

**FORTINET**<sup>®</sup>



# FortiAnalyzer

Version 5.4

QuickStart Guide

## REGISTER FOR SUPPORT

### REGISTER YOUR FORTINET PRODUCT TO RECEIVE:

- Technical Support
- New product features
- Protection from new threats

### LA REISTRAZIONE TI PERMETTE DI USUFRUIRE DI:

- Supporto Tecnico
- Nuove funzionalità
- Protezione dalle ultime minacce

### VOUS DEVEZ ENREGISTRER LE PRODUIT POUR RECEVOIR:

- Support technique
- Nouvelles fonctionnalités du produit
- Protection contre de nouvelles menaces

### DEBE REGISTRAR EL PRODUCTO PARA RECIBIR:

- Apoyo técnico
- Nuevas funcionalidades del producto
- Protección contra ataques

### 登録のお願い

本日、フォーティネット製品の登録をしてください。  
登録すると次のメリットがあります。  
テクニカルサポート・新機能の追加・新しい脅威への防御

### 请马上注册

您的飞塔产品  
您在注册以后才能得到技术支持、新产品特点信息、最新威胁防护

### SUPPORT

<http://forti.net/support>

Toll free: 1 866 648 4638

Phone: 1 408 486 7899

Fax: 1 408 235 7737

November 03, 2016  
OS-541-370731-20160513

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



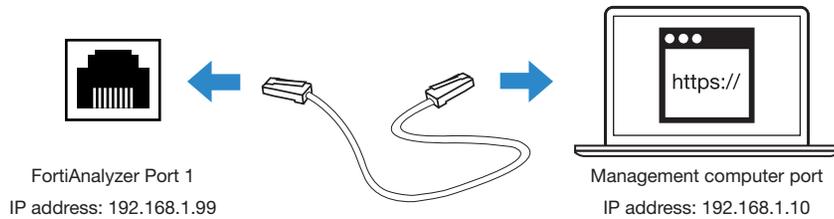
## DAY 1: SETUP

- Configure network settings and admin account
- Set up FortiGate to send logs
- View logs from Log View

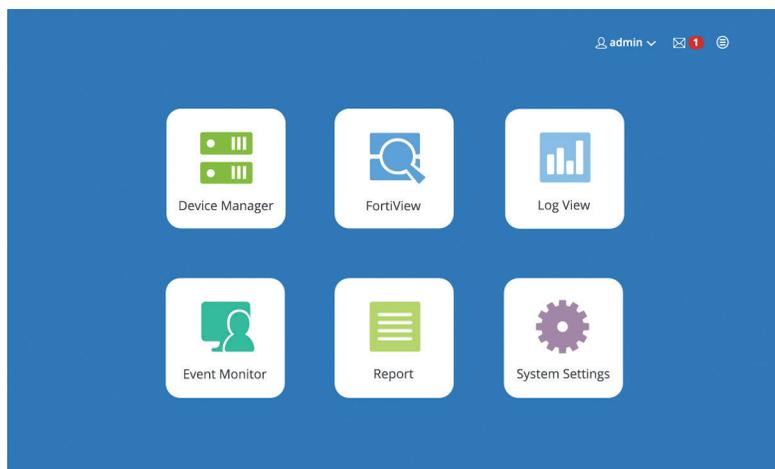
# 1 Set Up FortiAnalyzer

## Configure FortiAnalyzer Network Settings

1. Connect the FortiAnalyzer **Port 1** to the **Management computer port**.



2. Set the management computer to be on the same subnet as FortiAnalyzer.  
(The default is 192.168.1.99.)  
For Example:  
IP Address: 192.168.1.10  
Netmask: 255.255.255.0
3. Visit <https://192.168.1.99> in your web browser.
4. Log in with username **admin** and no password.



