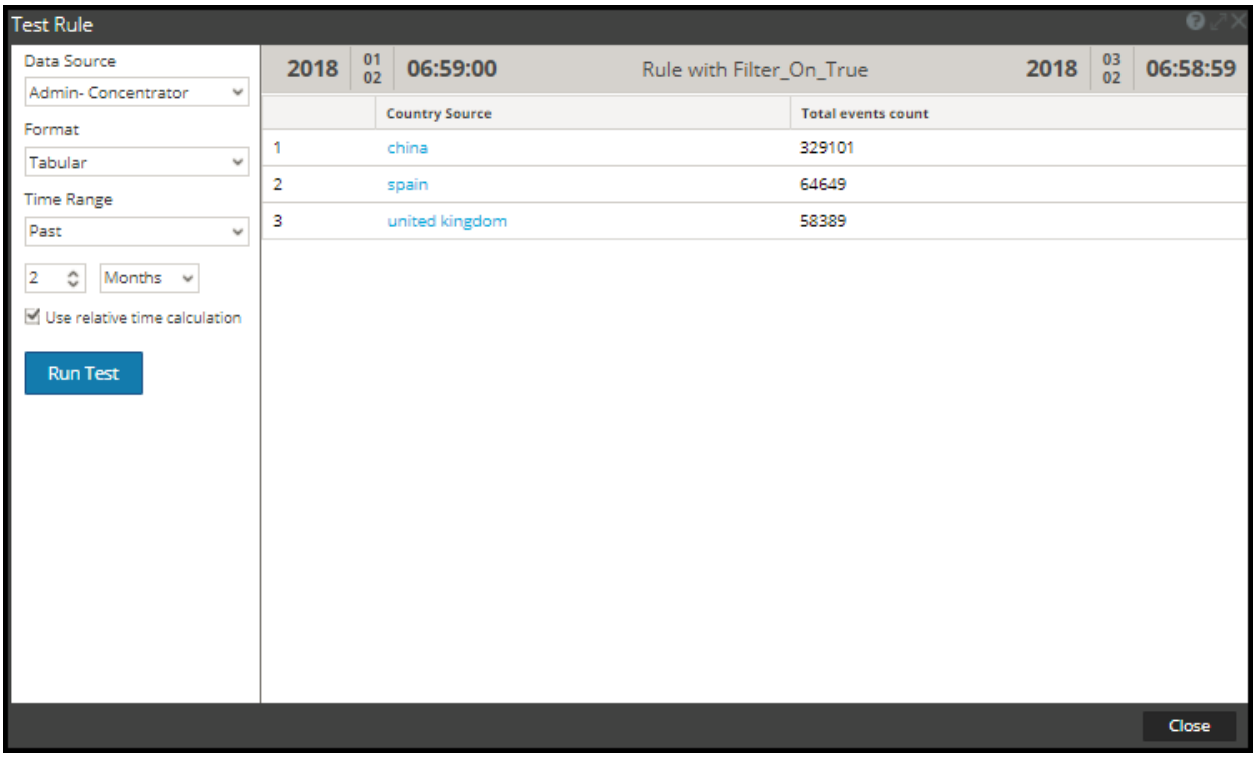
Example:

The following figure displays the list of countries and their event count.

The following figure shows a filter_on rule action to filter out countries except Spain, China, United States and United Kingdom from the result set.



The following figure shows the output with the filter_on rule action.



Another way of filtering out the entries from the result set is to create a list of variables which you want to filter out. For example, you can create a list with United Kingdom, France and Germany as values in the list. You can use this list in the rule action to get the same result set. For example, if you create a list called COUNTRY_LIST, you can use the list as follows:

```
filter_on ('$COUNTRY_LIST', 'country.src', 'false');
filter_out (string filter, string field)
filter_out (string filter, string field, bool matchExact)
```

filter_out removes the values that contain the *filter* criteria from the result set. If the result set contains multiple fields, you must select a specific field to which the filter is applied (for example, you can use a lookup_and_add to add results to a single result set).

The matchExact parameter determines if the match is an exact match or contains a match.

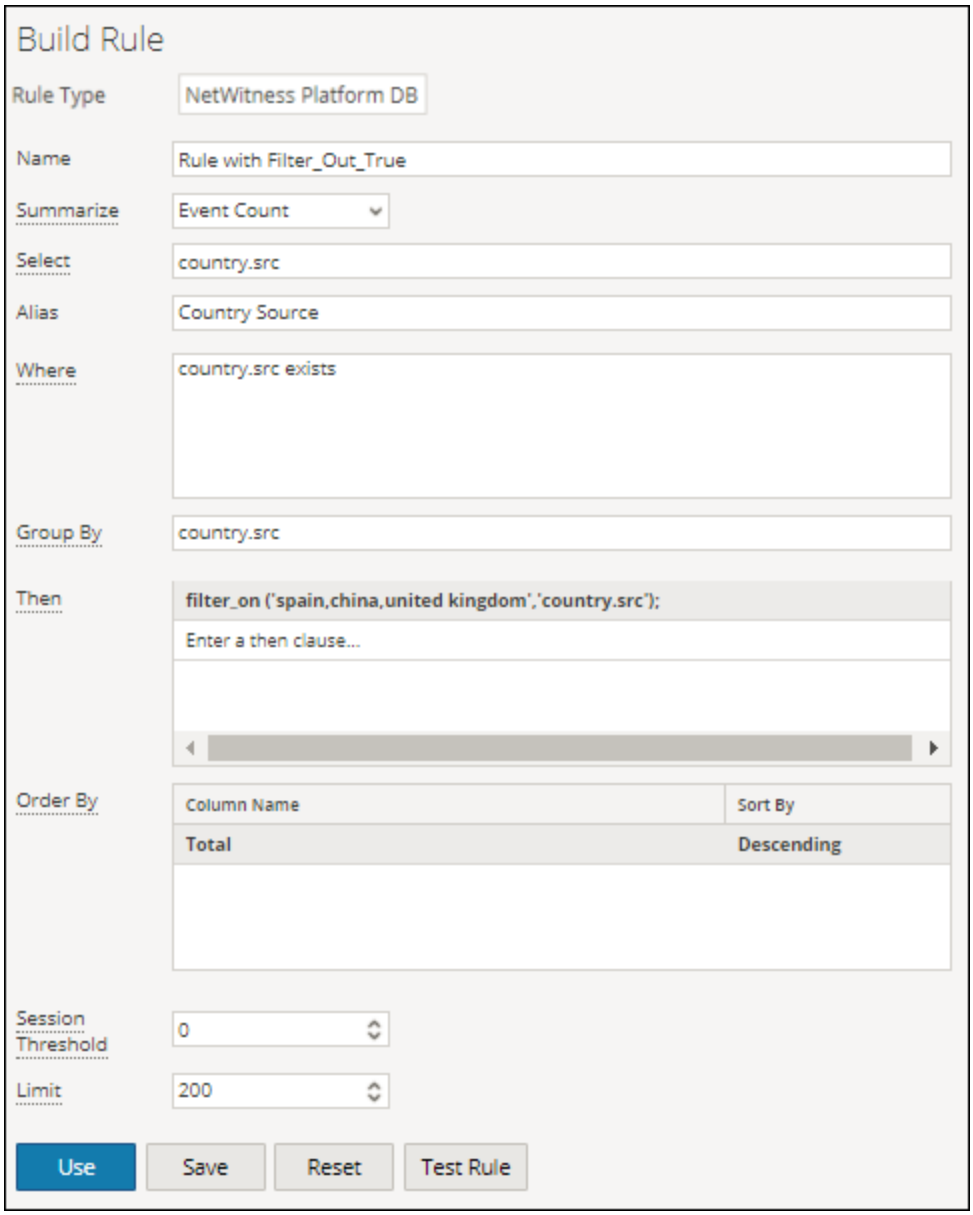
- If matchExact is set to false, any value that contains the filter text is considered a match.
- If matchExact is set to true, only values that match the provided filter text is excluded from the result set.

Note: Unless the `matchExact` parameter is specified, the default behavior of the rule action is to match exactly the text specified in the filter parameter. To specify that results containing the filter text must be removed from the result set, users must set the `matchExact` parameter to false.

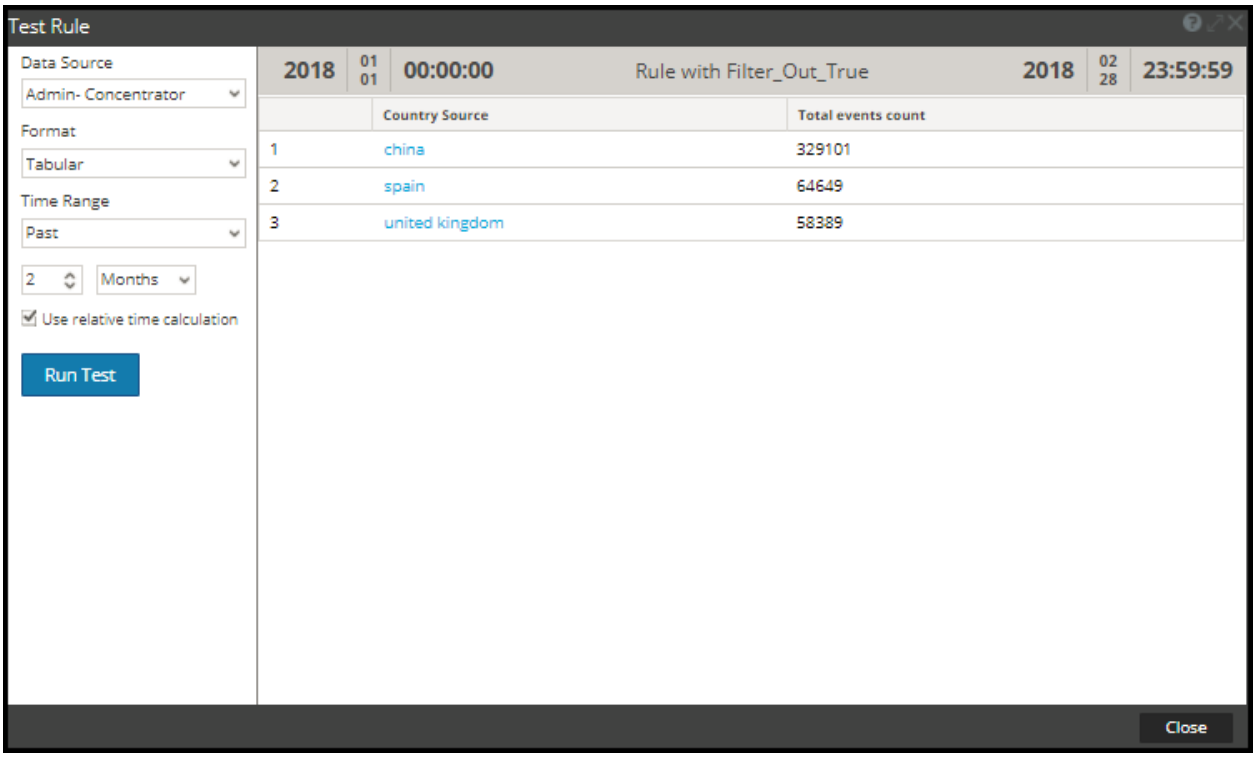
Example:

The following figure displays the list of countries and their event count.

The following figure shows the filter_out rule action to remove the event count for Spain, China, United States and United Kingdom from the result set.



The following figure shows the output with the filter_out rule action.




```
lookup_and_add (string select, string field)
lookup_and_add (string select, string field, int limit)
lookup_and_add (string select, string field, int limit, boolean inherit)
lookup_and_add (string select, string field, int limit, boolean inherit, string extraWhere)
lookup_and_add(string select, string field, int limit, boolean inherit, string extraWhere, boolean aggregate)
```

This rule action iterates through a list of values in a result set and lookup additional meta data to further describe the relationships between various elements in a result set.

Note: The lookup_and_add rule action can be used only with an aggregate rule.

The first parameter, select, designates the type of meta data that must be added to elements of the result set. The second parameter, field, specifies where in the result set the append must apply to. Also, a limit can be applied to avoid crowding the result set with a large result set.

By default, subsequent queries to the SDK will inherit the where clause of the parent rule. To use a unique where clause, you can specify a boolean value in the fourth parameter as false and in the fifth parameter you can specify a different where clause.

Note: If you are using a unique where clause in your query, make sure that you use a single quote (') for enclosing arguments and double quotes (") for string values.

Now, with the addition of **Custom** summarization and **Group By** feature, the result can be achieved even without having lookup_and_add rule action. The new rule syntax with groupby displays the result in a flat structure which is better than the earlier rule syntax without groupby Hence it is recommended to manually edit/update rules with lookup_and_add rule action and use groupby clause wherever it is applicable.

Note: Lookup_And_Add rule action is supported only if the SELECT clause has one meta and aggregate function.

For example, see below scenarios: In Example **2a**, lookup_and_add rule action is used. Instead of using lookup_and_add rule action, the same result can be achieved by using **Custom** summarization and **Group By** feature. See Example **2b** below.

But, lookup_and_add rule action is still supported for NWDB rules on the following conditions:

- All versions of NWDB rules with Summarization as Event Count, Packet Count, or Session Size.
- For Custom summarization, the lookup_and_add rule must have only one group by meta with only one aggregate function where the aggregate function must be either sum() or count().

Note: It is not supported for “Summarize-None”.

For example, lookup_and_add rule action can be used for the following rules:

- select ip.src, sum(size) group by ip.src
- select ip.src, count(filename) group by ip.src

It cannot be used for the following rules:

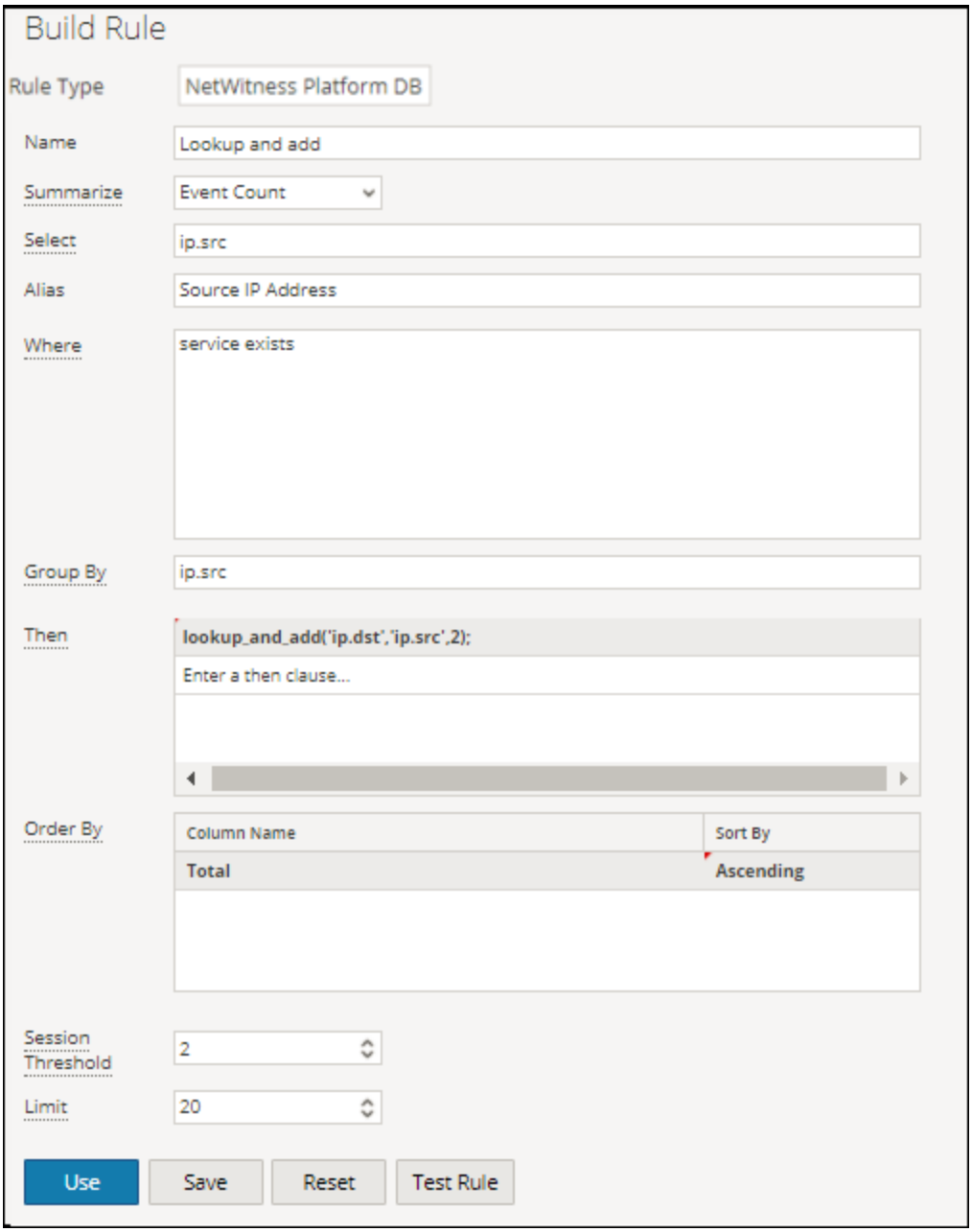
- select ip.src, sum(size),count(filename) group by ip.src
- select ip.src, sum(size),avg(size) group by ip.src
- select ip.src,ip.dst count(filename) group by ip.src,ip.dst

Examples:

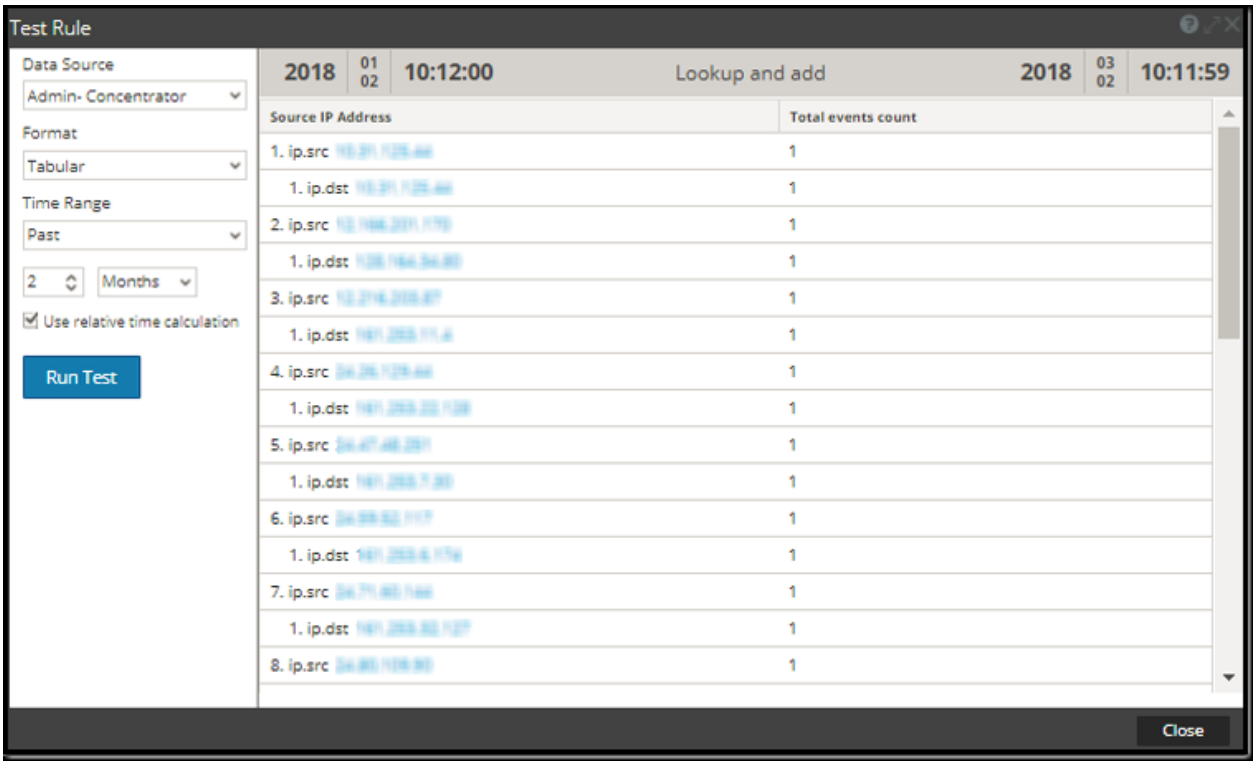
1. lookup_and_add('ip.dst','ip.src', 2);

This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src.

The following figure shows the rule definition.



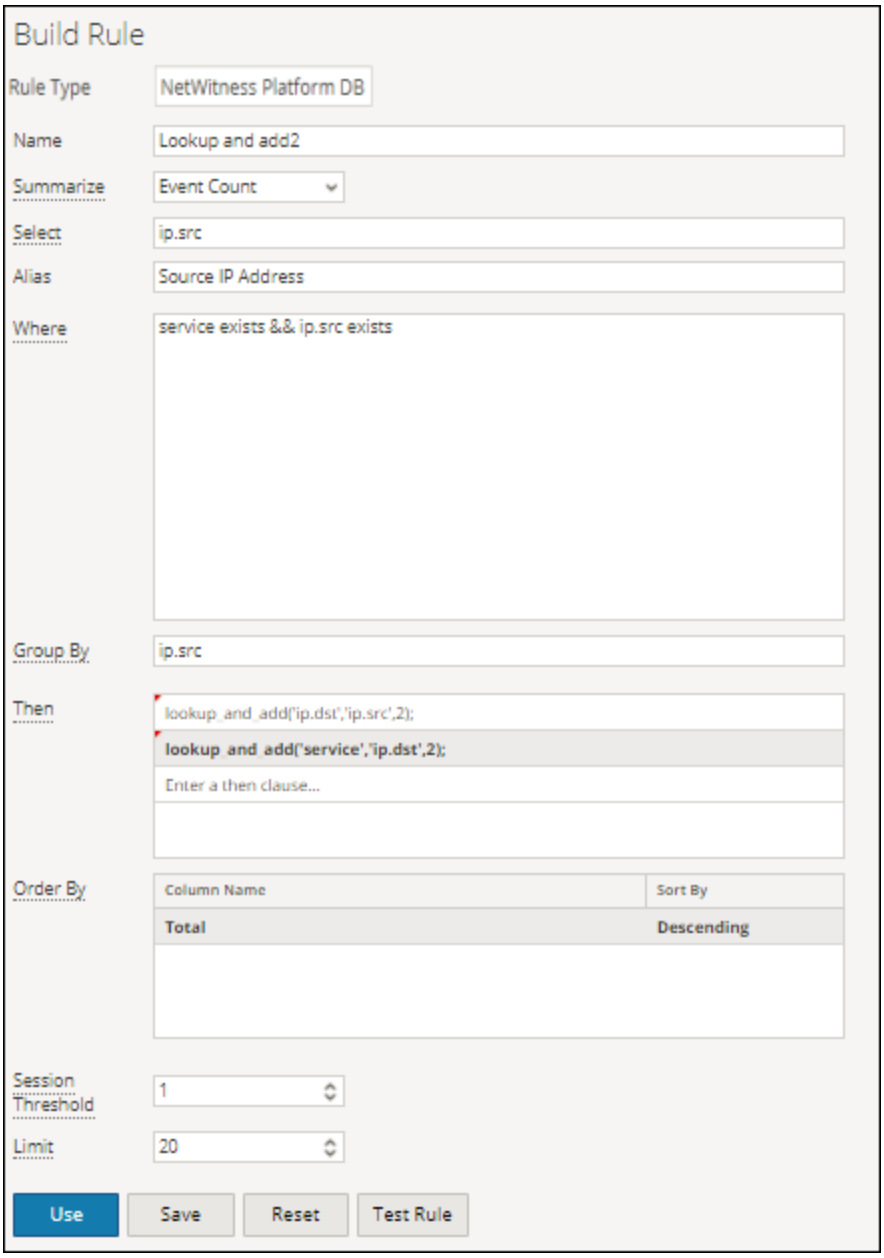
The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src.



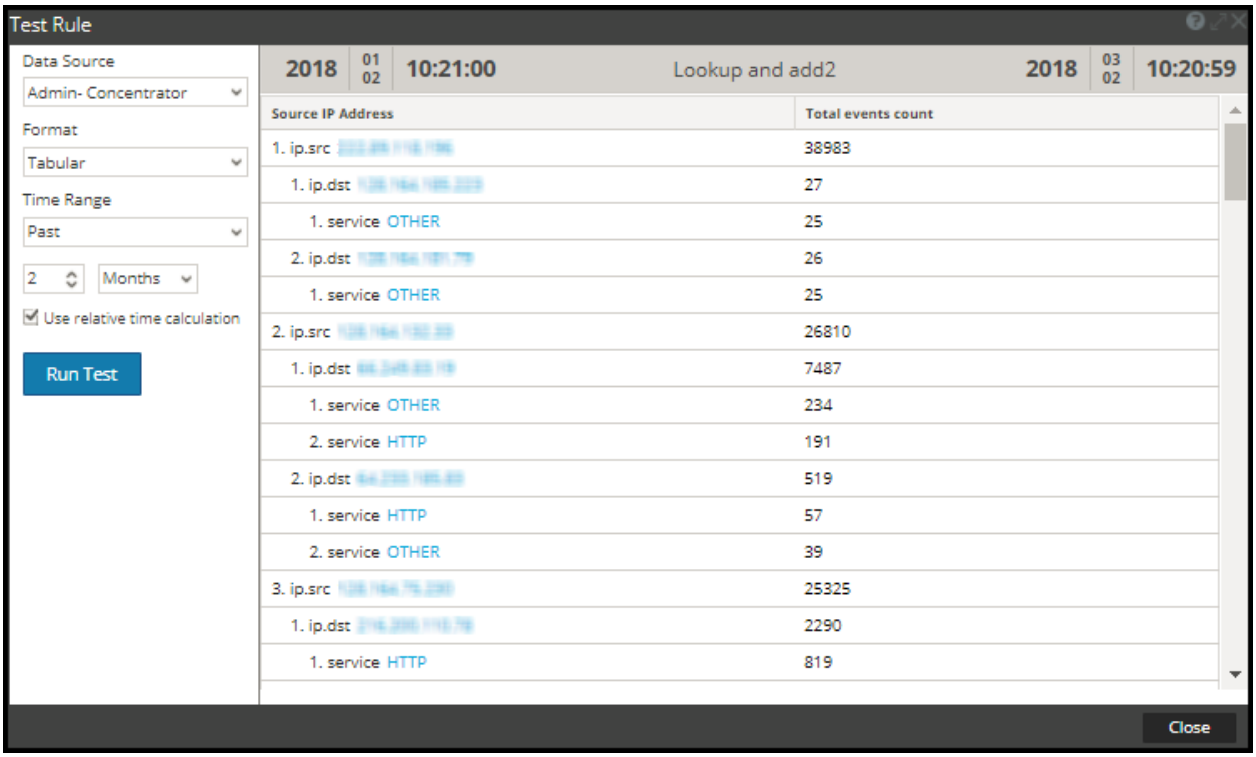
2a. lookup_and_add('ip.dst','ip.src', 2); lookup_and_add('service','ip.src', 3);

This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.

The following figure shows the rule definition.



The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.

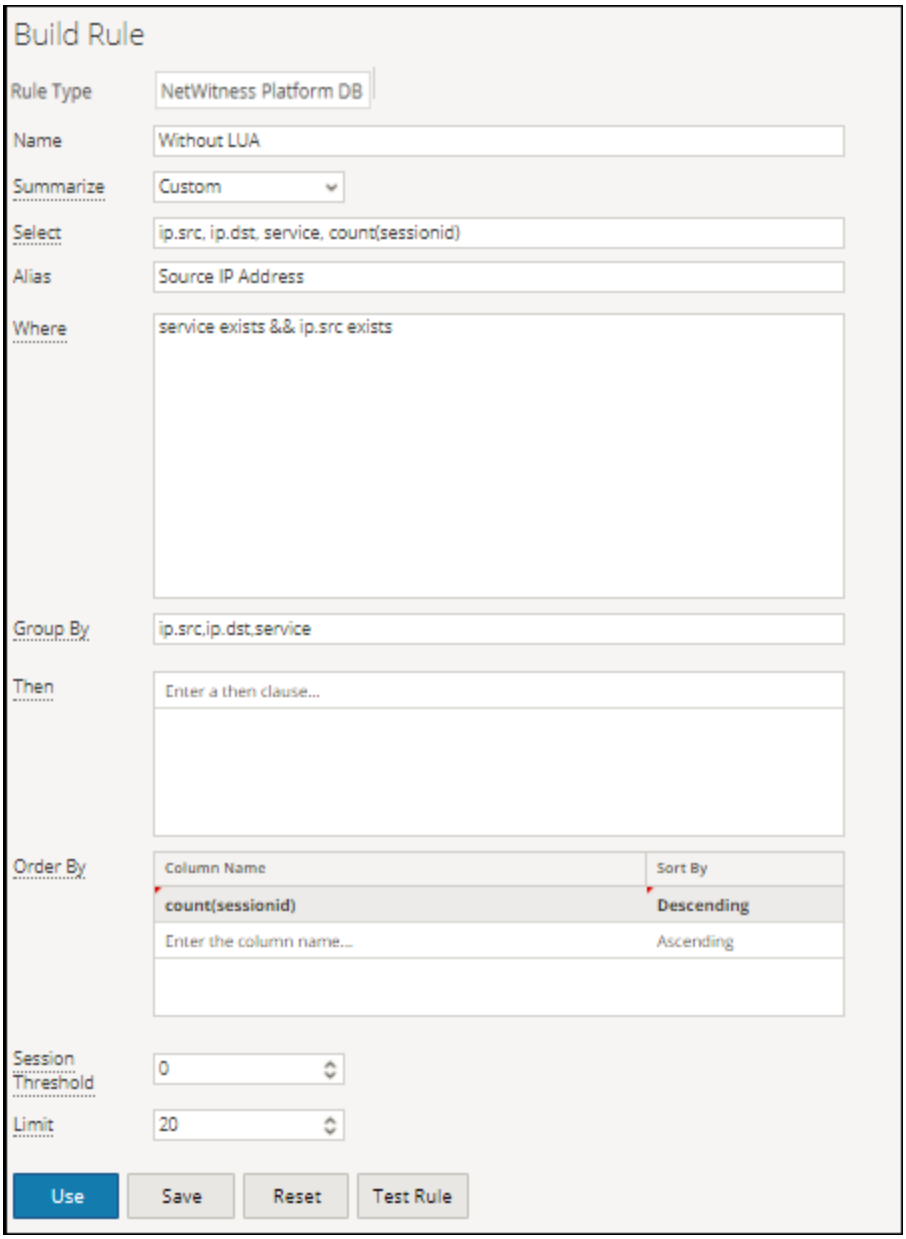


You can make the query as complex as you want by selecting different fields in the result set and by appending to different parts. For example, you may want to know what files each source IP had touched. However, because the parent rule has a WHERE clause of service = 6667 and the default behavior of this rule action is to append to the original WHERE clause, it becomes necessary to override the parent WHERE clause. The easiest way to understand this concept is to look at the previous lookup_ and_add call lookup_and_add('ip.dst','ip.src',2). The actual query that is sent to the server is SELECT ip.dst WHERE service = 6667 &&ip.src = 206.42.199.194. In order to force the WHERE clause to override the service = 6667 portion of the WHERE clause (inherited from the parent rule), the user can specify a 4th parameter of false as shown in example 3.

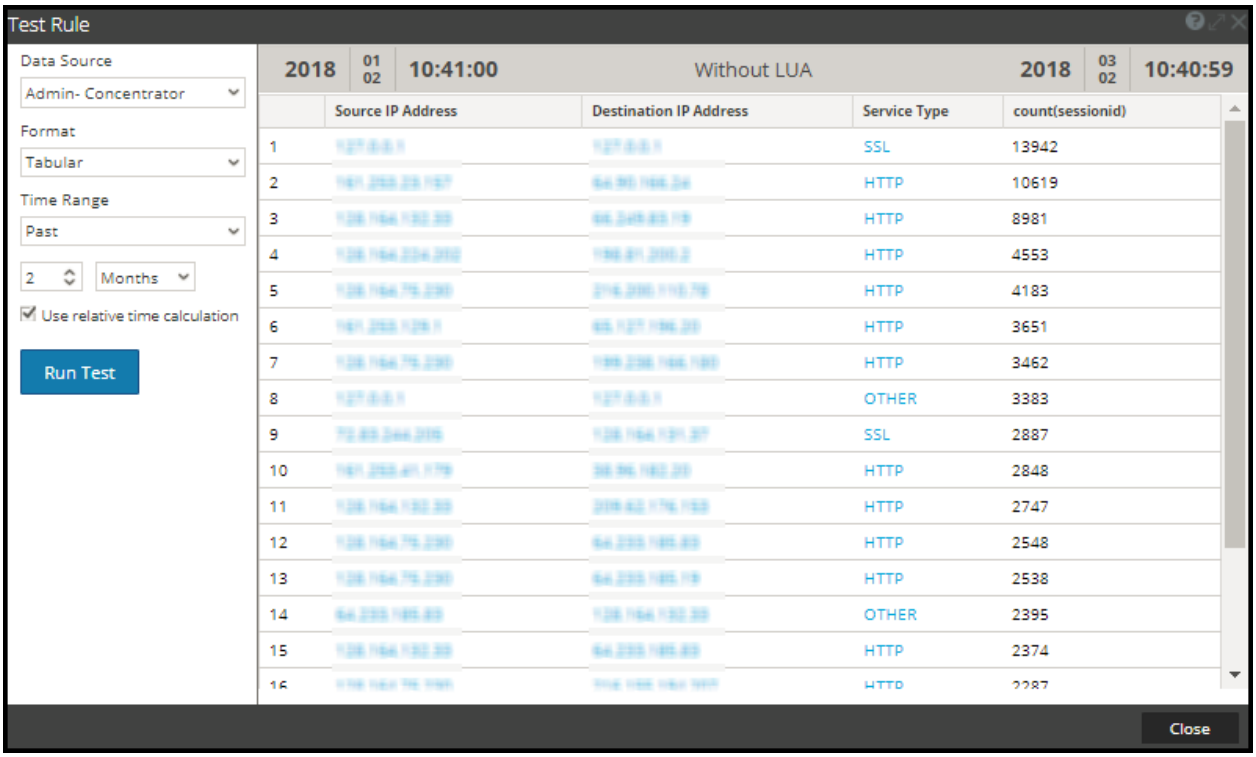
2b. Without Lookup_and_add Rule

This rule uses the Custom summarization and Group By feature to sort the results.

The following figure shows the rule definition.



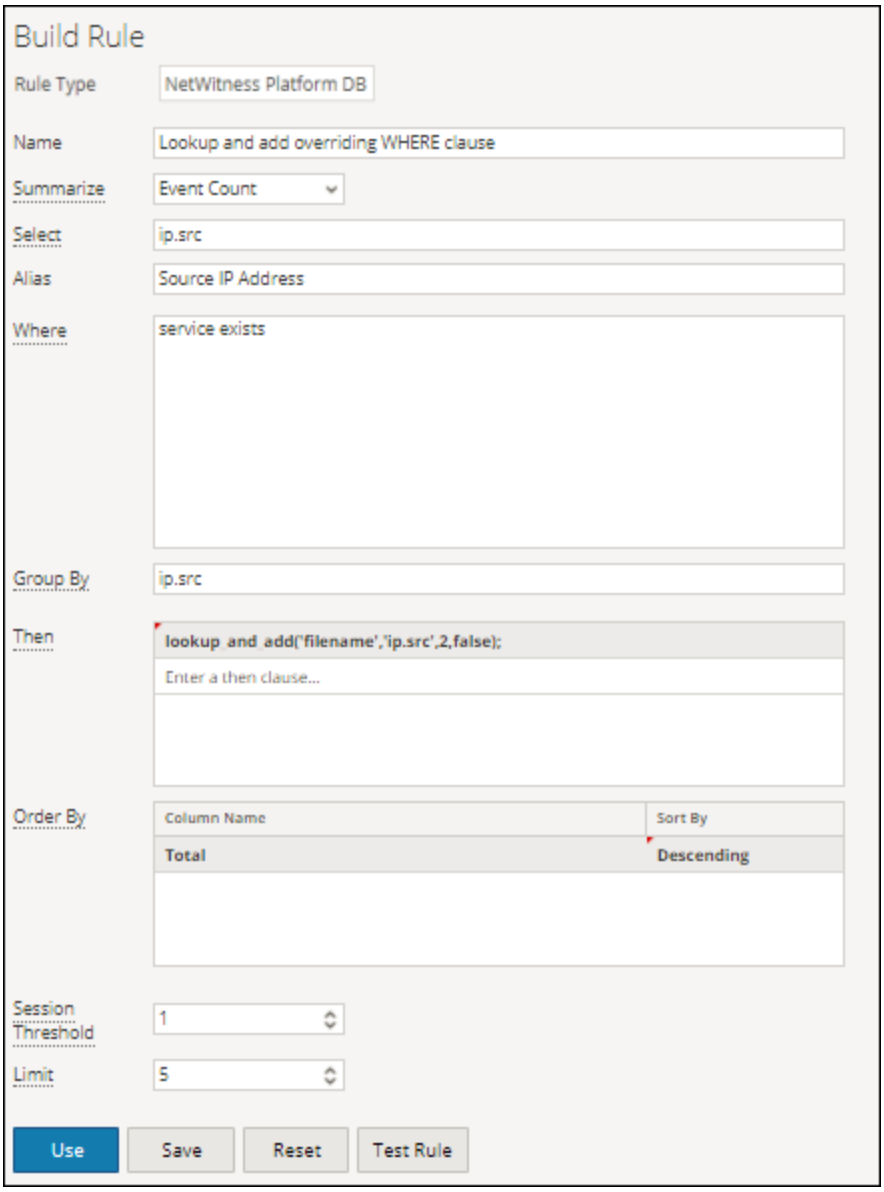
The following figure shows the result set containing the source IP addresses and the top two destination IP addresses with each ip.src and the top three ports used by each ip.src.



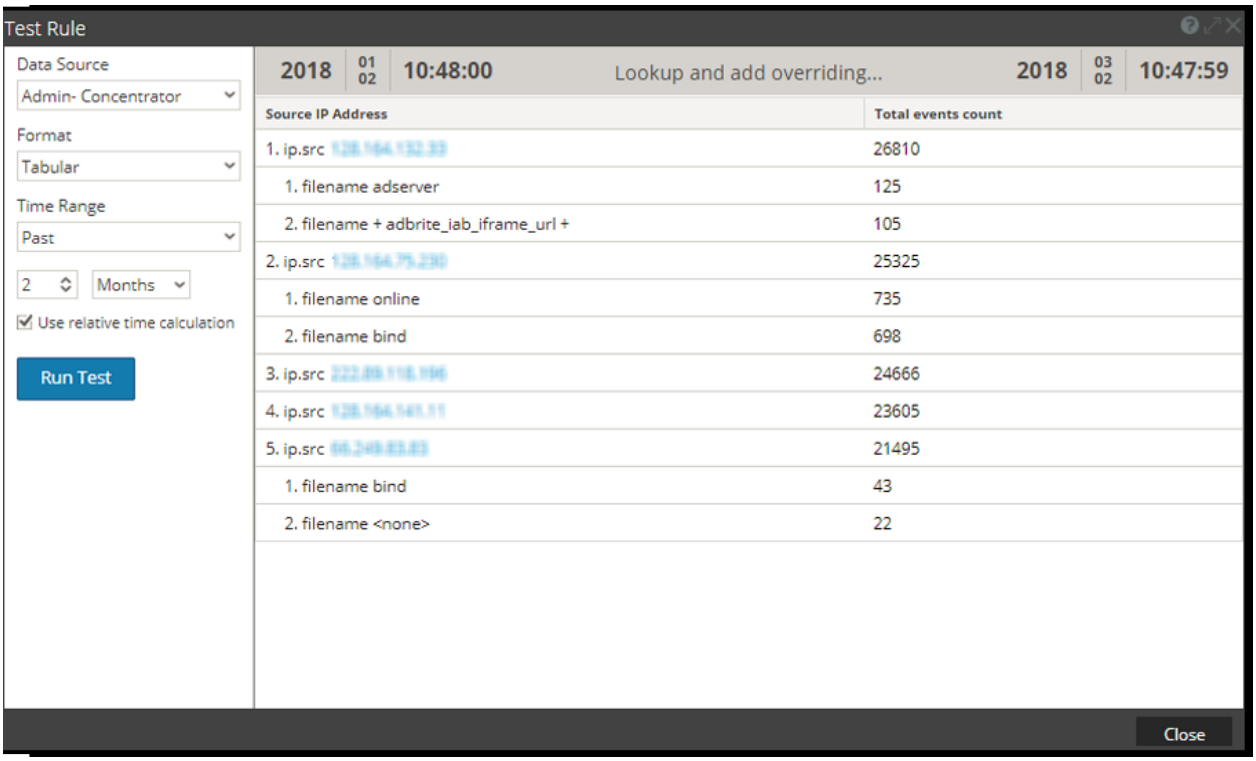
3. lookup_and_add('filename', 'ip.src', 2, false);

This call would issue a query to the server, like `SELECT filename WHERE ip.src = 90.0.0.142` rather than `SELECT filename WHERE service = 6667' && ip.src = 90.0.0.142` because you have specified the rule action to ignore the initial `WHERE` clause of the parent rule.

The following figure shows the rule definition.



The following figure shows the result set.

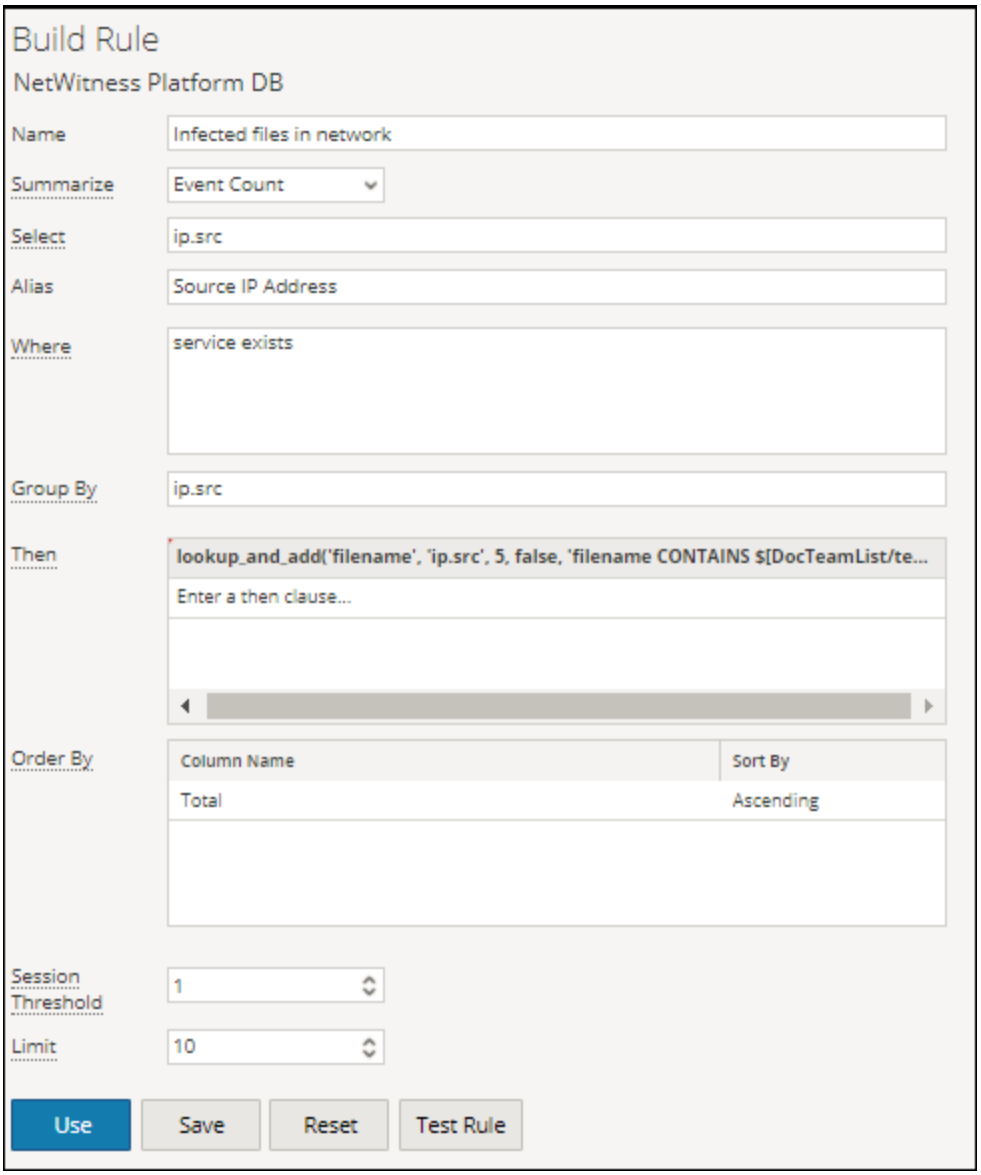


The test list is in a group name netwitness, you can access that list with the following syntax.

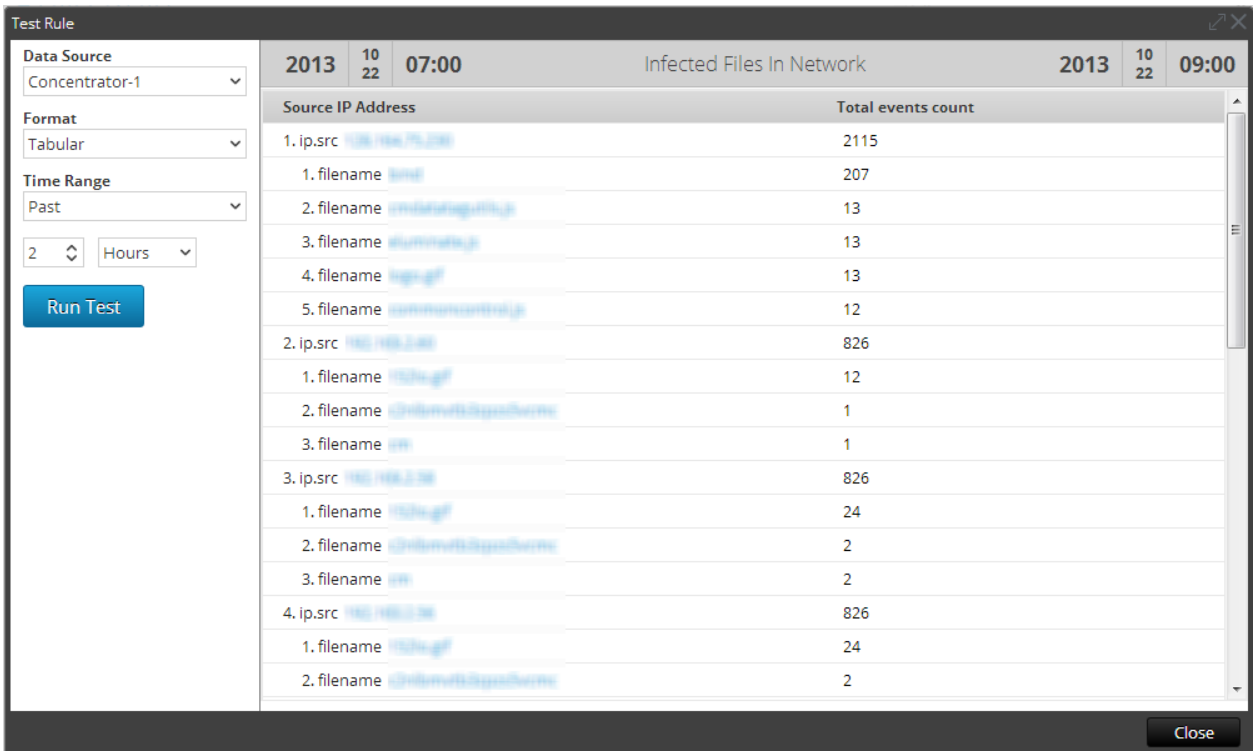
You can even narrow down these appended results even further to only include filenames that have .gif as filename extension by using the fifth parameter in the rule action. The fifth parameter allows you to specify additional WHERE clause criteria. The files with .gif filename extension would be stored in the **test** list within a group named **DocTeamList**. You can access this list with the following syntax: threat.source = $[DocTeamList/test]
This can be referenced in the extra where clause parameter in the following manner:

4. lookup_and_add('filename', 'ip.src', 5, false, 'filename CONTAINS $[DocTeamList/test]');

The following figure shows the rule definition.



The following figure shows the result set.

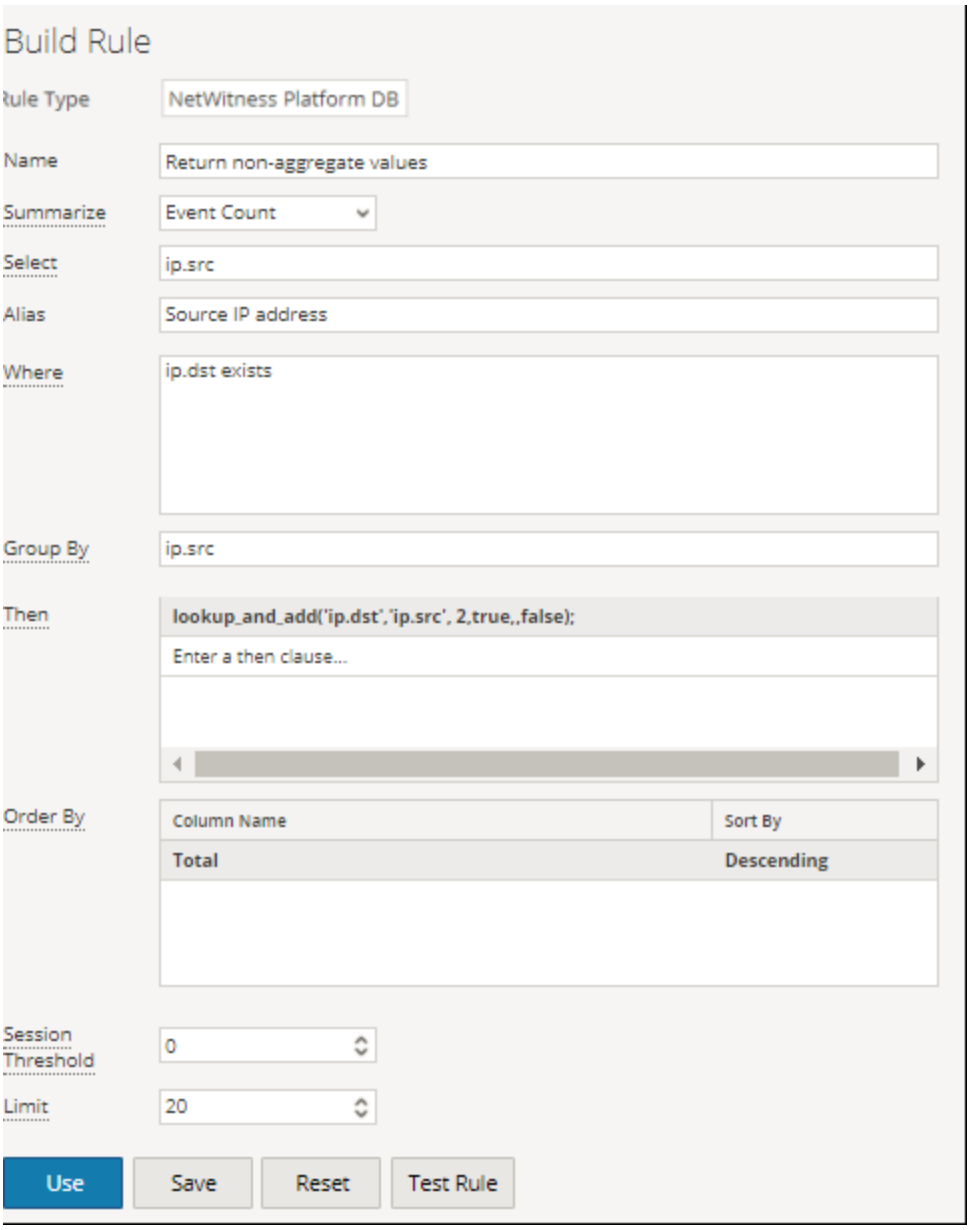


5. lookup_and_add('ip.dst','ip.src', 2,true,,false);

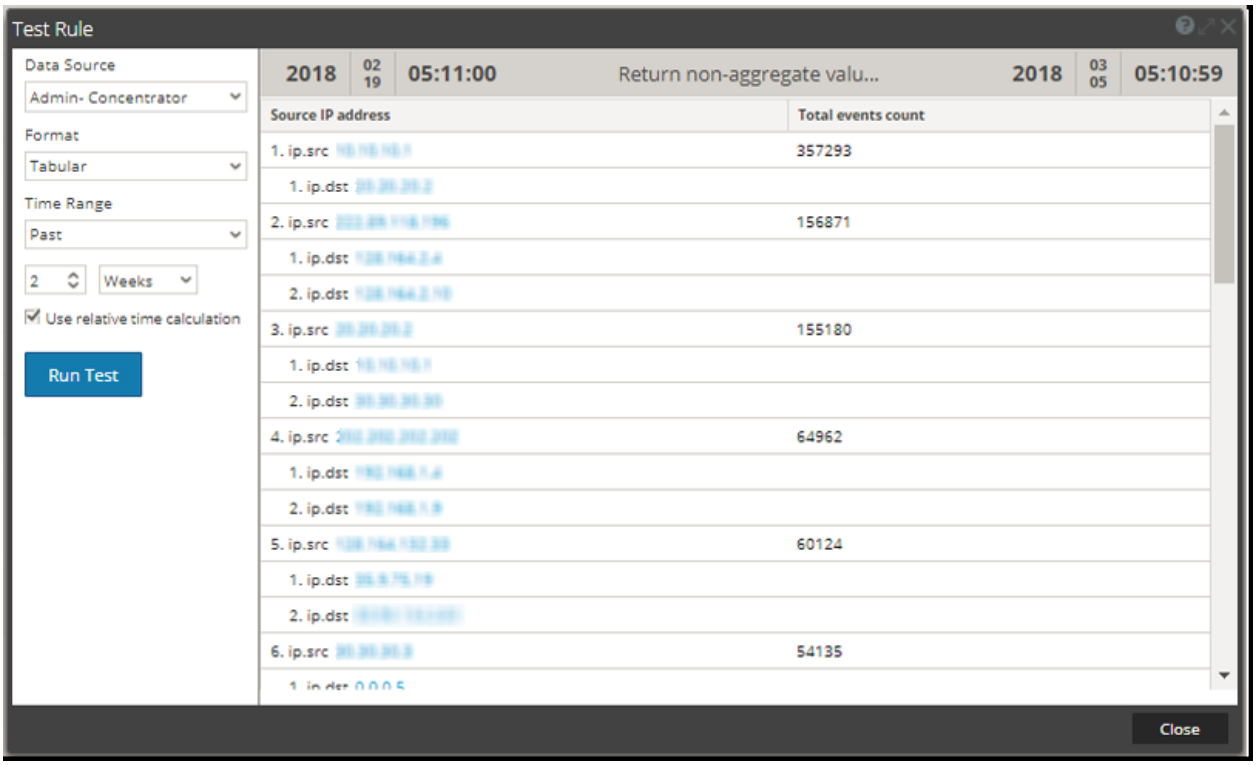
This rule action would iterate through each ip.src in the initial result set and lookup the top two destination IP addresses with each ip.src. The 'aggregate' parameter is set to 'false', this implies that aggregates would be skipped for lookup values and hence the lookup query executions will complete faster.

Note:
The default value for 'aggregate' is 'true'. When 'aggregate' is set to 'false', Reporting Engine passes threshold=1, Sort by='value' and Order=Ascending to NWDB to make lookup queries run faster.
. You must set the 'aggregate' to false, when rule contains aggregate functions or when the rule is run against a wide time range. This helps the rule to complete the execution faster.

The following figure shows the rule definition.



The following figure shows the result set.




```
max_threshold (string quantity)
max_threshold (string quantity, string field)
```

max_threshold removes any results with a quantity that is larger than the maximum threshold quantity from a result set. The quantity can either be in terms of count or size and it is relative to the sorting options of the parent rule. This means that if you sort a rule by size, the rule action expects you to specify the parameter in bytes (you can append KB, MB, GB, TB to the parameter to make size conversion easier).

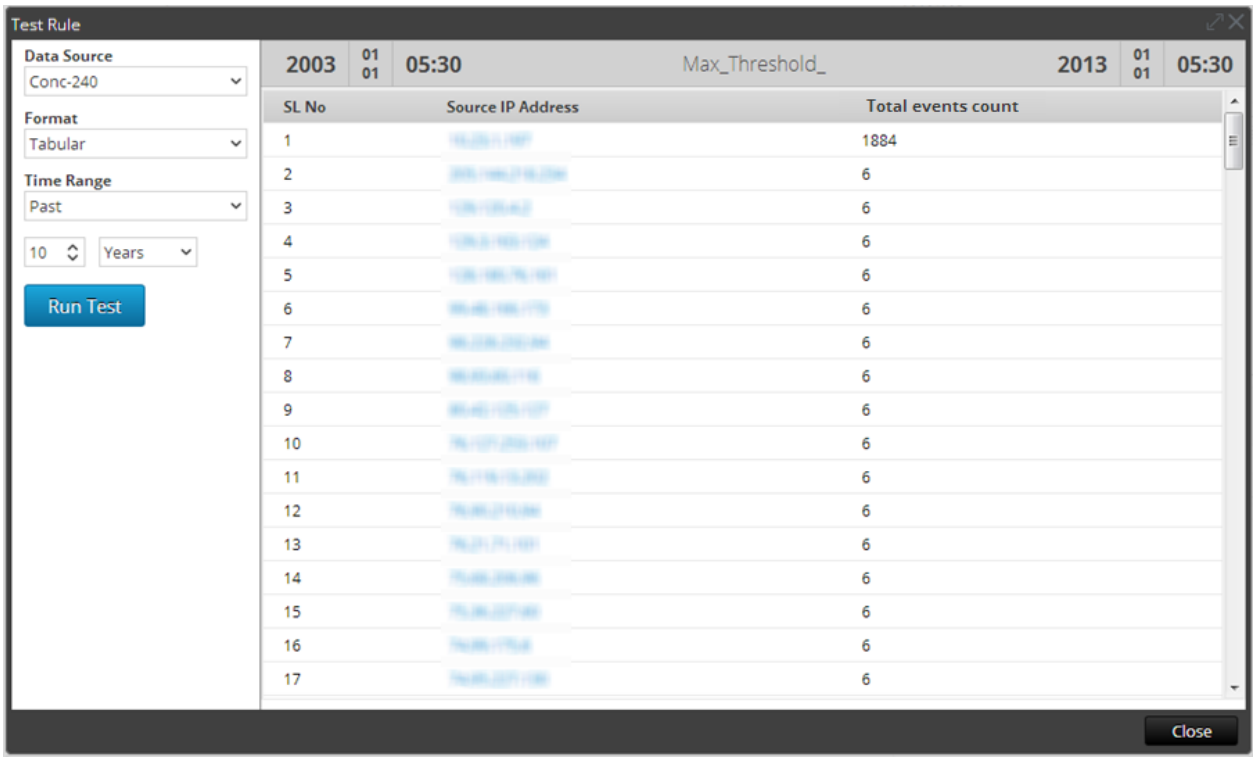
max_threshold rule can also be used to filter values based on the aggregate function values. Use the syntax based on the type of summarization used in the rule as below:

- max_threshold(String quantity): Can be used to filter Event Count, Packet Count, and Session Size.
- max_threshold(String quantity, String field): Can be used to filter values of Custom aggregates or any metas.

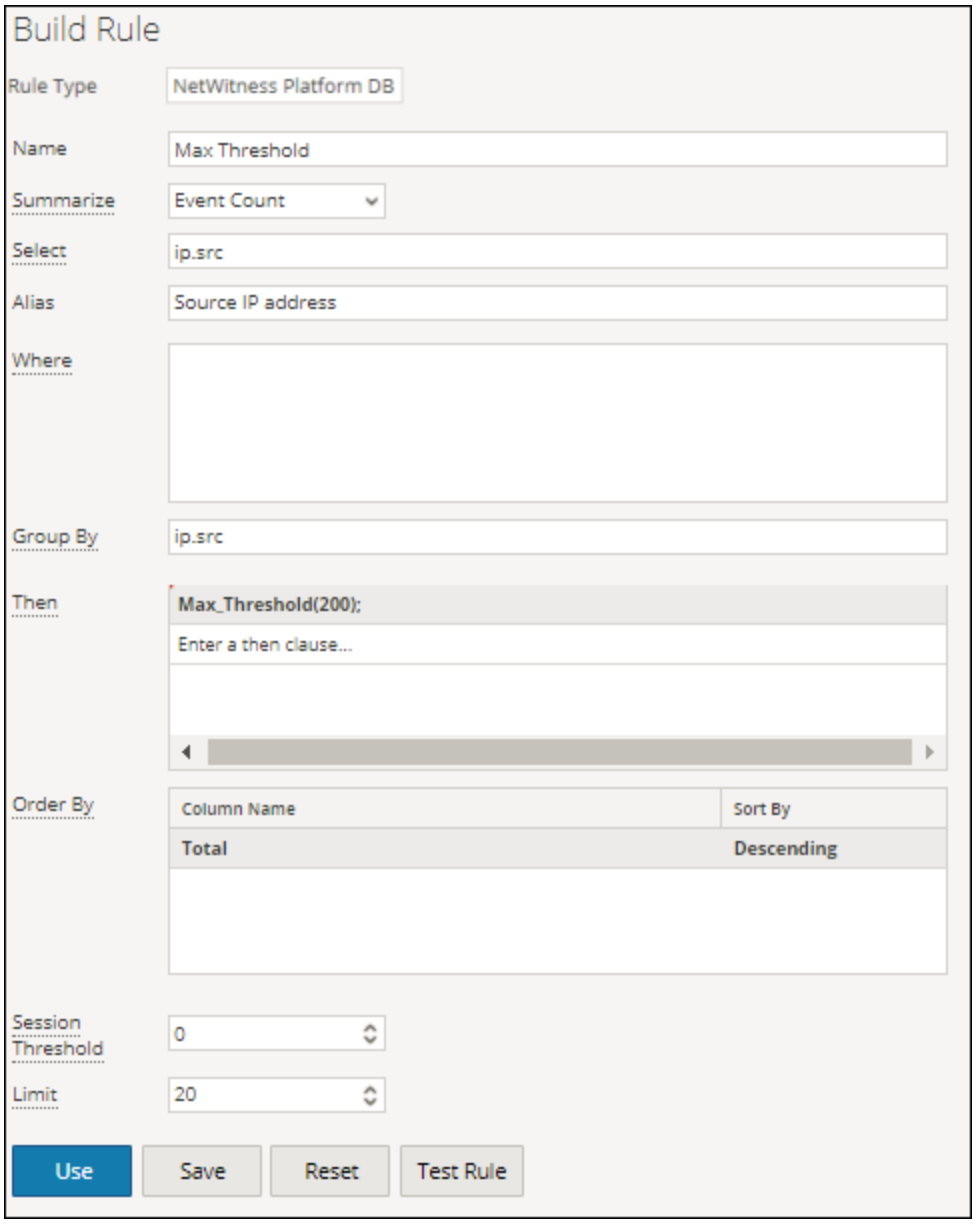
Examples:

1. max_threshold(200);

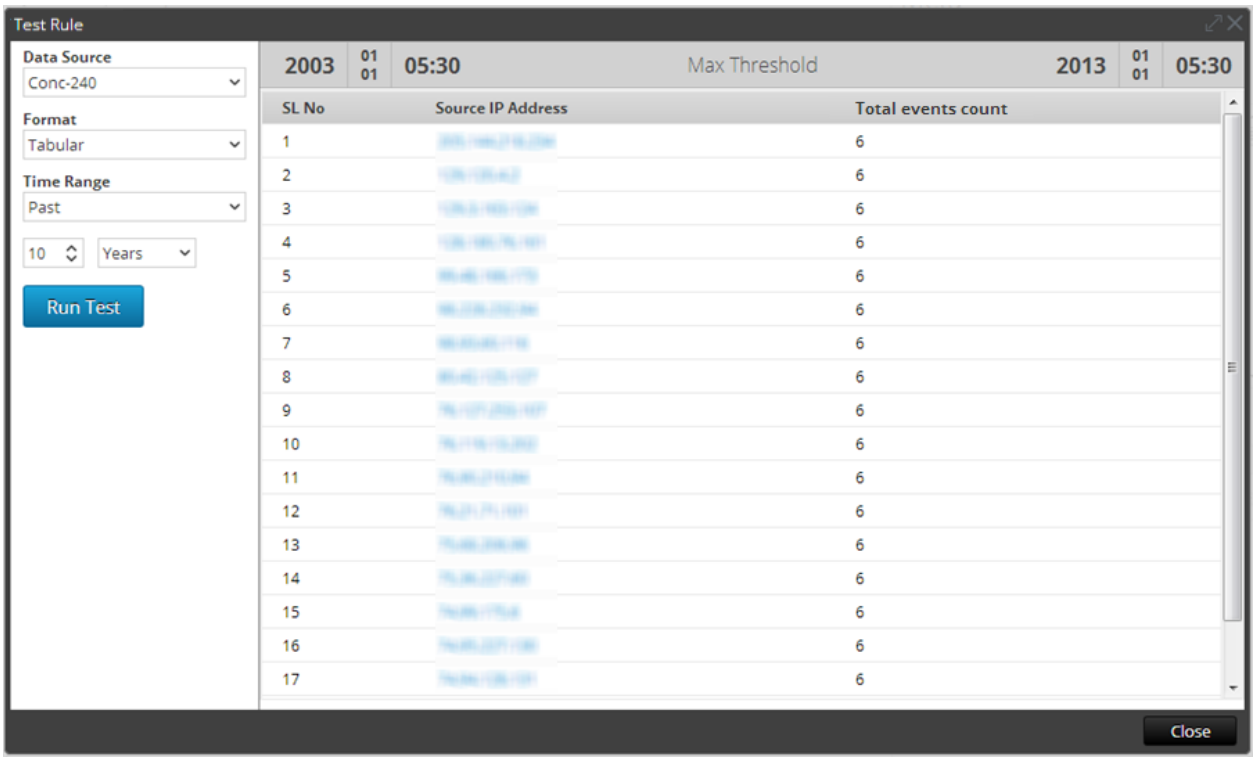
The following figure shows the result without the max_threshold argument. The output results have event counts exceeding 200.



The following figure shows a the max_threshold rule action that puts a limit of 200 bytes on the output. Any output having more than 200 bytes of data are not listed.

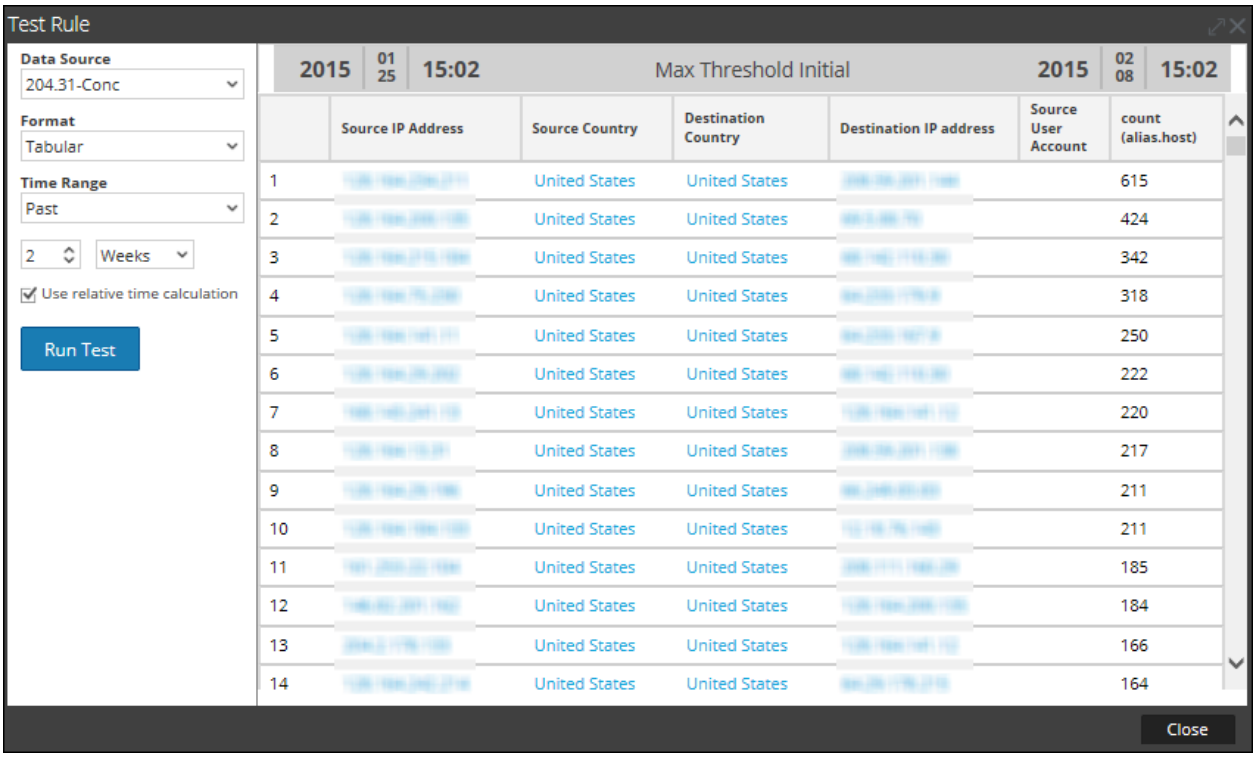


The following figure shows the result when the max_threshold rule action is applied. The result numbered 1 in the above screen capture is removed from the result.

