FortiAnalyzer - New Features Guide

Version 6.2.3

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

March 18, 2020
FortiAnalyzer 6.2.3 New Features Guide
05-623-528940-20200318

TABLE OF CONTENTS

Change Log 4
FortiAnalyzer 6.2.3 New Features Guide 5
Other 6
Self-Harm Report for education 6
Using FortiNAC data in FortiAnalyzer reports 8

Change Log

Date	Change Description
2020-01-14	Initial release.
2020-03-18	Added Using FortiNAC data in FortiAnalyzer reports on page 8.

FortiAnalyzer 6.2.3 New Features Guide

This document describes the new features added to FortiAnalyzer 6.2.3. The FortiAnalyzer new features are organized into the following categories:

- Other on page 6

Other

This section lists the other new features added to FortiAnalyzer.

List of new features:

- Self-Harm Report for education on page 6
- Using FortiNAC data in FortiAnalyzer reports on page 8

Self-Harm Report for education

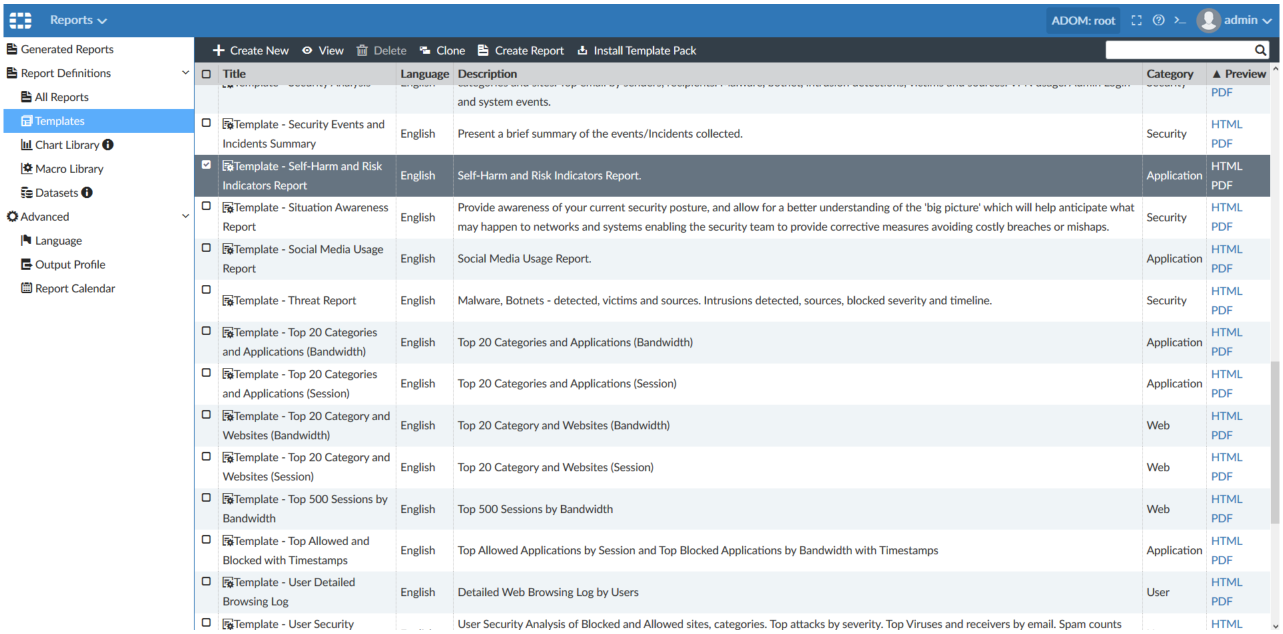
The *Self-Harm and Risk Indicators Report* monitors risky terms and phrases across all platforms.