4

## Configure FortiAnalyzer Network Settings

1. Go to **System Settings > Network**.
2. Change the **IP address/Netmask** to your internal network.
3. Keep the default **Administrative Access** settings.
4. Specify a **Default Gateway**.
5. Change the IP address/Netmask of the management computer accordingly to reconnect it to FortiAnalyzer.

System Network Management Interface

Name: port1

IP Address/Netmask: 10.3.112.95/255.255.0.0

IPv6 Address: ::0

Administrative Access:  HTTPS  HTTP  PING  SSH  TELNET  SNMP  Web Service  Aggregator  FortiManager

IPv6 Administrative Access:  HTTPS  HTTP  PING  SSH  TELNET  SNMP  Web Service  Aggregator  FortiManager

Default Gateway: 172.16.96.1

Primary DNS Server: 172.16.100.100

Secondary DNS Server: 172.16.100.80

All Interfaces | Routing Table | IPv6 Routing Table

Apply

## Set Up Administrator Accounts

1. Go to **System Settings > Admin > Administrator**, and click **Create New** in the toolbar.
2. Enter user name and password.
3. Click **OK** to save the change.

New Administrator

User Name: admin\_john

Comments: 0/127

Admin Type: LOCAL

New Password: •••••

Confirm Password: •••••

Admin Profile: Super\_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

Trusted Hosts: OFF

User Information >

OK | Cancel



5

## Configure Log Storage Policy

1. Go to **System Settings > Dashboard**.
2. In the **System Information** widget, under **Log Storage Policy**, select **Edit Log Storage policy**.
  - Data Policy:
    - ▶ Set **Keep Logs for Analytics** to **90 days**.
    - ▶ Set **Keep Logs for Archive** to **180 days**.
  - Disk Utilization:
    - ▶ Keep the default values.

Edit Log Storage Policy - ADOM : root

Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1000 MB Out of Available: 63.6 GB

Analytics : Archive: 70% (30%)  Modify

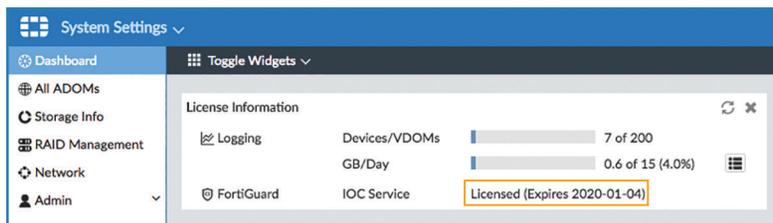
Alert and Delete When Usage Reaches: 90%

\*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

OK Cancel

You can monitor the log storage settings and adjust as you go.

## Check License and Registration

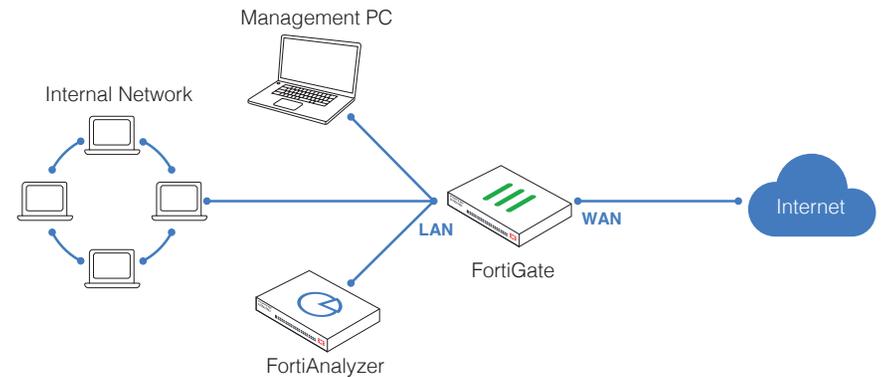


Check that you have a valid license for the **IOC Service**, to enable the feature.