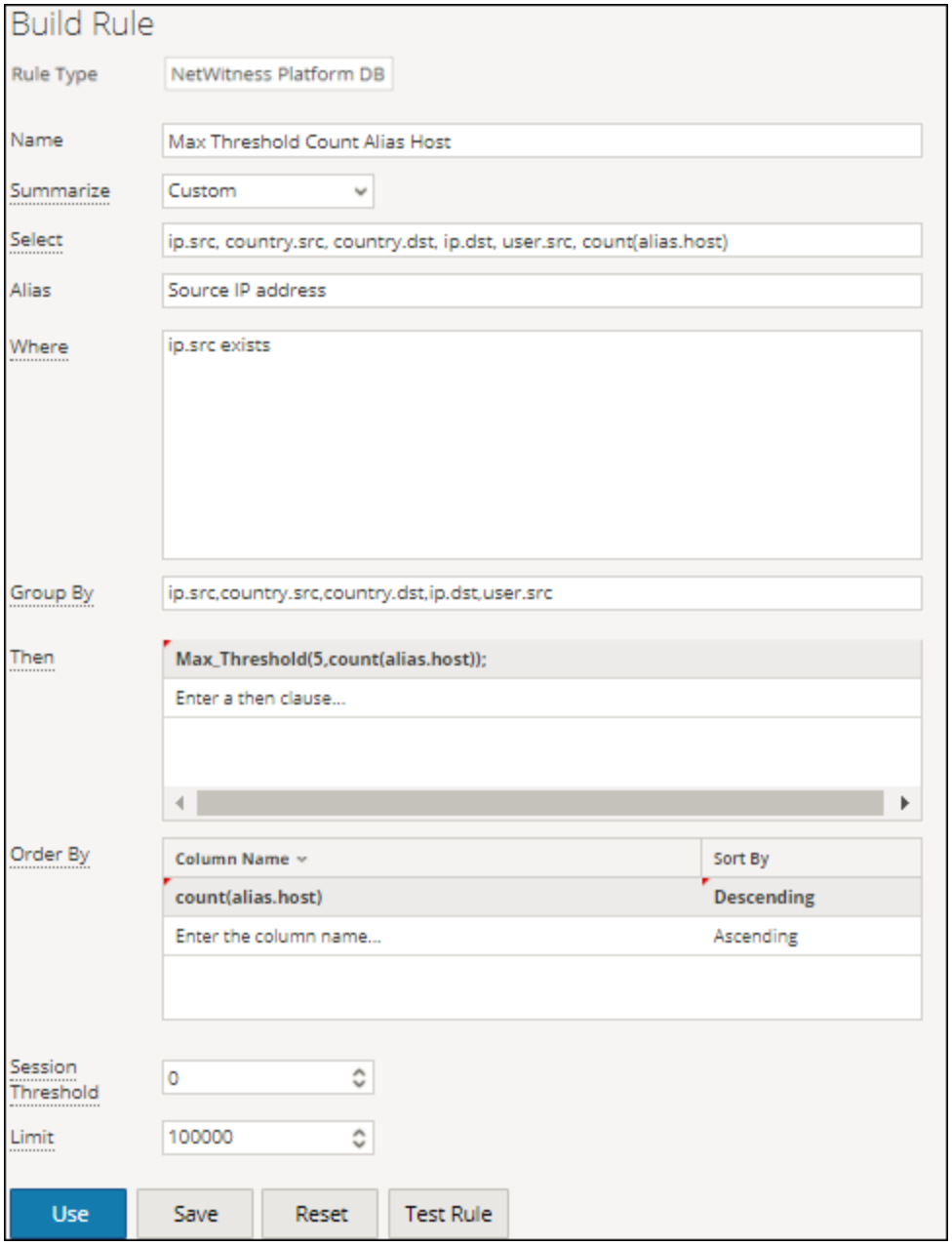


2. max_threshold(5,count(alias.host));

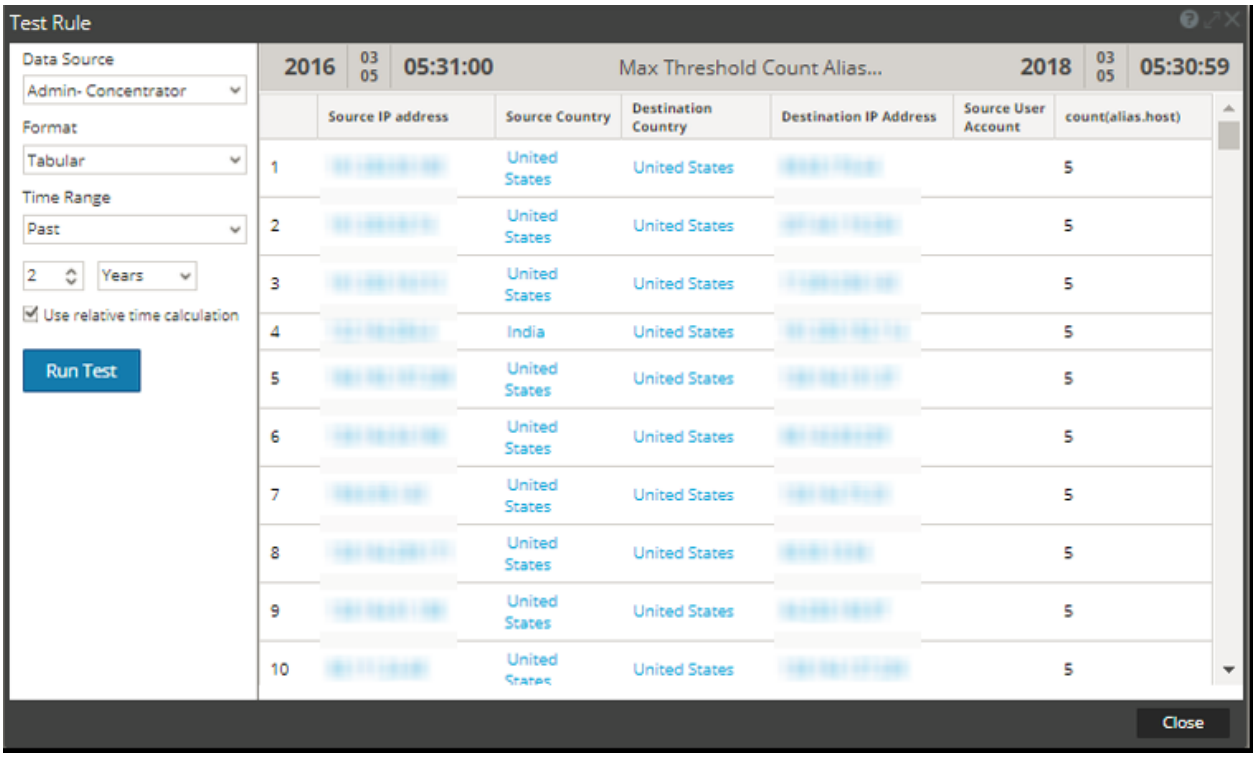
The following figure shows the result without the max_threshold argument. The output results have count of alias.host exceeding 5.



The following figure shows a the max_threshold rule action that puts a limit of 5 on the output. Any output having value more than 5 is not listed.



The following figure shows the result when the max_threshold rule action is applied. Any output having value more than 5 is removed from the result.



min_threshold (string quantity)

min_threshold removes results with a quantity that is smaller than the minimum threshold quantity from a result set. The quantity can either be in terms of count or size and it is relative to the sorting options of the parent rule. This means that if you sort a rule by size, the rule action expects you to specify the parameter in bytes (you can append KB, MB, GB, TB to the parameter to make size conversion easier).

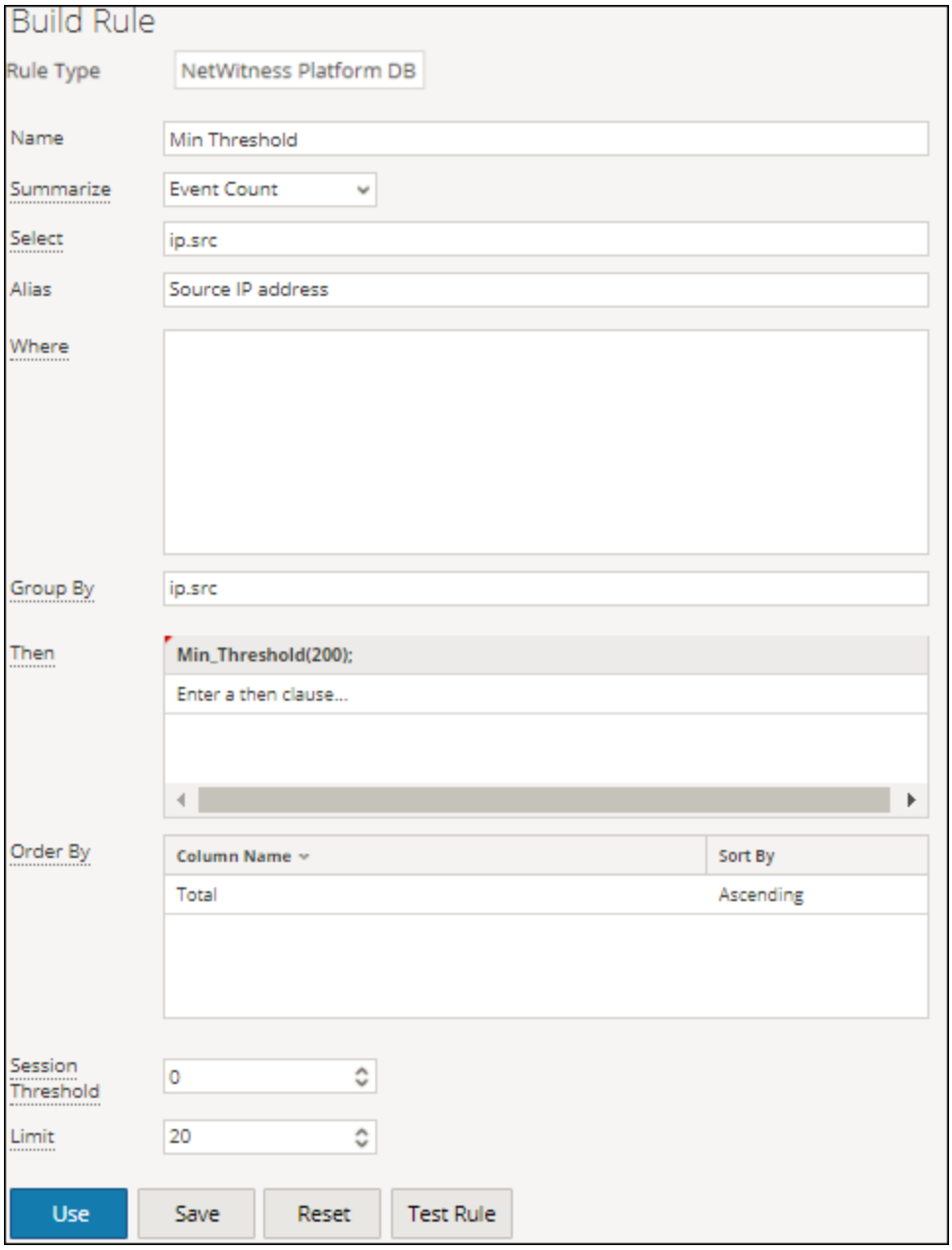
min_threshold rule can also be used to filter values based on the aggregate function values. Use the syntax based on the type of summarization used in the rule as below:

- min_threshold(String quantity): Can be used to filter Event Count, Packet Count, and Session Size.
- min_threshold(String quantity, String field): Can be used to filter values of Custom aggregates or any metas.

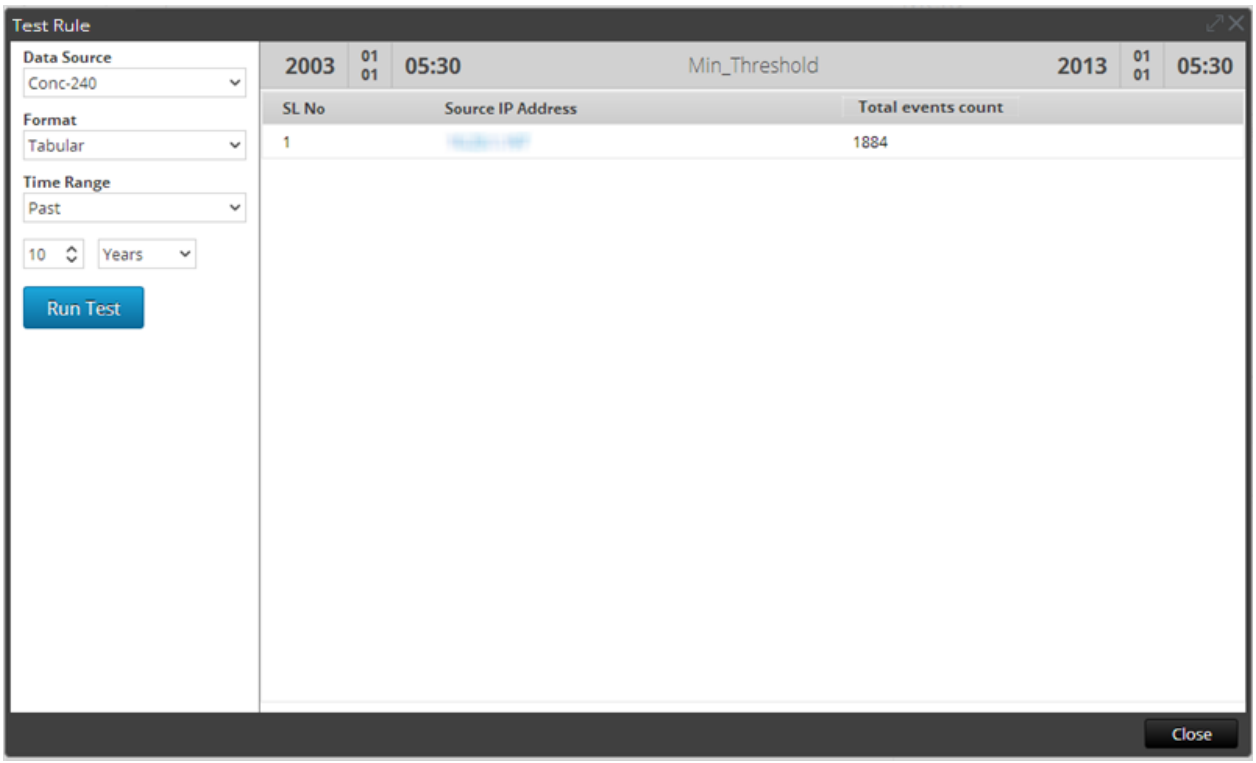
Examples:

1. min_threshold(200);

The following figure shows a sample of the min_threshold query.



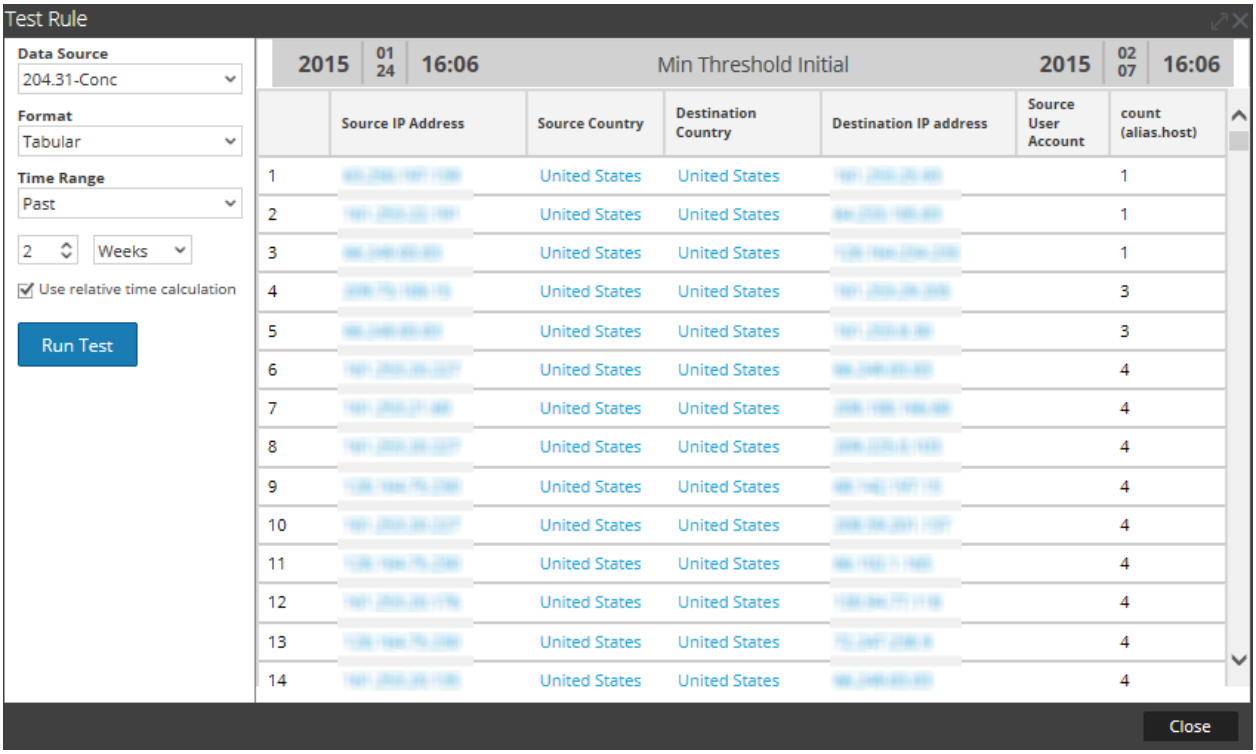
The above figure puts a limit of 200 bytes on the output. Any output having less than 200 bytes of data is not listed. The output with the min_threshold rule action is applied.



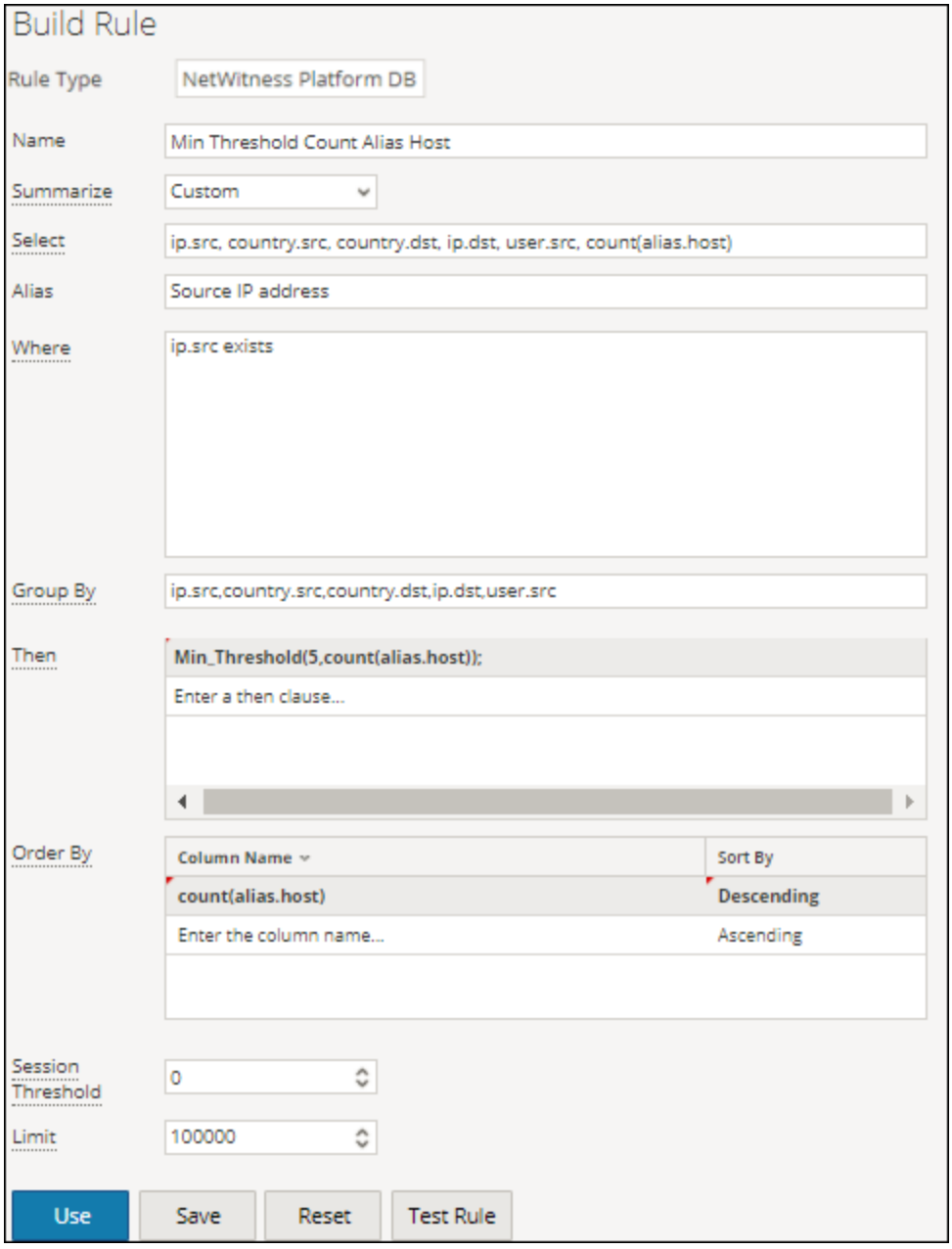
As shown, all the values are greater than 200 bytes.

2. min_threshold(100,count(alias.host));

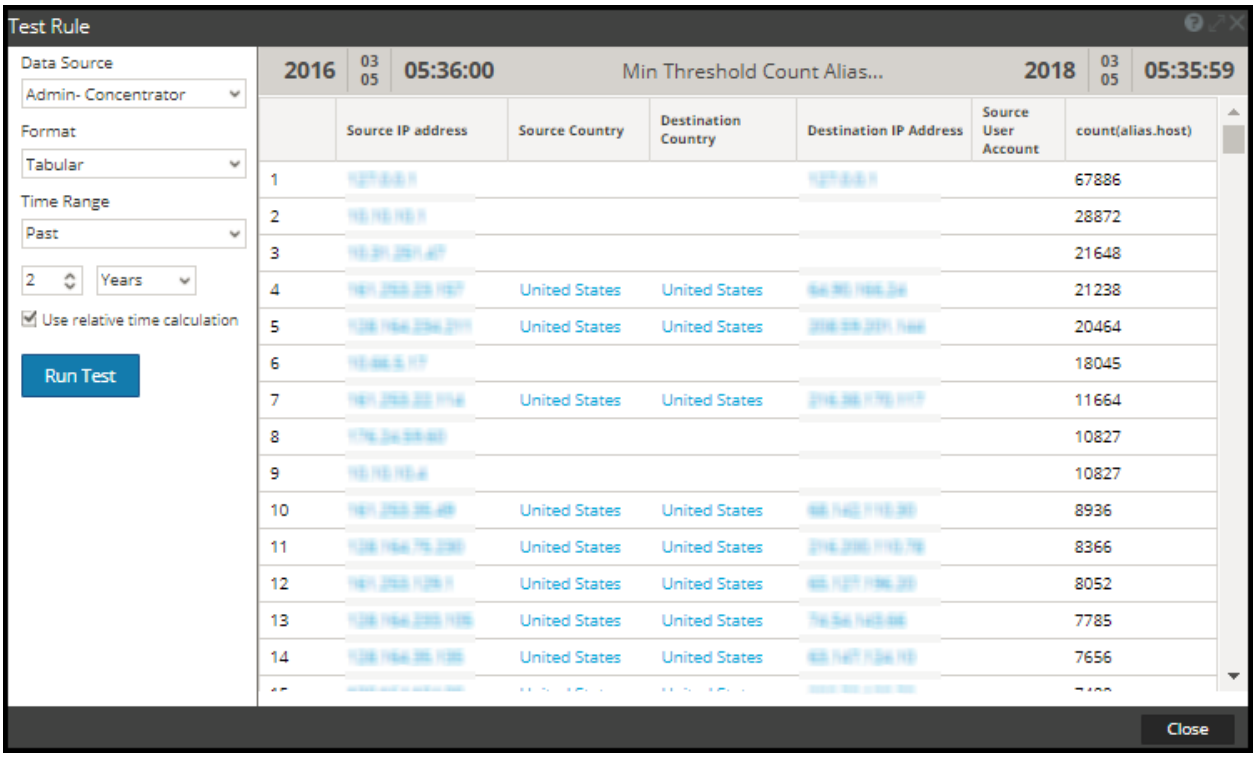
The following figure shows the result without the min_threshold argument. The output results have count of alias.host below 100.



The following figure shows a the min_threshold rule action that sets the minimum limit of 100 on the output. Any output having data less than 100 is not listed.



The following figure shows the result when the min_threshold rule action is applied. Any output having data less than 100 is removed from the result.



regex (string regex, string field)

The regex rule action applies regular expression to the result set. The following is the format of the regex rule action:

regex(regular_expression, meta_name)

Where:

- regular_expression - Regular expression to match the value of the meta.
- meta_name - Meta or field name on which the regex has to be applied.

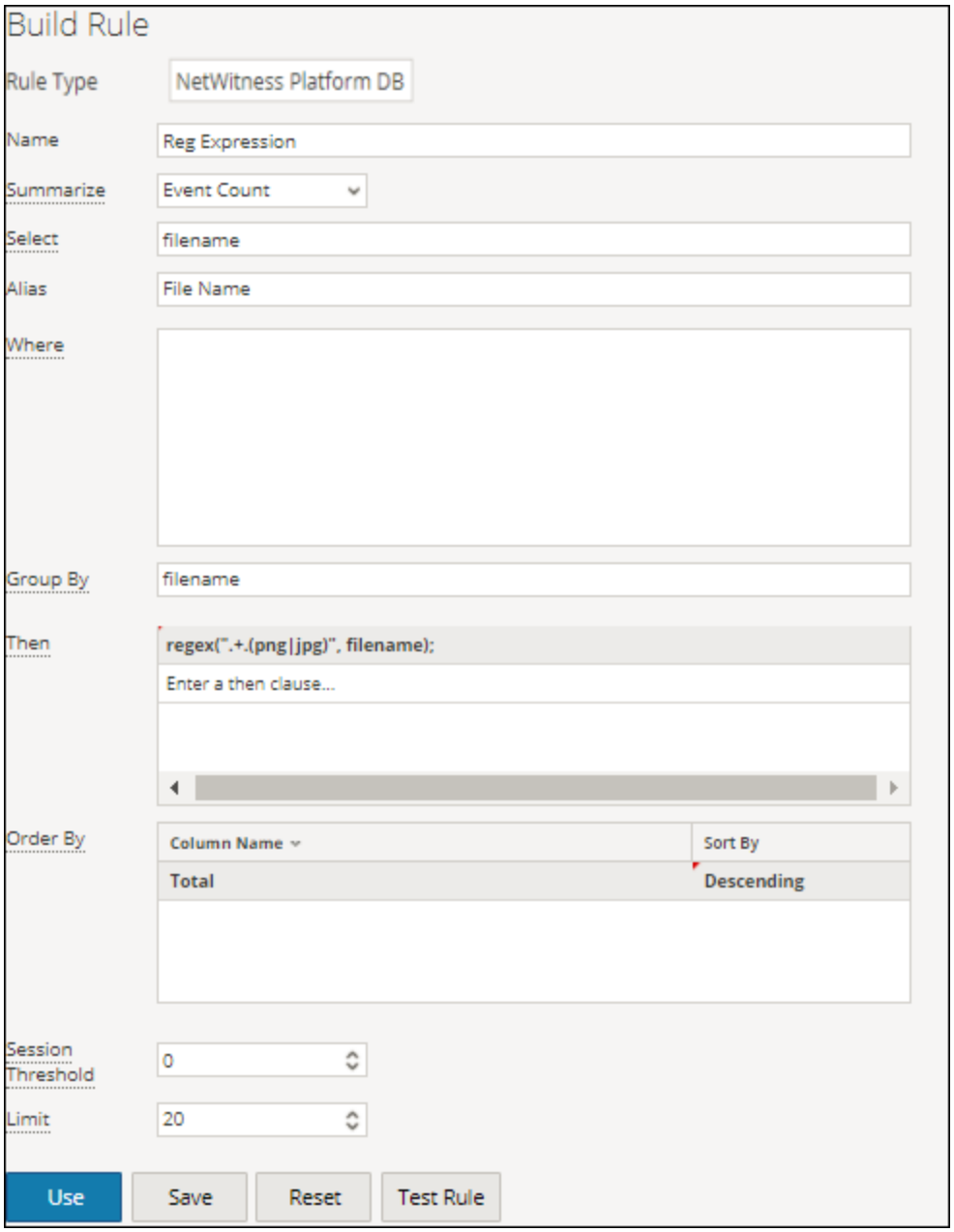
For a comprehensive list of supported regex patterns, refer to http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

Sample regex rule action:

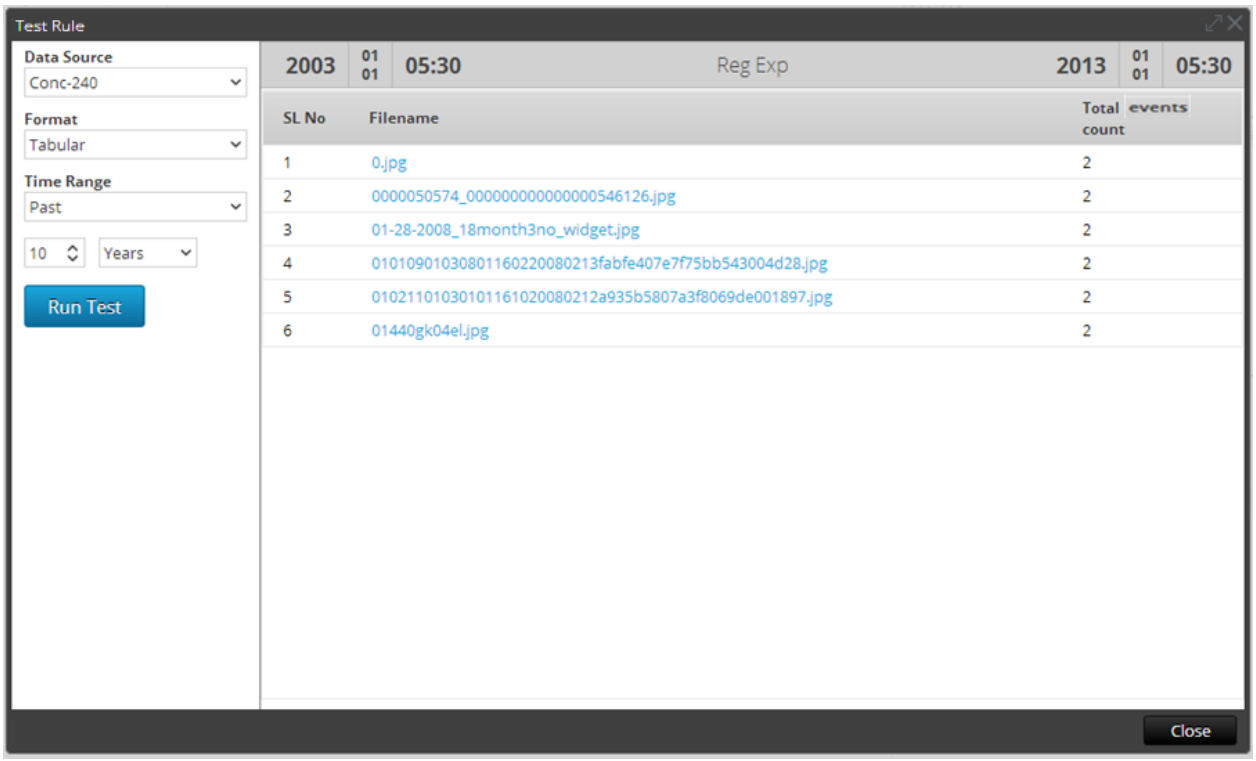
If you want to list filenames of all the PNG and JPEG format files from various sessions, you can write a rule with the following regex rule action:

regex(".+.(png|jpg)", filename);

The following figure shows the rule.



The output with the regex rule action applied is shown in the following figure.

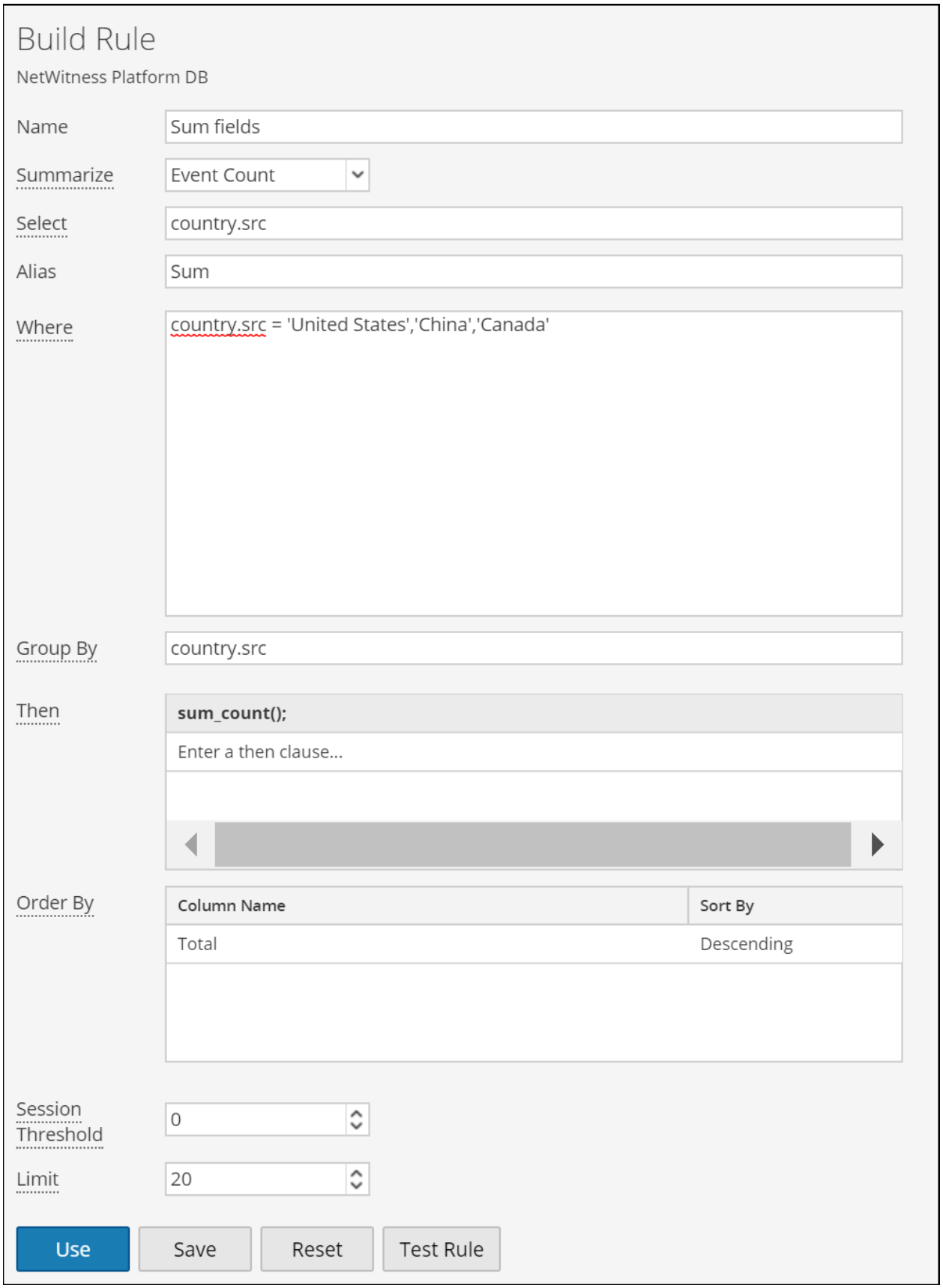


`sum_count()`

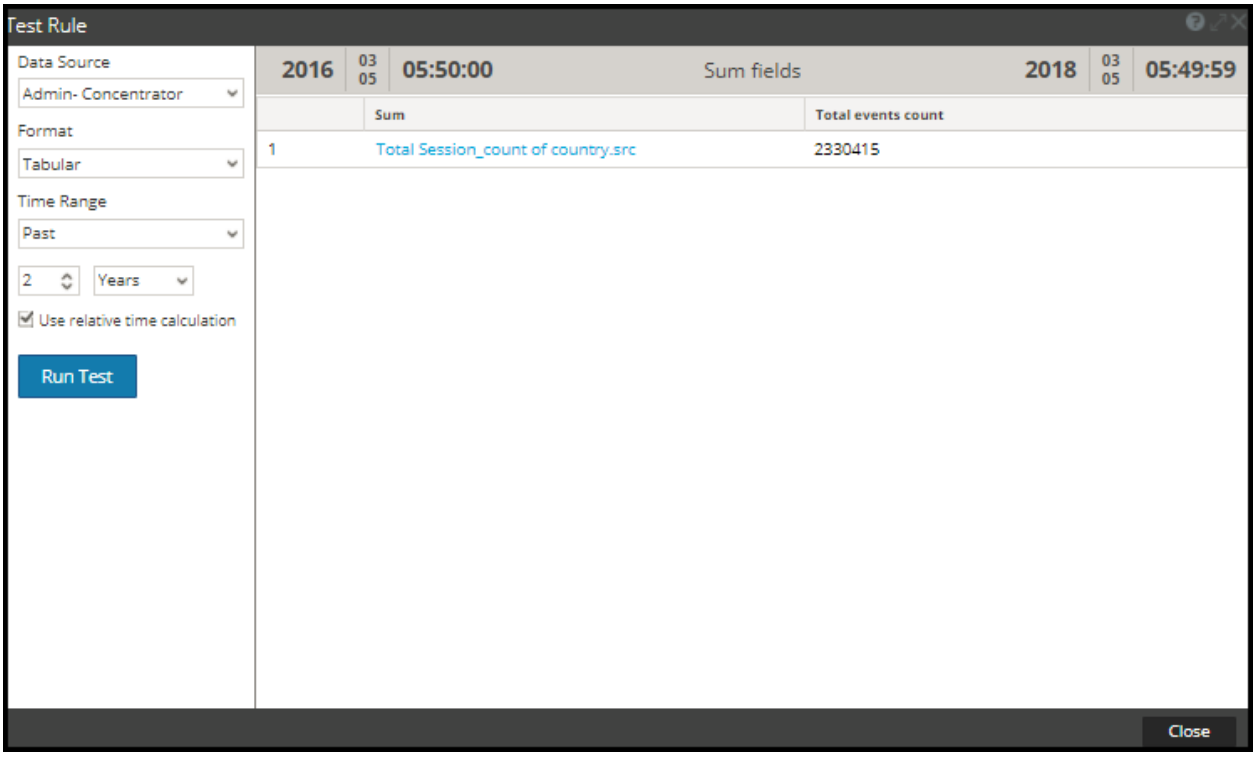
Totals the quantifiers for a given result set. For example, calling a sum_count() for a rule that is sorted by event count totals the size of all values in the result set and displays the total in place of the result set.

Example:

The following figure shows the sum_count() rule action.


Build Rule
NetWitness Platform DB
Name
Sum fields
Summarize
Event Count
Select
country.src
Alias
Sum
Where
country.src = 'United States','China','Canada'
Group By
country.src
Then
sum_count();
Enter a then clause...
Order By
Column Name
Sort By
Total
Descending
Session Threshold
0
Limit
20
Use
Save
Reset
Test Rule

With sum_count() rule action, the output shows the total size of all the event counts.

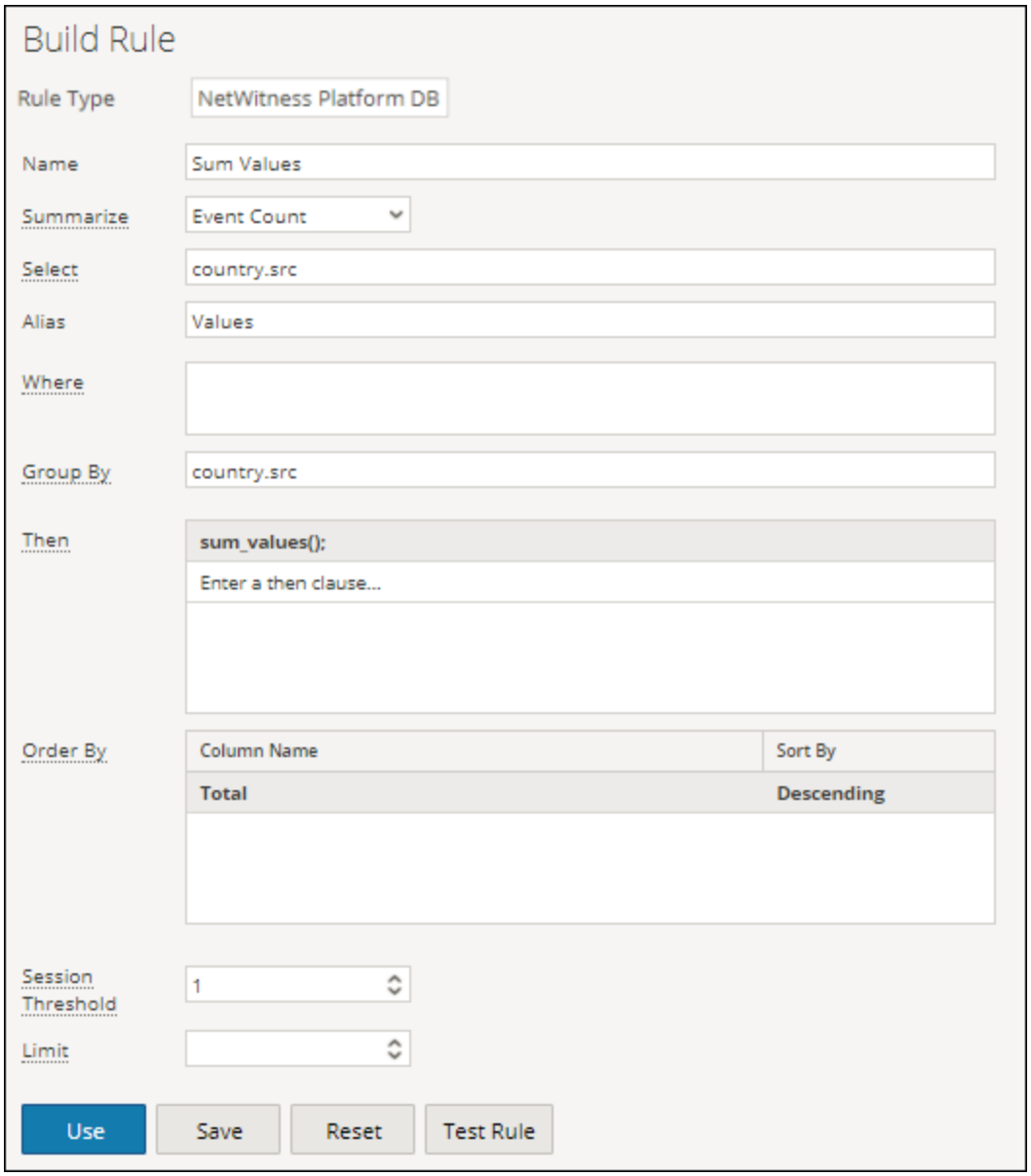


`sum_values()`

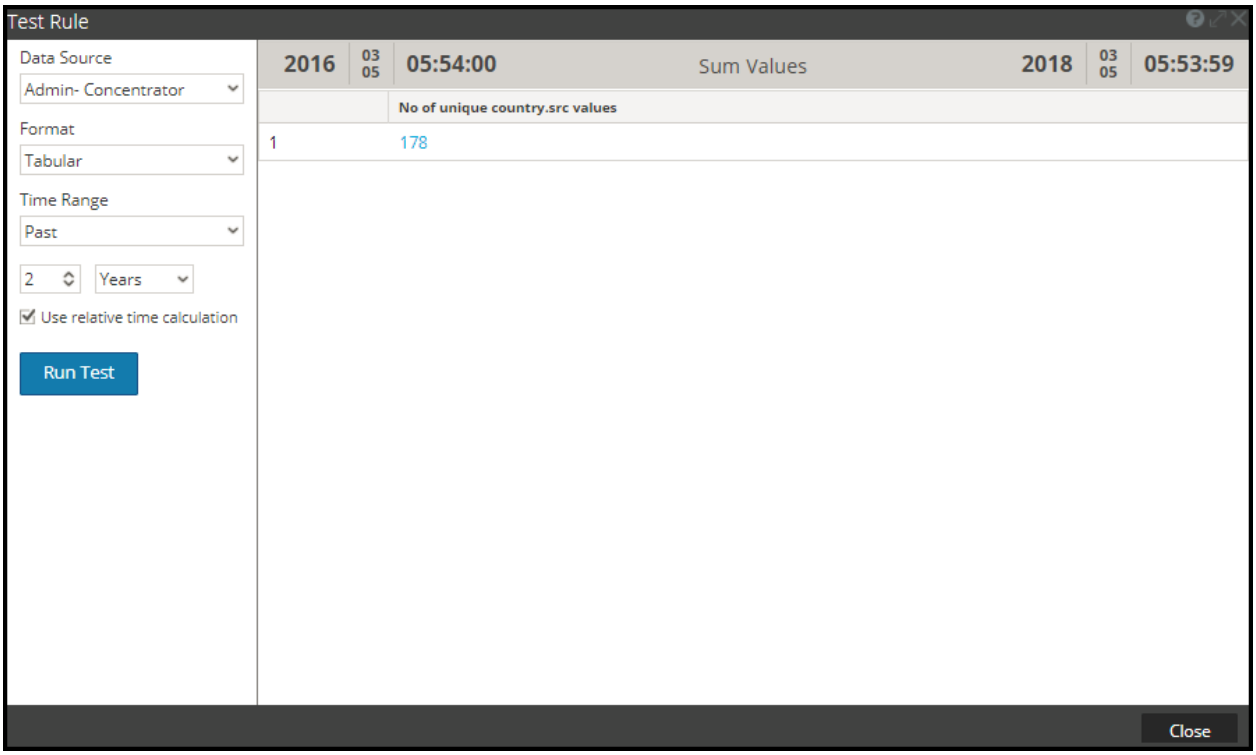
Totals the number of values for a given result set. Use this action to display how many matches exists for a given rule.

Example:

The following figure shows the sum_values() rule action.



The following figure shows the result with sum_values rule action.



show_whats_new()

The show_whats_new() rule action takes any result in a result set and filters out any value that is available in the NetWitness meta database prior to the time frame of the currently running report. When a report runs, NetWitness determines the ID of the first session in the time range of the report. If a value in a result set has a first session id that is greater than the first session id of the report time frame, it did not exist in the NetWitness meta database prior to the report being run and so is new to the NetWitness system relative to the time frame of the report.

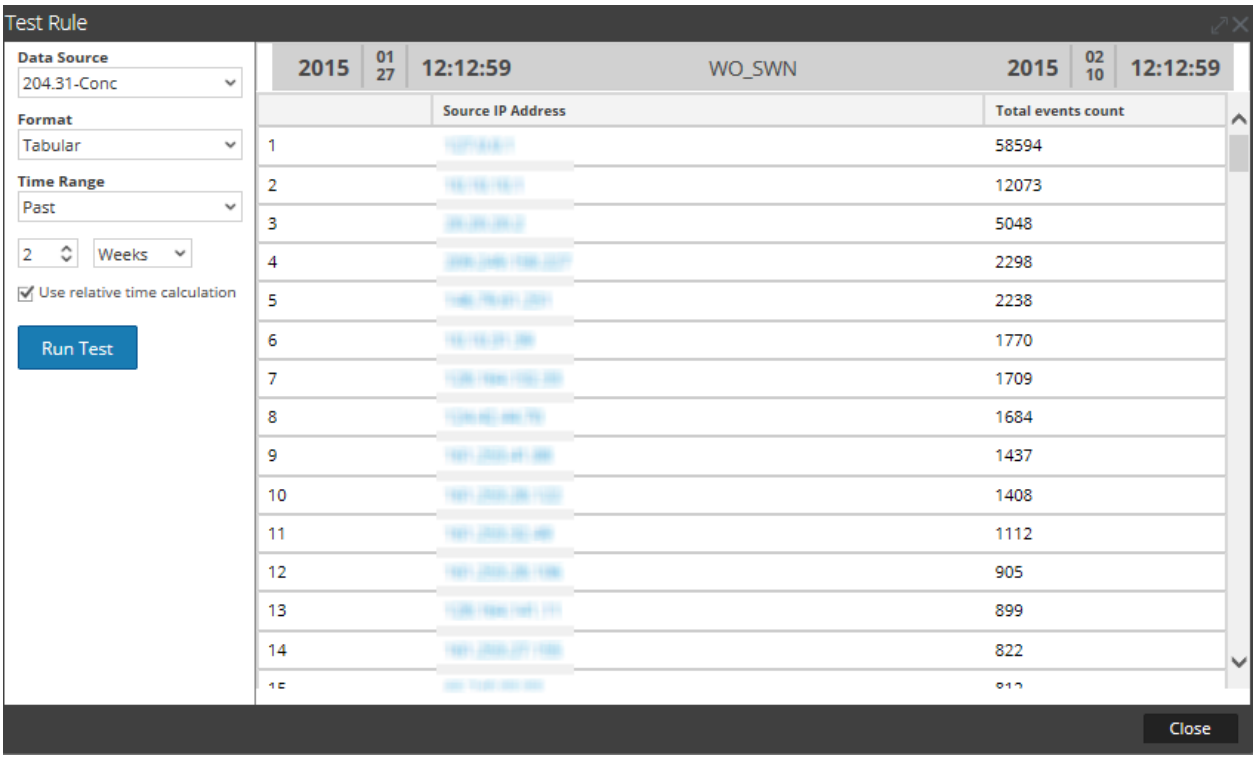
The show_whats_new() rule action is also supported for Custom Aggregate Rule. When multiple meta's are selected in the Custom rule, the first meta is considered for filtering out the old values. See "Example 2" below to understand how this rule action is used for Custom Aggregate Rule.

Note: The show_whats_new() rule action can be used only with an aggregate rule.

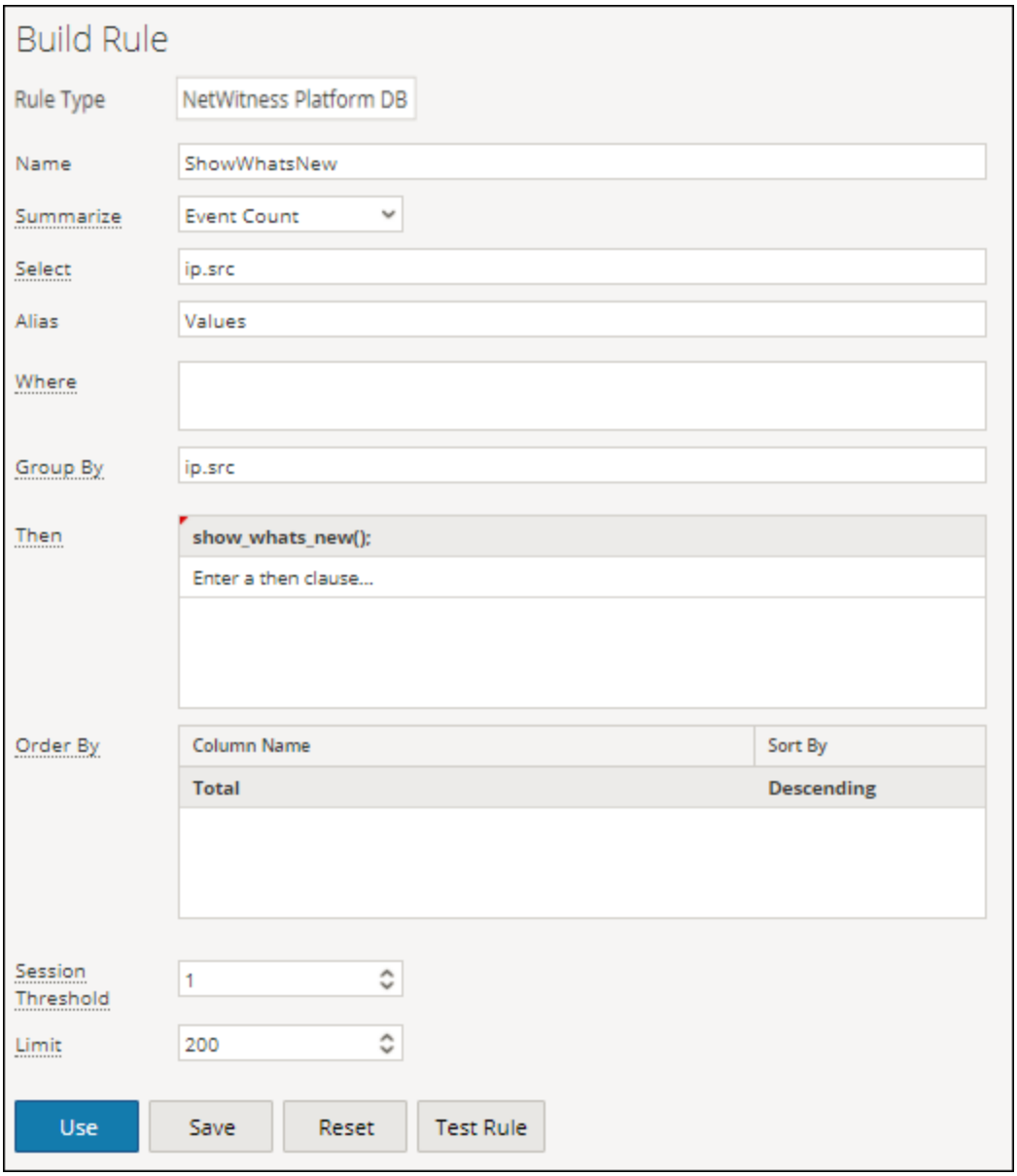
Examples:

1. show_whats_new() for aggregate rule with Event Count

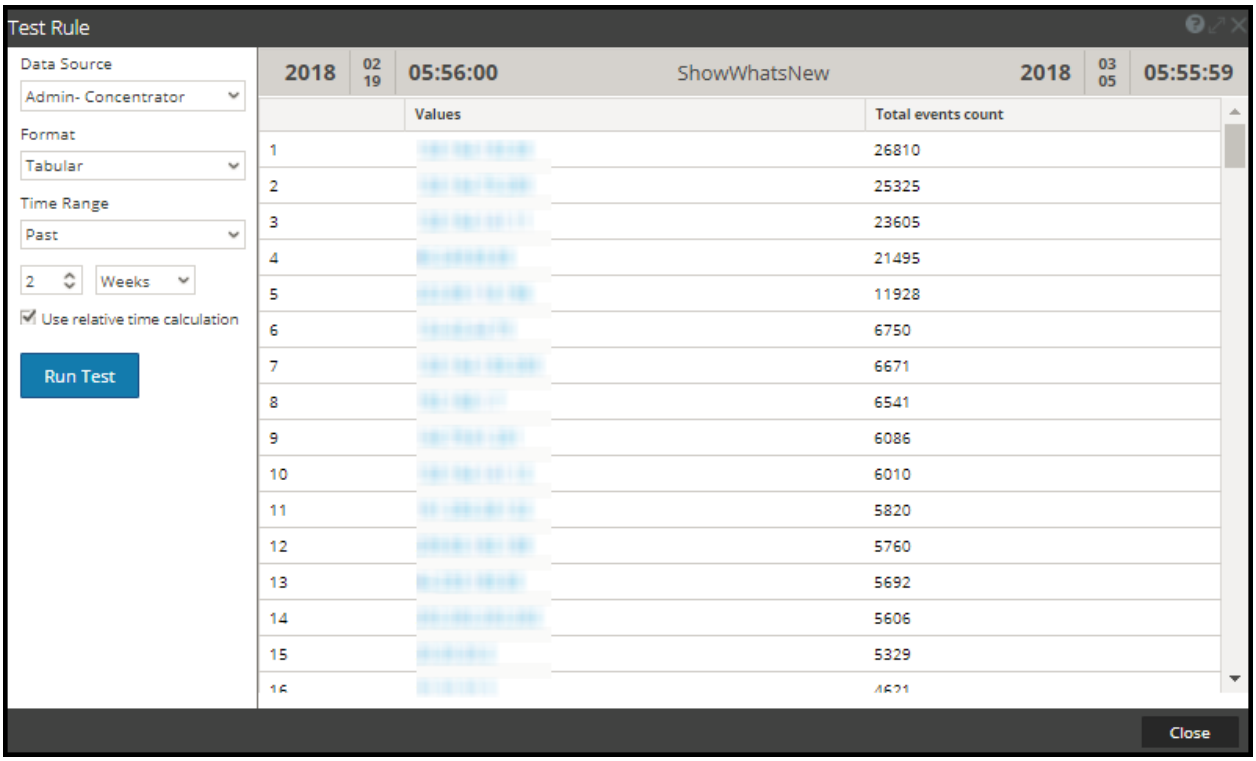
In the following example, all the Source IP Addresses available for the past two weeks are listed.



The following figure shows the use of the show_whats_new rule action to list only the new entries for the past two weeks.

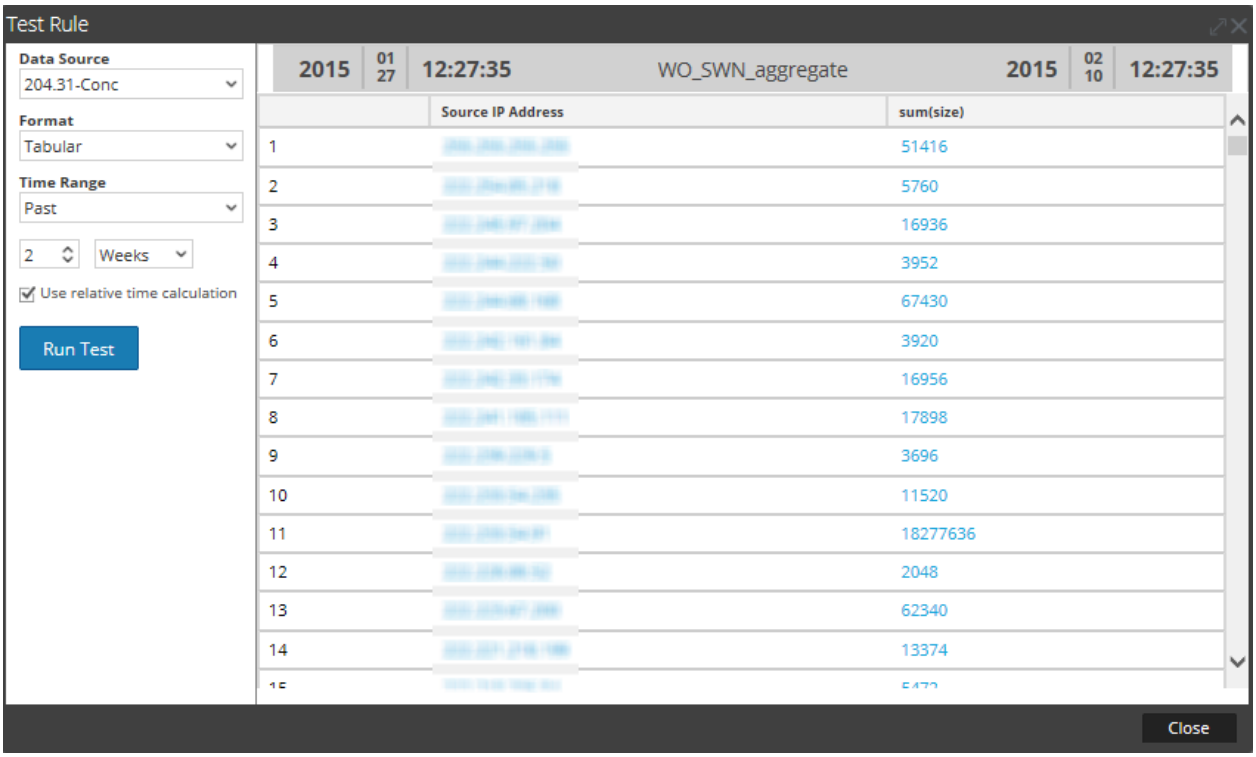


The following figure lists the new entries for the past two weeks.

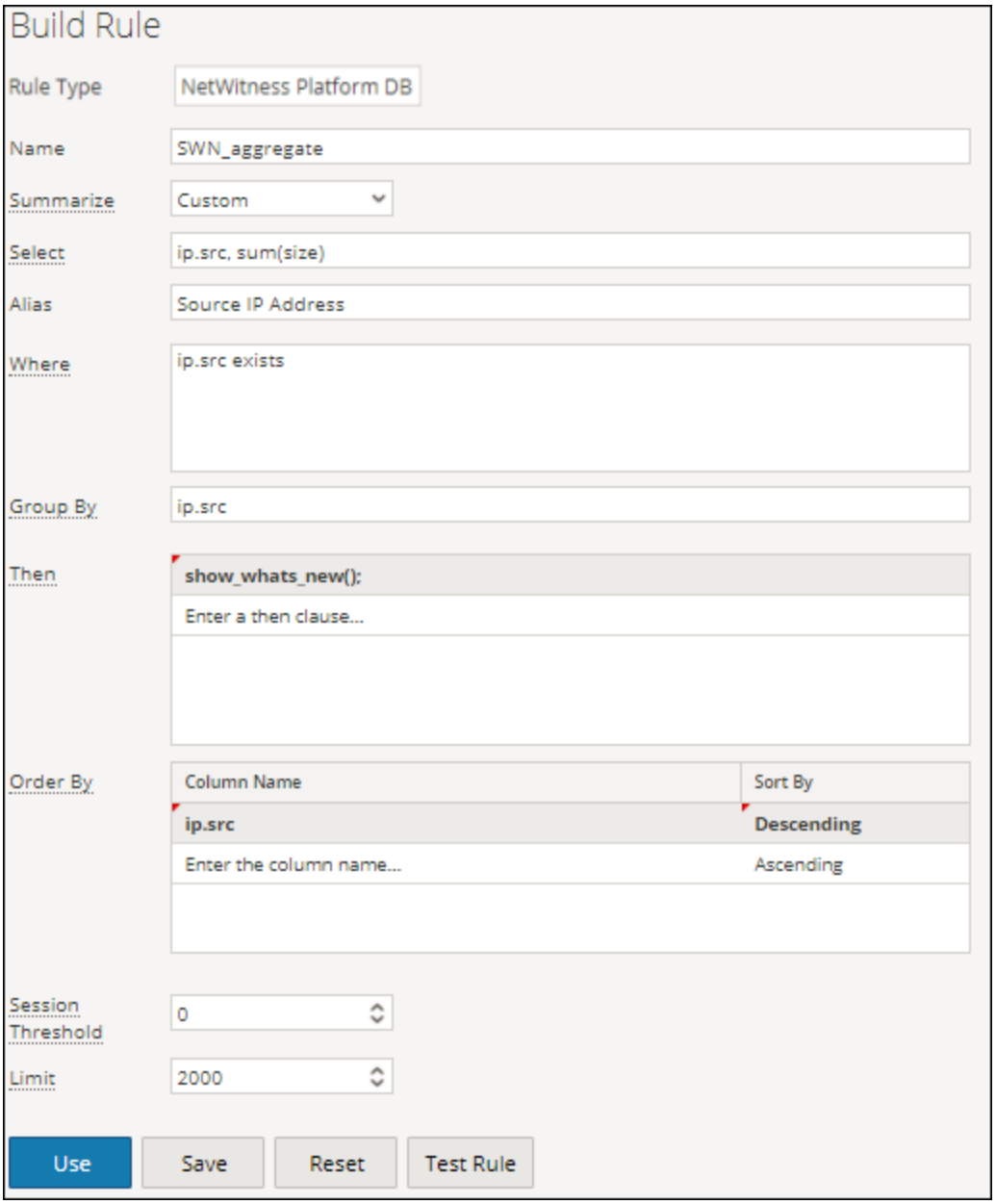


2. show_whats_new() for Custom aggregate rule

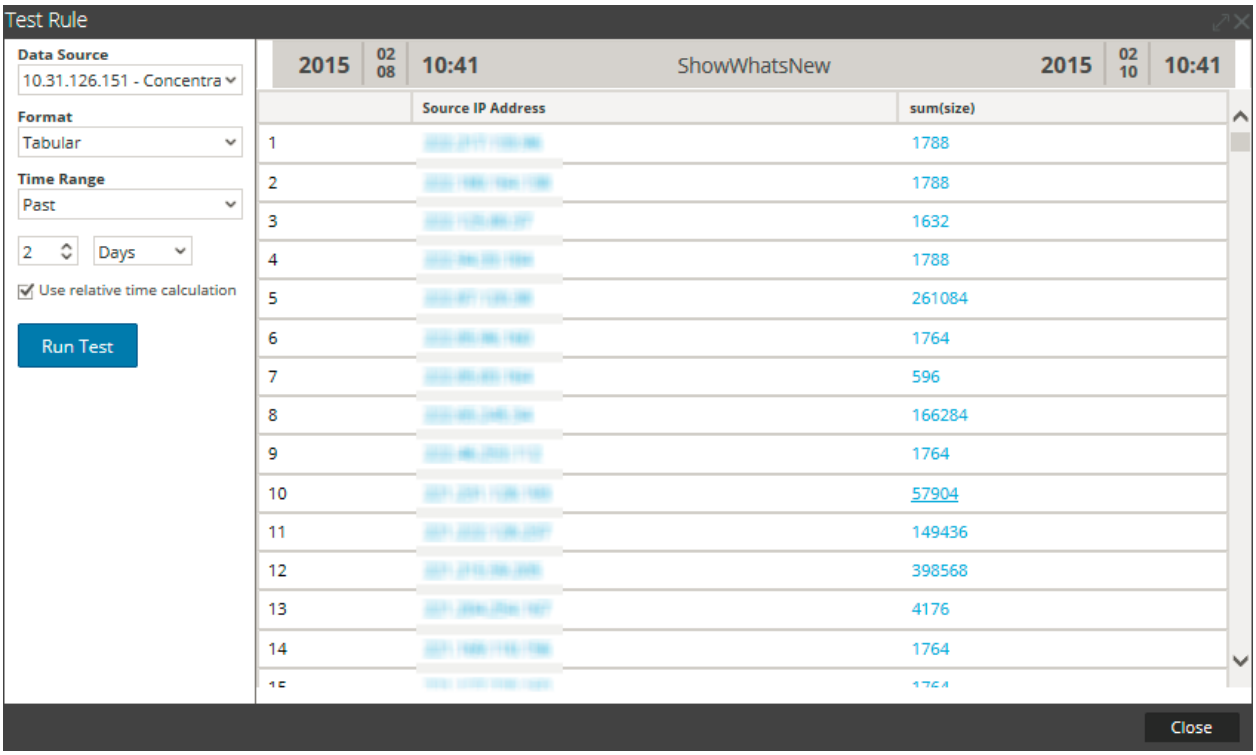
In the following example, all the Source IP Addresses available for the past two weeks are listed.



The following figure shows the use of the show_whats_new rule action to list only the new entries for the past two weeks.



The following figure lists the new entries of Source IP Addresses for the past two weeks.



The power of this feature is that it doesn't matter when the report is run in identifying values that are new to NetWitness. The caveat with this feature is that if a data reset occurs, you will lose your data. However, it is easy to baseline a system and identify changes and new items without a tremendous amount of strain on the system (depending on the size of your result set).

Supported Rule Operators

The NWDB Reporting Engine data source rule syntax supports a subset of rule operators that are supported by NetWitness.

Syntax	Description
*	Use an asterisk (*) as the sole operator in a rule to select all traffic.
=	Equals operator
!=	Does not equal operator
&&	Logical AND operator
||	Logical OR operator
-u	Upper boundary. For example, **tcp.port = 40000-u** selects all TCP ports above 40000.
l-	Lower boundary. For example, **tcp.port = l-40000** selects all TCP ports below 40000.
-	The dash (-) operator only applies to numeric values. Separate the lower and upper boundaries of the range with a dash (-). For example, **tcp.port = 25-443** selects all TCP ports between 25 and 443.

Sample Supported Queries

Respond Rule Syntax

The supported rule syntax for the Respond service through descriptions and examples of supported and unsupported syntax. There is a finite set of syntax that you can use to construct rules for reports using the Respond service in this release.

The Reporting Engine supports the following categories of Respond data source rule syntax:

- **select** clause
  - Non-Aggregate Rule
  - Aggregate Rule
- **alias**
- **where** clause
- **where** clause Operators
- Group By
- Order By
- **Limit** field

Note: List is not supported in Respond Data source rules.

Select Clause

The select clause is a comma separated list of values. For example: select alert.severity, alert.name, count (*).

There are two types of select clause for Respond Rule:

- Non-aggregate rule
- Aggregate rule

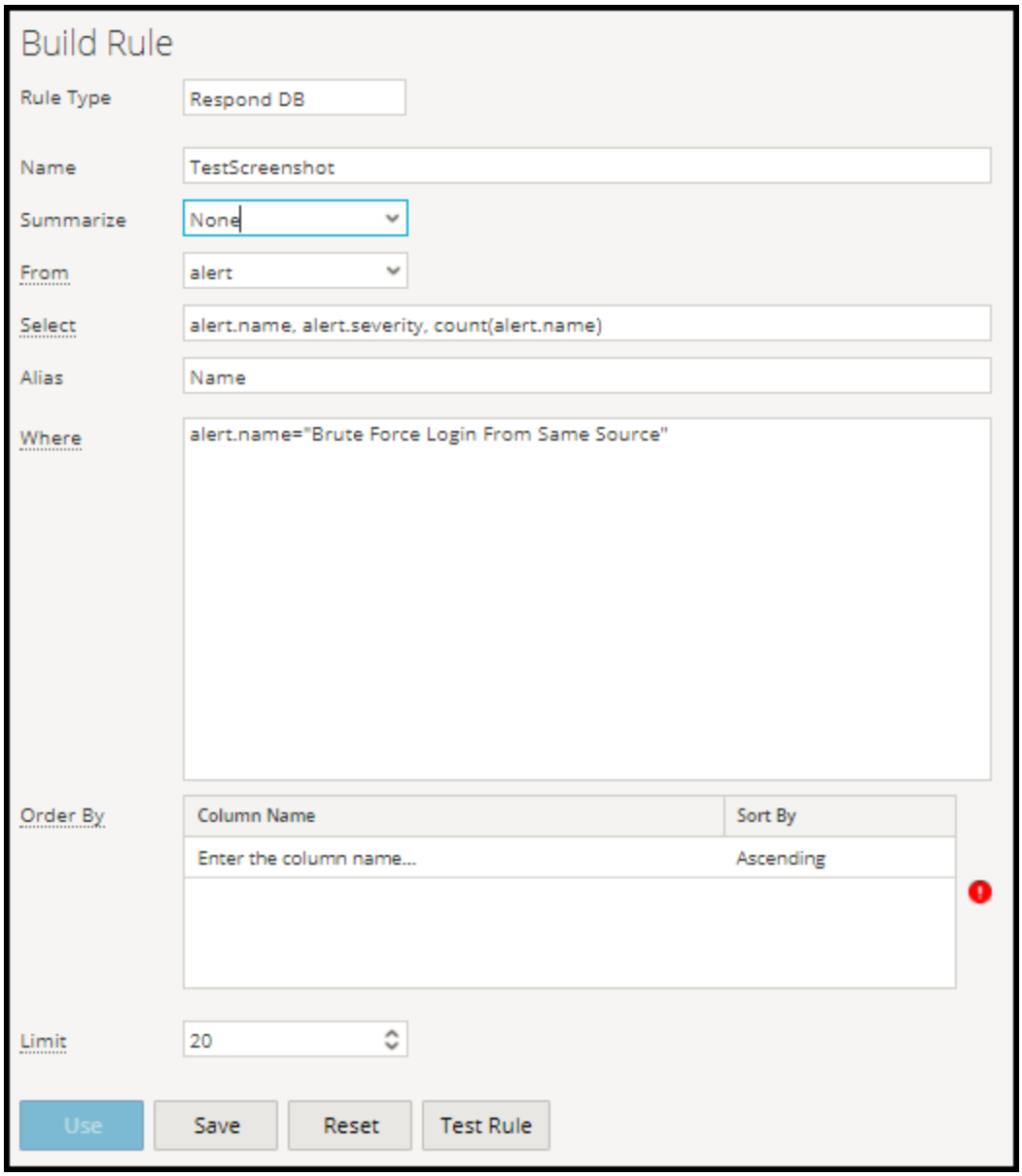
Non-Aggregate Rule

When you want to define a rule without any grouping, choose 'None' in the Summarize field. In a non-aggregate rule, you can select any number of metas in the *Select* clause. For example, select alert.severity, alert.name.

Aggregate Rule

When you want to query for a specific meta and its associated aggregate value then you must use the Aggregate rule. To get an aggregate, you must choose 'Custom' in the **Summarize** field to include an aggregate function in the *Select* clause. For example, select alert.severity, alert.name, count(*).

The following figure shows the Build Rule view for Aggregate Rule.



Supported Aggregate Functions

The rules on Respond service supports the following aggregate functions and syntax.

- count
- max
- min
- sum
- avg

Note: The aggregate functions must be added in the end of a select clause for aggregate query. For example, alert.name, alert.severity, sum(alert.numEvents). By default, a maximum of 10,000 rows results are fetched and this can be configured using the **rsa.response.query.QueryProperties**.

Examples of select Clause Syntax

The following table provides examples of the select Clause Syntax.

Examples	Descriptions
select *column1* ,*column2*,*column3*,...,*columnN*	Select specific metas from an Respond Data Source (You must separate each column with a comma.).

Examples of Supported Select Queries

select alert.name, alert.numEvents, count(alert.numEvents)

select alert.severity, avg(alert.severity)

select alert.timestamp, incidentCreated where alert.timestamp >= 1475658011

Summarize

Summarize determines the type of summarization or aggregation for the rule.

Name	Config Value
Summarize	To query metas without any custom grouping, select: • **None**: To get meta based aggregates, select: • **Custom**: This indicates that expected meta aggregate function is defined in rule select clause.

Alias

Some meta names may not be descriptive, in this case description can be added in the the alias field to make column names more readable. For example, **SELECT**: alert.severity, alert.name, count(*)
ALIAS: Alert Severity, Alert Name

In the alias field you can enter a name for columns used in the select clause. If you do not specify the alias for one of the field in the select clause, then the default description will be used. For example, if the select clause has Field1,Field2,Field3,Field4, and alias has only Field1, ,Field3,Field4, then for Field2 a default description is used.

Where Clause

The where clause is a language field values and ranges that is used by Respond function. In the where clause, string values have to be enclosed within single quotes.

Examples	Descriptions
alert.host summary =' (Primary) Link status "Down" on interface INTNAME.'	For TEXT or string type data, enclose the string or text in single or double quote. If there is any special character such as an apostrophe within the data then you need to add an additional single or double quotes. For example, alert.name = 'top alerts from Cote d"Ivoire'.
alert.timestamp >= 1475658011	For Date and Time (date/timestamp data type columns), use the EPOCH syntax.

