LOGZILLA DOCUMENTATION

PaloAlto SDWAN ION

Rules, dashboards, and triggers for Palo Alto Prisma SD-WAN ION device events

LogZilla App Store · Generated June 11, 2026 · logzilla.ai/docs/logzilla-appstore/paloalto-sdwan-ion

Overview

Palo Alto Prisma SD-WAN ION devices are edge appliances that provide software-defined wide area networking capabilities. ION devices generate syslog messages for authentication events, privilege escalation, VPN link alerts, system/hardware status, and network flow logs.

The Prisma SD-WAN ION app parses these logs, extracts metadata into user tags, and applies MITRE ATT&CK mappings for security-relevant events.

App Function

- Detects and auto-classifies all ION log types: **Event/Auth**, **Alert**, and **Flow** logs.
- Parses key/value pairs from event and alert logs into user tags for fast filtering.
- Parses CSV-formatted flow logs for network traffic visibility.
- Extracts high-value security fields: User, SrcIP, DstIP, Action for SOC analysis.
- Applies MITRE ATT&CK technique mappings (T1548, T1110, T1078, T1071).
- Automatically converts numeric ports to friendly service names (e.g., `53` → `domain`).
- Ships with an overview dashboard plus triggers for VPN failures, hardware issues, and authentication failures.

Vendor Documentation

- Prisma SD-WAN Documentation (https://docs.paloaltonetworks.com/prisma-sd-wan)
- Syslog Profile Configuration (https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-stacked-policies/configure-syslog-profiles)
- Incident and Alert Event Codes (https://docs.paloaltonetworks.com/prisma-sd-wan/incidents-and-alerts/incident-and-alert-event-codes)

LogZilla Configuration

The Prisma SD-WAN ION app requires a dedicated syslog port for ION events.

Navigate to **Settings > System > Application Ports**
Set **Prisma SD-WAN ION syslog port** to a dedicated port (e.g., `5519`)
Click **Save**
The syslog and parser services reload automatically. Both TCP and UDP listeners are enabled on the configured port.

Device Configuration

ION devices send syslog in **RFC 5424 format only**. Configure syslog export via the Prisma SD-WAN web interface.

Configure Syslog Profile

Log into the Prisma SD-WAN Controller (Strata Cloud Manager)
Navigate to **Configuration > Prisma SD-WAN > Profiles and Templates > Syslog**
Click **Create Syslog Profile**
Configure the following settings:

- **Name**: Enter a profile name (e.g., `LogZilla-Export`)
- **Enable Flow Logging**: Enable to capture network traffic flows
- **Severity Level**: Select `Minor` to capture all events
- **Protocol**: Select `UDP`, `TCP`, or `TLS`
- **Server IP**: Enter the LogZilla server IP address
- **Server Port**: `5519` (dedicated ION port configured above)

Click **Save**
Assign the Syslog Profile to ION devices via device configuration
For detailed instructions, see the Prisma SD-WAN Syslog Profile Configuration (https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-stacked-policies/configure-syslog-profiles) documentation.

TLS Configuration Notes

- Self-signed certificates are not supported for TLS connections
- Server FQDN must match the Subject Alternate Name (SAN) in the certificate
- Only TLS 1.2 is supported

Log Source Details

Item	Value
Vendor	Palo Alto Networks
Device Type	SD-WAN Edge Appliance
Collection Method	Syslog (TCP/UDP/TLS)
Configurable Log Output?	Yes

Item	Value
Log Source Type	Key-Value pairs and CSV

Incoming Log Formats

ION devices send three message types in RFC 5424 format:

Event/Auth Logs

Space-separated key/value pairs with double-quoted values:

```
ION_HOST="hostname" DEVICE_TIME="timestamp" MSG="message content"
SEVERITY="minor|major|critical" PROCESS_NAME="sudo|sshd|charon"
FACILITY="authpriv|auth|daemon" [USER="username"] ELEMENT_ID="id"
```

Alert Logs

Alert events with CODE field indicating the alert type:

```
ION_HOST="hostname" DEVICE_TIME="timestamp" STATUS="cleared|Not clear"
CODE="NETWORK_VPNLINK_DOWN" Severity="major" [REASON="reason_code"]
[VPN_LINK_ID="id"] ELEMENT_ID="id"
```

Flow Logs (CSV)

CSV format with program `cgxFlowLogV1`:

```
timestamp,srcip,srcport,dstip,dstport,protocol,,,bytes_in,bytes_out,
packets_in,packets_out,,wan_interface,flow_id,app,flow_type,rule:action:code
```

Legacy Format

Older ION devices (pre-Palo Alto acquisition) use `CLOUDGENIX_HOST` instead of `ION_HOST`. Both formats are supported.

Parsed Metadata Fields

The following user tags are extracted from ION log messages.