6

## 2 Connect FortiGate to FortiAnalyzer



## Configure FortiGate Log Settings

1. Log in to the FortiGate GUI from the management computer.
2. Go to **Log & Report > Log Settings**.
  - Turn on **Send Logs to FortiAnalyzer/FortiManager**.
  - Enter the IP address of the FortiAnalyzer and click **Apply**.

Log Settings

Remote Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager

Use FortiManager

IP Address: 172.16.96.5 Test Connectivity

Upload Option: Store & Upload Logs Realtime



Don't click **Test Connectivity** yet. You need to register this FortiGate on the FortiAnalyzer first.



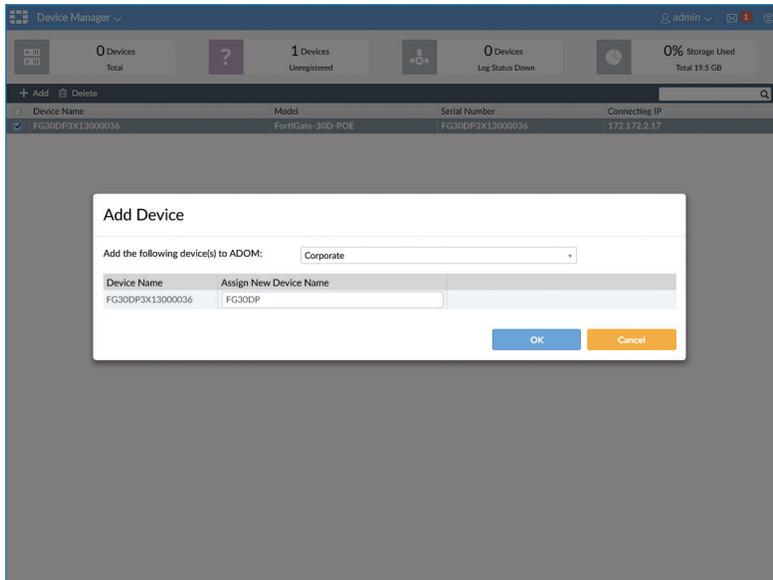
7

## Register FortiGate on FortiAnalyzer

- Go to **Device Manager** of FortiAnalyzer. Click the **Unregistered Devices** tab in the quick status bar.



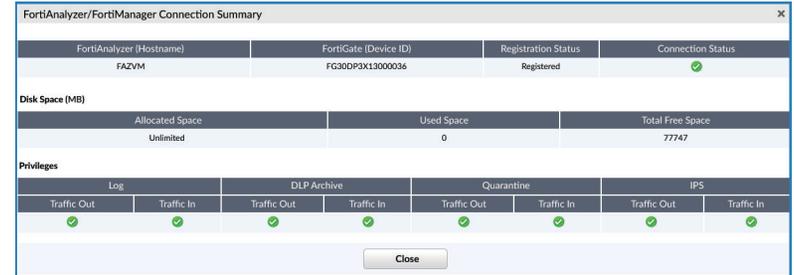
- Select the FortiGate device, and click **Add**.
- In the Add Device dialog box that opens, select the root ADOM, type a device name, and click **OK**.



