Integrate FortiAnalyzer

EventTracker Enterprise
Abstract

This guide provides instructions to configure FortiAnalyzer to send the event logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, and FortiAnalyzer 4.0, 5.0 and later.

Audience

FortiAnalyzer users, who wish to forward event logs to EventTracker Manager and monitor events using Event Tracker Enterprise.
Table of Contents

Abstract ........................................................................................................................................................................... 1
Scope ........................................................................................................................................................................... 1
Audience ................................................................................................................................................................... 1
Overview .......................................................................................................................................................................... 3
Prerequisites ................................................................................................................................................................... 3
Enable Syslog forwarding on FortiAnalyzer ................................................................................................................. 3
  Configure Operation Mode ......................................................................................................................................... 3
  Configure Syslog Server ............................................................................................................................................. 4
EventTracker Knowledge Pack (KP) ................................................................................................................................................ 5
  Categories ................................................................................................................................................................... 5
  Alerts ........................................................................................................................................................................... 6
  Reports ........................................................................................................................................................................ 7
  Dashboard ................................................................................................................................................................. 12
Import Knowledge Pack into EventTracker ...................................................................................................................... 13
  Import Category ........................................................................................................................................................ 14
  Import Alerts ............................................................................................................................................................ 15
  Import Flex Reports ................................................................................................................................................ 16
  Import Parsing Rules ............................................................................................................................................... 17
  Import Token Templates .......................................................................................................................................... 18
  Import Knowledge Object ........................................................................................................................................ 19
Verify Knowledge Pack in EventTracker ......................................................................................................................... 22
  Verify Categories ...................................................................................................................................................... 22
  Verify Alerts ............................................................................................................................................................ 22
  Verify Parsing Rules ............................................................................................................................................... 23
  Verify Token Templates .......................................................................................................................................... 24
  Verify Knowledge Object ........................................................................................................................................ 25
Verify Flex Reports ...................................................................................................................................................... 25
Create Dashboards in EventTracker ................................................................................................................................................ 26
  Schedule Reports .................................................................................................................................................... 26
  Create Dashlets ..................................................................................................................................................... 29
Overview

FortiAnalyzer logs and analyzes aggregated log data from Fortinet devices and other syslog-compatible devices. EventTracker examines this collection of logs and leverages machine learning to identify critical events, suspicious network traffic, configuration changes and user behavior analytics.

Prerequisites

- EventTracker v7.x and later should be installed.
- FortiAnalyzer 4.0, 5.0 and 5.2 should be installed.

Enable Syslog forwarding on FortiAnalyzer

Configure Operation Mode

1. Go to System Settings > Dashboard.
2. In the System Information widget, in the Operation Mode field, select [Change].
3. In the Change Operation Mode dialog box, select Collector, and then select OK.

![System Information](image-url)  

Figure 1
Figure 2

The Web-based Manager will refresh and the Device Manager, Log View, and System Settings tabs will be available.

Configure Syslog Server

1. Go to System settings > Advanced > Syslog Server > Create new.

Figure 3

2. Configure the following settings and then select OK
   - **Name**: Enter a name for the syslog server.
   - **IP address (or FQDN)**: Enter the IP address or FQDN of the syslog server.
   - **Port**: Enter the syslog server port number. The default port is 514.

Figure 4
EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker categories, alerts, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7 and later to support FortiAnalyzer monitoring:

Categories

- **FortiAnalyzer: Anomalies attack** - This category based report provides information related to attacks detected.
- **FortiAnalyzer: Certificates imported attack** - This category based report provides information related to certificate imported by unknown user.
- **FortiAnalyzer: Configuration back up failed** - This category based report provides information related to configuration backup failure.
- **FortiAnalyzer: Configuration changes** - This category based report provides information related to change in device configuration.
- **FortiAnalyzer: Configuration restored** - This category based report provides information related to external configuration restoration.
- **FortiAnalyzer: Critical error events** - This category based report provides information related to occurrence of critical errors.
- **FortiAnalyzer: Firmware updated** - This category based report provides information related to firmware update.
- **FortiAnalyzer: Added report language** - This category based report provides information related to addition of language report.
- **FortiAnalyzer: Deleted report language** - This category based report provides information related to deletion of language report.
- **FortiAnalyzer: Log backup failed** - This category based report provides information related to failure of log backup.
- **FortiAnalyzer: Log files imported** - This category based report provides information related to log file import.
- **FortiAnalyzer: Migration successfully** - This category based report provides information related to successful migration.
- **FortiAnalyzer: Reports restored** - This category based report provides information related to restoration of reports.
- **FortiAnalyzer: System configuration restored** - This category based report provides information related to restoration of system configuration.
- **FortiAnalyzer: System restarted** - This category based report provides information related to system restarts.
• **FortiAnalyzer: User access profile changed** - This category based report provides information related to change in access profile.
• **FortiAnalyzer: User logged out** - This category based report provides information related to user log off.
• **FortiAnalyzer: User login failed** - This category based report provides information related to user logon failure.
• **FortiAnalyzer: User login successfully** - This category based report provides information related to user logon success.
• **FortiAnalyzer: VPN subsystems** - This category based report provides information related to VPN sessions.
• **FortiAnalyzer: Firmware update failed** - This category based report provides information related to failure of firmware update.

**Alerts**

• **FortiAnalyzer: User logon failed** – This alert is generated when administrator attempt to log in to the web-based manager using GUI or CLI was failed.
  
  Log Considered:

  ```
  date=2009-12-21 time=15:55:00 log_id=0104000001 type=event subtype=admin pri=alert
device_id=FLG8002704000076 user=amdin ui=GUI(172.20.110.44) action=login status=failure
  reason=name_invalid msg="User ‘amdin’ login failed from GUI(172.20.110.44)"
  ```

• **FortiAnalyzer: Administrator deleted a device** – This alert is generated when administrator deleted the device.
  
  Log Considered:

  ```
  date=2009-12-15 time=14:32:41 log_id=0100000045 type=event subtype=config
  pri= warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10)
  action=config msg="User deleted device ‘FG200A3907550170’"
  ```

• **FortiAnalyzer: Removed a disk from RAID array** – This alert is generated when admin removes the disk from the RAID array.
  
  Log Considered:

  ```
  date=2009-06-24 time=10:31:26 log_id=0100000086 type=event subtype=config pri=warning
  device_id=FLG8002704000076 user=admin ui=console action=config msg="user admin delete
disk md1 from RAID array”
  ```
Reports

- **FortiAnalyzer – Administrator logon activity** – This report provides information related to user logon behavior which includes User Name, User Interface, Action, Status and Reason fields.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>User Interface</th>
<th>Source IP</th>
<th>Action</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/27/2016 02:59:41 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>login</td>
<td>success</td>
<td>none</td>
</tr>
<tr>
<td>01/27/2016 03:39:54 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>logout</td>
<td>success</td>
<td>none</td>
</tr>
<tr>
<td>01/27/2016 03:42:54 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>console</td>
<td>172.16.1.20</td>
<td>login</td>
<td>success</td>
<td>none</td>
</tr>
<tr>
<td>01/27/2016 03:45:55 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>SSH</td>
<td>172.16.1.20</td>
<td>login</td>
<td>success</td>
<td>none</td>
</tr>
</tbody>
</table>

Figure 5

Log Considered:

date=2009-12-22 time=17:01:57 log_id=0104000001 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=login status=success reason=none msg="User admin login successfully from GUI(172.16.1.20)"

