FORTINET Training Institute

FORTINET CERTIFIED SOLUTION SPECIALIST
Security Operations

Security Operations Analyst

Reporting

FortiAnalyzer 7.4

Last Modified: 22 January 2025

Lesson Overview

- Report Introduction
- SQL Queries
- Report Configuration
- Report Customization

Report Introduction

Objectives

- Describe the considerations of SOC reporting
- Review the basic components of a FortiAnalyzer report

Purpose of Reports

- Reports can have different purposes depending on your requirements

- Some common purposes include:

Summarizing | Analyzing | Correlating | Recommending

Report Types

- Within the SOC, the Red, Blue and Purple teams may be responsible for different types of reports
- The target audience should determine how technical the report is
- Examples:

Team	Report Type
Red	Penetration testing
	Attack simulation
	Vulnerability findings
Blue	Incident response
	Monitoring
	Threat intelligence
Purple	Comprehensive security assessment
	Combined red and blue team reports
	Training exercise findings

Report Scope

Which information should you include or exclude?

You can limit the **scope** of the report with FortiAnalyzer.

Included devices

- Include only relevant devices
- May need to exclude outliers that produce noise

Datasets

- Select or configure appropriate datasets
- Include appropriate functions (such as SUM, AVG)

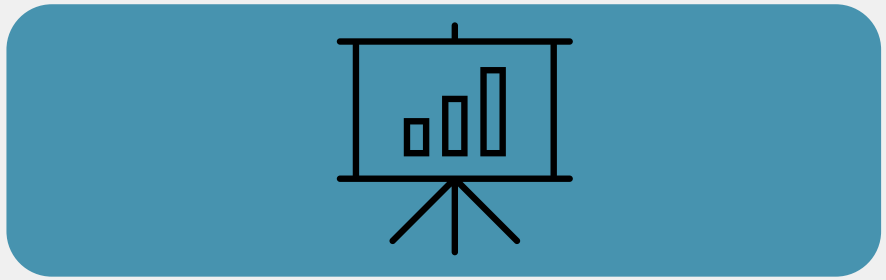
Charts and macros

- The chart types need to match the data presented
- Macros can be used if no visual representation is required

FortiAnalyzer Report Elements

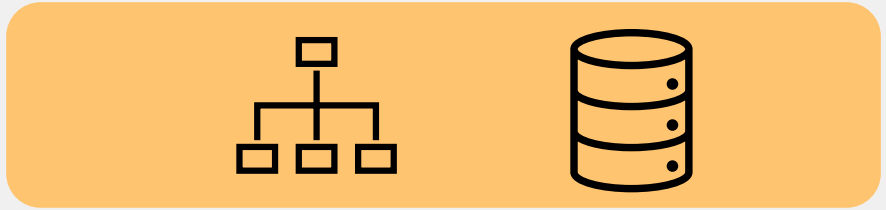
- A FortiAnalyzer report is a set of data organized in charts

Chart



- Which **data** from the SQL database is displayed
- Which **format** the data is displayed in

Dataset



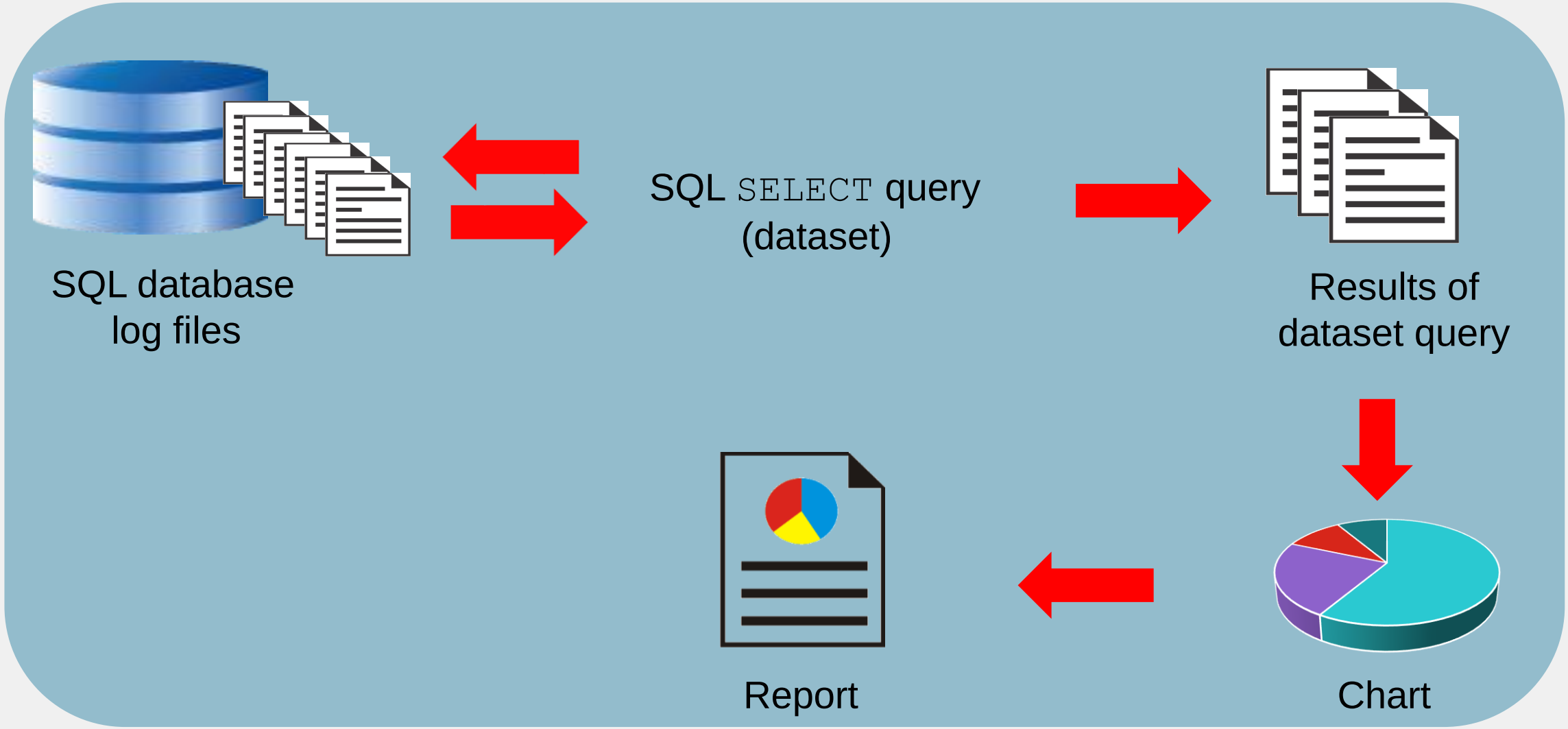
- Datasets are specific SQL `SELECT` queries

Format

- Format options:

pie charts, bar charts, tables, and more

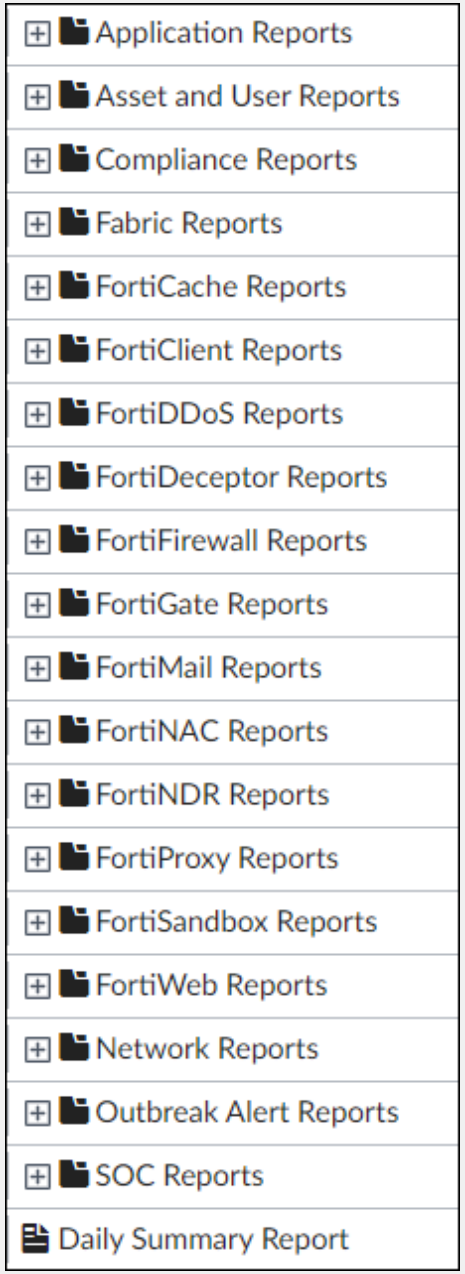
Report Workflow



Reports and ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Additional reports are available when specific ADOMs are enabled
- Verify you are in the right ADOM when creating reports

