LOGZILLA DOCUMENTATION

Cisco Wlc

LogZilla App Store application: Cisco Wlc

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/cisco—wlc

Overview

Cisco Wireless LAN Controller (WLC) is a family of devices that manage wireless network access points, enabling wireless devices to connect to the network. WLC devices centralize wireless network management, security policies, and user authentication for enterprise wireless deployments. Devices generate syslog messages for client authentication, AP management, rogue detection, and system health.

App Function

- Parse WLC events from AireOS and C9800 IOS-XE controllers
- Extract client authentication metadata (MAC, IP, username, SSID)
- Map security events to MITRE ATT&CK techniques
- Classify events by type (auth, security, network, system)
- Provide Event Class-aligned dashboards for different analyst roles
- Alert on security threats, authentication failures, and system issues

Vendor Documentation

- Cisco Wireless LAN Controllers (https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html)
- System and Message Logging (https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/configuring_system_and_message_logging.html)
- Syslog Server Configuration on Wireless LAN Controllers (https://www.cisco.com/c/en/us/support/docs/wireless/4100-series-wireless-lan-controllers/107252-WLC-Syslog-Server.html)

Device Configuration

GUI Configuration

Log into the WLC web interface
Navigate to **Management** > **Logs** > **Config**
In the **Syslog Server IP Address** field, enter the LogZilla server IP
Click **Add**
Set **Syslog Level** to **Informational** (severity level 6) or **Debugging** (severity level 7) for full visibility
Set **Syslog Facility** to **Local Use 0** (facility level 16) or leave as default
Click **Apply**

CLI Configuration

```
config logging syslog host <logzilla_ip>
config logging syslog level informational
config logging syslog facility local0
```

To configure AP-level logging:

```
config ap logging syslog level informational all
config ap logging syslog host global <logzilla_ip>
```

Verification

Generate test traffic or trigger a configuration change, then verify events appear in LogZilla with `Vendor: Cisco` and `Product: WLC` tags.

Incoming Log Format

Cisco WLC logs use standard Cisco IOS syslog format. The base Cisco app extracts the `cisco_mnemonic` from the message, then the WLC app processes events matching known WLC mnemonics.

```
%FACILITY-SEVERITY-MNEMONIC: message
```

- **FACILITY** - Cisco facility code (APF, DOT1X, CAPWAP, etc.)
- **SEVERITY** - Numeric severity level (0-7)
- **MNEMONIC** - Event type identifier
- **message** - Event description with variable data

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Cisco`	Device vendor
`Product`	`WLC`	Product line
`Event Class`	`auth`	Event classification (auth, security, network, system)

Tag Name	Example	Description
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic
Client MAC	11:22:33:44:cc:dd	MAC address of the wireless client
Client AP MAC	11:22:33:44:aa:bb	MAC address of the access point
Client Username	jsmith	Username of the authenticated client
Client IP	192.168.1.100	IP address assigned to the client
Client SSID	Corporate-WiFi	SSID of the wireless network

Log Examples

DOT1X Authentication Failure

```
%DOT1X-5-FAIL: Chassis 1 R0/7: wncd: Authentication failed for client
(3ecc.5479.faaf) with reason (Timeout) on Interface capwap_91c0051d
```

Client Authenticated

```
%APF-3-AUTHENTICATION_TRAP: apf_80211.c:21442 Client Authenticated:
MACAddress:11:22:33:44:cc:dd Base Radio MAC:11:22:33:44:aa:bb Slot:1
User Name:jsmith Ip Address:192.168.1.100 SSID:Corporate-WiFi
```

Rogue AP Detected

```
%APF-1-ROGUE_AP_DETECTED: Rogue AP detected: MAC aa:bb:cc:dd:ee:ff on channel 6
```

AP Disjoin

```
%CAPWAP-3-AP_DISJOIN: AP 00:11:22:33:44:55 has disjoined from controller
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
DOT1X/EAP failures	T1110	Credential Access
Rogue AP detection	T1200	Initial Access
IP address conflicts	T1557	Credential Access
Client exclusions	T1499	Impact

Dashboards

Dashboards are aligned with Event Class categories for different analyst roles:

Dashboard	Event Class	Description
Cisco Wireless: Security	auth, security	Threats, auth failures, MITRE tactics
Cisco Wireless: Network	network	Client activity, SSIDs, APs, roaming
Cisco Wireless: System	system	Controller health, HA events, errors

Triggers

Trigger	Description
Cisco Wireless: MITRE ATT&CK Threat Detected	Events with MITRE technique mapping
Cisco Wireless: Rogue AP Detected	Unauthorized access point detection (T1200)
Cisco Wireless: Authentication Failure	DOT1X/EAP authentication failures (T1110)
Cisco Wireless: IP Spoofing Detected	IP address conflicts (T1557)
Cisco Wireless: Client Excluded	Client exclusion events (T1499)
Cisco Wireless: AP Disjoin	Access point disconnection

Trigger	Description
Cisco Wireless: HA State Change	High availability failover events
Cisco Wireless: System Critical	Critical system events (severity 0-3)