- **FortiAnalyzer – Administrator logon failed** – This report provides information related to login failure which includes column such as User Name, User Interface, Source IP, Action, Status and Reason.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>User Interface</th>
<th>Source IP</th>
<th>Action</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/27/2016 03:29:54 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.20.110.44</td>
<td>login</td>
<td>failure</td>
<td>name_invalid</td>
</tr>
<tr>
<td>01/27/2016 03:39:55 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.20.110.45</td>
<td>login</td>
<td>failure</td>
<td>name_invalid</td>
</tr>
<tr>
<td>01/27/2016 03:42:54 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.20.110.48</td>
<td>login</td>
<td>failure</td>
<td>name_invalid</td>
</tr>
<tr>
<td>01/27/2016 03:45:55 PM</td>
<td>FORTIANALYZER22</td>
<td>admin</td>
<td>GUI</td>
<td>172.20.110.41</td>
<td>login</td>
<td>failure</td>
<td>name_invalid</td>
</tr>
</tbody>
</table>

Figure 6
EventTracker – Integrate FortiAnalyzer

Log Considered:

date=2009-12-21 time=15:55:00 log_id=0104000001 type=event subtype=admin pri=alert
device_id=FLG8002704000076 user=amdin ui=GUI(172.20.110.44) action=login status=failure
reason=name_invalid msg="User 'amdin' login failed from GUI(172.20.110.44)"

- **FortiAnalyzer – Backup and restore activity** – This report provides information related to
  backup, restore, reboot and upload which includes columns such as User Name, User
  Interface, Source IP, Action, Status and Message details.

![Figure 7](image)

Log Considered:

date=2010-01-15 time=16:31:52 log_id=0104000008 type=event subtype=admin pri=information
device_id=FLG8002704000076 user=admin ui=ssh(172.16.1.20) action=restore_reports
status=success reason=none msg="User admin restored reports from ssh(172.16.1.20)(ftp)
successfully."

- **FortiAnalyzer – Configuration changes activity** – This report provides information related to
  change in authentication server which includes columns such as User Name, User Interface,
  Source IP, Status and Message details.
Log considered:

date=2010-01-06 time=12:02:17 log_id=0100032133 type=event subtype=config pri=notice
device_id=FL800B39080000420 user=admin ui=GUI(172.16.1.20) action=config msg="User admin
changed a radius server radius3 setting from GUI(172.16.1.20). name=radiuss3 old
server=192.168.1.10 new server=192.168.1.20 secret=my secret"

Figure 8

- **FortiAnalyzer- Network share management** – This report provides information related to
  network area storage and network file sharing which includes columns such as User Name,
  User Interface, Source IP, Status and Message Details.

Figure 9
Log Considered:

date=2016-01-25 time=12:55:10 log_id=0100000031 type=event subtype=config pri=information device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.10) action=config msg="User 'system-built-in' changed the NAS user 'share-user3' settings"

- **FortiAnalyzer – IPsec activity** – This report provides information related to IPsec VPN connections which includes columns such as Local IP, Local Port, Remote IP, Remote Port, Outbound Interface, Action, Initiated, Mode, Direction, and Status.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Local IP</th>
<th>Local Port</th>
<th>Remote IP</th>
<th>Remote Port</th>
<th>Outbound Interface</th>
<th>Action</th>
<th>Initiated</th>
<th>Mode</th>
<th>Direction</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/27/2016 03:52:48 PM</td>
<td>FORTIANALYZER6</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>negotiate</td>
<td>remote</td>
<td>quick</td>
<td>outbound</td>
<td>success</td>
<td></td>
</tr>
<tr>
<td>01/27/2016 03:55:48 PM</td>
<td>FORTIANALYZER6</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>negotiate</td>
<td>remote</td>
<td>aggressive</td>
<td>Inbound</td>
<td>success</td>
<td></td>
</tr>
<tr>
<td>01/28/2016 12:11:30 PM</td>
<td>FORTIANALYZER5</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>install_sa</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/27/2016 03:10:12 PM</td>
<td>FORTIANALYZER5</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>negotiate</td>
<td>remote</td>
<td>quick</td>
<td>outbound</td>
<td>success</td>
<td></td>
</tr>
<tr>
<td>01/27/2016 03:30:20 PM</td>
<td>FORTIANALYZER5</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>negotiate</td>
<td>remote</td>
<td>aggressive</td>
<td>Inbound</td>
<td>success</td>
<td></td>
</tr>
<tr>
<td>01/29/2016 12:40:22 PM</td>
<td>FORTIANALYZER5</td>
<td>172.16.1.20</td>
<td>500</td>
<td>172.16.1.30</td>
<td>500</td>
<td>vpn_tunnel=Gateway_Firewall</td>
<td>install_sa</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 10