Common Fields (All Log Types)

Tag Name	Example	Description
Vendor	Palo Alto	Vendor name
Product	Prisma SD-WAN ION	Product name
ION Host	US-DA7-SDW-102	ION device hostname
Event Class	Auth	Event classification
Event Type	Session	Event type
Action	deny	Action taken

Event/Auth Log Fields

Tag Name	Example	Description
ION Process	sudo	Process name
User	admin	Username
SrcIP	192.168.1.100	Source IP address
Auth Success	true	Whether authentication succeeded

Alert Log Fields

Tag Name	Example	Description
ION Alert Code	NETWORK_VPNLINK_DOWN	Alert code
ION Alert Status	cleared	Alert status

Tag Name	Example	Description
ION Alert Reason	NETWORK_VPNBFD_DOWN	Alert reason

Flow Log Fields

Tag Name	Example	Description
SrcIP	10.2.53.102	Source IP address
DstIP	10.2.13.100	Destination IP address
DstPort	http	Destination port (service name)
Protocol	tcp	Network protocol
ION WAN Interface	LondonPriWI1	WAN interface
Application	enterprise-http	Application name
ION Flow Type	New Flow	Flow event type
ION Rule	Allow-All	Policy rule name

MITRE ATT&CK Tags

Tag Name	Example	Description
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic

MITRE mappings applied:

- **T1548** (Privilege Escalation) - sudo commands
- **T1110** (Brute Force) - SSH authentication failures
- **T1078** (Valid Accounts) - SSH authentication success
- **T1071** (Application Layer Protocol) - denied flow traffic

Alert Codes

ION devices generate alerts with the following CODE prefixes:

Prefix	Category	Examples
NETWORK_VPN*	VPN/Tunnel	VPNLINK_DOWN, VPNBFD_DOWN, VPNPEER_UNAVAILABLE
NETWORK_DIRECT*	Connectivity	DIRECTINTERNET_DOWN, DIRECTPRIVATE_DOWN
DEVICEHW_*	Hardware	INTERFACE_DOWN, POWER_FAILURE, DISK_FAILURE
DEVICESW_*	Software	PROCESSRESTART, CPU_HIGH, DATABASE_CORRUPT
SPOKEHA_*	HA	FAILOVER

Log Examples

Sudo Command

```
ION_HOST="US-DA7-SDW-102" DEVICE_TIME="2025-11-19T17:47:39.610Z"
MSG="pam-all:root : PWD=/ ; USER=root ; COMMAND=/usr/bin/fp-cpu-usage --json"
SEVERITY="minor" PROCESS_NAME="sudo" FACILITY="authpriv"
ELEMENT_ID="1706032838379022596"
```

SSH Authentication Failure

```
ION_HOST="NZ-AUK-4342-01" DEVICE_TIME="2025-11-19T17:47:39.135Z"
MSG="pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=192.168.1.100 user=admin"
SEVERITY="minor" PROCESS_NAME="sshd" FACILITY="authpriv"
ELEMENT_ID="17249535962630020"
```

VPN Link Down Alert

```
ION_HOST="US-CH3-SDW-203" DEVICE_TIME="2025-11-19T17:47:44.121Z"
STATUS="Not clear" CODE="NETWORK_VPNLINK_DOWN" Severity="major"
VPN_LINK_ID="1742910199997015396" AL_ID="1742909979692020596"
```

```
REASON="NETWORK_VPNBFD_DOWN" IDENTIFIER="1742910199995015196"
ELEMENT_ID="1697819626867008996"
```

VPN Link Restored

```
ION_HOST="US-DA7-SDW-202" DEVICE_TIME="2025-11-19T17:47:50.390Z"
STATUS="cleared" CODE="NETWORK_VPNLINK_DOWN" Severity="major"
VPN_LINK_ID="1742910199080011596" AL_ID="1742909979973021796"
REASON="NETWORK_VPNBFD_DOWN" IDENTIFIER="1742910199053011396"
ELEMENT_ID="1706032829676008596"
```

Flow Log (Allowed)

```
2020-01-28T23:46:17,10.2.53.102,52520,10.2.13.100,80,tcp,,,0,0,0,0,,
LondonPriWI1,15796434157670062,enterprise-http,New Flow,Allow-All:allow:1
```

Flow Log (Denied)

```
2020-01-28T23:50:00,192.168.1.50,44123,8.8.8.8,53,udp,,,0,0,0,0,,WAN1,
15796434157670099,dns,New Flow,Block-DNS:deny:2
```

Triggers

Trigger	Description
`Palo Alto ION: MITRE ATT&CK Threat Detected`	Catch-all for MITRE-mapped events
`Palo Alto ION: SSH Authentication Failure`	SSH auth failure (actionable)
`Palo Alto ION: Privilege Escalation`	Sudo command execution
`Palo Alto ION: VPN Alert Active`	VPN link failure (actionable, notify)
`Palo Alto ION: VPN Alert Cleared`	VPN link recovered
`Palo Alto ION: Network Alert`	Direct internet/private WAN down
`Palo Alto ION: Hardware Alert`	Hardware failure (actionable, notify)

Trigger	Description
`Palo Alto ION: Software Alert`	Software issue (actionable)
`Palo Alto ION: HA Failover`	HA failover event (actionable, notify)
`Palo Alto ION: IKE/IPsec Event`	IKE tunnel events
`Palo Alto ION: Flow Denied`	Blocked network traffic