The report template contains the following sections:

- Risky Term distribution across Platforms
- Top 10 Users logged with Risky Terms or Phrases
- Top 10 Users at Risk
- Top 10 Users with Risky Terms or Phrases
- Top 50 Risky Terms across the Time Frame
- Top 10 Users with Risky Terms or Phrases in Searches
- Top 50 Risky Terms used in Searches
- Top 10 Users with Risky Terms or Phrases in Facebook
- Top 10 Users with Risky Terms used in Tweets
- Top 50 Risky Terms used in Tweets
- Top 10 Users with Risky Terms used in Gmail Subjects and Google Chat
- Top 50 Risky Terms used in Gmail Subjects and Google Chat Messages

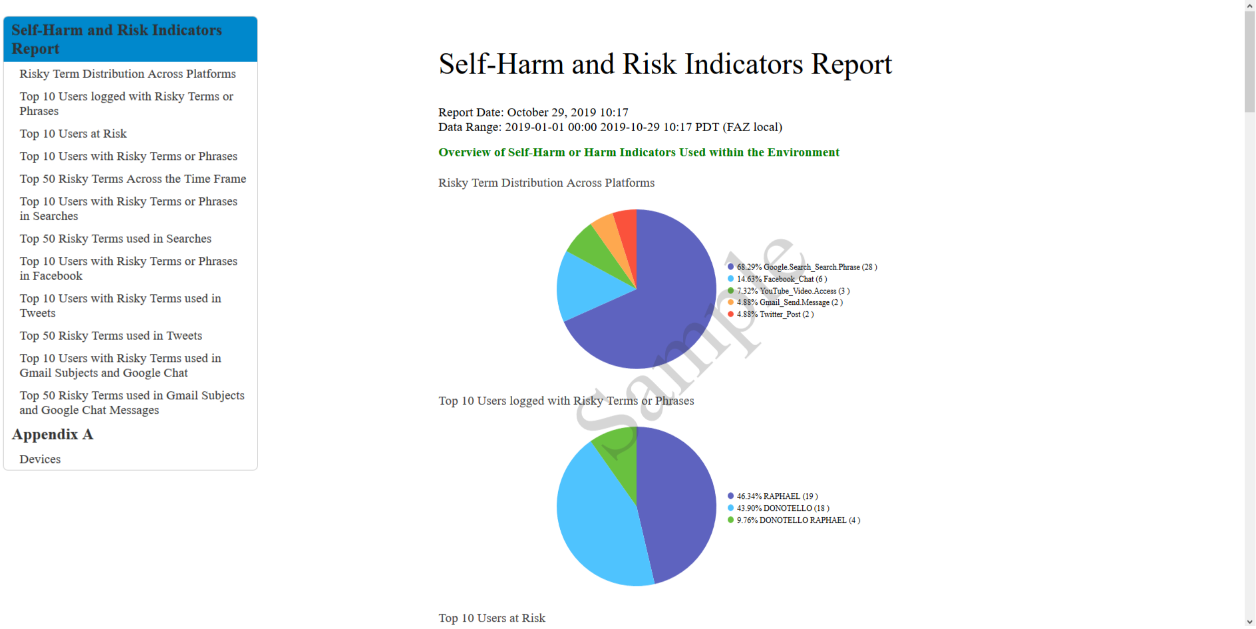
To view the Self-Harm and Risk Indicators Report template:

1. Go to *Reports* > *Templates*, then search for *Self-Harm and Risk Indicators Report*.



☐	Title	Language	Description	Category	▲ Preview
	Template - Security Analysis	English	categories and sites. Top email by senders, recipients. Malware, botnet, intrusion detections, victims and sources. VPN usage. Admin Login and system events.	Security	PDF
☐	Template - Security Events and Incidents Summary	English	Present a brief summary of the events/Incidents collected.	Security	HTML PDF
☑	Template - Self-Harm and Risk Indicators Report	English	Self-Harm and Risk Indicators Report.	Application	HTML PDF
☐	Template - Situation Awareness Report	English	Provide awareness of your current security posture, and allow for a better understanding of the 'big picture' which will help anticipate what may happen to networks and systems enabling the security team to provide corrective measures avoiding costly breaches or mishaps.	Security	HTML PDF
☐	Template - Social Media Usage Report	English	Social Media Usage Report.	Application	HTML PDF
☐	Template - Threat Report	English	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.	Security	HTML PDF
☐	Template - Top 20 Categories and Applications (Bandwidth)	English	Top 20 Categories and Applications (Bandwidth)	Application	HTML PDF
☐	Template - Top 20 Categories and Applications (Session)	English	Top 20 Categories and Applications (Session)	Application	HTML PDF
☐	Template - Top 20 Category and Websites (Bandwidth)	English	Top 20 Category and Websites (Bandwidth)	Web	HTML PDF
☐	Template - Top 20 Category and Websites (Session)	English	Top 20 Category and Websites (Session)	Web	HTML PDF
☐	Template - Top 500 Sessions by Bandwidth	English	Top 500 Sessions by Bandwidth	Web	HTML PDF
☐	Template - Top Allowed and Blocked with Timestamps	English	Top Allowed Applications by Session and Top Blocked Applications by Bandwidth with Timestamps	Application	HTML PDF
☐	Template - User Detailed Browsing Log	English	Detailed Web Browsing Log by Users	User	HTML PDF
☐	Template - User Security		User Security Analysis of Blocked and Allowed sites, categories. Top attacks by severity. Top Viruses and receivers by email. Spam counts		HTML