Supported Where Clause Operators

Operator	Syntax
= (equals)	*column1* = '*value*'
!= (does not equal)	*column1* != '*value*'
>	*column1* > '*value*'
>=	*column1* >= '*value*'
<	*column1* < '*value*'
<=	*column1* <= '*value*'

Group By

Syntax	Function
group by : alert.severity, alert.timestamp, incidentCreated **Note:** Group by field is enabled for Aggregate queries and are not editable.	Respond picks the metas for Group By field from the selected Select clause automatically.

Order By

Order By determines how to sort the result set and is not case sensitive.

Name	Configuration Value
Column Name	The Column Name is the name of the columns by which you want to sort the results. By default, the value is empty. When you click on a column, the value gets populated based on the Summarize field. • order by alert.name asc • order by incidentCreated desc • order by count(numEvents) • order by status
Sort By	Sort By determines the order in which you want to sort the results such as ascending or descending. **Note:** For all queries, it is mandatory for you to select the order by field.

Limit field

This indicates the limit to be put on the query while fetching data from the database. If a result set is sorted by event count, packet count, or session size, the limit represents the top (or bottom) N values to be returned. If the result set is not sorted, the first N values are returned.

Warehouse DB Simple Rules Syntax

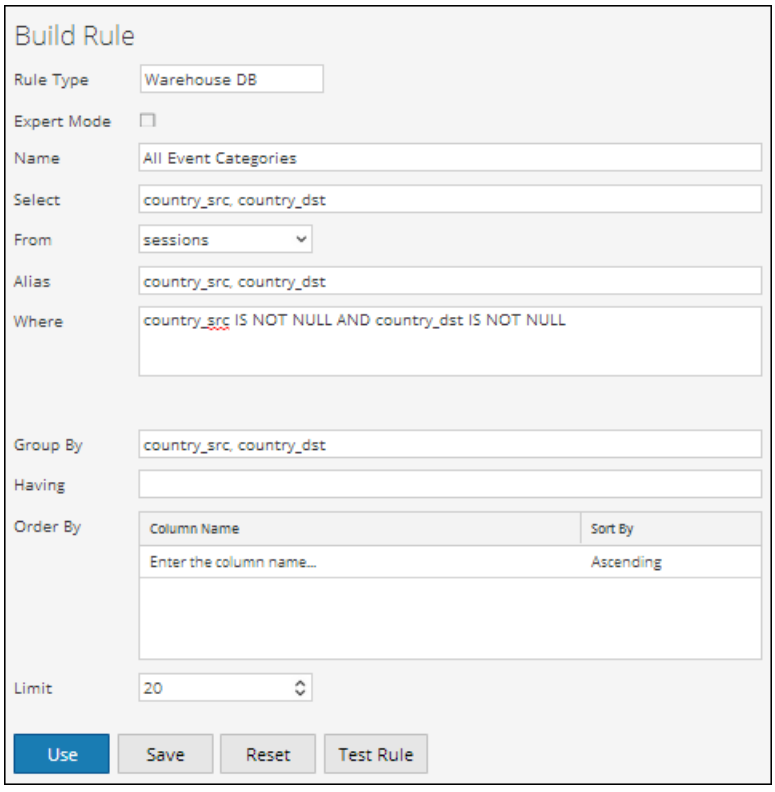
The section explains the simple rules query syntax and examples.

The following examples illustrate simple rules in the default mode:

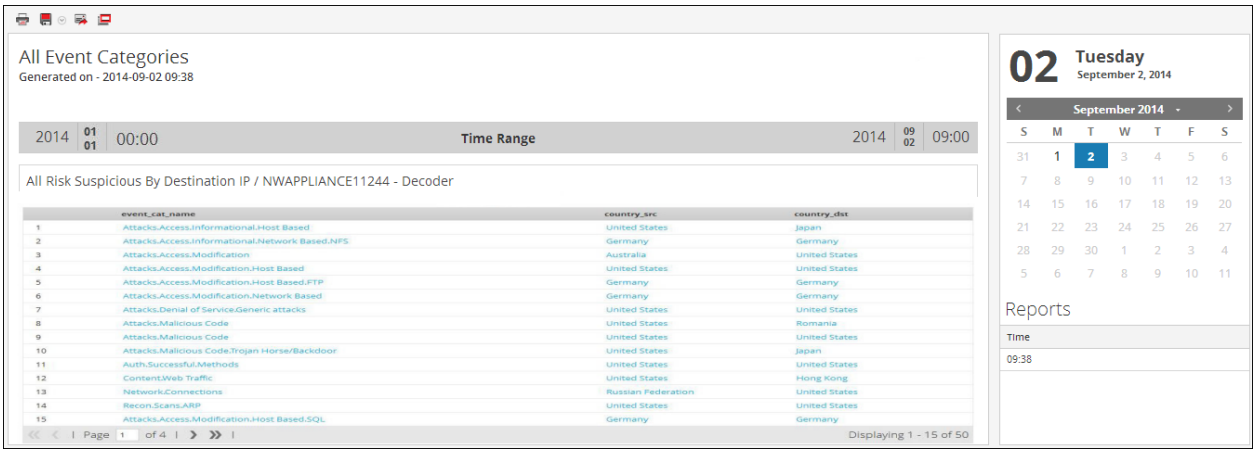
- All Event Categories Report
- Attacks Event Categories Report
- Source: China Event Categories Report
- IP Source and Destination Event Categories Report
- Time Threat Categories Report
- Array Query Report
- Raw Log Query Report

All Event Categories Report

This rule fetches all event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table, that is, **country_src** for the source country, and **country_dst** for the destination country.

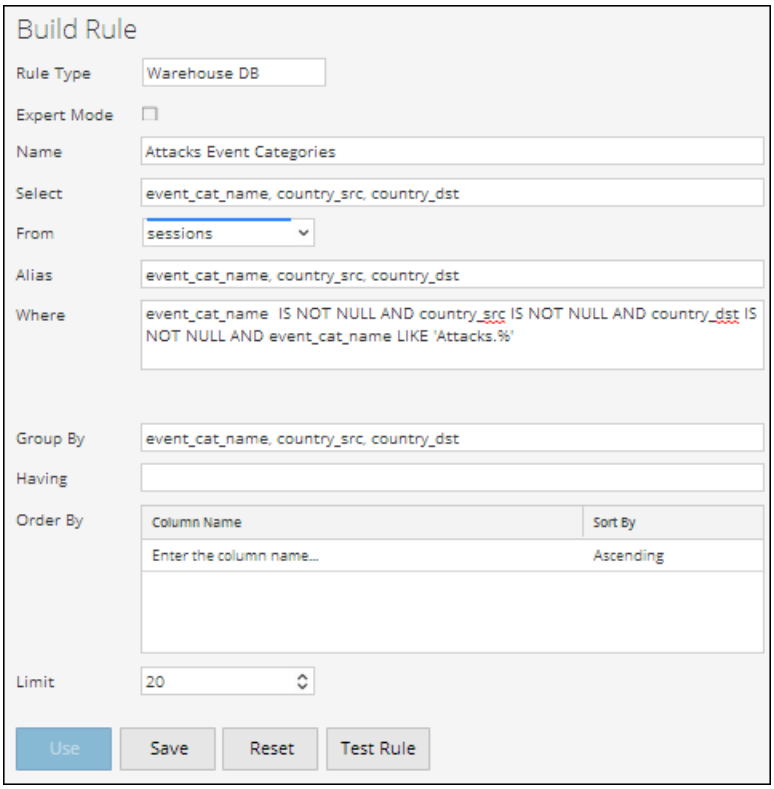


The following figure shows the result set of the All Event Categories rule.

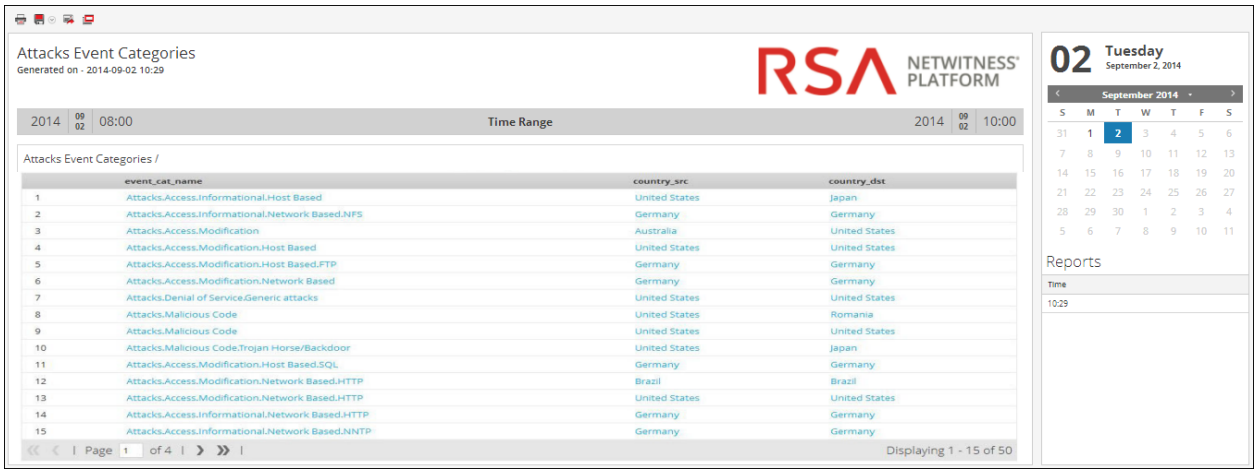


Attacks Event Categories Report

This rule fetches the event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose event category name like 'Attacks.%'.

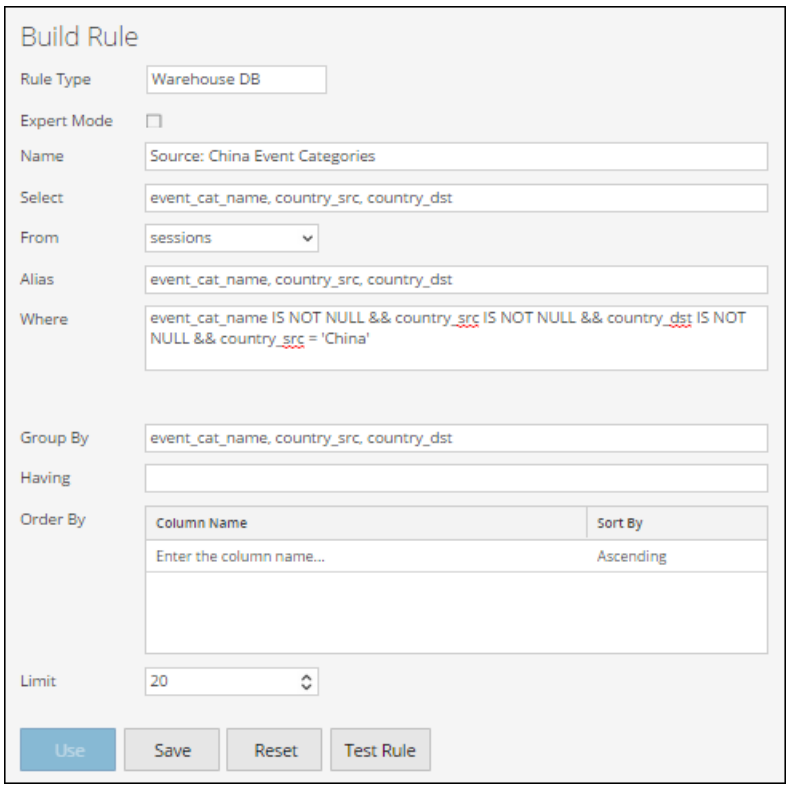


The following figure shows the result set of the Attacks Event Categories rule.

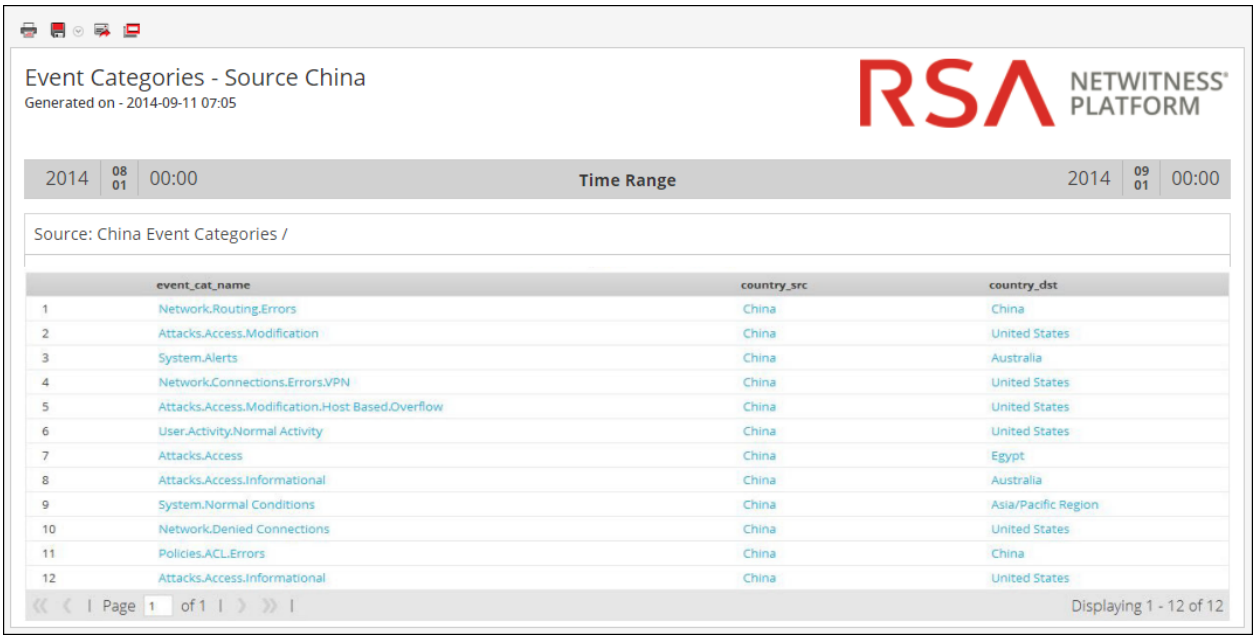


Source: China Event Categories Report

This rule fetches the event categories, source country, and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose source country is 'China'.



The following figure shows the result set of the Source: China Event Categories rule.



Event Categories - Source China
Generated on - 2014-09-11 07:05

RSA NETWITNESS PLATFORM

2014 08 01 00:00 **Time Range** 2014 09 01 00:00

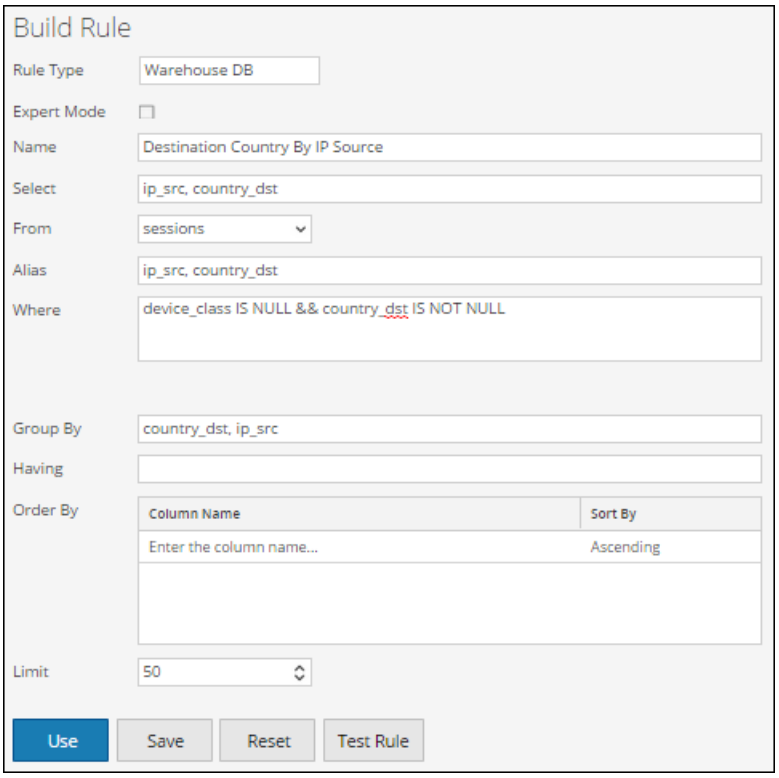
Source: China Event Categories /

	event_cat_name	country_src	country_dst
1	Network.Routing.Errors	China	China
2	Attacks.Access.Modification	China	United States
3	System.Alerts	China	Australia
4	Network.Connections.Errors.VPN	China	United States
5	Attacks.Access.Modification.Host Based.Overflow	China	United States
6	User.Activity.Normal Activity	China	United States
7	Attacks.Access	China	Egypt
8	Attacks.Access.Informational	China	Australia
9	System.Normal Conditions	China	Asia/Pacific Region
10	Network.Denied Connections	China	United States
11	Policies.ACL.Errors	China	China
12	Attacks.Access.Informational	China	United States

Page 1 of 1 Displaying 1 - 12 of 12

IP Source and Destination Event Categories Report

This rule fetches the IP address of source and destination country from the **sessions** table by defining alias names (temporary column names) for each of the fields to be fetched from the table and selecting only those columns whose destination country is NOT NULL.



Build Rule

Rule Type: Warehouse DB

Expert Mode: ☐

Name: Destination Country By IP Source

Select: ip_src, country_dst

From: sessions

Alias: ip_src, country_dst

Where: device_class IS NULL && country_dst IS NOT NULL

Group By: country_dst, ip_src

Having:

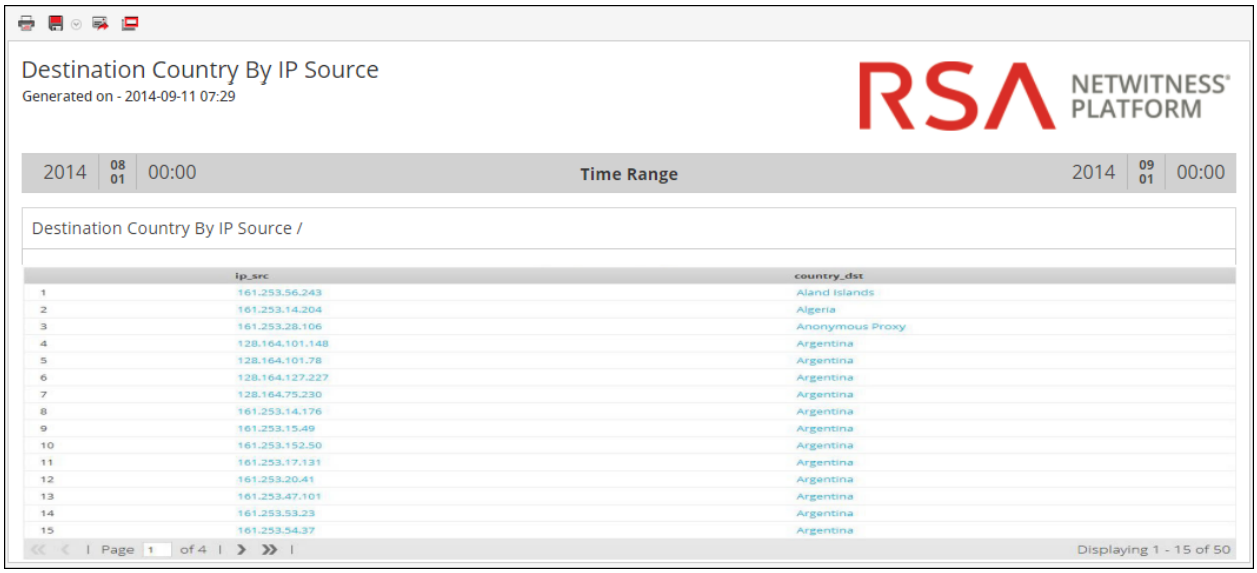
Order By:

Column Name	Sort By
Enter the column name...	Ascending

Limit: 50

Use | Save | Reset | Test Rule

The following figure shows the result set of the IP Source and Destination Event Categories rule.



Destination Country By IP Source

Generated on - 2014-09-11 07:29

RSA NETWITNESS PLATFORM

2014	08 01	00:00	Time Range	2014	09 01	00:00

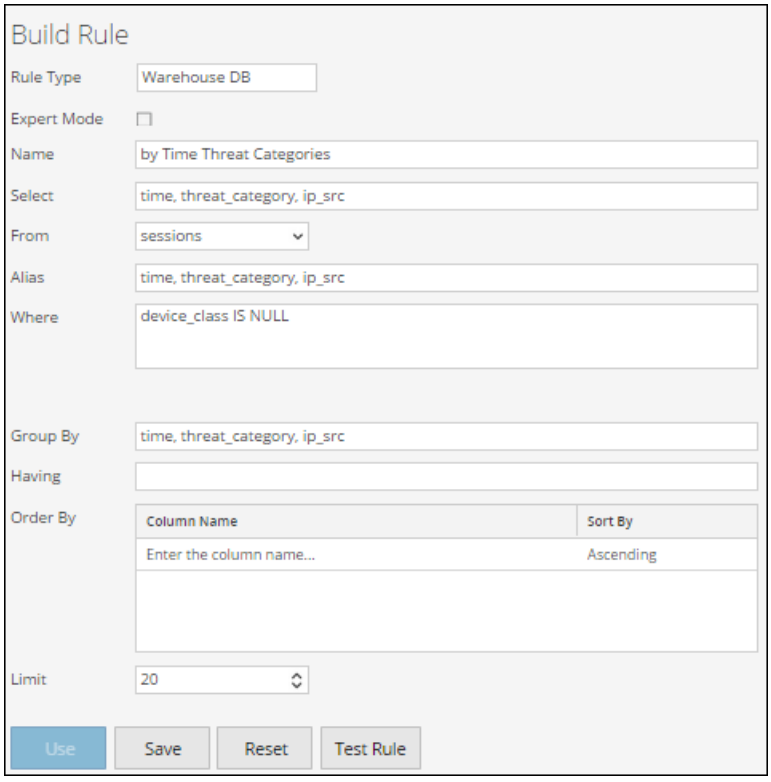
Destination Country By IP Source /

	ip_src	country_dst
1	161.253.56.243	Aland Islands
2	161.253.14.204	Algeria
3	161.253.28.106	Anonymous Proxy
4	128.164.101.148	Argentina
5	128.164.101.78	Argentina
6	128.164.127.227	Argentina
7	128.164.75.230	Argentina
8	161.253.14.176	Argentina
9	161.253.15.49	Argentina
10	161.253.152.50	Argentina
11	161.253.17.131	Argentina
12	161.253.20.41	Argentina
13	161.253.47.101	Argentina
14	161.253.53.23	Argentina
15	161.253.54.37	Argentina

Page 1 of 4 Displaying 1 - 15 of 50

Time Threat Categories Report

This rule fetches the threat category events, the time the log or event was ingested into Log Decoder/Decoder, and the source IP addresses from the **sessions**table by defining alias names (temporary column names) for each of these fields to be fetched from the table.



Build Rule

Rule Type: Warehouse DB

Expert Mode: ☐

Name: by Time Threat Categories

Select: time, threat_category, ip_src

From: sessions

Alias: time, threat_category, ip_src

Where: device_class IS NULL

Group By: time, threat_category, ip_src

Having:

Order By:

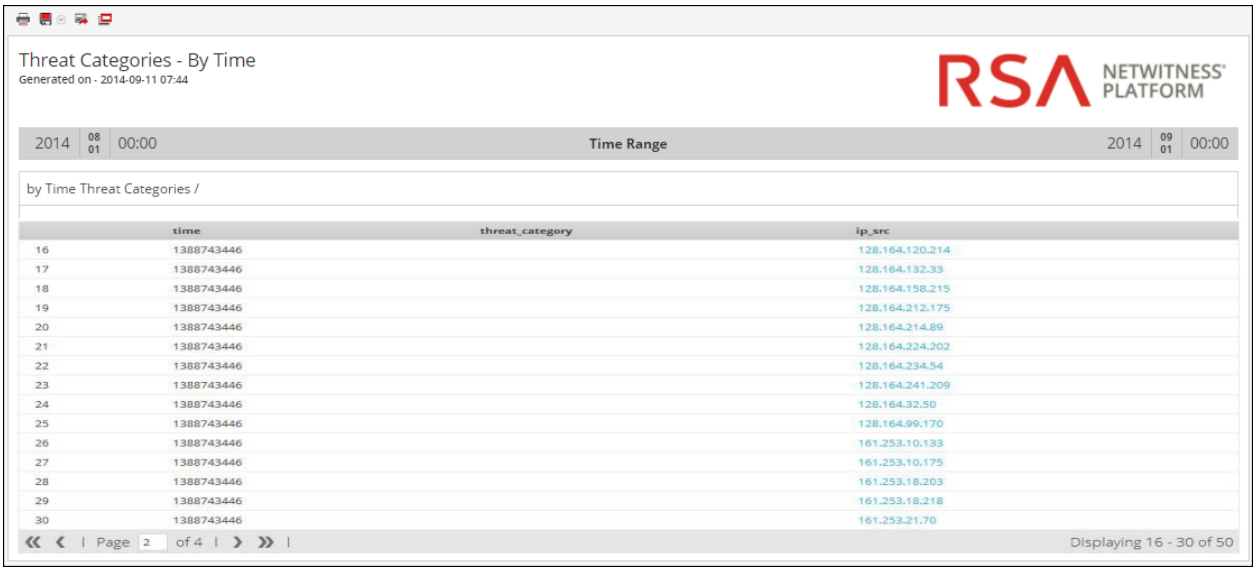
Column Name	Sort By
Enter the column name...	Ascending

Limit: 20

Use | Save | Reset | Test Rule

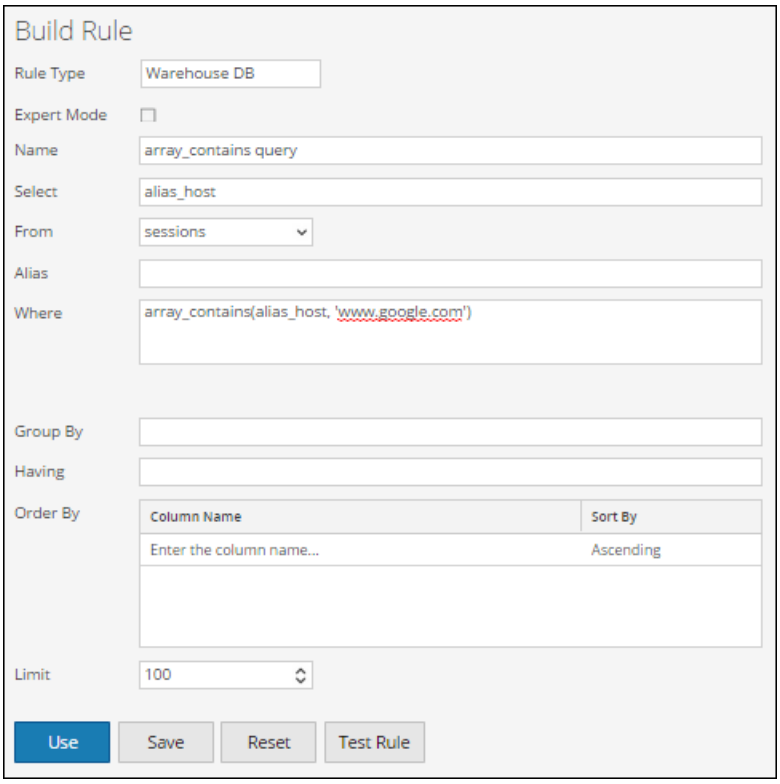
The following figure shows the result set of the by Time Threat Categories rule. The time displayed in the time field is the UNIX time (For example, 1388743446).

Note: In the “Select” clause the syntax would be “UNIX time” to convert to UTC time in report. For example, you can use the Epoch time converter tool to convert UNIX time (1388743446) to UTC (Coordinated Universal Time) (1/3/2014 3:34:06 PM).

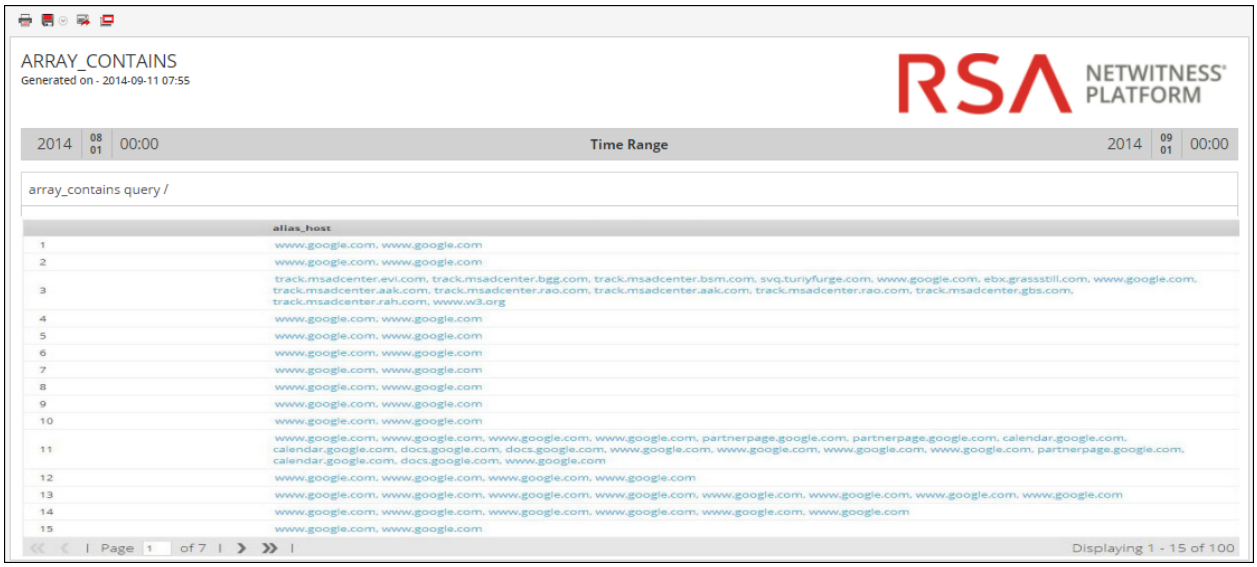


Array Query Report

This rule fetches an array of alias host names from the **sessions** table which contains the value 'www.google.com'.



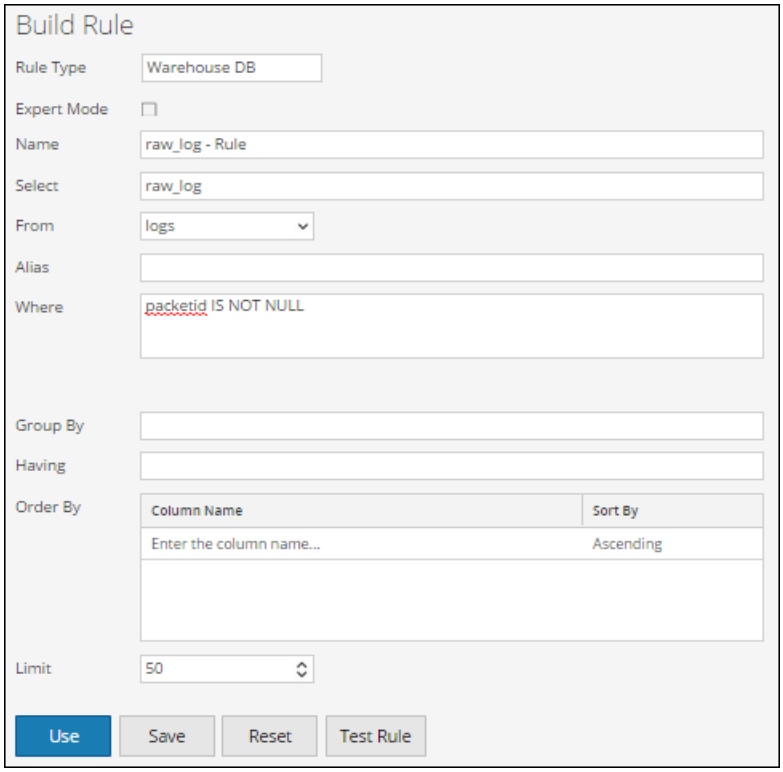
The following figure shows the result set for querying an array from sessions.



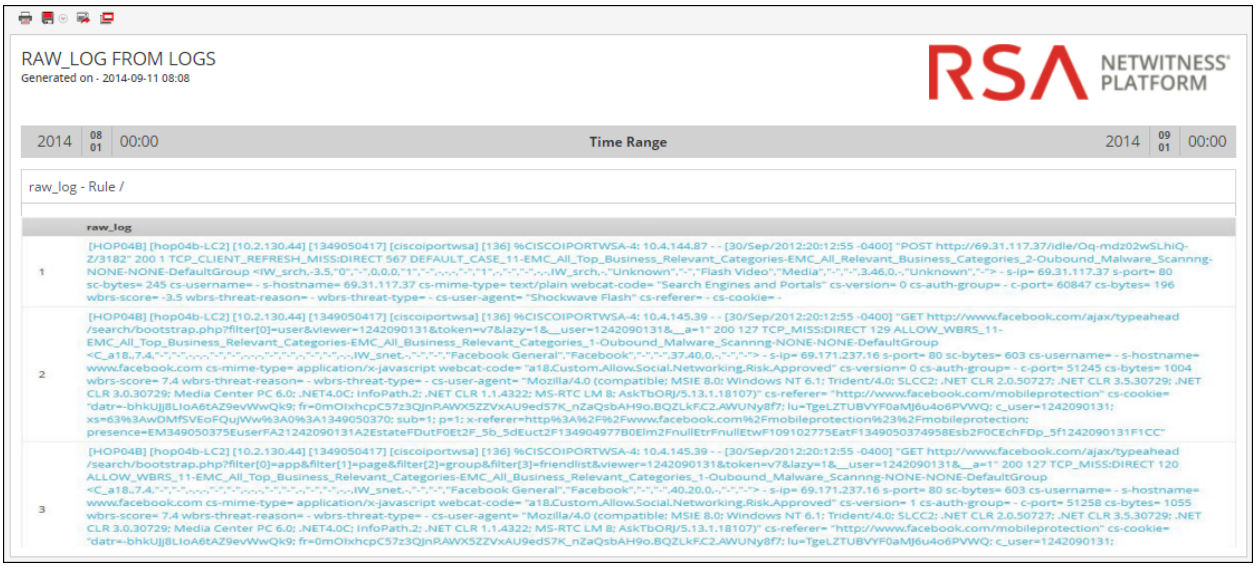
Raw Log Query Report

Raw logs can be queried either from the logs or sessions table.

This rule uses **raw_log** as a meta for querying raw log from logs whose packet ID is NOT NULL.



The following figure shows the result set for querying raw logs from logs.



RAW_LOG FROM LOGS
Generated on - 2014-09-11 08:08

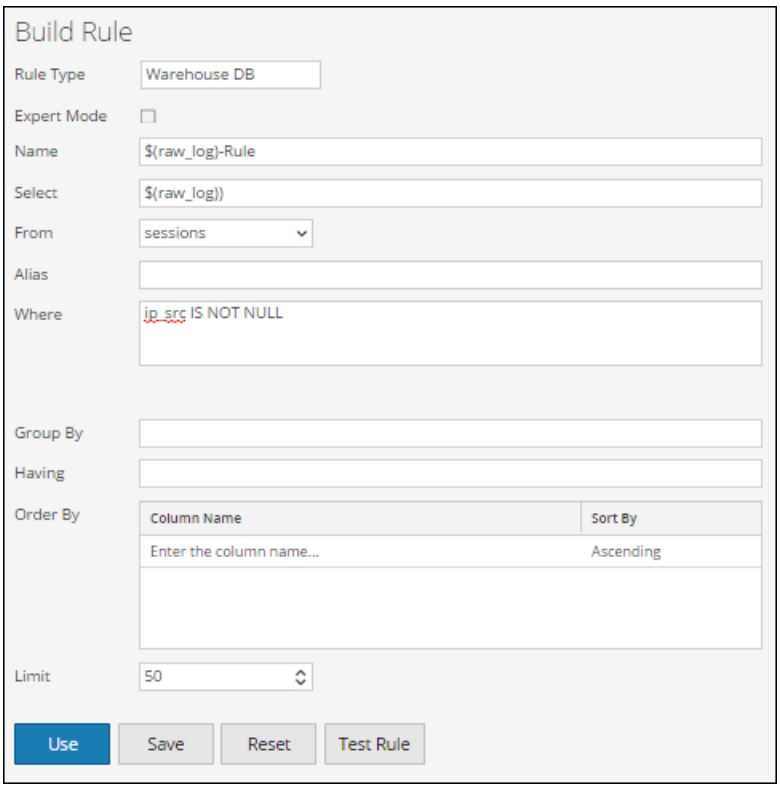
RSA NETWITNESS PLATFORM

2014	08 01	00:00	Time Range	2014	09 01	00:00

raw_log - Rule /

	raw_log
1	[HOP04B] [hop04b-LC2] [10.2.130.44] [1349050417] [ciscoipportwsa] [136] %CISCOIPORTWSA-4: 10.4.144.87 - - [30/Sep/2012:20:12:55 -0400] "POST http://69.31.117.37/idle/Oq-mdz02wSLhiQ-Z/3182" 200 1 TCP_CLIENT_REFRESH_MISS:DIRECT 567 DEFAULT_CASE_11-EMC_All_Top_Business_Relevant_Categories-EMC_All_Relevant_Business_Categories_2-Oubound_Malware_Scannng-NONE-NONE-DefaultGroup <IW_srch,-3.5,"0","-",0,0,0,"1","-",-,-,-,"-","1",-,"-","-","-",-,-,IW_srch,-,"Unknown","-","Flash Video","Media","-","-",3.46.0,-,"Unknown","-"> - s-ip= 69.31.117.37 s-port= 80 sc-bytes= 245 cs-username= - s-hostname= 69.31.117.37 cs-mime-type= text/plain webcat-code= "Search Engines and Portals" cs-version= 0 cs-auth-group= - c-port= 60847 cs-bytes= 196 wbrs-score= -3.5 wbrs-threat-reason= - wbrs-threat-type= - cs-user-agent= "Shockwave Flash" cs-referer= - cs-cookie= -
2	[HOP04B] [hop04b-LC2] [10.2.130.44] [1349050417] [ciscoipportwsa] [136] %CISCOIPORTWSA-4: 10.4.145.39 - - [30/Sep/2012:20:12:55 -0400] "GET http://www.facebook.com/ajax/typeahead/search/bootstrap.php?filter[0]=user&viewer=1242090131&token=v7&lazy=1&__user=1242090131&__a=1" 200 127 TCP_MISS:DIRECT 129 ALLOW_WBRS_11-EMC_All_Top_Business_Relevant_Categories-EMC_All_Business_Relevant_Categories_1-Oubound_Malware_Scannng-NONE-NONE-DefaultGroup <C_a18.,7.4,"-","-",-,-,-,"-","-",-,-,"-","-",-,-,IW_snet,-,"-","-","Facebook General","Facebook","-","-",37.40.0,-,"-","-"> - s-ip= 69.171.237.16 s-port= 80 sc-bytes= 603 cs-username= - s-hostname= www.facebook.com cs-mime-type= application/x-javascript webcat-code= "a18.Custom.Allow.Social.Networking.Risk.Approved" cs-version= 0 cs-auth-group= - c-port= 51245 cs-bytes= 1004 wbrs-score= 7.4 wbrs-threat-reason= - wbrs-threat-type= - cs-user-agent= "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.2; .NET CLR 1.1.4322; MS-RTC LM 8; AskTbORJ/5.13.1.18107)" cs-referer= "http://www.facebook.com/mobileprotection" cs-cookie= "datr=-bhkUJj8LIoA6tAZ9evWwQk9; fr=0mOIxhcpC57z3QJnP.AWX5ZZVxAU9ed57K_nZaQsbAH9o.BQZLkF.C2.AWUNy8f7; lu=TgeLZTUBVYF0aMJ6u4o6PVWQ; c_user=1242090131; xs=63%3AwDMfSVEoFQujWw%3A0%3A1349050370; sub=1; p=1; x-referer=http%3A%2F%2Fwww.facebook.com%2Fmobileprotection%23%2Fmobileprotection: presence=EM349050375EuserFA21242090131A2EstateFDutF0Et2F_5b_5dEuct2F134904977B0Elm2FnullEtrFnullEtwF109102775EatF1349050374958Esb2F0CEchFDp_5f1242090131F1CC"
3	[HOP04B] [hop04b-LC2] [10.2.130.44] [1349050417] [ciscoipportwsa] [136] %CISCOIPORTWSA-4: 10.4.145.39 - - [30/Sep/2012:20:12:55 -0400] "GET http://www.facebook.com/ajax/typeahead/search/bootstrap.php?filter[0]=app&filter[1]=page&filter[2]=group&filter[3]=friendlist&viewer=1242090131&token=v7&lazy=1&__user=1242090131&__a=1" 200 127 TCP_MISS:DIRECT 120 ALLOW_WBRS_11-EMC_All_Top_Business_Relevant_Categories-EMC_All_Business_Relevant_Categories_1-Oubound_Malware_Scannng-NONE-NONE-DefaultGroup <C_a18.,7.4,"-","-",-,-,-,"-","-",-,-,"-","-",-,-,IW_snet,-,"-","-","Facebook General","Facebook","-","-",40.20.0,-,"-","-"> - s-ip= 69.171.237.16 s-port= 80 sc-bytes= 603 cs-username= - s-hostname= www.facebook.com cs-mime-type= application/x-javascript webcat-code= "a18.Custom.Allow.Social.Networking.Risk.Approved" cs-version= 1 cs-auth-group= - c-port= 51258 cs-bytes= 1055 wbrs-score= 7.4 wbrs-threat-reason= - wbrs-threat-type= - cs-user-agent= "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.2; .NET CLR 1.1.4322; MS-RTC LM 8; AskTbORJ/5.13.1.18107)" cs-referer= "http://www.facebook.com/mobileprotection" cs-cookie= "datr=-bhkUJj8LIoA6tAZ9evWwQk9; fr=0mOIxhcpC57z3QJnP.AWX5ZZVxAU9ed57K_nZaQsbAH9o.BQZLkF.C2.AWUNy8f7; lu=TgeLZTUBVYF0aMJ6u4o6PVWQ; c_user=1242090131;

This rule uses **${raw_log}** as a meta for querying raw log from sessions whose source IP address is NOT NULL.



Build Rule

Rule Type: Warehouse DB

Expert Mode: ☐

Name: $(raw_log)-Rule

Select: $(raw_log))

From: sessions

Alias:

Where: ip_src IS NOT NULL

Group By:

Having:

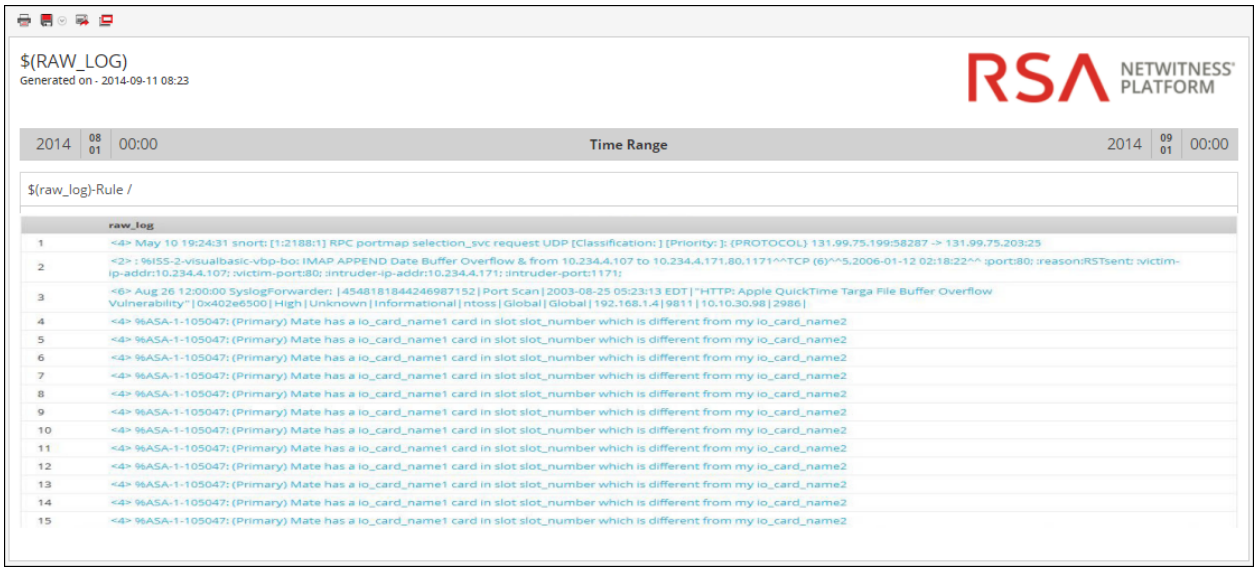
Order By:

Column Name	Sort By
Enter the column name...	Ascending

Limit: 50

Use | Save | Reset | Test Rule

The following figure shows the result set for querying raw logs from sessions.



$(RAW_LOG)
Generated on - 2014-09-11 08:23

RSA NETWITNESS PLATFORM

2014	08 01	00:00	Time Range	2014	09 01	00:00

$(raw_log)-Rule /

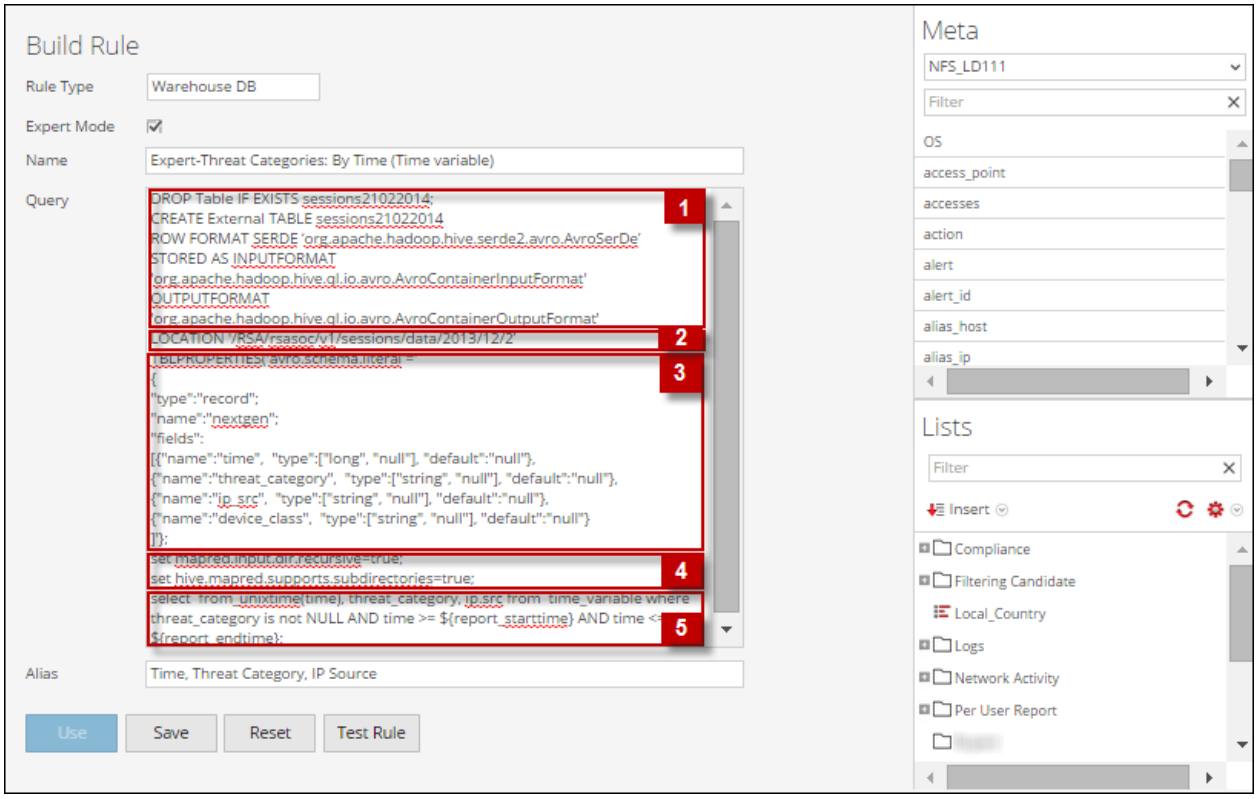
	raw_log
1	<4> May 10 19:24:31 snort: [1:2188:1] RPC portmap selection_svc request UDP [Classification:] [Priority:]: {PROTOCOL} 131.99.75.199:58287 -> 131.99.75.203:25
2	<2> : %IS5-2-visualbasic-vbp-bo: IMAP APPEND Date Buffer Overflow & from 10.234.4.107 to 10.234.4.171.80.1171^^TCP (6)^^5,2006-01-12 02:18:22^^ :port:80; :reason:RSTsent; :victim-ip-addr:10.234.4.107; :victim-port:80; :intruder-ip-addr:10.234.4.171; :intruder-port:1171;
3	<6> Aug 26 12:00:00 SyslogForwarder: |4548181844246987152| Port Scan |2003-08-25 05:23:13 EDT| "HTTP: Apple QuickTime Targa File Buffer Overflow Vulnerability"|0x402e6500|High|Unknown|Informational|ntoss|Global|Global|192.168.1.4|9811|10.10.30.98|2986|
4	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
5	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
6	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
7	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
8	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
9	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
10	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
11	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
12	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
13	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
14	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
15	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2

Warehouse DB Advanced Rules Syntax

The section explains the advanced rules query syntax and examples.

General Syntax of an Advanced Rule

The following figure shows how to define an advanced query.



The following syntax is an example of an advanced query:

```
DROP Table IF EXISTS sessions21022014;
CREATE External TABLE sessions21022014
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
STORED AS INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2'
TBLPROPERTIES('avro.schema.literal'='
 {
"type":"record";
"name":"nextgen";
"fields":
 [
 {"name":"time",  "type":["long", "null"], "default":"null"},
{"name":"threat_category",  "type":["string", "null"], "default":"null"},
```

```
{"name":"ip_src",  "type":["string", "null"], "default":"null"},
{"name":"device_class",  "type":["string", "null"], "default":"null"}
 ]
 '};
set mapred.input.dir.recursive=true;
set hive.mapred.supports.subdirectories=true;
```

select `from_unixtime(time), threat_category, ip.src` from `time_variable` where `threat_category` is not `NULL` and `time >= ${report_starttime}` and `time <= ${report_endtime};`

Note: Reporting Engine treats a line beginning with <hyphen> <hyphen> as a comment in Expert Warehouse Rule.
For example,

```
set mapred.input.dir.recursive=true;
-- This is an Expert comment
 set hive.mapred.supports.subdirectories=true;
```

The general syntax of an advanced query is as explained below:

1. Drop and create an external table, and then format the row:
   Firstly, we drop the table, if the table already exists and create an external table **sessions21022014**

   ```
   DROP TABLE IF EXISTS sessions21022014
    CREATE EXTERNAL TABLE sessions21022014
   ```

   Note: You must create an external table only if you are using an other table. For example, if you are using an other table apart from **sessions21022014** then you must drop the table and create an external table.

   Then, specify the row format as Avro.SerDe interface to instruct HIVE as to how a record is to be processed. Avro.SerDe allows you to read or write Avro data as HIVE tables and store them as input format and output format.

   ```
   ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.Avro.SerDe'
    STORED AS INPUTFORMAT
   'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
   ```

2. Specify the HDFS location:
   Secondly, you must specify the HDFS location '/RSA/rsasoc/v1/sessions/data/2013/12/2' from where the data is queried before executing the HIVE statements.The location parameter specifies the data to be fetched depending on the date input provided. This is a variable parameter hence you can fetch values depending on the date entered.

3. Define the table schema:
   Thirdly, you define the table schema by defining columns with a specific data type and default value as 'null'.

   ```
   TBLPROPERTIES('avro.schema.literal'='
    {"type":"record";
    "name":"nextgen";
    "fields":
    [
    {"name":"ip_src",  "type":["string", "null"], "default":"null"}
    ]
    '};
   ```

4. Import data from directory which contains sub directories:
   Then, you must enable HIVE to recursively scan all sub-directories and fetch all the data from all sub-directories.
   ```
   set mapred.input.dir.recursive=true;
   set hive.mapred.supports.subdirectories=true;
   ```
5. Fetch data from the HIVE table:
   Once you execute all the above statements, you can query the database with the HIVE query **select** clause to fetch the data from the HIVE table.

The following examples illustrate advanced rules in the expert mode:

- Hourly, daily, weekly, and monthly report
- Table partition based on location report
- Join logs and sessions based on unique_id report
- List report
- Parameterized report
- Partition based table with multiple locations
- Automated partition using custom function (10.5.1 onwards)

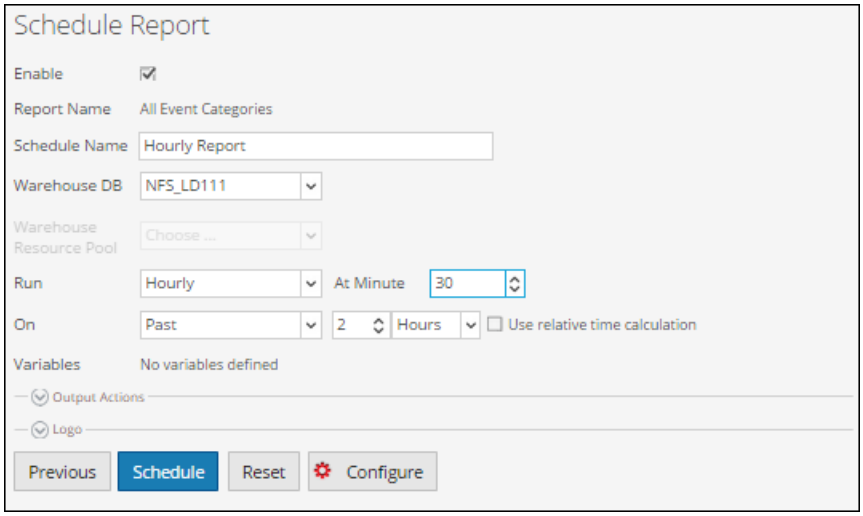
Hourly, Daily, Weekly, and Monthly Report

In these example rules, you can create various reports for December 02, 2013 (as in the below figure). The date variable in the LOCATION statement can be altered, depending on which you can create an hourly, daily, weekly, and monthly report.

Hourly Report

In this example rule, you can create an houly report for December 02, 2013. The LOCATION statement can be altered to generate an hourly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2' - the date input (2013/12/2) indicates year/month/day. The entire data for 02 December, 2013 is retrieved using this location statement.

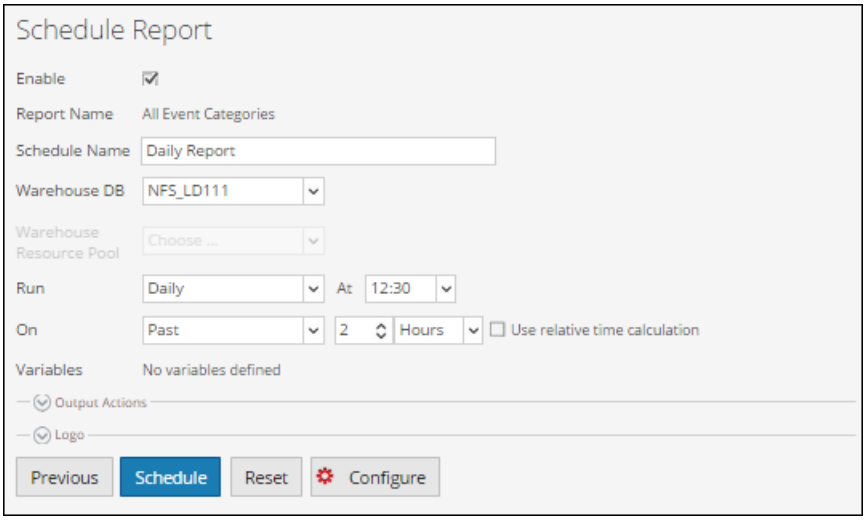


The result set of this query would be an hourly report.

Daily Report

In this example rule, you can create a daily report for December 2013. The LOCATION statement can be altered to generate a daily report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - the date input (2013/12) indicates year/month. The entire data for December, 2013 is retrieved using this location statement.

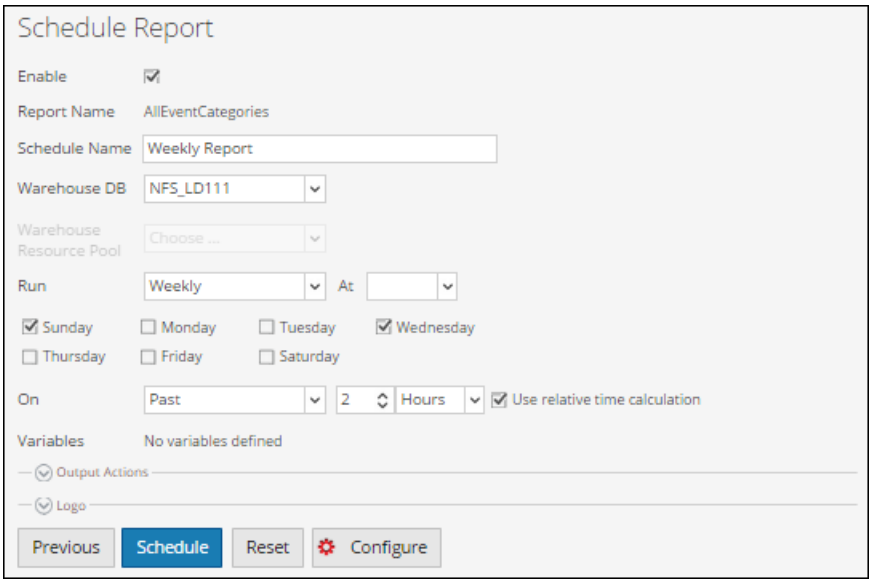


The resultset of this query would be a daily report.

Weekly Report

In this example rule, you can create a weekly report for December 2013. The LOCATION statement can be altered to generate a weekly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - the date input (2013/12) indicates year/month. The entire data for December, 2013 is retrieved using this location statement.

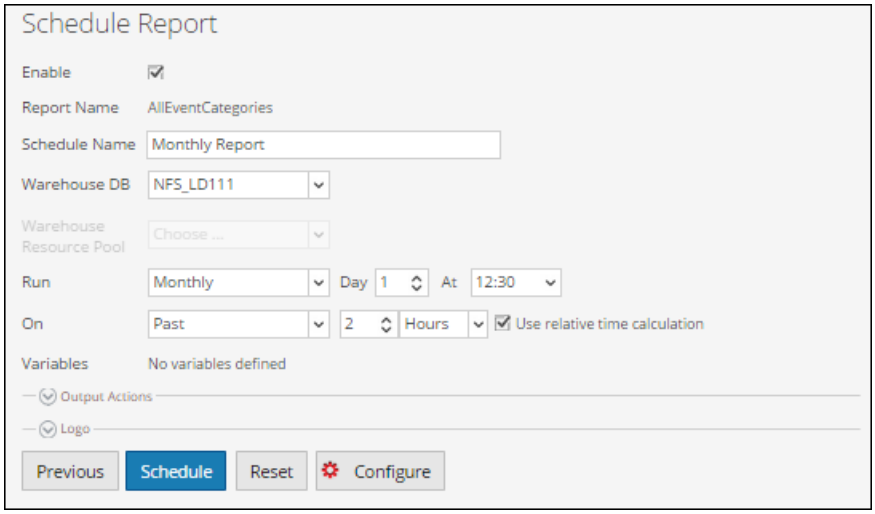


The result set of this query would be a weekly report.

Monthly Report

In this example rule, you can create a monthly report for the year 2013. The LOCATION statement can be altered to generate a monthly report.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013' - the date input (2013) indicates year. The entire data for the year 2013 is retrieved using this location statement.



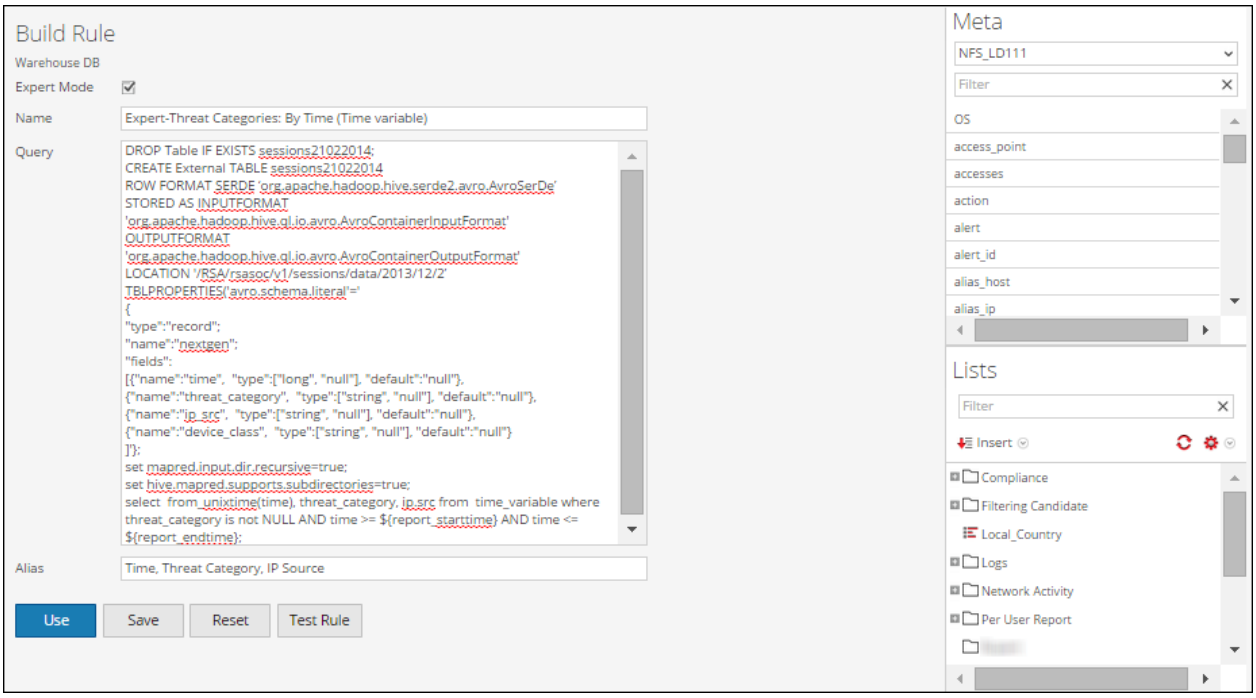
The result set of this query would be a monthly report.

For more information on LOCATION definition, see **Specify the HDFS location** in the **"General Syntax of an Advanced Rule"** section.

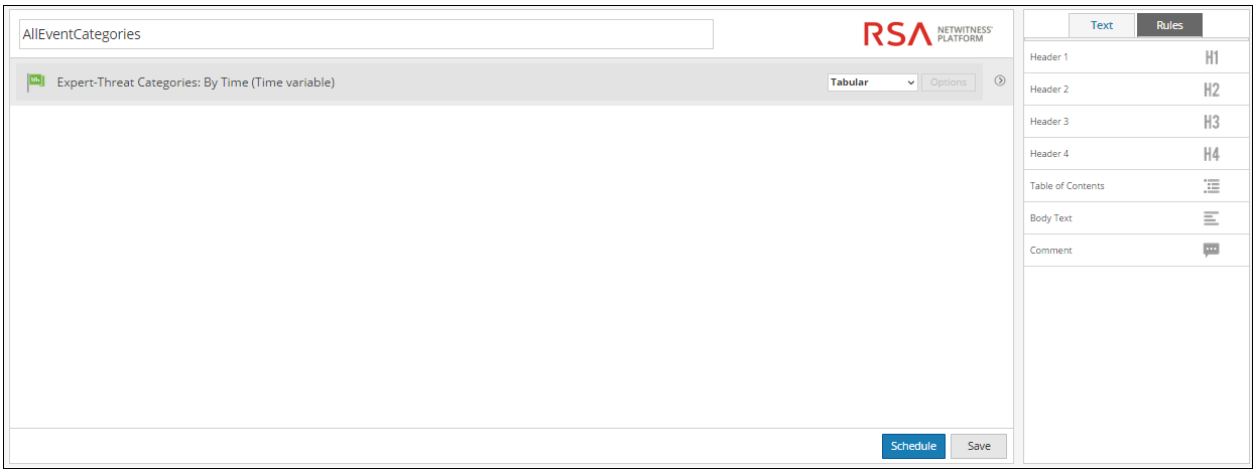
You must perform the following steps in sequence to view the resultset of an advanced rule:

1. Define an Advanced Rule
2. Add an advanced rule to a Report
3. Schedule a Report
4. View a scheduled Report

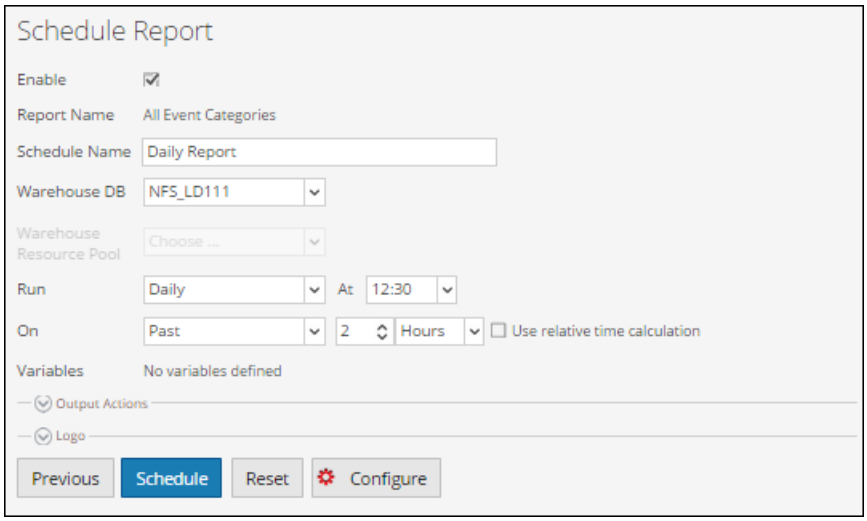
The following figure shows how to define an advanced rule.



The following figure shows how to add an advanced rule to a report (For example, **AllEventCategories**).



The following figure shows how to schedule a daily report.



If you want to generate a report for a specific time range, you need to manually define the time range in the query using the following two variables:

`${report_starttime} - The starting time of the range in seconds.`
`${report_endtime} - The ending time of the range in seconds.`

For example, `SELECT from_unixtime(time), threat_category, ip.src FROM time_variable WHERE threat_category is not NULL AND time >= ${report_starttime} AND time <= ${report_endtime};`

The following figure shows the result set of scheduling a daily report.

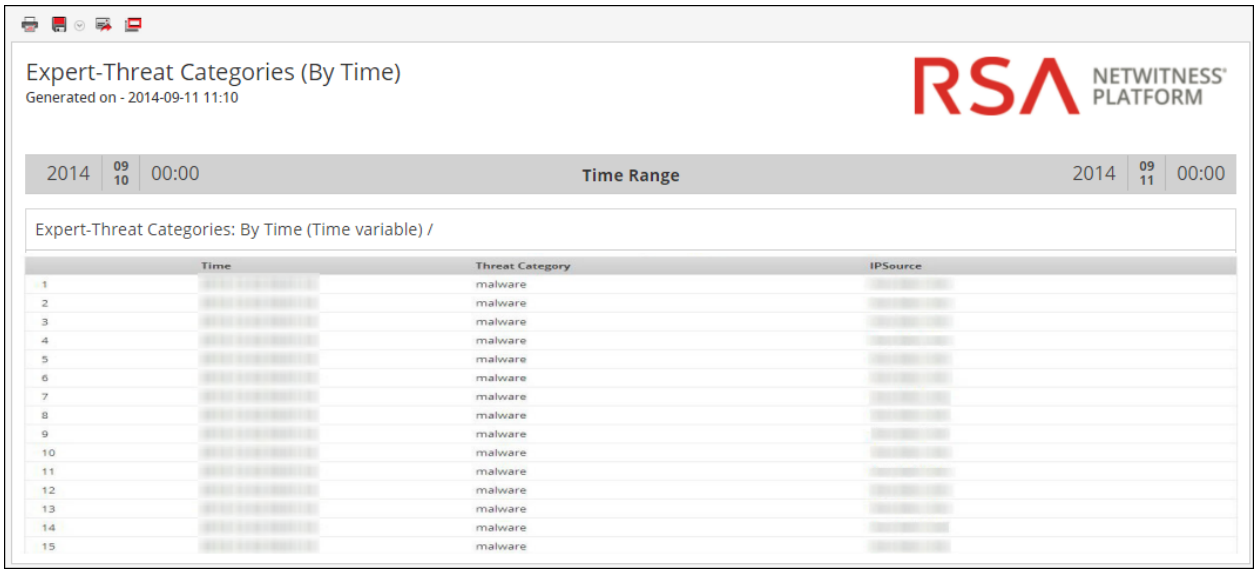
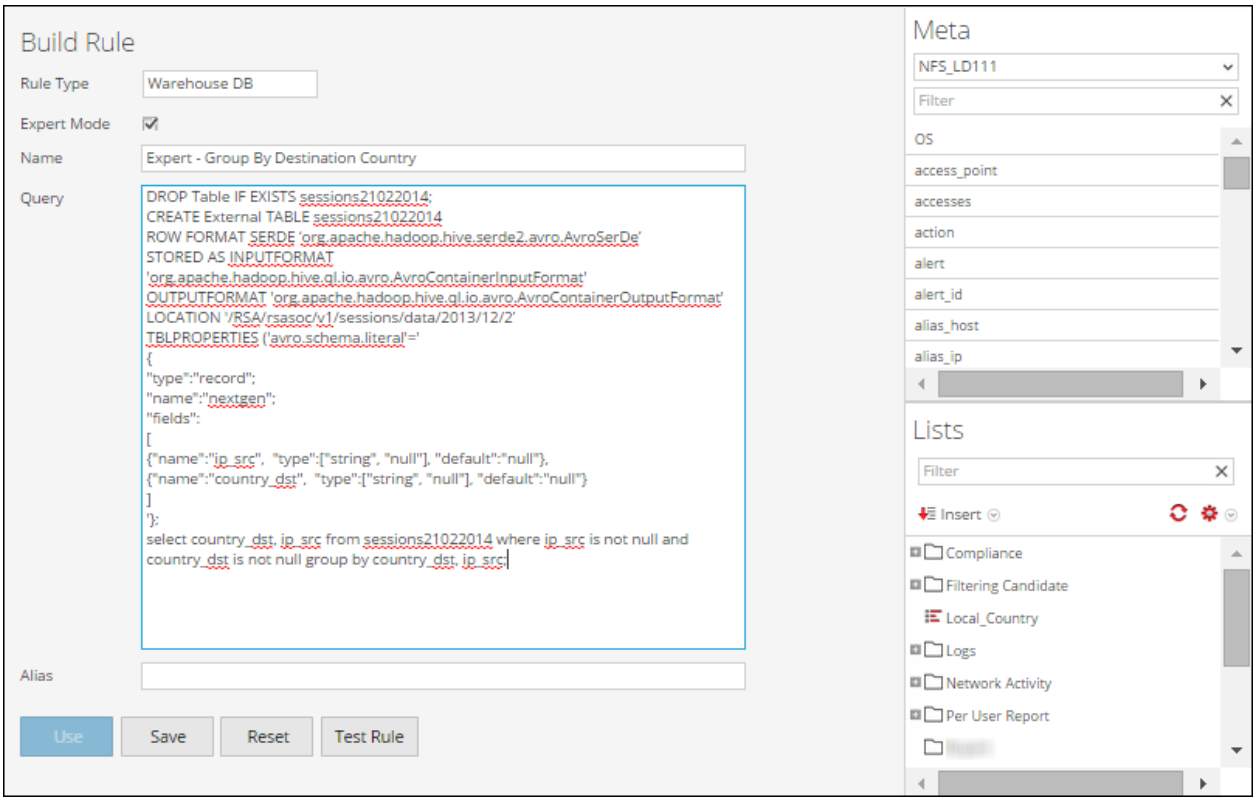


Table Partition Based on Location Report

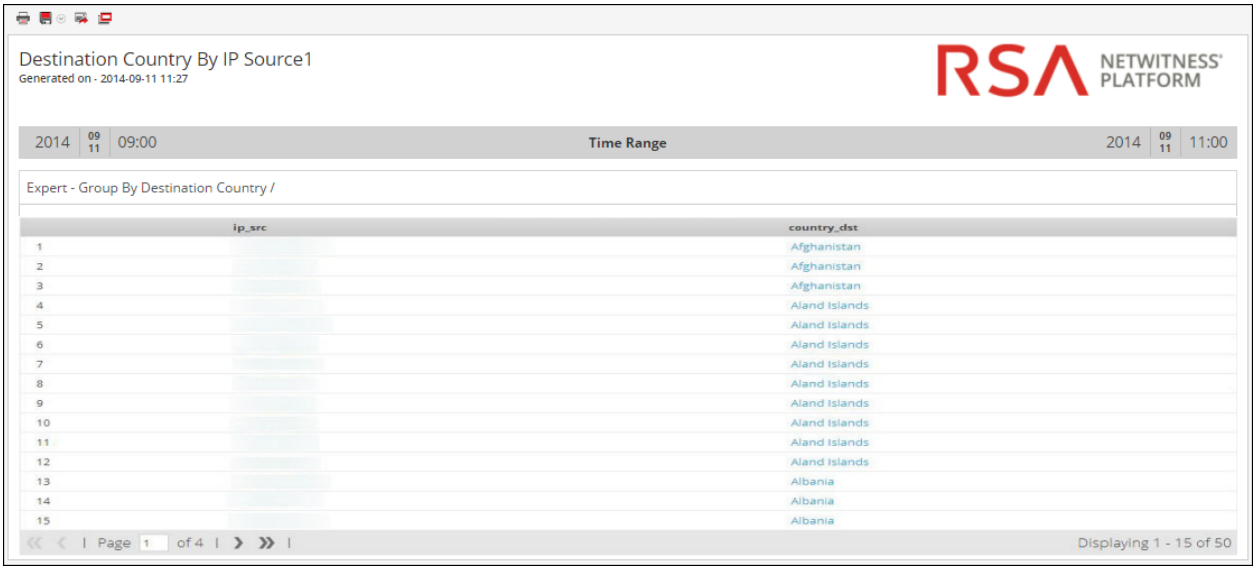
In this example rule, you can create a table partition based on location. Each table can have one or more partition keys which determines how the data is stored. For example, a country_dst of type STRING and an ip_src of type STRING. Each unique value of the partition keys defines a partition of the table.

