LOGZILLA DOCUMENTATION

Cisco Meraki

Rules, dashboards, and triggers for Cisco Meraki network devices including MX security appliances, MR wireless access points, and MS switches

LogZilla App Store · Generated October 31, 2026 · logzilla.ai/docs/logzilla-appstore/cisco-meraki

© LogZilla Corporation · logzilla.ai

Overview

Cisco Meraki is a cloud-managed networking platform that provides wireless, switching, security, and SD-WAN solutions. Meraki devices send syslog messages for network flows, URL requests, wireless events, IDS alerts, DHCP leases, content filtering, firewall decisions, VPN connections, and authentication.

App Function

- Parse Meraki syslog events (flows, URLs, wireless, IDS, DHCP, firewall, VPN)
- Extract network metadata (IPs, ports, protocols, MACs)
- Map IDS priority levels to human-readable values (High, Medium, Low)
- Parse user DN fields for identity correlation
- Categorize events by class (network, security, auth)
- Provide dashboards for network monitoring and security analysis

Vendor Documentation

- Meraki Syslog Configuration (https://documentation.meraki.com/General_Administration/Monitoring_and_Reporting/Syslog_Server_Overview_and_Configuration)

LogZilla Configuration

Meraki devices send logs with a non-standard timestamp format (epoch instead of RFC 3164/5424 date format). This requires a dedicated syslog port with a `source_type` to identify Meraki traffic.

Navigate to **Settings > System > Application Ports**
Set **Cisco Meraki syslog port** to a dedicated port (e.g., `5517`)
Click **Save**
The syslog and parser services will reload automatically. Both TCP and UDP listeners are enabled on the configured port.

LogZilla Cloud: the Application Ports page is not available on the cloud platform, where devices reach LogZilla through a relay rather than a direct syslog listener. To enable parsing there, tag Meraki events at the relay with `_source_type=meraki`. See Application Ports on LogZilla Cloud (https://www.logzilla.ai/docs/logzilla-cloud/application-ports-on-cloud).

Meraki Configuration

Configure each Meraki network to send syslog to LogZilla:

Log in to the Meraki Dashboard
Navigate to **Network-wide > General**
Scroll to **Reporting > Syslog servers**
Click **Add a syslog server**
Enter the LogZilla server IP address
Set the **Port** to **5515** (or the port configured above)
Select the desired **Roles** (URLs, Flows, IDS Alerts, etc.)
Click **Save**

Verification

Generate test traffic, then verify events appear in LogZilla with `Vendor` tag set to `Cisco` and `Product` tag set to `Meraki`.

Incoming Log Format

Meraki devices send logs with an epoch timestamp and device name prefix:

```
1566076596.550975289 MX_BRANCH_06 urls src=192.168.1.1:54060 dst=192.168.1.9:443
mac=00:0A:E6:3E:FD:E1 agent='Mozilla/5.0 (Windows NT 10.0; Win64; x64)'
request: POST http://192.168.1.9:443/common/EventPoller.jsp
```

- **Timestamp** - Unix epoch with nanoseconds
- **Device** - Meraki device name (MX, MR, MS, etc.)
- **Role** - Log category token that selects the parser:
  - `urls` - HTTP/HTTPS requests (MX, MR)
  - `flows` - MR flows (leading `allow`/`deny`) and pre-MX18.101 MX flows (verdict in the trailing `pattern:` text; inbound rules use `1 all` for deny and `0 all` for allow)
  - `firewall`, `vpn_firewall`, `cellular_firewall`, `bridge_anyconnect_client_vpn_firewall` - MX18.101+ replacements for `flows`, same body
  - `l7_firewall` - Layer 7 rule matches with `decision=`
  - `ip_flow_start`, `ip_flow_end` - NAT session records
  - `security_event` - `ids_alerted` (IDS), `security_filtering_file_scanned` and `security_filtering_disposition_change` (AMP)
  - `ids-alerts` - legacy IDS role (source only, no destination or message)
  - `events`, `airmarshal_events` - MX/MR/MS event log messages

Optional keys are common: `mac=` is absent on WAN-inbound flows, `sport=` and `dport=` are absent for icmp, icmp6, and numeric protocols, and IDS records may omit `shost=`/`dhost=`, `decision=`, and `action=`. The rule tags only the keys present.