Note: A fabric ADOM has predefined reports for multiple device types



Knowledge Check

1. Charts consist of which two elements?
   - ✔ A. Dataset and format
   - B. Data and queries

2. Which statement about reports is true?
   - A. Reports are ADOM-specific.
   - ✔ B. Reports are not ADOM-specific.

Lesson Overview

- ✓ Report Introduction
- SQL Queries
- Report Configuration
- Report Customization

SQL Queries

Objectives

- Describe SQL basics
- Describe FortiAnalyzer schemas
- Use FortiAnalyzer tools for simplifying SQL queries

SQL—The Declarative Language

```
SELECT dstip as destination_ip, count(*) as Session
FROM $log WHERE $filter and dstip is not null GROUP
BY dstip ORDER BY session desc LIMIT 7
```

- SQL is a *declarative* language: describes *what* needs to be done rather than *how* to do it
- All information in the database is represented as tables
  - Each table consists of a set of rows and columns
  - Two types of tables: user tables and system tables
- A *record* is a single row in a table

Basic Data Manipulation Constructs

This is the *only* query statement used by FortiAnalyzer for reports

Select

- Retrieve and display data from one or more database tables (read-only query)
- `SELECT ... FROM ... WHERE`

Insert

- Add new rows of data into a table
- `INSERT INTO ... VALUES ...`

Update

- Modify existing data in a table
- `UPDATE ... SET ... WHERE`

Delete

- Remove rows of data from a table
- `DELETE FROM ... WHERE`

These elements are not used *for reports*

SELECT Statement

Clauses	Definition
`FROM`	From which tables or views the data will be extracted
`WHERE`	Sets the conditions (only rows that satisfy the conditions appear in the output)
`GROUP BY`	Collects data across multiple records and groups the results by one or more columns
`ORDER BY`	Orders the results by specific columns, ascending or descending
`LIMIT`	Limits the number of records returned based on a limit value
`OFFSET`	Often used with the `LIMIT` clause to offset the results by a set value

Following `SELECT`, you must use these clauses in a specific sequence

SELECT Statement (Contd)

Function	Definition
DISTINCT	Removes duplicate rows from the results
COALESCE	Returns the first non-null value from a list of expressions, or substitutes null with a default value
NULLIFNA	Filters out n/a values, often used with COALESCE
COUNT	Returns the number of rows that match the criteria
SUM	Returns the total sum of a column
AVG	Returns the average value of a column
MIN	Returns the minimum value of a column
MAX	Returns the maximum value of a column
FROM_DTIME	Returns the device timestamp without its time zone
FROM_ITIME	Returns FortiAnalyzer's timestamp without its time zone
AS	Creates an alias for a column or table
UPPER	Converts a string to uppercase letters
LOWER	Converts a string to lowercase letters

Accessing the SQL Schema

Reports > Report Definitions > Datasets

Name	Test Dataset
Log Type	Traffic
Query	1 `select * from $log`

Select log type

This query returns everything from the log type selected

Go Stop

Time Period	Previous 7 Days
Devices	All Devices

Column headings indicate what is available in the database schema for the log type selected

id	bid	dvid	itime	dtime	euid	epid	dsteuid	dstepid	logflag	logver
7285771809847446860	650012	1064	1696350940	1696325646	3	104	3	1032		704012463

Accessing the SQL Schema (Contd)

Name	Test Dataset
Log Type	Traffic
Query	1 `select * from $log`

Hover your mouse over the hyperlink to display the schema

These are all the available fields you can use for queries from the **Traffic** log table

```
Table "Logs" has the following fields:

id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, logver,
sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srcip,
dstip, tranip, transip, srcport, dstport, tranport, transport, trandisp,
duration, proto, vrf, slot, sentbyte, rcvdbyte, sentdelta, rcvddelta,
sentpkt, rcvdpkt, logid, user, unauthuser, dstunauthuser, srcname, dstname,
group, service, app, appcat, fctuid, srcintfrole, dstintfrole, srcserver,
dstserver, appid, appact, apprisk, wanoptapptype, policytype, centralnatid,
channel, vwpvlanid, shapingpolicyid, eventtime, vwlid, shaperdropsentbyte,
shaperdroprcvdbyte, shaperperipdropbyte, wanin, wanout, lanin, lanout,
crscore, craction, crlevel, countapp, countav, countdlp, countemail,
countips, countweb, countwaf, countssl, countssh, countdns, srcuuid, dstuuid,
poluuid, srcmac, mastersrcmac, dstmac, masterdstmac, srchwvendor,
srchwversion, srcfamily, srcswversion, dsthwvendor, dsthwversion, dstfamily,
dstswversion, devtype, devcategory, dstdevtype, dstdevcategory, osname,
osversion, dstosname, dstosversion, srccountry, dstcountry, srcssid, dstssid,
srcintf, dstintf, srcinetsvc, dstinetsvc, unauthusersource,
dstunauthusersource, authserver, applist, vpn, vpntype, radioband,
policyname, policymode, sslaction, url, agent, comment, ap, apsn, vwlservice,
vwlquality, collectedemail, dstcollectedemail, shapersentname,
shaperrcvdname, shaperperipname, msg, custom_field1, utmevent, utmsubtype,
sender, recipient, virus, attack, hostname, catdesc, dlpsensor, utmref,
tdinfoid, dstowner, tdtype, tdscantime, tdthreattype, tdthreatname, tdwfcate,
threatwgts, threatcnts, threatlvls, saasinfo, ebtime, clouduser, threats,
threattyps, apps, countff, identifier, securityid, securityact, tz,
srcdomain, counticap, dstregion, srcregion, dstcity, srccity, signal, snr,
dstauthserver, dstgroup, dstuser, tunnelid, vwlname, srcthreatfeed,
dstthreatfeed, psrcport, pdstport, countsctpf, srcreputation, dstreputation,
vip, accessproxy, gatewayid, clientdeviceid, clientdeviceowner,
clientdevicetags, httpmethod, referralurl, saasname, srcmacvendor,
shapingpolicyname, accessctrl, countcifs, proxyapptype,
clientdevicemanageable, emsconnection, realserverid, fwdsrv, replydstintf,
replysrcintf, countvpatch, countcasb, devid, vd, devname, csf, devgrps
```

Accessing the SQL Schema (Contd)

- `srcip` and `srcport` chosen from the schema

```
Table "Logs" has the following fields:

sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srcip,
dstip, tranip, transip, srcport, dstport, tranport, transport, trandisp,
```

- Sample query using `srcip` and `srcport`

```
select srcip as "Source IP", srcport as "Source Port"
from $log
where $filter and srcip = '10.0.1.10'
group by srcip, srcport
order by srcport desc
```

- Results

Source IP	Source Port
10.0.1.10	60999
10.0.1.10	60998
10.0.1.10	60993

Example Query

- Data populates a chart
- Datasets are SQL SELECT queries, used to extract data from the database
- The keywords from the previous slides are in **purple**

Chart

Name	Top 5 Attacks by Severity
Description	Top 5 attacks by severity
Dataset	threat-Attacks-By-Severity

Dataset

Name	threat-Attacks-By-Severity
Log Type	Intrusion Prevention
Query	

```
1 select (case when severity='critical' then
'Critical' when severity='high' then 'High' when
severity='medium' then 'Medium' when severity='low'
then 'Low' when severity='info' then 'Info' end) as
severity, count(*) as totalnum from $log where
$filter group by severity order by totalnum desc
```

FORTINET Training Institute

Knowledge Check

1. Which clause is required after a `SELECT` statement?
   - ✓ A. FROM
   - B. WHERE

2. If `ORDER BY` is not specified, what is the default sorting setting?
   - A. Ascending
   - ✓ B. No sorting

Lesson Overview

- ✓ Report Introduction
- ✓ SQL Queries
- Report Configuration
- Report Customization