8

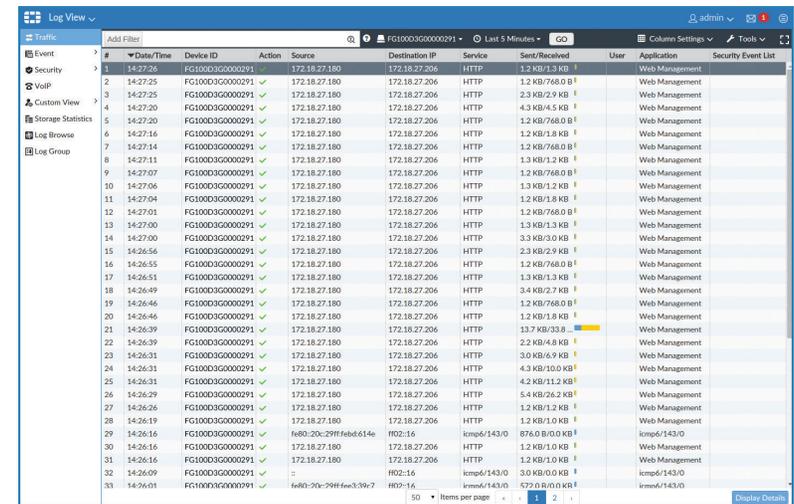
## Test Connectivity on FortiGate

- Go back to the Log Settings pane of FortiGate, and click **Test Connectivity**. If the connection is successfully established, a connection summary is shown.



## Verify Logs Being Received

- Go to **Log View** of the FortiAnalyzer. Select **Last 5 minutes** from the time period list and press **GO**. You should be able to see the FortiGate logs.



9



# DAY 2: NAVIGATE

- Interact with FortiView
- Generate reports
- Monitor events

## 1 Look into FortiView Summaries

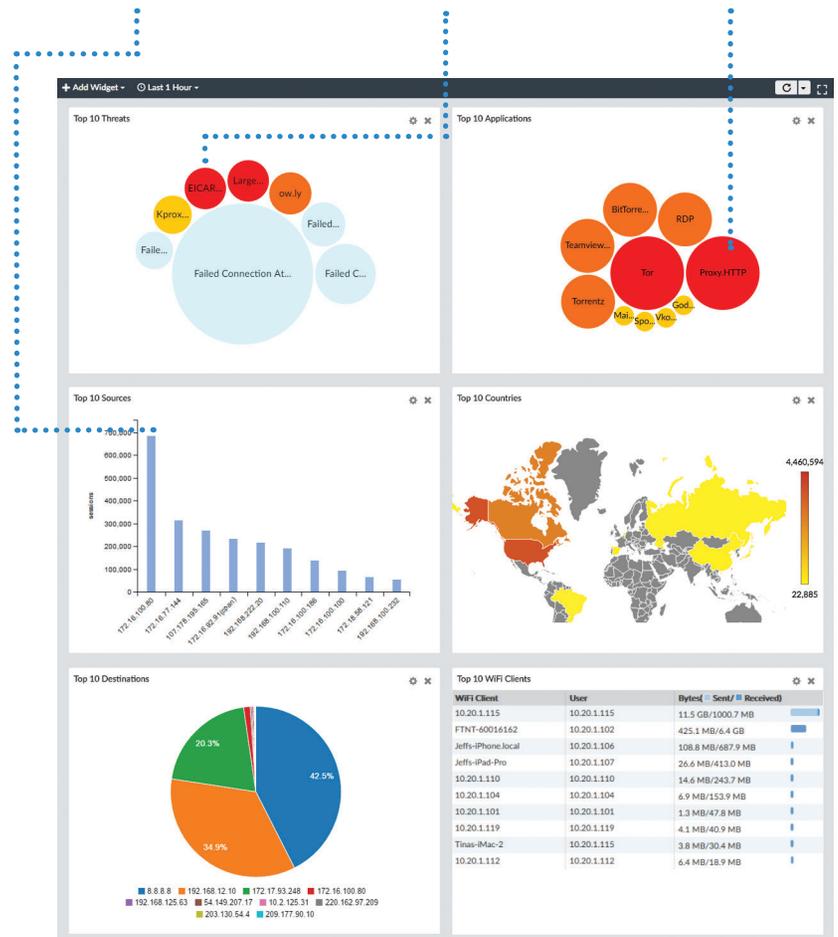
In FortiView, the Summary view provides different Fortinet summaries as widgets. You can customize the widgets being displayed, and also drill down into each widget for further info.

### FortiView Summary

Source IP 172.16.100.80 used the most bandwidth.

EICAR is the top threat to your network.

Torrent used the most bandwidth.

