LOGZILLA DOCUMENTATION

Fortianalyzer

LogZilla App Store application: Fortianalyzer

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/fortianalyzer

Overview

Fortinet FortiAnalyzer is a centralized log management and analytics appliance that collects, stores, and forwards logs from FortiGate firewalls and other Fortinet Security Fabric devices. The parser handles FortiAnalyzer-forwarded logs in the `logver=` key-value format, extracting security, traffic, wireless, and operational metadata.

App Function

- Parses FortiAnalyzer-forwarded logs (`logver=` prefix format)
- Extracts traffic metadata: source/destination IPs, ports, interfaces, countries, actions
- Classifies events into Event Class/Type taxonomy for cross-vendor dashboards (SecOps, NetOps, AuthOps)
- Maps UTM security events to MITRE ATT&CK techniques
- Extracts wireless metadata: SSIDs, access points, client MACs
- Applies compliance framework tags (SOX, PCI-DSS, HIPAA, GDPR, ISO-27001, NIST-800-53, etc.) based on event type
- Strips FortiAnalyzer forwarding headers and timestamps to enable effective event deduplication
- Provides dashboards for network traffic, security threats, and wireless operations
- Fires triggers on actionable events: intrusions, rogue APs, VPN failures, auth failures, link down

Vendor Documentation

- FortiAnalyzer Administration Guide (https://docs.fortinet.com/document/fortianalyzer/7.6.6/administration-guide/)
- FortiAnalyzer Log Forwarding (https://docs.fortinet.com/document/fortianalyzer/7.6.6/administration-guide/621804/log-forwarding)
- FortiOS Log Types and Subtypes (https://docs.fortinet.com/document/fortigate/7.6.6/fortios-log-message-reference/160372/list-of-log-types-and-subtypes)
- FortiOS Log Message Reference (https://docs.fortinet.com/document/fortigate/7.6.6/fortios-log-message-reference/)

Prerequisites / Device Configuration

Configure FortiAnalyzer to forward logs to LogZilla via syslog:

Log in to the FortiAnalyzer web interface.
Navigate to **System Settings > Log Forwarding**.
Click **Create New** to add a log forwarding rule.
Configure the syslog server:

- **Name**: LogZilla
- **Mode**: Forwarding

- **Server Type**: Syslog
- **Server IP**: `<LogZilla IP>`
- **Server Port**: `514` (or custom port)
- **Reliable Syslog**: Enable for TCP transport

Select the device logs to forward (all ADOMs or specific devices).
Apply the configuration.
Verify logs are arriving at LogZilla by checking the User Tags menu for `Vendor = Fortinet` and `Product = FortiAnalyzer`.

Incoming Log Format

FortiAnalyzer-forwarded logs use a key-value format with a `logver=` prefix header:

Template:

```
logver=<version> timestamp=<epoch> devname="<device>"
devid="<device_id>" vd="<vdom>" date=<YYYY-MM-DD>
time=<HH:MM:SS> eventtime=<ns_epoch> tz="<offset>"
logid="<log_id>" type="<type>" subtype="<subtype>"
level="<level>" [key=value ...]
```

Fields:

Field	Description
logver	Log format version
timestamp	Unix epoch timestamp
devname	Source device name
devid	Source device serial number
vd	Virtual domain
logid	Unique log message identifier
type	Log type (traffic, event, utm)
subtype	Log subtype (forward, wireless, app-ctrl, etc.)

Field	Description
level	Severity level

Parsed Metadata Fields

Tag	Source	Description
Vendor	(set)	Always "Fortinet"
Product	(set)	Always "FortiAnalyzer"
Event Class	taxonomy	Auth, HA, Network, Security, System
Event Type	taxonomy	Session, Threat, Access Control, etc.
SrcIP	srcip/remip	Source IP address
DstIP	dstip	Destination IP address
DstPort	dstport	Destination port (translated to name)
SrcInt	srcintf	Source interface
DstInt	dstintf	Destination interface
User	user	Username
Action	action	Event action
SrcMAC	stamac/srcmac	Source MAC address
SrcIP Country	srccountry	Source country
DstIP Country	dstcountry	Destination country
Domain	hostname/sni	Requested hostname or SNI
MitreId	(mapped)	MITRE ATT&CK technique ID
MITRE Tactic	(mapped)	MITRE ATT&CK tactic
FA Type	type	Log type (traffic, event, utm)

Tag	Source	Description
FA Subtype	subtype	Log subtype
FA App	app	Detected application
FA App Category	appcat	Application category
FA Web Category	catdesc	Web filter category
FA SSID	ssid	Wireless SSID
FA AP Name	ap	Access point name

High-Cardinality (HC) Tags

- SrcIP
- DstIP
- User
- SrcMAC

Log Examples

Traffic Forward (Accept)

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="0000000013" type="traffic" subtype="forward"
level="notice" srcip=10.0.0.10 srcport=50000
srcintf="port2" dstip=10.0.0.20 dstport=53
dstintf="port3" srccountry="Reserved"
dstcountry="Reserved" proto=17 action="accept"
policyid=1 service="DNS"
```

Wireless Client Authentication

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="0104043573" type="event" subtype="wireless"
```

```
level="notice" logdesc="Wireless client authenticated"
ap="AP-Office-1" ssid="CorpSecure"
stamac="00:00:5e:00:53:01" user="user1"
action="client-authentication"
```

Rogue AP Detected

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="0104043563" type="event" subtype="wireless"
level="notice" logdesc="Rogue AP detected"
ssid="Evil-AP" bssid="00:00:5e:00:53:02"
action="rogue-ap-detected"
```

SSL VPN Login Failure

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="0101039426" type="event" subtype="vpn"
level="alert" logdesc="SSL VPN login fail"
action="ssl-login-fail" tunneltype="ssl-web"
remip=192.0.2.10 user="user1"
reason="sslvpn_login_permission_denied"
```

UTM Application Control (Blocked)

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="1059028705" type="utm" subtype="app-ctrl"
level="warning" srcip=10.0.0.10
dstip=198.51.100.10 dstport=4379 action="block"
appcat="P2P" app="BitTorrent"
```

FortiSwitch Link Down

```
logver=704112878 timestamp=1700000000 devname="FGT-1"
devid="FG100F" vd="root" date=2026-01-01
time=00:00:00 eventtime=1700000000000000000 tz="-0000"
logid="0115032695" type="event"
subtype="switch-controller" level="notice"
```

```
logdesc="FortiSwitch link" name="FSW-1"
switchphysicalport="port5" action="port-down"
status="down"
```

Dashboards

- **FortiAnalyzer: Network** - Traffic analysis by action, top IPs, interfaces, ports, and countries
- **FortiAnalyzer: Security** - UTM threats, MITRE techniques, blocked apps, web categories, top domains
- **FortiAnalyzer: Wireless** - Wireless operations by SSID, AP, client MAC, auth events, DHCP

Triggers

Trigger	Description
MITRE ATT&CK Threat Detected	Any event with MITRE technique
SSL VPN Login Failure	Failed SSL VPN authentication
Rogue AP Detected	Unauthorized wireless AP detected
RADIUS Authentication Failure	Wireless RADIUS auth failure
Traffic Denied	Firewall deny/drop actions
IPS Threat Detected	Intrusion prevention alert
Virus Detected	Antivirus detection
Web Content Blocked	Web filter blocked URL
Application Blocked	App control blocked app
FortiSwitch Link Down	Switch port down event
SSL Certificate Anomaly	SSL inspection block
User Authentication Failure	Failed user authentication