

**LOGZILLA DOCUMENTATION**

# Symantec EPM

Adds rules, triggers, and dashboards for Symantec Endpoint Protection firewall logs. Extracts source/destination IPs, ports, protocols, users, and actions.

LogZilla App Store · Generated June 11, 2026 · [logzilla.ai/docs/logzilla-appstore/symantec-epm](https://logzilla.ai/docs/logzilla-appstore/symantec-epm)

## Overview

Symantec Endpoint Protection (SEP) is an enterprise security suite that protects endpoints from malware, viruses, and network threats. SEP provides antivirus, firewall, intrusion prevention, and application control capabilities. The firewall component generates events for blocked traffic, policy violations, and potential security threats.

## App Function

- Parse Symantec EPM firewall events from dedicated syslog port
- Extract source/destination IPs, ports, protocols, and applications
- Identify blocked traffic and policy violations
- Map security events to MITRE ATT&CK techniques
- Categorize events with `Event Class: security`
- Provide dashboards for threat analysis and endpoint monitoring

## Vendor Documentation

- [Symantec Endpoint Protection Documentation](https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html) (https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html)
- [SEP Administration Guide](https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/endpoint-security-and-management/endpoint-protection/generated-pdfs/Installation_and_Administration_Guide_SEP14.3.1.pdf) (https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/endpoint-security-and-management/endpoint-protection/generated-pdfs/Installation\_and\_Administration\_Guide\_SEP14.3.1.pdf)

## Device Configuration

### LogZilla Dedicated Port

Symantec EPM requires a dedicated syslog port:

Navigate to **Settings > System > Application Ports**

Set **Symantec Endpoint Protection syslog port** (e.g., 5520)

Click **Save**

Both TCP and UDP listeners are enabled on the configured port.

### SEPM Syslog Configuration

Log in to Symantec Endpoint Protection Manager console

Navigate to **Admin > Servers > Local Site**

Right-click the management server and select **Edit Site Properties**

Select the **Log Settings** tab

Check **Enable transmission of logs to a Syslog server**

Enter the LogZilla server IP and the dedicated port configured above

Select **UDP** or **TCP** protocol

Click **OK** to save

## Firewall Policy Logging

In SEPM, navigate to **Policies > Firewall**

Edit the firewall policy applied to endpoints

Under **Logging**, ensure firewall events are logged

Apply the policy to client groups

## Verification

Generate firewall events on a managed endpoint, then verify events appear in LogZilla with `Vendor` tag set to `Symantec`.

## Incoming Log Format

Symantec EPM firewall events use this format:

```
<date> <host> <device>: <id>,Local: <src_ip>,Local: <src_port>,Local: <src_mac>,
Remote: <dst_ip>,Remote: <dst_host>,Remote: <dst_port>,Remote: <dst_mac>,
<proto>,<dir>,Begin: <begin>,End: <end>,Occurrences: <count>,
Application: <app>,"Rule: <rule>","Location: <loc>,User: <user>,
Domain: <domain>,Action: <action>
```

## Parsed Metadata Fields

| Tag Name    | Example        | Description                 |
|-------------|----------------|-----------------------------|
| Event Class | security       | Cross-vendor classification |
| SEP Device  | workstation-01 | Endpoint device name        |
| SrcIP       | 192.168.1.100  | Source IP address           |

| Tag Name        | Example    | Description                  |
|-----------------|------------|------------------------------|
| DstIP           | 10.0.0.1   | Destination IP address       |
| DstPort         | https      | Destination port (resolved)  |
| Protocol        | TCP        | Network protocol             |
| Direction       | outbound   | Traffic direction            |
| SEP Application | chrome.exe | Application triggering event |
| SEP Rule        | Block All  | Firewall rule that matched   |
| User            | jdoe       | Username                     |
| Action          | blocked    | Action taken                 |

## Log Examples

### Allowed Traffic

```
May 5 12:34:56 hostname device1: id1,Local: 10.0.0.1,Local: 1234,  
Local: 01:23:45:67:89:ab,Remote: 192.168.1.1,Remote: example.com,  
Remote: 80,Remote: ff:ff:ff:ff:ff:ff,TCP,inbound,  
Begin: 2023-05-05 12:00:00,End: 2023-05-05 12:30:00,Occurrences: 10,  
Application: HTTP,"Rule: Allow web traffic",Location: Office,  
User: jdoe,Domain: EXAMPLE,Action: allow
```

### Blocked Outbound Traffic

```
Jun 15 08:22:33 server firewall1: blocked_conn,Local: 192.168.1.50,  
Local: 54321,Local: aa:bb:cc:dd:ee:ff,Remote: 10.10.10.10,  
Remote: malware.bad,Remote: 443,Remote: 11:22:33:44:55:66,TCP,outbound,  
Begin: 2023-06-15 08:20:00,End: 2023-06-15 08:22:33,Occurrences: 5,  
Application: unknown.exe,Rule: Block malware,Location: Default,  
User: admin,Domain: CORP,Action: blocked
```

## MITRE ATT&CK Mappings

| Event                          | MITRE ID | Tactic              |
|--------------------------------|----------|---------------------|
| Blocked outbound traffic       | T1071    | Command and Control |
| Blocked inbound traffic        | T1595    | Reconnaissance      |
| Unknown/suspicious application | T1204    | Execution           |
| PowerShell/script blocked      | T1059    | Execution           |
| PsExec/WMIC blocked            | T1570    | Lateral Movement    |

## Triggers

| Trigger                                      | Description                 |
|--|-----------------------------|
| Symantec EPM: MITRE ATT&CK Threat Detected   | Catch-all for MITRE events  |
| Symantec EPM: Outbound Blocked (T1071)       | Potential C2 communication  |
| Symantec EPM: Reconnaissance Blocked (T1595) | Inbound scan/probe blocked  |
| Symantec EPM: Suspicious Execution (T1204)   | Unknown application blocked |
| Symantec EPM: Script Execution (T1059)       | PowerShell/script blocked   |
| Symantec EPM: Lateral Movement (T1570)       | PsExec/WMIC blocked         |

## Dashboards

| Dashboard              | Purpose  |
|------------------------|--|
| Symantec EPM: Overview | Blocked traffic, MITRE analysis, endpoint monitoring |