Log Considered:

date=2009-12-23 time=05:41:56 log_id=0101000000 type=event subtype=ipsec pri=notice device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500 out_if=vpn_tunnel=Gateway_Firewall action=negotiate init=remote mode=aggressive stage=1 dir=outbound status=success msg="Responder: sent 172.16.1.30 aggressive mode message #1 (OK)"

- **FortiAnalyzer – Resource Monitoring** – This report provides information related to resource usage which includes columns such as Status and Message Details.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/28/2016 04:42:35 PM</td>
<td>FORTIANALYZER6</td>
<td>success</td>
<td>Network Interface (port 1) is up</td>
</tr>
<tr>
<td>01/28/2016 04:50:35 PM</td>
<td>FORTIANALYZER6</td>
<td>failure</td>
<td>Killing process httpsd due to high memory usage [RSS:271044 KB, VM:730440 KB]</td>
</tr>
</tbody>
</table>
Log Considered:

<table>
<thead>
<tr>
<th>date</th>
<th>time</th>
<th>log_id</th>
<th>type</th>
<th>subtype</th>
<th>pri</th>
<th>device_id</th>
<th>user</th>
<th>ui</th>
<th>action</th>
<th>status</th>
<th>msg</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-11-27</td>
<td>09:15:57</td>
<td>0106000037</td>
<td>log</td>
<td>event</td>
<td>warning</td>
<td>FLG8002704000076</td>
<td>system</td>
<td>system</td>
<td>monitor</td>
<td>success</td>
<td>Network Interface(port 1) is up</td>
</tr>
</tbody>
</table>

- **FortiAnalyzer – User management** – This report provides information related to user profile accessed, deleted, changed which includes columns such as User Name, User Interface, Source IP, Status and Message Details.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>User Interface</th>
<th>Source IP</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/23/2016 10:43:09 AM</td>
<td>FORTIANALYZER29</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>config</td>
<td>deleted</td>
<td>access profile reports_only2</td>
</tr>
<tr>
<td>02/23/2016 10:45:29 AM</td>
<td>FORTIANALYZER29</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.21</td>
<td>config</td>
<td>changed</td>
<td>password of admin user admin4</td>
</tr>
<tr>
<td>02/23/2016 10:47:32 AM</td>
<td>FORTIANALYZER29</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>config</td>
<td>deleted</td>
<td>an admin user admin4</td>
</tr>
<tr>
<td>02/23/2016 10:49:40 AM</td>
<td>FORTIANALYZER29</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>config</td>
<td>added</td>
<td>an admin user admin3</td>
</tr>
<tr>
<td>02/23/2016 10:51:09 AM</td>
<td>FORTIANALYZER29</td>
<td>admin</td>
<td>jconsole</td>
<td></td>
<td></td>
<td>changed</td>
<td>the system max concurrent users</td>
</tr>
</tbody>
</table>

Log Considered:

<table>
<thead>
<tr>
<th>date</th>
<th>time</th>
<th>log_id</th>
<th>type</th>
<th>subtype</th>
<th>pri</th>
<th>device_id</th>
<th>user</th>
<th>ui</th>
<th>action</th>
<th>status</th>
<th>msg</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-02-17</td>
<td>12:01:19</td>
<td>0100000000</td>
<td>log</td>
<td>event</td>
<td>notice</td>
<td>FL800B3908000420</td>
<td>admin</td>
<td>GUI(172.16.1.20)</td>
<td>config</td>
<td>success</td>
<td>User &quot;admin&quot; deleted access profile reports_only2 from GUI(172.16.1.20)</td>
</tr>
</tbody>
</table>