2. In the *Preview* column, click the *HTML* or *PDF* link to view sample output for the report.


Self-Harm and Risk Indicators Report
Risky Term Distribution Across Platforms
Top 10 Users logged with Risky Terms or Phrases
Top 10 Users at Risk
Top 10 Users with Risky Terms or Phrases
Top 50 Risky Terms Across the Time Frame
Top 10 Users with Risky Terms or Phrases in Searches
Top 50 Risky Terms used in Searches
Top 10 Users with Risky Terms or Phrases in Facebook
Top 10 Users with Risky Terms used in Tweets
Top 50 Risky Terms used in Tweets
Top 10 Users with Risky Terms used in Gmail Subjects and Google Chat
Top 50 Risky Terms used in Gmail Subjects and Google Chat Messages
Appendix A
Devices
68.29% Google.Search_Search.Phrase (28)
14.63% Facebook_Chat (6)
7.32% YouTube_Video.Access (3)
4.88% Gmail_Send.Message (2)
4.88% Twitter_Post (2)
Sample
46.34% RAPHAEL (19)
43.90% DONOTELLO (18)
9.76% DONOTELLO RAPHAEL (4)

Self-Harm and Risk Indicators Report

Report Date: October 29, 2019 10:17
Data Range: 2019-01-01 00:00 2019-10-29 10:17 PDT (FAZ local)

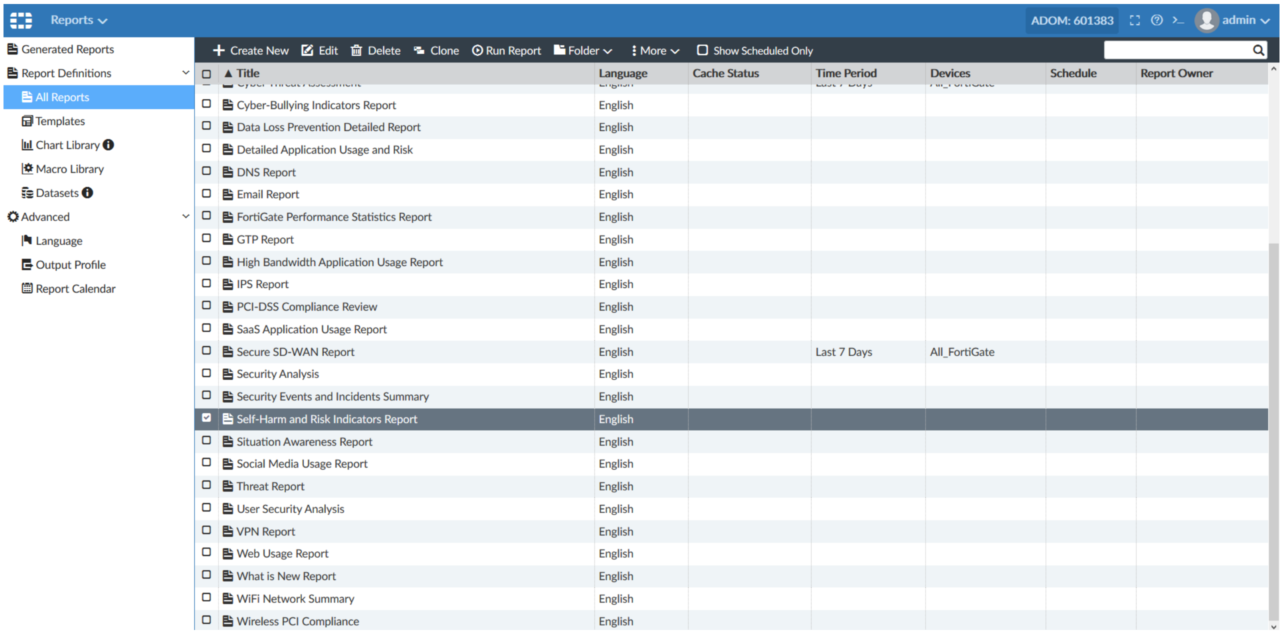
Overview of Self-Harm or Harm Indicators Used within the Environment