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Cisco`	Vendor identifier
`Product`	`Meraki`	Product identifier
`Event Class`	`security`	Cross-vendor event classification
`Event Type`	`association`	Specific event type
`SrcIP`	`192.168.1.1`	Source IP address
`DstIP`	`8.8.8.8`	Destination IP address
`DstPort`	`https`	Destination port service name
`Protocol`	`tcp`	Network protocol
`MAC`	`00:0A:E6:3E:FD:E1`	Client MAC address
`Agent`	`Mozilla/5.0...`	HTTP user agent
`Request`	`POST`	HTTP request method
`Priority`	`High`	IDS alert priority
`Direction`	`ingress`	Traffic direction
`Decision`	`deny`	Normalized verdict for flows, firewall, and IDS (`allow`, `deny`)
`Action`	`block`	Enforcement action reported by IDS or AMP (`block`, `allow`, `rst`)
`Disposition`	`malicious`	AMP file disposition (`malicious`, `clean`, `unknown`)

Tag Name	Example	Description
Translated SrcIP	203.0.113.10	NAT translated source IP (HC)
Translated DstIP	198.51.100.20	NAT translated destination IP (HC)
Category	Web Advertisements	Content filter category
User	john.smith	Username
User CN	John Smith	User common name from DN
User OU	Engineering	User organizational unit from DN
Leased IP	192.168.1.100	DHCP leased IP address
Client MAC	A0:AA:00:EE:11:D1	DHCP client MAC
Server IP	192.168.1.254	DHCP server IP
Local IP	10.0.0.5	VPN local IP
Remote IP	203.0.113.50	VPN remote IP
Connection Type	connect	VPN connection type

Triggers

Trigger	Description
Cisco Meraki: IDS High Priority Alert	High priority IDS alert (notification enabled)
Cisco Meraki: IDS Medium Priority Alert	Medium priority IDS alert
Cisco Meraki: Rogue AP Detected	Air Marshal rogue AP detection (notification enabled)

Dashboards

- **Cisco Meraki: Network Overview** - Overall network activity, top devices, protocol distribution, firewall decisions
- **Cisco Meraki: Security** - IDS alerts by priority, content filter blocks, attack sources and targets
- **Cisco Meraki: Client Access** - Wireless events, DHCP leases, VPN connections, authentication activity

Log Examples

URL Request

```
1566076596.550975289 MX_BRANCH_06 urls src=192.168.1.1:54060 dst=192.168.1.9:443
mac=00:0A:E6:3E:FD:E1 agent='Mozilla/5.0 (Windows NT 10.0; Win64; x64)'
request: POST http://192.168.1.9:443/common/EventPoller.jsp
```

Network Flow

```
1374543986.038687615 MX84 flows src=192.168.1.186 dst=8.8.8.8
mac=00:0A:E6:3E:FD:E1 protocol=udp sport=55719 dport=53 pattern: allow all
```

IDS Alert

```
1563886829.297656222 MX250 security_event ids_alerted signature=1:28423:1
priority=1 timestamp=1468531589.810079 dhost=98:5A:EB:E1:81:2F direction=ingress
protocol=tcp/ip src=151.101.52.238:80 dst=192.168.128.2:53023
message: EXPLOIT-KIT Multiple exploit kit single digit exe detection
```

Legacy IDS Alert (`ids-alerts` role)

```
1377449842.514782056 MX84 ids-alerts signature=129:4:1 priority=3
timestamp=1377449842.512569 direction=ingress protocol=tcp/ip
src=74.125.140.132:80
```

AMP File Scan

```
1637691298.984398273 MX84 security_event security_filtering_file_scanned
url=http://www.eicar.org/download/eicar.com.txt src=192.168.128.2:53150
```

```
dst=188.40.238.250:80 mac=98:5A:EB:E1:81:2F
name='EICAR:EICAR_Test_file_not_a_virus-tpd'
sha256=275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
disposition=malicious action=block
```

The `name` value may be empty (`name=''`). The URL, file name, and hash are left in the message and are not tagged.

AMP Retrospective Disposition Change

```
1637783435.239819833 MX84 security_event security_filtering_disposition_change
name=EICAR:EICAR_Test_file_not_a_virus-tpd
sha256=275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
disposition=malicious action=allow
```

Firewall (MX18.101+)

```
1374543986.038687615 MX84 firewall src=192.168.1.186 dst=8.8.8.8
mac=58:1F:AA:CE:61:F2 protocol=udp sport=55719 dport=53 pattern: allow all
```

Layer 7 Firewall

```
1787058162.285901262 MX67 l7_firewall src=10.10.10.3 dst=104.21.4.210
protocol=tcp sport=59526 dport=443 decision=blocked
```

NAT Session

```
1647479278.997155282 MX100 ip_flow_start src=10.0.0.234 dst=81.2.69.145
protocol=tcp sport=34294 dport=80 translated_src_ip=1.128.3.4
translated_port=34294
```

DHCP Lease

```
1563902014.000926451 MX250 events dhcp lease of ip 192.168.1.103
for client mac A0:AA:00:EE:11:D1 from router 192.168.1.254
on subnet 255.255.255.0 with dns 10.9.8.99, 10.9.8.100
```

Content Filter Block

```
1563899990.039345558 MX250 events content_filtering_block
url='https://adserver-us.adtech.advertising.com/...' category0='Web Advertisements'
server='10.19.2.12:443' user='CN=Bob\20J.\20Foo,OU=Cloud,DC=foo,DC=net'
client_mac='00:0A:E6:3E:FD:E1'
```

VPN Connection

```
1563903781.810242867 MX250 events client_vpn_connect user id 'bob.l.bar'
local ip 1.2.3.4 connected from 4.3.2.1
```