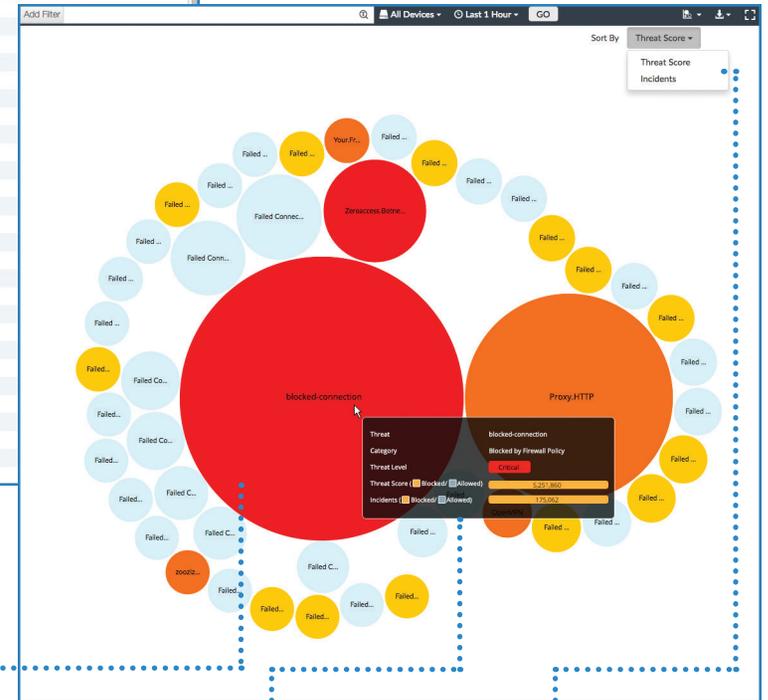


## Top Threats

Drill Down  
Double-click  
the entry.

Sort Entries  
Click a column  
heading.

Threat	Category	Threat Level	Threat Score (Blocked/# Allowed)	Incidents (Blocked/# Allowed)
blocked-connection	Blocked by Firewall Policy	Critical	5,251,860	175,062
Proxy.HTTP	Proxy	High	2,807,590	56,157
blocked-connection	Blocked by Firewall Policy	High	800,790	26,693
Zeroaccess.Botnet	Botnet	Critical	592,900	5,929
Failed Connection Attempts to 208.91.113.179	Failed Connection Attempts	Low	375,205	75,041
Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Low	259,635	51,927
Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Medium	191,400	38,280
Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Low	115,690	23,138
Failed Connection Attempts to 172.16.100.100	Failed Connection Attempts	Low	109,435	21,887
Failed Connection Attempts to 192.175.48.42	Failed Connection Attempts	Low	79,185	15,837
Failed Connection Attempts to 208.91.113.241	Failed Connection Attempts	Low	74,130	14,826
Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Medium	71,650	14,330
Failed Connection Attempts to 192.175.48.6	Failed Connection Attempts	Low	67,850	13,570
Failed Connection Attempts to 172.16.100.100	Failed Connection Attempts	Medium	60,620	12,124
Failed Connection Attempts to 208.91.113.206	Failed Connection Attempts	Low	51,835	10,367
Failed Connection Attempts to 208.91.113.104	Failed Connection Attempts	Low	50,895	10,179
OpenVPN	Proxy	High	46,440	1,526
Failed Connection Attempts to 172.16.86.107	Failed Connection Attempts	Medium	44,690	8,938
Failed Connection Attempts to 208.91.113.201	Failed Connection Attempts	Low	41,350	8,270
Failed Connection Attempts to 208.91.112.53	Failed Connection Attempts	Medium	40,630	8,126
Failed Connection Attempts to 172.16.86.91	Failed Connection Attempts	Medium	38,450	7,690
Failed Connection Attempts to 208.91.113.101	Failed Connection Attempts	Low	36,890	7,378
Failed Connection Attempts to 208.91.113.122	Failed Connection Attempts	Low	33,005	6,401
Failed Connection Attempts to 172.16.86.104	Failed Connection Attempts	Medium	30,960	6,192
Failed Connection Attempts to 192.168.224.161	Failed Connection Attempts	Low	29,315	5,863
Failed Connection Attempts to 172.16.86.241	Failed Connection Attempts	Medium	27,805	5,561
Failed Connection Attempts to 172.16.96.86	Failed Connection Attempts	Medium	27,140	5,428
Failed Connection Attempts to 192.168.224.162	Failed Connection Attempts	Low	26,295	5,259
Failed Connection Attempts to 107.167.16.11	Failed Connection Attempts	Low	25,875	5,175
Failed Connection Attempts to 2.2.2.2	Failed Connection Attempts	Medium	25,540	5,128
Failed Connection Attempts to 208.91.113.186	Failed Connection Attempts	Low	22,520	4,504
Your.Freedom	Proxy	High	18,170	457
Failed Connection Attempts to 12.12.12.123	Failed Connection Attempts	Medium	18,070	3,614
Failed Connection Attempts to 216.239.38.10	Failed Connection Attempts	Low	17,965	3,593
Failed Connection Attempts to 208.91.113.240	Failed Connection Attempts	Low	17,890	3,578
Failed Connection Attempts to 172.16.106.128	Failed Connection Attempts	Medium	16,685	3,337