Report Configuration

Objectives

- Configure datasets
- Configure charts
- Configure macros

If Predefined Charts or Datasets Do Not Meet Requirements

- By default, the **Chart Library** contains hundreds of charts, and the **Datasets** library contains hundreds of datasets
  - Can’t edit default charts and datasets
- However, just like templates and reports, you can clone and edit both charts and datasets, and create new ones
- Gives you the flexibility to pull a unique combination of data from the database that doesn’t exist in any default chart or dataset

Configuring a Dataset

- Define a name and log type
- Define your SQL query

Reports > Report Definitions > Datasets

Name: threat-Top-Attacks-Blocked

Log Type: Intrusion Prevention

Query:

```
select attack, count(*) as attack_count from $log
where $filter and nullifna(attack) is not null
and action not in ('detected', 'pass_session')
group by attack order by attack_count desc
```

Recommendations

Validate | Analyze Query | Format

Formatting a Query

Reports > Report Definitions > Datasets

Query

```
1 select attack, count(*) as attack_count from $log
  where $filter and nullifna(attack) is not null
  and action not in ('detected', 'pass_session')
  group  by attack order by attack_count desc
```

Recommendations

Validate | Analyze Query | Format

Click **Format** to change the query display to a readable format

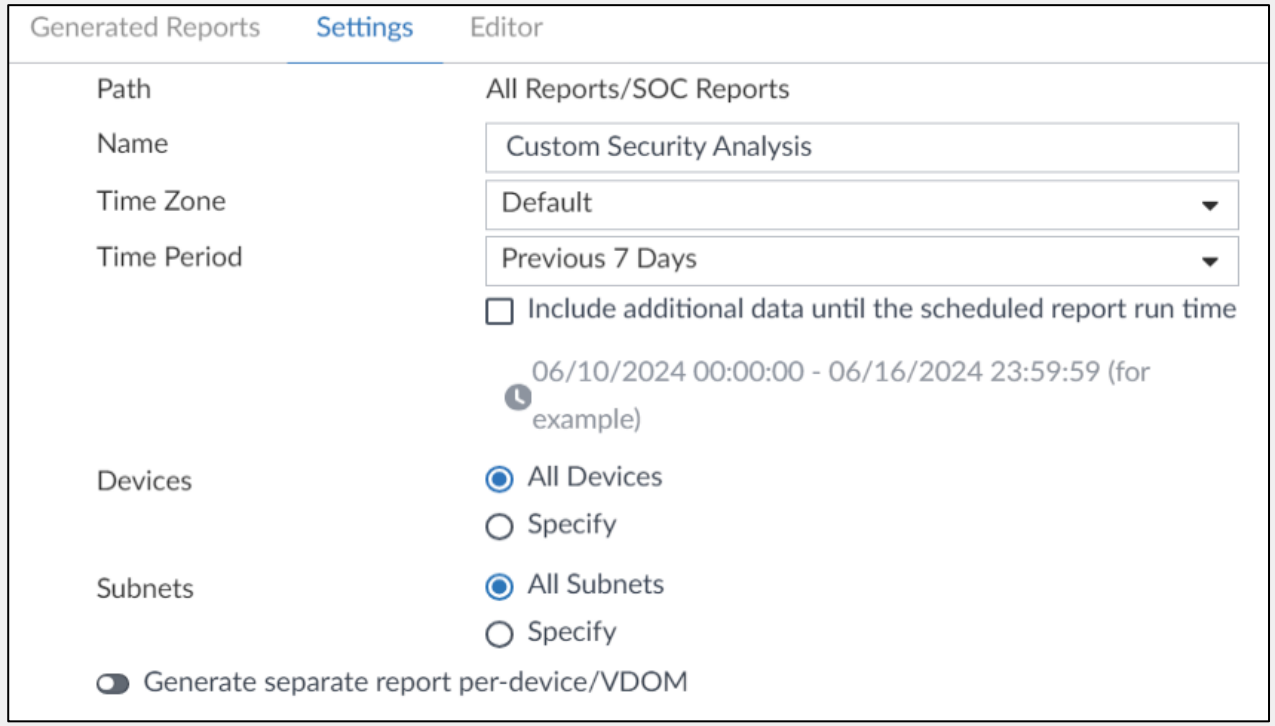
```
SELECT
  attack,
  count(*) AS attack_count
FROM
  $log
WHERE
  $filter
  AND nullifna(attack) IS NOT NULL
  AND ACTION NOT IN ('detected', 'pass_session')
GROUP BY
  attack
ORDER BY
  attack_count DESC
```

FORTINET Training Institute

Specificity in the Dataset

- Use specific SQL queries to retrieve the exact logs you want without further filtering
- The downside is that if you need to adjust the filters (such as the device), you must change the SQL query
- Alternatively, specify filters in the report instead of the dataset so that you can use one dataset to generate different reports

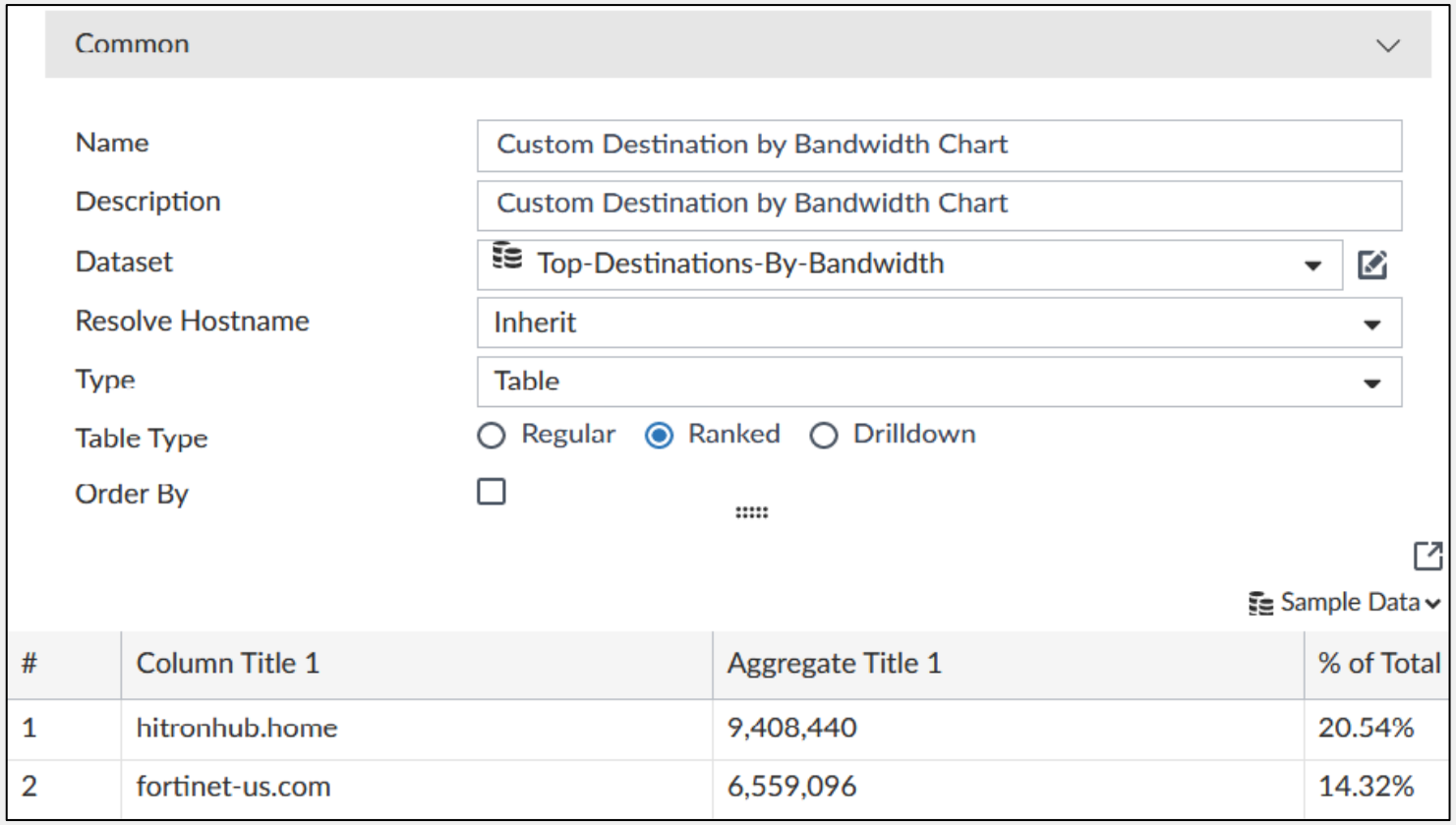
Reports > Report Definitions > All Reports > Settings



