

Ruijie Integration Guide

This guide walks you through the complete integration between a **Ruijie / Reyee gateway** and Useroam Cloud — captive portal authentication (WiFiDog external portal) and legal 5651 syslog forwarding.

“ **Before you start:** you need administrator access to the Ruijie web interface, the gateway's active WAN IP address, and the hardware serial number printed on the device label.

1 - Adding the device to the Useroam panel

First, sign in to your panel at panel.useroam.com and add a **New Device**.

- **Device Type:** select **Ruijie**.
- **5651 Logging:** tick the 5651 Logging checkbox.
- **Device Serial Number:** **[CRITICAL STEP]** enter the original hardware serial number in full, exactly as printed on the label underneath the device or as shown in the web interface. The Ruijie integration will not work reliably unless this serial number is correct.
- **Device Address:** enter the active WAN IP address the gateway uses to reach the internet.

USEROAM

HOTSPOT & REPORTING

Yeni Cihaz

Cihaz Detayları

Useroam Teknoloji LTD. ŞTİ.

Lütfen hesap seçiniz

Cihaz Tipi
Ruijie

☒ 5651 Loglama

Cihaz Seri Numarası

Cihaz Adresi

Cihaz Adı

Kaydet

2 - Allowlist settings for trusted IPs (Allowlist ? Dest. IP)

In the Ruijie management interface, go to **Object > User Authentication > Authentication Settings** from the top menu. Under the **Allowlist** tab, select the **Dest. IP** option and allow the Useroam Cloud server IP address (`104.247.174.120`) together with your hotspot service networks.

The screenshot displays the Ruijie Cybrey management interface. The top navigation bar includes Home, O&M, Policy, Object, Network, and System. The left sidebar shows a hierarchy of settings, with 'User Authentication' expanded to 'Authentication Settings'. The main content area is titled 'Allowlist' and contains a table of IP addresses.

Sec. IP	Dest. IP	URL	Sec. MAC	Description	Operation
☐	104.247.174.120			-	Edit Delete
☐	157.240.0.0/16			-	Edit Delete
☐	31.13.64.0/18			-	Edit Delete
☐	31.13.24.0/21			-	Edit Delete
☐	179.60.192.0/22			-	Edit Delete
☐	185.60.216.0/22			-	Edit Delete
☐	102.132.96.0/20			-	Edit Delete
☐	129.134.0.0/16			-	Edit Delete
☐	69.171.224.0/19			-	Edit Delete
☐	66.220.144.0/20			-	Edit Delete

3 - Allowlist settings for trusted domains (Allowlist ? URL)

Switch to the **URL** tab in the same menu. Add `*.useroam.com` to the allowlist — guests must be able to reach it *before* they authenticate. Also define URL rules for the messaging and operating-system captive-portal detection domains that mobile devices use to verify the hotspot network in the background (for example the WhatsApp networks).

Ruijie Cybrey

Home O&M Policy Object Network System

Search

Quick Onboarding Policy Wizard Customer Service English admin

Address App Service Region Time Plan User Authentication User Management User Tag Import User User Package Mgmt Online User Authentication Domain Authentication Policy Authentication Template Authentication Settings Authentication Server Content Identification Lib. Content Template Security Rule Base ISP Address Library Certificate

Allowlist SSO Other Authentication Settings

Create Delete Refresh

Search whitelist

Src: IP Dest: IP URL Src: MAC

	Allowlist	Description	Operation
☐	whatsapp.net	-	Edit Delete
☐	whatsapp.com	-	Edit Delete
☐	g.whatsapp.net	-	Edit Delete
☐	v.whatsapp.net	-	Edit Delete
☐	mmg.whatsapp.net	-	Edit Delete
☐	media.whatsapp.net	-	Edit Delete
☐	static.whatsapp.net	-	Edit Delete
☐	cdn.whatsapp.net	-	Edit Delete
☐	web.whatsapp.com	-	Edit Delete
☐	*.useroam.com	useroam.com	Edit Delete