Drill Down  
Double-click the graphical  
element.

Get an Overview  
Hover over a graphical  
element.

Sort Entries  
Select from the drop-down  
menu.

## Filter Data in FortiView

### Regular Search

Select a filter from the list and specify a value.



### Advanced Search

Click the icon to switch between regular and advanced search.

A screenshot of the FortiView main interface. The top navigation bar shows 'FortiView' and 'ADOM: root'. The left sidebar contains navigation options: Summary, Threats, Threat Map, IOC, Traffic, Applications & Websites, VPN, WiFi, System, and EndPoints. The main area displays a table of threat data with columns for Threat, Category, Threat Level, Threat Score, and Incidents. The table is filtered to show 'Failed Connection Attempts'.

Threat	Category	Threat Level	Threat Score (Blocked/ Allowed)	Incidents (Blocked/ Allowed)
blocked-connection	Blocked by Firewall Policy	Critical	5,251,860	175,062
Proxy.HTTP	Proxy	High	2,807,590	56,157
blocked-connection	Blocked by Firewall Policy	High	800,790	26,693
Zeroaccess.Botnet	Botnet	Critical	592,900	5,929
Failed Connection Attempts to 208.91.113.179	Failed Connection Attempts	Low	375,205	75,041
Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Low	259,635	51,927
Failed Connection Attempts to 172.16.100.80	Failed Connection Attempts	Medium	191,400	38,280
Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Low	115,690	23,138
Failed Connection Attempts to 172.16.100.100	Failed Connection Attempts	Low	109,435	21,887
Failed Connection Attempts to 192.175.48.42	Failed Connection Attempts	Low	79,185	15,837
Failed Connection Attempts to 208.91.113.241	Failed Connection Attempts	Low	74,130	14,826
Failed Connection Attempts to 8.8.8.8	Failed Connection Attempts	Medium	71,650	14,330

### Filter by Device

Select devices from the drop-down menu.



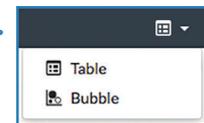
### Filter by Time Period

Select a predefined time period or create a custom one.



### Export to Chart

Export a filtered FortiView (or a drill-down) to charts, and save to the Chart Library.



### FortiView Summary Formats

Use this drop-down menu to switch between different formats.

## Drill Down and View Log Details

Here is the drill-down view of threat ow.ly at log level.

View Data from Different Tabs  
Click the corresponding tab.