Configuring a New Chart

- Define a name, description (optional)
- Pick a dataset
- Pick a chart type
- Inherit, disable, or enable hostname resolution
- Toggle between **Sample Data** and **Real Data** in the preview section

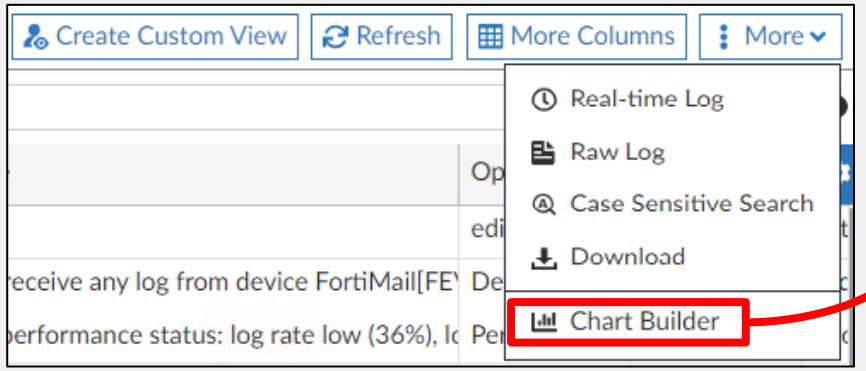
Reports > Report Definitions > Chart Library