In the example provided, we execute a HIVE query to fetch destination country and IP address of source from the sessions05032014 table and group the result set by these fields.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see "General Syntax of an Advanced Rule" section.



The following figure shows the result set of creating a table partition based on location report.

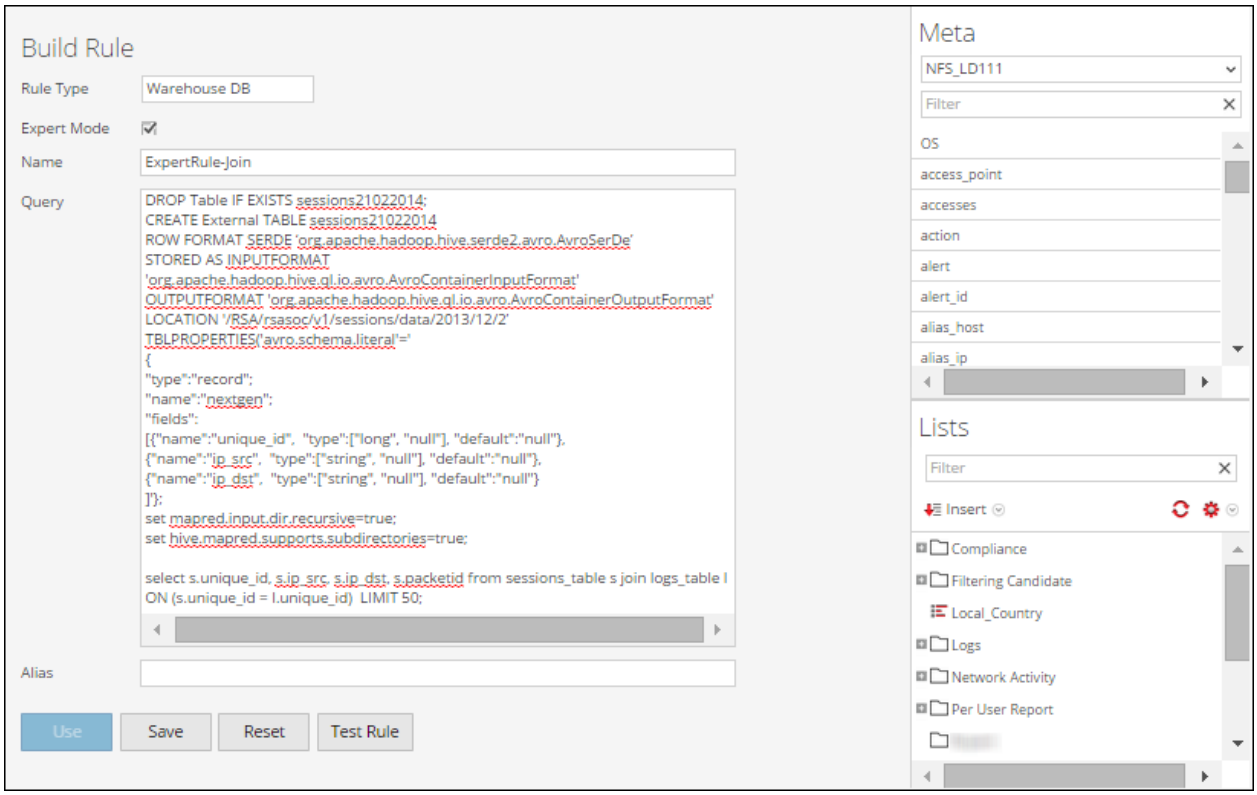


Join Logs and Sessions Based on unique_id Report

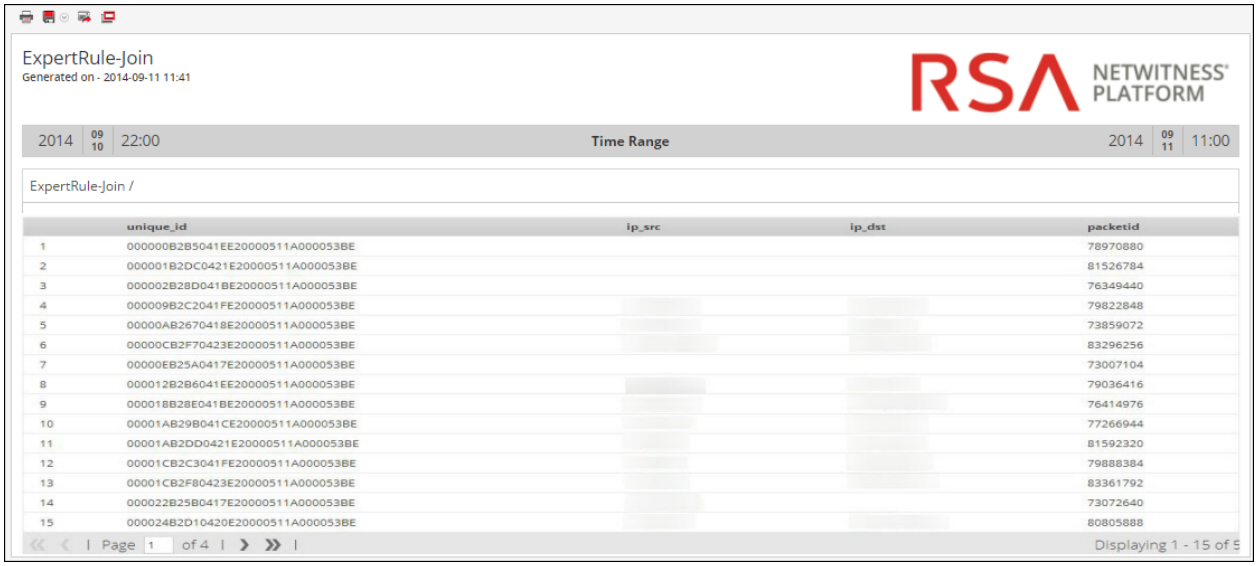
In this example rule, you can create a rule to join logs and sessions table to fetch unique_id, IP address of source and destination, and packet ID based on unique_id.

In the example provided, we execute a HIVE query to fetch certain fields from both the sessions_table and logs_table by performing a join based on the 'unique_id' field.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the **"General Syntax of an Advanced Rule"** section.



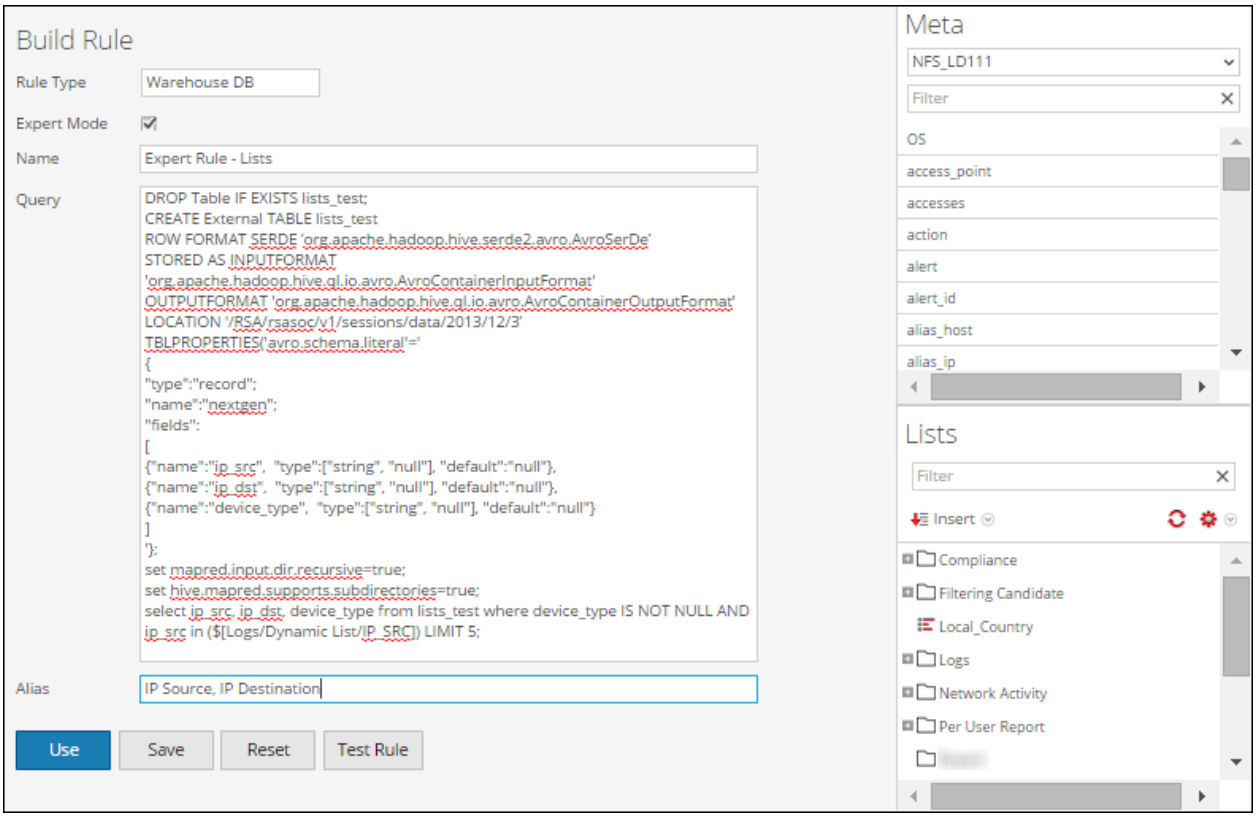
The following figure shows the result set of joining logs and sessions table based on unique_id.



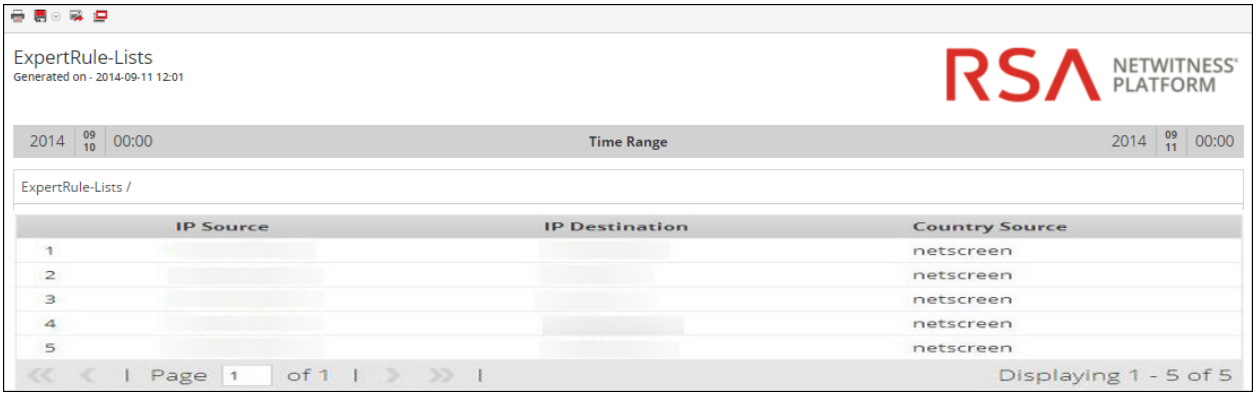
List Report

In this example rule, you can create a List report to fetch IP address of source and destination, and device type from the **lists_test** table where device type is not null and IP address of source is fetched from the appropriate event list.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the "General Syntax of an Advanced Rule" section.



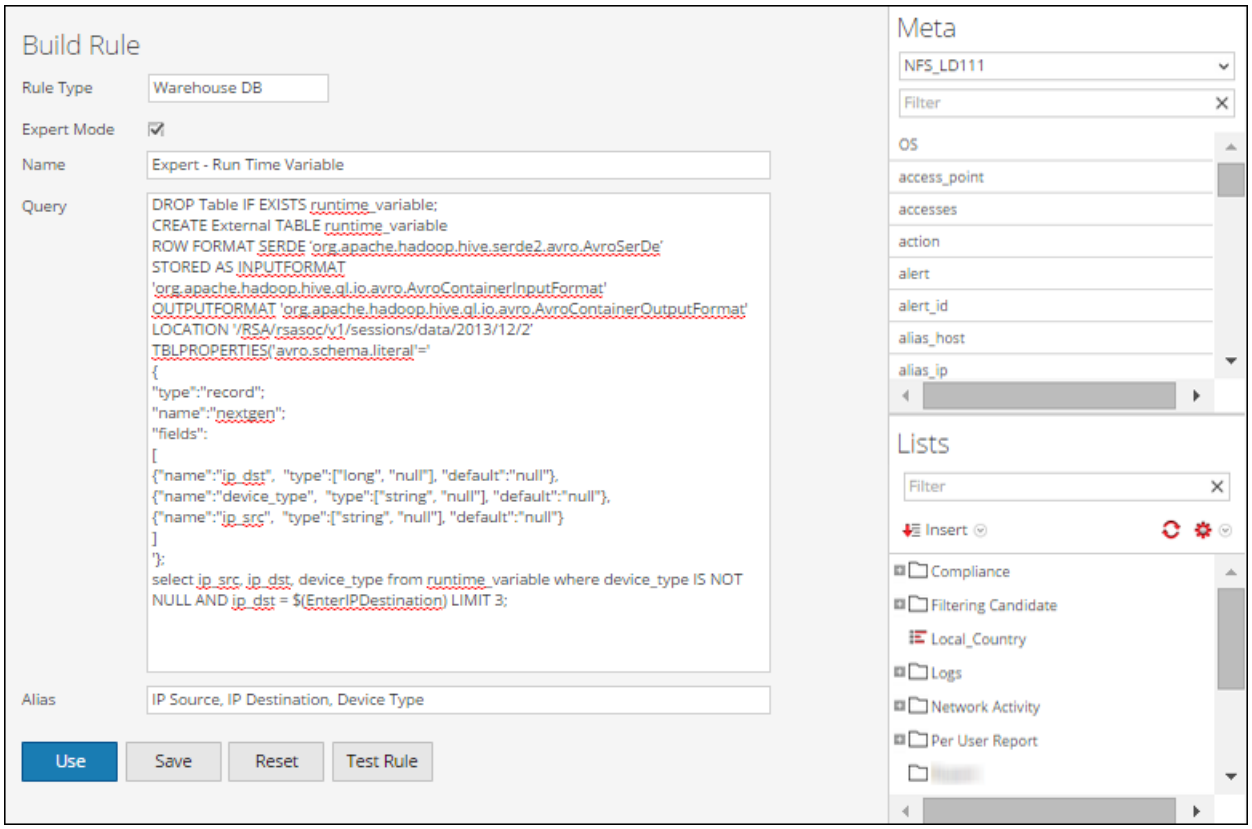
The following figure shows the result set of executing a list report.



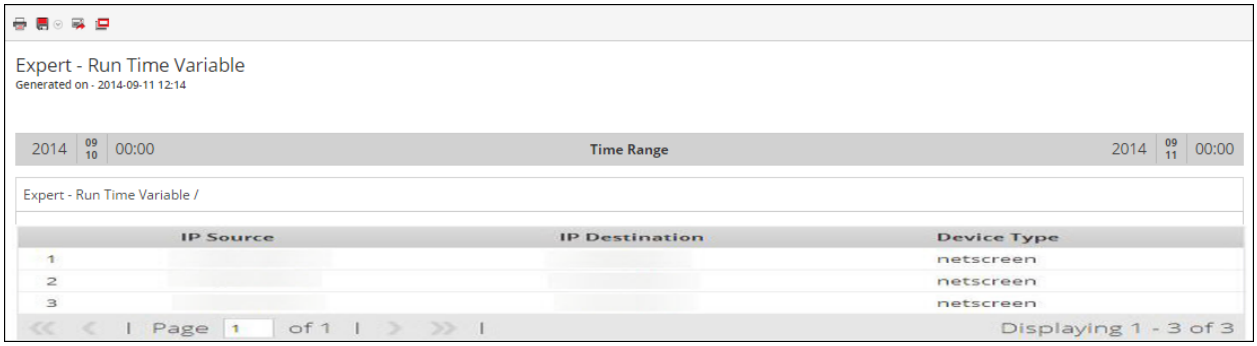
Parameterized Report

In this example rule, you can create a rule to fetch IP addresses of source and destination, and device type from the **runtime_variable** table based on the specified run time variable `${EnterIPDestination}`. At run time, you are prompted to enter a value for the IP address of destination ip_dst. Based on the value entered, the result set is displayed.

This rule provides information about the table created, row formatted, location (directory path) for avro data files in Warehouse, and returns a result set as per the HIVE query to indicate that the query returned a result set. For more information on these statements, see the "General Syntax of an Advanced Rule" section.



The following figure shows the result set of executing a parameterized report.



Partition Based Table with Multiple Locations

The following is an example of partition based table with multiple locations:

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
 {"name":"sessionid", "type":["null", "long"], "default" : null},
 {"name":"time", "type":["null", "long"], "default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
 SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >= ${report_
starttime} AND time
 <= ${report_endtime};
```

The partition based table with multiple location is as explained below:

1. Enable HIVE to recursively scan all sub-directories and read all the data from the sub-directories.
   ```
   set mapred.input.dir.recursive=true;
    set hive.mapred.supports.subdirectories=true;
   ```
2. Drop and create an external table, and then format the rows:
   ```
    DROP TABLE IF EXISTS AVRO_COUNT;
    CREATE EXTERNAL TABLE AVRO_COUNT
    PARTITIONED BY (partition_id int)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
    WITH SERDEPROPERTIES (
    'avro.schema.literal'='{
    "name": "my_record", "type": "record",
    "fields": [
    {"name":"sessionid", "type":["null", "long"], "default" : null},
    {"name":"time", "type":["null", "long"], "default" : null}
    ]}'
    )
   ```

```
STORED AS
INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
```

Note: You must create an external table only if you are using any other table. For example, if you are using any other table apart from **AVRO_COUNT** then you must drop the table and create an external table.

Note: Points to remember when you create a table:
- Dropping a 'non-external' table deletes the data.
- The table is partitioned on a single column called partition_id and this is the standard column for Reporting Engine.
- The default value of any column is null as the AVRO file may not contain the specified column.
- The column names should be in the lowercase as HIVE is case insensitive but AVRO is case sensitive.
- You must specify **avro.schema.literal** in the *SERDEPROPERTIES* .

For more information on the "rule syntax", refer to *Apache HIVE*.

3. Add partitions:
   Once you define a table, you must specify the HDFS locations from where the data needs to be queried before you execute the HIVE statements.The location parameter specifies the data to be fetched depending on the specified date. The data is spread across multiple locations or directories in HDFS. For each location you need to add a partition with unique values assigned to the partition column. The locations can be any directory in the HDFS

```
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
```

   Note: HIVE reads each file in these locations as AVRO. Incase if there is a non-AVRO file available in one of these locations then the query may fail.

4. Run the query

```
SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >= ${report_
starttime} AND time
<= ${report_endtime};
```

   When a table is created, you can execute specific queries to filter the data. For example, after you create the table you can filter the data as shown in the below examples:
   Sessions with a specific Source IP Address:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime} AND time
<= ${report_endtime}  AND ip_src = '127.0.0.1';
```

Group by based on user destination:

```
SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime} AND time
<= ${report_endtime}  GROUP BY usr_dst;
```

Automated Partition using Custom function

In 10.5.1, you can use the custom function to automate the addition of partitions to a user defined table in the expert mode.

General syntax

```
RE WH CUSTOM ADDPARTITIONS(table, namespace, rollup, [starttime,
endtime])
```

The following table describes the custom function syntax:

S.No	Name	Description
1	table	The table name for which the partition has to be added.
2	namespace	The namespace can be sessions or logs.
3	rollup	This value determines the level of directory path to be included in partitions. The value can be HOUR, DAY, or MINUTE. If Warehouse Connector is configured for Day rollup, setting this value as HOUR produces ZERO results. The number and location of each partition is based on time range used to run the rule and the rollup value.
4	(Optional) starttime, endtime	To generate partitions for a specific time range other than the time range mentioned in the rule, you must specify the starttime and endtime in **Epoch Seconds**. **Note:** Expressions are not supported for the starttime and endtime.

The custom function is invoked when Reporting Engine executes the rule either during test rule or scheduled report. While running a expert rule, whenever Reporting Engine identifies the function declaration, it extracts the required arguments and insert *n* number of ADD PARTITION HiveQL statements and executes them on the Hive Server.

The location and directory structure is determined by the argument passed in the rule and the Hive data source configuration in Reporting Engine. The number of partitions depends on the rollup specified and the time range used while executing the rule. For example, with the rollup as HOUR and the time range as PAST 2 Days results in 48 partitions for 48 Hours while with the rollup as DAY, Reporting Engine creates 2 partitions, one for each day.

The partition query is generated by the Syntax Template as set in Reporting Engine's Hive Configuration attribute AlterTableTemplate.

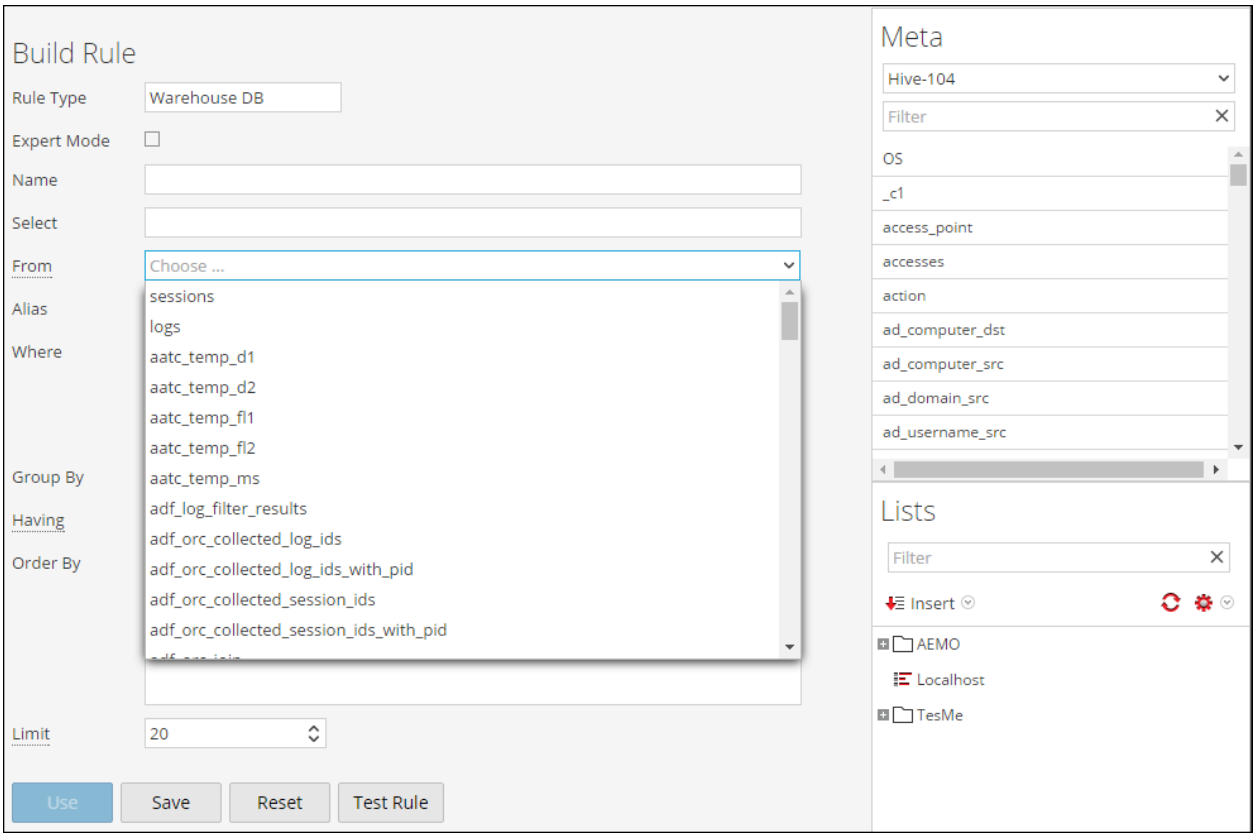
Note: By default, this function starts adding partitions to a table with partition id from 0 to N-1. Hence this requires that the table must be partitioned by single integer column named partition id.

The following is an example of automated partition using custom function:

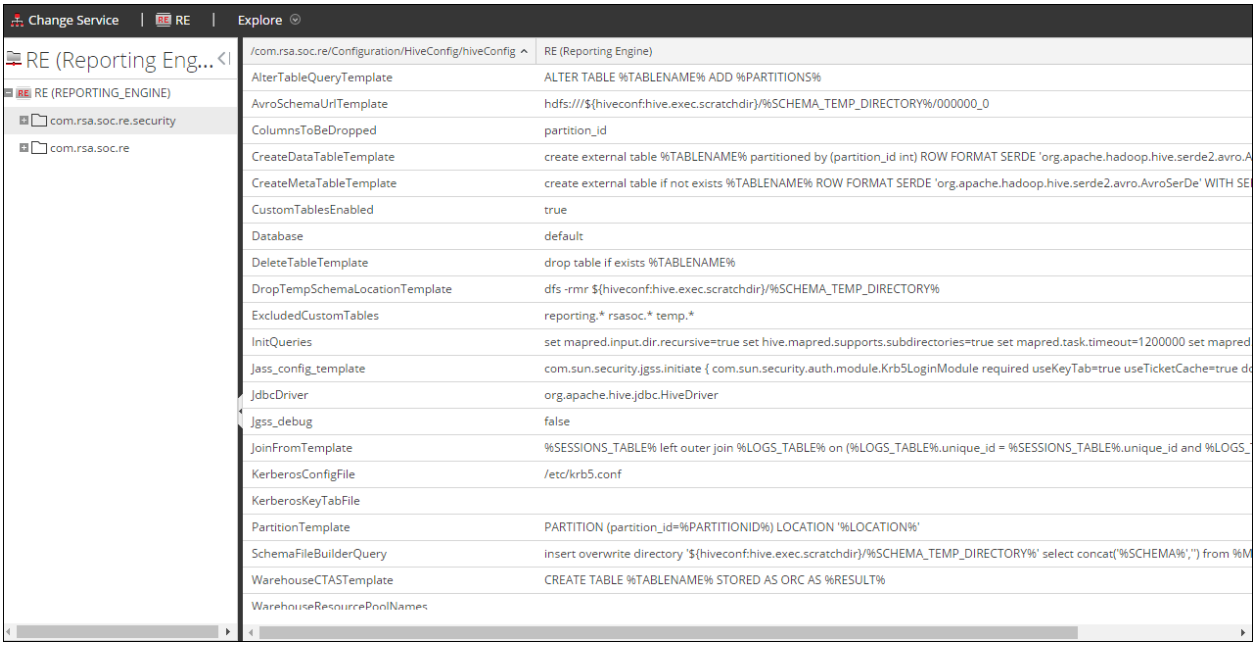
```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;

CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
  "name": "my_record", "type": "record",
  "fields": [
  {"name":"sessionid", "type":["null", "long"], "default" : null}
  ,{"name":"time", "type":[ "null" , "long"], "default" : null}
  ,{"name":"unique_id", "type":["null", "string"], "default" : null}
  ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';

RE_WH_CUSTOM_ADDPARTITIONS(AVRO_COUNT, 'sessions', 'DAY');
 SELECT COUNT(*) as TotalSessions FROM AVRO_COUNT
 WHERE time >= ${report_starttime} AND time <= ${report_endtime};
```

Creating Custom Tables Report

In 10.6.1, you can use and create Custom Tables on the Hive Server. Reporting Engine supports running queries on user defined tables and the ability to create a new table from a Single Rule output. When this feature is enabled in the Warehouse Rule Builder UI, user can see a list of custom tables available in Hive Server.



To enable this feature set **customTablesEnabled** to **TRUE** by navigating to **Reporting Engine** -> **Explore** ->**Hive Config**.



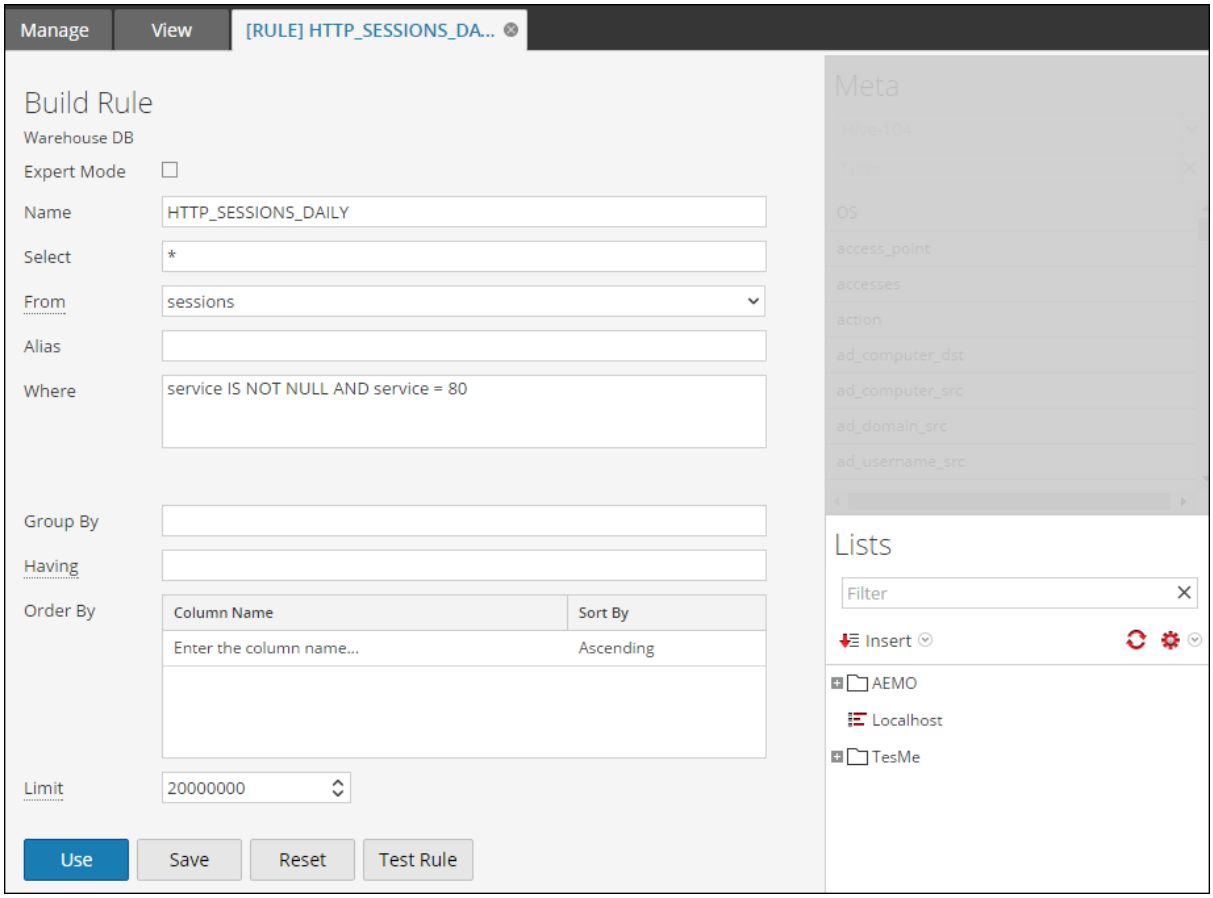
Creating Custom Table from Regular Rules

To schedule a report which contains a single SAW rule, a new text input with a **Warehouse CTAS Name** is added. The user can now specify a Custom Table name that will be created out of the output of the rule in Report.

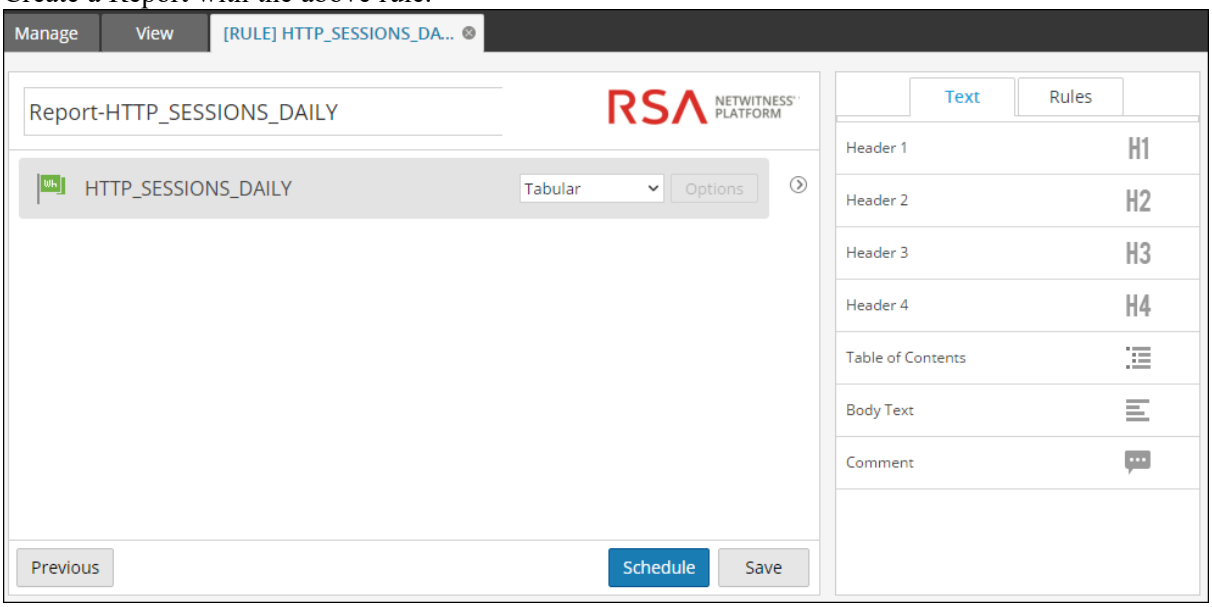
Note: This feature is available only if the Report contains a single SAW rule on the Schedule page. Otherwise, this option is hidden.

The process to use the feature is explained below:

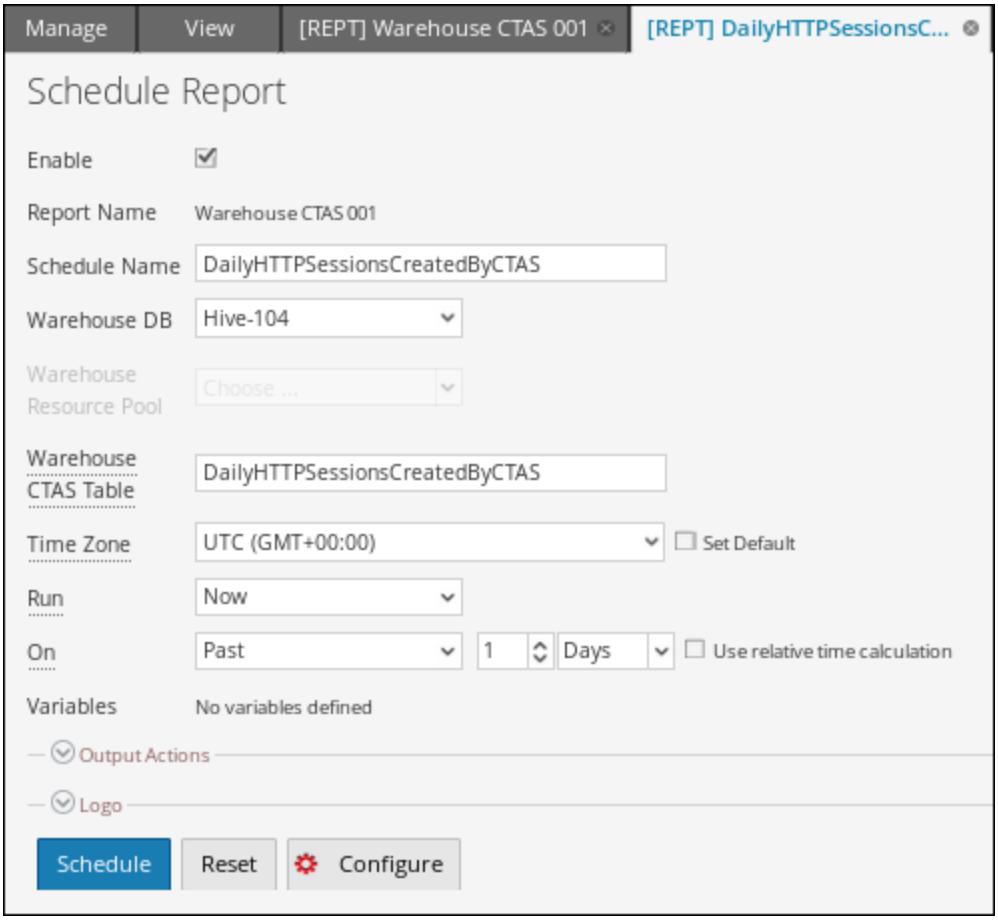
1. Create a rule to filter with data in SAW.



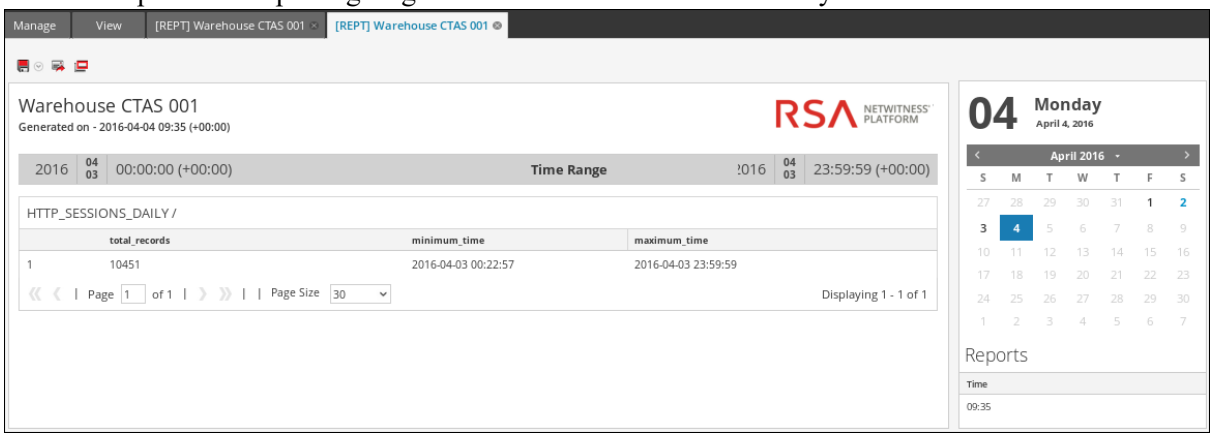
2. Create a Report with the above rule.



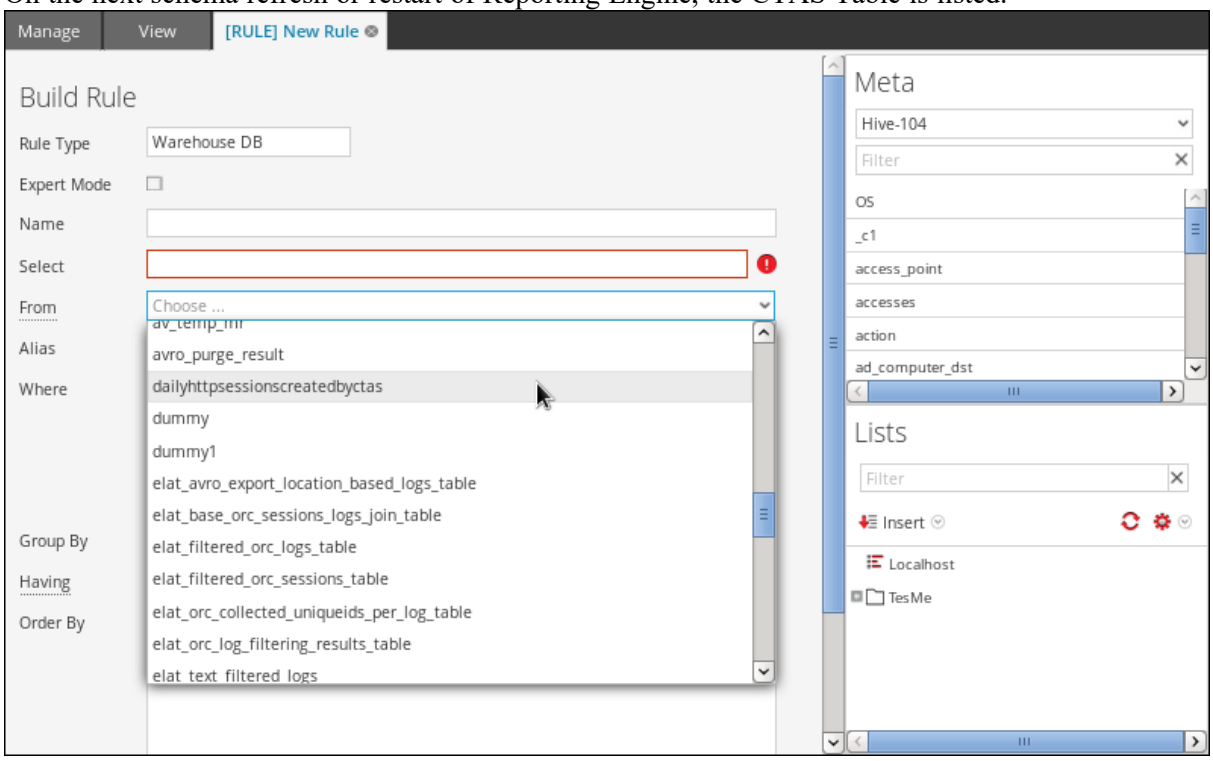
3. Create a Schedule and enter the CTAS Table Name.



4. Run the Report and Reporting Engine will create the Result Summary as below for the Schedule.



5. On the next schema refresh or restart of Reporting Engine, the CTAS Table is listed.



Task Scheduler for Warehouse Reporting

A task scheduler in a Hadoop cluster schedules the jobs consisting of tasks, and allocates specific resources to each job running in a cluster. By default, the task scheduler allocates equal number of resources to all the jobs. For example, if 10 jobs are running they will share resources of the cluster equally. However, you can configure the task scheduler to control the execution of the jobs such that one job runs faster than others by allocating more resources (pools or queues) to the job. This helps you prioritize to run a few reports over others.

Features

NetWitness supports two task schedulers:

- Fair Scheduler (`org.apache.hadoop.mapred.FairScheduler`)
- Capacity Scheduler (`org.apache.hadoop.mapred.CapacityTaskScheduler`)

Fair Scheduler

This scheduler divides the total capacity of the cluster into logical pools. You can submit a job to any one of these pools. All the jobs submitted to a pool share the resources allocated to the pool only. Once a pool has free resources, the freed resources are given to other pools with jobs running. For example, a fair scheduler has 100% resources with two pools namely Pool A and Pool B which share the total resources at 40% and 60% respectively. If Pool A has four jobs running, it allocates 10% resources to each job. When the four jobs are completed, the freed resources are allocated to Pool B.

Note: You can configure a pool to run more than one job in parallel.

Capacity Scheduler

This scheduler divides the total capacity of the cluster into queues. Each queue is allocated a pre-configured share of the total capacity. A job may be submitted to any of these queues. If more than one job is submitted to the same queue, the jobs will be executed sequentially. For example, if a capacity scheduler has 100% resources with three queues namely the Default, Low and High and they share the total resources at 20%, 30% and 50% respectively. If Default has two jobs D1 and D2, Low has three jobs L1, L2 and L3, and High has four jobs H1, H2, H3 and H4, these jobs are executed in their respective queues sequentially. If the jobs in a queue are completed, the freed resources will not be distributed to other queues.

Query Aggregates

This section explains the supported aggregate functions.

Supported Aggregate Functions

The following table lists the supported Aggregate Functions.

Aggregate Function	Description	Input data types	Output data types
count	Returns the count of meta values, which includes duplicate values as well.	Numeric	Numeric
countdistinct	Returns the total number of distinct or unique values.	Numeric	Numeric
distinct	Returns all the unique values.	Any	Any
first	Returns the first occurrence of the meta value.	Any	Same as input
last	Returns the last occurrence of the meta value.	Any	Same as input
sum	Returns a sum of all non-NULL values of metaKey in a group.	Numeric	Numeric
avg (Average)	Returns the average value of all non-NULL values of the metaKey within a group.	Numeric	Numeric
min (Minimum)	Returns the minimum for all values of metaKey in each group. This value is based on order by field.	Any	Any
max (Maximum)	Returns the maximum for all values of metaKey in each group. The maximum value is the value that is returned by order by field.	Any	Any
length	Returns the length of the values of metakey. This is called a "scalar function" in SQL.	Any	Numeric

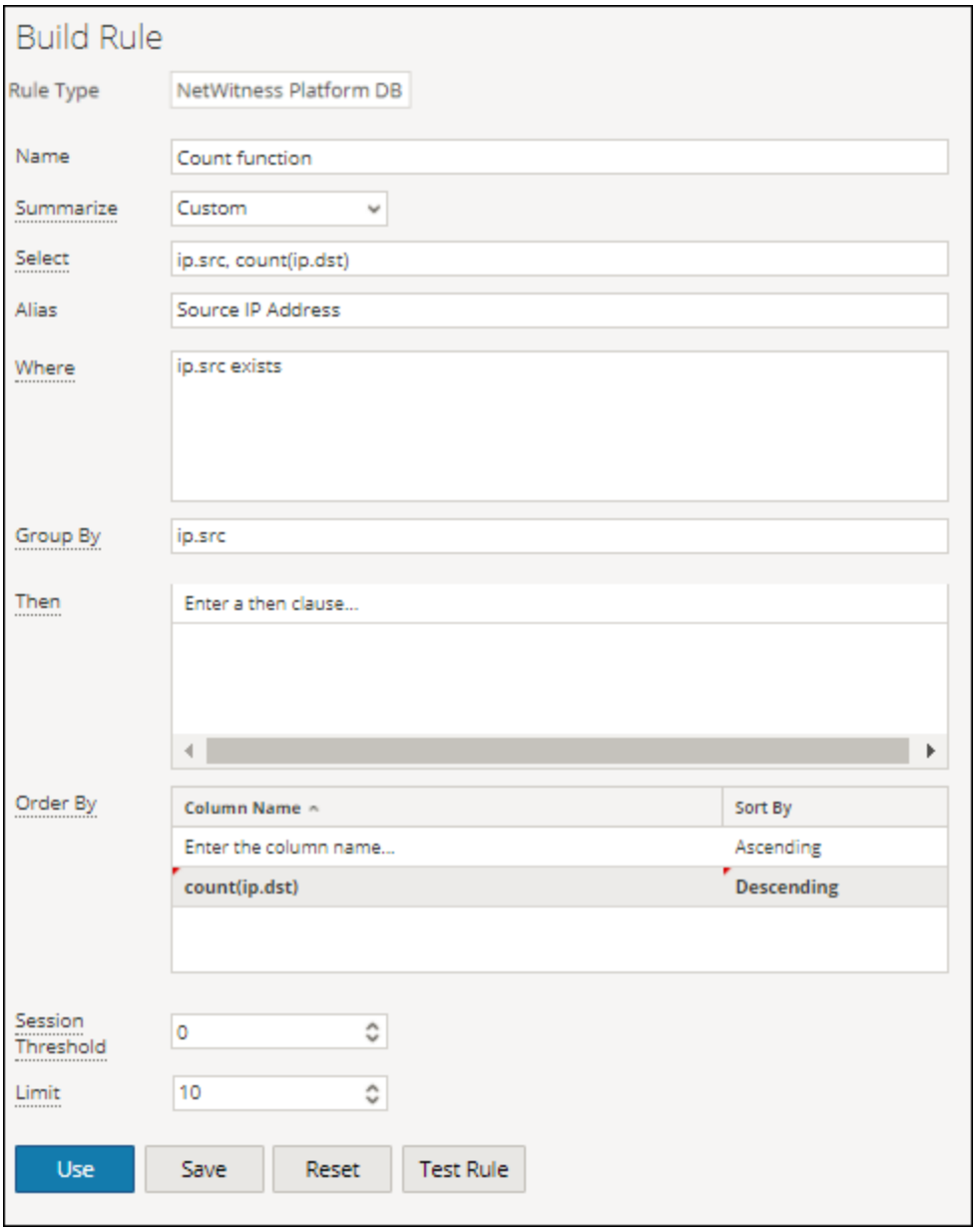
Examples of Queries and Results per Function

Count

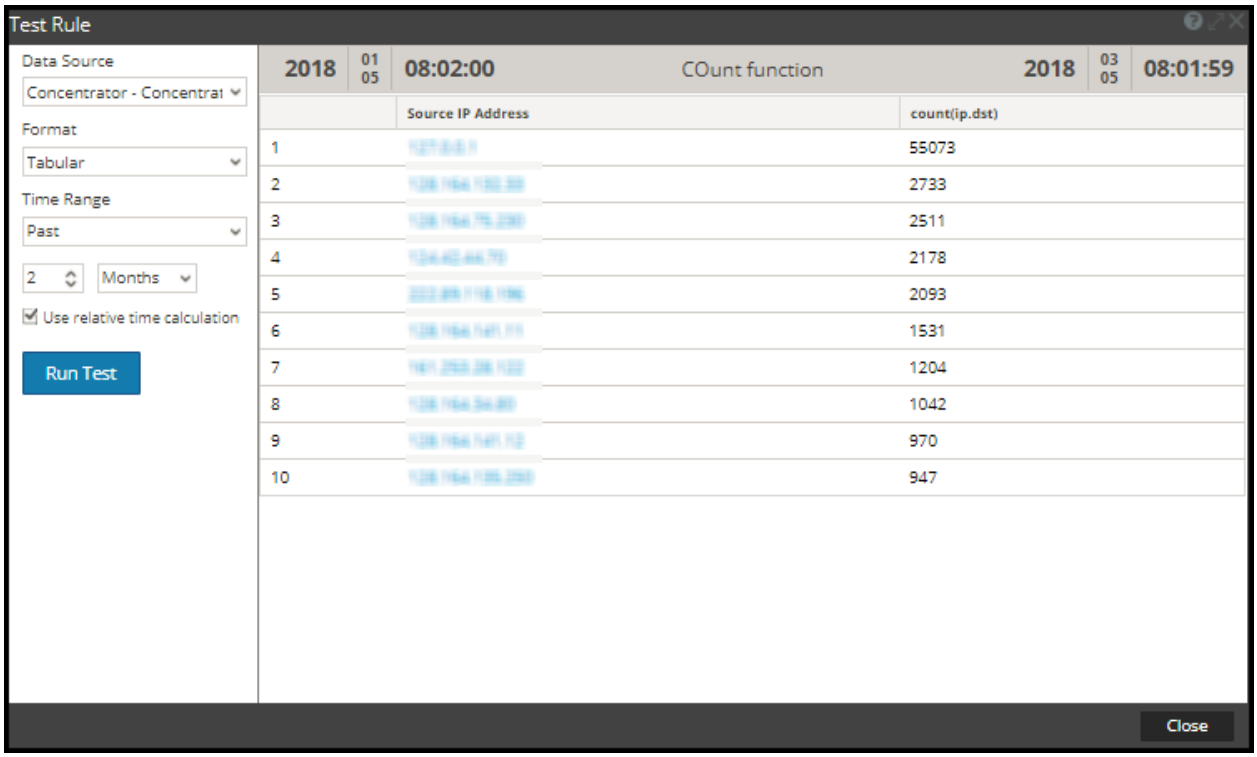
This function returns the number of values for a specified meta key, that exclude null values but include duplicate ones. .

Example

The following figure shows a sample query for count function used for the destination IP and the respective source IP.



The following figure shows the result for the above query.



Here, for each unique ip.src (source IP), the page returns the total number or count of ip.dst (destination IP) values, which include the duplicate values as well.

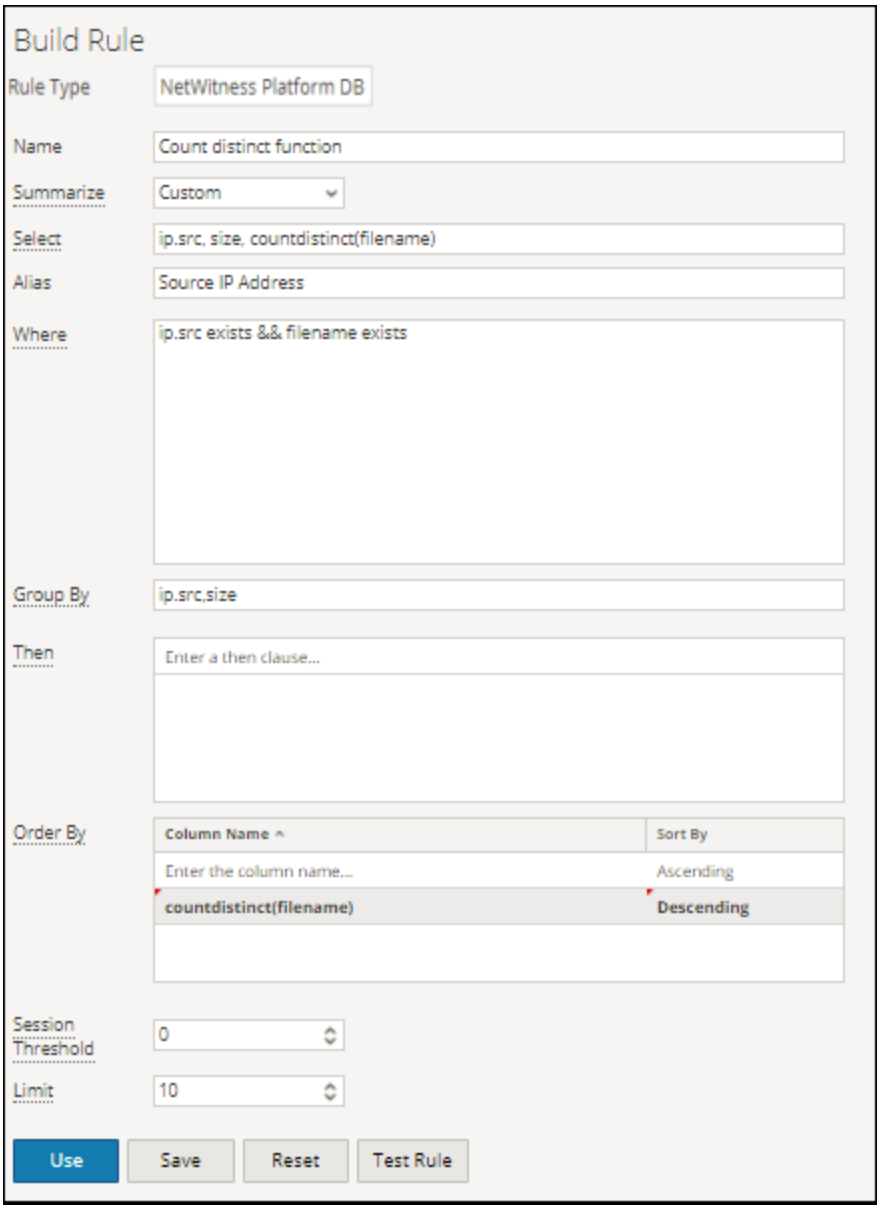
Note: If your NetWitness is currently on 10.5 or newer version and any of the NetWitness Core devices are on 10.3 or 10.4 versions, then some of the aggregate functions may display unexpected errors. However, aggregate functions such as sum() and count() are supported in 10.4 version.

Countdistinct

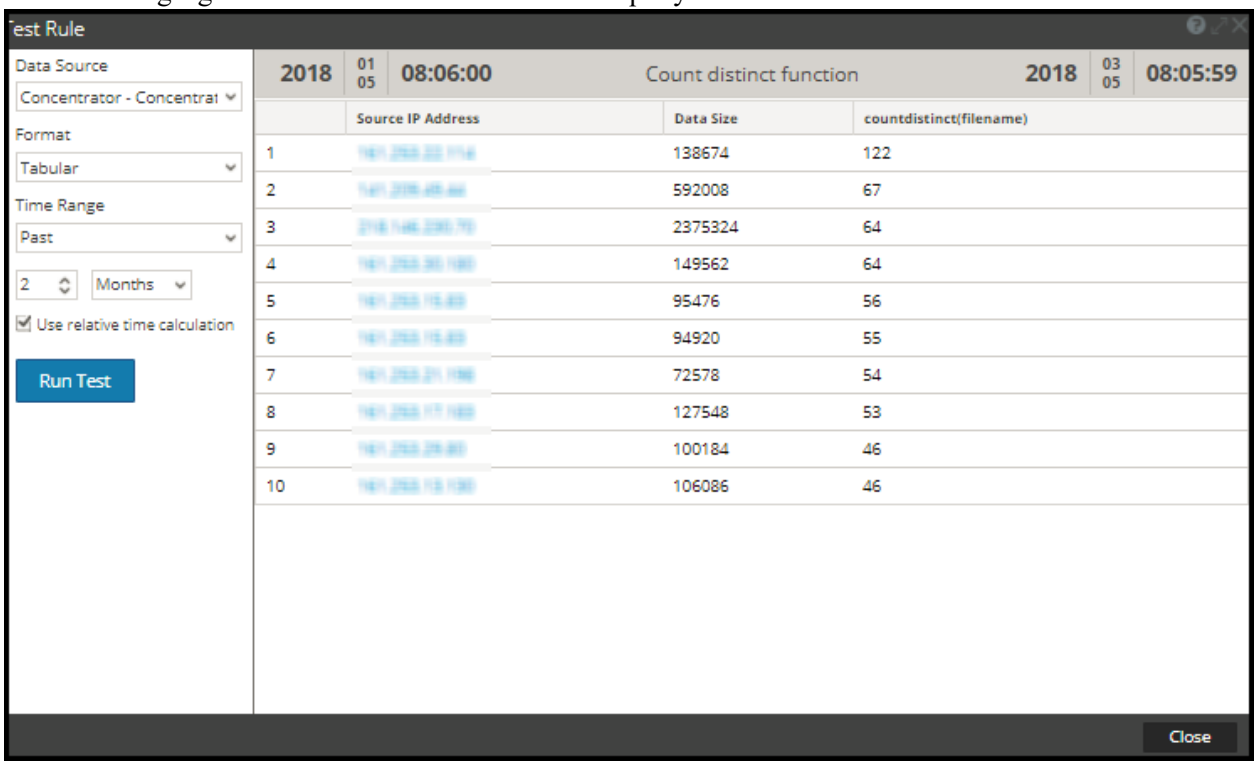
The countdistinct function returns the count of unique or distinct values for the metakey. In other words, countdistinct function can be used to retrieve a number of distinct values for the specified metakey.

The following figure shows a sample query where the countdistinct function is used along with IP source (ip.src) and data size(size).

Example


Build Rule
Rule Type
NetWitness Platform DB
Name
Count distinct function
Summarize
Custom
Select
ip.src, size, countdistinct(filename)
Alias
Source IP Address
Where
ip.src exists && filename exists
Group By
ip.src,size
Then
Enter a then clause...
Order By
Column Name
Sort By
Enter the column name...
Ascending
countdistinct(filename)
Descending
Session Threshold
0
Limit
10
Use
Save
Reset
Test Rule

The following figure shows the result for the above query.



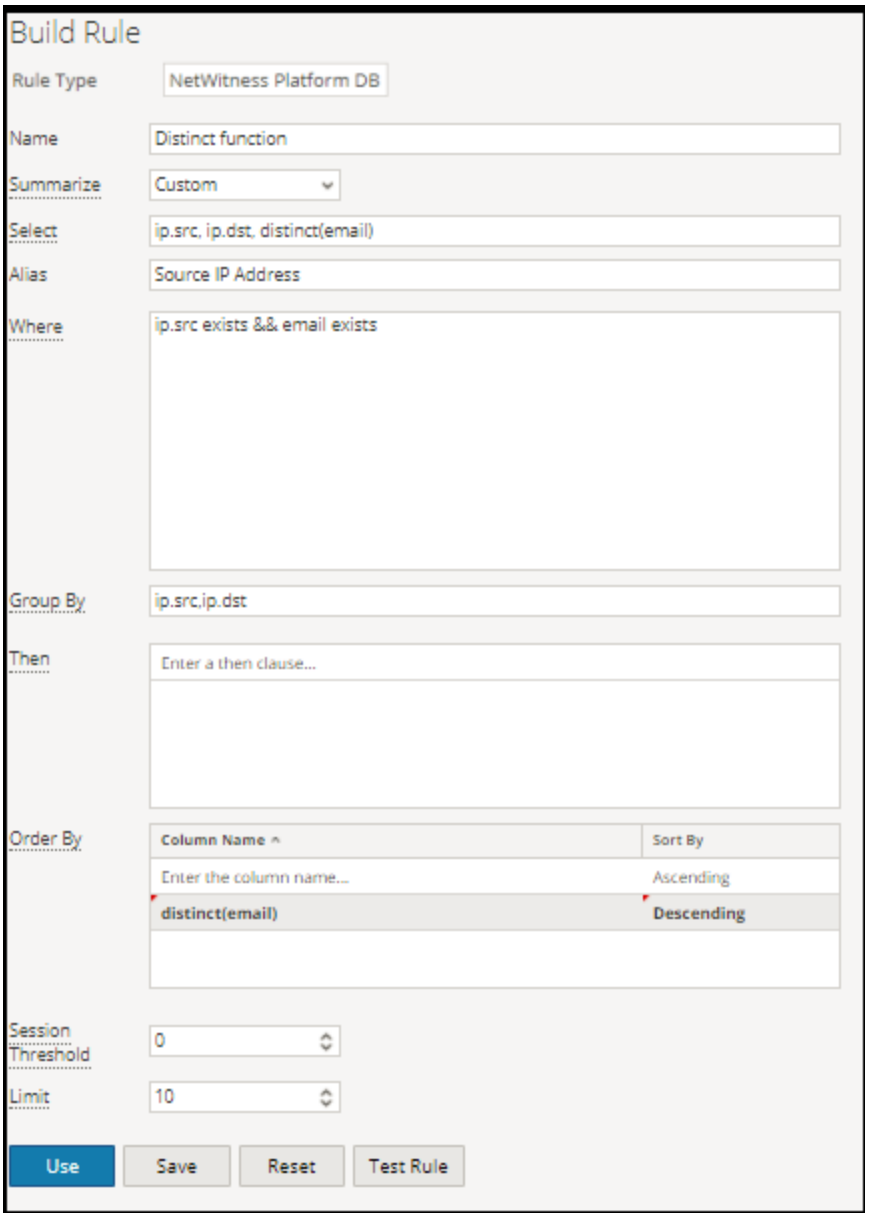
Here, the page displays the data size along with the total number or count of distinct filenames from the respective IP source. Unlike the count function, the countdistinct excludes the duplicate values from the result.

Distinct

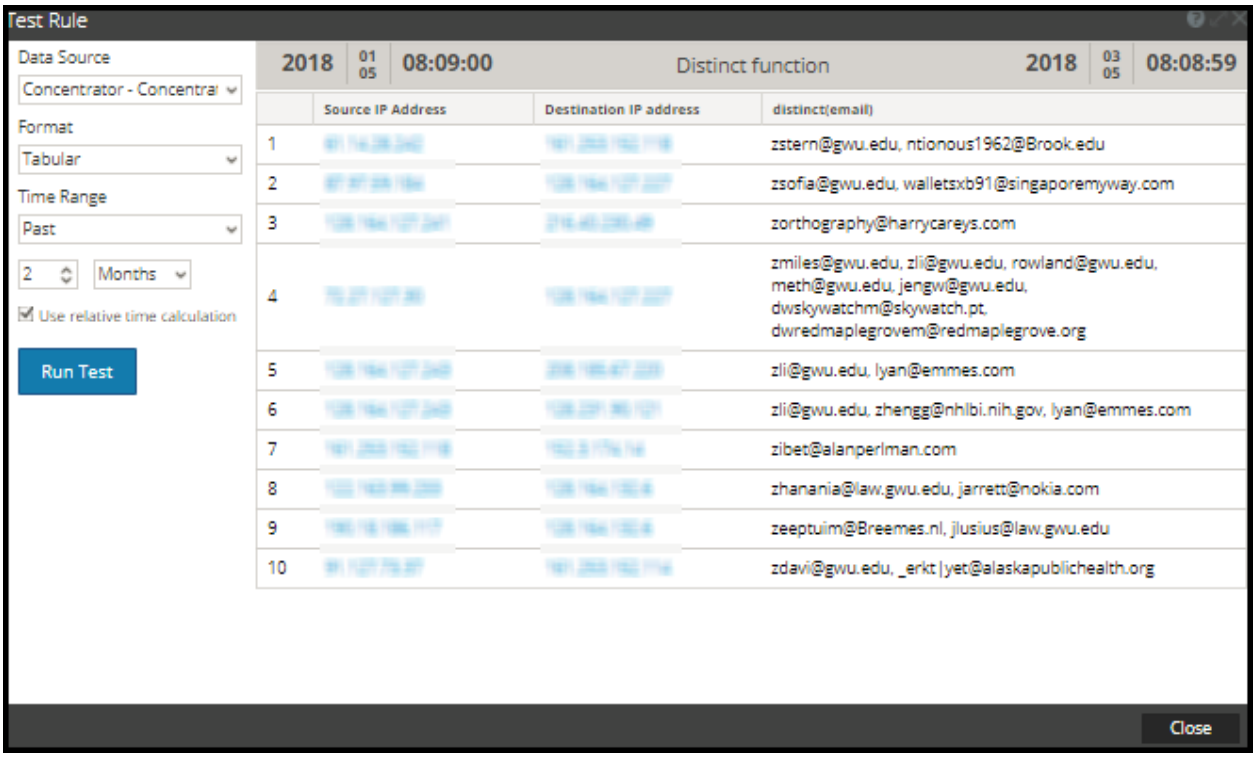
This function returns all the unique or distinct values of the metakey.

Example

The following figure shows a sample query for distinct function used to retrieve e-mails, between various source and destination IP (ip.dst).



The following figure shows the result for the above query.



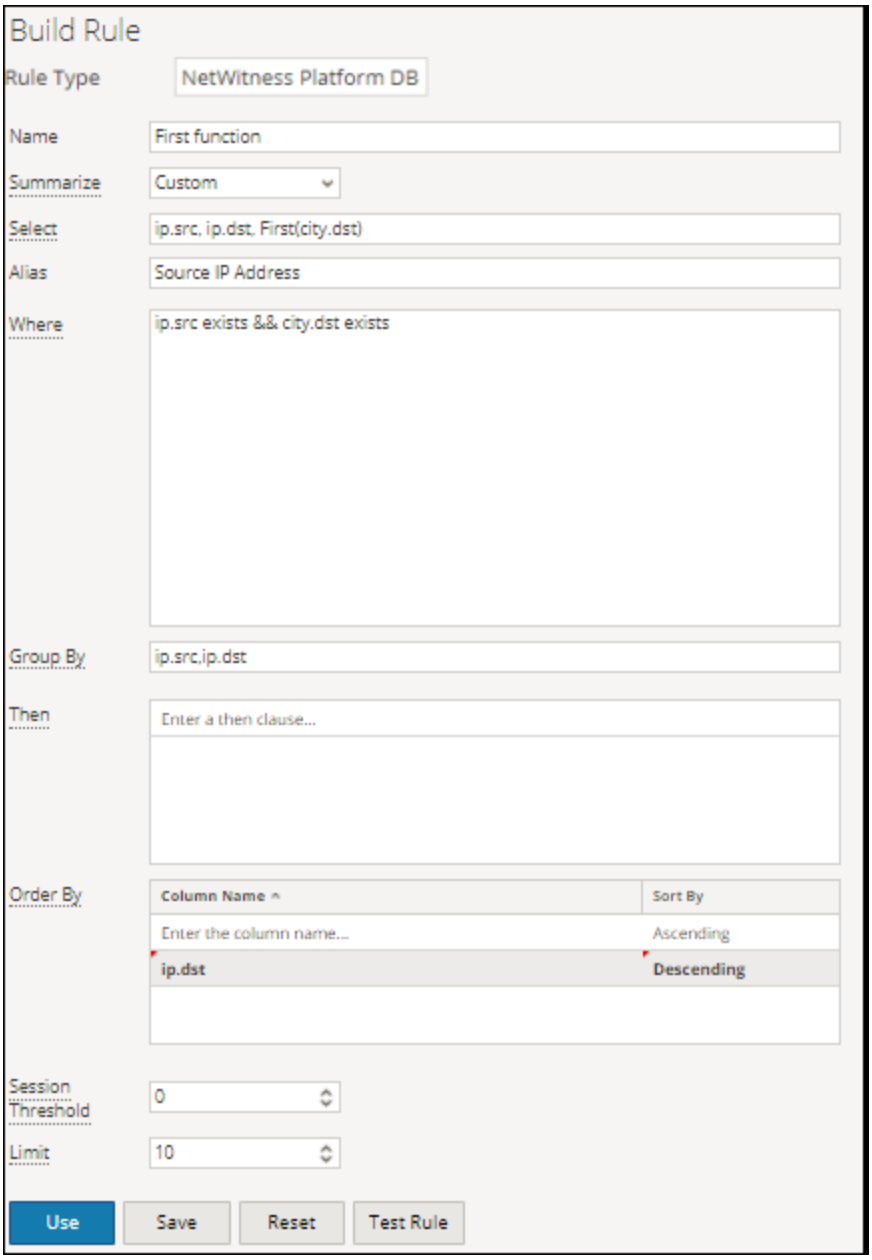
Here, the page displays the list of unique e-mails that were exchanged between the respective IP source and destination.