- **FortiAnalyzer – Device management** – This report provides information related to device added, deleted, rename, changed, registered and unregistered details which includes columns such as User Name, User Interface, Source IP, Action, Status and Message Details.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>User Interface</th>
<th>Source IP</th>
<th>Action</th>
<th>Status</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/29/2016 06:47:11 PM</td>
<td>FORTIANALYZER40</td>
<td>admin</td>
<td>console</td>
<td>172.16.1.20</td>
<td>config</td>
<td></td>
<td>User &quot;admin&quot; changed device FGt_400-Floor2 settings</td>
</tr>
<tr>
<td>01/29/2016 06:47:11 PM</td>
<td>FORTIANALYZER40</td>
<td>admin</td>
<td>GUI</td>
<td>172.16.1.20</td>
<td>config</td>
<td></td>
<td>Device FortWeb_100B added</td>
</tr>
<tr>
<td>01/29/2016 06:47:11 PM</td>
<td>FORTIANALYZER40</td>
<td>system</td>
<td>system</td>
<td></td>
<td>config</td>
<td></td>
<td>The FortiAnalyzer added new device FG200A3907550170 automatically</td>
</tr>
<tr>
<td>01/29/2016 06:47:11 PM</td>
<td>FORTIANALYZER40</td>
<td>system</td>
<td>oftp</td>
<td></td>
<td>config</td>
<td></td>
<td>User's system renamed device FG36002804033057 to FortGate-3600-Floor2</td>
</tr>
<tr>
<td>01/29/2016 06:47:11 PM</td>
<td>FORTIANALYZER40</td>
<td>system</td>
<td>fortilogd</td>
<td></td>
<td>config</td>
<td></td>
<td>A higher and FortiAnalyzer is recommended for this model of FortGate(FG36002804033057)</td>
</tr>
<tr>
<td>01/29/2016 06:47:12 PM</td>
<td>FORTIANALYZER40</td>
<td>system</td>
<td>system</td>
<td></td>
<td>add_device</td>
<td>success</td>
<td>Log device FM390035F0800109 is registered automatically</td>
</tr>
</tbody>
</table>
Log Considered:

```
date=2010-01-05 time=14:24:39 log_id=0106000028 type=event subtype=system
  pri=warning device_id=FL800B3908000420 user=system ui=system action=add_device
  status=success msg="Log device FMG3KB3F09000109 is registered automatically."
```

- **FortiAnalyzer – System management** – This report provides information related to bootup, downgraded, migration, delete log and delete archive which includes columns such as User Name, User Interface, Source IP, Action, Status and Message details.

![Table showing FortiAnalyzer log details](image)

Log Considered:

```
date=2009-05-28 time=07:51:36 log_id=010600001 type=event subtype=system
  pri=alert device_id=FLG8002704000076 user=system ui=system action=bootup
  status=success msg="The configured secondary DNS server is not reachable. A valid DNS server is required for resolving IP addresses to hostnames in reports."
```

Dashboard

**FortiAnalyzer- Administrator logon activity**: This dashboard gives the information about user login, user logout and user exit from the specific user interface and source IP.
Import Knowledge Pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export/Import Utility, and then click the Import tab.
Import **Categories, Alerts, and Reports** as given below.

**Import Category**

1. Click **Category** option, and then click the **browse** button.

![Figure 17](image)

2. Locate **All FortiAnalyzer group categories.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

### Import Alerts

1. Click **Alert** option, and then click the **browse** button.

   ![Export Import Utility](image)

   **Figure 19**

   - Provide the path and file name of the Alerts file. Use the ‘...’ button to browse and locate the import file.
   - Click the **Import** button.
2. Locate All FortiAnalyzer group alerts.isalt file, and then click the Open button.