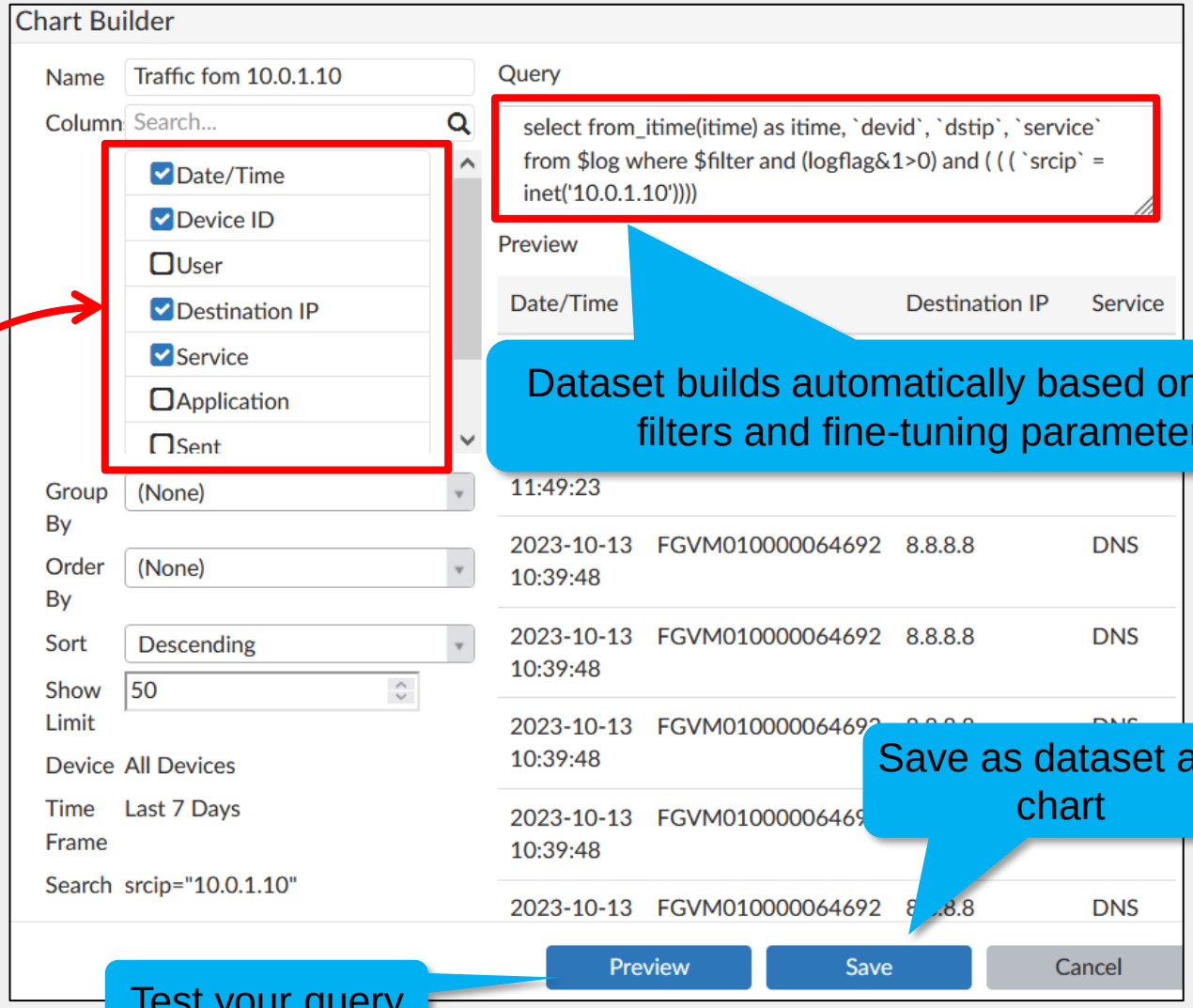


Building Datasets and Charts From Search Results

- In **Log View**, set filters to search for logs and then use the chart builder

Log View > More > Chart Builder





Dataset builds automatically based on search filters and fine-tuning parameters

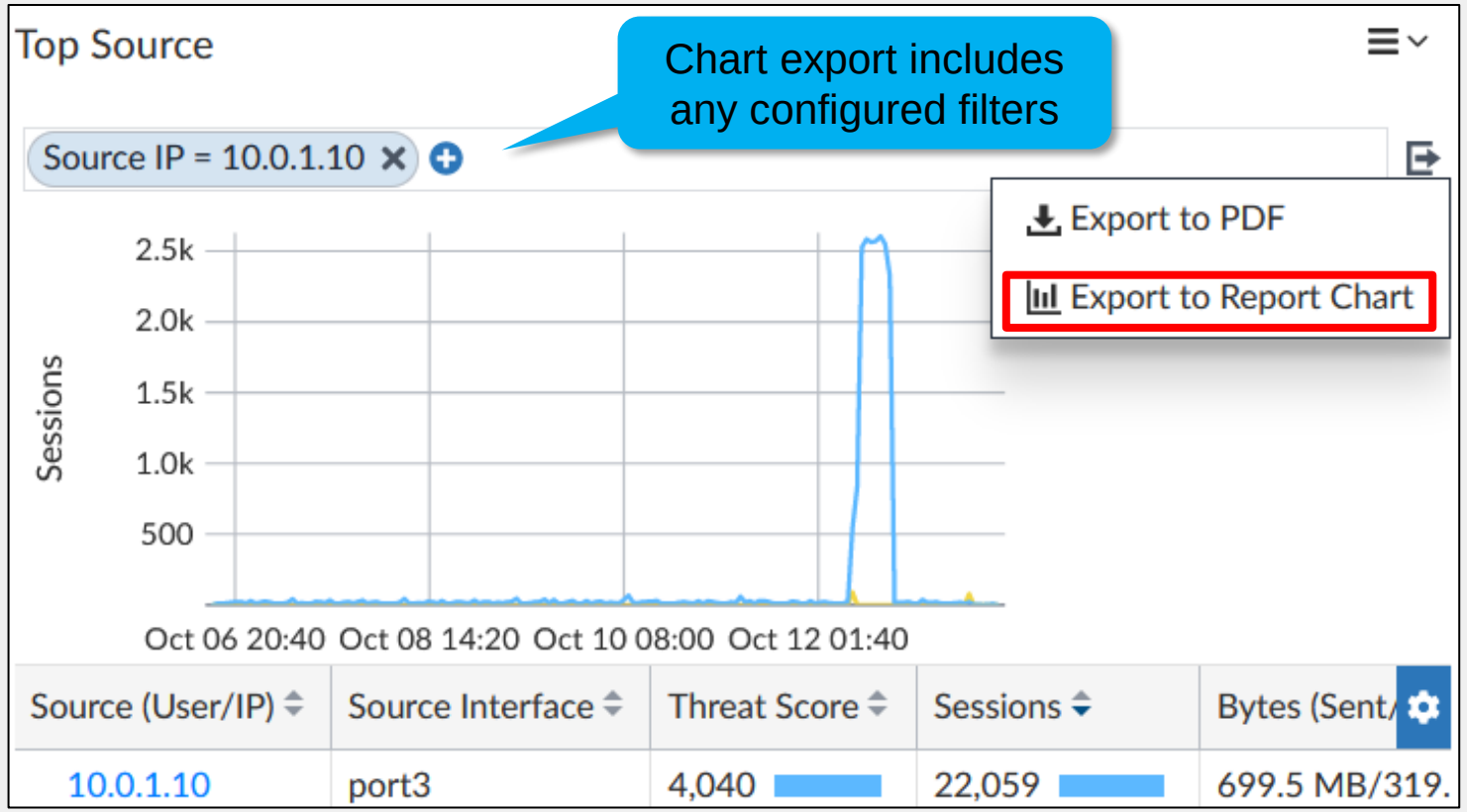
Save as dataset and chart

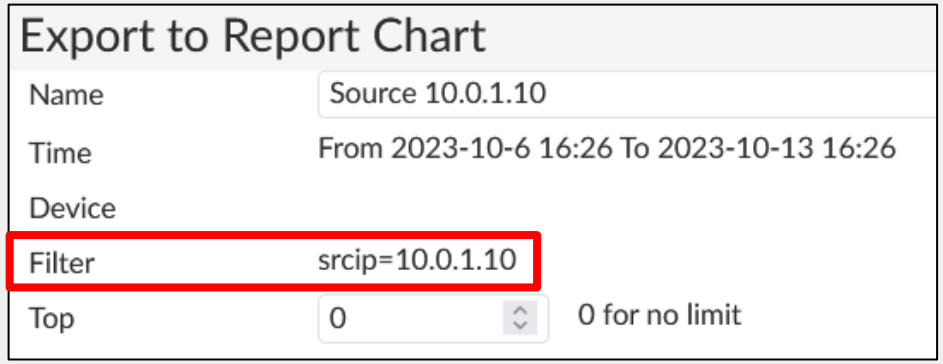
Test your query

Export a Chart From FortiView

- Similar to the **Chart Builder** feature in **Log View**, you can export a chart from **FortiView**

FortiView





Macros

- Macros output query results in abbreviated form

Reports > Report Definitions > Macro Library

Name	Total Destination Count
Description	Total Destination Count
Dataset	bandwidth-app-Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count total_endpoint, count(distinct dstip) as total_
Data Binding	total_dest
Display	Counter (K/M/G)

The total number of destinations is 68 , and the average session count is 46.09 K .

- Insert macros as data into templates and reports

Generated Reports | Settings | Editor

Insert Chart | Insert Macro | Normal | Font | Size

Save as Template | Find | Replace | Replace All

The total number of destinations is [Total Destination Co...] , and the average session count is [Average Session Cou...] .

Output

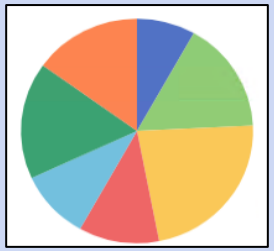
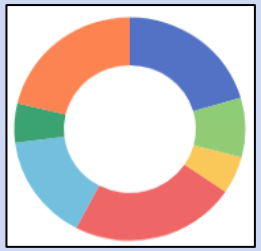
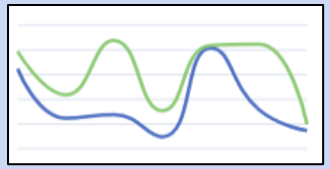
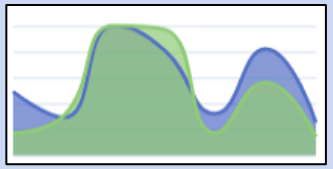
Configuring Macros

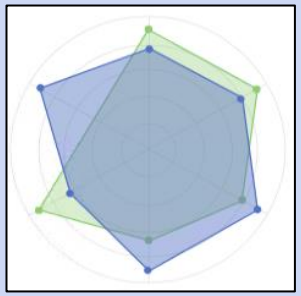
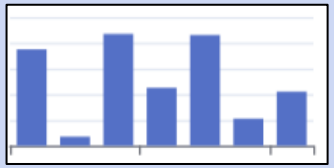
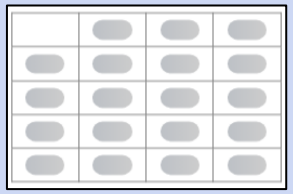
- **Name**, **Description**: Type a name and description (optional)
- **Dataset**: Pick an existing dataset
- **Query**: Displays the dataset query
- **Data Binding**: Select a field in the results of the query to bind the macro
- **Display**: Select how the macro will display the data

Reports > Report Definitions > Macro Library

Name	Total Session Count
Description	Total Number of Sessions
Dataset	bandwidth-app-Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count(distinct appcat) as total_appcat, count(distinct user_src) as total_users, count(distinct
Data Binding	total_sessions
Display	Counter (K/M/G)

Chart Types

Pie	Donut	Sankey	Line	Area
				

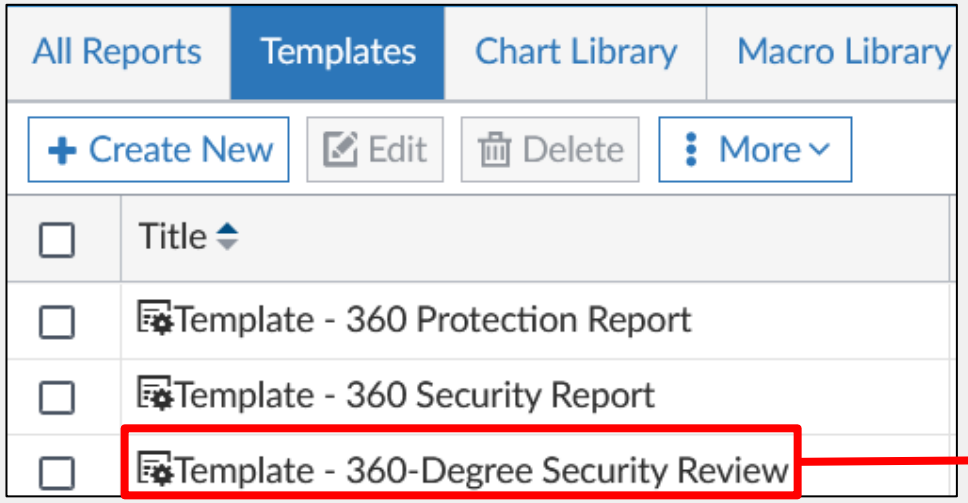
Radar	Bubble	Bubble Ring	Bar	Table
				

Templates

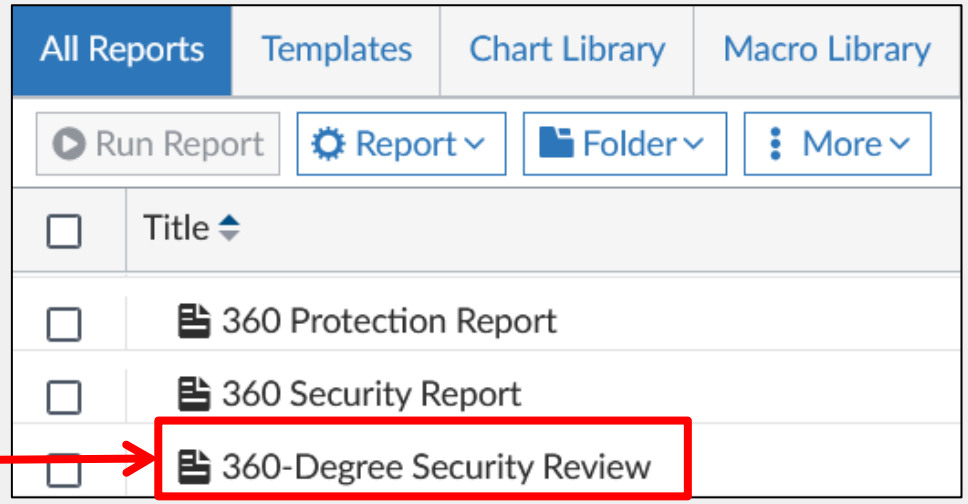
- A template specifies the layout—text, charts, and macros—to include in the report that uses it