First

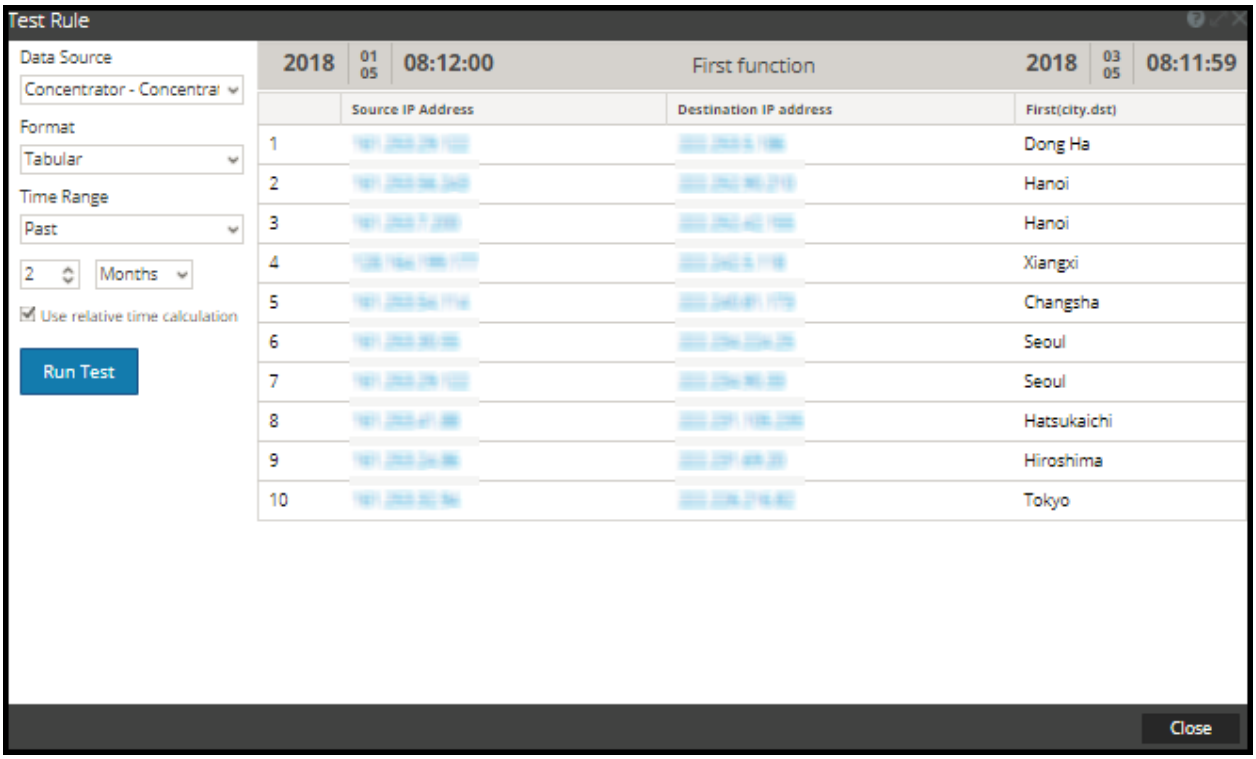
This function is used to retrieve the first value from an ordered sequence of values for a specified metakey.

Example

The following figure shows a sample query for first function used to retrieve the first destination city name.



The following figure shows the result for the above query.



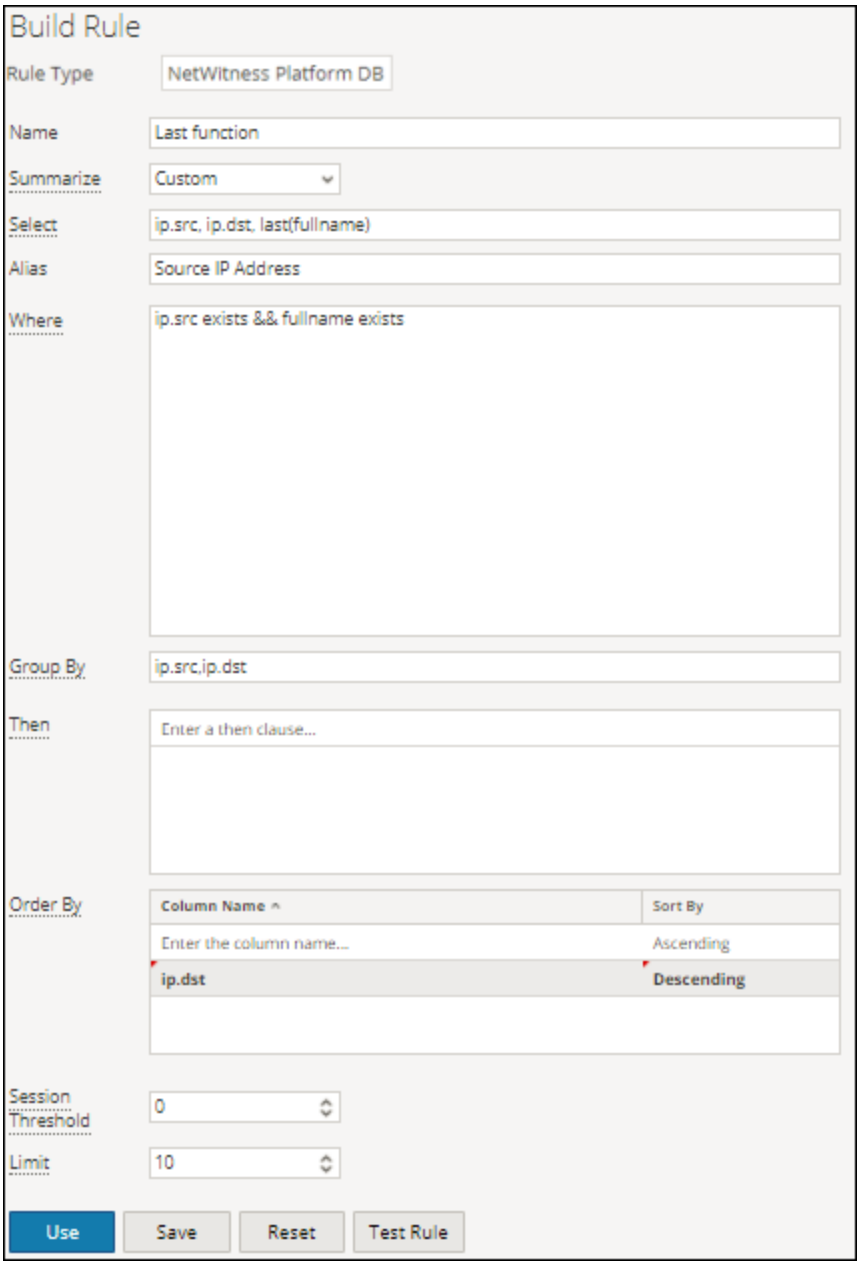
Here, the page displays the the first destination city for the corresponding source and destination IP. You can use the first function to isolate a particular value from a search result.

Last

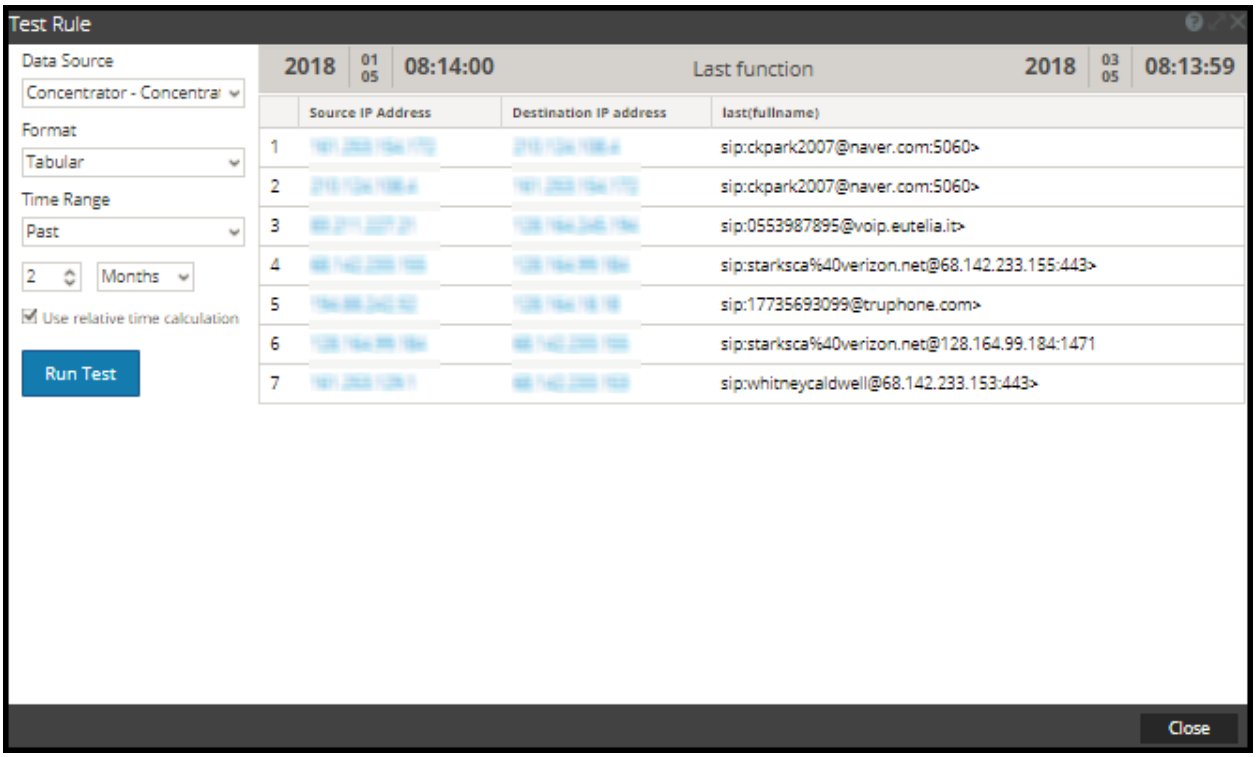
This function is used to retrieve the last value from an ordered sequence of values for a specified metakey.

Example

The following figure shows a sample query for last function used to retrieve the most recent user name.



The following figure shows the result for the above query.



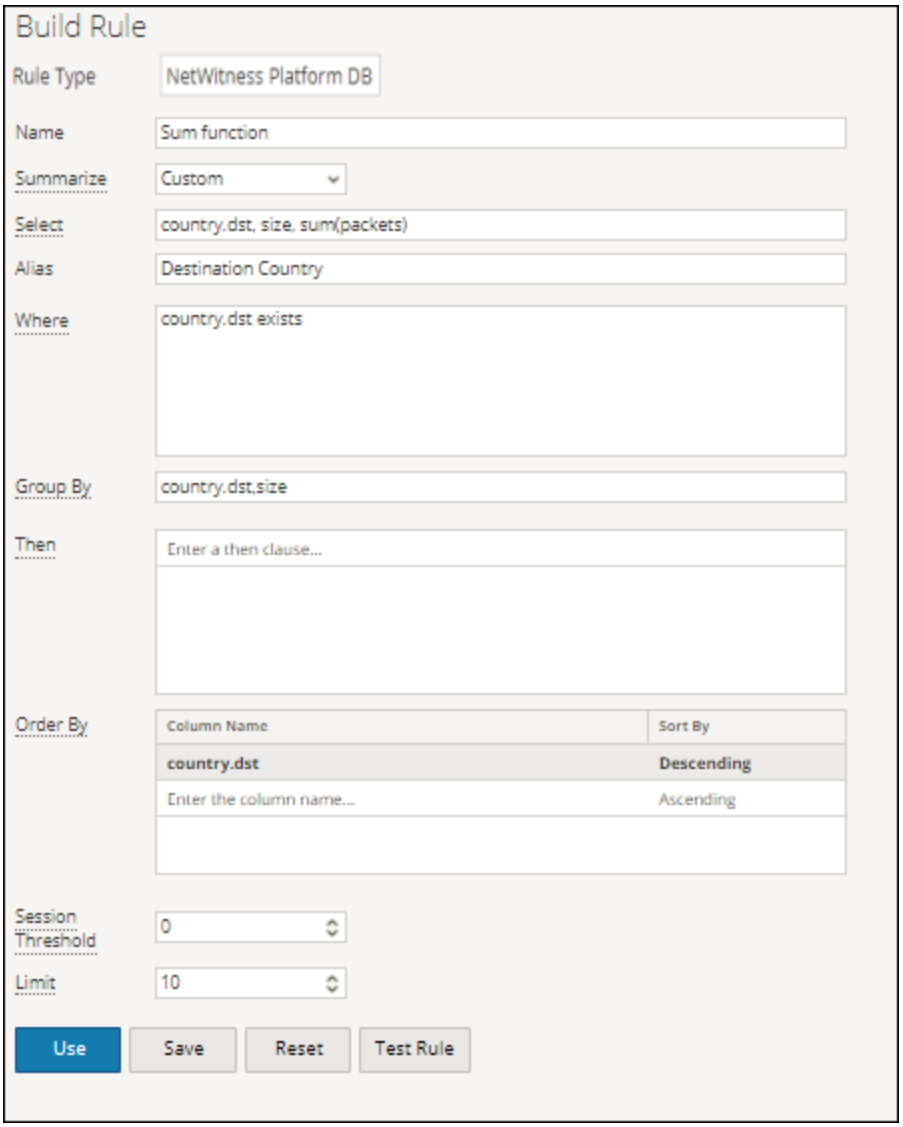
Here, the page displays the list of most recent or last usernames in full, that were exchanged between the source and destination IP.

Sum

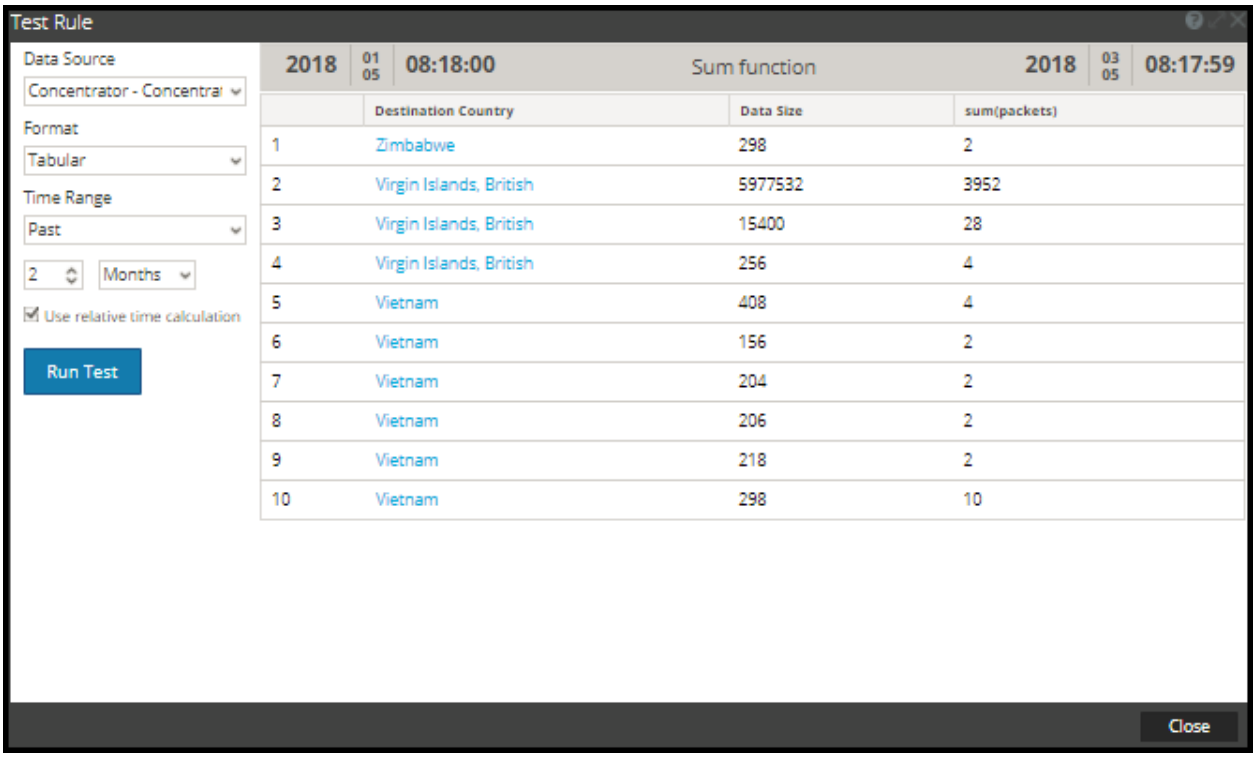
This function returns the total of the non-NULL values of the metaKey within a group.

Example

The following figure shows the query for the Sum function used for packets.



The following figure shows the result of the above query.



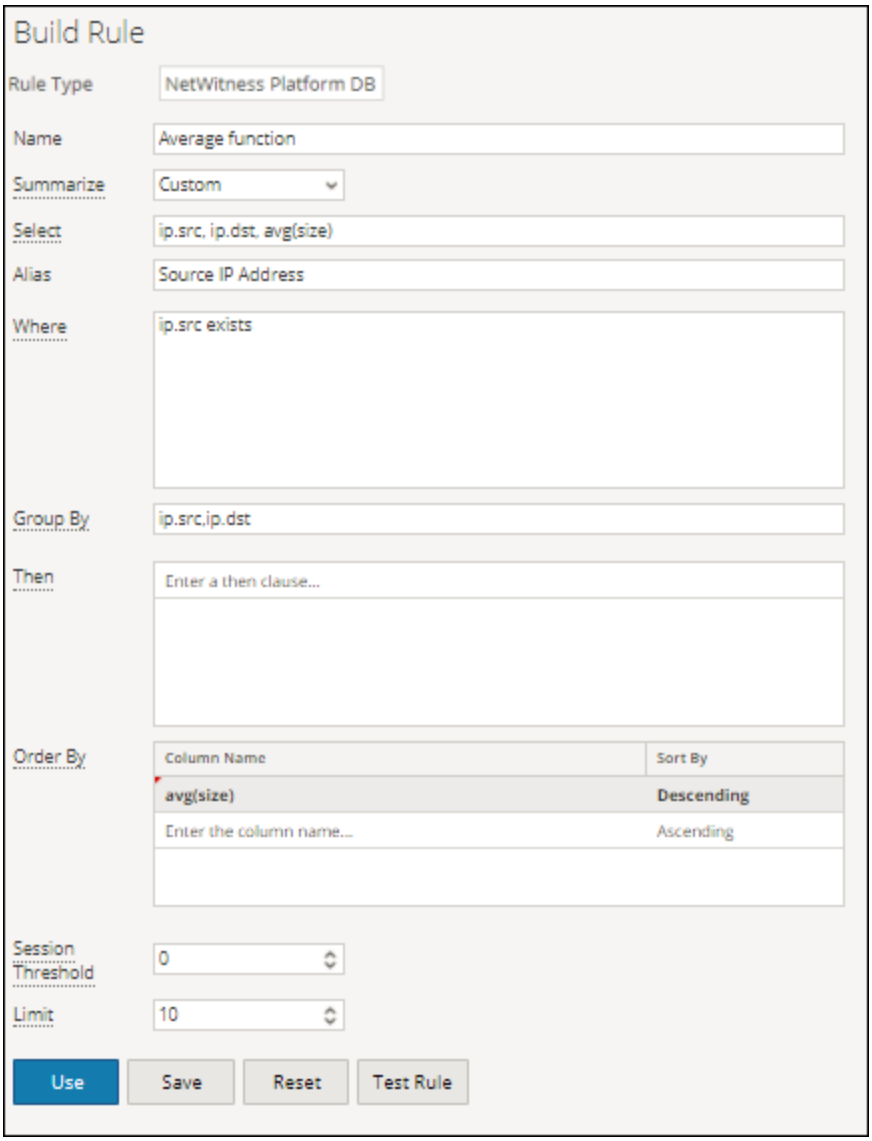
Here the page displays the total or sum of the packets along with the size of the data for the respective destination country.

Avg

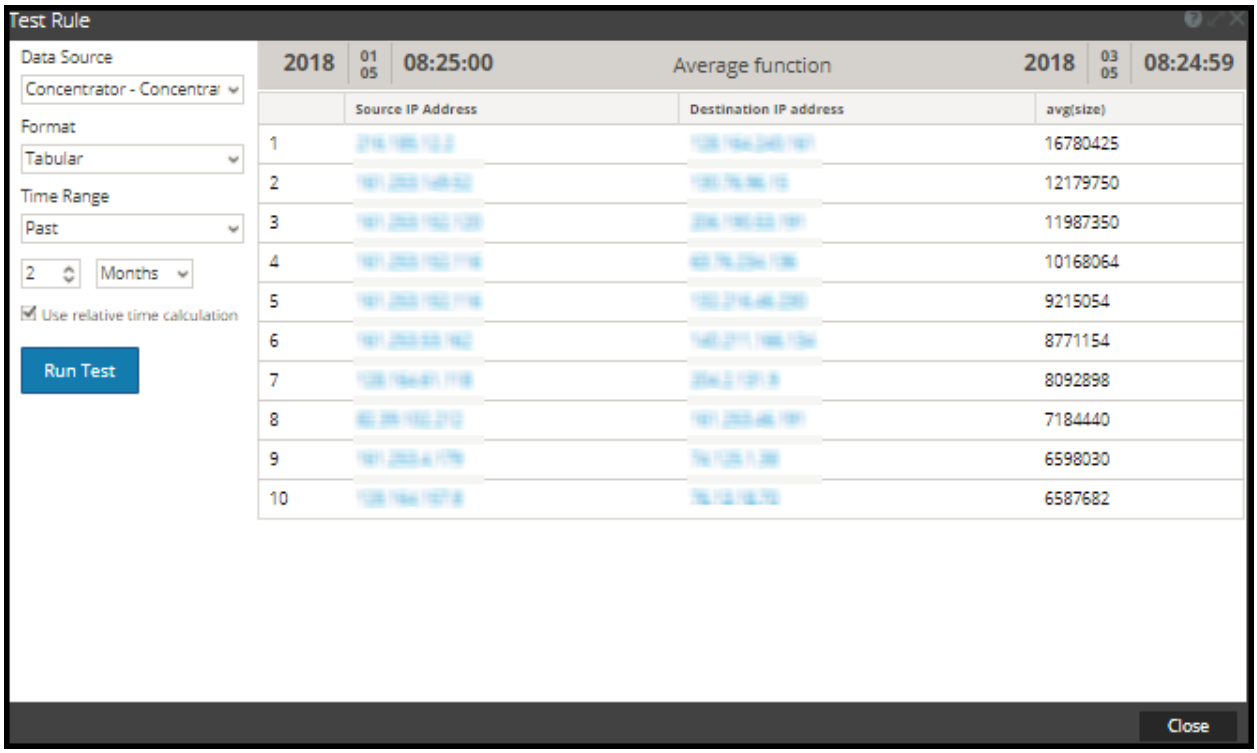
The average function returns the average of non-NULL values of the meta within a group.

Example

The following figure shows a sample query for average data size transmitted between a source and destination IP.



The following figure shows the result for the above query.



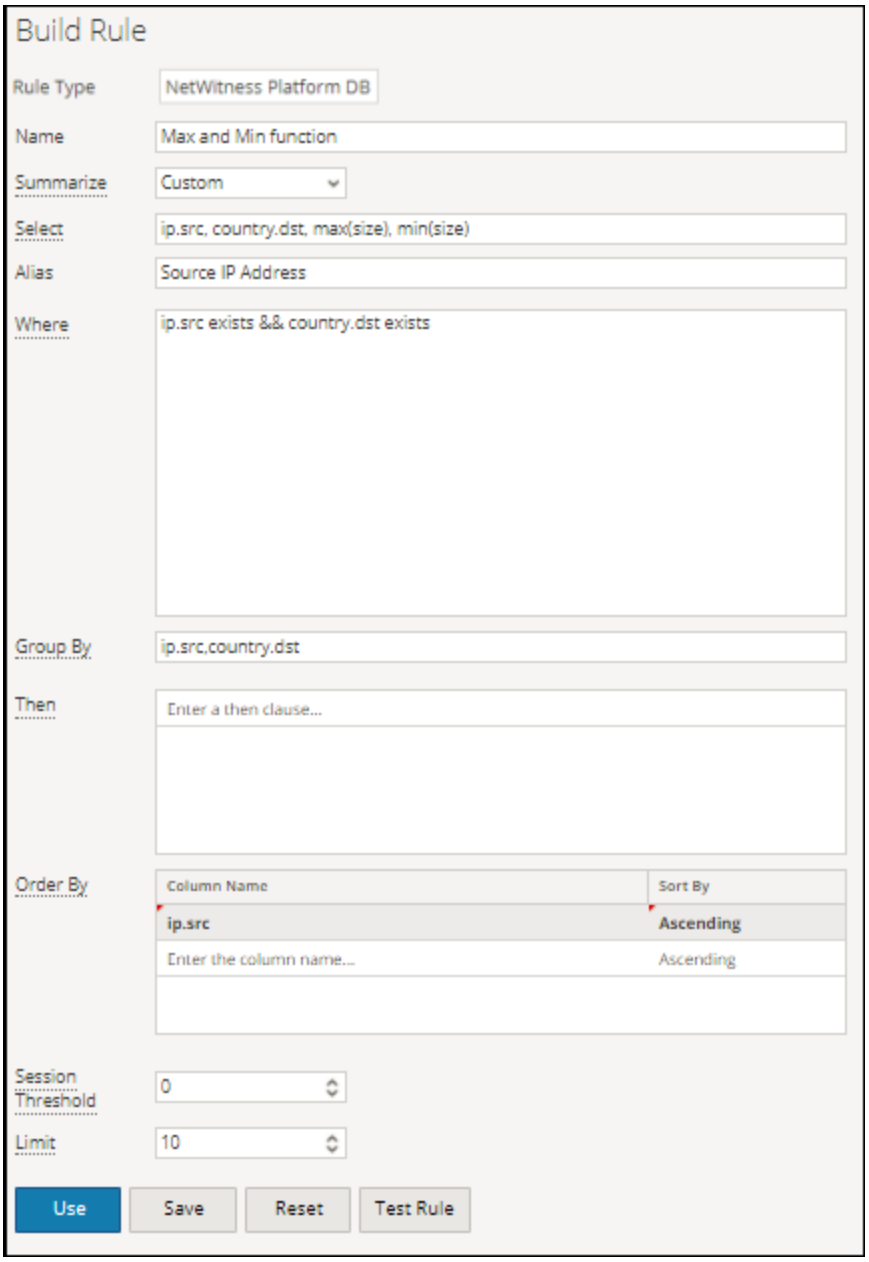
Here, the page displays the average size of data exchanged between source and destination IP:

Max and Min

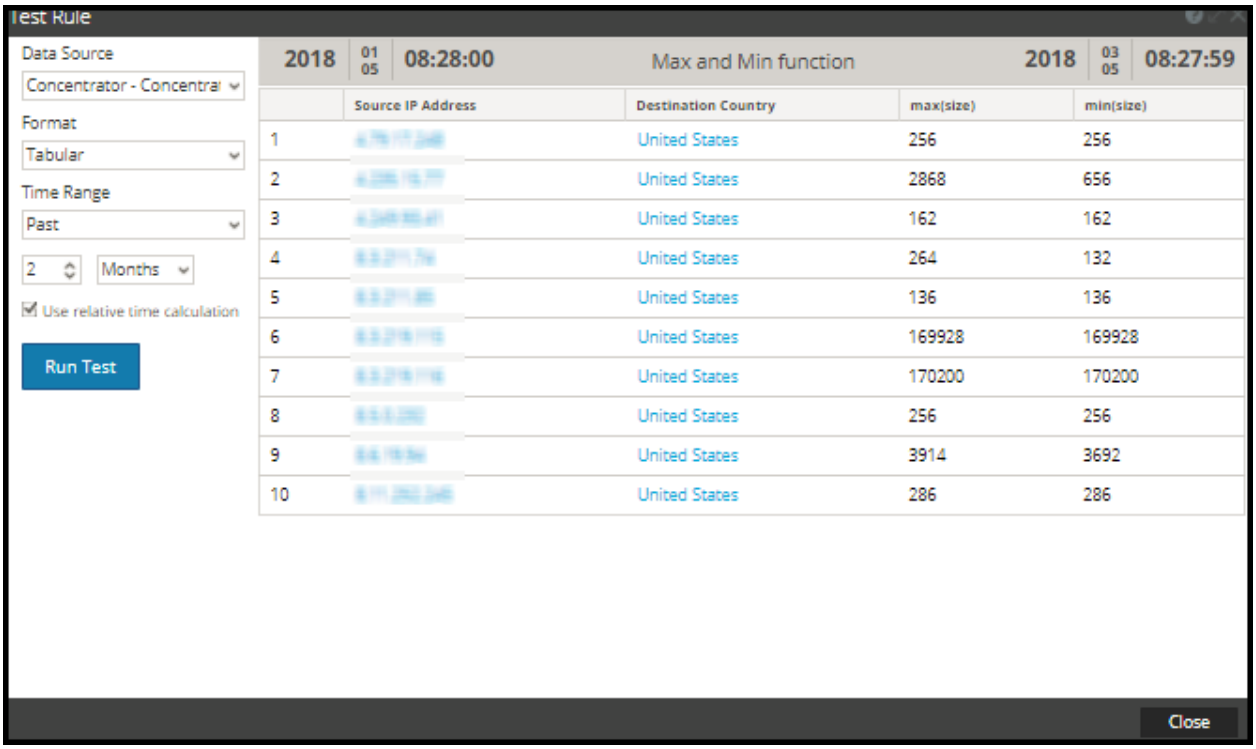
Max and Min functions provide the maximum and minimum for given values of a meta respectively.

The following figure shows a sample query for max and min functions for various data sizes, for source IP and destination country.

Example



The following figure shows the result for the above query.



Here, the page displays the max(size) and min(size) columns, along with the list of source IP and destination country. The max(size) column lists the maximum data sizes exchanged while the min(size) column lists the minimum data sizes that were exchanged.

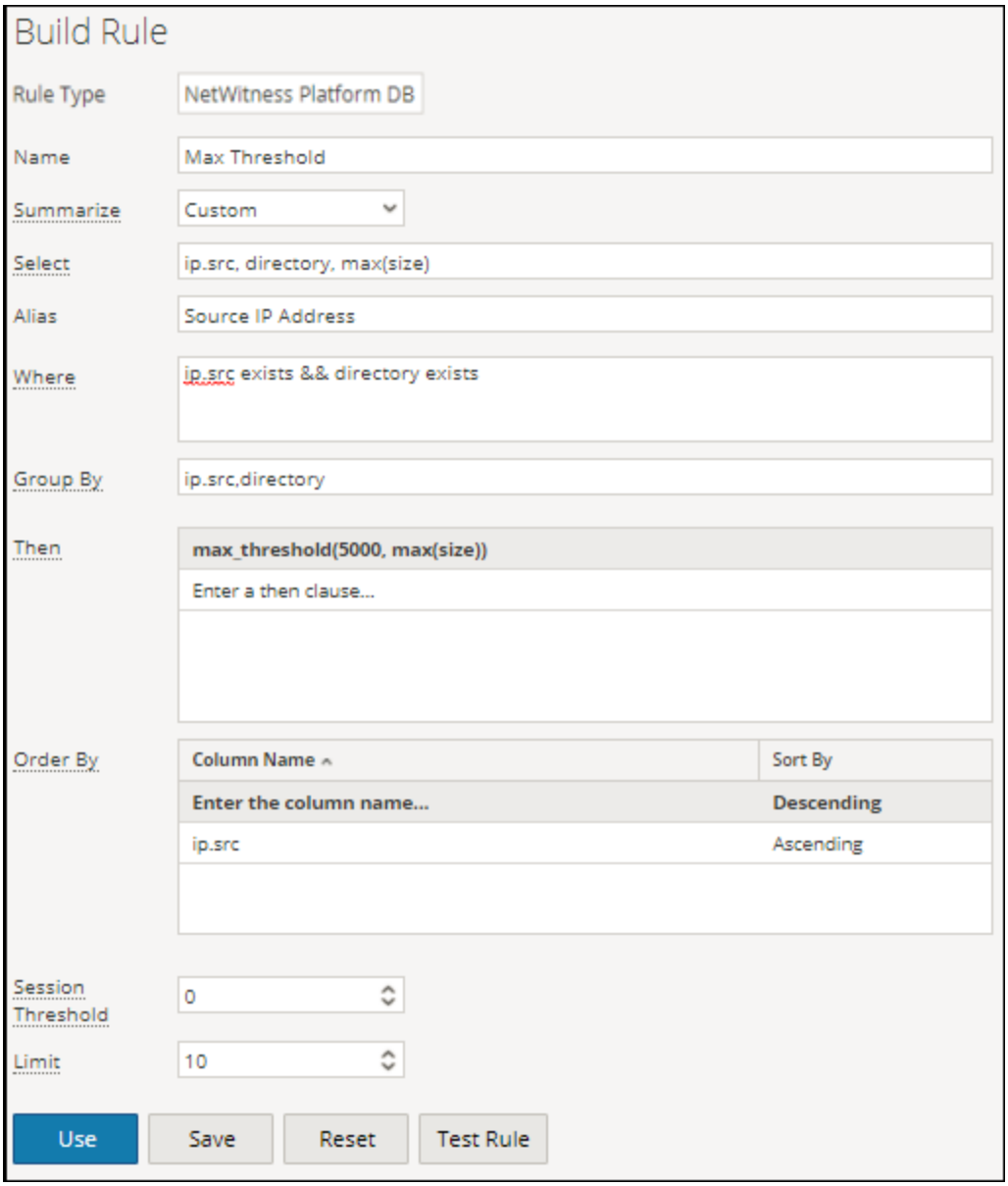
Filter aggregate meta results with Max_threshold

You can further filter the results of any function by using the threshold rule action.

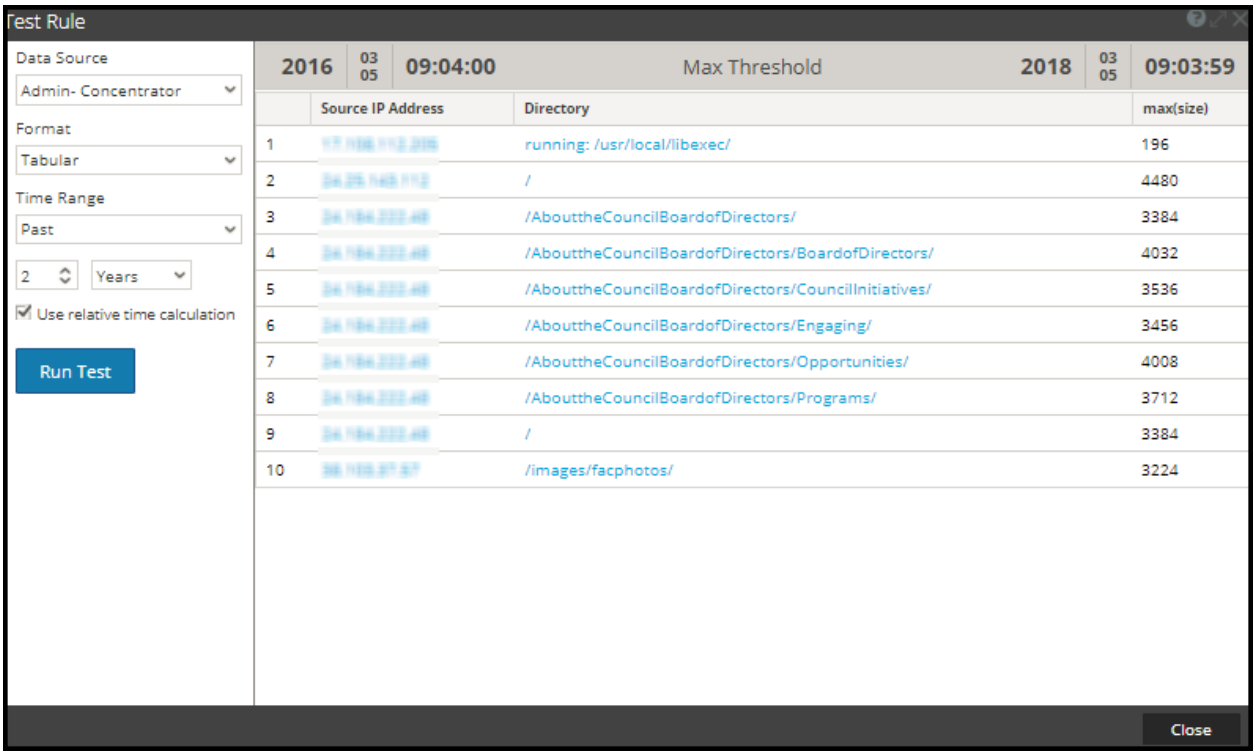
Example

Following is a sample query for max_threshold used along with the Max function in the **Then** field is:
max_threshold(5000,max(size))

The following figure shows the Build Rule screen for the above query.



Here the max_threshold is applied for data size with an upper limit of 5000. The following figure shows the result.



Here, the result page displays the max(size) column, that lists the data sizes lesser than 5000 as this is the maximum threshold in the query, along with the corresponding IP source and the respective directory.

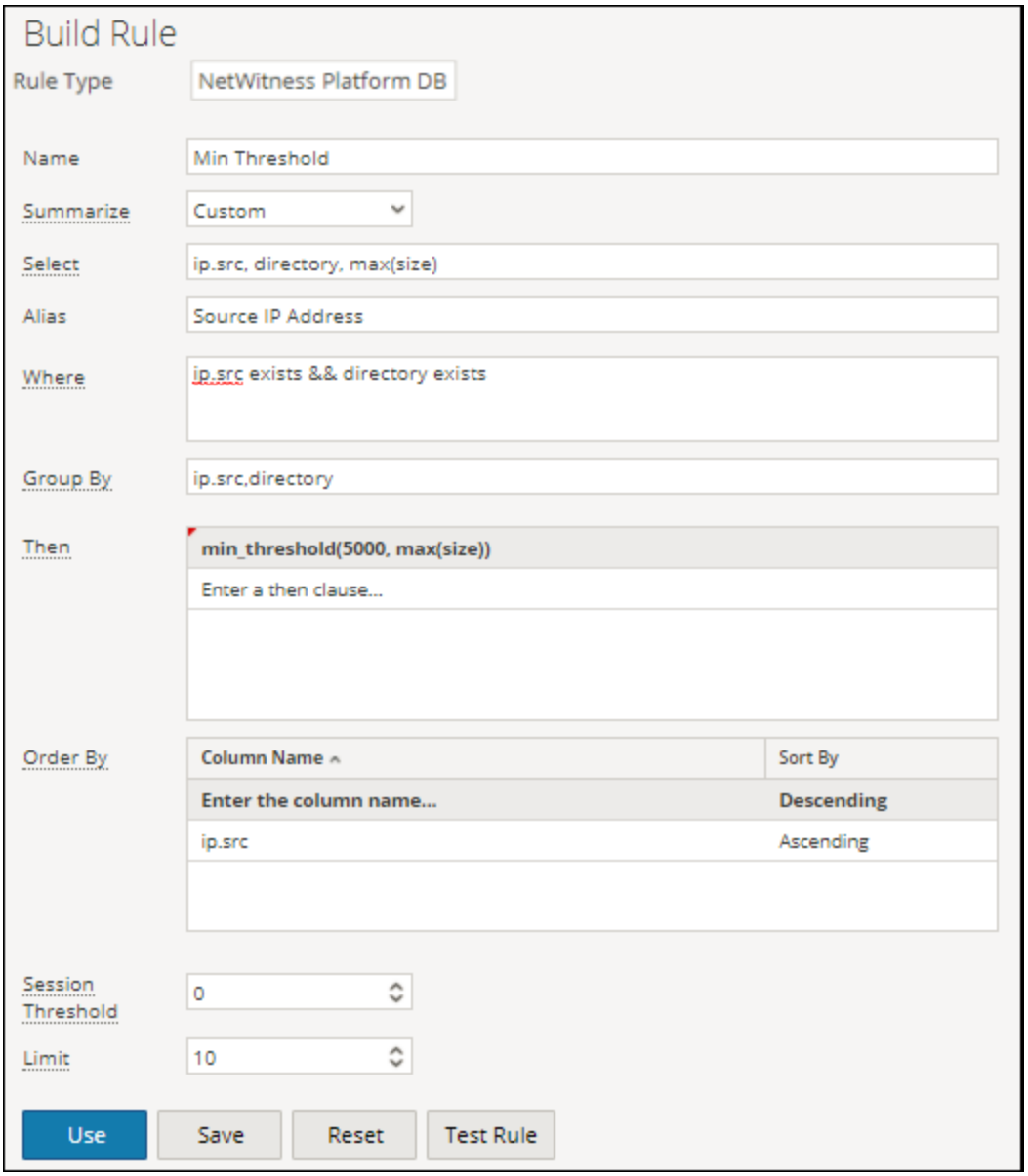
Filter aggregate meta results withMin_threshold

Similarly, min_threshold is used to filter the results for any function. A similar scenario as max_ threshold is considered to explain this.

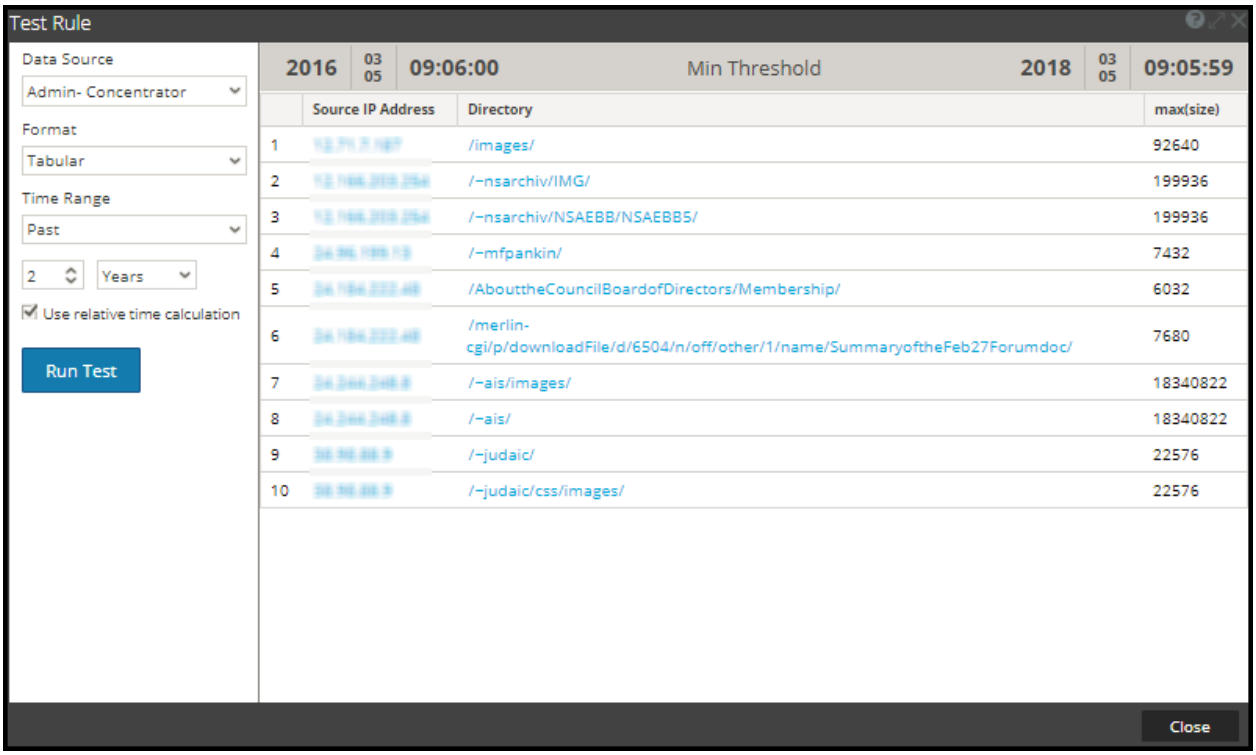
Example

Query for min_threshold used along with the Max function in the **Then** field is:
min_threshold(5000,max(size))

The following figure shows the Build Rule screen for the above query.



Here the min_threshold is applied for data size with a lower limit of 5000. The following figure shows the result.



Here, the result page displays the max(size) column, that lists the data sizes greater than 5000 as this is the minimum threshold in the query, along with the corresponding IP source and the respective directory.

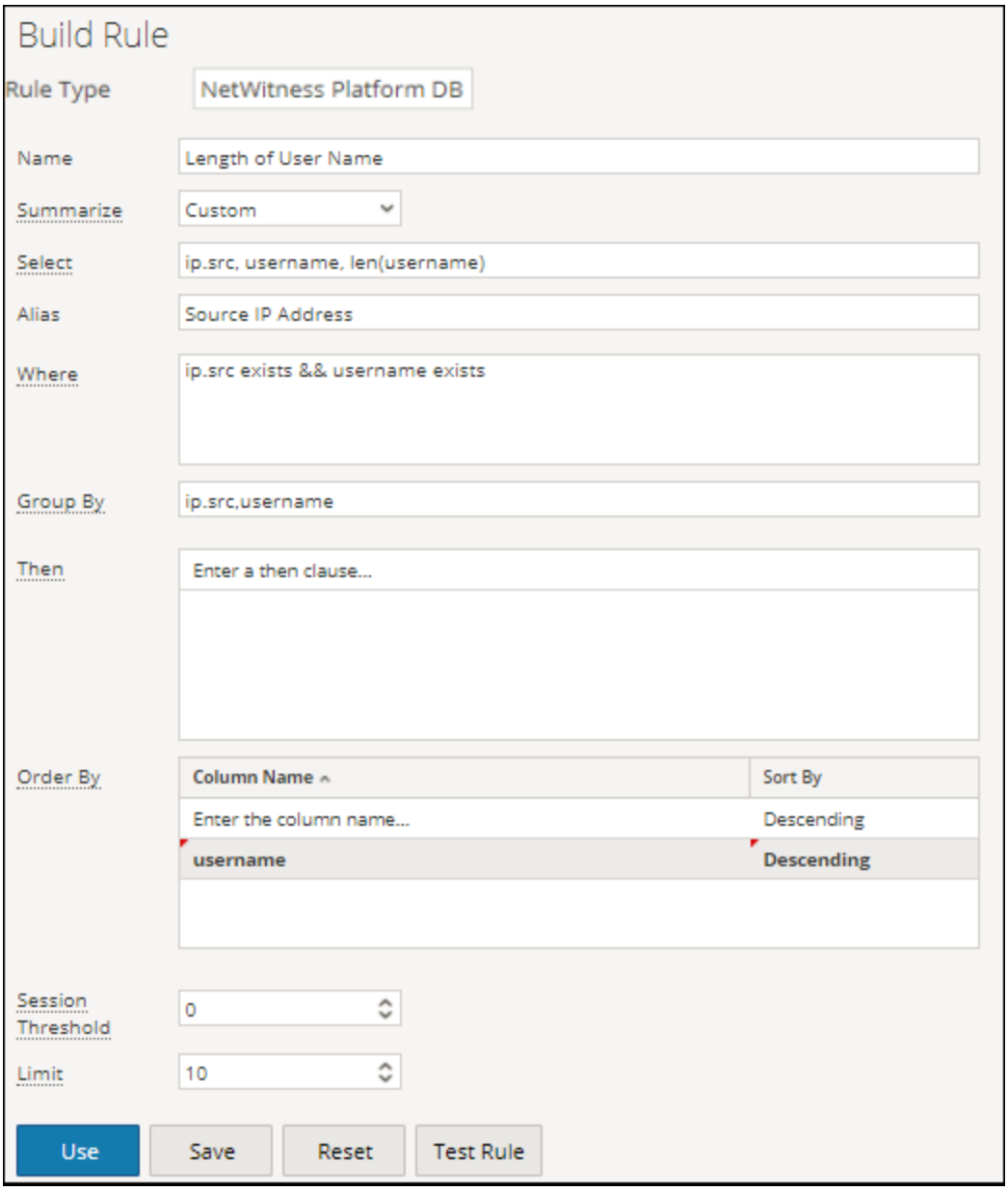
Note: Max_threshold and Min_threshold rule actions are common across all the functions, and can be used along with the other queries in the **Then** field to retrieve the respective output.

Length

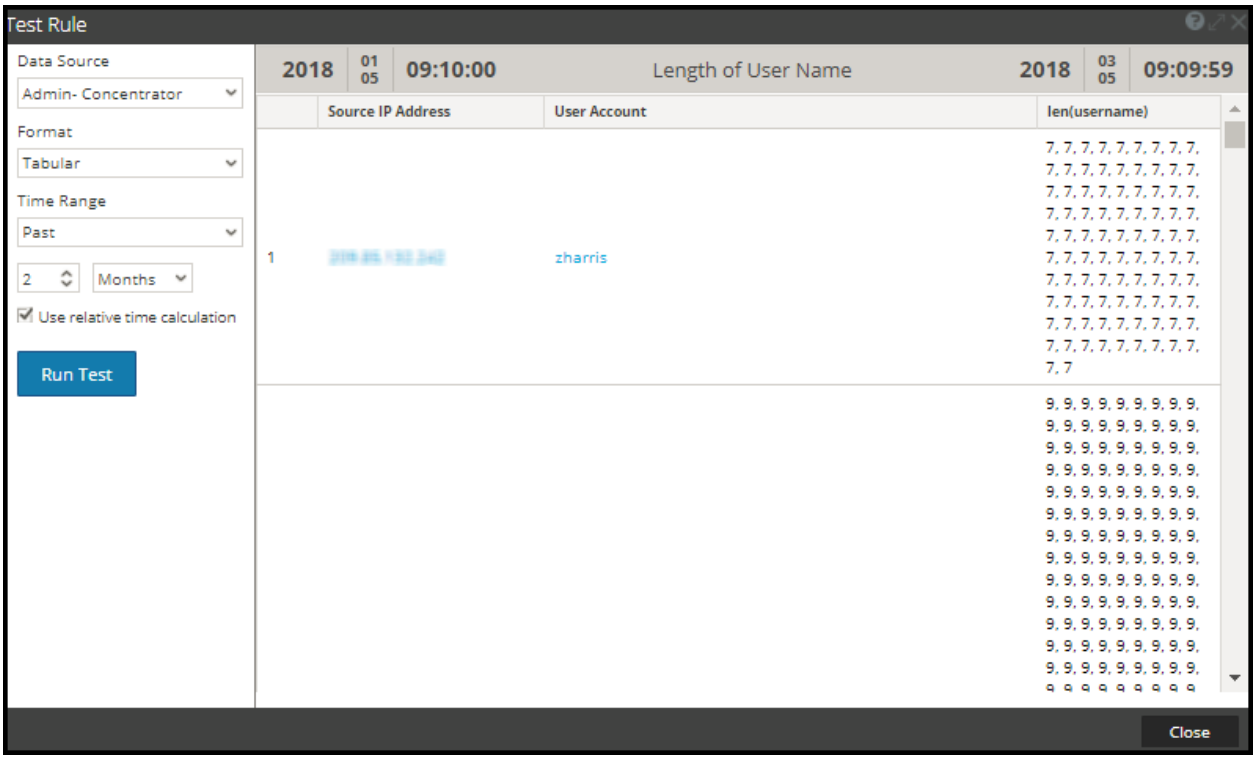
This function returns the length of a meta value. In other words, Length function returns the number of bytes used to store the actual value.
For instance, for the value "Analytics" it returns the length as 9. Similarly, for an IPv4 ip.src, it returns 4 (representing 4 bytes).

Example

The following figure shows a sample query for the length function used for usernames.



The following figure shows the result for the above query.



Here, the page displays the length of the usernames associated with the user account and their respective source IP.

Additional Information

When you query for aggregates (E.g. sum(size)) with **Group By** on a meta which has multiple values in a session, then the session with multiple values is accounted for aggregate calculation for each value of that meta.

Example

When you query for the Count aggregate function with Group By on Alias.host and if the column has multiple values in a session, then the session is counted for each occurrence, including the duplicate values.

Consider the following table.

SessionID	Alias.host	Ip.src	Size
1	host-a, host-b, host-a	a	10
2	host-b, host-c, host-a, host-c	c	20
3	host-b, host-c, host-d	b	30
4	host-c, host-a	a	40

In the above table, alias.host for **host-a** and **host-c** has duplicate values listed for a single session. Let us consider the following query:

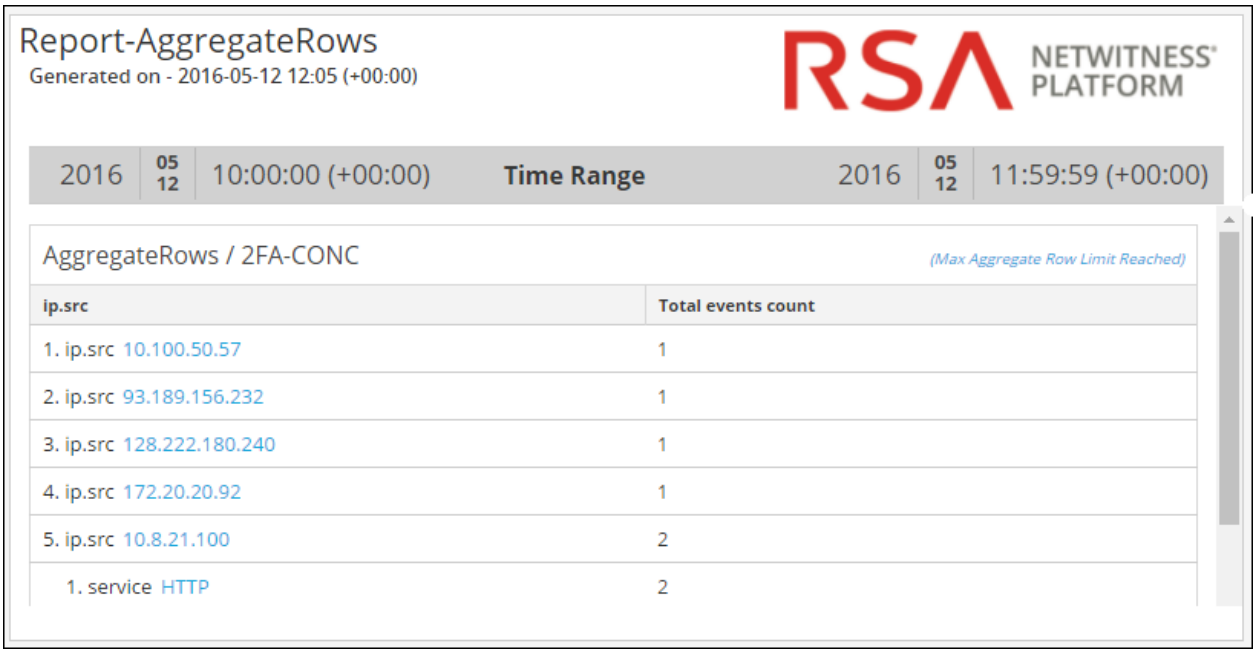
Select : alias.host, count(ip.src), sum(size)
Group By : alias.host

Here, **host-a** and **host-c** are present in 3 sessions and they are duplicated for two different sessions. However, the output is as shown below.

Alias.host	count(lp.src)	Sum (size)
host-a	4	80
host-b	3	60
host-c	4	110
host-d	1	30

Output table shows that the count for **host-a** and **host-c** is 4. This is because for each alias.host value, the entire session is considered. Similarly to calculate sum (size), the same sessions are considered for each alias.host value.

In the report output if the number of rows has reached **NWDB maximum aggregate rows** defined in RE configuration, then a message **Max Aggregate Row Limit Reached** is displayed to indicate that there is more information to be displayed. The default limit is 1000, and you can change this value as per your requirement, in the Reporting Engine Configuration page .



Troubleshoot Reporting

This section provides troubleshooting instructions for issues faced when using the Reporting module in NetWitness.

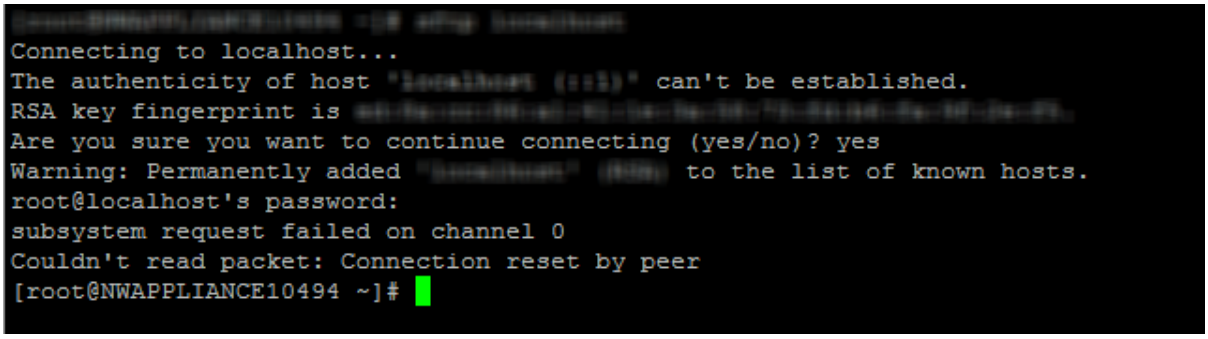
Configuring SFTP Server Issue

Procedure

Try the following steps if you face any issues while configuring the Linux SFTP server:

1. If the Report Output Action for the configured SFTP fails, you must SSH to the SFTP server and try to connect locally to check if SFTP is working fine.

   Connect to SFTP server:

2. If the Local connection fails, open the file **sshd_config> vi /etc/ssh/sshd_config.**
3. Check for the entry in the file:

   ```
   # override default of no subsystems
   Subsystem sftp /usr/libexec/openssh/sftp-server
   ```

4. If this entry does not exist, add the two lines mentioned in Step 3 at the bottom of the file and **Save** it.
5. Restart service from **SSH > service sshd restart**.
6. Retry the SFTP connection now.
7. Make sure SFTP port is not blocked by SA server appliance firewall. Update iptables rules to allow sftp port.

Meta Values in Investigation Link Issue

Issue	When the device information on the datasource is changed, the Investigation link for the meta values of the executed reports is not displayed on the NWDB results page.
Resolution	Remove and re-add the datasource to Reporting Engine. *Note: This workaround is not applicable for reports that are already generated.*

Internet Explorer 10 Browser Issue

Issue	When you click the Test Rule multiple times in quick succession, results with large input data may not displayed in Internet Explorer 10.
Resolution	If this issue occurs, try one of the following steps: • Close the Test Rule window on Internet Explorer 10 and run the test again. • Use other browsers like Chrome or Mozilla Firefox to test the rule execution.

Dynamic List Editing Issue

Issue	A dynamic list cannot be added from the Edit option on the 'View All Schedules' page to an existing schedule.
Resolution	1. Reports > Select the report > 2. Click the #Schedules for the specific report 3. Select the schedule to be modified from the Report Schedule page 4. Edit the schedule

Deployment Failure Issue

Issue	Deployment of reports fail, if the dependencies of certain compliance reports in Live are not deployed prior to the reports.
Resolution	Retry the deployment. If the problem persists, try to deploy the rule or list dependencies first and then deploy the reports.

Respond Server Issue

Issue	When the Forward Alerts to Respond option is enabled and RabbitMQ connections to the Respond Server are blocked, some of the Reporting Engine threads may be blocked.
Resolution	Disable the Forward Alerts to Respond option until the RabbitMQ broker in the NetWitness server at the Respond has begun and accepts the connections.

Post-Upgrade Issue

Issue	Post-upgrade from 10.6.x to 11.2, Categories meta for incident collection is not supported.
Resolution	When using the Categories meta for incident collection, the results rendered are in an incorrect format. Hence this meta is not supported and you cannot use the categories meta in either select clause or where clause. Also, it is not available in the list of metas for selection in the Rule Builder page.

Report Query Timeout Issue

Issue	When scheduling the report, if you choose a high time range, the query may timeout with the error message **`Query on channel 12345 was canceled by the system for exceeding time usage limits. Check timeout values.`**
Resolution	Set the **Summarize** option to **None** in the **Build Rule** view to exclude the **Group-By** clause (that is performance intensive) and then re-schedule the report. If the query still times out after 60 minutes, increase the timeout value from 60 minutes to 90 minutes on all the core services. To increase the timeout value: 1. Go to **Admin** > **Services** > **Security** > **Users** and set the **Core Query Timeout** to 90 minutes. 2. Enter the Service Admin Password and click **Save**. 3. Re-schedule the report.

Reporting References

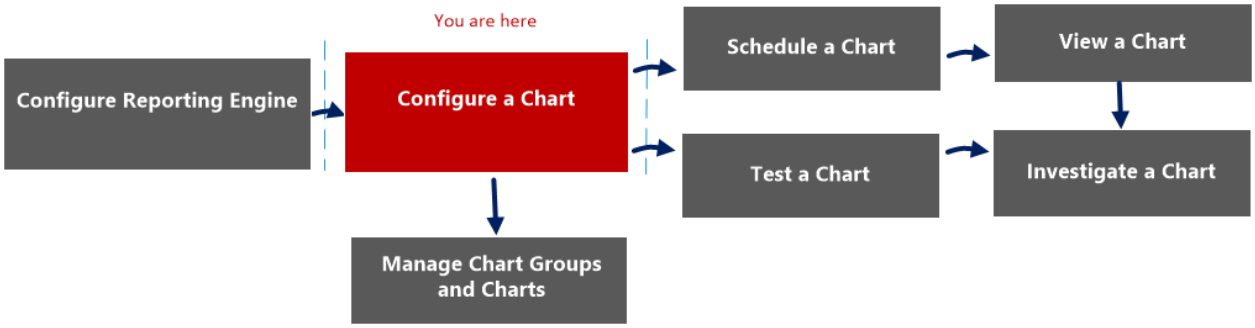
This section provides information about the Reporting user interface. You can look at your place in the workflow for creating and generating a report with theNetWitness, get a quick look at the important features, and follow links to the detailed concepts and procedures.

Build Chart View

In the Build Chart view, you can define and test a chart. You build a chart by assigning a name and then selecting a rule to include.

Note: Only the NetWitness DB rules can be used in charts.

Workflow



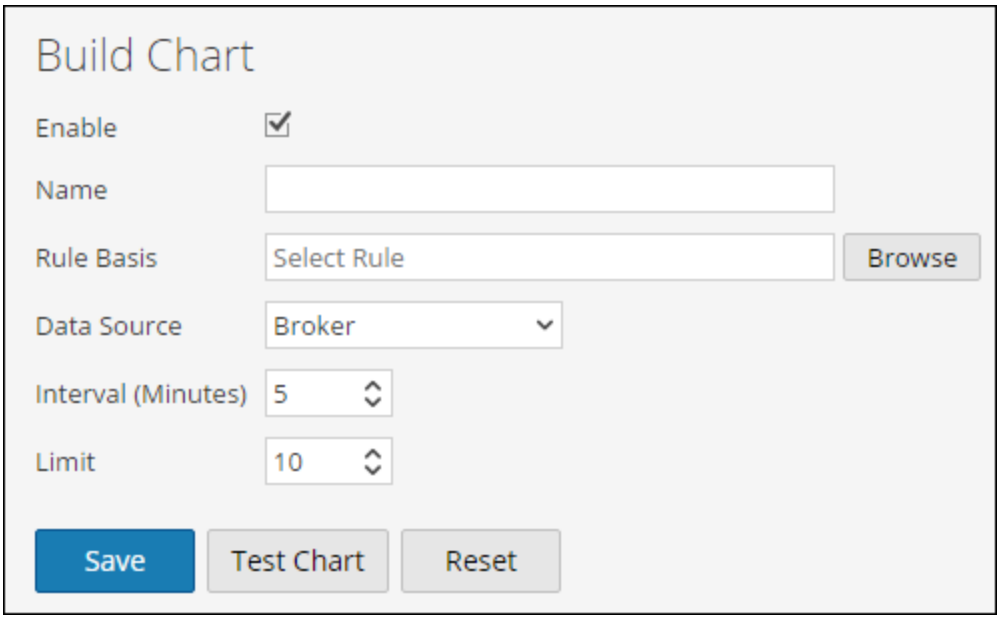
What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart*	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

*You can complete these tasks here.

Quick View

The following figure is an example of the Build Chart view.



The following table describes the features in the Build Chart view.

Field	Description
Enable	Specifies if the Reporting Engine must collect the data and generate chart results. If the **Enable** checkbox is not selected, the results are not rendered.
Chart Name	Identifies the name of the chart.
Rule Basis	Displays the Add Rules dialog box from which you select a rule that is the basis of a chart. The rule that you select must be a rule which is not sorted by none.
Data Source	If the default data source is configured in the Reporting Engine, the data source is displayed on the Build Chart page. If a chart is configured to run on any other data source, that data source is displayed on the Build Chart page instead of the default data source. The Reporting module works with the following data sources: • Broker • Concentrator • Decoder • Log Decoder • Log Collector
Interval (Minutes)	The chart data refresh interval in minutes.
Limit	The number of records for which a chart is generated.
Save	Saves a chart to the database.
Test Chart	Plots a test chart based on the chart definition.

Field	Description
Reset	Resets the chart details.

Build List View

In the Build List view, you can enter or import values to create a list and save or reset the values. You can use lists when you are writing reporting rules to simplify the process of specifying values in the rule.

Workflow

This workflow shows the procedure to define lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists.

You must ensure that Reporting Engine is configured on the NetWitness.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

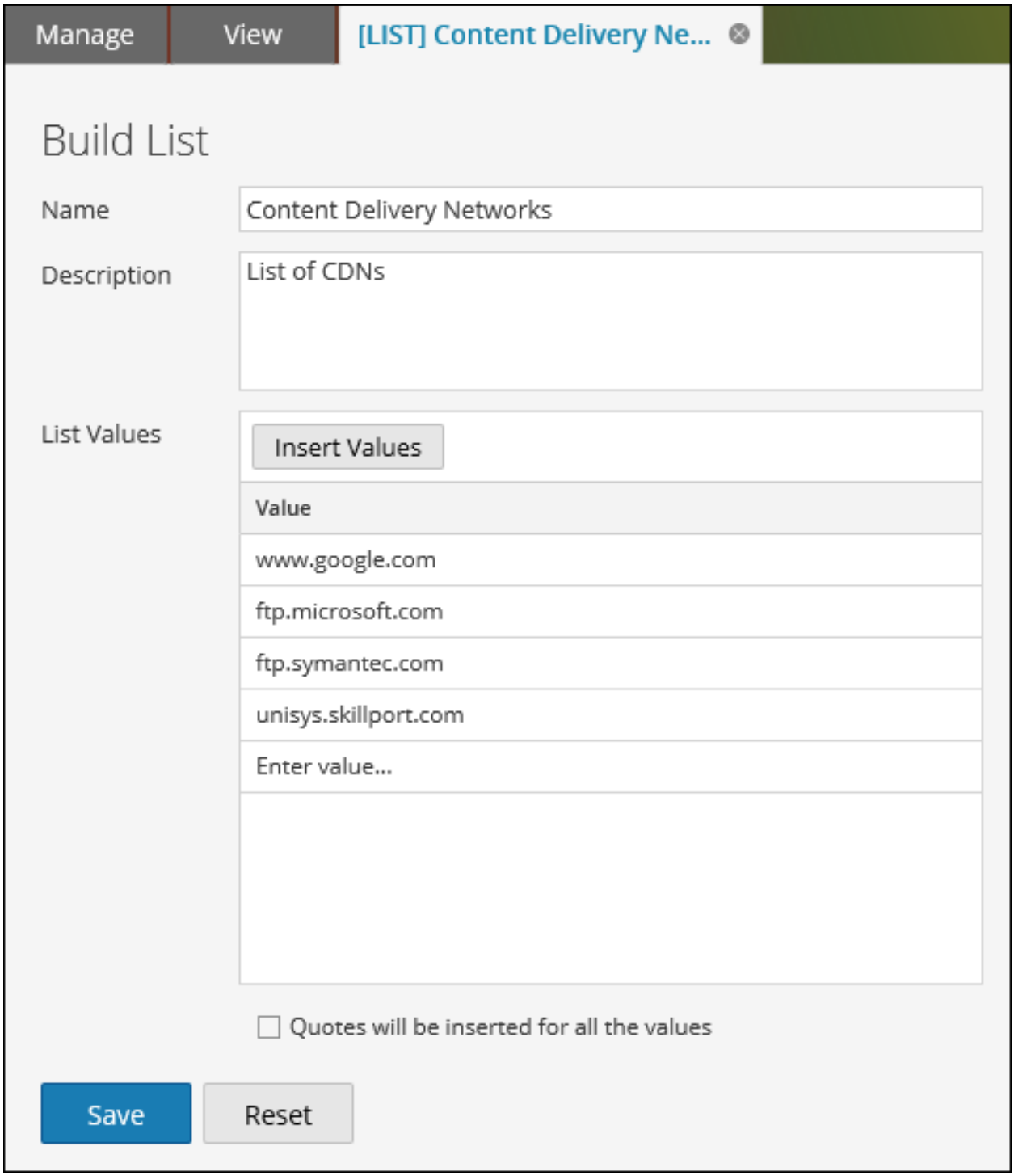
*You can complete these tasks here.

Related Topics

- List View
- Lists Permissions Dialog

Quick View

The following figure shows the Build List View.



To access this view

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The Lists view is displayed.

3. In the **Lists** toolbar, click  .

   The Build List tab is displayed.

The following table describes the features in the Build List view.

Feature	Description
Name	Identifies and labels the list.
Description	Provides a short description for the list.
List Values	Provides the grid of values associated with selected list from the List Library panel. You can import these values from a file or list. You can also enter values manually.
Quotes will be inserted for all the values	Automatically includes quotes for the values at runtime if checkbox is selected. If the checkbox is not selected and if a value in the list contains a comma, then that value has to be enclosed within single quotes. This syntax does not apply to list values for an NWDB rule.
Save	Saves the rule which can be used to create a report, a chart or an alert.
Reset	Deletes all the information from the fields.

Build Report View

In the Build Report view, you can create a report, add text and rules, and schedule a report.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

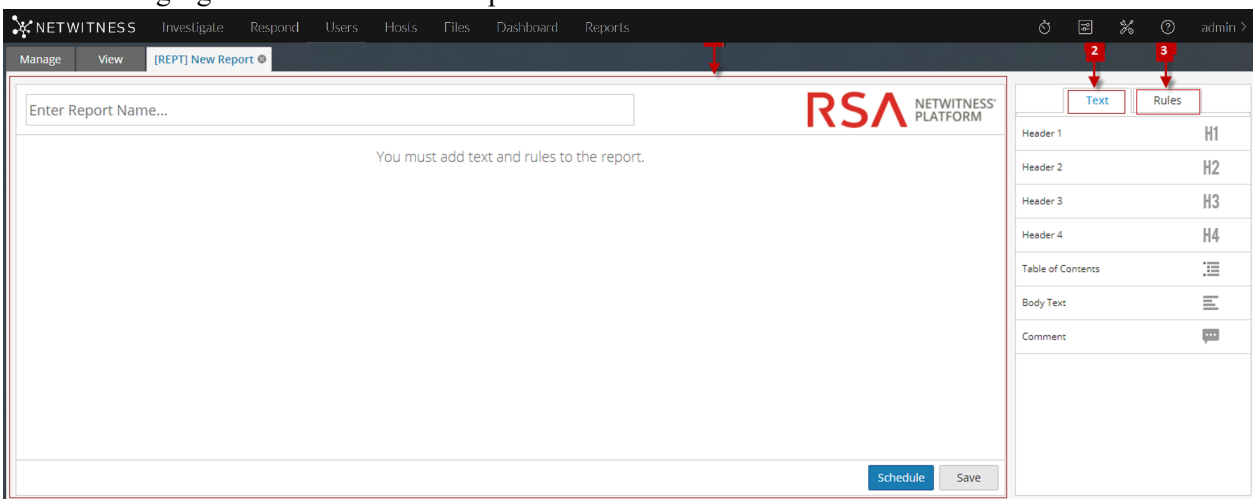
Related Topics

- Configure and Generate a Report
- Report View

- Scheduled Reports View
- Reports Permissions Dialog

Quick View

The following figure shows the Build Report View.



To access this view

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Reports view is displayed.

3. In the **Reports** toolbar, click + .

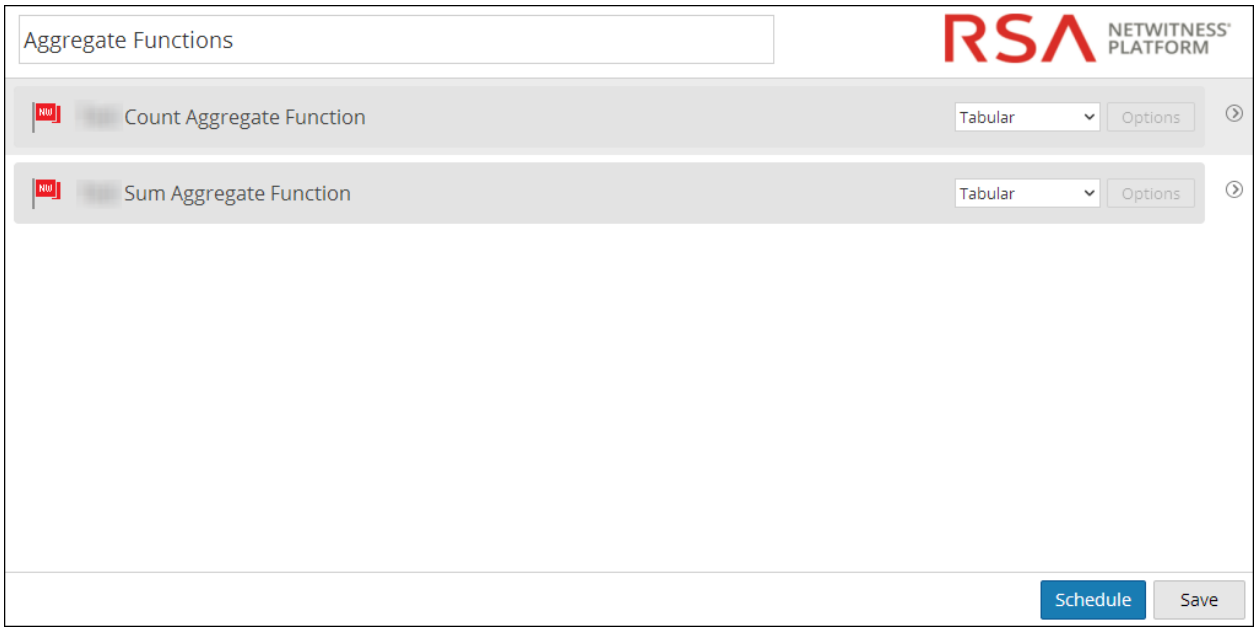
   The Build Report tab is displayed.