3. To import alerts, click the Import button.

   EventTracker displays success message.

4. Click OK, and then click the Close button.

Import Flex Reports

1. Click Report option, and then click the browse button.
2. Locate the FortiAnalyzer.issch file, and then click the **Open** button.

3. Click the **Import** button to import the scheduled reports.

   EventTracker displays success message.

   ![Figure 22](image)

---

### Import Parsing Rules

1. Click **Token Value** option, and then click the browse **...** button.

2. Locate **All FortiAnalyzer group of tokens.istoken** file, and then click the **Open** button.

   ![Figure 23](image)

3. To import token value, click the **Import** button.

   EventTracker displays success message.
4. Click OK, and then click the Close button.

Import Token Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on ‘Import’ option.

3. Click on Browse button.
4. Locate All **FortiAnalyzer token template.ettd** file, and then click the **Open** button.

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

6. Click on **OK** button.

**Import Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **Import** option.
3. In **IMPORT** pane click on **Browse** button.

4. Locate **FortiAnalyzer KO.etko** file, and then click the **UPLOAD** button.
5. Now select the check box and then click on ‘MERGE’ option.

EventTracker displays success message.

6. Click on OK button.
Verify Knowledge Pack in EventTracker

Verify Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. To view the imported categories, in the Category Tree, expand FortiAnalyzer group folder.

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type ‘FortiAnalyzer’, and then click the search button.

Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column and then click the **Activate Now** button.

   EventTracker displays message box.

   ![Figure 34](image)

   **Figure 34**

   Successfully saved configuration.

   ![Figure 35](image)

   **Figure 35**

5. Click **OK**.

**Verify Parsing Rules**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules** from the dropdown options.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **FortiAnalyzer group** folder.

   Token values are displayed in the token value pane.
Verify Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab.
3. In Token Value Group Tree to view imported token values, scroll down and click FortiAnalyzer group folder.

Imported token template is displayed in the template pane.
EventTracker – Integrate FortiAnalyzer

Verify Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.
2. Scroll down and select FortiAnalyzer in Objects pane.

Imported FortiAnalyzer object details are shown.

Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported flex reports, scroll down and click FortiAnalyzer group folder.
Create Dashboards in EventTracker

Schedule Reports

1. Open **EventTracker** in browser and logon.

1. Navigate to **Reports>Configuration**.
3. Select **FortiAnalyzer** in report groups. Check **defined** dialog box.

4. Click on **‘schedule’** icon to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault Explorer** box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

![Figure 44](image)

3. Navigate to **Dashboard>Flex**.

   Flex Dashboard pane is shown.

![Figure 45](image)

4. Click **+** to add a new dashboard.
5. Fill fitting title and description and click **Save** button.

6. Click the icon 🌡️ to configure a new Flex dashlet.

**Widget configuration pane is shown.**
7. Locate earlier scheduled report in **Data Source** dropdown.

8. Select **Chart Type** from dropdown.

9. Select extent of data to be displayed in **Duration** dropdown.

10. Select computation type in **Value Field Setting** dropdown.

11. Select evaluation duration in **As Of** dropdown.

12. Select comparable values in **X Axis** with suitable label.

13. Select numeric values in **Y Axis** with suitable label.

14. Select comparable sequence in **Legend**.

15. Click **Test** button to evaluate.

Evaluated chart is shown.

![Evaluated chart is shown.](image)

**Figure 4B**
16. If satisfied, click **Configure** button.

![Customize Widgets](image)

**Figure 49**

17. Click 'customize' to locate and choose created dashlet.

18. Click to add dashlet to earlier created dashboard.

**NOTE:** For Version 4.0 log field Priority is pri for Version 5.0 pri is replaced with level. For more information please go through the link: [http://docs.fortinet.com/d/log-message-reference](http://docs.fortinet.com/d/log-message-reference)