- FortiAnalyzer provides predefined templates (which match the predefined reports)
  - Can clone predefined templates or create custom templates
    - Can't edit or delete predefined templates

Reports > Report Definitions > Templates

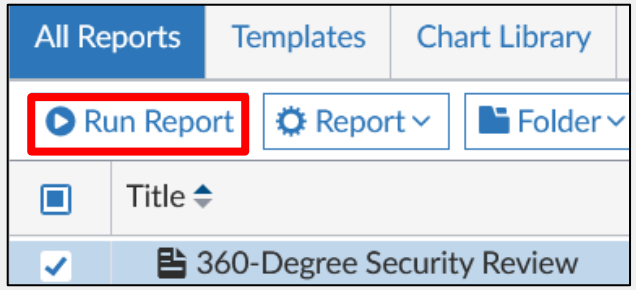


Reports > Report Definitions > All Reports

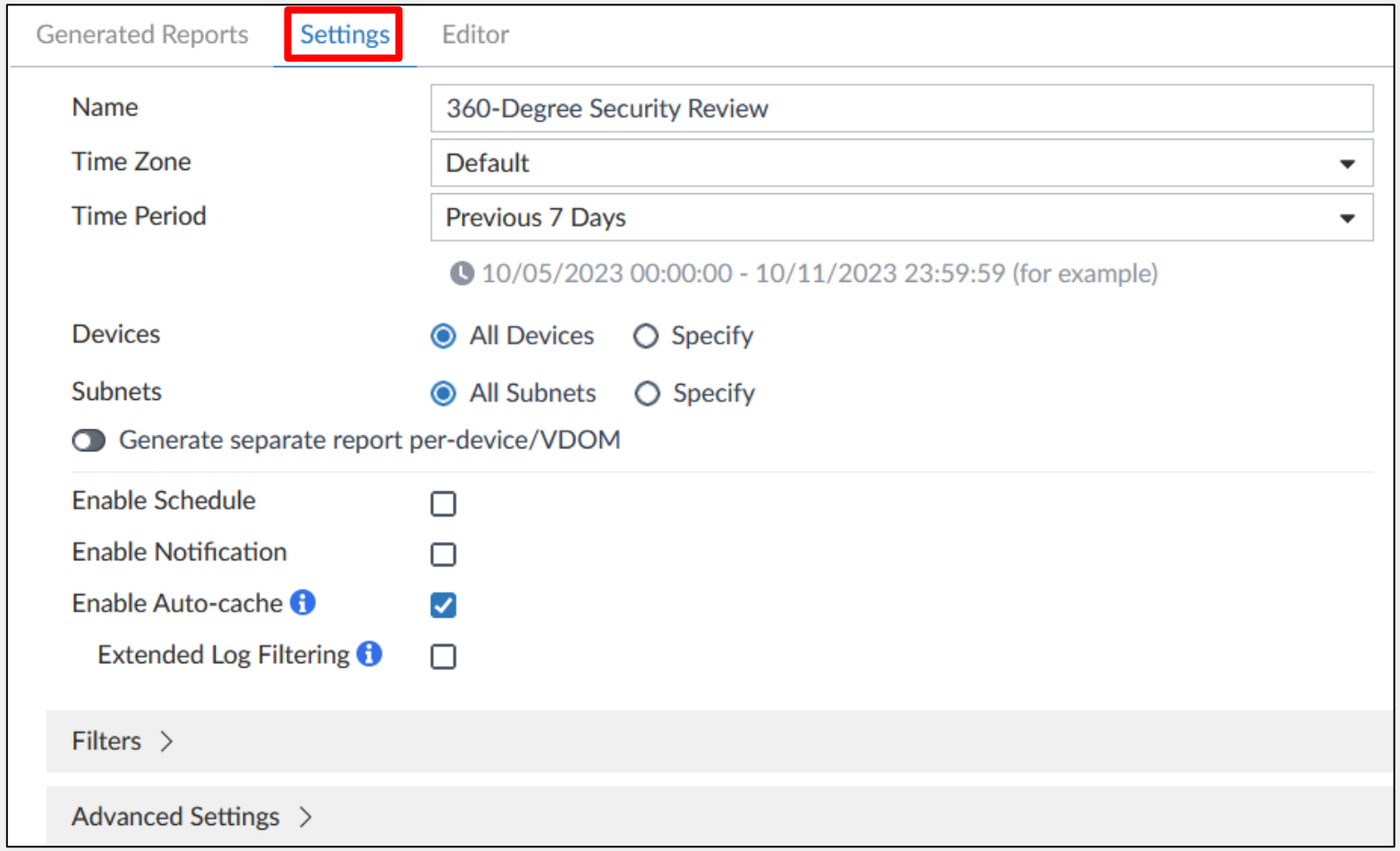


Running Predefined Reports

Reports > Report Definitions > All Reports



- Run reports with default settings



- Optionally, edit settings:
  - Time period
  - Devices
  - Filters
  - Report schedule (on demand or scheduled)

Running Predefined Reports (Contd)

- You can filter which logs to include in a report

Reports > Report Definitions > All Reports > Settings

Filters

Log messages that match ◉ All ○ Any of the Following Conditions

Log Field	Match Criteria	Value	Action
Severity (severity)	Equal To	critical	✖ +
& Destination Interface (dstintf)	Equal To	port3	✖ +

Note: You can also configure filters on the charts a report uses

- **Advanced Settings** allows you to change the report's appearance

Advanced Settings

Language	English
Bundle Rest into "Others"	Auto
Print Orientation	◉ Portrait ○ Landscape
Chart Heading Level	Heading 2
Default Font	Open Sans
Hide # Column	☑
Layout Header	☑
Header Text	
Header Image	Select Image fortinet_grey.png
Layout Footer	☑ ◉ Default ○ Custom
Print Cover Page	☑
Print Table of Contents	☑
Print Device List	☑ Compact
Display Device Name	By Device Name
Print Report Filters	☑
Obfuscate User	☐
Resolve Hostname	☐
Date Format	Default
Allow save maximum	99
Color Code	Purple
Report Owner	Click to select

FORTINET Training Institute

Knowledge Check

1. What is the main difference between charts and macros?
   A. Only charts use datasets.
   ✔ B. Macros output query results in abbreviated form.

Lesson Overview

- Report Introduction
- SQL Queries
- Report Configuration
- Report Customization