The Build Report view consists of the following panels:

1	Report Panel
2	Text Panel
3	Rules Panel

Report Panel

The Report panel allows you to create a report by assigning a name to the report. The content in a report depends on the items selected from the Text and Rules panels.



When you add rules to a report, you can change the output format of these rules either to tabular, area, line or pie by clicking the ⌄ button.

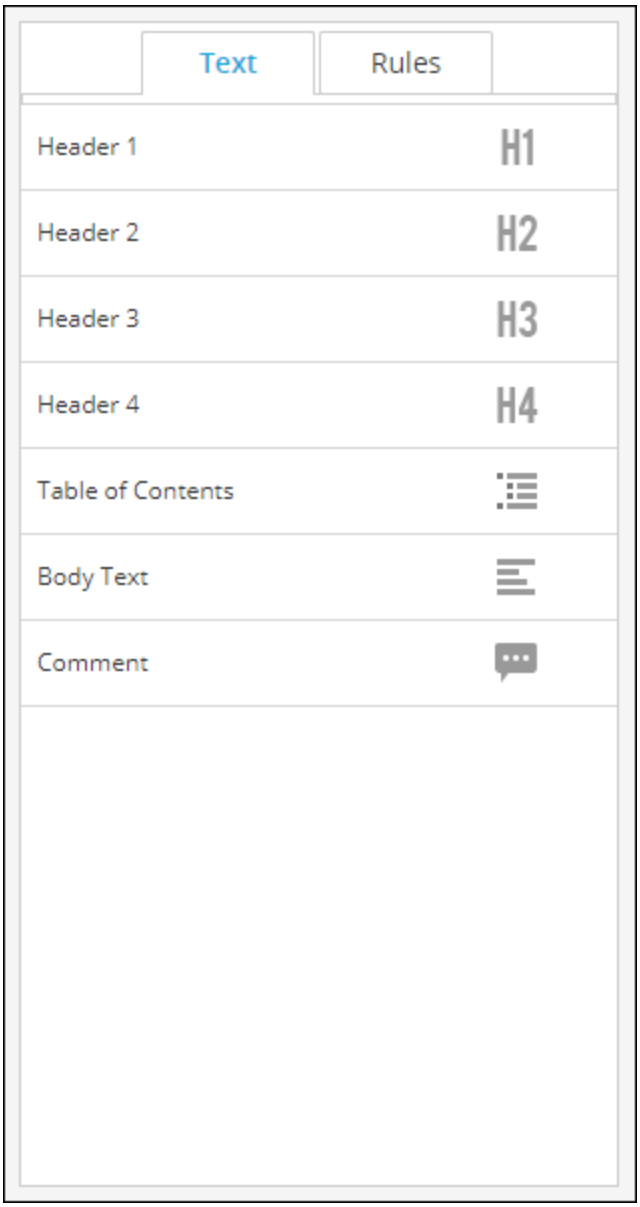
The following table lists the features of the Report Panel and the description.

Feature	Description
Name	This field allows you enter the name of the report.
Options	This field allows you to select the output format of the report such as Tabular, Area, Bar, Bubble, Column, Line, Pie, Step Line, Step Area, Spline Area and Spline.
Schedule	Clicking this option generates the report.
Save	Clicking this option saves the report.

Text Panel

The Text panel consists of a list of text elements that add to the look and feel of the report. You can use these text elements to format the report.

- To add more structure to reports, you can use these headers defined in the Text panel to indent up to four levels. This allows you to identify specific sections in a report that can be included in the Table of Contents for easy navigation in the report result.
- To add headers to the Report panel, drag and drop H1, H2, H3, or H4 onto the Report pane based on the desired level of indentation.



The following table lists the text elements used to format a report:

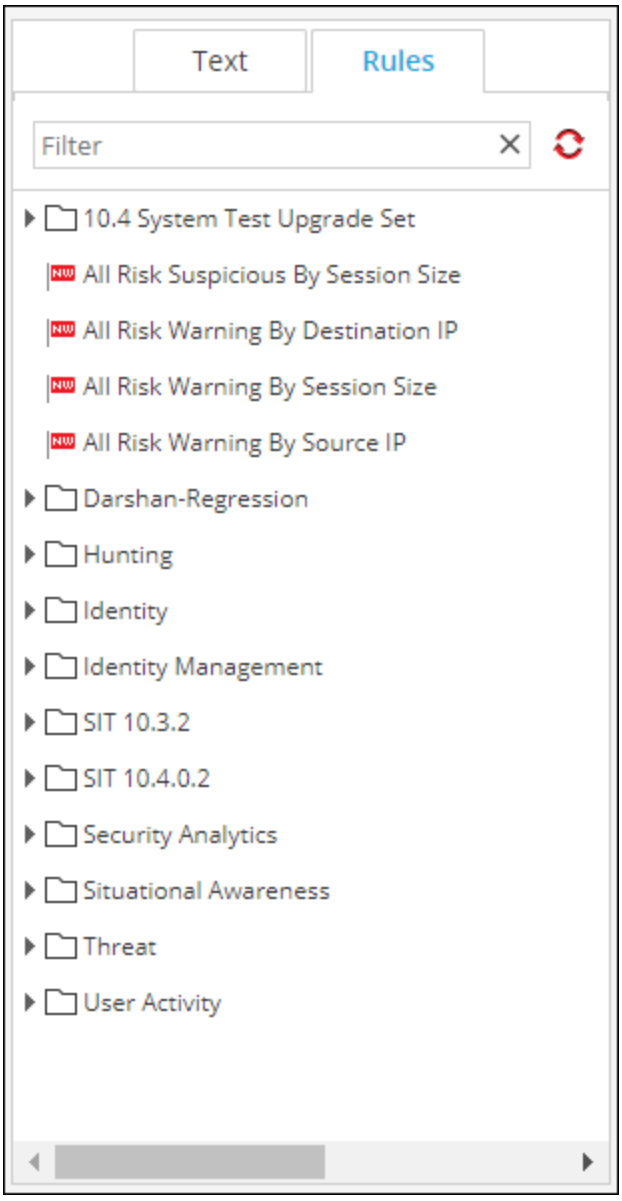
Text Elements	Description
Header 1 H1	The Header 1 element adds a first-level heading to the report definition.
Header 2 H2	The Header 2 element adds a second-level heading to the report definition.
Header 3 H3	The Header 3 element adds a third-level heading to the report definition.

Text Elements	Description
Header 4 	The Header 4 element adds a fourth-level heading to the report definition.
Table of Contents 	The Table of Contents adds table of contents to the report definition.
Body Text 	The Body Text element adds body text to the report definition.
Comment 	The Comment element adds comments to the report definition. **Note:** The Comment element is not displayed when you view all the reports.

Rules Panel

The Rules panel consists of a list of rules that are defined in the Rules. From the rules list, you can drag and drop rules onto the Report panel to associate those rules with the report.

You can search for a specific rule using search text box provided in the Rules panel.


Text
Rules
Filter
10.4 System Test Upgrade Set
All Risk Suspicious By Session Size
All Risk Warning By Destination IP
All Risk Warning By Session Size
All Risk Warning By Source IP
Darshan-Regression
Hunting
Identity
Identity Management
SIT 10.3.2
SIT 10.4.0.2
Security Analytics
Situational Awareness
Threat
User Activity

Build Rule View

The Build Rule view explains the actions and associated procedures that you can perform under Rules.

Workflow

This workflow shows the procedure to create or deploy a rule.

What do you want to do?

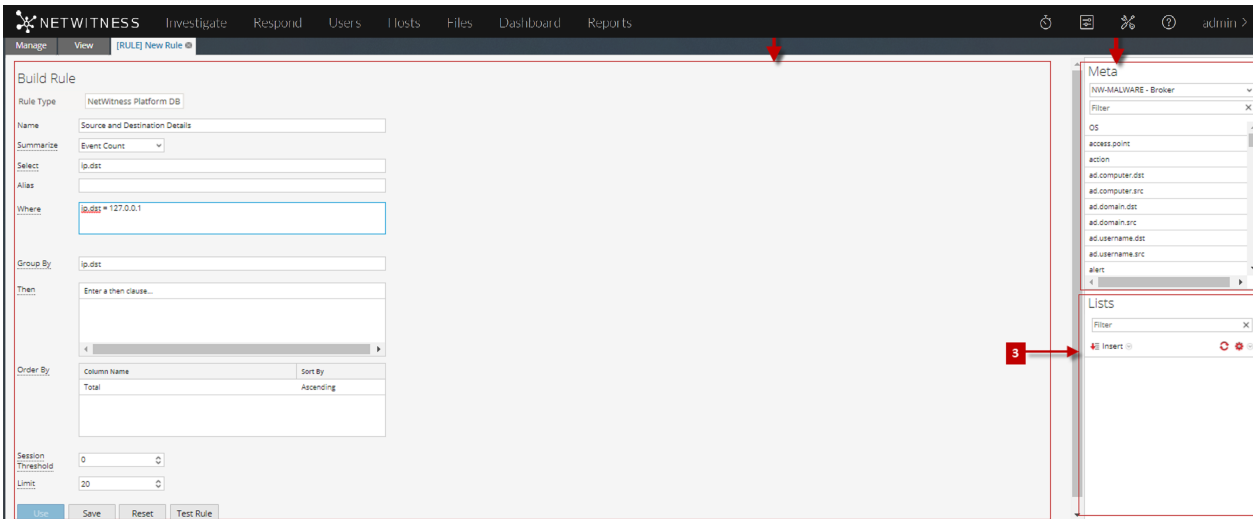
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Rule Permissions Dialog
- Rule View

Quick View



To access the Build Rule view:

1. Go to **Reports**.
   The Manage tab is displayed.

2. In the **Rules** toolbar, click + > **NetWitness Platform DB**.
   The Build Rule view tab is displayed

Features

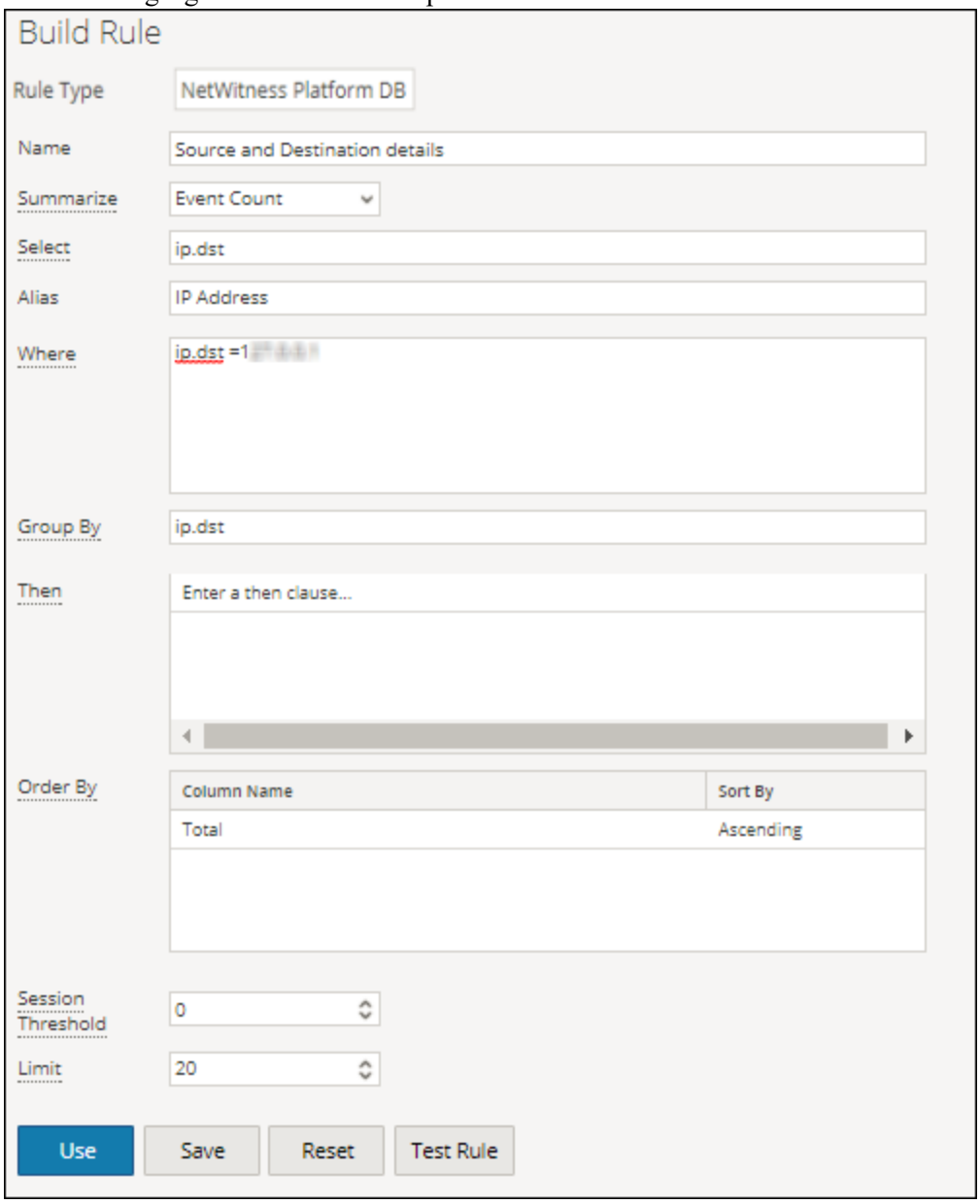
The Build Rule view includes the following panels.

1	Rule panel
2	Meta panel
3	Lists panel

Rule Panel

The Rule panel allows you to create a rule for the selected database type.

The following figure shows the Rule panel.



The following table describes the features in the Rule panel.

Feature	Description
Rule Type	A drop-down list of supported database types for which you can create rules. The options are: NetWitness DB and Warehouse DB.
Name	The name of the rule that you are creating or editing.
Summarize	A drop-down list of summarize options. The options are: None, Event Count, Packet Count, Session Count and Custom.
Select	The meta key for which you need the aggregate values; for example, ip.dest.

Feature	Description
Where	A Where clause that defines the conditions that trigger the rule execution; for example, ip.dest = 127.0.0.1.
Group By	The grouping method for the results. For example, specifying ip.dest produces a report in which like ip.dest values are grouped.
Then	A Then clause that defines the rule actions for additional processing on the output.
Order By	The sequencing method used to show results. For example, specifying Order By the value in the Total column, Ascending, produces a report in which the results are sorted in ascending order based on the value in the Total column.
Session Threshold	A selection list for the session threshold, which specifies maximum number of sessions that should be processed for aggregate functions.
Limit	A selection list for the maximum number of result rows to be fetched.
Use	Clicking Use enables you to use the Rule to generate a Report, Alert of Chart.
Save	Clicking Save saves the rule that you are editing and the Build Rule panel remains open. Before testing a rule, you must save it if you want to keep your changes.
Reset	Clicking Reset clears all the field information .
Test Rule	Clicking test rule opens the Test Rule dialog.

Test Rule Dialog

To access the Test Rule view:

1. Go to **Reports**.

   The Manage tab is displayed.

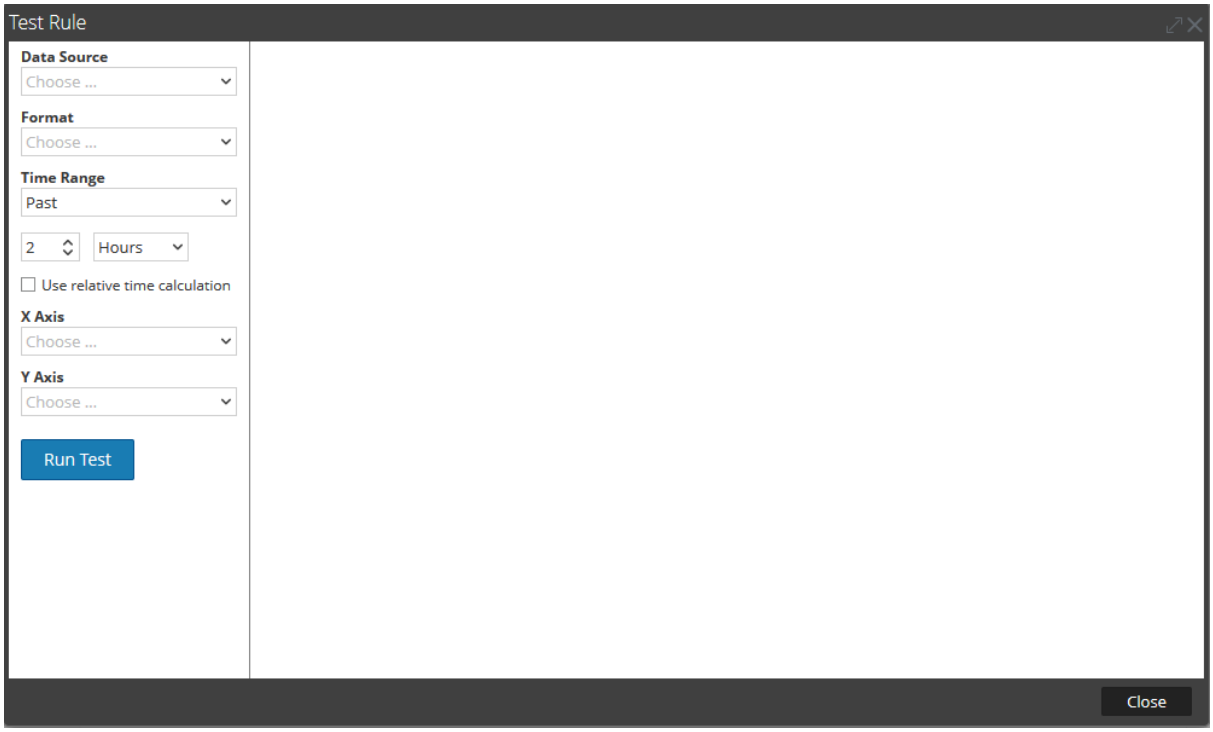
2. In the **Rules** panel, do one of the following:

   - Select a rule and click  in the Rules toolbar.
   - Click  > **Edit**.

     The Build Rule view tab is displayed.

3. Click **Test Rule**.

The Test Rule view is displayed.



The following table describes the features in the Test Rule Dialog.

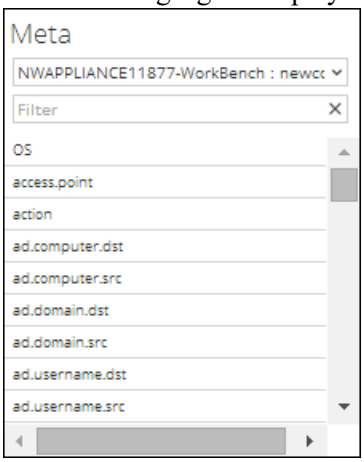
Feature	Description
Data Source	A drop-down list of data sources for the type of rule you are testing. Possible data sources are: Concentrator, Broker, Decoder or Log Decoder.
Format	A drop-down list of the formats for displaying results for the rule. Possible formats are: Tabular, Area, Bar, Bubble, Column, Line, Pie, Step Line, Step Area, Spline Area, and Spline.
Time Range	A drop-down list of time range specification methods. • Selecting Past allows you to specify a number of years, months, days, weeks, or hours. For example, Hours, Days, Weeks, Months, or Years. • Selecting Range allows you to specify a date range and time period. For example, start date to end date. In the user interface, the date or time displayed depends on the time zone profile selected by the user.
Use relative time calculation	Selecting this option calculates the time range relative to the current time.

Feature	Description
X Axis	X-Axis and Y-Axis specify the metadata to be plotted in charts. In the X-Axis drop-down list, the meta types for the `Group by` setting in the rule are listed. You can select multiple meta types when the rule has a single `Group by` setting. For Custom Rules with multiple `Group by` values, you can select only the first meta type for the X-Axis.
Y Axis	In the Y-Axis drop-down list, the aggregate functions used in the rule are listed. Sum, Count, Countdistinct and Average are the supported aggregate functions for rules. You can select one or more aggregate functions.
Run Test	Clicking Run Test executes a test of the rule last saved in the Rule Builder dialog. When the test is complete, the rule data (if any) for the selected time range is displayed.

Meta Panel

The Meta panel provides a list of available meta types that you can use to build the rule. You can use the meta types in the Select, Where, and Then clauses. The Reporting Engine maintains an active list of the available meta names by continuously synchronizing with the data source to which it is connected.

The following figure displays the Meta panel.



The following table describes the features in the Meta panel.

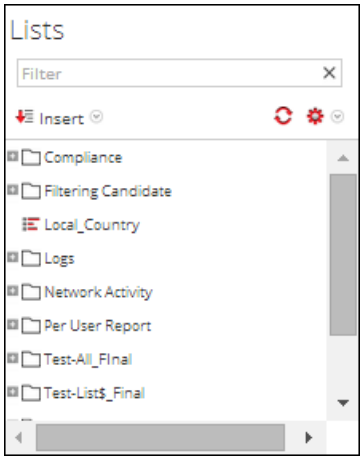
Operation	Description
Choose	Based on the rule type that you have selected, the available data sources are displayed in the drop-down list of the Meta panel. Select the required data source. The available meta types for the data source are displayed. Select a meta.
Filter	Filter the meta for a specific meta value.

Lists Panel

A List is a placeholder for a set of values that you can use in a meta or a variable. For example, you can define a list with all the whitelisted event source IP addresses. Once the List is defined then you can use the List name in the rule. This provides the flexibility of adding, modifying, and deleting the list values.

The Lists panel is a collection of Lists. The Reporting Engine maintains an active list of the available list names by continuously synchronizing with the collection to which it is connected.

The following figure displays the Lists panel.



The following table describes the features in the Lists panel.

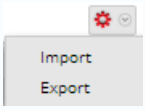
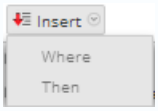
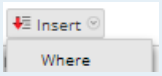
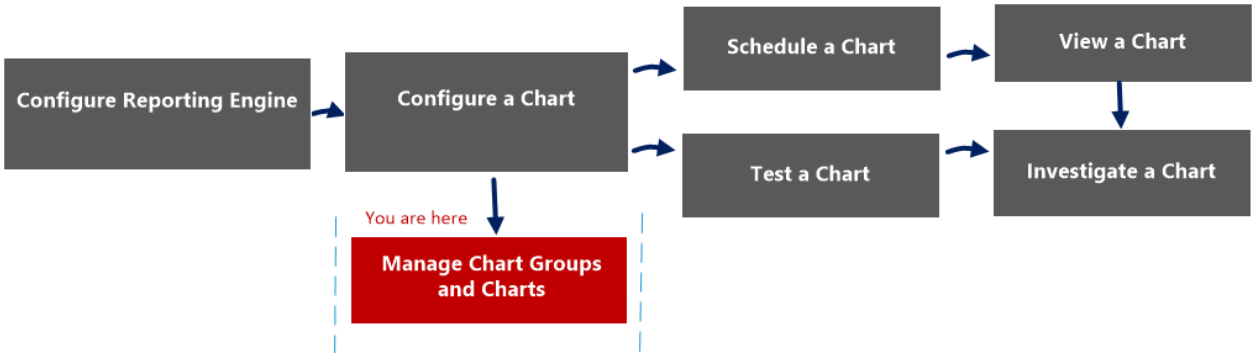
Operation	Description
	Import or Export a list.
	Refresh the Lists.
	If you select the **NetWitness DB** rule type, the options Where and Then are displayed. Insert the list in the Where or Then clause in the rule.
	If you select the **Warehouse DB** rule type, the option Where is displayed. Insert the list in the Where clause in the rule.

Chart Permissions Dialog

In the Chart Permissions dialog, you can manage access permissions for user roles at the chart and chart group level. Only a user with the 'Read & Write' permission can configure the chart in the Reporting module.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart*	Manage a Chart Group and Chart

*You can complete these tasks here.

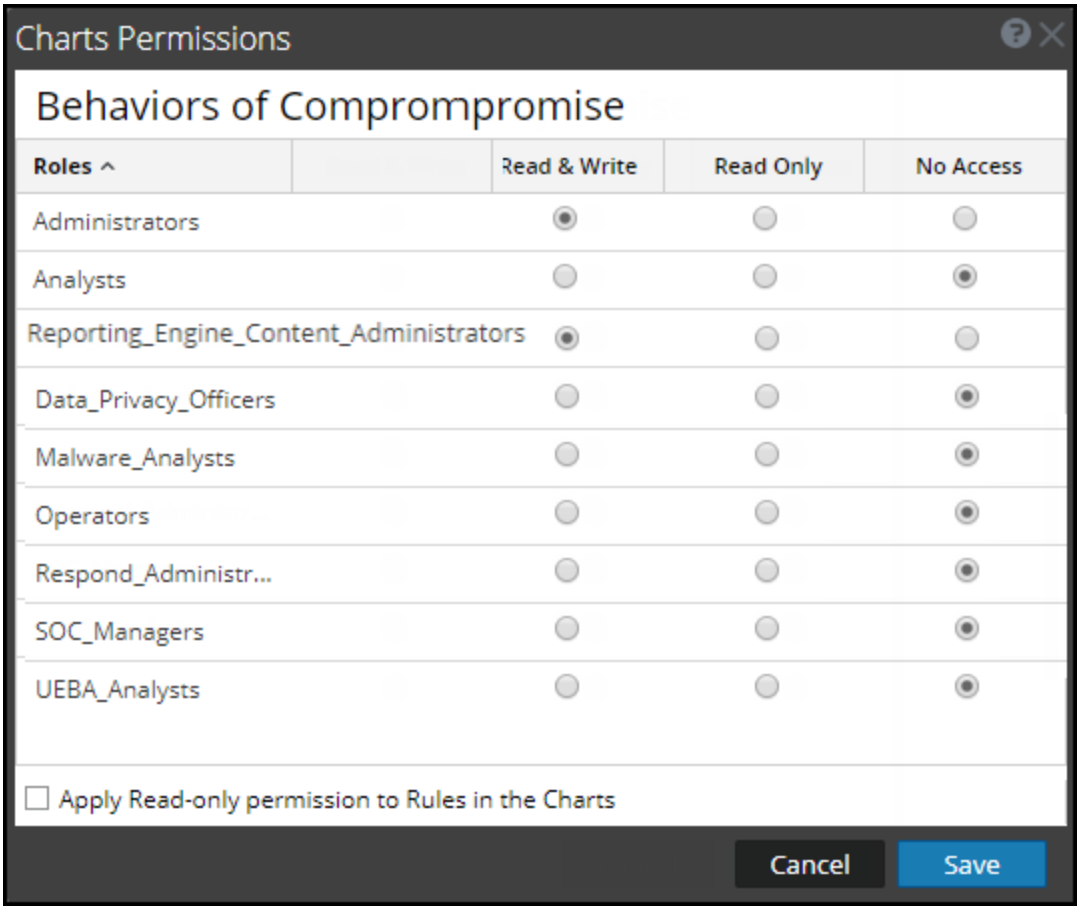
Related Topics

- Configure and Generate a Chart

Quick View

The Chart permissions dialog allows you to set chart permissions depending on the user role.

The following figure is an example with the important features labeled.



1. Click **Reports** to view the Manage tab.
2. Click **Charts** to open the Chart view.
3. In the **Charts** panel, select a report and click > **Permissions**. The Chart Permissions dialog box is displayed.
4. Based on the user role, select the appropriate options.
5. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.
6. Click **Save**.

The following table lists the columns in the Charts Permission dialog.

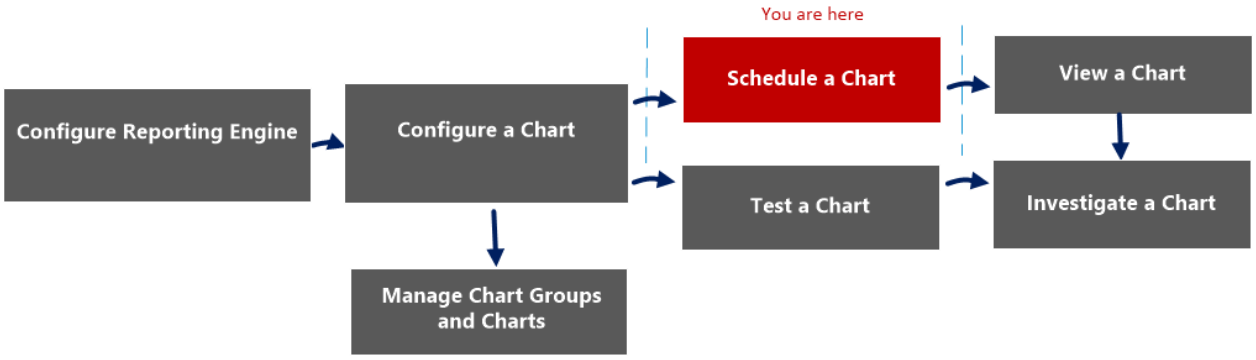
Column	Description
Roles	Displays all the user roles in the NetWitness user interface.
Read & Write	Allows you to apply 'Read&Write' access to the chart.
Read Only	Allows you to apply only 'Read' access to the chart.

Column	Description
No Access	By selecting this permission, you cannot access or view the chart.
☐ Apply these permissions to sub-groups and Charts in this group	Allows you to apply permissions to the chart group, subgroups in the group and charts in the group. **Note:** This checkbox is populated only when you set access permissions for a Chart Group.
☐ Apply Read-only permission to Rules in the Charts	Allows you to automatically apply permissions to the rules in the charts.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selection and provides access to the role based on the selection.

Chart View

In the Chart View, you can see the available charts and groups in a grid format and also schedule them by enabling the charts.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart*	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

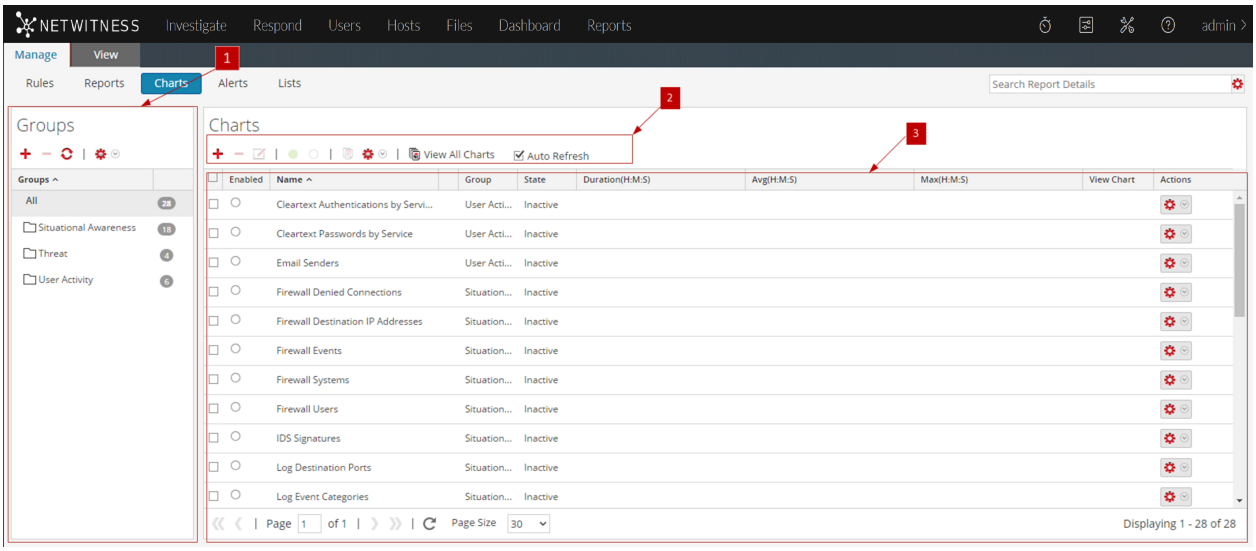
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.

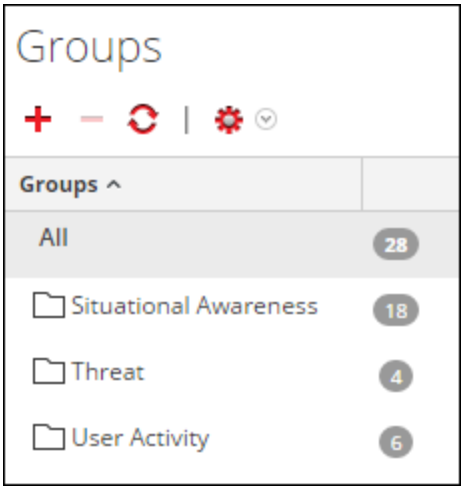


The Chart view includes the following panels:

1 Charts Groups panel
2 Charts toolbar
3 Charts panel

Charts Groups Panel

The Charts Groups panel allows you to organize charts in a group. You can create a group, add charts to the group and move charts among groups. The following figure shows the Charts Groups panel.



The Charts Groups Panel includes the following options:

Feature	Description
+	Adds a new chart to the Reporting module.

Feature	Description
	Deletes one or more selected charts.
	Edits a chart.
	Refreshes the view.
	Provides the following options: Import, Export and Permissions.

Charts Toolbar

The Charts toolbar allows you to add, modify, delete, duplicate, activate, deactivate, import and export a chart. You can also set access permissions for charts in a group.

The Chart toolbar includes the following options:

Feature	Description
	Adds a new chart to the Reporting module.
	Deletes one or more selected charts.
	Edit charts.
	Enables the selected charts.
	Disables the selected charts.
	Creates a duplicate copy of the selected chart.
	Provides the following options: Import, Export, Export as Text and Permissions.
View All Charts	Displays all the executed charts.
Auto Refresh	Automatically refreshes the charts list.
	Allows users to filter unused charts.

Charts Panel

The Charts Panel presents all the charts in a tabular or grid format.

The following table lists the columns in the Chart panel and their description.

Feature	Description
Enabled	● - The chart is enabled. ○ - The chart is disabled.
Name	The name of the chart.
Group	The Chart Group to which the chart belongs.
State	The state of the chart: • Queued • Completed • Failed
Duration (H:M:S)	The time taken to execute the latest chart.
Avg(H:M:S)	The average time taken to run the chart.
Max(H:M:S)	The maximum time taken to run the chart.
View Chart	A hyperlink that redirects to the View a Chart panel.
	The actions menu has the following options: Enable, Disable, View, Delete, Edit, and Export.

Execution History Panel

The Execution History panel allows you to fetch and display history details.

Workflow

This workflow shows the procedure to view report or report groups.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access control for lists, rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

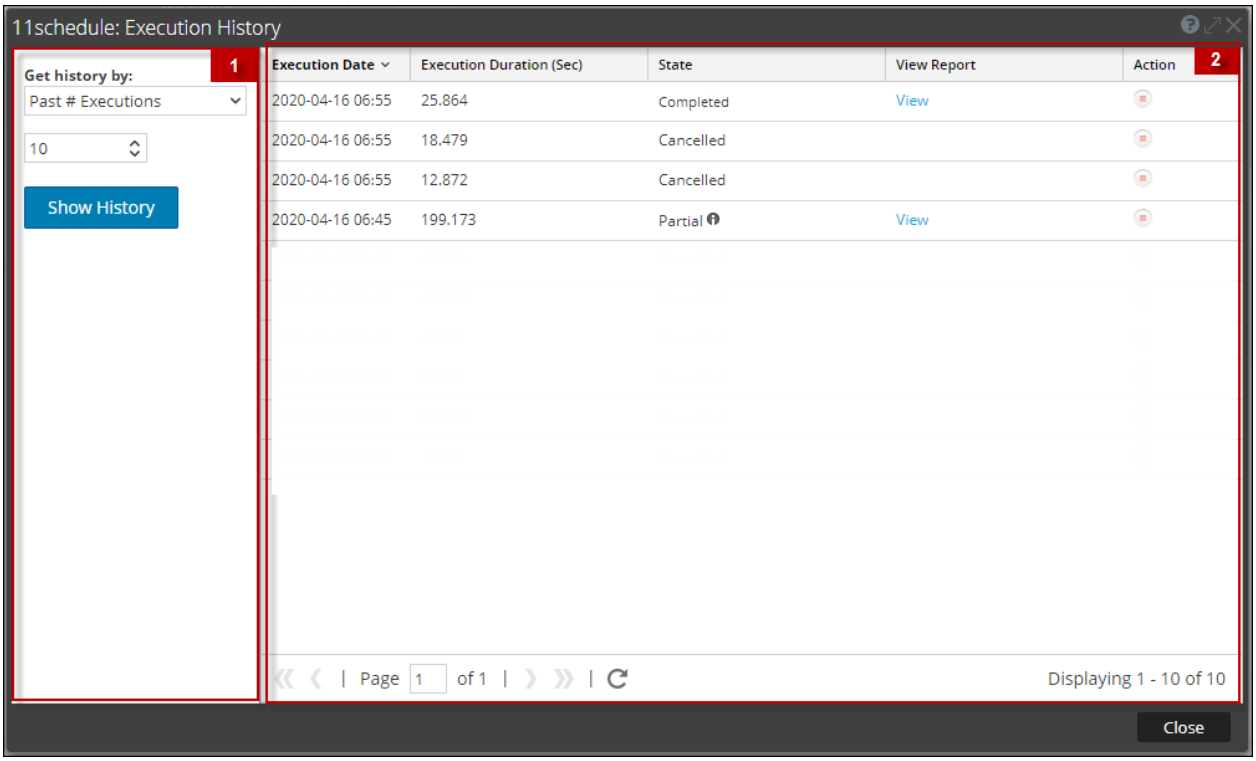
Related Topics

- Configure and Generate a Report
- Generate List Panel

- Scheduled Reports View

Quick View

The following figure is an example of the Execution History view.



Features

The View Execution History has the following panels:

1 Execution History Options panel
2 Execution History Output panel

To access this view:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, do one of the following:

   - Hover the mouse over a report and click > **View Scheduled Reports**.
   - Click **#Schedules** column.
     The Schedule Reports view is displayed with the status of each of the scheduled report.
4. Select a scheduled report and do one of the following:

- Click  > **Execution History**.
- Click  from the **Scheduled Reports** Toolbar Panel.

Execution History Options Panel

The Execution History Options panel allows you to fetch the history details based on either past n number of scheduled reports or a specific date range.

The following table lists the operations in the Execution History Options panel:

Operation	Description
Get history by:	This is the criteria to view the execution history: • **Past # Executions**: The past n number of scheduled reports. By default this option is displayed. • **Range (specific)**: The start date and end date for the date range. **Note:** The **From** and **To** field is populated in the NetWitness UI only when you select 'Range (Specific)' from the **Get history by** list.
From	The start date for the date range.
To	The end date for the date range.
Count	The number of execution history of the scheduled report to be displayed.
Show History	Shows the history details based on the selected criteria.

Execution History Output Panel

The Execution History Output panel displays the history details with the execution date, execution duration (seconds), state of the scheduled report, and a link to view the report.

The following table lists the various columns in the Execution History Output panel:

Column	Description
Execution Date	The date on which the scheduled report was executed. By default, the execution date is in descending order.
Execution Duration (Sec)	The time duration taken to execute the scheduled report.

Column	Description
State	The state of the scheduled report: • Scheduled: If a report is scheduled to run on an hourly, daily, weekly, monthly, or later time, the state of the report is displayed as scheduled, for the first run. • Queued: If a report is still waiting to get executed, the state of the report is displayed as queued. • Running: If the report schedule is in progress, the state of the report is displayed as running. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule schedule executions failed, the state of the report is displayed as failed. • Completed: If a report schedule is successfully executed, the state of the report is displayed as completed. • Canceled: When cancel request is completed, the state of the report is displayed as canceled. • Inactive: If a report schedule is disabled, the state of the report is displayed as Inactive. • Not available: If the report schedule executed information is not available, the state of the report is displayed as not available.
View Report	The hyperlink to View a Report on full screen.
Action	Displays the icon to stop the execution schedule.
Close	Closes the execution history view.

Generate List Panel

The Generate List dialog allows you to generate and customize a list.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

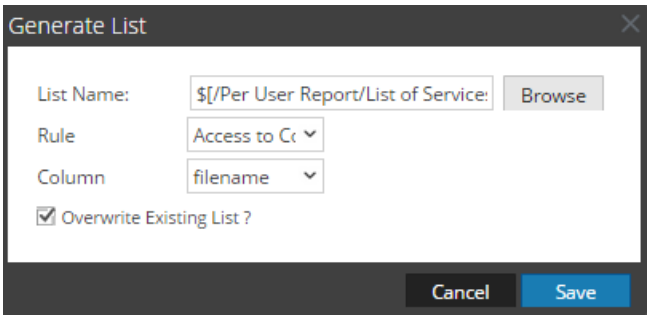
Related Topics

- List View
- Build List View

- Lists Permissions Dialog

Quick View

The following figure is an example of the Generate List dialog.



To access this view:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, select a report and click > **Schedule Report**.

   The Schedule a Report view tab is displayed.

4. In the **Output Actions** section, in **Dynamic List** panel, click .

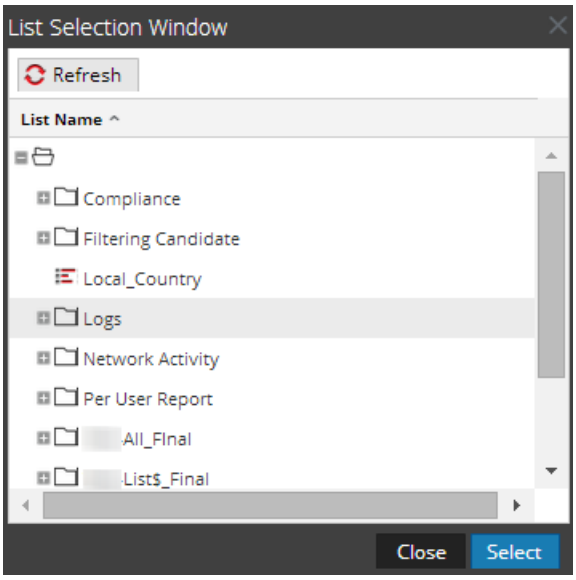
   The Generate List dialog is displayed.

Features

The following table lists the features in the Generate List dialog.

Field	Description
List Name	The name of the list chosen from the List Selection panel.
Browse	Click this button to select a list from the List Selection Window dialog.
Rule	Select a rule to be used to create the list.
Column	Select a value for the column.
Overwrite Existing List?	Overwrites the existing list.
Save	Adds the desired list to the Generate List panel of the Schedule Report view.

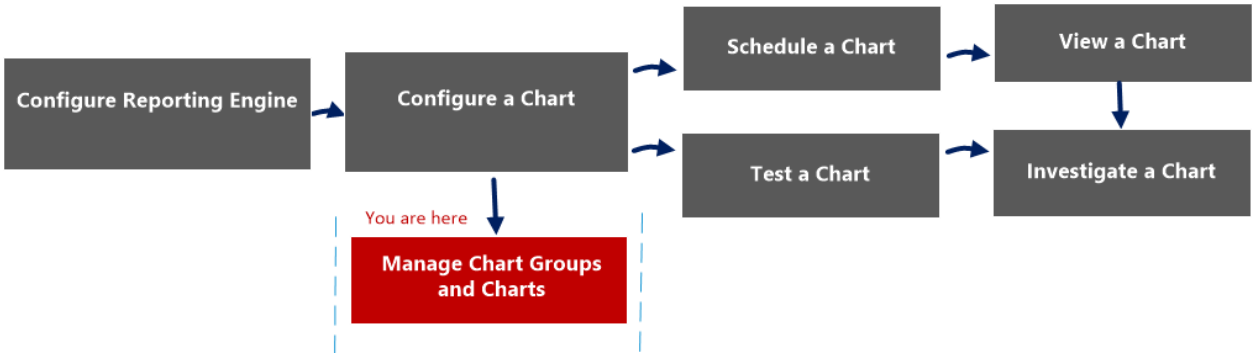
The List Selection Window dialog consists of lists that are defined in the Lists panel. Here, you can select a list to associate it with the report. The following figure shows the dialog.


List Selection Window
Refresh
List Name
Compliance
Filtering Candidate
Local_Country
Logs
Network Activity
Per User Report
All_FInal
List$_Final
Close
Select

Import Chart Dialog

In the Import Chart dialog, you can import charts containing subgroups and charts from other instances of NetWitness into the Chart Groups panel. Charts must be in a valid binary file that was exported from another NetWitness instance.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart*	Manage a Chart Group and Chart

*You can complete these tasks here.

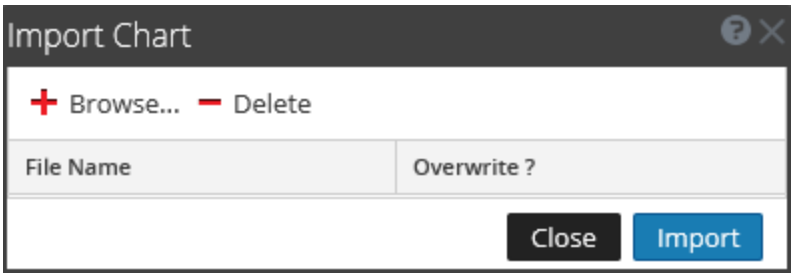
Related Topics

- Configure and Generate a Chart

Quick View

This dialog displays differently when you use it to import groups containing subgroups and charts from other instances of NetWitness into the Chart Groups panel.

The following figure is an example of the Import Chart dialog.



1. Click **Reports** to view the Manage tab.
2. Click **Charts** to open the Chart view.
3. In the **Charts Groups** panel, select a folder to import the file.
4. In the **Charts Groups** panel or **Charts** toolbar, click > **Import** to import the file.

The following table describes the features in the Import Chart dialog.

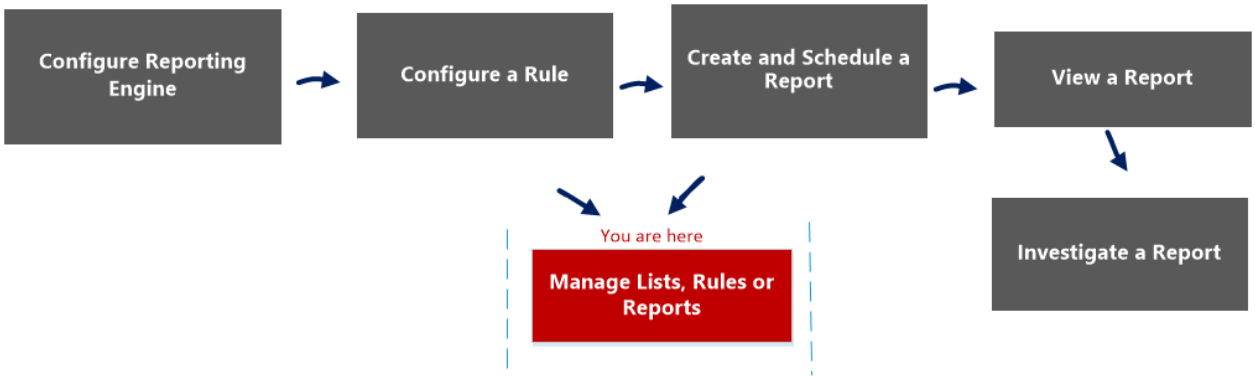
Feature	Description
Browse	Displays a view of the local file system so that you can select the chart to be imported.
Delete	Deletes an imported report from the list of imported charts.
File Name	Displays a list of chart files that will be imported to your Charts module when you click Import.
Overwrite?	Allows you to select the option to overwrite an existing version of the chart you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	Closes the dialog. If you have charts to select for import, but have not clicked Import. The charts are not imported, and are not saved in this dialog.
Import	Imports the selected charts to your Charts module.

Import Report Dialog

In Import Report dialog, you can import groups containing subgroups and reports from other instances of NetWitness into Report Groups panel. Reports must be in a valid binary file that was exported from another NetWitness instance.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

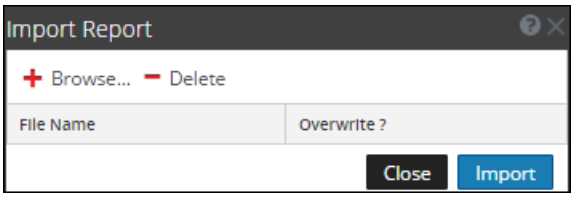
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Reports Permissions Dialog

Quick View



To access the Import Report dialog:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports Groups** panel, select a folder to import the file.
4. Do one of the following:
   - In the **Reports Groups** panel, click > **Import** to import a group.
   - In the **Reports** toolbar, click > **Import** to import a report.

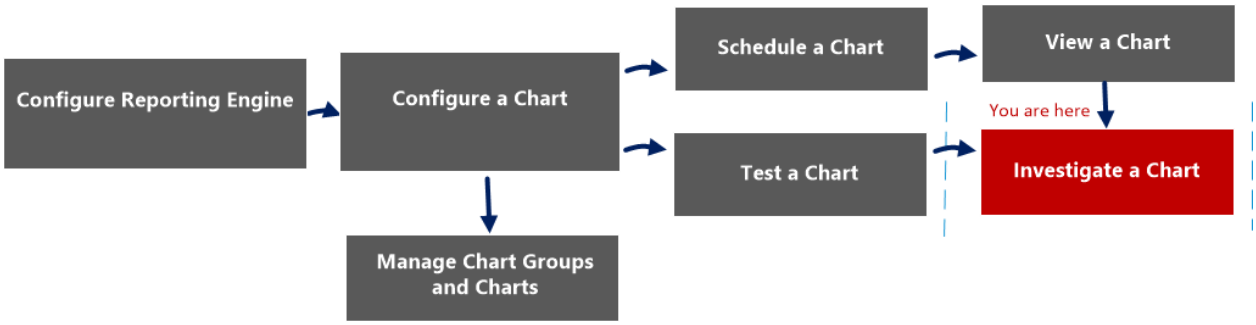
The following table lists the features of the Import Report dialog.

Feature	Description
Browse	This option displays a view of the local file system so that you can select the report to be imported.
Delete	This option deletes an imported report from the list of imported reports.
File Name	Displays a list of report files that will be imported to your Reports module when you click Import.
Overwrite?	Allows you to select the option to overwrite an existing version of the report you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	This option closes the dialog. If you select a report and not clicked Import. The reports are not imported, and are not saved in this dialog.
Import	This option imports the selected reports to your Reports module.

Investigate a Chart View

In the Investigate a Chart view, you can view and investigate chart details. There are options for filtering and sorting the information in the chart, as well as options for the type of chart, the number of items to chart, and charting values or totals. When viewing a chart, you can open the charted sessions in the Investigation module and save the chart as a PDF.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engin" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart*	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

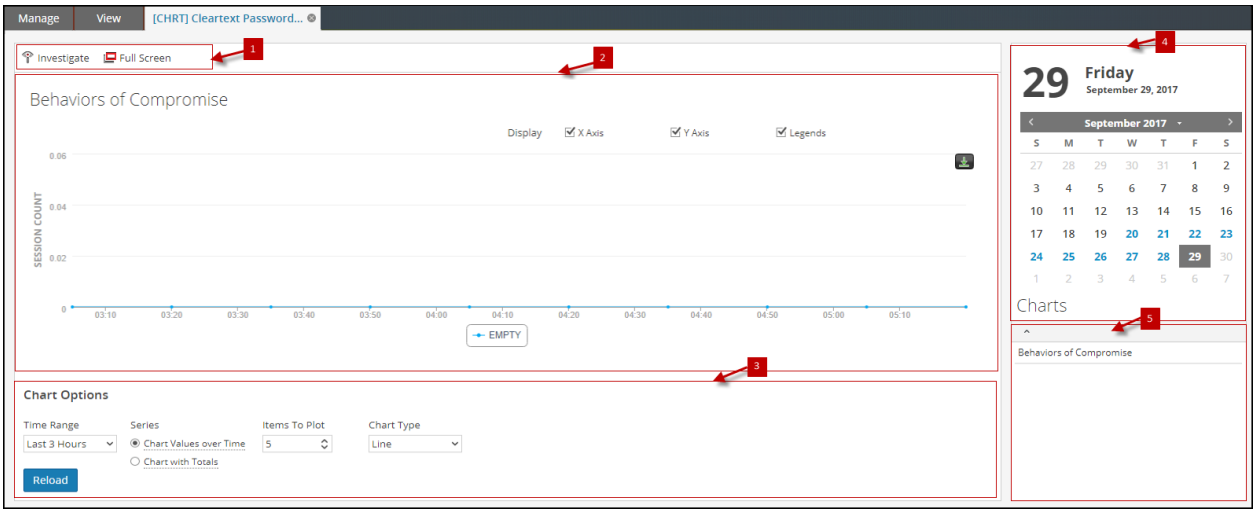
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The View a Chart panel includes the following panels:

1. Chart toolbar
2. Chart Output panel
3. Chart Calendar panel
4. Chart Options panel
5. Chart Executed list

Chart Toolbar

The Chart toolbar has options that allow you to investigate, and view the chart on another screen.

The following table lists the options in the Chart toolbar.

Operation	Description
Investigate	Investigates the chart details.
Full Screen	Displays the chart on a full screen.

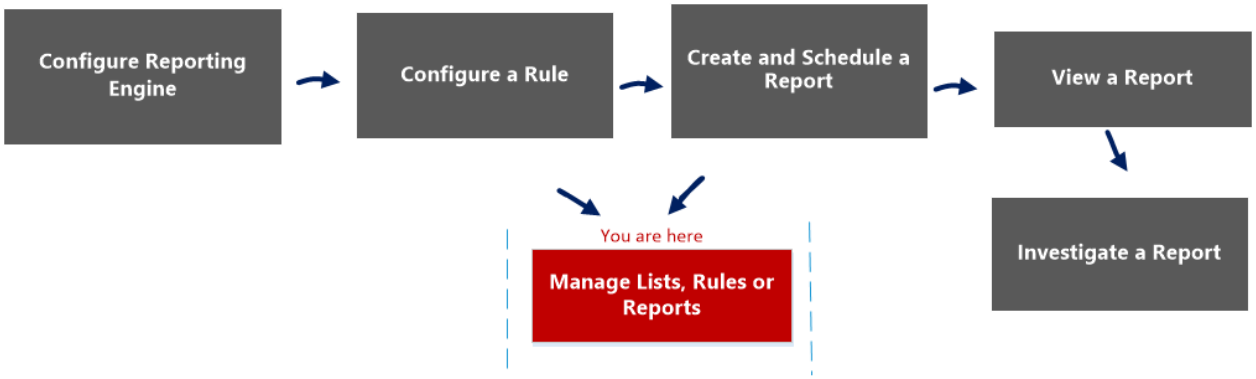
Lists Permissions Dialog

In the Lists Permissions dialog, you can manage access permissions for a user role at the list or list group level. Only a user with **Read and Write** permission can configure the list in the Reporting Module.

Workflow

This workflow shows the procedure to manage lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists. You can use lists to define rules for generating reports, charts and alerts.

You must ensure that Reporting Engine is configured on NetWitness.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

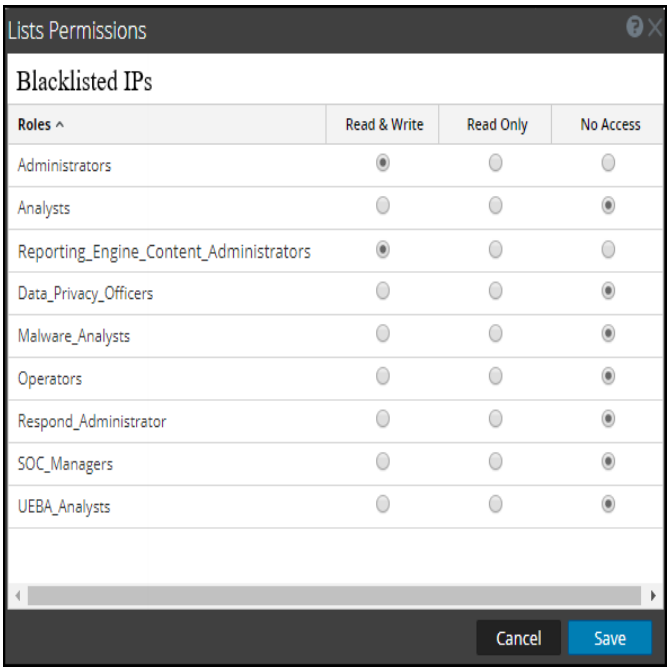
*You can complete these tasks here.

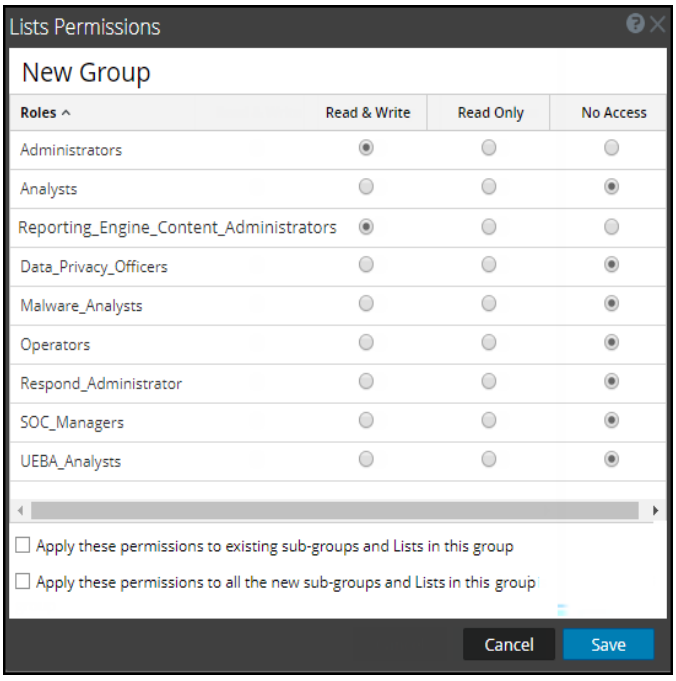
Related Topics

- List View
- List section in the "Role Permissions" topic in the *System Security and User Management Guide*.

Quick View

The following figures are examples of the Lists Permissions dialog and List Group Permission dialog:





To access this view

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Lists**.
   The Lists view is displayed.
3. In the **Lists** view, select a report.
4. In the **Lists** toolbar, click  > **Permissions**.
   The Reports Permissions dialog is displayed.

The following table describes the features in the Lists Permissions dialog:

Feature	Description
Roles	Describes roles of the users logged into the NetWitness user interface.
Read & Write	Allows users to access, view, edit, delete, import, and export lists on the Lists view. Users can also change the permission on the rule.
Read Only	Allows users to only access and view the list on the lists view.
No Access	Doesn't allow users to access or view the lists.
Apply these permissions to subgroups and lists in this groups	Automatically applies permissions to the subgroups and lists in the groups, if checkbox is selected.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selections and provides access to the roles based on the selections.

List View

In the List view you can see available lists and groups in a grid.

Workflow

This workflow shows the procedure to define lists or list groups. You can set access control at the list or list group level so that only users with specific roles can access the lists. You can use lists to define rules for generating reports, charts and alerts.

You must ensure that Reporting Engine is configured on NetWitness.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

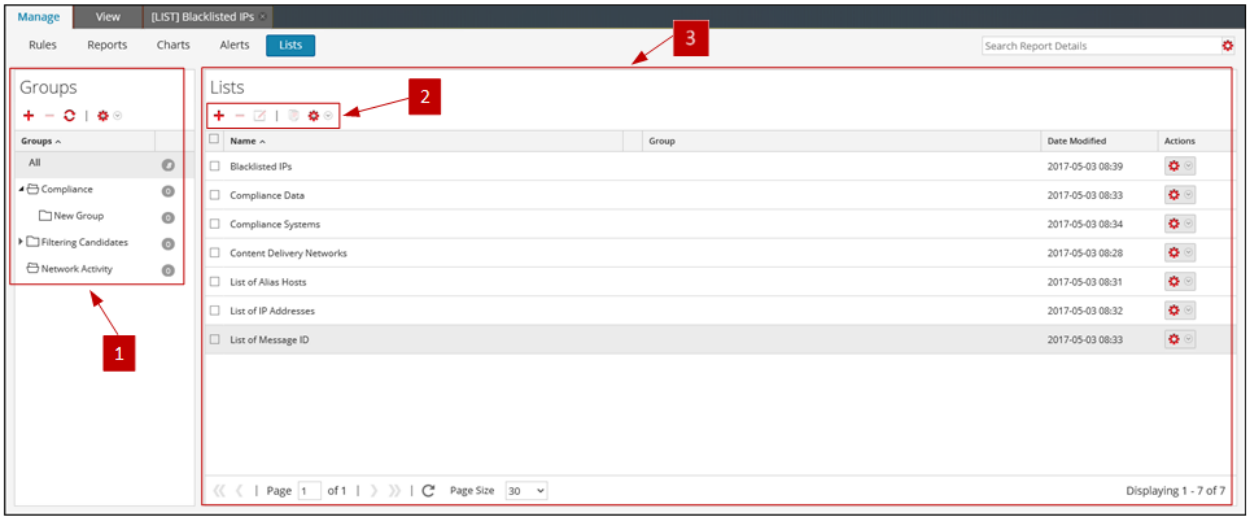
*You can complete these tasks here.

Related Topics

- Lists Permissions Dialog
- Build List View

Quick View

The following figure shows the List view.



To access this view

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Lists**.

   The Lists view is displayed.

The List view includes the following panels:

1 Lists Groups panel
2 Lists toolbar
3 Lists panel

Lists Groups Panel

The Lists Groups panel provides a list of groups used to organize lists and has a toolbar that allows you to create and manage the groups.

Feature	Description
	Allows users to add a new group to the Reporting module.
	Allows users to delete groups.
	Refreshes the view.

Feature	Description
	Allows users to access following options: Import, Export and Permissions.
	Allows users to filter unused lists.

You can perform the following actions using the Lists Groups panel.

- Refresh lists in a group.
- Move lists between different groups. You can move a list from one group to another by dragging and dropping the list in the required group.
- Create list groups.
- Delete list groups.
- Import list groups.
- Export list groups.
- Set access control for list groups.

Lists Toolbar

Feature	Description
	Allows user to add a new list to the Reporting module.
	Allows user to delete one or more selected lists.
	Allows user to edit lists.
	Creates a duplicate copy of the selected list.
	Allows user to access the following options: Import, Export and Permissions.

Lists Panel

The Lists panel displays all the lists defined in a tabular format.

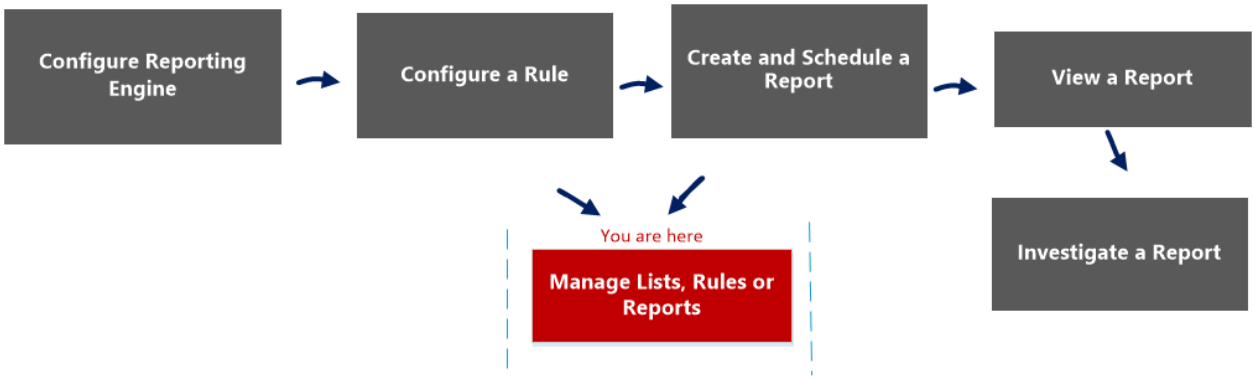
Column	Description
Name	Displays the name of the list. **Note:** For **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.
Group	Displays the list group to which the list belongs.
Date Modified	Displays the date and time when the list was modified.

Reports Permissions Dialog

In the Reports Permissions dialog, the users with 'Read & Write' access permission can configure permissions.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

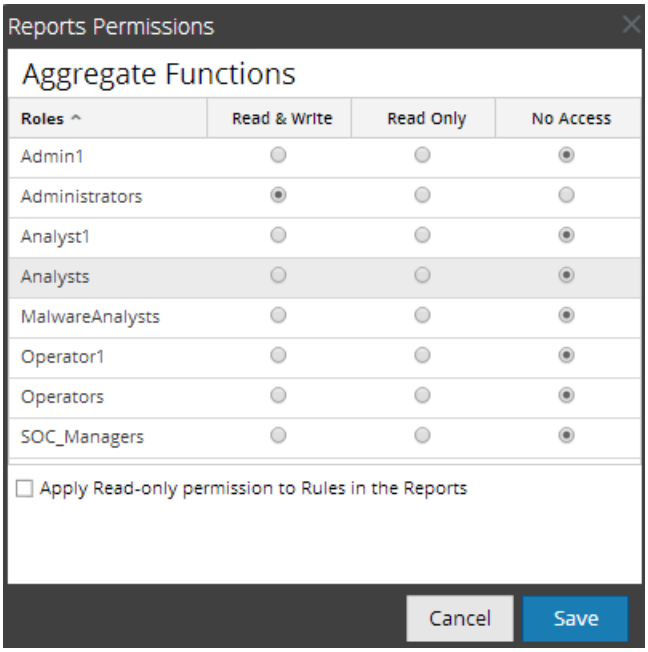
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Import Report Dialog

Quick View



To display the Reports Permissions dialog:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, select a report.
4. Click > **Permissions**.
   The Reports Permissions dialog is displayed.

Note: When you select the check box, all dependent rules are given READ access permission, provided the permissions for the report is higher compared to the permissions of the rules.

The following table describes the features in the Reports Permissions dialog.

Feature	Description
Roles	Displays all the roles who can get access to the permissions.

Feature	Description
Read&Write	Allows you to get Read&Write access to the Rules in the Reports.
Read Only	Allows you to get Read Only permissions to the Rules in the Reports.
No Access	If you select this option, you will not get permission to the Rules in the Reports.
Apply Read-only permissions to Rules in the Reports	Allows to set Read Only permissions to the Rules in the Reports for all the roles .
Cancel	This option cancels all the changes made to the permissions.
Save	This option saves the selections and provides access to the roles based on the selections.

Report View

In the Report view, you can create and manage the report or report groups.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

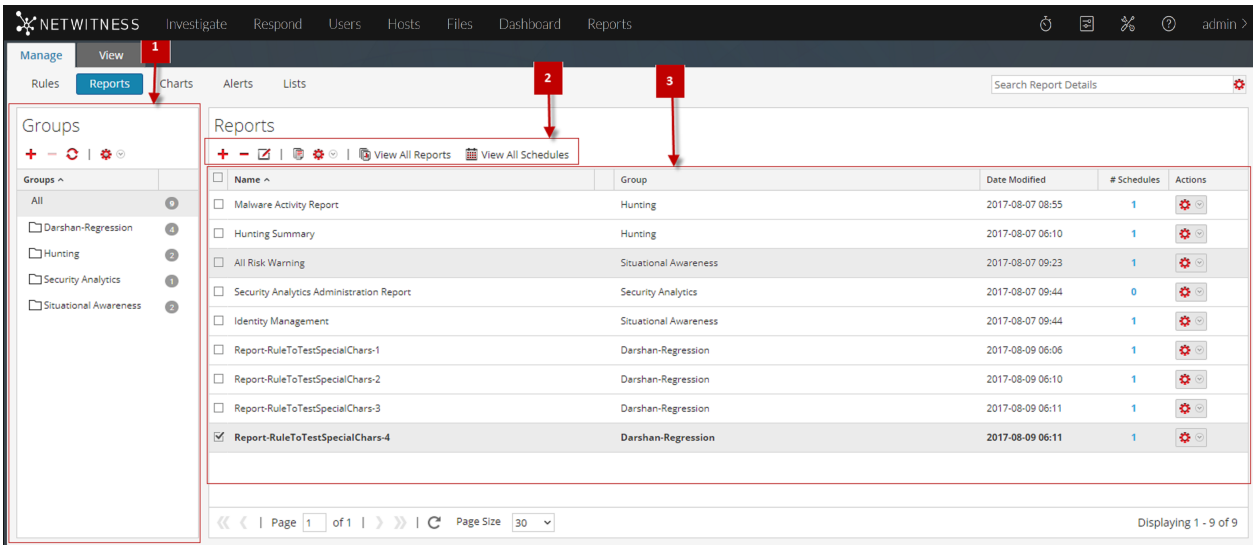
*You can complete these tasks here.

Related Topics

- Build Report View
- Import Report Dialog

- Scheduled Reports View
- Reports Permissions Dialog

Quick View



To access this view:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Reports view is displayed.

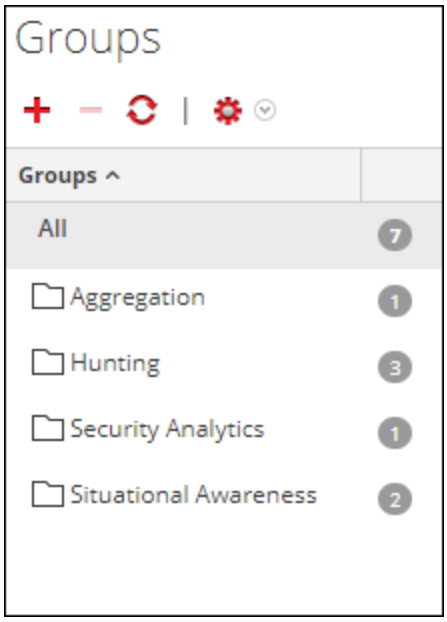
Features

The Report view includes the following sections:

1	Reports Groups panel
2	Reports toolbar
3	Reports panel

Report Groups Panel

The Report Groups panel allows you to organize reports in a group. You can create a report group, add reports to the group, and move reports among groups. You can view all reports by selecting All option under the Groups column.



Feature	Description
+	This option allows you to add a new report to the Reporting module.
−	This option allows you to delete one or more selected report.
↻	This option refreshes the view.
⚙	The actions menu has the following options: Import, Export and Permissions.

Reports Toolbar

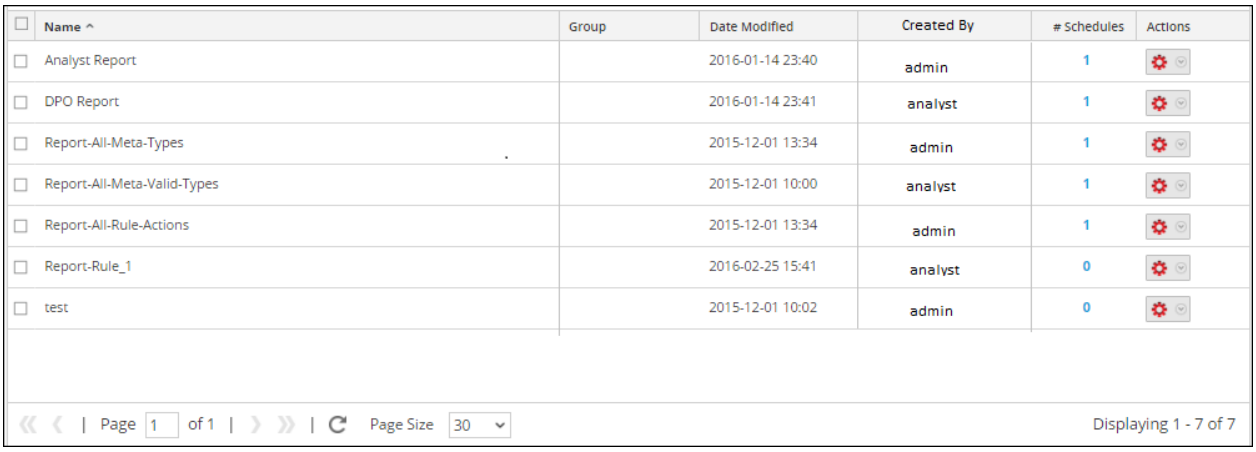
The Reports toolbar allows you to add, modify, delete, duplicate, import and export reports. You can also set access permissions for a report in a group.

