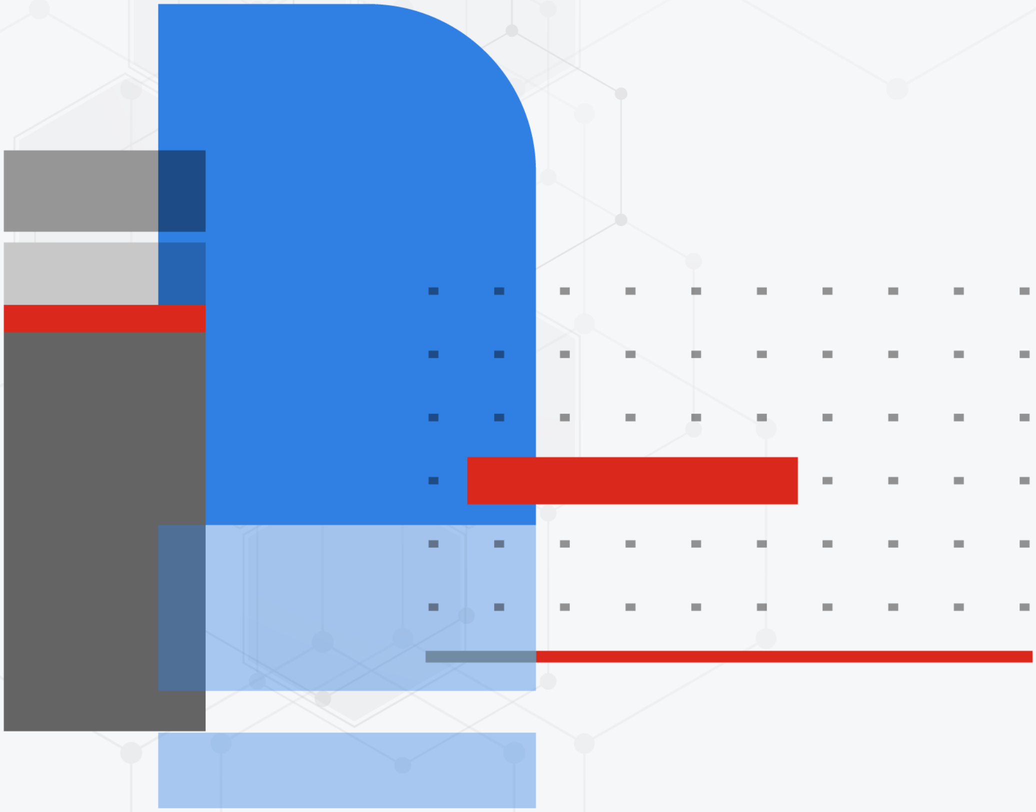
SQL Log Database Query

FortiAnalyzer 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 15, 2023
FortiAnalyzer 7.4.0 SQL Log Database Query
02-740-912144-20230515

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-15	Initial release.

Introduction

This document describes how to write your own SQL query statements to create custom datasets.

FortiAnalyzer supports local PostgreSQL databases for the storage of log tables.

For additional information about the FortiAnalyzer dataset, see the FortiAnalyzer Administration Guide on the Fortinet Docs Library.

To create a report based on log messages in the local database, you can use either the predefined datasets or create your own custom dataset by querying the log message in the SQL database on the FortiAnalyzer.