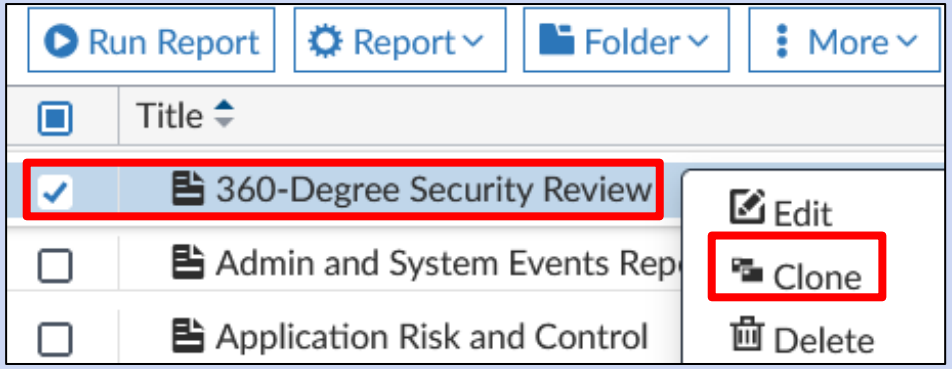
Report Customization

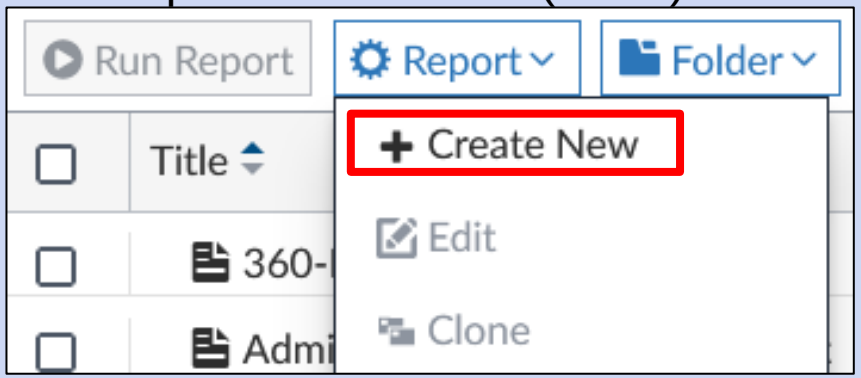
Objectives

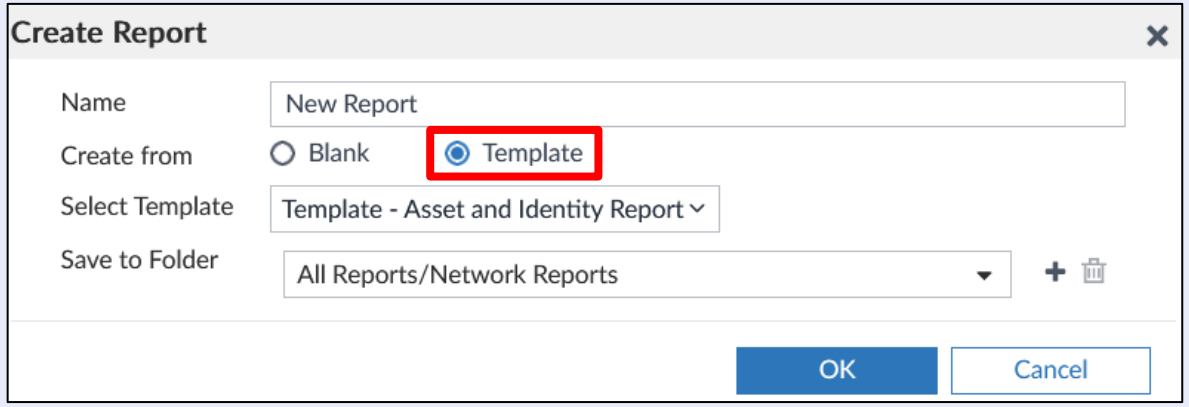
- Describe report customization options
- Configure and generate custom reports

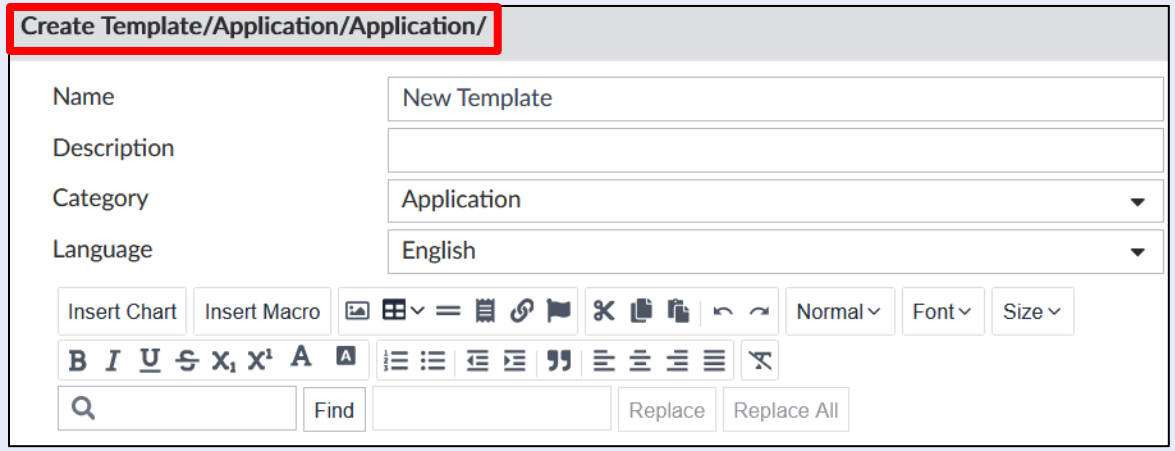
Customization—Template vs. Report

Minor/Moderate Customizations	Major Customizations
Clone a report or template, then edit the clone	Create a new report from scratch (blank)
Create a new report from an existing template, then edit	Create a new template (to use in a report)





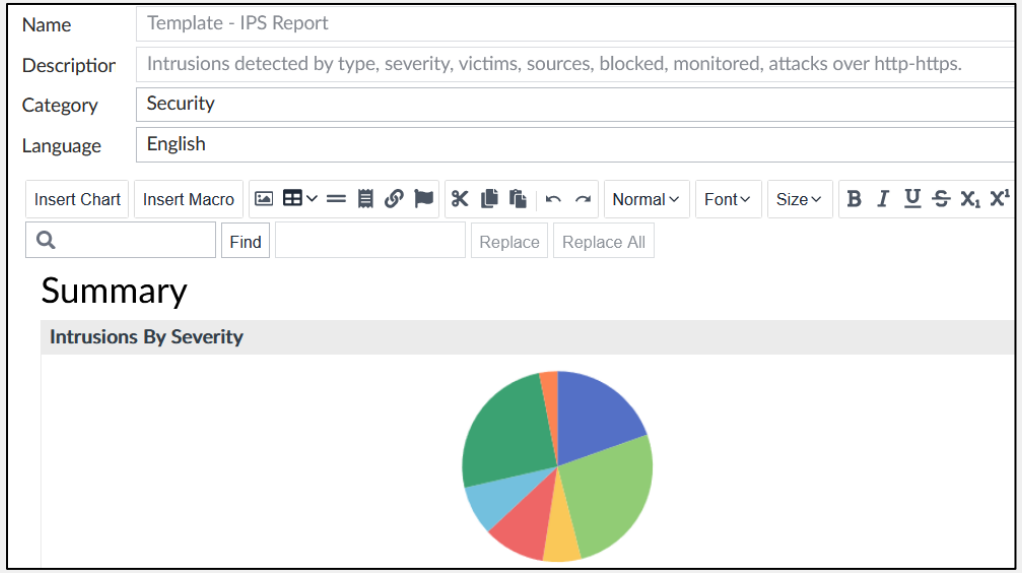




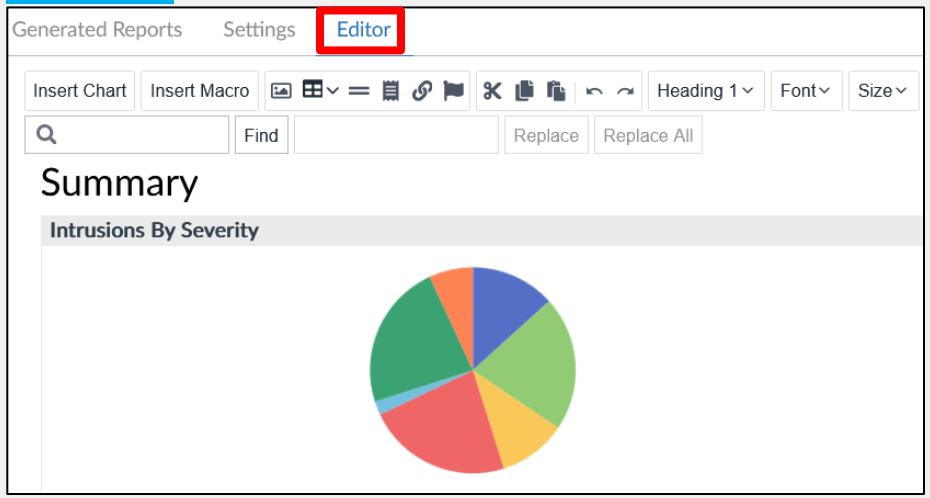
Customization—Template vs. Report (Contd)