Risky Term Distribution Across Platforms

Top 10 Users logged with Risky Terms or Phrases

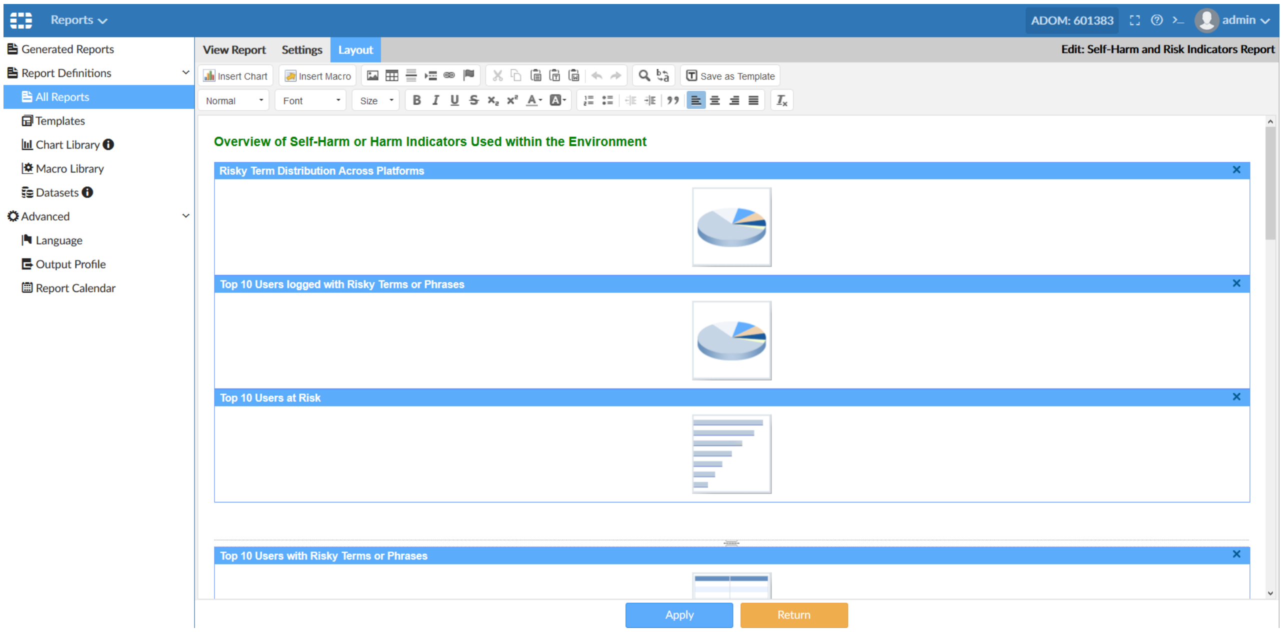
Top 10 Users at Risk

3. Click *All Reports* to edit, run, or view a completed report.



	Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner
□	Cyber Threat Assessment	English		Last 7 Days	All_FortiGate		
□	Cyber-Bullying Indicators Report	English					
□	Data Loss Prevention Detailed Report	English					
□	Detailed Application Usage and Risk	English					
□	DNS Report	English					
□	Email Report	English					
□	FortiGate Performance Statistics Report	English					
□	GTP Report	English					
□	High Bandwidth Application Usage Report	English					
□	IPS Report	English					
□	PCI-DSS Compliance Review	English					
□	SaaS Application Usage Report	English					
□	Secure SD-WAN Report	English		Last 7 Days	All_FortiGate		
□	Security Analysis	English					
□	Security Events and Incidents Summary	English					
☑	Self-Harm and Risk Indicators Report	English					
□	Situation Awareness Report	English					
□	Social Media Usage Report	English					
□	Threat Report	English					
□	User Security Analysis	English					
□	VPN Report	English					
□	Web Usage Report	English					
□	What is New Report	English					
□	WiFi Network Summary	English					
□	Wireless PCI Compliance	English					