View Log Details  
Double-click a row to open the log detail pane in tree view.

View UTM Logs  
Click the UTM log icon to open the UTM log view window.

The screenshot shows the FortiView interface with the following components:

- Summary Panel:** Shows threat details for 'ow.ly' with a Threat Score of 5,928 (Blocked/Allowed) and 92 Incidents (Blocked/Allowed). The Threat Level is Critical.
- Table:** A table of log entries with columns: Date/Time, Device ID, Action, Source, Destination IP, Service, Sent/Received, User, Application, and Security Event List. All actions are 'Malicious W...'. Applications include DNS and HTTP.
- Right Panel:** A tree view showing details for the selected log entry, including Security (APP Count, Level, Threat Score, Webfilter Count), General (Log ID, Session ID, Time Stamp, Tran Display, Virtual Domain), and Source (Device ID, Device Name, Source, Source Country, Source IP, Source Interface, Source Port).

Annotations with dotted lines indicate:

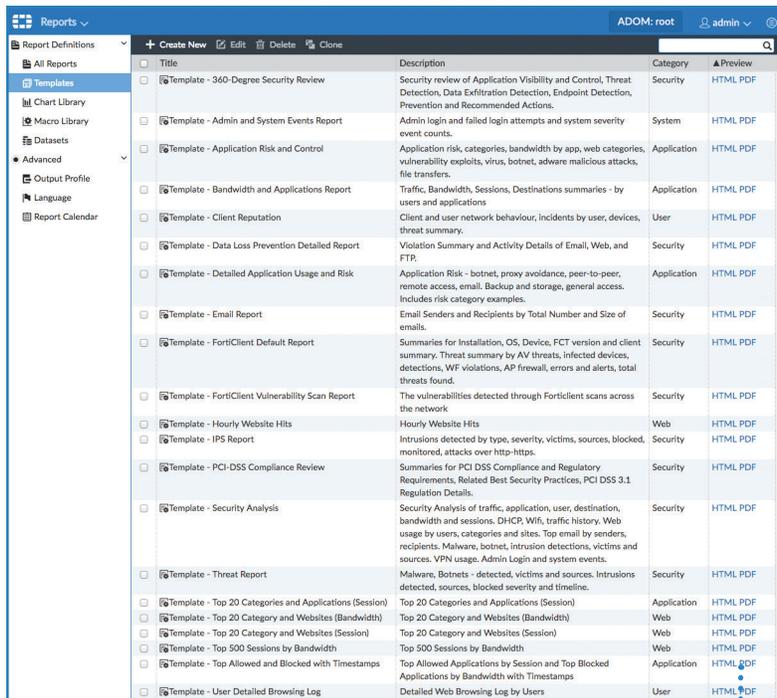
- Clicking a tab in the left sidebar (e.g., Threats, Traffic) to view data from different tabs.
- Double-clicking a row in the table to open the log detail pane in tree view.
- Clicking the UTM log icon (notice icon) to open the UTM log view window.

## 2 Generate Reports

FortiAnalyzer provides a comprehensive set of easily customizable report templates for you to quickly build reports.

### Predefined Report Templates

1. Go to **Reports > Report Definitions > Templates** to view the predefined report templates.



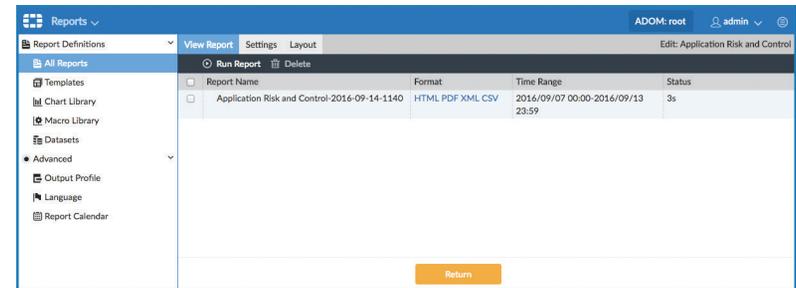
2. Click **HTML** or **PDF** in the preview column to view the sample report.