Creating datasets

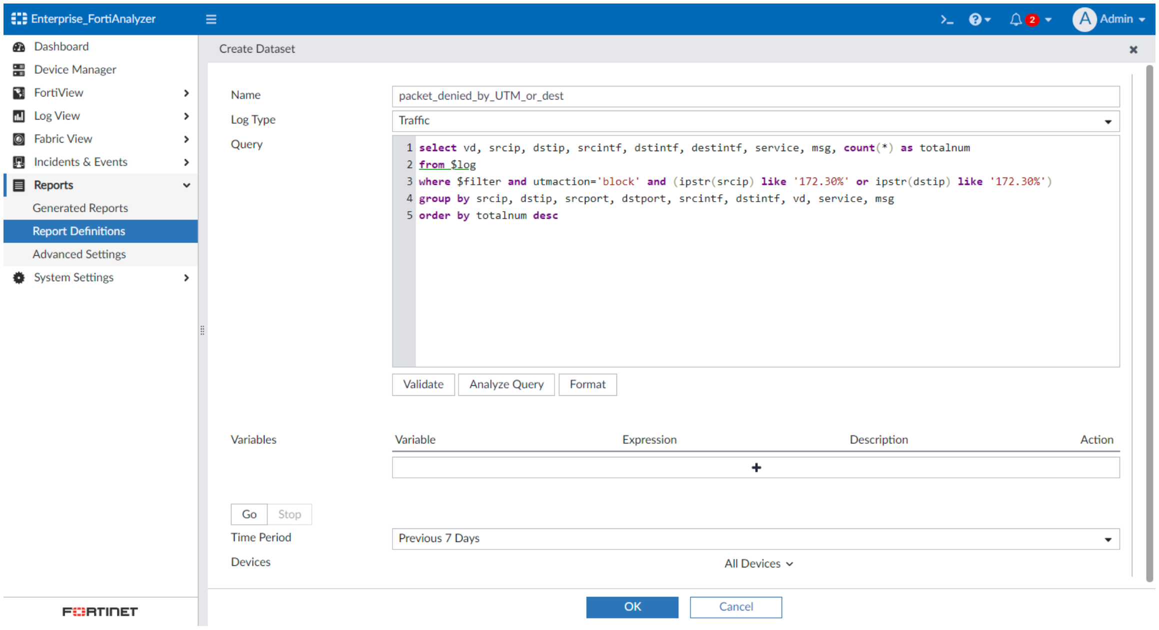
The following procedure describes how to create datasets in FortiAnalyzer.

Datasets define what data is extracted from the database and represented in a report's chart. While FortiAnalyzer does provide pre-defined datasets that address the most common queries, you need to understand Structured Query Language, also known as SQL, in order to modify those datasets or create your own.

For additional details, see the FortiAnalyzer Administration Guide and the FortiAnalyzer CLI Reference in the Fortinet Docs Library.

To create a custom dataset:

1. Go to *Reports > Report Definitions > Datasets*.
2. Click *Create New*.
3. Configure the dataset.



Name: packet_denied_by_UTM_or_dest

Log Type: Traffic

Query:

```
select vd, srcip, dstip, srcintf, dstintf, destintf, service, msg, count(*) as totalnum
from $log
where $filter and utmaction='block' and (ipstr(srcip) like '172.30%' or ipstr(dstip) like '172.30%')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```

Variables

Time Period: Previous 7 Days

Devices: All Devices

Name	Enter a name for the dataset.
Log Type	Select the log type to be used in the dataset. `$log` is used in the SQL query to represent the log type you select, and it is run against all tables of this type.
Query	Enter the SQL query used for the dataset. An easy way to build a custom query is to clone and edit a predefined dataset. While entering the SQL query in this field, automatic suggestions display a list of possible commands, table names, log fields, and more to use in your query where applicable. You can also mouse over related areas in the *Query* field to view the log fields available in the table. For example, you can mouse over `from $log` to view the log fields in that table.

Validate	Click to validate the entered SQL query. If any errors are present in the query, the details of the error are displayed below. If there are no errors in the query, the message will display *OK*.
Analyze Query	Click to perform a detailed analysis on the SQL query. *Analyze Query* displays the original SQL query, the transformed SQL query (if applicable), and the SQL validation results. This function also allows users to view the hcache query that is used when a report using this dataset has enabled the auto-cache option for faster report generation. For more information on hcache, see the FortiAnalyzer Administration Guide.
Format	Click to automatically format the entered SQL query, making it easier to read, update, and detect errors.
Variables	Click the *Add* button to add variable, expression, and description information. If added, the expression for the variable will be used when configuring filters for reports that use this dataset. For example, if *Variable = User (user)* and *Expression = coalesce(nullifna(\`user\`), ipstr(\`srcip\`))*, then the expression will be used when *User (user)* is selected as the *Log Field* in a report's filter. See Filtering report output in the *FortiAnalyzer Administration Guide*.
Go	Click to test the SQL query before saving the dataset configuration. Click *Stop* to end a test in progress.
Time Period	From the dropdown, select a time period to run the SQL query against. When selecting *Custom*, enter the start date and time, and the end date and time.
Devices	From the dropdown, select devices to run the SQL query against.

4. Click *Go*.
   The query results are displayed. If the query is not successful, an error message is displayed instead.
5. Click *OK*.

The SQL dataset test function (*Go*) can be used to determine if any errors are present in the SQL format. It should not be used to test returned values as those may be different than the ones used in reports.

To add a dataset to a chart:

1. Go to *Reports > Report Definitions > Chart Library*, and click *Create New* or edit an existing chart.
2. From the *Dataset* dropdown, select your custom dataset.
3. Configure the remaining chart details, and click *OK*.

   The chart based on your custom dataset is now available for use in reports.|

To use a chart in reports:

1. Go to *Reports > Report Definitions > All Reports*.
2. From the *Report* dropdown, click *Create New*.
   You can also edit an existing report to add the chart.
3. In the *Create Report* dialog, configure the options and click *OK*.

4.

Name	Enter a name for the report.
Create from	Select *Blank* or *Template*. If *Template* is selected, select a template for the report from the *Select Template* dropdown.
Save to Folder	From the dropdown, select a folder to save the report in. You can click the *Add* button to save the report to multiple locations.

5. Go to the *Editor* tab for the report, and click *Insert Chart*.
6. From the *Chart* dropdown, select the chart that you created.
7. Click *OK*.

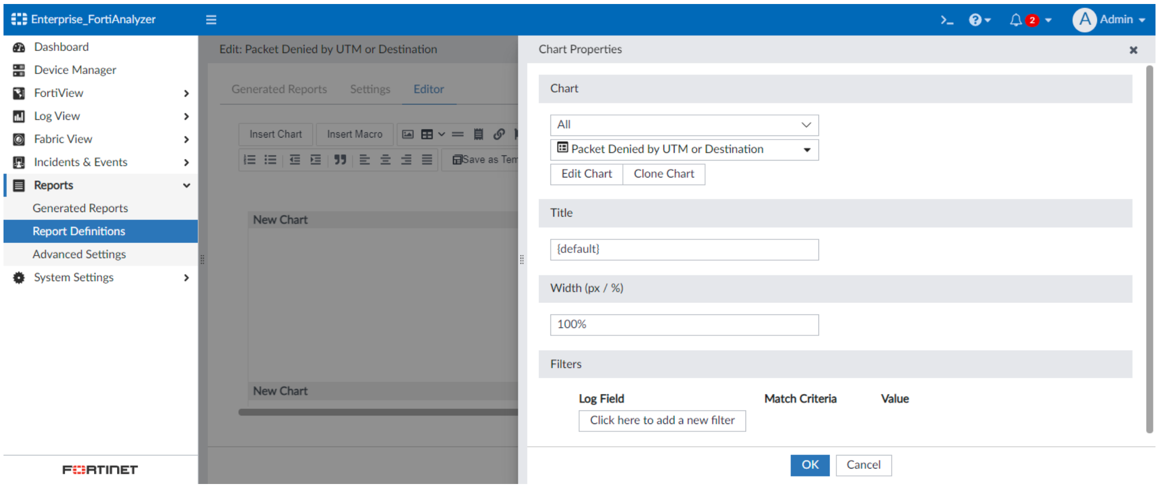


Chart: All

Packet Denied by UTM or Destination

Title: {default}

Width (px / %): 100%

8. Configure the remaining report settings, and save your changes.

For more information, about creating charts and creating reports, see the FortiAnalyzer Administration Guide.

Testing datasets queries

Once a dataset has been created, you can test the dataset query to confirm it works as intended.

To test a dataset query:

1. Follow the procedures in Creating datasets on page 6 or clone an existing dataset.
2. From the *Time Period* dropdown, select a time period to use for the test.
3. From the *Devices* dropdown, select the devices to use for the test.
4. Click *Go*.
   You can click *Stop* to end a test in progress.

   Once the test is finished, the query results are displayed. If the query is not succesful, an error message is displayed instead. See Troubleshooting SQL test queries on page 9.
5. Click *OK*.

Troubleshooting SQL test queries

If the SQL test is unsuccessful, an error message is displayed to indicate the cause of the problem in the query.

Following are some example error messages and possible causes:

```
ERROR: syntax error at or near...
```

- Check that SQL keywords are spelled correctly and that the query is well-formed. Table and column names are demarked by grave accent (`) characters. Single (') and double (") quotation marks will cause an error.

```
No Data
```

- The query is correctly formed, but no data has been logged for the specified log type. Check that you have configured and authorized a logging device of that type on the FortiAnalyzer.

You can click *Format* to automatically format the entered SQL query in a dataset, making it easier to read, update, and detect errors.

SQL tables

SQL is the database language that FortiAnalyzer uses for logging and reporting. Log data is inserted into the SQL database for log view and report generation. FortiAnalyzer uses a PostgreSQL database.

In an SQL database all information is represented as tables, and each table consists of a set of rows and columns. There are two types of tables:

- User tables, which contain information that is in the database, and
- System tables, which contain the database description.

You can use information from SQL tables to create custom datasets for use in report charts.

Log types and subtypes

Log types each have a SQL table that can be specified when creating datasets.

Log types also include log subtypes, which are types of log messages that are within the main log type.

For more information on log types and subtypes, see the FortiAnalyzer and FortiGate Log Message Reference guides on the Fortinet Document Library.

Log types available in FortiAnalyzer datasets

Source	Log type
FortiGate	Application
	Intrusion Prevention
	Content
	Data Leak Prevention
	DNS
	Email Filter
	Event
	FortiClient System Event
	FortiClient Security Event
	FortiClient Traffic
	File Filter
	GTP
	Vulnerability Scan
	Protocol
	SSH
	SSL
	Traffic
	Antivirus
	VoIP
	Web Application Firewall
	Web Filter
	Local Event
FortiMail	Email Filter
	Event
	History
	Antivirus

Source	Log type
FortiAnalyzer	Application
	Event
	Local Event
FortiWeb	Attack
	Event
	Traffic
FortiCache	Application
	Intrusion Prevention
	Content
	Data Leak Prevention
	Email Filter
	Event
	Vulnerability Scan
	Traffic
	Antivirus
	VoIP
	Web Filter
FortiClient	FortiClient System Event
	FortiClient Security Event