Feature	Description
+	This option allows you to add a new report to the Reporting module.
−	This option allows you to delete one or more selected reports.
✎	This option allows you to edit a chart.
⧉	This option creates a duplicate copy of the selected report.
⚙	The actions menu has the following options: Import, Export , Export as Text and Permissions.

Feature	Description
View All Reports	This option allows you to view a list of reports along with their schedule name and time.
View All	This option allows you to view all the scheduled reports.

Report List Panel

The Report List panel lists all the reports in a tabular format.



The following table describes the columns in the Report List panel.

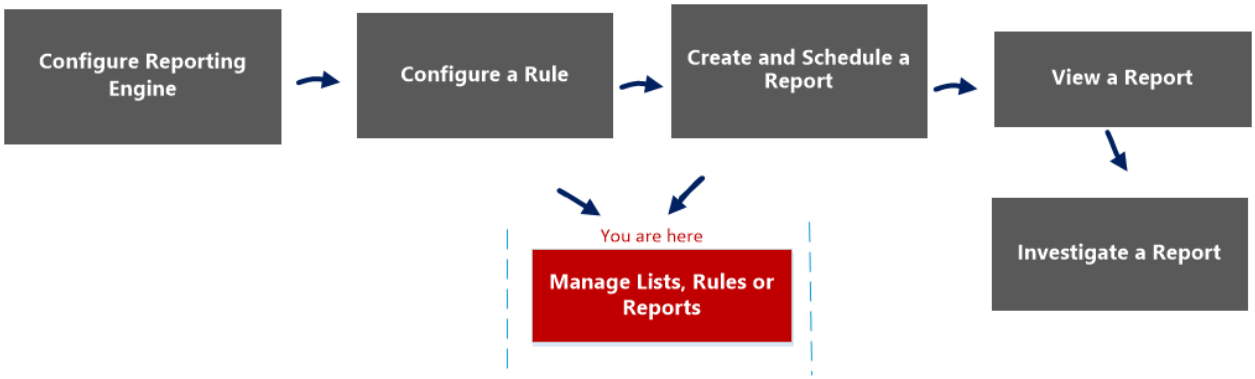
Column	Description
Name	The name of the report.
Group	The Report Group to which the report belongs.
Date Modified	The date and time when the report was modified.
Created By	The creator of the report.
#Schedules	The count indicates the number of schedules created for a report.
Actions	The actions menu has the following options: Schedule Report, View Scheduled Reports, Delete, Edit, and Export.

Rule Permissions Dialog

The Reporting module provides access control at the rule level. Only a user who has the right set of permissions can perform tasks on the rule. When creating user roles, the administrator must ensure that the roles created for specific tasks have access to all the permissions higher in the hierarchy of roles.

Workflow

This workflow shows the procedure to manage rule or rule groups.



What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

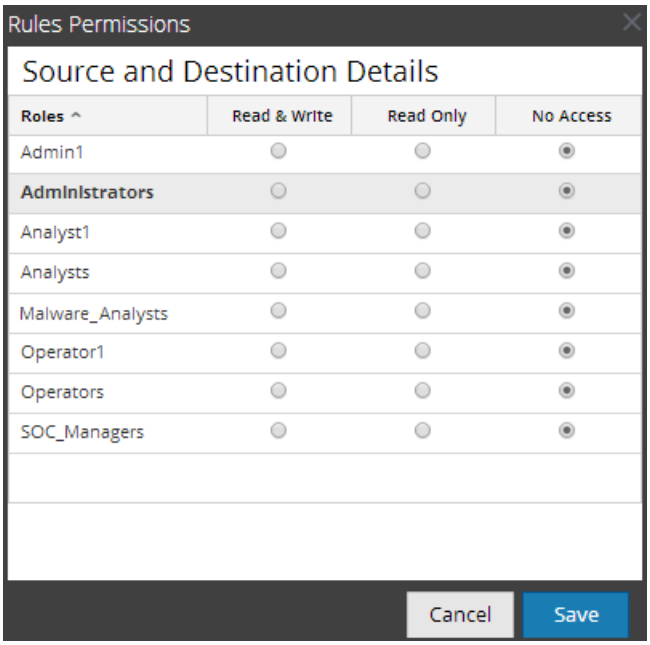
*You can complete these tasks here.

Related Topics

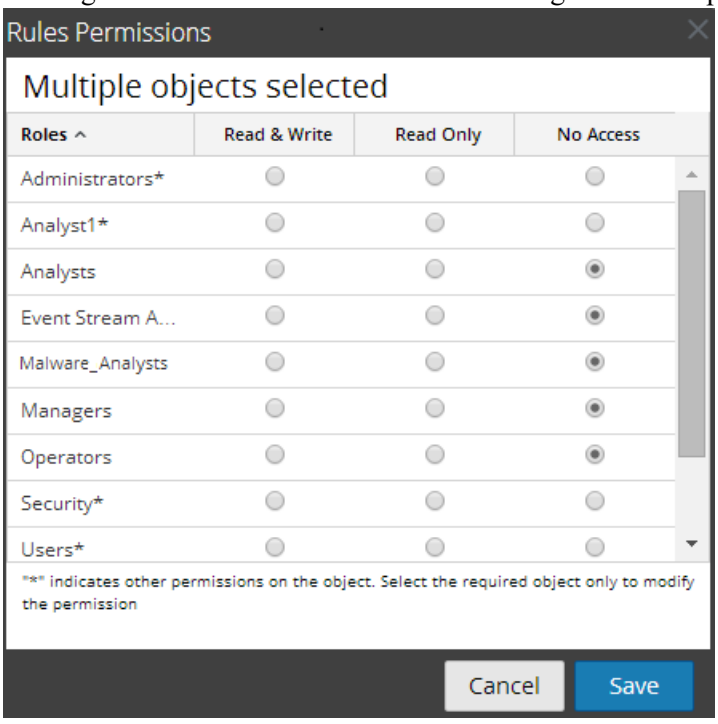
- Rule View

Quick View

This figure shows the Rules Permissions dialog for a single rule.



This figure shows the Rules Permissions dialog when multiple rules are selected.



The dialog has a different appearance for rule groups versus rules. To access the dialog:

1. Go to **Reports**.
   The Manage tab is displayed.
2. In the **Rules** panel, select one or more rules or a rule group.

3. Click  > **Permissions** in the toolbar.

   The Rules Permissions dialog is displayed.

Feature	Description
Roles column	Lists the NetWitness user roles, both built-in and custom roles. Each user who is logged in to NetWitness has user roles assigned. When multiple rules are selected, the asterisk beside the role name, for example, `Security*`, indicates there are other permissions available on that user role. To change the other permissions, you must select the user role and change the access permission.
Read & Write column	When the checkbox in this column is selected, the corresponding user role has permission to view, edit, delete, import, and export rules in the Rules view. The user can also change the permission on the rule.
Read Only column	When the checkbox in this column is selected, the corresponding user role has permission to view the rules in the rule group.
No Access column	When the checkbox in this column is selected, the corresponding user role cannot view or edit the rules in the rule group. Before applying rule permissions, this is the default permission set for all the user roles though the checkbox is unchecked.
Apply these permissions to sub-groups and Rules in this group checkbox	When checked, NetWitness applies permissions to sub-groups and rules in the group.
Cancel option	Clicking Cancel closes the dialog without saving any changes made.
Save option	Clicking Save closes the dialog and updates the rule group permissions for user roles. If specified, the access permissions are applied to subgroups and child objects of this group. When multiple rules are selected, the access permission is applied to all the selected rules.

Rule View

The Rule view is the user interface for managing rules.

Workflow

This workflow shows the procedure to define rule or rule groups.

What do you want to do?

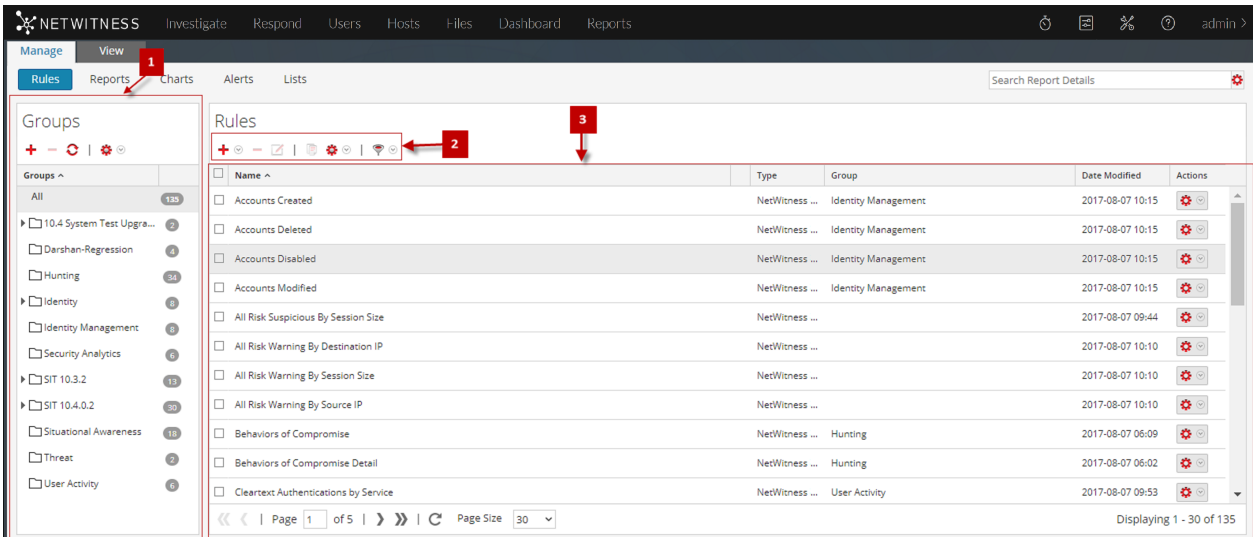
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule*	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Rule Permissions Dialog
- Build Rule View

Quick View



To access the Rules view:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Rules**.

   The Rules view is displayed.

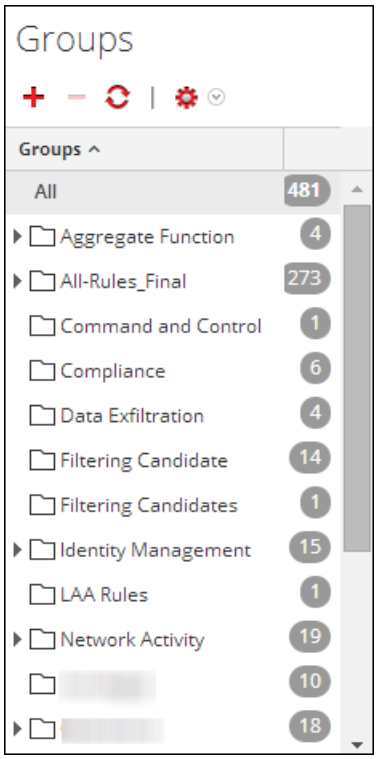
The Rule view includes the following panels.

1	Rules Groups
2	Rules panel
3	Rules Toolbar

Rule Groups Panel

The Rule Groups panel allows you to organize rules into groups using the options in the toolbar. You can create groups and sub-groups and add rules to them. You can also group and move rules between different groups.

The following figure shows the groups in the Rule Groups panel:



The following table describes the features in the Rule Groups Panel.

Feature	Description
+	This option allows you to add a new rule group to the Reporting module.
−	This option allows you to delete one or more rule groups.
↻	This option refreshes the rule group list.
⚙	The actions menu has the following options: Import, Export and Permissions.
All	Displays a list of all the rule groups.

Rule Toolbar

The Rule toolbar allows you to add, delete, edit, and duplicate a rule. The following figure shows the toolbar.

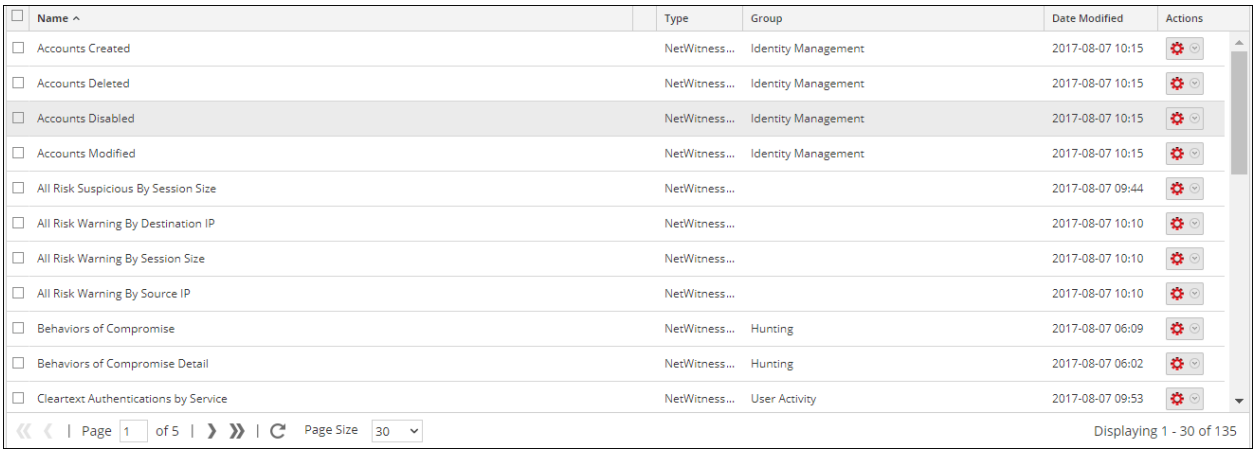
The following table describes the features in the Rule Toolbar

Feature	Description
+	This option allows you to add a new rule to the Reporting module.

Feature	Description
	This option allows you to delete one or more selected rules.
	This option allows you to edit a rule.
	This option allows you to duplicate a rule.
	The actions menu has the following options: Use, Import, Export and Permissions.
	This option allows you to filter the rule type.

Rule List Panel

The following figure shows the list of rules in the Rule List panel.



The following table describes the features in the Rule List Panel.

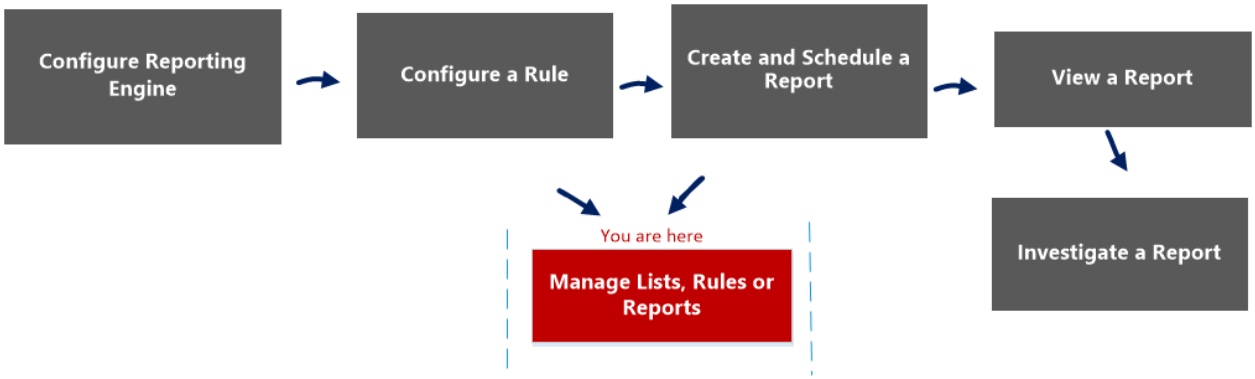
Feature	Description
Name	Displays the name of the rule that you are created or edited. **Note:** For the **Name** field, the icon to extend the column size is not displayed at the end of the column field. You have to hover the mouse a little to the left side to see the icon for extending the column.
Type	Displays the supported database type for the rule you created.
Group	Displays the values which are grouped.
Date Modified	Displays the date when the rule was last modified.
Actions	Displays the actions menu has the following options: Create Alert, Create Chart, Create Report, Delete, Edit, Export, and Dependents.

Select a Logo Dialog

In the Select a Logo dialog, you can upload a new logo that is not available in Reporting Engine Services Config view or choose an existing logo from the Reporting Engine Services Config view.

Workflow

This workflow shows the procedure to manage reports or report groups.



What do you want to do?

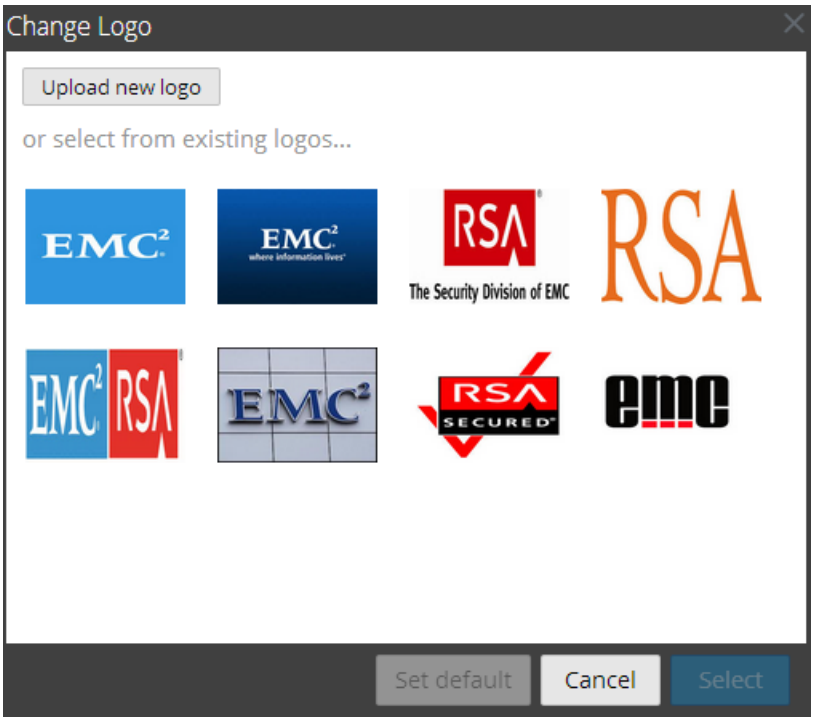
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Scheduled Reports View
- Report View

Quick View



To access this dialog:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Reports view is displayed.

3. In the **Reports** panel, select a report.

4. Click > **View Scheduled Reports**.

   The View scheduled reports view tab is displayed.

5. Select a scheduled report and click > **Edit Schedule**.

   The Schedule a Report view tab is displayed.

6. Click the **Logo** panel.

   The Change a Logo dialog box is displayed.

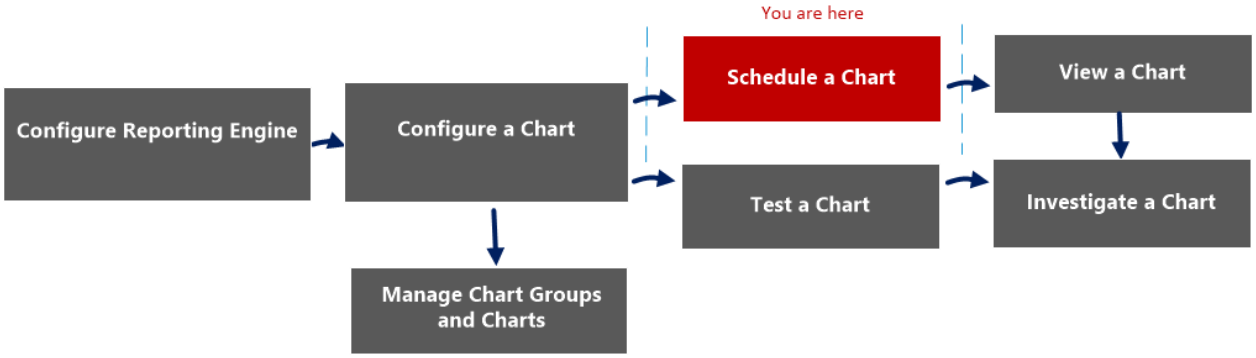
The following table lists the fields in the Select a Logo dialog.

Field	Description
Upload new logo	Click the icon to upload a new logo from the local directory.
Select	Select a logo from the existing list to be used as a logo in the scheduled report.
Cancel	Cancels the logo selection and returns to the Schedule a Report panel.
Set Default	Select a logo to set it as the default logo.

Schedule a Chart View

In the Schedule a Chart View, you can enable or disable a chart.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart*	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

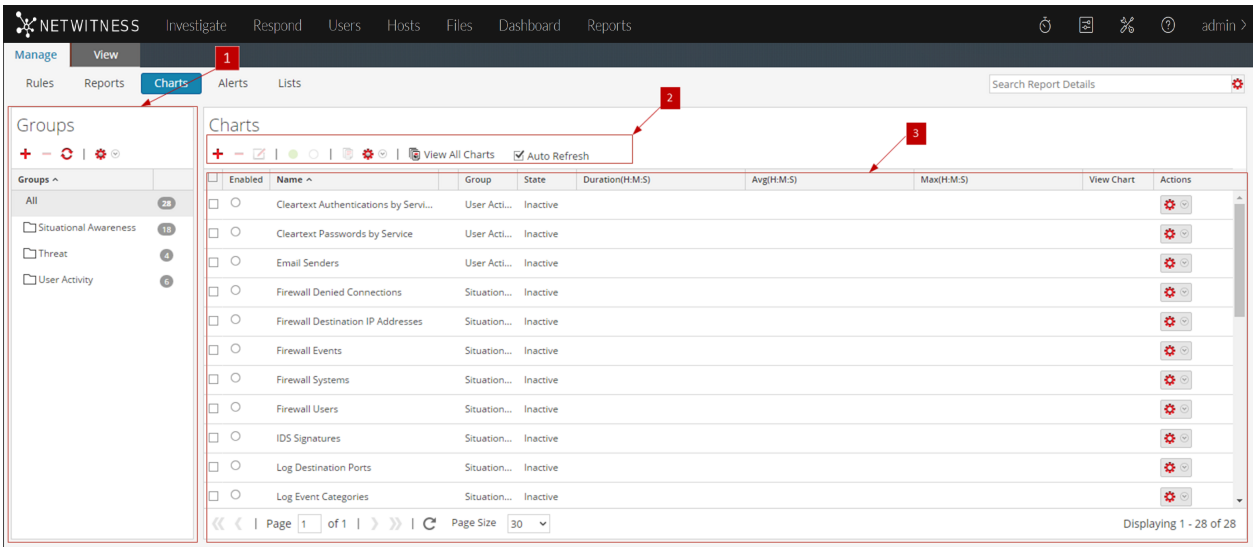
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure shows the Schedule a Chart view.



The Schedule a Chart view includes the following panels:

1 Charts Groups panel
2 Charts toolbar
3 Charts panel

Charts Toolbar

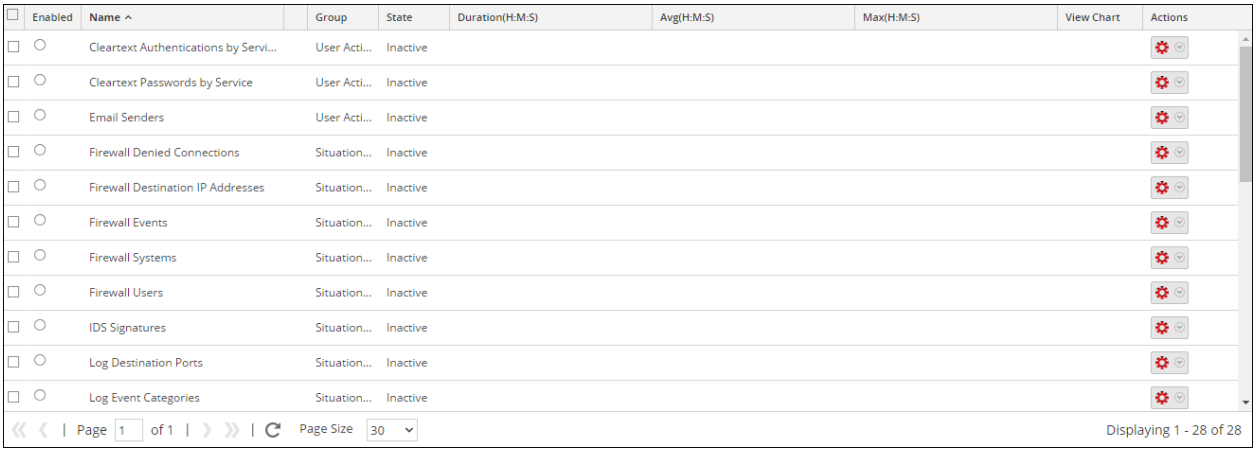
The Charts toolbar allows you to add, modify, delete, duplicate, enable, disable, import and export a chart. You can also set access permissions for charts in a group.

The Charts toolbar includes the following options:

Feature	Description
	Adds a new chart to the Reporting module.
	Deletes one or more selected charts.
	Edit charts.
	Enables the selected charts.
	Disables the selected charts.
	Creates a duplicate copy of the selected chart.
	Provides the following options: Import, Export, Export as Text and Permissions.
View All Charts	Displays all the executed charts.
Auto Refresh	Automatically refreshes the charts list.

Charts Panel

The Charts Panel presents all the charts in a tabular or grid format.



The following table lists the columns in the Charts panel and their description.

Feature	Description
Enabled	- The chart is enabled. - The chart is disabled.
Name	The name of the chart.
Group	The Chart Group to which the chart belongs.
State	The state of the chart: • Queued • Completed • Failed
Duration (H:M:S)	The time taken to execute the latest chart.
Avg(H:M:S)	The average time taken to run the chart.
Max(H:M:S)	The maximum time taken to run the chart.
View Chart	A hyperlink that redirects to the View a Chart panel.
	The actions menu has the following options: Enable, Disable, View, Delete, Edit, and Export.

Schedule Report Panel

The Schedule Report panel allows you to schedule a customized report. Prior to scheduling a report, you can create a dynamic list (with the overwrite option selected) with services added. For more information, see "Generate a List from the Scheduled Report" section in Create and Schedule a Report. Then use the list to generate a report with details in the report like services and host names.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

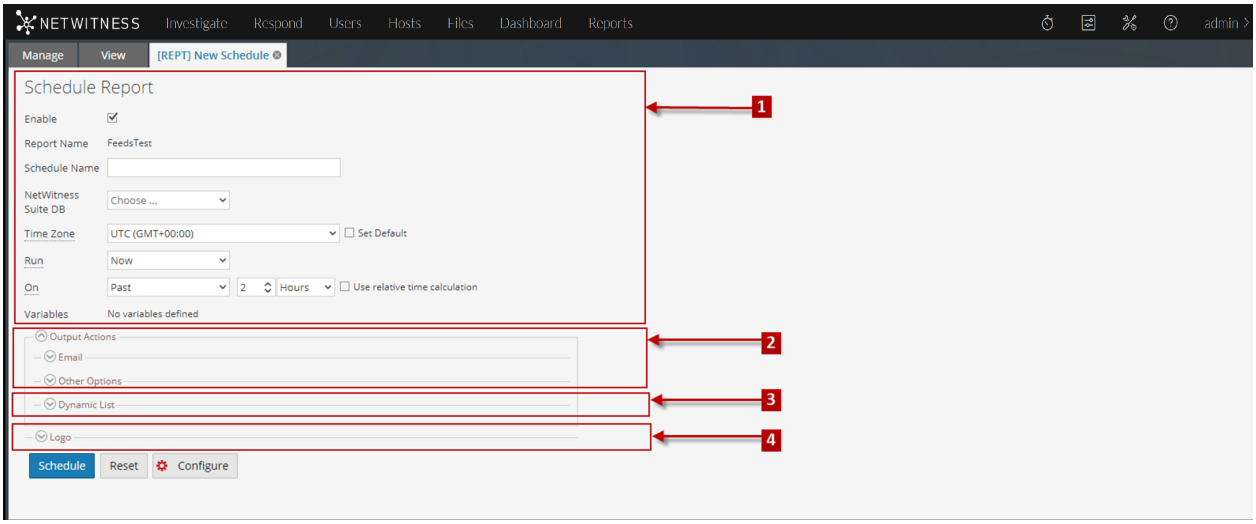
Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Report View
- Build Report View
- Scheduled Reports View

Quick View



To access this view:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Reports view is displayed.
3. In the **Reports** panel, click  > **Schedule Report**.

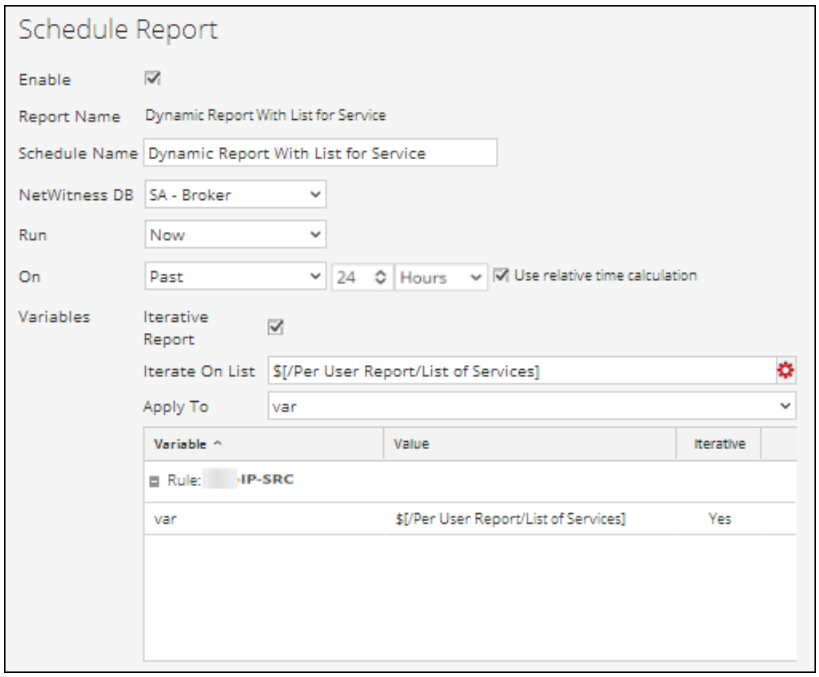
Features

The Schedule Report view consists of the following panels:

1	Schedule Report View
2	Output Actions Panel
3	Dynamic List Panel
4	Logo Panel

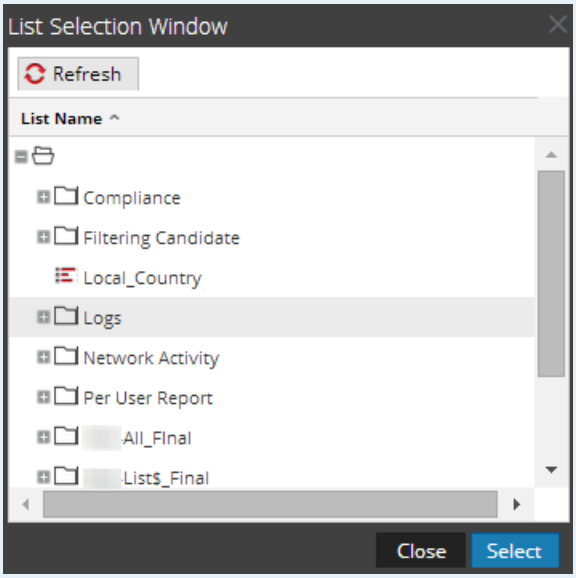
Schedule Report View

The Schedule Report view allows you to schedule reports.



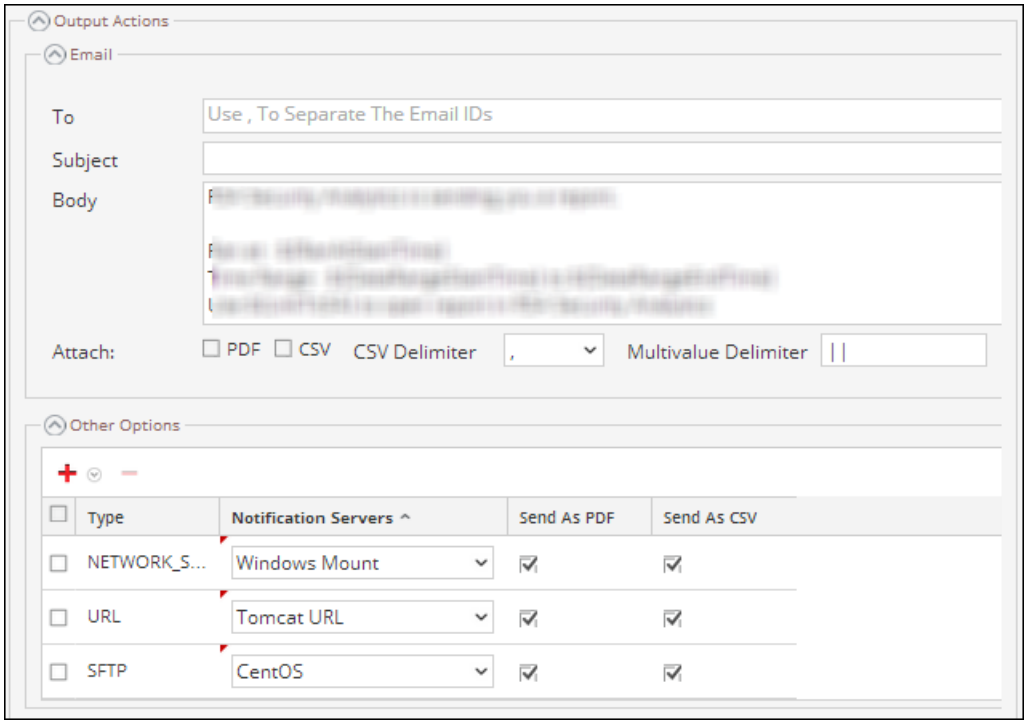
The following table lists the fields in the Schedule Report panel.

Field	Description
Enable	Enables the report schedules and runs the report.
Report Name	The name of the report.
Schedule Name	The name of the scheduled report configuration.
NetWitness DB	The database can be NWDB and Warehouse DB depending on the type of database that you selected in the rule definition. If the report has rules of NWDB and Warehouse DB types, all the database types or rule types are displayed.
Warehouse Resource Pool	If the report has rules of Warehouse DB, the Warehouse Resource Pool drop-down is displayed to select the pools or queues available in the cluster. If no pools or queues are entered for the Reporting engine, this field is disabled. For more information, see "Step 5: Configure Task Scheduler for a Reporting Engine" topic in the *Host and Services Configuration Guide*.
Run	Provides the type of schedule for the run configuration: • Ad-hoc execution • Hourly execution • Daily execution • Weekly execution • Monthly execution
On	The data range on which the query is run.

Field	Description
Use relative time calculation	Uses the relative time duration to schedule a report.
Iterative Report	Select the checkbox to schedule a report for the selected list value.
Iterate on List	Click this button to navigate to the List Selection panel and select a list. The following figure displays this panel:  The List Selection panel is a collection of Lists. The Reporting Engine maintains an active list of the available list names by continuously synchronizing with the collection to which it is connected.
Apply To	Apply list values on the selected variable.
Variables	Displays the rule variables along with their associated values and the iterative properties included in the report. **Note:** Depending on the rule chosen while creating a report, you can view dynamic variables defined for the rule in the **Variables** field of the Schedule Report panel. For example, Test-Country is the rule having the dynamic variable var.
Schedule	Schedules the report.
Reset	Resets the scheduled report.
Configure	Allows you to alter the Reporting Engine configuration details on the "Reporting Engine General Tab" topic in the *Host and Services Configuration Guide*. **Note:** This button is visible on the Schedule Report panel only when you have the 'Manage Device' access permissions on the Reporting module.

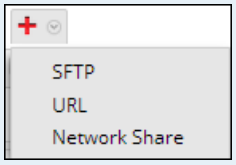
Output Actions Panel

The Output Actions panel specifies output actions to notify the email recipient when the report execution completes and also sends reports in PDF and CSV formats as attachments in the email, based on your selection.



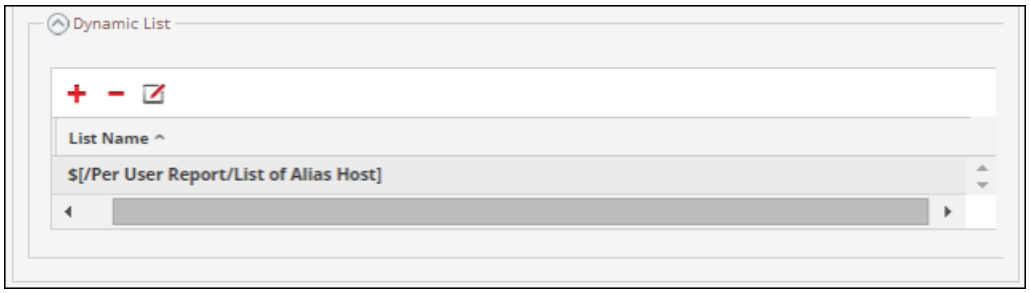
The following table lists the fields in the Output Actions panel.

Field	Description
To	A comma-separated list of email addresses to receive the output.
Subject	The subject entered in the mail.
Body	The body of the email. By default, the body field is populated with pre-defined text that has certain variables that will add meta appropriate to the generated report. In the Reporting Engine, these variables are replaced with actual values. • `${RanAtStartTime}` : The Start time of the report. • `${DataRangeStartTime}` : The Start time of the data time range. • `${DataRangeEndTime}` : The End time of the data time range. • `${LinkToSA}` : The link to the NetWitnessHost from the email which in turn opens the report in NetWitness interface. • `${ReportName}` : The name of the report. • `${DataSource}` : The name of the data source.

Field	Description
Attach:	The output format in which the report is attached to the email, such as PDF or CSV as configured in the Schedule Report dialog.
CSV Delimiter	The default CSV delimiter is comma (,). If the CSV content contains a comma, you must identify a unique separator so the content is stored in its original form. For example, if msg is a column in the report to be saved as CSV and the msg content is as follows: `ASA-SSM-CSC-20 Module in slot 1," application reloading ""CSC SSM""," version ""6.2.1599.0"" CSC SSM scan services are reloading because of a pattern file or configuration update` The above content will be included in three columns due to the commas (,). To avoid this, you must specify a different delimiter such as a pipe line character "|". **Note:** To import the CSV file into Microsoft Excel, use the Data > From Text option in the Excel application. When you import the CSV file you must specify the file type of the file being imported as Delimited and use the same delimiter that you specify to generate the CSV file.
Multivalue Delimiter	The data in multivalued fields are separated by the multivalue delimiter. The default Multivalue delimiter is two pipe line characters (||).
Other Options	You can select an SFTP, URL, or Network Share location configured in ((RE}} and then send the report either in PDF or CSV format based on the requirement.
	Select this option to send the report to the SFTP, URL or Network Share location configured in the Reporting Engine Services Config view.
Type	The type of output action chosen. For example, SFTP, URL or Network Share.
Output Actions	Select the SFTP, URL or Network Share name configured in the Reporting Engine Services Config view.
Send as PDF / Send as CSV	Select these options to send the report either in PDF or CSV format, or both to the configured Notification Server (SFTP, URL or Network Share).

Dynamic List Panel

The Dynamic List panel populates the lists created and you can add, edit or delete the list. The list is generated based on the scheduled report which can be viewed in the Lists view.



The following table lists the operations in the Generate List panel.

Operation	Description
	Adds a new list to the report.
	Deletes all the lists added to the report.
	Displays the Generate List dialog.
List Name	The name of the list chosen from the List Selection panel. For more information on the List Selection panel topic, see Generate List Panel.

Logo Panel

The Logo panel populates the default logo from the Select a Logo panel. For more information on choosing a logo from this panel, see "Manage and Select a Report Logo" section in the Manage Lists, Rules or Reports.

You can set the default logo for a Reporting Engine. This is the logo that is used in the generated reports. For more information on choosing a logo, see Select a Logo Dialog.

Note: If you have not selected any logo then the default RSA logo is used on the report. The option **Save as PDF** for the previously executed reports does not support a new customer logo. It displays the default RSA Logo, if the customer logo must be displayed in the Schedule a Report view.

Scheduled Reports View

The Scheduled Reports view allows you to create, view and manage scheduled reports.

Workflow

This workflow shows the procedure to create and schedule a report.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Configure the Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report*	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports*	Manage Lists, Rules or Reports

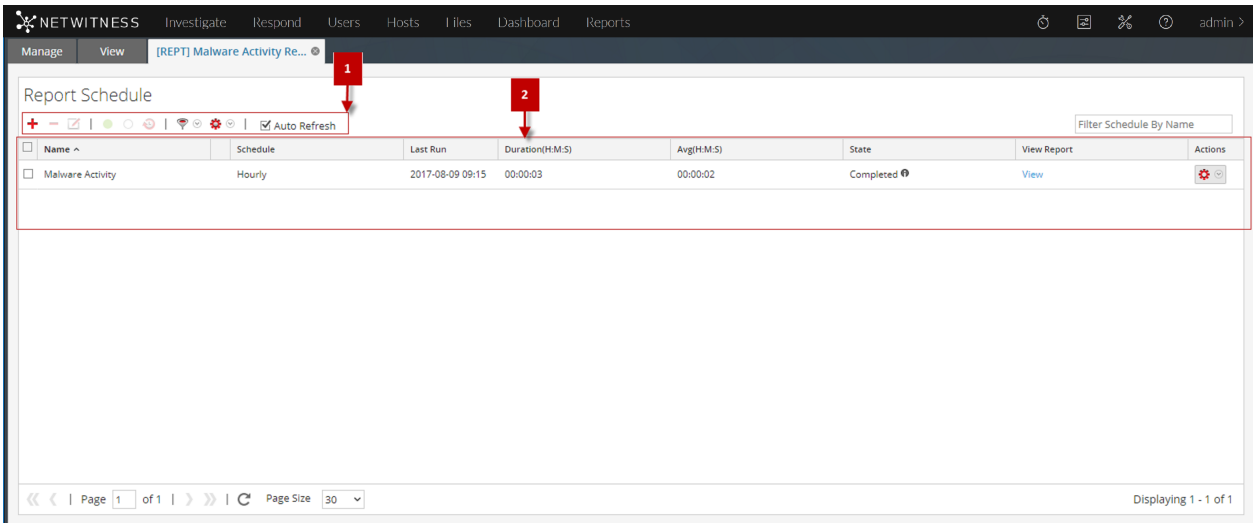
*You can complete these tasks here.

Related Topics

- Build Report View
- Report View

- Schedule Report Panel
- Reports Permissions Dialog

Quick View



To access this view:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, do one of the following:

   - Click  > **View Scheduled Reports**.
   - Click the **Schedules** column.

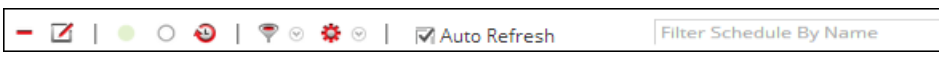
Features

The View Scheduled Reports has the following features:

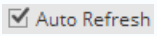
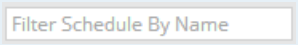
1	Report Schedule Toolbar
2	Report Schedule List panel

Report Schedule Toolbar

The Scheduled Reports has options to add, modify and delete the scheduled report as well as options to enable or disable the selected run configuration.



The following table lists the operations in the Scheduled Reports toolbar.

Operation	Description
	Create a new report schedule.
	Delete the selected report schedule.
	Edit the selected report schedule. **Note:** Double-click on a desired report schedule to edit it.
	Enables the selected report schedule.
	Disables the selected report schedule.
	View the history of the scheduled report.
	Filter schedules based on the type of schedule. (For example, AdHoc)
	Allows you to set permissions for the selected scheduled report.
	Automatically refreshes the scheduled reports list.
	Searches schedules based on the schedule name.

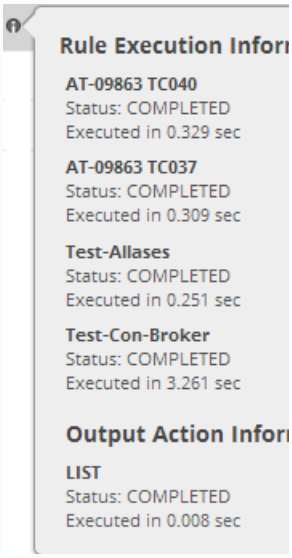
Report Schedule List Panel

The Scheduled Reports List panel lists the scheduled reports in a tabular format.

The following table lists the columns in the Scheduled Reports List panel:

Column	Description
Name	The name of the scheduled report.
Schedule	The type of schedule for the run configuration: • Ad-hoc execution • Hourly execution • Daily execution • Weekly execution • Monthly execution
Last Run	Displays the last time the report was run.
Duration(H:M:S)	Displays the time taken for last execution of the report.

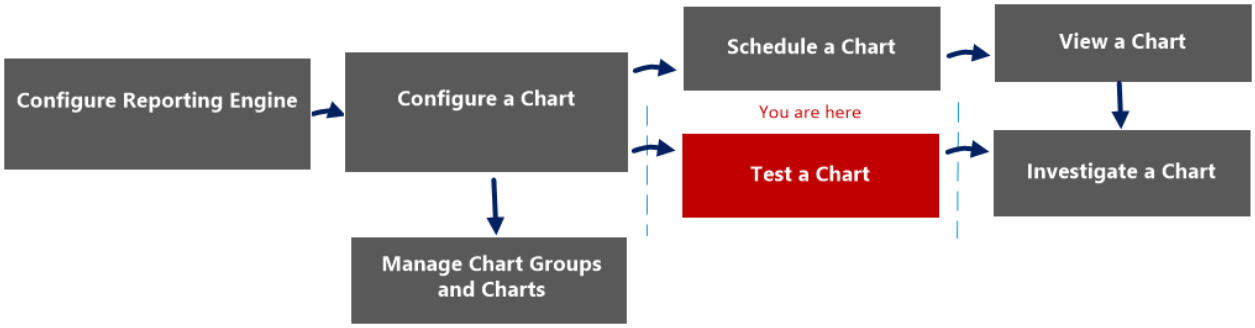
Column	Description
Avg (H:M:S)	Displays the average time taken to run the report.
State	Indicates the state of the scheduled report. • Scheduled: If a report is scheduled to run on an hourly, daily, weekly, monthly, or later time, the state of the report is displayed as scheduled, for the first run. • Queued: If a report is still waiting to get executed, the state of the report is displayed as queued. • Running: If the report schedule is in progress, the state of the report is displayed as running. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule schedule executions failed, the state of the report is displayed as failed. • Completed: If a report schedule is successfully executed, the state of the report is displayed as completed. • Canceled: When cancel request is completed, the state of the report is displayed as canceled. • Inactive: If a report schedule is disabled, the state of the report is displayed as Inactive. • Not available: If the report schedule executed information is not available, the state of the report is displayed as not available.

Column	Description
	Click to view the rule execution information and output action information. This pop-up notifies the status of multiple rules in a report and the time taken for its execution. **Note:** You can view the rule execution and output action information for a scheduled report having the state **Completed**, **Running**, **Partial** or **Failed**. By default, the Output Actions for Completed Report on Reporting Engine Config page is set to enable, to receive an email when the report status is completed. To receive an email for **Failed** or **Partial** reports, you must disable this option.
View Report	Click to view the rule execution information on the View a Report Panel. You can view the rule execution information for a scheduled report having the state 'running' as well.

Test a Chart View

In the Test a Chart view, you can view and test the charts.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart	View a Chart
Administrator/ Analyst	Test a chart*	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

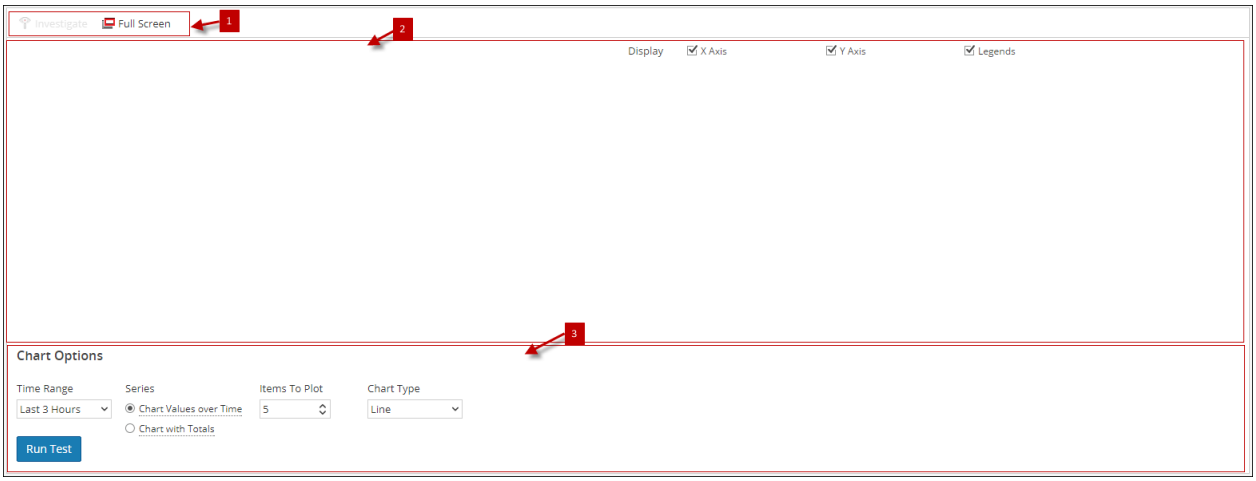
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The Test a Chart view consists of the following panels:

1 Chart toolbar
2 Chart Output panel
3 Chart Options panel

Chart Toolbar

The Charts toolbar allows you to investigate on a particular chart and change the screen to full screen.

Feature	Description
Investigate	Investigates further on the selected chart.
Full Screen	Displays the chart in full screen.

Chart Output Panel

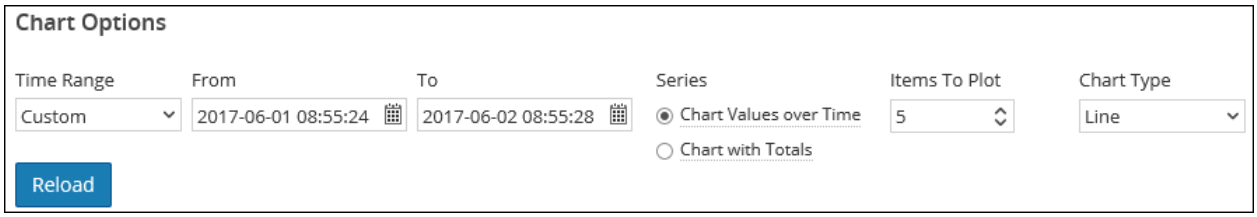
The Chart Output panel displays the information in a chart format for the selected time chart options.

The following table lists the features in the Test a Chart View and their descriptions.

Feature	Description
Display	Allows you select the values that needs to be displayed and have the following options: X Axis, Y Axis and Legends.
X Axis	Displays the session count.
Y Axis	Displays the actual output.
Legends	Displays the list of variables appearing in the chart.

Chart Options Panel

The following figure shows the Chart Options panel, which displays the time range, series, and chart type fields to configure the chart display.



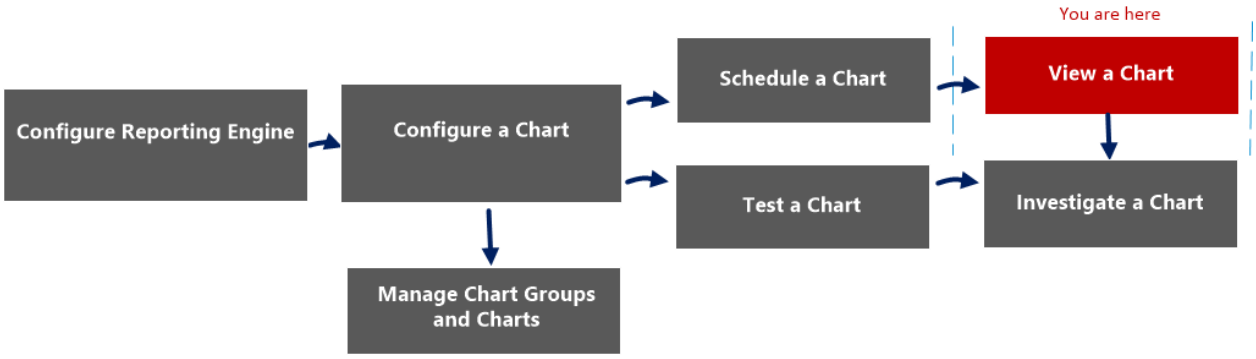
The following table lists the fields in the Charts Options panel and the descriptions.

Feature	Description
Time Range	The default time range is Last 3 Hours. However, you can select a different value from the drop-down list, for example, Last Hour, or Last 6 Hours which are the preset values. Or you can customize by selecting Last N Days or the Custom option.
From	The start date and time. (only for custom options).
To	The end date and time. (only for custom options).
Series	The series field provides you with two options: • Chart Values over Time: Renders the chart for the entire time range selected. • Chart with Totals: Renders the summary of data for the selected date range.
Items to Plot	The maximum number of events the user wants to view on the chart.
Chart Type	The type of chart to be rendered either area, bar, column, line, step line, step area, spline area or spline.

View a Chart Panel

In the View a Chart panel, you can view and manage charts. There are options for filtering and sorting the information in the chart, as well as options for the type of chart, the number of items to chart, and charting values or totals. When viewing a chart, you can open the charted sessions in the Investigation module and save the chart as a PDF.

Workflow



What do you want to do?

Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart*	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

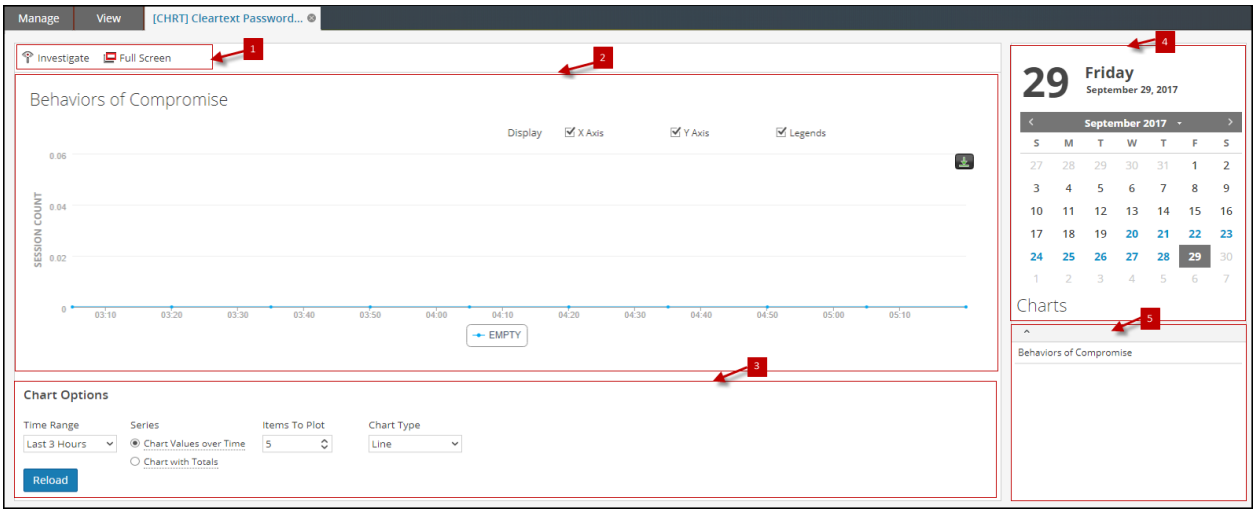
*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View

The following figure is an example with the important features labeled.



The View a Chart panel includes the following panels:

1. Chart toolbar
2. Chart Output panel
3. Chart Calendar panel
4. Chart Options panel
5. Chart Executed list

Chart Toolbar

The Chart toolbar has options that allow you to investigate, and view the chart on another screen.

The following table lists the options in the Chart toolbar.

Operation	Description
Investigate	Investigates the chart details.
Full Screen	Displays the chart on a full screen.

Chart Output Panel

The Chart Output panel displays the chart with sortBy on the Y-axis, time on the X-axis and legends.

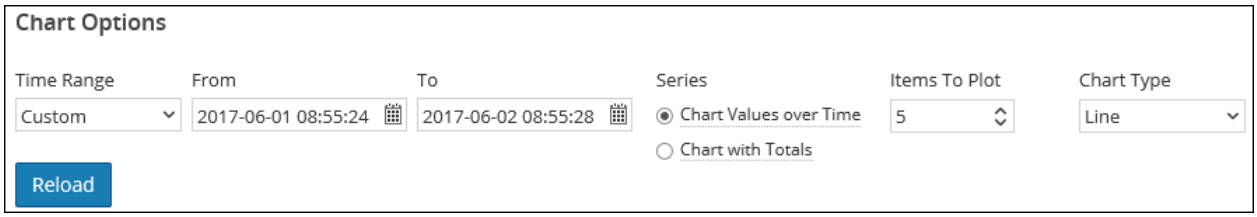
Note: You can save the chart as PDF using the icon on the Chart Output panel.

Chart Calendar Panel

The Chart Calendar panel is the default calendar with which you can filter the list of charts depending on the date you select from the Calendar, as shown in the following figure.

Chart Options Panel

The Chart Options panel displays the time range, series, and chart type fields to configure the chart is displayed.



The following table lists the fields in the Chart Options panel.

Field	Description
Time Range	The default time range is Last 3 Hours. However, you can select a different value from the drop-down list, for example, Last Hour, or Last 6 Hours which are the preset values. Or you can customize by selecting Last N Days or the Custom option. **Note:** The time range selected by you for a chart will be saved. When you open the same chart the next time, the time range that is saved will be displayed. This behavior is not applicable for the custom option.
From	The start date and time. (only for custom options)
To	The end date and time. (only for custom options)
Series	The series field provides the user with two options: • Chart Values over Time: Renders the chart for the entire time range selected. • Chart with Totals: Renders the summary of data for the selected date range.

Field	Description
Items to Plot	The maximum number of events the user wants to view on the chart.
Chart Type	The type of chart to be rendered. Either area, bar, column, line, step line, step area, spline area or spline.

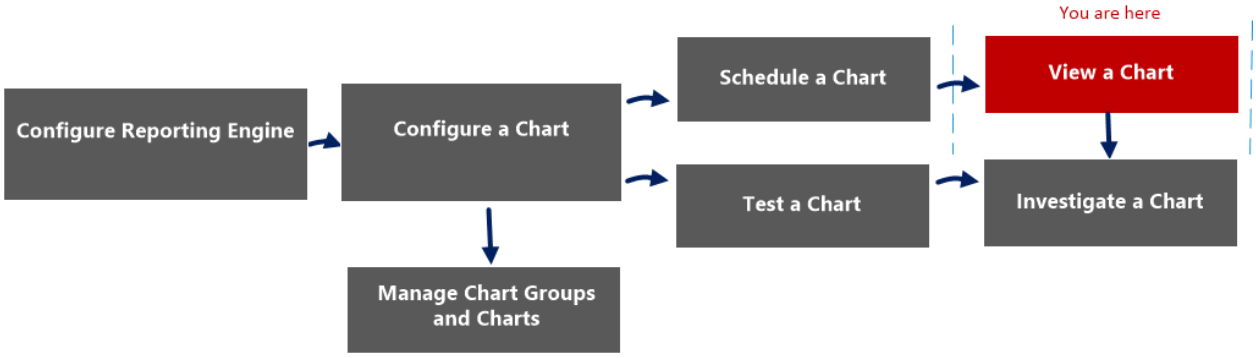
Chart Executed List Panel

The Chart Executed List panel displays all the executions for a particular chart for the selected date. Double-clicking on any chart execution loads the chart on the Chart Output panel. By default, the last executed chart is displayed in the Chart Output panel.

View All Charts View

In the View All Charts view, you can display, print, save and email charts.

Workflow



What do you want to do?

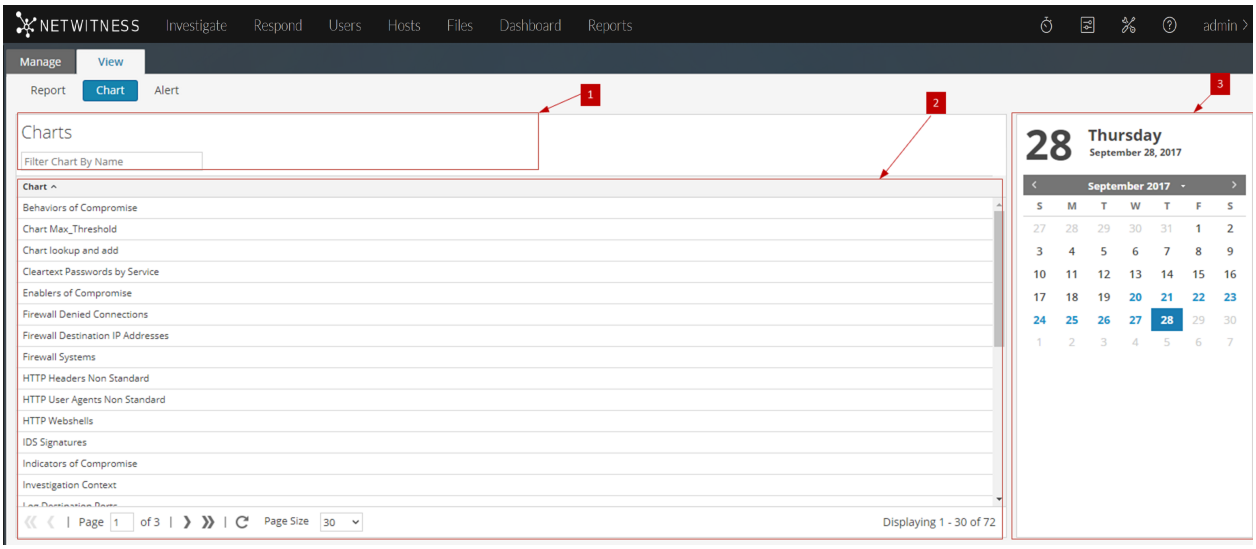
Role	I want to ...	Documentation
Administrator/ Analyst	Configure Reporting Engine	For more information, see "Configure Reporting Engine" in the *Reporting Engine Configuration Guide*.
Administrator/ Analyst	Configure a chart	Configure a Chart
Administrator/ Analyst	Schedule a chart	Schedule a Chart
Administrator/ Analyst	View a chart*	View a Chart
Administrator/ Analyst	Test a chart	Test a Chart
Administrator/ Analyst	Investigate a chart	Investigate a Chart
Administrator/ Analyst	Manage a chart group and chart	Manage a Chart Group and Chart

*You can complete these tasks here.

Related Topics

- Configure and Generate a Chart

Quick View



The View All Charts panel includes the following panels.

1 Charts Toolbar
2 Charts Output panel
3 Charts Calendar panel

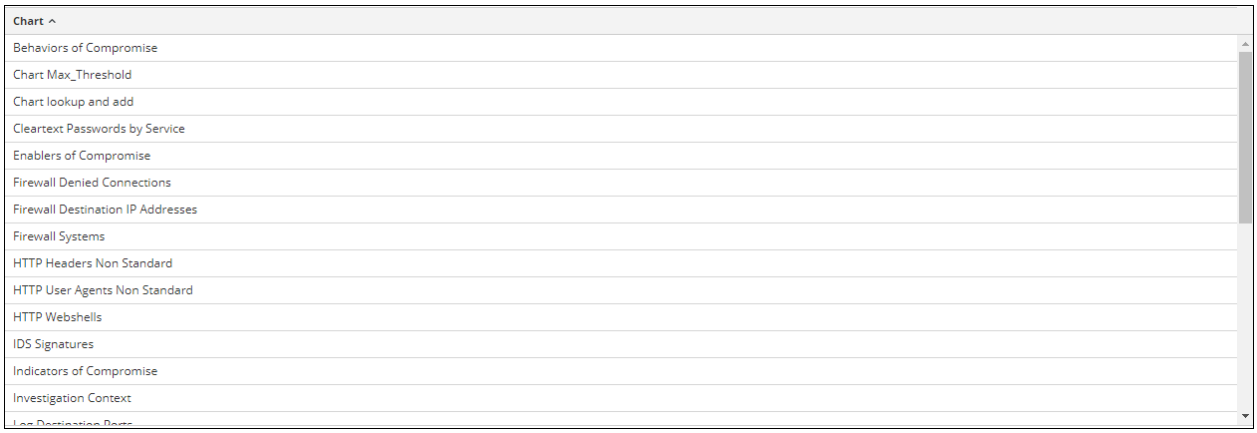
Charts Toolbar

The following table lists the options in the View All Charts toolbar:

Operation	Description
Filter Chart By Name	Searches schedules based on the chart name for a selected calendar day.

Charts Output Panel

The Charts Output panel displays the chart with the chart schedule name.



Feature	Description
Chart	This field displays all the successfully executed charts.

Charts Calendar Panel

The Charts Calendar panel is used to select a date from the Calendar. Based on the date you select, the list of successfully run charts for the date is displayed.


28
Thursday
September 28, 2017
September 2017
S M T W T F S
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7

View a Report Panel

The View a Report panel is used to review the reports.

Workflow

This workflow shows the procedure view a report or list of all reports.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

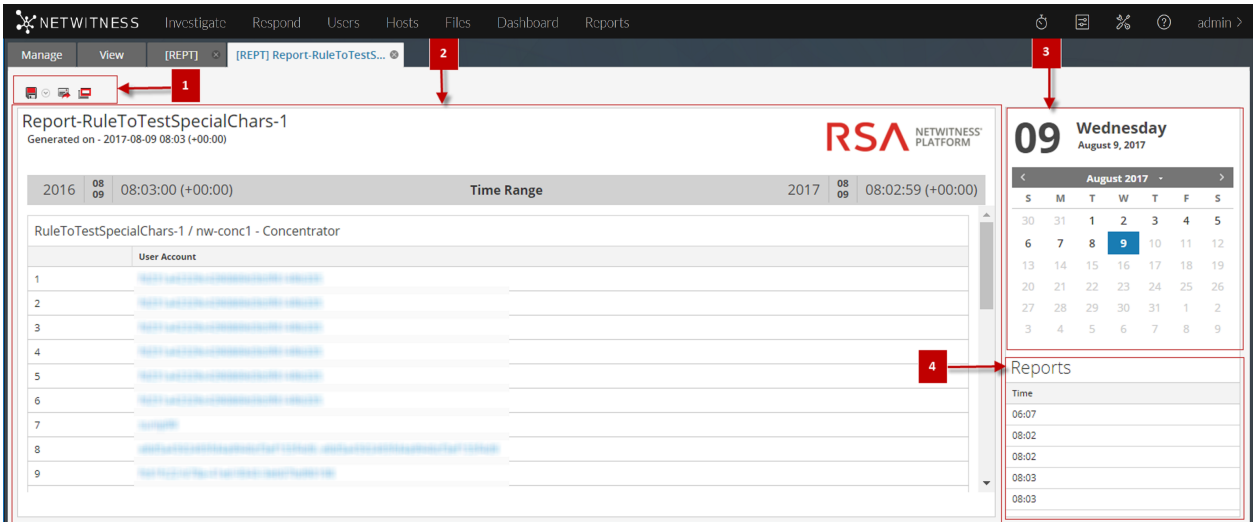
*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Build Report View

- Import Report Dialog
- Scheduled Reports View
- Reports Permissions Dialog
- View All Reports View
- Report View

Quick View



To access this view:

1. Go to **Reports**.

   The Manage tab is displayed.

2. Click **Reports**.

   The Report view is displayed.

3. In the **Reports** panel, do one of the following:

   - Click  >**View Scheduled Reports**.
   - Click the **#Schedules** column.

     The Report Schedule view is displayed.

4. Click **View**.

Features

The View a Report panel has the following sections.

1	Reports Toolbar
2	Reports Output panel
3	Reports Calendar panel
4	Reports Time panel

Reports Toolbar

The Reports toolbar allows you to print, save, email, and view reports on full screen.

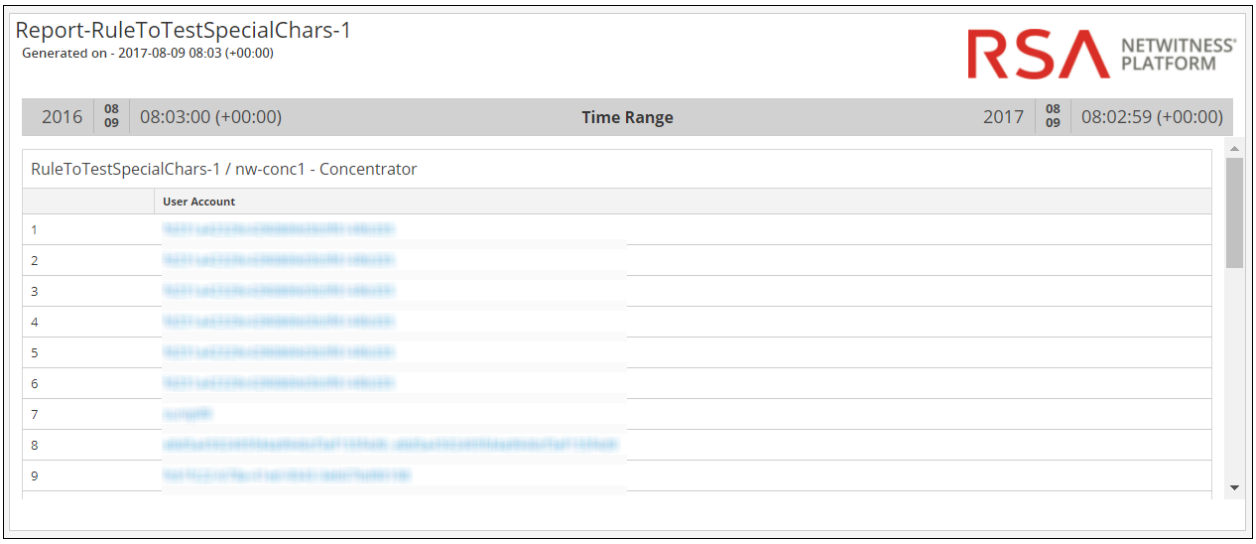
Note: The Reporting Engine is responsible for generating PDF and CSV output of the reports based on the report definition. The size of the PDF files for a report must not exceed 50,000 cells.

The following table lists the options in the Reports toolbar.

Operation	Description
	Prints the generated report.
	Saves the report as a PDF and a CSV file. **Note:** The **Save As PDF** option is not available for a large report. If you are generating a PDF for a report and it takes a longer time than expected, you get a warning message stating **PDF generation is in progress, please try after some time**. When you click download as a CSV file, the Select Rule to download dialog is displayed. You must select a rule from this dialog to download the rule result in a CSV file. If the file generation takes a while, you can click on the **Notify me** option to be notified once the PDF or CSV is generated. Once the PDF or CSV is generated, you can view the Notifications for the status.
	Emails the report with the PDF or CSV attachment.
	Opens the generated report on a new window.

Reports Output View

The Reports Output panel view the report with the report schedule name, report generated time and the actual report with the selected rule variables.



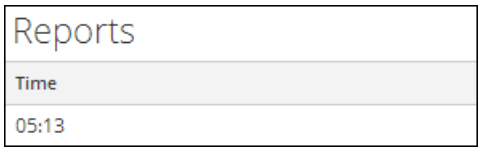
Feature	Description
Name	This field displays the name of the scheduled report.
Time	This field displays the time when the report is generated.
Report	This field displays the details report with the selected rule variables.