4. Click the *Layout* tab in the report, then double-click a chart to customize it.



Edit: Self-Harm and Risk Indicators Report

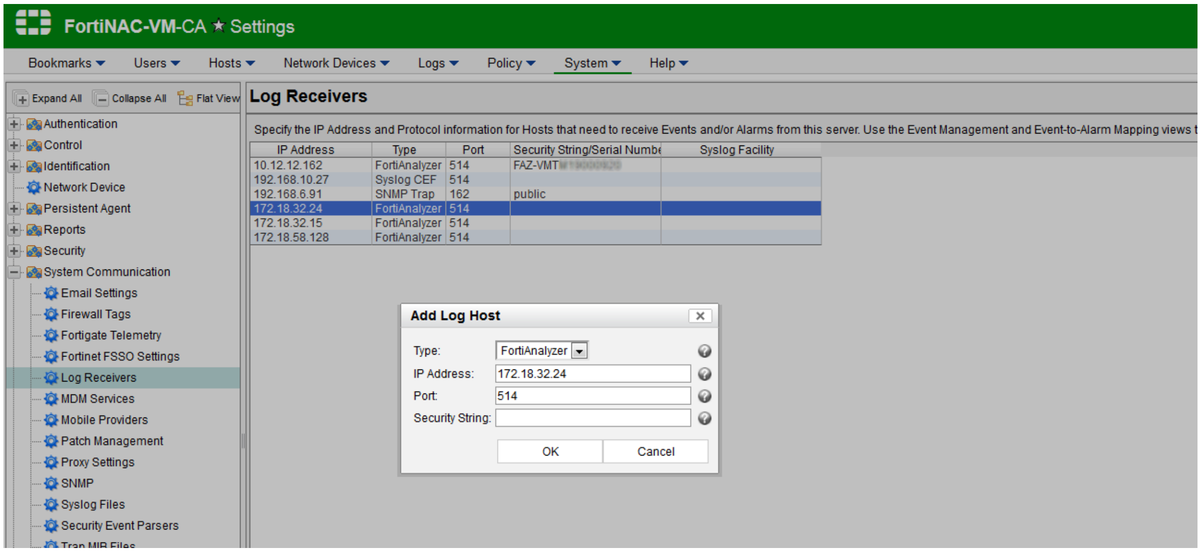
Overview of Self-Harm or Harm Indicators Used within the Environment

Using FortiNAC data in FortiAnalyzer reports

When authorized on FortiAnalyzer, FortiNAC sends data to FortiAnalyzer which can be used in reports.

To create FortiNAC reports on FortiAnalyzer:

1. Configure FortiNAC to send logs to FortiAnalyzer.
   Log in to FortiNAC and configure log receivers from *System* > *Settings* > *System Communication* > *Log Receivers*, and click *Add.*



Log Receivers

Specify the IP Address and Protocol information for Hosts that need to receive Events and/or Alarms from this server. Use the Event Management and Event-to-Alarm Mapping views t

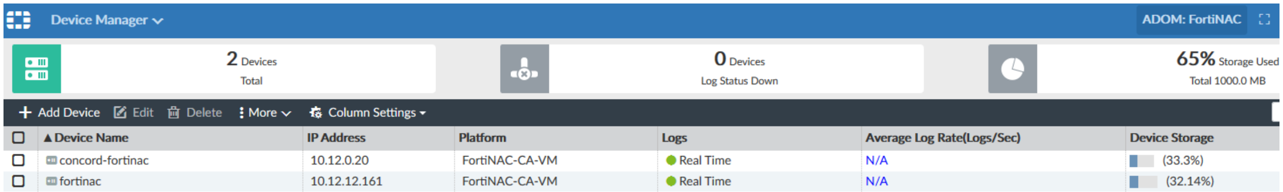
IP Address	Type	Port	Security String/Serial Numbe	Syslog Facility
10.12.12.162	FortiAnalyzer	514	FAZ-VMT[redacted]	
192.168.10.27	Syslog CEF	514		
192.168.6.91	SNMP Trap	162	public	
172.18.32.24	FortiAnalyzer	514		
172.18.32.15	FortiAnalyzer	514		
172.18.58.128	FortiAnalyzer	514		

Add Log Host

Type: FortiAnalyzer
IP Address: 172.18.32.24
Port: 514
Security String:

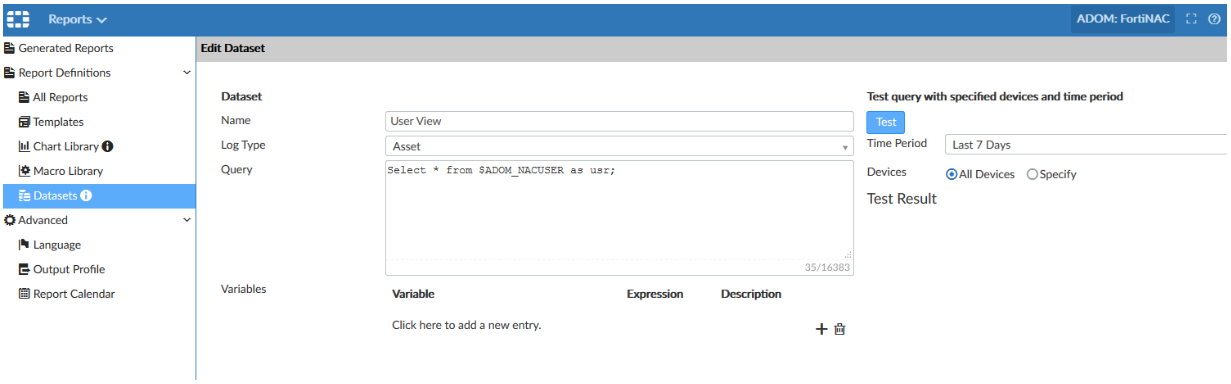
OK Cancel

2. On FortiAnalyzer, authorize the FortiNAC device on a Fabric ADOM.



□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage
□	concord-fortinac	10.12.0.20	FortiNAC-CA-VM	● Real Time	N/A	(33.3%)
□	fortinac	10.12.12.161	FortiNAC-CA-VM	● Real Time	N/A	(32.14%)

3. Create a new dataset.
   a. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
   b. Configure the dataset, including selecting a FortiNAC log type from the dropdown.
   c. Click OK.



Edit Dataset

Dataset

Name: User View
Log Type: Asset
Query:

```
Select * from $ADOM_NACUSER as usr;
```

35/16383

Variables

Variable	Expression	Description
Click here to add a new entry.		

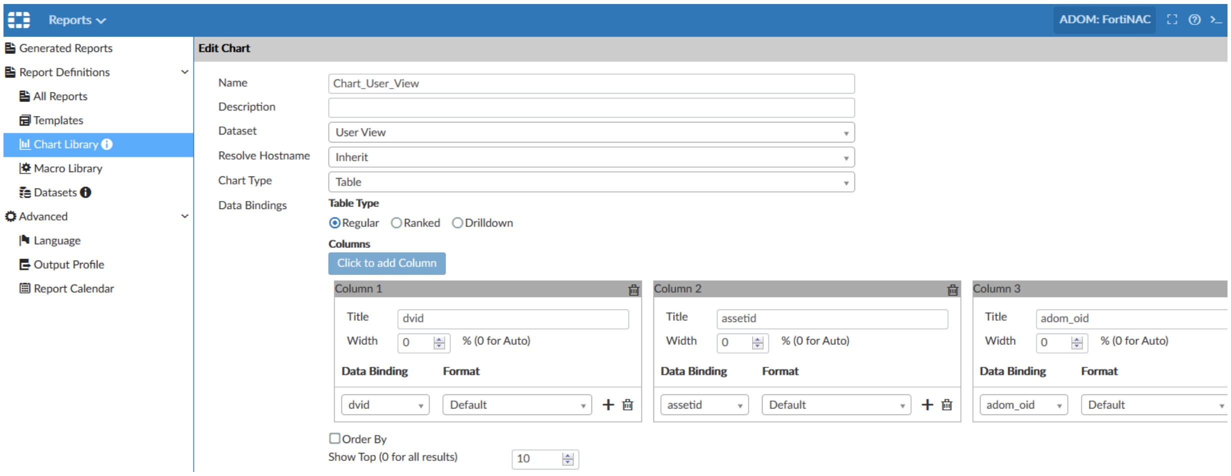
Test query with specified devices and time period

Time Period: Last 7 Days
Devices: ● All Devices ○ Specify

Test Result

4. Create a new chart using the dataset.
   a. Go to *Reports* > *Report Definitions* > *Chart Library*, and click *Create New*.
   b. Configure the chart, including selecting the previously configured dataset.

   c. Click OK.