	FortiClient Traffic
Syslog	Syslog
FortiManager	Application
	Event
FortiSandbox	Event
	Vulnerability Scan
	Antivirus
FortiDDoS	Intrusion Prevention
	Event
FortiAuthenticator	Event

Source	Log type
FortiProxy	Application
	Intrusion Prevention
	Data Leak Prevention
	DNS
	Email Filter
	Event
	SSH
	Traffic
	Antivirus
	VoIP
	Web Filter
FortiNAC	Asset
	Event
FortiFirewall	DNS
	Event
	File Filter
	GTP
	SSH
	SSL
	Traffic
FortiSOAR	Event
FortiADC	Intrusion Prevention
	Event
	Traffic
FortiDeceptor	Event
FortiNDR	Attack
	Event
Fabric	Normalized

Log severity levels

Each log entry contains a level field that indicates the estimated severity of the event that caused the log entry. When a logging severity level is defined, the FortiAnalyzer unit logs all messages at and above the selected severity level. For example, if you select Error, FortiAnalyzer logs Error, Critical, Alert, and Emergency level messages.

The Debug log severity level is rarely used. Debug log messages are useful when the FortiAnalyzer unit is not functioning properly. Debug log messages are only generated if the log severity level is set to Debug. Debug log messages are generated by all subtypes of the event log.

To view information about log severity levels, see the FortiAnalyzer Log Message Reference.

Log fields

Each log table stored in an SQL database contains log fields that can be used in datasets.

You can view a full list of the fields available for each log type in the *FortiAnalyzer Postgres Schema* file available from the FortiCloud Support page.

Examples of custom datasets

The following examples show how to write custom datasets.

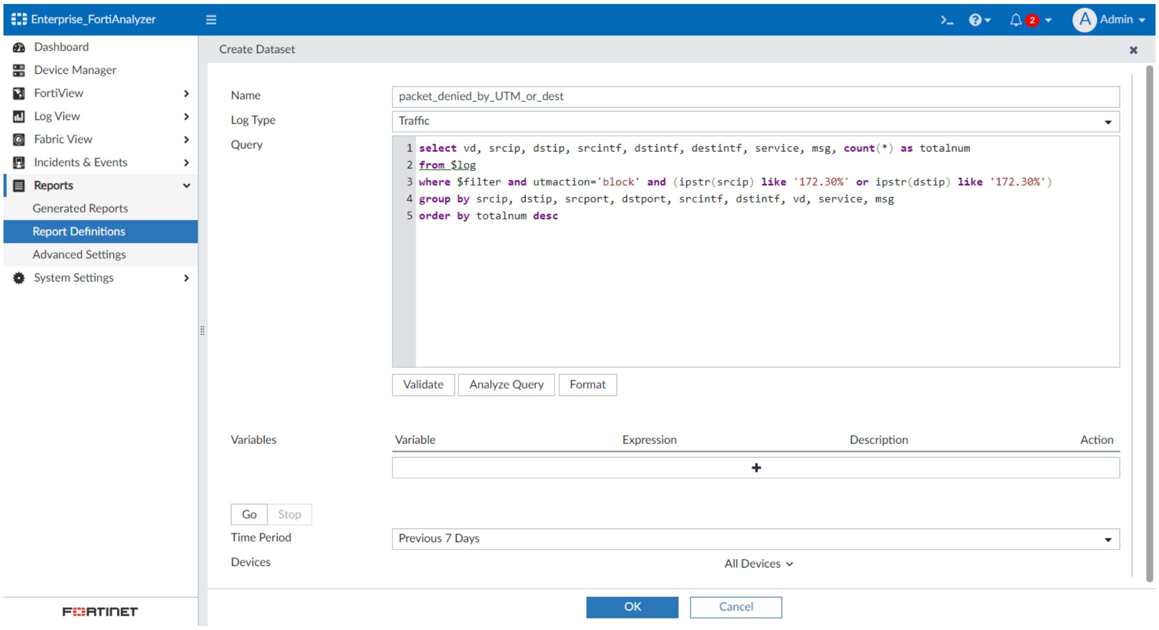
After you create the datasets, you can use them when you configure charts under *Reports* > *Report Definitions* > *Chart Library*. Configured charts can be selected when creating or modifying reports.

For more information on creating charts and reports, see the FortiAnalyzer Administration Guide.

Example 1: Packets denied by UTM for a source or destination matching '172.30.xx.xx':

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *packet_denied_by_UTM_or_dest*.
3. From the *Log Type* dropdown, select *Traffic*.
4. Configure *Time Period* and *Devices*.
5. In the *Query* field, enter the following:

```
select vd, srcip, dstip, srcport, dstport, srcintf, dstintf, service, msg, count(*) as
      totalnum
from $log
where $filter and utmaction='block' and (ipstr(srcip) like '172.30%' or ipstr(dstip)
      like '172.30%')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```



Name: packet_denied_by_UTM_or_dest

Log Type: Traffic

Query:

```
select vd, srcip, dstip, srcintf, dstintf, destintf, service, msg, count(*) as totalnum
from $log
where $filter and utmaction='block' and (ipstr(srcip) like '172.30%' or ipstr(dstip) like '172.30%')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```

Time Period: Previous 7 Days

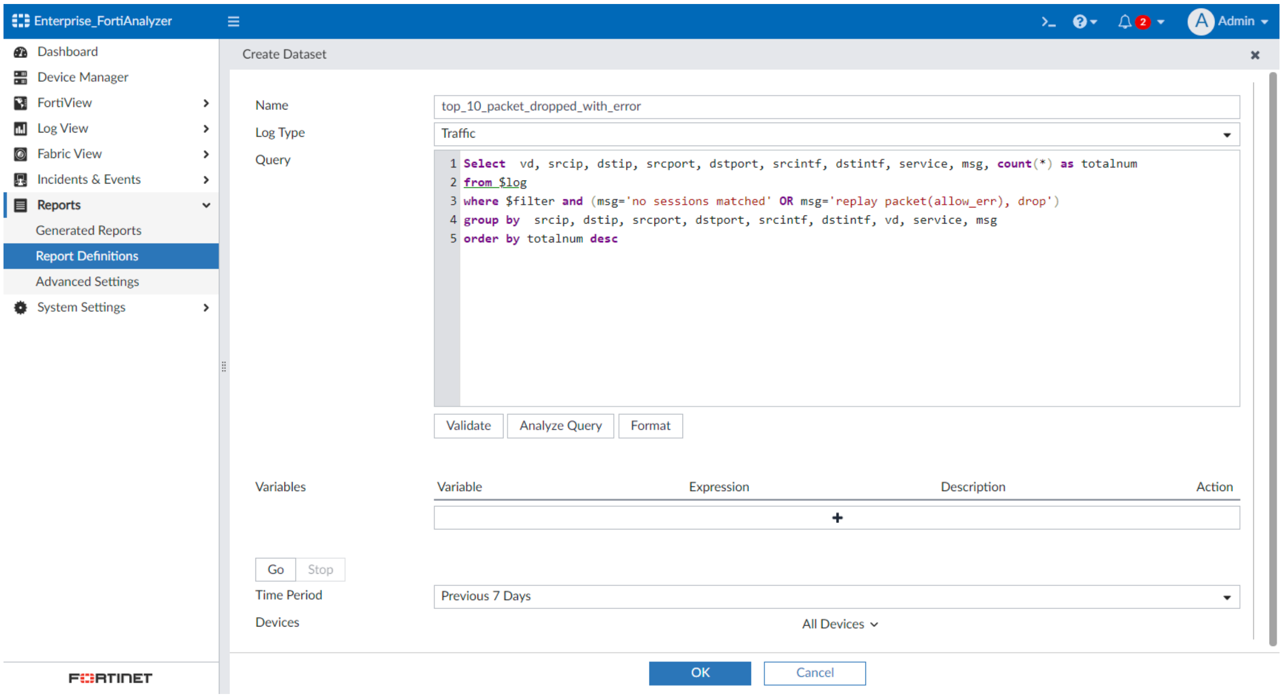
Devices: All Devices

Example 2: Top 10 hosts that had the most packets dropped with error message 'no session matched' or 'replay packet(allow_err), drop':

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *top_10_packet_dropped_with_error*.
3. From the *Log Type* dropdown, select *Traffic*.

4. Configure *Time Period* and *Devices*.
5. In the *Query* field, enter the following:

```
Select vd, srcip, dstip, srcport, dstport, srcintf, dstintf, service, msg, count(*) as
      totalnum
from $log
where $filter and (msg='no sessions matched' OR msg='replay packet(allow_err), drop')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```



