LOGZILLA DOCUMENTATION

Ruckus Wireless

LogZilla App Store application: Ruckus Wireless

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/ruckus-wireless

Overview

Ruckus Wireless provides enterprise-grade Wi-Fi access points, controllers, and management software for high-density wireless deployments. Ruckus devices generate syslog messages for client authentication, association events, rogue AP detection, and system status. Operators monitor these logs to troubleshoot connectivity issues, detect security threats, and track client activity.

App Function

- Parse Ruckus syslog messages for authentication and client activity events
- Extract metadata tags for filtering and analysis
- Categorize events by type (auth, network, security, config, system)
- Detect rogue access points and ad-hoc networks

Vendor Documentation

- Ruckus Support Portal (https://support.ruckuswireless.com/)
- SmartZone Syslog Configuration (https://docs.ruckuswireless.com/smartzone/3.6.2/sz100-vsze-administrator-guide/GUID-6EE4F072-821C-414F-8F42-531152F27511.html)

Device Configuration

Configure Ruckus devices to send syslog messages to LogZilla:

ZoneDirector / Unleashed

Log into the Ruckus web interface
Navigate to **Admin & Services > System > System Info**
Scroll to **Log Settings** section
Enable **Remote Syslog** and enter the LogZilla server IP address
Select log content: **All Syslog**, **Client Connection Logs Only**, or **Client Flow Data Only**
Optionally enable **Inherit remote syslog server for APs**
Configure **Facility Name** (Keep Original or select facility)
Set **Priority Level** (All or specific level)

SmartZone

Log into the SmartZone web interface

Navigate to **System > General Settings > Syslog**
Select **Enable logging to remote syslog server**
Configure the primary syslog server:

- Enter the LogZilla server IP address
- Enter the port number (default: 514)
- Select protocol (UDP or TCP)
- Click **Ping Syslog Server** to verify connectivity

Configure **Facility** (0-7)
Configure **Filter Severity** (Debug recommended for full visibility)
Select **Event Filter**:

- **All events** - Recommended for full visibility
- **All events except client association/disassociation** - Reduces volume
- **All events above a severity** - Filter by severity level

Click **OK**

Verification

Trigger a client authentication event, then verify events appear in LogZilla with the program name `Ruckus`.

Incoming Log Format

Ruckus syslog messages follow several formats depending on event type:

Authentication Events

```
<date> <device> User[<mac>] fails authentication in WLAN[<wlan>] from AP[<ap>]
```

Client Activity Events

```
<date> <device> User[<mac>] <action> WLAN[<wlan>] from AP[<ap>]
```

Rogue Detection Events

```
<date> <device> A new Rogue [<mac>] with SSID[<ssid>] is detected
```

- **date** - Syslog timestamp

- **device** - Ruckus controller or AP hostname
- **mac** - Client MAC address
- **wlan** - Wireless network name
- **ap** - Access point name
- **action** - Client action (joins, rejoins, leave, disconnects)
- **ssid** - Detected SSID name

Parsed Metadata Fields

Tag Name	Example	Description
`Event Class`	`auth`	Cross-vendor event classification
`Event Type`	`login_failure`	Specific event type (login_failure, intrusion)
`SrcMAC`	`00:11:22:33:44:55`	Client MAC address
`Action`	`fails authentication`	Event action
`Ruckus WLAN`	`Guest`	Wireless network name
`Ruckus AP`	`Lobby-AP1`	Access point name
`Ruckus SSID`	`Corporate`	Detected SSID (rogue events)
`Ruckus Detection Type`	`Rogue`	Detection type (Rogue, ad-hoc)
`Ruckus BSSID`	`aa:bb:cc:dd:ee:ff`	BSSID for WLAN deployments
`Ruckus Radio`	`radio0`	Radio identifier
`Ruckus Reason`	`inactivity`	Disconnect reason

MITRE ATT&CK Mappings

Event	MITRE ID	Tactic
Rogue AP detected	T1200	Initial Access

Event	MITRE ID	Tactic
Ad-hoc network detected	T1200	Initial Access
Authentication failure	T1110	Credential Access

Triggers

Trigger	Description
`Ruckus: MITRE ATT&CK Threat Detected`	Catch-all for any MITRE-mapped threat
`Ruckus: Rogue AP or ad-hoc network detected (T1200)`	Rogue AP or ad-hoc network detected
`Ruckus: Client authentication failure (T1110)`	Client authentication failure
`Ruckus: Client join failure`	Client failed to join WLAN (capacity/config issue)

Log Examples

Authentication Failure

```
Nov 12 10:32:51 device1 User[00:11:22:33:44:55] fails authentication in WLAN[WLAN1] from AP[AP1] for [10 minutes]
```

Client Join

```
Nov  3 23:12:34 device1 User[aa:bb:cc:dd:ee:ff] joins WLAN[Guest] at AP[Lobby1]
```

Rogue AP Detection

```
Nov 10 10:30:15 localhost-1 A new Rogue [00:11:22:33:44:55] with SSID[evil_network] is detected
```

WLAN Deployment

```
Jan  1 00:00:00 device1 WLAN[wlan0] has been deployed on radio [radio0] of AP[ap1] with
BSSID[00:11:22:33:44:55]
```