LOGZILLA DOCUMENTATION

Fireeye

LogZilla App Store application: Fireeye

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

Overview

FireEye (now Trellix) provides advanced threat protection across network, email, and endpoint security:

- **MPS** - Malware Protection System for network malware detection
- **NX** - Network Security for network threat detection
- **EX** - Email Security for email threat detection
- **HX** - Endpoint Security for endpoint detection and response

App Function

- Parse Common Event Format (CEF) logs from all FireEye product types
- Extract security event metadata for filtering and analysis
- Detect command and control (C&C) callback activity
- Identify CVE exploits and attack modes
- Verify threats via MVX sandbox confirmation
- Provide analyst-focused dashboards for security monitoring
- Alert on C&C activity, CVE exploits, and MVX-confirmed threats

Vendor Documentation

- FireEye Products Overview (https://www.fireeye.com/products.html)
- FireEye Network Security Documentation (https://docs.fireeye.com/docs/index.html#Network%20Security)

LogZilla Configuration

FireEye requires a dedicated syslog port in LogZilla:

Navigate to **Settings > System > Application Ports**
Set **FireEye syslog port** to a dedicated port (e.g., `5516`)
Click **Save**
The syslog and parser services will reload automatically. Both TCP and UDP listeners are enabled on the configured port.

Device Configuration

Configure FireEye appliances to send syslog to LogZilla:

Log into the FireEye appliance management console
Navigate to **Settings > Notifications > Syslog**
Add a new syslog server with the LogZilla server IP address
Set the port to the dedicated FireEye port configured above (e.g., 5516)
Enable CEF format for log output
Save the configuration

Verification

Generate a test alert or wait for normal traffic, then verify events appear in LogZilla with `Vendor` tag set to `FireEye` and `Product` tag set to `MPS`, `NX`, `EX`, or `HX` depending on the appliance type.

Incoming Log Format

FireEye logs follow the Common Event Format (CEF) standard:

```
<timestamp> <sensor> fenotify-<n>.<level>: CEF:0|FireEye|<product>|<version>|
<sig_id>|<sig_name>|<severity>|<key=value pairs>
```

- **timestamp** - Syslog timestamp
- **sensor** - FireEye sensor name
- **level** - Log level (alert, warning, info)
- **product** - FireEye product (MPS, NX, EX, HX, CMS)
- **sig_id** - Signature identifier
- **sig_name** - Signature name
- **severity** - CEF severity (1-10)

Parsed Metadata Fields

Global Tags

Tag Name	Example	Description
`Vendor`	`FireEye`	Vendor name
`Product`	`MPS`	Product name
`Event Class`	`security`	Cross-vendor event classification

Tag Name	Example	Description
MitreId	T1071	MITRE ATT&CK technique ID
MITRE Tactic	Command and Control	MITRE ATT&CK tactic

FireEye Tags

Tag Name	Example	Description
Signature Name	Malware.Generic	Signature name describing the threat
SrcIP	192.168.1.100	Source IP address
DstIP	10.0.0.1	Destination IP address
DstPort	HTTPS	Destination port with service name
Protocol	TCP	Network protocol
CNC Host	malware.example.com	Command and control host
CNC Port	8080	Command and control port
Source Host	workstation-01	Affected endpoint hostname
Source User	john.doe	Source username
Dest User	admin	Destination username
Action	blocked	Action taken on the threat
Attack Mode	callback	Attack classification mode
CVE ID	CVE-2021-44228	CVE identifier for vulnerability correlation
MVX	true	Multi-Vector Virtual Execution sandbox result

Log Examples

Basic Alert

```
Feb  2 14:14:12 MPS001 fenotify-1.warning: CEF:0|FireEye|MPS|1.2.3|sig1|
signature1|1|rt=Feb  2 2023 14:14:12 UTC dst=1.2.3.4 src=5.6.7.8
```

C&C Detection

```
Feb  2 14:14:12 MPS001 fenotify-1.alert: CEF:0|FireEye|MPS|1.2.3|callback|
Malware.Callback|8|dst=10.0.0.1 src=192.168.1.100 cs5Label=cncHost
cs5=malware.example.com cn3Label=cncPort cn3=8080
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
C&C Detection	T1071	Command and Control
CVE Exploit	T1203	Execution
Malware Detection	T1204	Execution

C&C callback activity receives T1071 (Application Layer Protocol). CVE exploits receive T1203 (Exploitation for Client Execution). All other malware detections receive T1204 (User Execution) as the default.

Dashboards

Dashboard	Description
FireEye: Security Overview	Alerts, C&C, CVE, blocked, attackers, MITRE tactics

Triggers

Trigger	Description
`FireEye: MITRE ATT&CK Threat Detected`	Events with MITRE technique mapping
`FireEye: Command and Control Activity`	C&C host detection
`FireEye: CVE Exploit Detected`	Known vulnerability exploitation
`FireEye: Threat Blocked`	FireEye blocked a threat
`FireEye: MVX Confirmed Threat`	Sandbox verified threat