- Which customization approach to take: template or report?
- Most important difference: templates only include the layout of the report, but not report settings (basic or advanced)
- Best practice is to approach it from an efficiency and needs standpoint
- Think about:
  - The amount of customization you need
  - Whether you want to preserve report settings
  - Whether you want to use the layout for one report or many reports

Template



Report



Report Customization Settings

Reports > Report Definitions > Settings > Advanced Settings

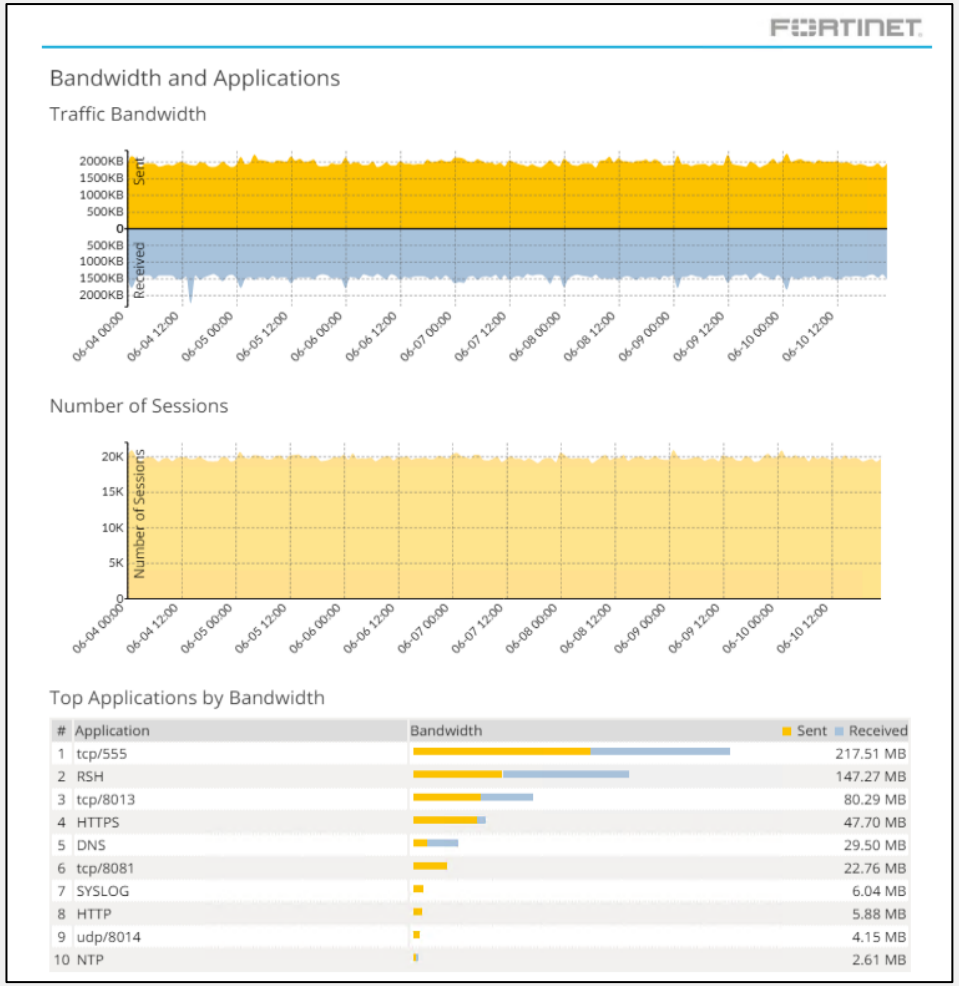
Advanced Settings

Language	English
Bundle Rest into "Others"	Auto
Print Orientation	○ Portrait ◉ Landscape
Chart Heading Level	Heading 2
Default Font	Open Sans
Hide # Column	☐
Layout Header	☐
Layout Footer	☐
Print Cover Page	☐
Print Table of Contents	☐
Print Device List	☐

Display Device Name	By Device Name
Print Report Filters	☑
Obfuscate User	☐
Resolve Hostname	☐
Date Format	Default
Allow save maximum	99
Color Code	Bold Blue
Report Owner	Click to select
Enable Report Filter Caching	☑
Enable High Accuracy Caching	☐

Report Customization Settings (Contd)

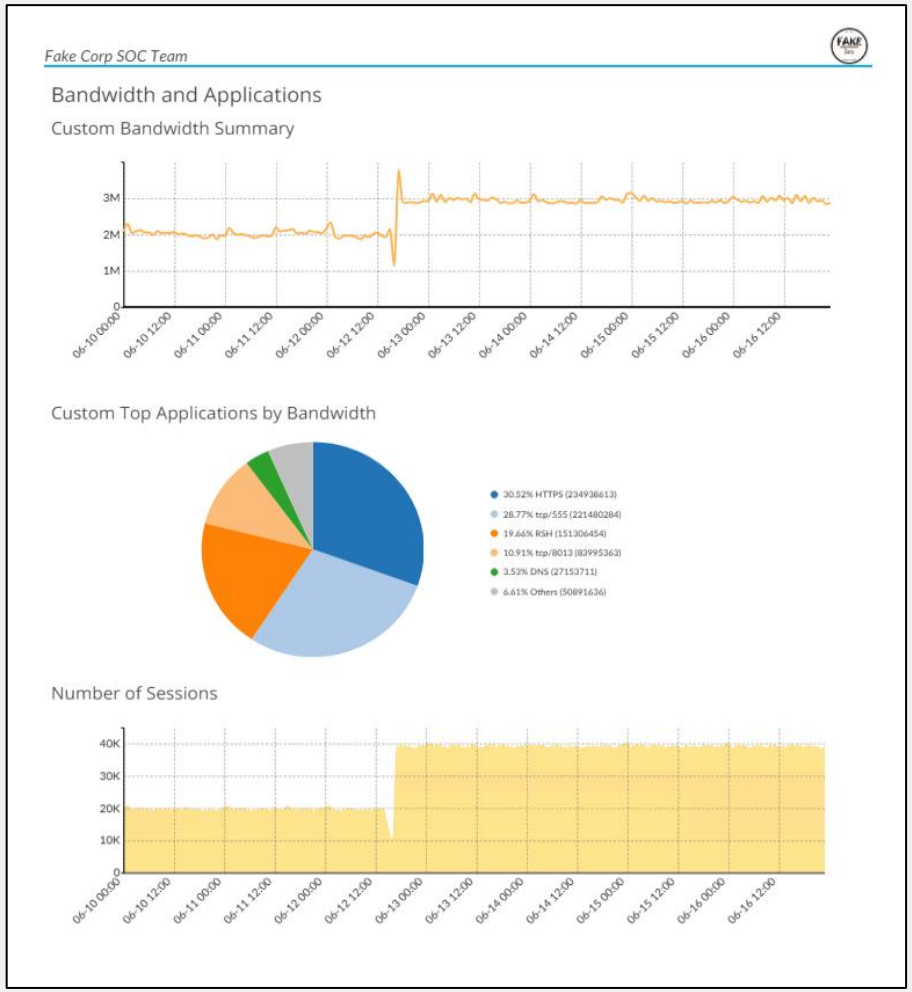
Reports > Generated Reports



#	Application	Bandwidth (Sent / Received)
1	tcp/555	217.51 MB
2	RSH	147.27 MB
3	tcp/8013	80.29 MB
4	HTTPS	47.70 MB
5	DNS	29.50 MB
6	tcp/8081	22.76 MB
7	SYSLOG	6.04 MB
8	HTTP	5.88 MB
9	udp/8014	4.15 MB
10	NTP	2.61 MB

Report Customization Settings (Contd)

Reports > Generated Reports



Knowledge Check

1. Which element do templates not contain?
   - ✓ A. Report settings
   - B. Report layout

2. Which setting protects the privacy of users?
   - ✓ **A. Obfuscate User**
   - **B. Resolve Hostname**

Lesson Overview

- Report Introduction
- SQL Queries
- Report Configuration
- Report Customization

Review

- ✓ Describe the considerations of SOC reporting
- ✓ Review the basic components of a FortiAnalyzer report
- ✓ Describe SQL basics
- ✓ Describe FortiAnalyzer schemas
- ✓ Use FortiAnalyzer tools for simplifying SQL queries
- ✓ Configure datasets, charts, and macros
- ✓ Describe report customization options
- ✓ Configure and generate custom reports