Edit Chart

Name	Chart_User_View
Description	
Dataset	User View
Resolve Hostname	Inherit
Chart Type	Table
Data Bindings	Table Type ● Regular ○ Ranked ○ Drilldown

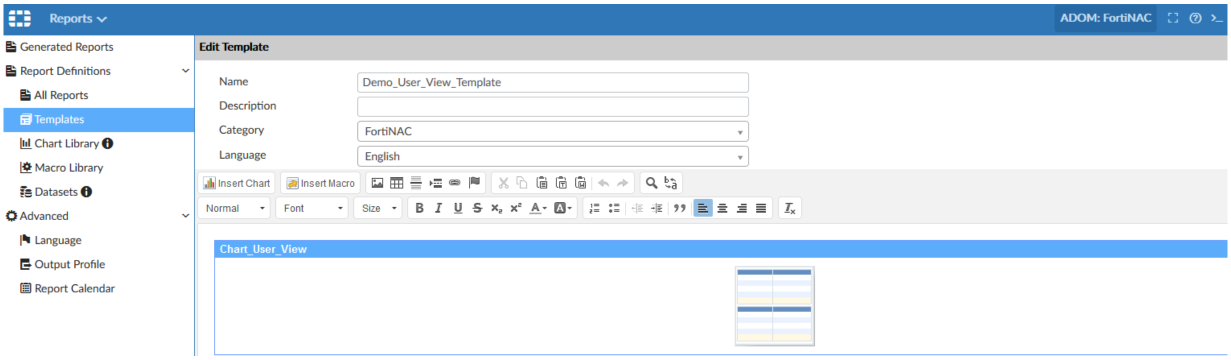
Columns

	Column 1	Column 2	Column 3
Title	dvid	assetid	adom_oid
Width	0 % (0 for Auto)	0 % (0 for Auto)	0 % (0 for Auto)
Data Binding	dvid	assetid	adom_oid
Format	Default	Default	Default

□ Order By

Show Top (0 for all results) 10

5. Create a new template using the chart.
   a. Go to *Reports* > *Report Definitions* > *Templates*, and click *Create New*.
   b. Configure the template fields as desired.
   c. Click *Insert Chart*, and locate the previously configured chart to insert it into the template.
   d. Click *OK*.



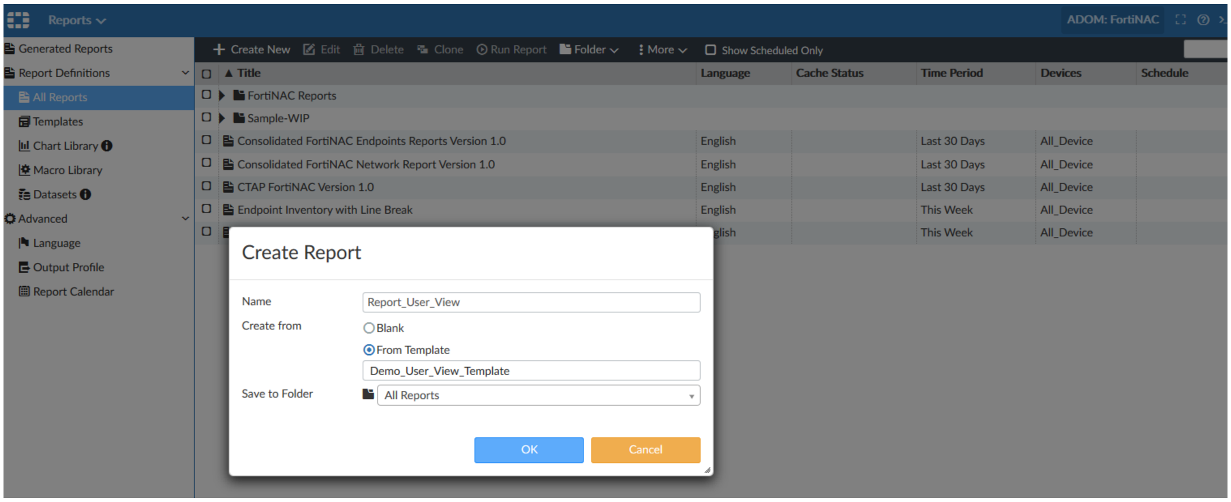
Edit Template

Name	Demo_User_View_Template
Description	
Category	FortiNAC
Language	English

Chart_User_View

6. Create a report using the template.
   a. Go to *Reports* > *Report Definitions* > *All Reports*, and click *Create New*.
   b. Configure the report details as desired.
   c. Click *From Template*, and select the previously created template.

d. Click *OK*.



