LOGZILLA DOCUMENTATION

Avaya

LogZilla App Store application: Avaya

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/avaya

Overview

Avaya Communication Manager is an enterprise telephony platform that provides voice communications, unified messaging, and contact center capabilities. The system manages VoIP phone registrations, call routing, and network connectivity for enterprise telephony deployments.

App Function

The Avaya app parses log messages from Avaya Communication Manager and extracts metadata for network connectivity, security threats, system health, and authentication events. The app provides MITRE ATT&CK mapping for security events and Event Class-aligned dashboards for different analyst roles.

Vendor Documentation

- Avaya Aura Communication Manager Support (https://support.avaya.com/support/en/products/P0001/10.2.x)

Device Configuration

To send logs to LogZilla, the Avaya Communications Manager (https://www.logzilla.ai/docs/receiving-data/avaya-communications-manager) must be configured appropriately:

Access the Avaya System Administration Terminal (SAT)
Configure syslog destination with the LogZilla server IP
Enable logging for IP events, security events, and system events
Save the configuration

Incoming Log Format

Log messages are sent as syslog messages from the Communications Manager with program name `logmanager`. The log format uses key-value pairs delimited by = and separated by spaces. Event types are prefixed with category identifiers:

- **IPEVT** - IP/network events (registrations, connections)
- **SECEVT** - Security events (toll fraud, violations)
- **SYSEVT** - System events (failovers, alarms, license warnings)
- **AUTHEVT** - Authentication events (login success/failure)

Event Classes

The app categorizes events into the following Event Classes:

Event Class	Description	Example Events
network	VoIP endpoint connectivity	IPT_REG, IPT_TCP_UP, IPT_TCP_DOWN
security	Security threats and violations	TOLL_FRAUD, SECURITY_VIOLATION
system	System health and alarms	BOARD_ALARM, LICENSE_WARNING
ha	High availability events	PROCR_FAILOVER
auth	Authentication events	LOGIN success/failed

Parsed Metadata Fields

Tag Name	Example	Description
Event Class	network	Cross-vendor event classification
Avaya Event	IPT_TCP_UP	Avaya event type
Avaya Board	PROCR	Avaya board identifier
Board IP	11.22.33.44	IP address of the Avaya board
VoIP IP	55.66.77.88	IP address of the VoIP endpoint
Avaya Reason	recovery	Reason for the event
Station	7768	Station or terminal identifier
User	admin	Username for authentication events
Action	success	Result of authentication attempt
MitreId	T1110	MITRE ATT&CK technique identifier
MITRE Tactic	Credential Access	MITRE ATT&CK tactic category

MITRE ATT&CK Mapping

Event	MITRE Technique	Tactic
TOLL_FRAUD	T1498 (Network Denial of Service)	Impact
SECURITY_VIOLATION	T1110 (Brute Force)	Credential Access
LOGIN failed	T1110 (Brute Force)	Credential Access

Log Examples

VoIP Phone Registration

```
IPEVT IPT_REG board=PROCR ip=11.22.33.44 net_reg= 241 ext= 7768 ip=55.66.77.88; 1024 net_reg= 241
reason=recovery
```

VoIP Phone Network Status Change

```
IPEVT IPT_TCP_UP board=PROCR ip=11.22.33.44 net_reg= 241 ext= 7632 the 1st ip=55.66.77.88;35770 the
2nd ip=0.0.0.0; 0 net_reg= 241 reason=endpoint_request
```

Toll Fraud Detection

```
SECEVT TOLL_FRAUD station=7768 called=19005551234 trunk=1 duration=3600
```

Authentication Failure

```
AUTHEVT LOGIN user=admin station=SAT result=failed reason=invalid_password
```

PROCR Failover

```
SYSEVT PROCR_FAILOVER from=01A07 to=01B07 reason=heartbeat_loss
```

Dashboards

The Avaya app includes the following dashboards:

- **Avaya: Network** - VoIP connectivity events, endpoints, boards, registrations
- **Avaya: Security** - Toll fraud, security violations, MITRE ATT&CK mapping
- **Avaya: Operations** - System health, HA failovers, license warnings, auth events

Triggers

Trigger	Description	Actionable
Avaya: VoIP Endpoint Down	VoIP endpoint disconnection	Yes
Avaya: VoIP Endpoint Up	Endpoint recovery	No
Avaya: Phone Registration	Phone registration	No
Avaya: MITRE ATT&CK Threat Detected	Any MITRE-mapped threat	Yes
Avaya: Toll Fraud Detected	Toll fraud attempt	Yes
Avaya: Security Violation	Security policy violation	Yes
Avaya: Authentication Failure	Failed login attempt	Yes
Avaya: Authentication Success	Successful login	No
Avaya: PROCR Failover	HA failover event	Yes
Avaya: Critical Board Alarm	Critical hardware alarm	Yes
Avaya: License Warning	License expiration warning	Yes