Reports Calendar View

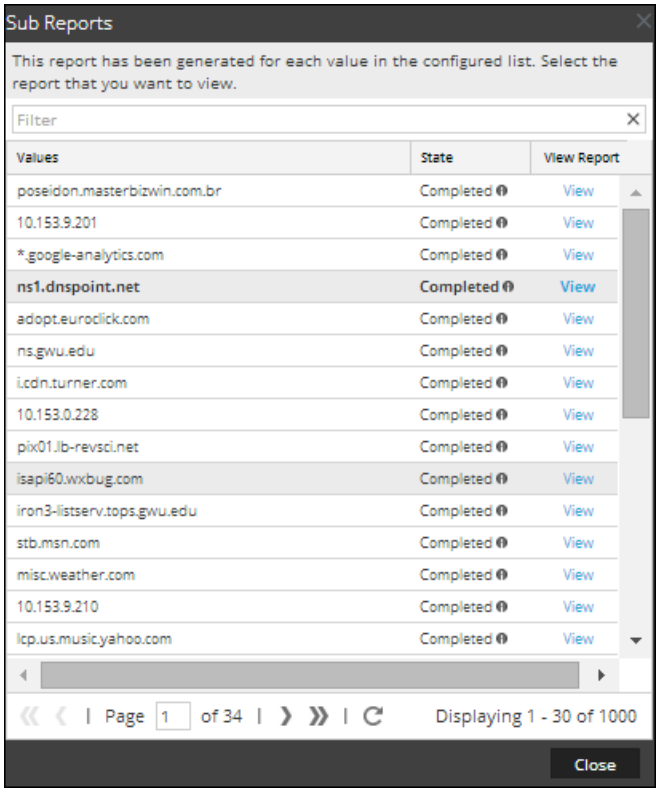
The Reports Calendar view is used to select a date from the Calendar. Based on the date you select, the list of successfully run reports for the date is displayed.

Reports Time View

The Reports Time view displays the time when the report was actually run.



When you click **View** on the scheduled report having **Iterative** selected, the **Sub Reports** panel is displayed. For each value in the configured list a report is generated.



The following table lists the columns in the Sub Reports panel.

Column	Description
Values	The List values chosen for a dynamic variable from the List Selection panel.
State	Indicates the state of the scheduled report for each of the list values. • Partial: If in a report with several rules, a single rule execution failed or an output action failed or creation of PDF/CSV failed, the state of the report is displayed as partial. For example, consider a report with five rules and four rules are executed successfully and one fails, then the state is displayed as Partial. • Failed: If in a report with several rules, all the rule executions failed, the state of the report is displayed as failed. • Completed: If a report is successfully executed, the state of the report is displayed as completed.

Column	Description
View	Clicking on any of the report schedules or sub reports listed and then **View** displays the desired report. **Note:** You can view the completed rules on the **View a Report** page even when the report is 'running'.

View All Reports View

In the View All Reports view, you can display, print, save and email reports.

Workflow

This workflow shows the procedure view a report or list of all reports.

What do you want to do?

Role	I want to ...	Show me how
Administrator / Analyst	Configure Reporting Engine	For more information, see "Step 3: Configure Reporting Engine Data Sources" topic in the *Reporting Engine Configuration Guide*
Administrator / Analyst	Create a List or List Group/Create or Deploy a Rule/Test a Rule	Configure a Rule
Administrator / Analyst	Create and Schedule a Report	Create and Schedule a Report
Administrator / Analyst	View a report or list of all reports*	View a Report
Administrator / Analyst	Investigate a Report	Investigate a Report
Administrator / Analyst	Manage/Access Control for lists, Rules or Reports	Manage Lists, Rules or Reports

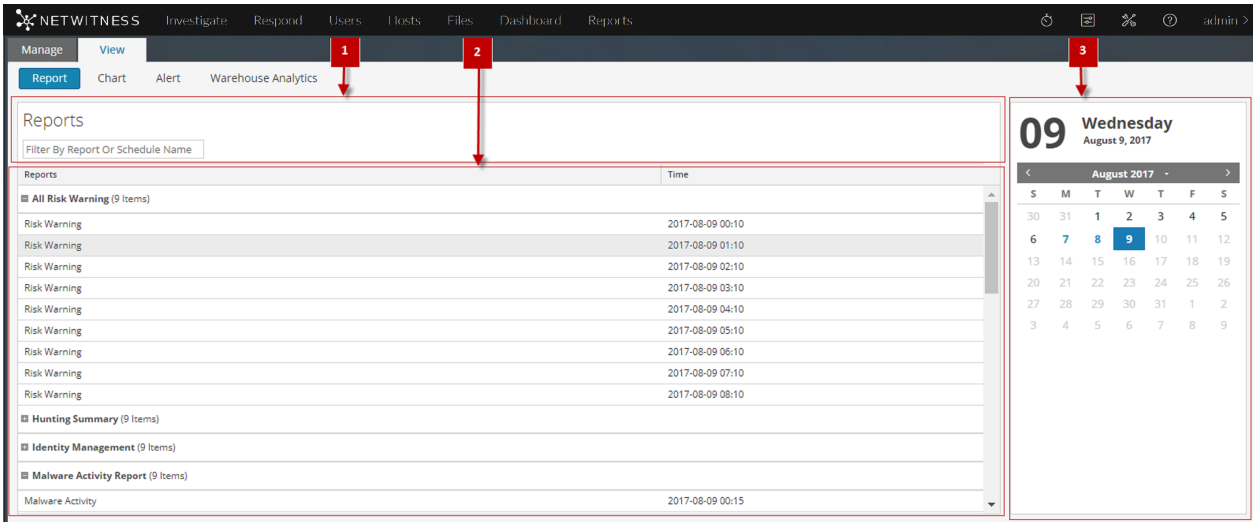
*You can complete these tasks here.

Related Topics

- Configure and Generate a Report
- Build Report View

- Import Report Dialog
- Scheduled Reports View
- Reports Permissions Dialog
- View a Report Panel
- Report View

Quick View



To access this view:

1. Go to **Reports**.
   The Manage tab is displayed.
2. Click **Reports**.
   The Report view is displayed.
3. In the **Reports** panel, click **View All Reports**.
   The Reports panel is displayed, clicking on any of the reports listed allows you to view the report.

Features

The View All Reports panel has the following features.

1	Reports Toolbar
2	Reports Output panel
3	Reports Calendar panel

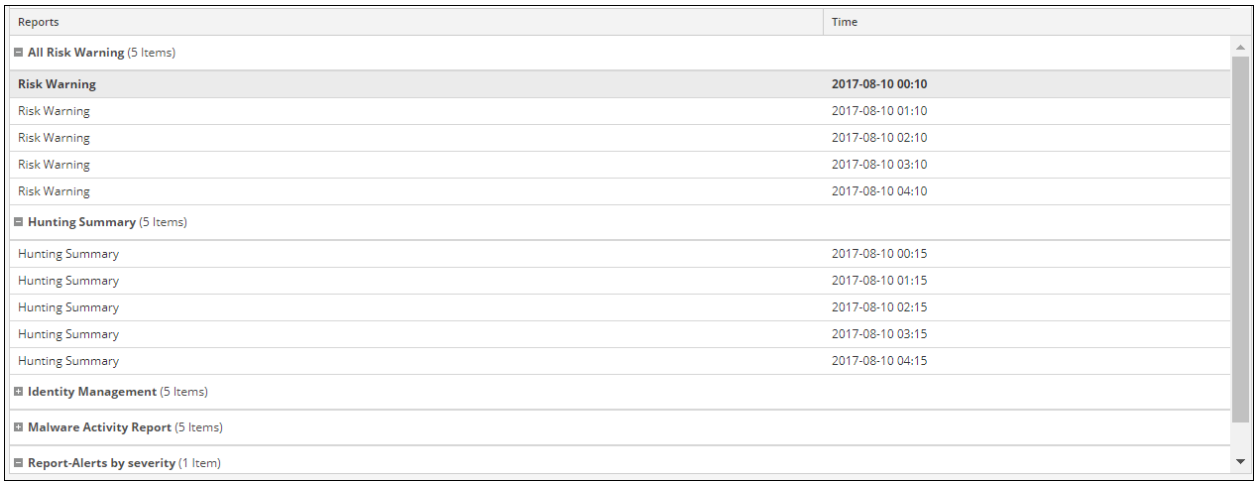
Reports Toolbar

The following table lists the options in the View All Reports toolbar:

Operation	Description
Filter By Report Or Schedule Name	Searches schedules based on the report name or schedule name for a selected calendar day.

Reports Output Panel

The Reports Output panel displays the report with the report schedule name and report generated time.



Feature	Description
Reports	This field displays the detailed report with the selected rule variables.
Time	This field displays the time when the report is generated.

Reports Calendar View

The Reports Calendar view is used to select a date from the Calendar. Based on the date you select, the list of successfully run reports for the date is displayed.


10
Thursday
August 10, 2017
August 2017
S M T W T F S
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9

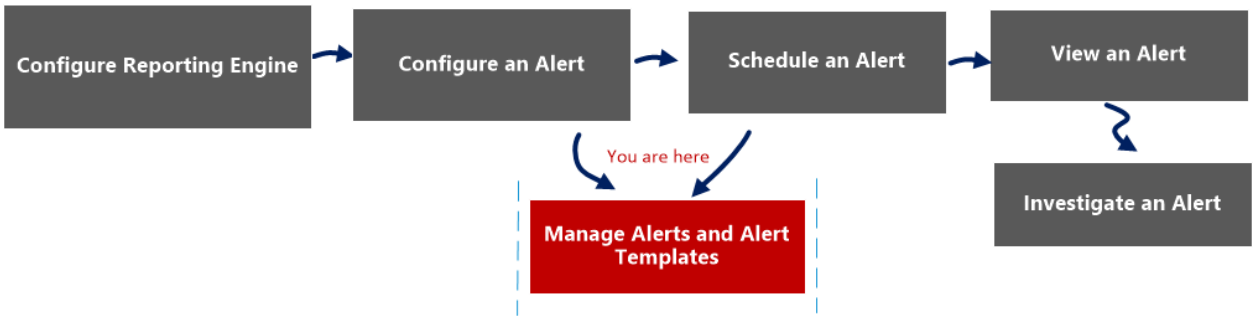
Alerting References

The Reporting module user interface provides access to NetWitness alerts. This topic contains descriptions of the user interface as well as other reference information to help users manage Alerts.

Alert List View

The Alert List view allows you to import, export, manage, and add alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

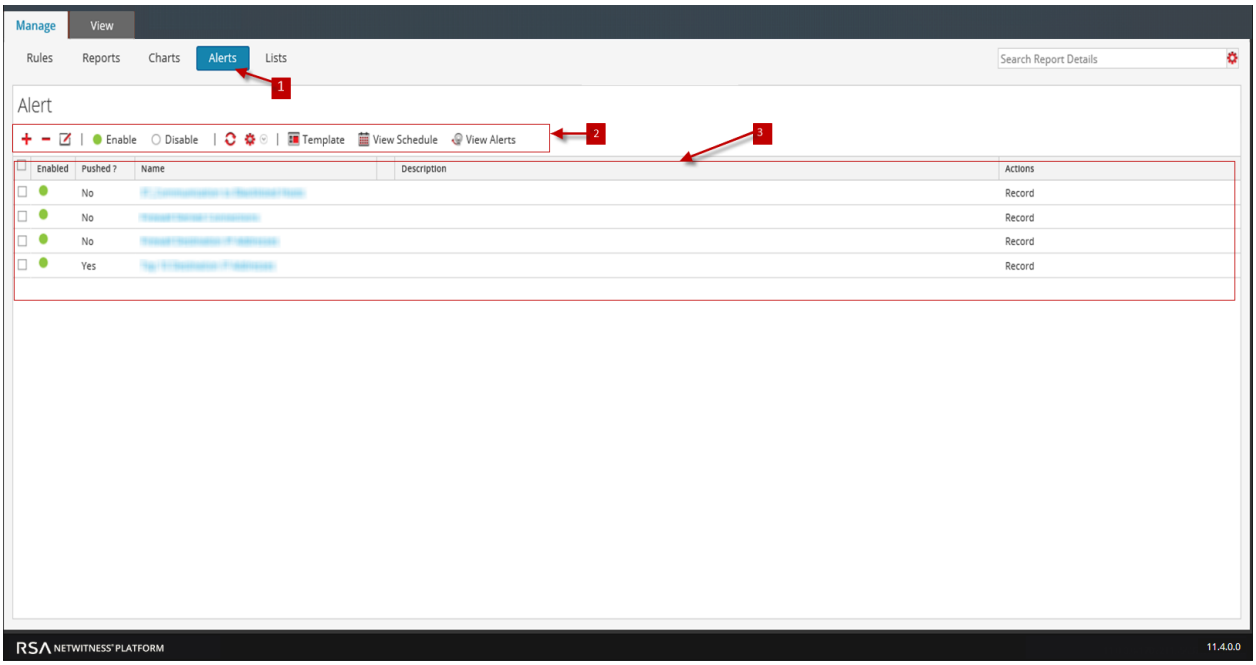
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



1 Click **Alerts** to open the Alert view.

2 The Alert toolbar allows you to add, modify, delete, enable, disable, refresh, import, and export an alert. Using this toolbar, you can also set access permissions for the selected alert.

3 The Alert panel lists all the alerts in a tabular format.

The Alerts List view has the following panels:

- Alert Toolbar
- Alert

Alert Toolbar

The Alert toolbar panel has the following features:

Feature	Description
+	Adds a new alert to the Reporting module.
−	Deletes one or more selected alerts.
	Edits an alert.
Enable	Enables the selected alerts.
Disable	Disables the selected alerts.
	Refreshes the view.
	Enables the following options: Import, Export and Permissions.

Alert

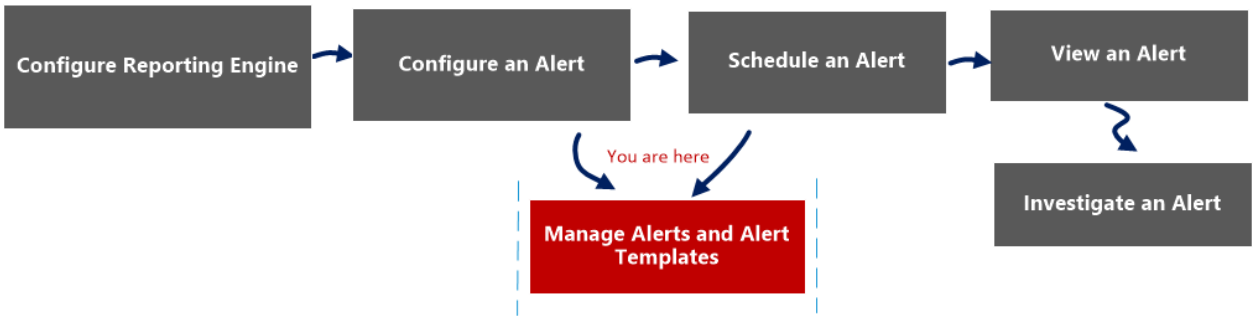
The Alert panel lists all the alerts in a tabular format. The following table lists the columns in the Alert panel and their descriptions.

Feature	Description
Enabled	Displays the state of the alert: • Enabled - the alert is active and fires based on the rule assigned to it. • Disabled - the alert is not active.
Pushed?	Indicates whether the alert is sent to Decoders or Log Decoders: • Yes - Alert is pushed to Decoders or Log Decoders. • No - Alert is not pushed to Decoders or Log Decoders.
Name	Identifies the name of the alert. Clicking the alert name displays the rule on which this alert is based in the Define Rules panel.
Description	Indicates the alert description.
Actions	Indicates the action the system takes when the alert fires. The different available action types are as follows: • Record • SMTP • SNMP • Syslog

Alert Permissions Dialog

In the Alert Permissions dialog, the users with 'Read & Write' access permission can set access permissions for an alert to configure permissions in the Alert Permissions dialog.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

*You can complete these tasks here.

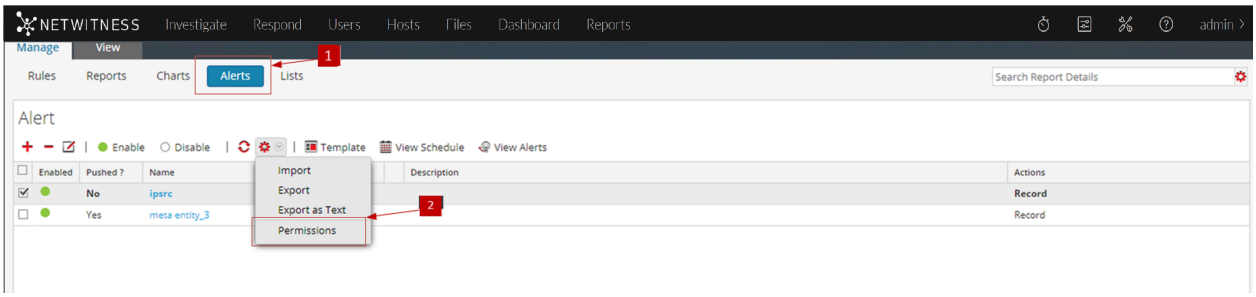
Related Topics

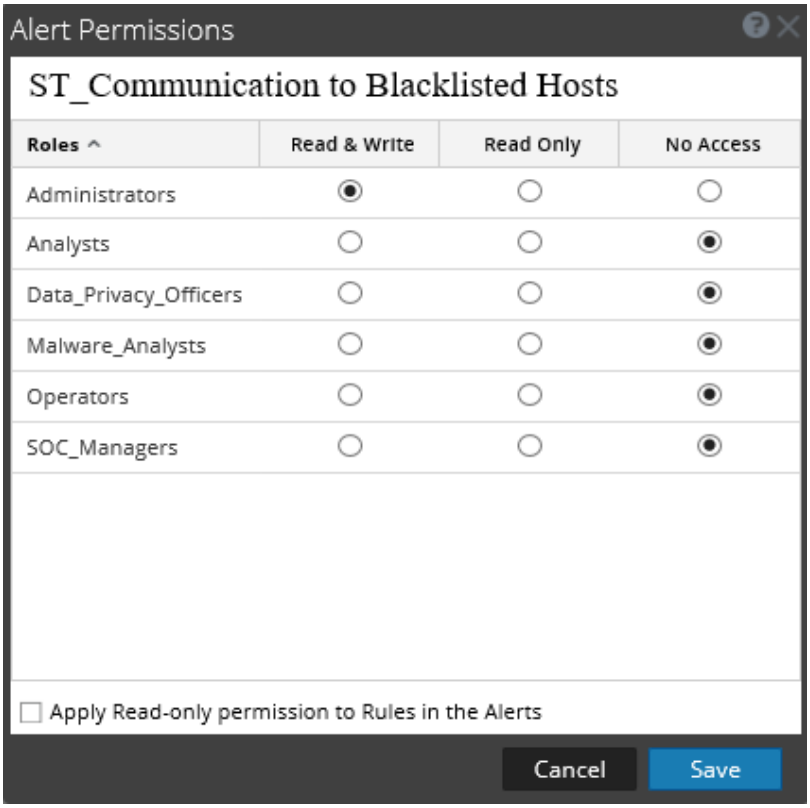
Alerting Overview

Quick View

The Alert permissions dialog allows you to set alert permissions depending on the user role.

The following figure is an example with the important features labeled.





1. Click **Alerts** to open the Alert view.
2. Click ⚙ > **Permissions**. The Alert Permissions dialog box is displayed.
3. Based on the user role, select the appropriate options.
4. (Optional) Select the checkbox if you want to automatically provide read access permission to dependent rules.
5. Click **Save**.

Note: If a User (other than a super user) creates an alert, super users will not be able to access the alert.

The following table lists the columns in the Alert Permissions dialog.

Column	Description
Roles	Displays all the user roles in the NetWitness user interface.

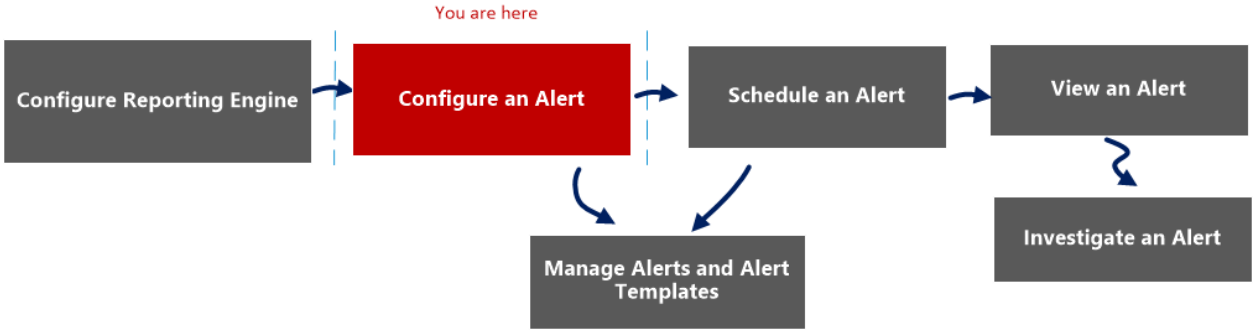
Read & Write	Allows you to apply 'Read&Write' access to the alert.
Read Only	Allows you to apply only 'Read' access to the alert.
No Access	By selecting this permission, you cannot access or view the alert.
Apply Read-only permission to Rules in the Alerts	Allows you to automatically apply permissions to the rules in the alerts.
Cancel	Cancels all the changes made to the permissions.
Save	Saves the selection and provides access to the role based on the selection.

Alert Schedules View

In the Alert Schedules view, you can view all the alerts scheduled. Alternately, you can also disable the scheduled alerts.

Workflow

The following workflow shows the tasks involved in creating or modifying an alert.



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert*	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

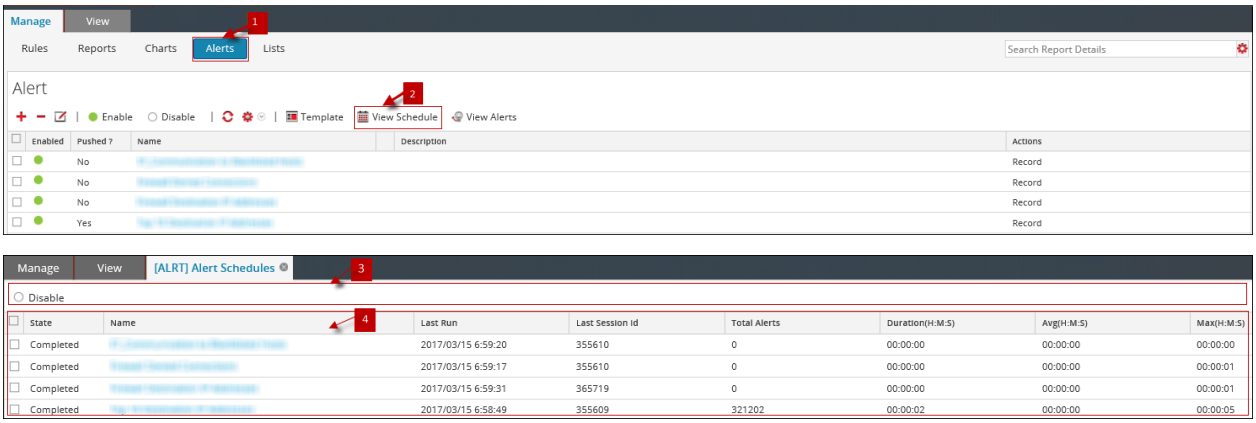
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following example shows you how to access the Alert Schedules view dialog.



1 Click **Alerts** to open the Alert view.
2 Click **View Schedule** to open the View Alerts Schedule view.
3 The Alerts Schedule toolbar allows you to modify the state of the scheduled alert.
4 The Alerts Schedule List panel lists only the Enabled alerts in a tabular format.

Features

The different panels on the Alert Schedules View dialog are:

- Alerts schedule toolbar panel
- Alerts schedule list panel

Alerts Schedule Toolbar Panel

In the Alerts Schedule Toolbar panel, the Disable icon disables the selected alert. When schedule alerts are no longer needed or are determined to be ineffective, you can disable them so that they are no longer executed. You can select one of more alerts to disable. When an alert is disabled, it is removed from the scheduled alerts list so that you cannot view it here, and it will not execute again unless you manually execute the alert or set up a new schedule for it.

Alerts Schedule List Panel

The following table lists the columns in the Alerts Schedule List panel and their description.

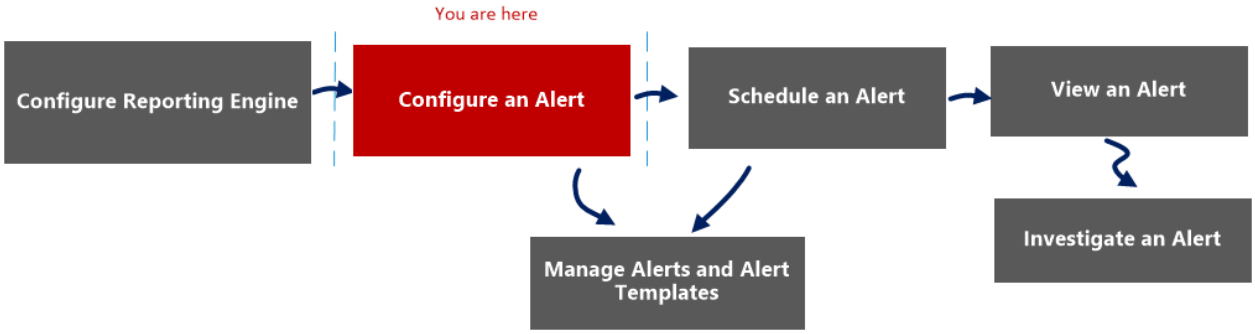
Column	Description
State	The state of the scheduled alert: • Completed • Failed
Name	The name of the scheduled alert.
Last Run {#time}	The last time the scheduled alert was run.
Last Session Id	The Session Id of the last scheduled alert.
Total Alerts	The total number of event occurrences.
Duration	The time taken to run the scheduled alert.

Column	Description
Avg (s)	The average time taken to run the scheduled alert.
Max (s)	The maximum time taken to run the scheduled alert.

Create or Modify Alert Panel

The Create or Modify alert panel is a panel in the Alert List view. This panel allows you to create or modify an alert as per the requirement.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert*	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

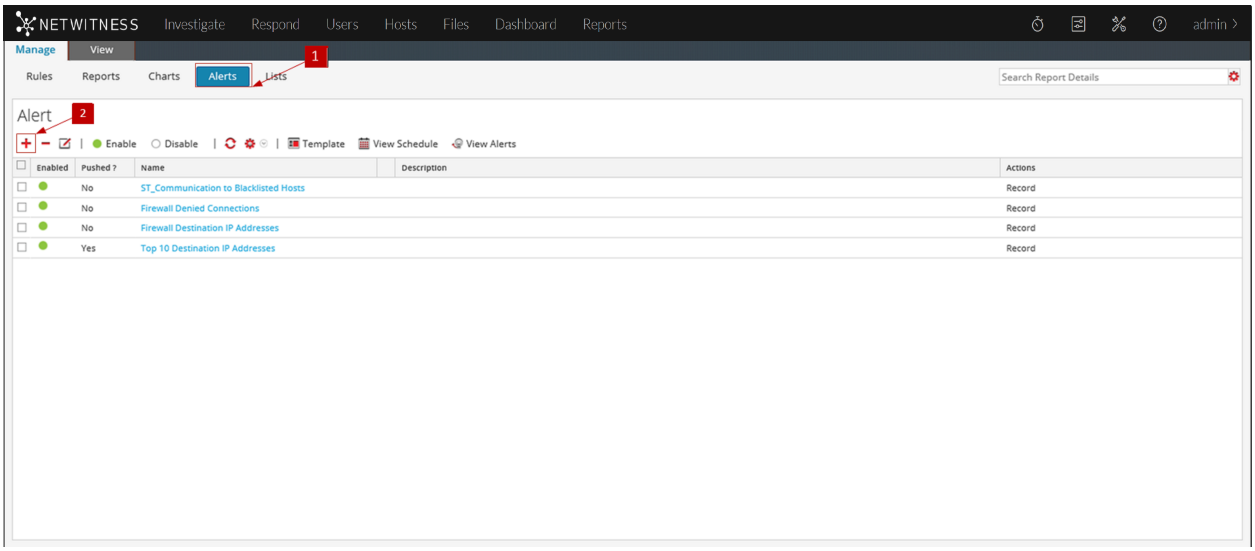
*You can complete these tasks here.

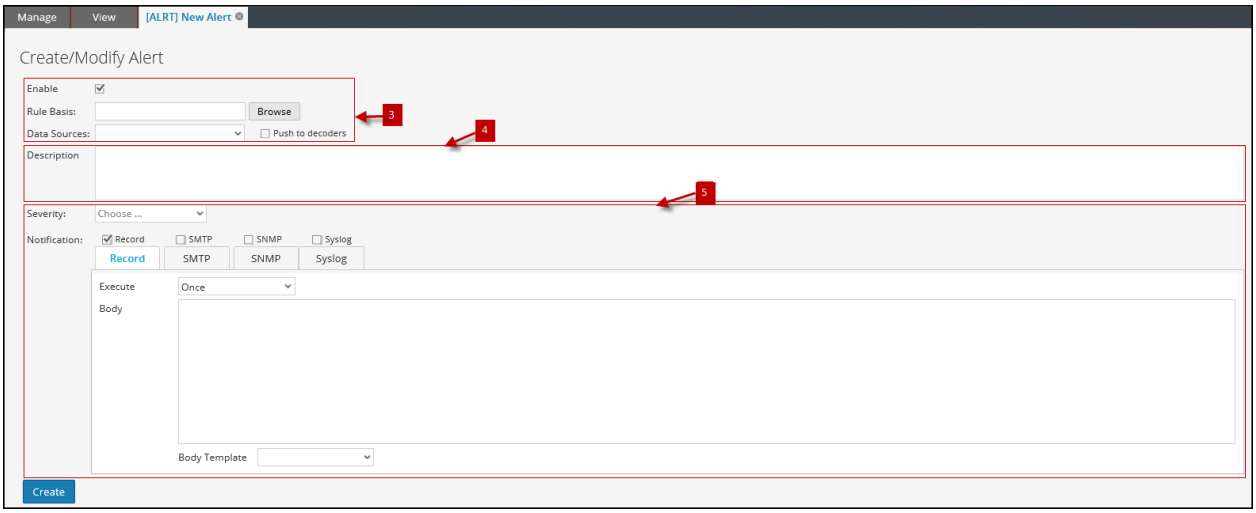
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1. Click **Alerts** to open the Alert view.
2. Click + to navigate to the Create or Modify Alert panel.
3. Enable the alert, navigate the rule, and select a data source to alert.
4. Enter a brief description of an alert.
5. Define the alert notification methods(RECORD, SMTP, SNMP, Syslog) to alert, when an alert condition is matched.

The Create or Modify Alert panel has the following sections:

- Alert Definition
- Alert Description
- Alert Notification

Alert Definition

The following table describes the fields in the Alert Definition:

Field	Description
Enable	• **Enable** activates the alert. The alert executes and sends output actions every minute (by default) when the alert conditions are met. • **Disable** deactivates the alert. The alert does not execute and does not send any output actions.
Rule Basis	Click **Browse** to display the Rules Library panel from which you select the rule that is the basis of this alert. You must select a rule that has a unique 'where' clause for an alert.
Data Sources	Specifies the data source for the alert.
Push to decoders	Pushes the ‘where’ clause of the alert rule to Decoders connected to the selected NWDB data source. This is the recommended option used to create RE alerts, as the alert conditions are checked on the Decoder itself and the alert queries will be comparatively faster in NWDB. If you deselect this option, the alert rule ‘where’ clause will be queried against the selected NWDB data source. Based on the complexity and metas in the ‘where’ clause of the rule, the alert queries might take more time to process in NWDB. **Note:** RSA NetWitness does not send rules to the Decoder automatically.

Alert Description

The following table describes the fields in the Alert Description:

Field	Description
Description	Describes the alert.
Create	Creates the alert. (This option is displayed when you create an alert.)
Save	Saves the changes made to the alert. (This option is displayed when you modify an alert.)

Alert Notification

The Alert Notification allows you to define the notification action NetWitness takes when an alert is generated, for example, recording or sending the alert using one of the defined output actions. The output actions are Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), or Syslog message.

The Notification contains the default Record tab, which you use to create an alert. The icon beside the Record tab allows you to select the notification type from the drop-down list for the output to specify for the alert: SMTP, SNMP, or Syslog.

Depending on the selected notification type, the Notification section is populated with predefined text that contains variables that add Meta that is appropriate for the alert. In the Reporting Engine, these variables are replaced with actual values. The following table lists the variables and their descriptions.

Variable	Description
`${meta.<metakey>}`	The meta key value. **Note:** If the <metakey> did not fetch any value, an empty string("") is printed. By default, Reporting Engine displays all the repeated values for a meta key. If you do not want the meta values to repeat in the Alert output, enable the "removeRepeatedMetaValue" option by navigating to **Configuration > Alert Configuration** available for the Reporting Engine in the **Services - Configuration > Explore** view. For example, in an HTTP Session the value for the action is displayed as get, get, put, put, post, get. When this option is enabled, the value is displayed as get, put, post.
`${meta.time}` / `${meta.time:<time_format>}`	`${meta.time}` - The session time is printed in "yyyy-MMM-dd HH:mm:ss" format. `${meta.time:<time_format>}` - The session time is printed in the user-defined custom time format. For example, `${meta.time:dd-MM-yyyy HH:mm:ss}`. For more information on the supported time formats, see http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html **Note:** If the time format provided by the user is invalid, the default time format will be used. The default time format is "yyyy-MMM-dd HH:mm:ss".
`${name}`	The alert name defined in Reporting Engine.
`${count}`	The number of times an alert is detected in a given time frame. (By default, it is one minute)
`${nw.host}`	The NetWitness host name as configured in Reporting Engine.
`${device.id}`	The NetWitness device ID of the data source.

The Alert Notification view has four tabs:

- **Record Tab**
- **SMTP Tab**
- **SNMP Tab**
- **Syslog Tab**

Record Tab

Use the Record tab to define the frequency for recording an alert and the message to generate when an alert is generated.

The following table lists the fields in the Record tab and their description.

Field	Description
Execute	The frequency for recording an alert. • **Once** - Record the alert only once based on the alert interval no matter how often the alert is generated. NetWitness records the number of times the alert has actually generated during that interval in the log file so that analysts know how many times the alert registered a match over a given day. • **Each Event** - Record the alert each time as it generates. If an alert generates unlimited number of times during a day, that alert is often treated as noise and can be ignored, except in case of alerts that require continuous monitoring such as network configuration changes and DDOS attacks. **Note:** Select **Each Event** setting from the **Execute** drop-down list for SNMP and Syslog output actions.
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the alert message.

SMTP Tab

The SMTP tab allows you to define the SMTP (email) output for this alert.

The following table lists the fields in the SMTP tab and their description.

Field	Description
Execute	The frequency to send an email message for the alert. • **Once** - Sends only one email for an interval, if an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Send an email with the alert for every event in which the rule criteria are met.
To	The email addresses to which to send this alert.
Subject	The subject of the email message.
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the SMTP message that you can use as is or modify.

SNMP Tab

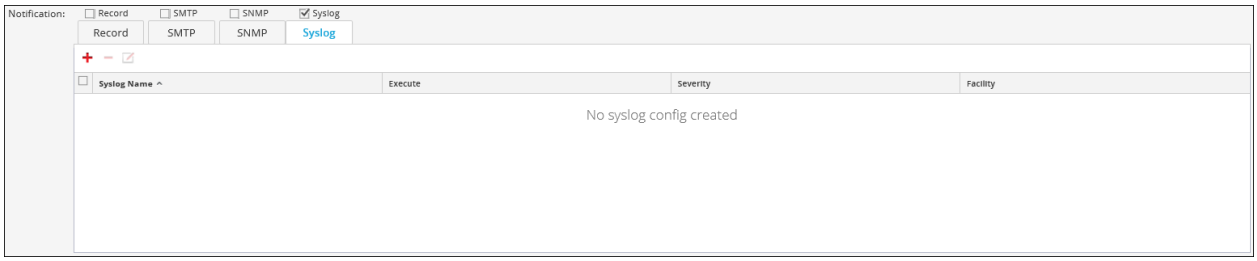
The SNMP tab allows you to define the SNMP output for the alert.

The following table lists the various fields in the SNMP tab and their description.

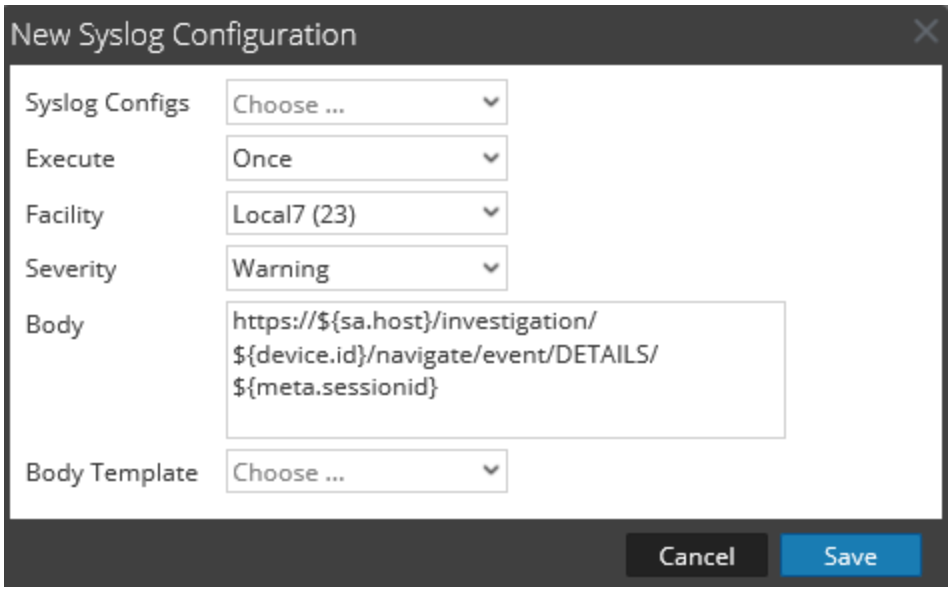
Field	Description
Execute	The frequency to send an SNMP output for an alert. • **Once** - Sends an SNMP message along with an email for an interval, if an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Sends an SNMP message with the alert for every event in which the rule criteria are met.
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the SNMP message to use as is or modify.

Syslog Tab

The Syslog tab allows you to define the Syslog message output for this alert.



Click  to add Syslog configuration to an alert. The New Syslog Configuration dialog box is displayed:



The following table describes the fields in the New Syslog Configuration dialog:

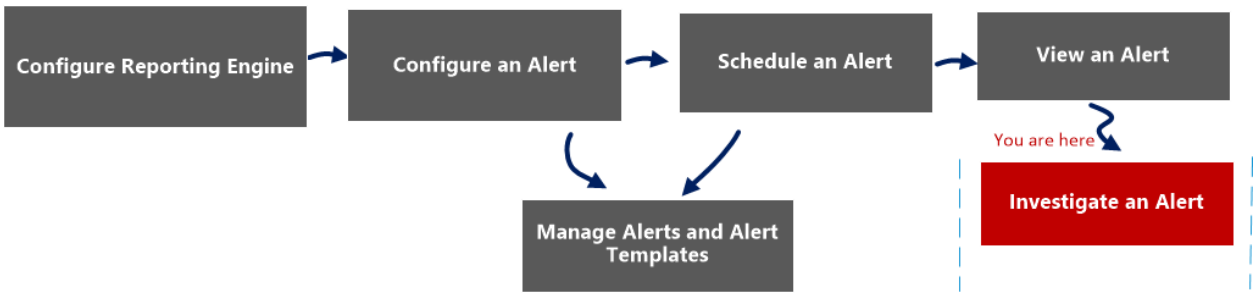
Field	Description
Syslog Configs	The Syslog configuration of the Device Config view located at the Syslog Configuration panel.
Execute	The number of times that you want to send a Syslog output for the alert. • **Once** - Sends a Syslog output along with an email for an interval, an alert generates in that interval, irrespective of how many alerts generated. • **Each Event** - Sends a Syslog output with the alert for every event in which the rule criteria are met.
Facility	The type of program logging the message. Examples for the type of programs are Syslog, Daemon, Mail, and Kernel.

Field	Description
Severity	The severity level of the alert that generated. • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Body	The body of the message.
Body Template	(Optional) If templates have been defined, select a template for the Syslog message to use as is or modify.

Investigate an Alert View

In the Investigate an Alert view, you can view and investigate alert details. When investigating an alert, you can open the sessions in the Investigation module for further investigation.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert*	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

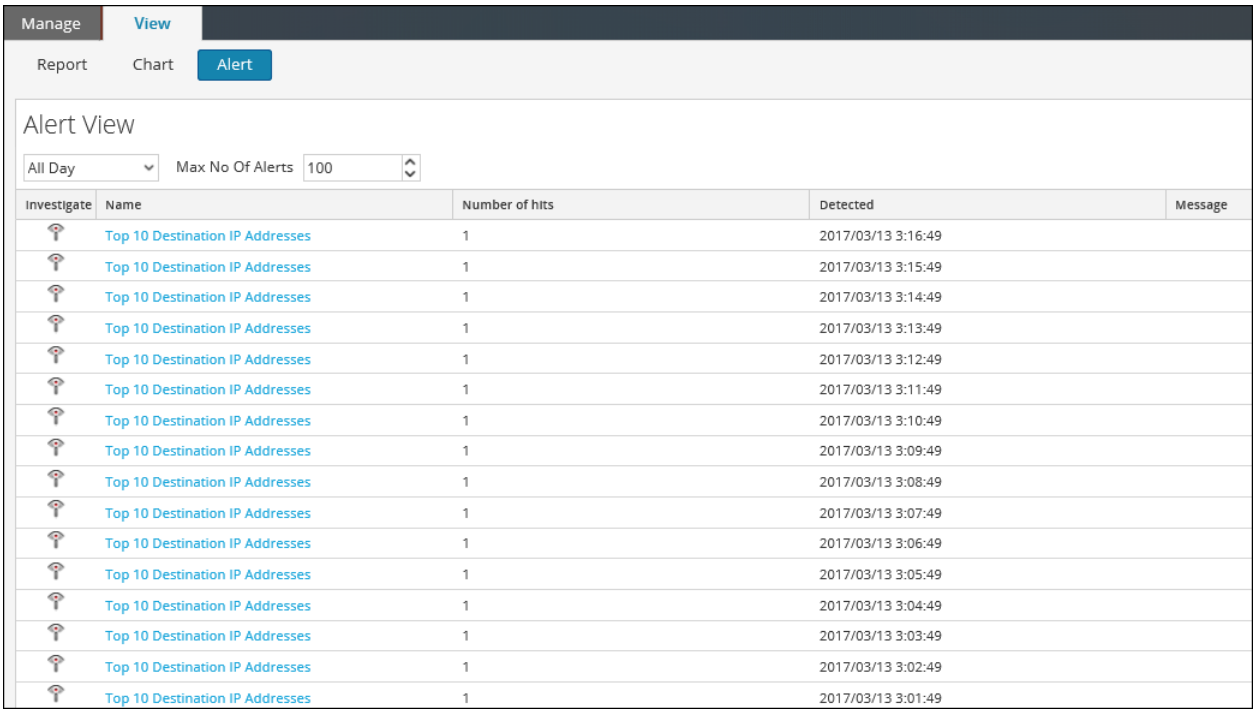
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



The View an Alert view has the following panels:

- View Alerts Toolbar
- View Alerts List

View Alerts List

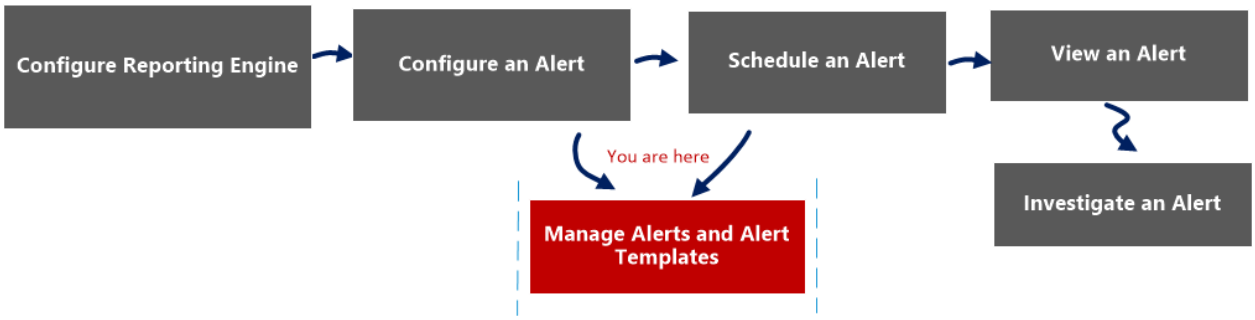
The following table lists the columns in the View Alerts List panel.

Column	Description
	The icon that opens the Investigation module, where the details of the first session that registered the match for the given alert is displayed for immediate analysis. **Note:** You are not redirected to the Investigation module when: -You reconfigure a data source for an existing alert and run an alert on the new data source. -You enter a host name instead of an IP address in the data source field.
Name	The name of the alert that registered the match. The hyperlink on the name opens the Investigation module to view all matches for that particular alert for the hour surrounding the registered alert.
Number of hits	The number of times the alert is generated.
Detected	The date and time at which the alert generates.
Message	The alert message.

Import Alert Dialog

The Import Alert dialog allows you to import an alerts archive and specify whether to overwrite existing rules, lists, and alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

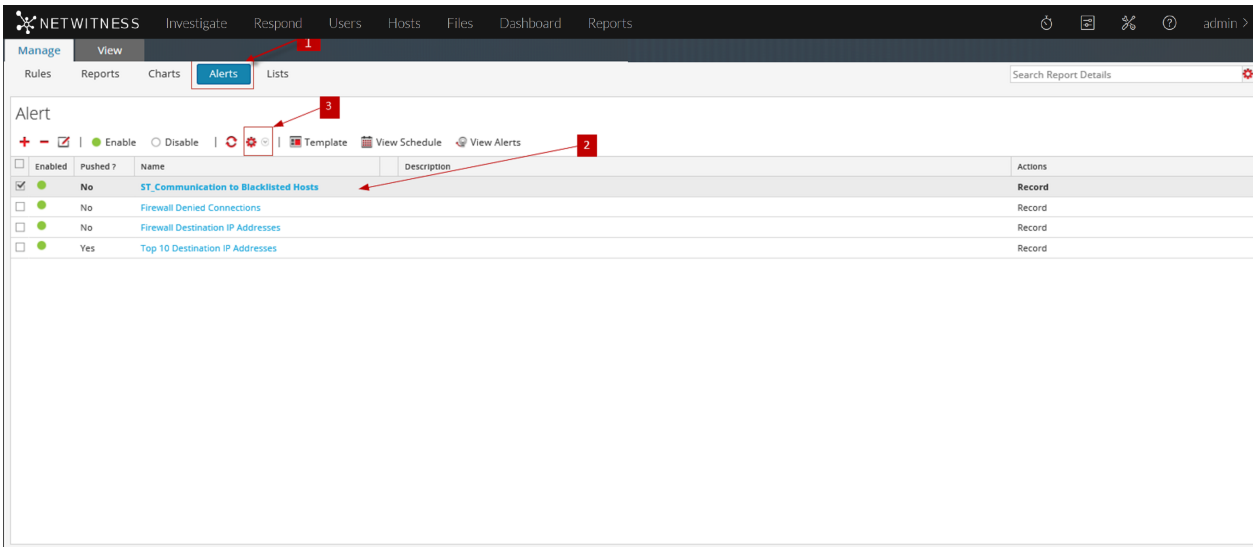
*You can complete these tasks here.

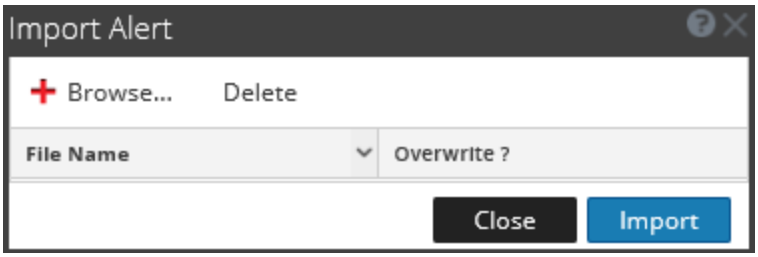
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1 Click **Alerts** to open the Alert view.
2 In the **Alert** panel, select a folder to import the file.
3 In the **Alert** toolbar, click > **Import** to import an alert.

The following table lists the actions in the Import Alert dialog and their description.

Actions	Description
Browse...	Displays a view of the local zip file system so that you can select the alert to be imported.
−	Deletes the selected alert from the Import Alert dialog.
File Name	Name of the imported binary file.
Overwrite?	Selects the option to overwrite an existing version of the alert you are importing. If you do not select the Overwrite option, a duplicate file is imported and no error message is displayed.
Close	Closes the Import Alert dialog.
Import	Imports the alert with a confirmation message.

Alert Template References

The Reporting module user interface provides access to NetWitness alerts and alert templates as well. This topic contains descriptions of the user interface as well as other reference information to help users manage alert templates.

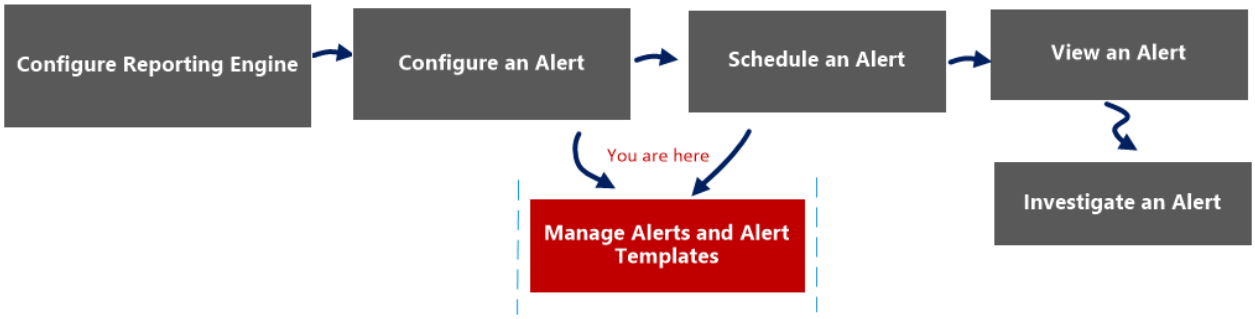
Topics:

- Create or Modify Template View
- Template View

Alert Template View

In the Template view, you can add, modify, view, and delete alert templates.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

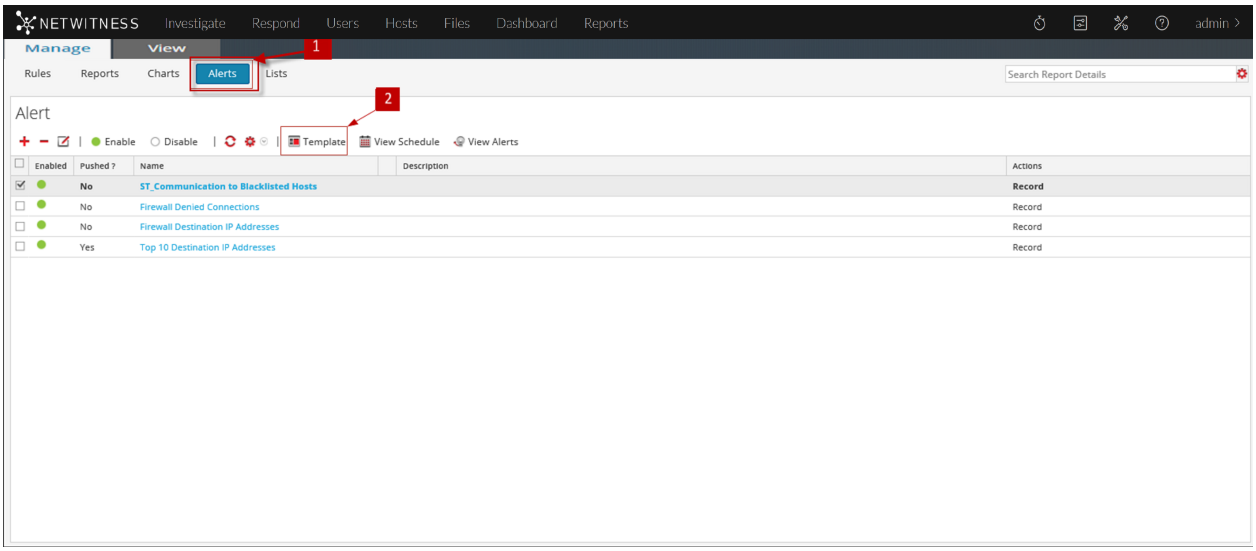
*You can complete these tasks here.

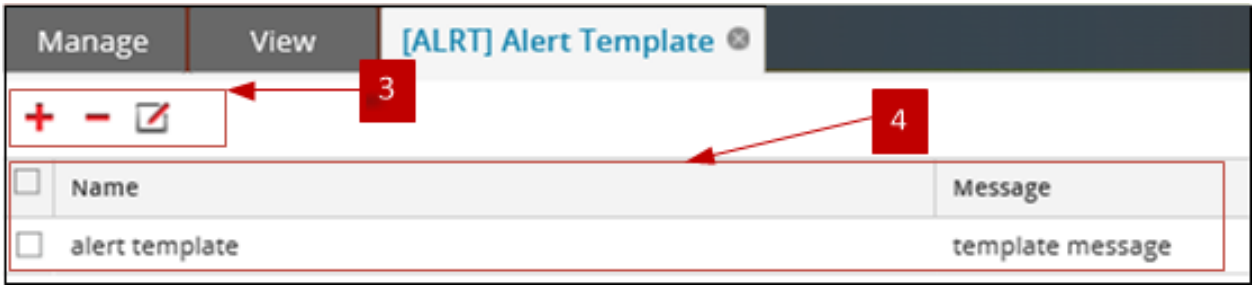
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1 Click **Alerts** to open the Alert view.
2 Click Template to open the Template view.
3 The Template toolbar allows you to add, modify, and delete alert templates.
4 The Template List panel allows you to view a list of all the templates in a tabular format.

The Alert Template view has the following panels:

- Template Toolbar
- Template List

Template Toolbar

Once the templates are defined, you can select a template to simplify defining and modifying alert messages.

The following table lists the various actions in the Template view and their description.

Actions	Description
+	Creates a new alert template.
−	Deletes the selected alert template.
✎	Edits an existing alert template.

Template List

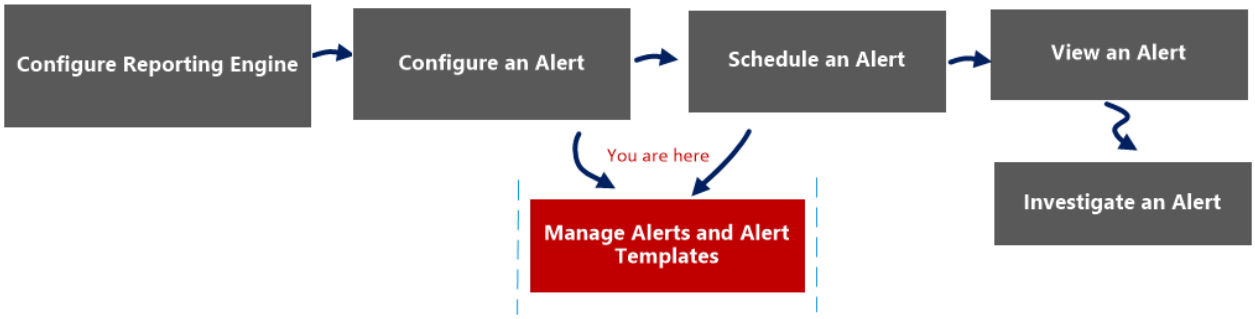
The following table describes the columns in the Templates List panel.

Column	Description
Name	Name of the template.
Message	Alert message defined for the template.

Create or Modify Template View

In the Create/Modify Template view, you can customize alert templates to use when creating alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template*	Manage an Alert and Alert Template

*You can complete these tasks here.

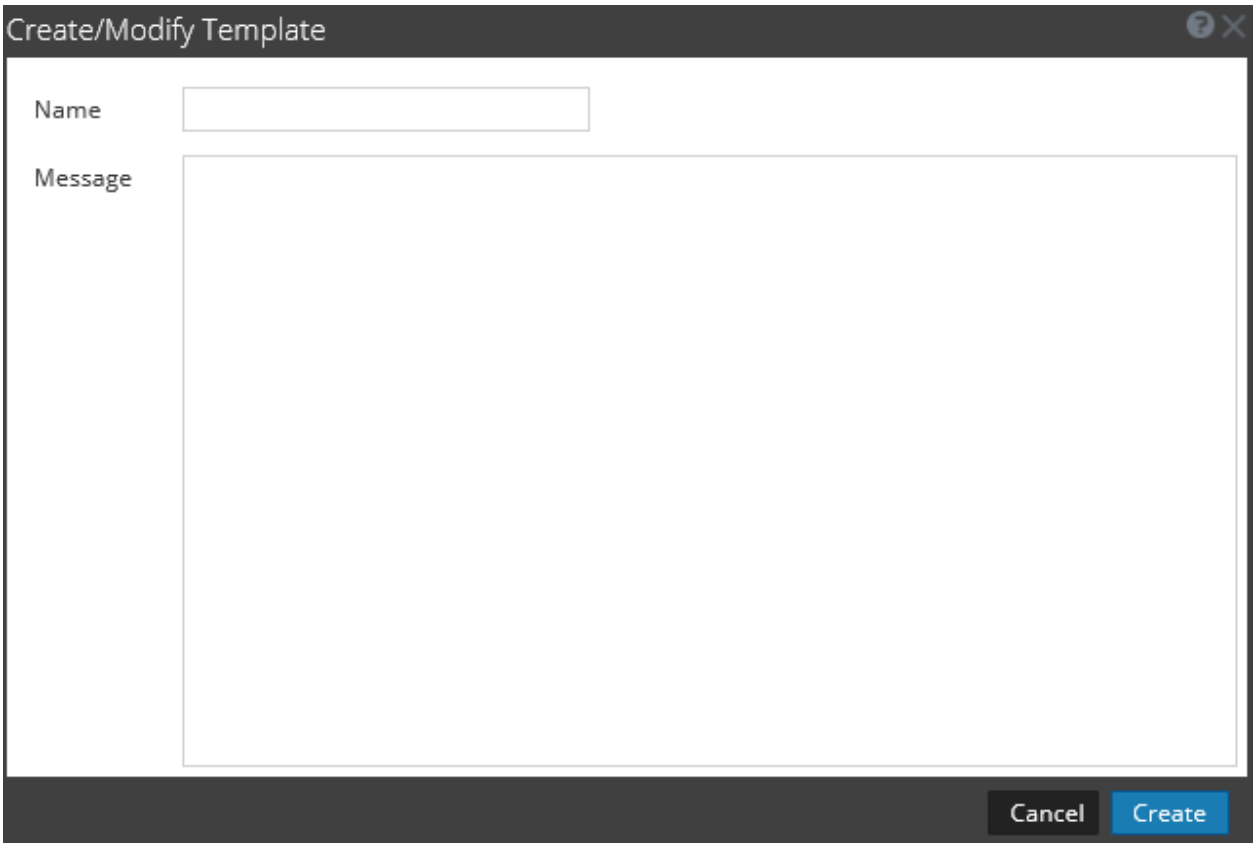
Related Topics

Alerting Overview

Quick View

You can create or modify an alert template name and message on this view.

The following figure is an example of the Create or Modify alert template.



The following table describes the fields in the Create/Modify template.

Feature	Description
Name	Indicates the name of the template for Reporting alerts. For example, source IP.
Message	Specifies the message that will be sent when an alert is triggered.
Create	Creates the template with a confirmation message and becomes available for use in Reporting immediately.
Save	Saves the template with the edited details or when a new template is created. This button is visible only in the edit mode.
Cancel	Closes the dialog without saving the template or any changes made to the template.

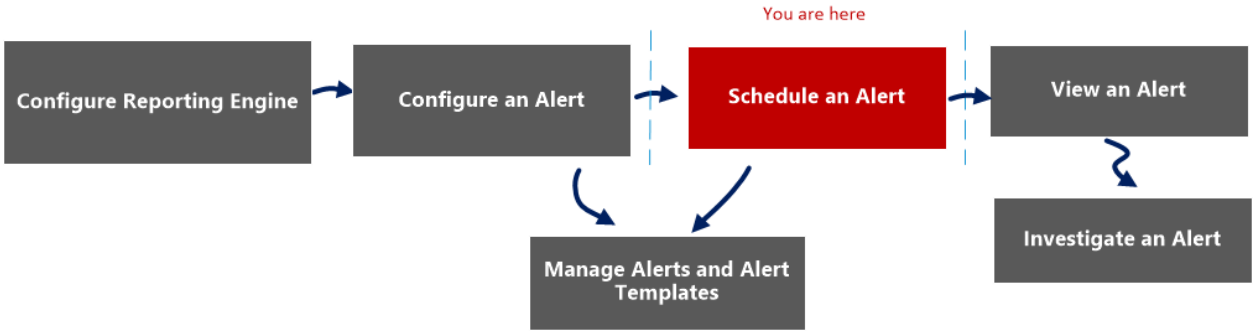
View Alerts Schedule View

In the View Alerts Schedule view, you can view the following information about each of your scheduled alerts.

- Completion status, name, last run time, last session ID, total alerts triggered.
- Statistics about the time taken to run the scheduled alert: duration, average duration, maximum duration.

Note: You can also disable the scheduled alerts.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert*	Schedule an Alert
Administrator/ Analyst	View an alert	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

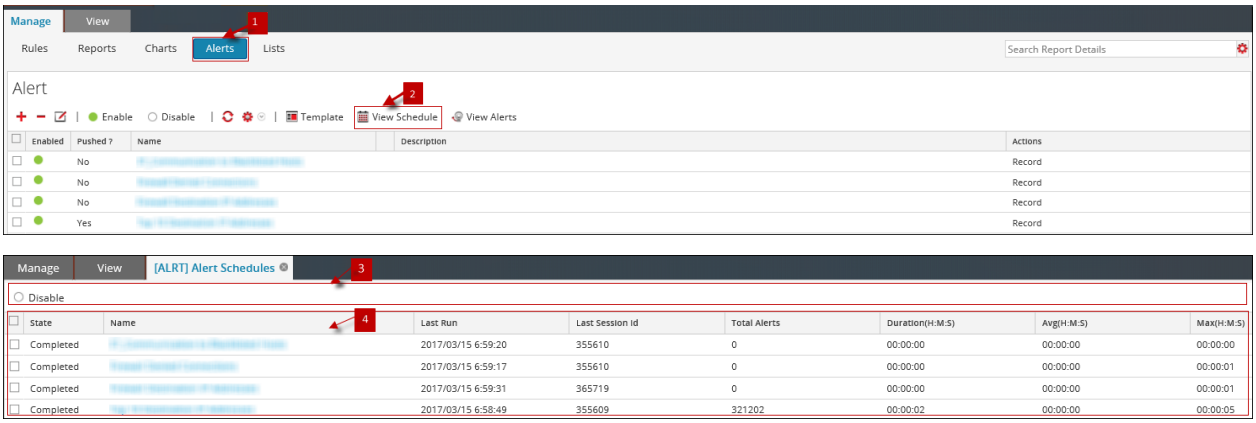
*You can complete these tasks here.

Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.



1. Click **Alerts** to open the Alert view.
2. Click **View Schedule**to view all the alerts scheduled.
3. The Alerts schedule toolbar allows you to disable the scheduled alert.
4. The Alerts schedule list allows you to view the scheduled alert details.

The View Alerts Schedule view includes the following panels:

1. Alerts Schedule toolbar
2. Alerts Schedule list

Alert Schedule Toolbar

The Alerts Schedule Toolbar panel allows you to modify the state of the scheduled alert.

Feature	Description
Disable	Clicking **Disable** disables the selected alert. When schedule alerts are no longer needed or are determined to be ineffective, you can disable them so that they are no longer executed. You can select one of more alerts to disable. When an alert is disabled, it is removed from the scheduled alerts list so that you can't view it here, and it will not execute again unless you manually execute the alert or set up a new schedule for it.

Alert Schedule List Panel

The Alerts Schedule List panel lists only the Enabled alerts in a tabular format. The following table lists the columns in the Alerts Schedule List panel and their description.

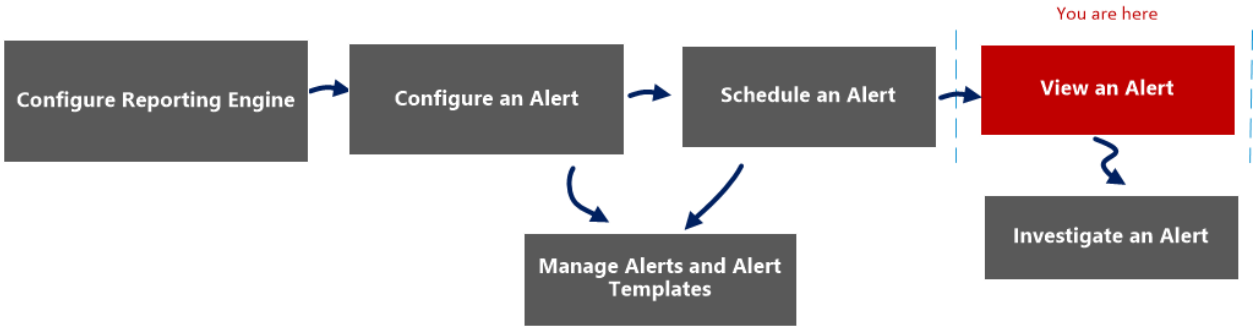
Feature	Description
State	The state of the scheduled alert: • Completed • Failed

Feature	Description
Name	The name of the scheduled alert.
Last Run {#time}	The last time the scheduled alert was run.
Last Session Id	The Session Id of the last scheduled alert.
Total Alerts	The total number of event occurrences.
Duration	The time taken to run the scheduled alert.
Avg (s)	The average time taken to run the scheduled alert.
Max (s)	The maximum time taken to run the scheduled alert.

View Alerts View

In the View Alerts view, you can view all the alerts. Also, you can also customize the view to show alerts for a specific period of time, and set the maximum number of alerts displayed in a single page.

Workflow



What do you want to do?

Role	I want to...	Documentation
Administrator/ Analyst	Configure Reporting Engine	Configure Reporting Engine
Administrator/ Analyst	Configure an alert	Configure an Alert
Administrator/ Analyst	Schedule an alert	Schedule an Alert
Administrator/ Analyst	View an alert*	View an Alert
Administrator/ Analyst	Investigate an alert	Investigate an Alert
Administrator/ Analyst	Manage an alert and alert template	Manage an Alert and Alert Template

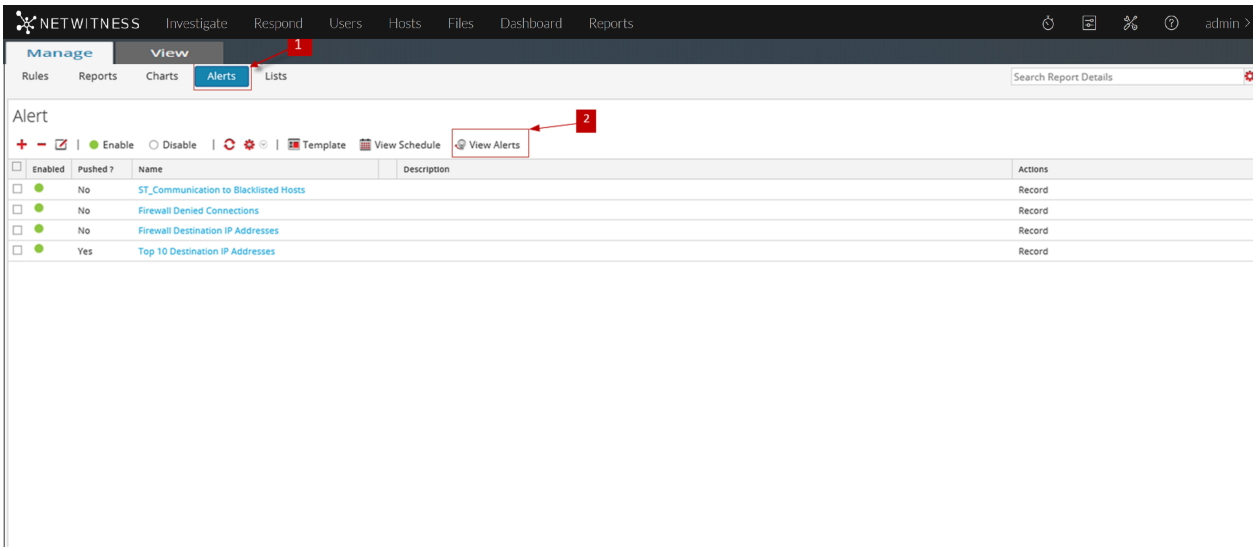
*You can complete these tasks here.

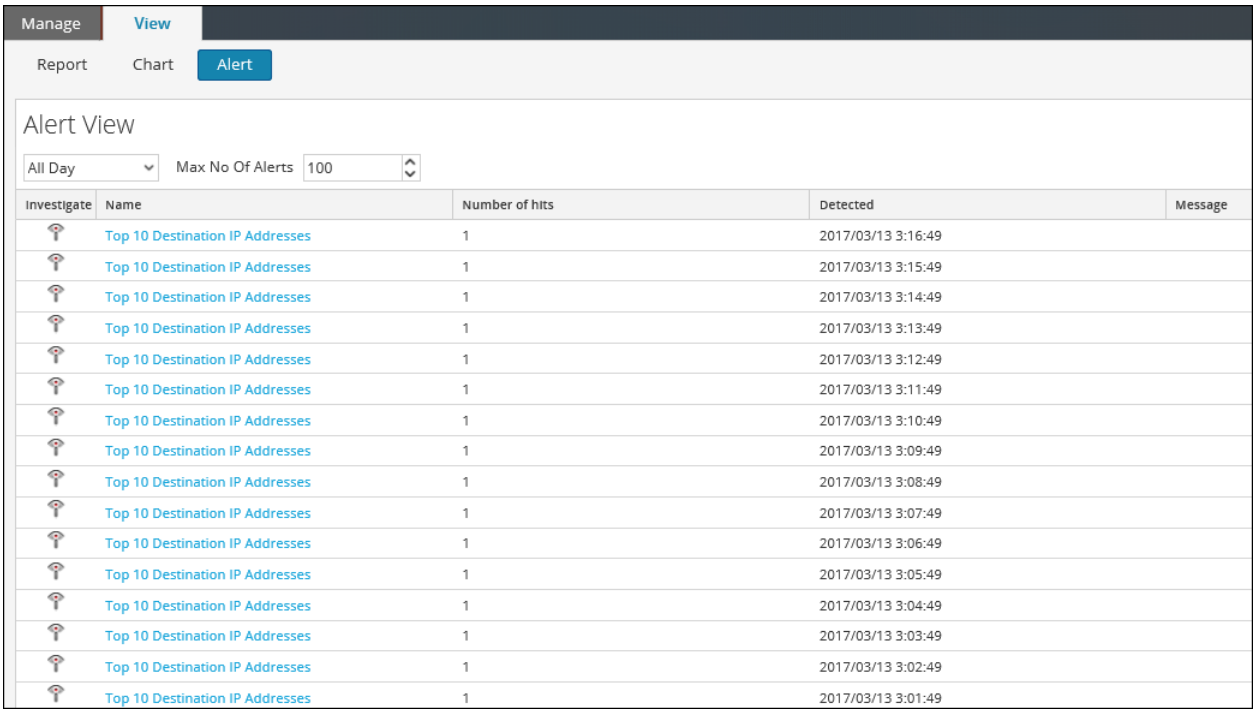
Related Topics

Alerting Overview

Quick View

The following figure is an example with the important features labeled.





1. Click **Alerts** to open the Alert view.
2. Click **View Alerts** to view the different panels on View Alerts.
3. The View Alerts toolbar allows you to filter alerts based on a count, or the start and end date of the alerts.
4. The View Alerts List lists all the filtered alerts in a tabular format.

The View Alerts view has the following panels:

- View Alerts Toolbar
- View Alerts List

View Alerts Toolbar

The following table lists the operations in View Alerts toolbar panel.

Option	Description
Last Hour(s) data	The data fetched from the previous execution.
Max No Of Alerts	The maximum number of alerts that you want to fetch from the Reporting Engine service for a specific time-range.

View Alerts List

The following table lists the columns in the View Alerts List panel.

Column	Description
	The icon that opens the Investigation module, where the details of the first session that registered the match for the given alert is displayed for immediate analysis. **Note:** You are not redirected to the Investigation module when: -You reconfigure a data source for an existing alert and run an alert on the new data source. -You enter a host name instead of an IP address in the data source field.
Name	The name of the alert that registered the match. The hyperlink on the name opens the Investigation module to view all matches for that particular alert for the hour surrounding the registered alert.
Number of hits	The number of times the alert is generated.
Detected	The date and time at which the alert generates.
Message	The alert message.