Name: top_10_packet_dropped_with_error

Log Type: Traffic

Query:

```
Select  vd, srcip, dstip, srcport, dstport, srcintf, dstintf, service, msg, count(*) as totalnum
from $log
where $filter and (msg='no sessions matched' OR msg='replay packet(allow_err), drop')
group by  srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```

Variables

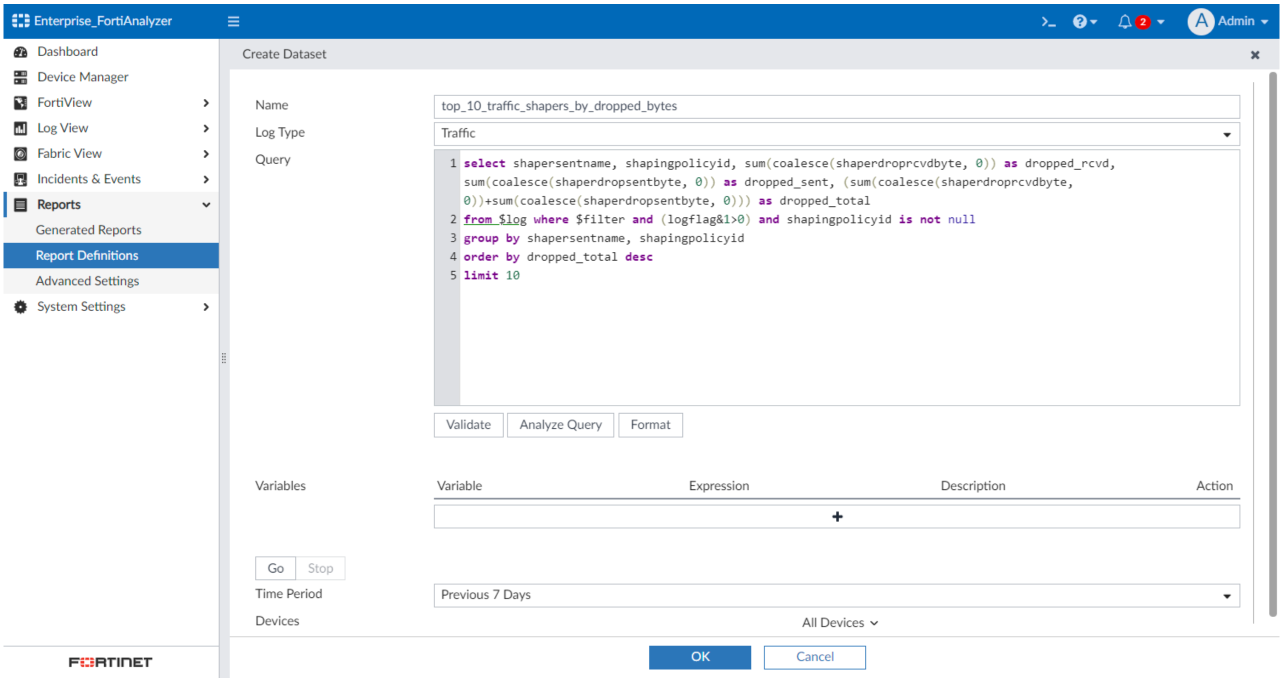
Time Period: Previous 7 Days

Devices: All Devices

Example 3: Top 10 traffic shapers by dropped bytes

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *top_10_traffic_shapers_by_dropped_bytes*.
3. From the *Log Type* dropdown, select *Traffic*.
4. Configure *Time Period* and *Devices*.
5. In the *Query* field, enter the following:

```
select shapersentname, shapingpolicyid, sum(coalesce(shaperdroprcvdbyte, 0)) as
      dropped_rcvd, sum(coalesce(shaperdropsentbyte, 0)) as dropped_sent, (sum
      (coalesce(shaperdroprcvdbyte, 0))+sum(coalesce(shaperdropsentbyte, 0))) as
      dropped_total
from $log where $filter and (logflag&1>0) and shapingpolicyid is not null
group by shapersentname, shapingpolicyid
order by dropped_total desc
limit 10
```



Name: top_10_traffic_shapers_by_dropped_bytes

Log Type: Traffic

Query:

```
select shapersentname, shapingpolicyid, sum(coalesce(shaperdroprcvdbyte, 0)) as dropped_rcvd,
sum(coalesce(shaperdropsentbyte, 0)) as dropped_sent, (sum(coalesce(shaperdroprcvdbyte,
0))+sum(coalesce(shaperdropsentbyte, 0))) as dropped_total
from $log where $filter and (logflag&1>0) and shapingpolicyid is not null
group by shapersentname, shapingpolicyid
order by dropped_total desc
limit 10
```

Variables:

Variable	Expression	Description	Action
+			

Time Period: Previous 7 Days

Devices: All Devices

FORTINET®

www.fortinet.com