18

## Generate Reports

1. Go to **Reports > Report Definitions > All Reports**.
2. Double click the **Application Risk and Control** Report.
3. Click **Run Report** from the view report tab.
4. Once the report is generated, click on a format link to view and/or download it.

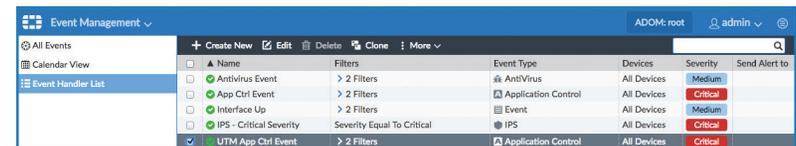


## 3 Monitor Events

### Configure Event Handler

Events are triggered when the values of certain log fields meet the criteria defined in the Event Handlers. To create an event handler to catch the Botnet events:

1. Go to **Event Management > Event Handler Lists**.
2. Select the default handler: **UTM App Ctrl Event**.
3. Click **Clone**.



19

4. Enter a custom name.
5. Remove the application category **Proxy** from the matching criteria.
6. Click **OK** to save the handler.

**Clone Handler: UTM App Ctrl Event**

Status:  ON

Name: Botnet App Ctrl Event

Description: Botnet Application Control event handler

Devices:  All Devices  Specify  Local Device

Severity: Critical

---

**Filters**

Log Type: Application Control

Group By: Application Name

Logs match:  All  Any of the following conditions

Log Field	Match Criteria	Value
Application Category	Equal To	Botnet

Generic Text Filter:

---

**Notifications**

Generate alert when at least  matches occurred over a period of  minutes

Send Alert Email

To: security@company.com

From: admin@company.com

Subject: Corporate\_FGT

Email Server: Corporate: smtp.company.com

Send SNMP(v1/v2) Trap

Send SNMP(v3) Trap

## View Events

All triggered events are displayed on the event list page. To view events:

1. Go to **Event Management > All Events**.
2. Click an entry from the list to view more details.





## DAY 3: EXPLORE FURTHER

### Enable Event Notification

You can send alert notifications via Email, SNMP, to Syslog Server.

To configure notifications:

**Event Monitor > Event Handler List > [Event Handler] Edit**

### Create Custom Report

Create reports from predefined FortiAnalyzer templates, or use any of the 300+ predefined charts and 400+ datasets.

To create a custom report:

**Reports > All Reports > Create New**

### Monitor Storage Usage Graphs

Monitor FortiAnalyzer disk space, data policy, storage and disk utilization, as well as drill down to Analytic and Archive usage by device.

To monitor storage usage:

**Log View > Storage Statistics**

### System Dashboard Log Rate Widgets

Monitor logging rates and performance from the Dashboard. Useful widgets include **Insert Rate vs Receive Rate**, **Log Receive Monitor** and **Log Insert Lag Time**.

To add Widgets to monitor log rates:

**System Settings > Dashboard > Toggle Widgets**

### Indicators of Compromise for APT Detection

**FortiView > Threats > IOC**



For more information, see [Administration Guide](#) and videos in [Fortinet Video Library](#)

---

## LEARN MORE

FortiAnalyzer Administration Guide

<http://docs.fortinet.com/fortianalyzer/admin-guides>

Fortinet Document Library

<http://docs.fortinet.com>

Fortinet Video Guide

<http://video.fortinet.com>

Fortigate Cookbook

<http://cookbook.fortinet.com>

Training Services

<http://www.fortinet.com/training>

## SUPPORT AND FEEDBACK

Customer Service & Support

<https://support.fortinet.com>

Feedback on Fortinet technical document

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)

**FORTINET.COM**