□	Title	Language	Cache Status	Time Period	Devices	Schedule
□	FortiNAC Reports					
□	Sample-WIP					
□	Consolidated FortiNAC Endpoints Reports Version 1.0	English		Last 30 Days	All_Device	
□	Consolidated FortiNAC Network Report Version 1.0	English		Last 30 Days	All_Device	
□	CTAP FortiNAC Version 1.0	English		Last 30 Days	All_Device	
□	Endpoint Inventory with Line Break	English		This Week	All_Device	
□		lish		This Week	All_Device	

Create Report

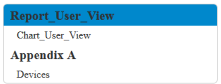
Name: Report_User_View

Create from: ○ Blank ● From Template

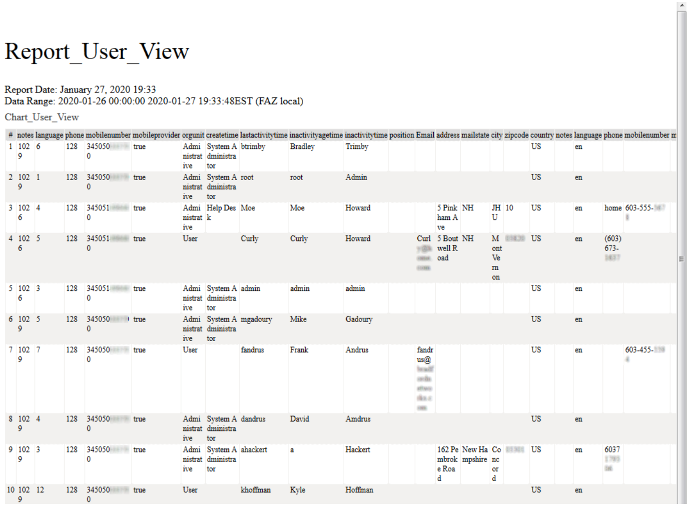
Demo_User_View_Template

Save to Folder: All Reports

7. Generate and view the report.



Report_User_View
Chart_User_View
Appendix A
Devices



Report_User_View

Report Date: January 27, 2020 19:33
Data Range: 2020-01-26 00:00:00 2020-01-27 19:33:48EST (FAZ local)

Chart_User_View

#	notes	language	phone	mobilenumber	mobileprovider	orgunit	createtime	lastactivitytime	inactivityagetime	inactivitytime	position	Email	address	mailstate	city	zipcode	country	notes	language	phone	mobilenumber	m
1	1029	6	128	345050[redacted]0	true	Administrative	System Administrator	btrimby	Bradley	Trimby							US		en			
2	1029	1	128	345050[redacted]0	true	Administrative	System Administrator	root	root	Admin							US		en			
3	1026	4	128	345051[redacted]0	true	Administrative	Help Desk	Moe	Moe	Howard			5 Pinkham Ave	NH	JHU	10	US		en	home	603-555-[redacted]	
4	1026	5	128	345051[redacted]0	true	User		Curly	Curly	Howard		Curl[redacted]	5 Boutwell Road	NH	Mont Vernon	[redacted]	US		en	(603) 673-[redacted]		
5	1026	3	128	345051[redacted]0	true	Administrative	System Administrator	admin	admin	admin							US		en			
6	1029	5	128	345050[redacted]0	true	Administrative	System Administrator	mgadoury	Mike	Gadoury							US		en			
7	1029	7	128	345050[redacted]0	true	User		fandrus	Frank	Andrus		fandrus@[redacted]					US		en		603-455-[redacted]	
8	1029	4	128	345050[redacted]0	true	Administrative	System Administrator	dandrus	David	Amdrus							US		en			
9	1029	3	128	345050[redacted]0	true	Administrative	System Administrator	ahackert	a	Hackert			162 Pembroke Road	New Hampshire	Concord	[redacted]	US		en	6037[redacted]		
10	1029	12	128	345050[redacted]0	true	User		khoffman	Kyle	Hoffman							US		en			