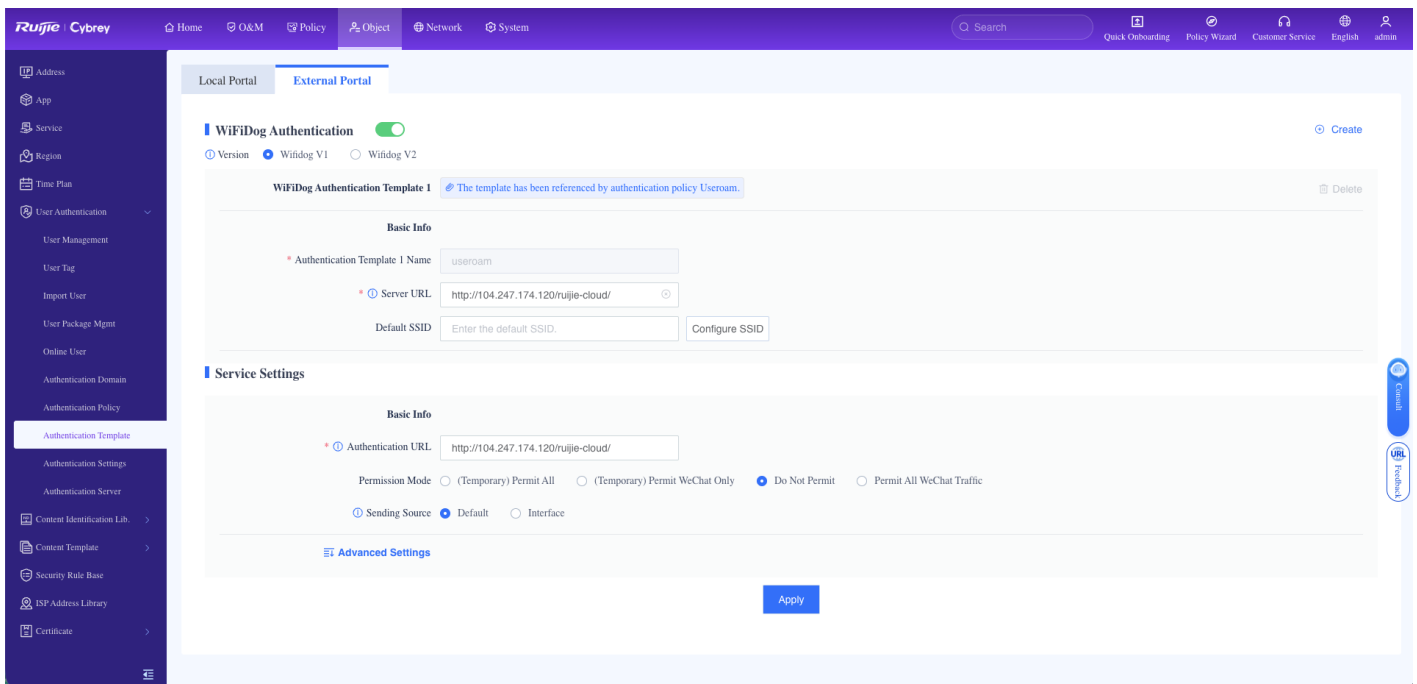
10 / Page Total: 10

Go to 1 < 1 >

4 - External Portal & WiFiDog authentication template

From the left-hand menu, open **Authentication Template** and select the **External Portal** tab. Enable **WiFiDog Authentication**, then create the template:

- **Version:** select **Wifidog V1**.
- **Authentication Template Name:**
- **Server URL:**
- **Permission Mode:** select **Do Not Permit**.
- **Sending Source:** leave as **Default**.



5 - Authentication policy (Edit Authentication Policy)

As the final configuration step, go to **Authentication Policy** in the left menu and either add a new rule or edit your existing guest policy:

- **Name:**
- **Enabled State:** set to **Enable**.
- **Src. Security Zone:** select the zone your guest network belongs to (for example).
- **Src. Address:**
- **Authentication Action:** tick **Authentication**.
- **Authentication Template Name:** select the template you created in the previous step and save.

Ruijie Cybrey Home O&M Policy **Object** Network System Search Quick Onboarding Policy Wizard Customer Service English admin

Address App Service Region Time Plan User Authentication User Management User Tag Import User User Package Mgmt Online User Authentication Domain

Authentication Policy

Authentication Template Authentication Settings Authentication Server

Content Identification Lib. Content Template Security Rule Base ISP Address Library Certificate

Edit Authentication Policy

* Name: Useroam

Enabled State: ☒ Enable ☐ Disable

Description: Enter the authentication policy name description.

* Src. Security Zone: Guest

* Src. Address: any

Authentication Action: ☒ Authentication ☐ Authentication-free

* Authentication Template Name: useroam [Go to Authentication Template](#)

Save

6 - Forwarding logs to Useroam (Syslog config)

So that guest internet traffic and hotspot session activity can be legally signed under Turkish Law No. 5651, the logs must be forwarded to the Useroam Cloud server. In the Ruijie management interface go to **Advanced > Syslog** and use the **Add** button to define a new syslog server:

- **Syslog Server Status:** set to **Enable**.
- **Server IP:** enter the Useroam Cloud IP address `104.247.174.120`.
- **Server Port:** `514` (the default syslog port).

Ruijie Cybrey Home O&M Policy Object **Network** **System** Search Quick Onboarding Policy Wizard Customer Service English admin

Admin Account Mgmt Role Mgmt System Config Association Config Log Config Cloud Management Platform UX Improvement Plan Signature Library Upgrade Overload Protection High Availability Info Push System Maintenance

SYSLOG Settings Storage Mgmt

The SYSLOG protocol can be used to send firewall logs to a third-party log analysis platform for unified storage, analysis, and processing. DHCP logs can be displayed only after a DHCP server is configured and enabled. Note: When the fast SYSLOG forwarding feature is enabled, it will occupy bandwidth and affect existing network services. Exercise caution when performing the operation. If the log type includes logs generated on the forwarding plane, SYSLOG fast forwarding will be automatically enabled. When the MGMT management interface is used as the SYSLOG log forwarding outlet, the normal forwarding mode is used by default and the fast forwarding is not supported.

Fast SYSLOG Forwarding: ☒

SYSLOG Server1 Delete

* Server IP: 104.247.174.120

* Port: 514

Device SN Field Name: Enter the device SN field name.

* Standard Protocol Version: ☐ rfc3164 ☒ rfc5424 ☐ USER

Log Language Encoding: Default Format

* Logs to Be Sent to SYSLOG Server

☐ System Log [Edit Template](#)

☒ Session Log [Edit Template](#)

☒ Send All Session Logs ☐ Send NAT Logs Only

☐ Security Log [Edit Template](#)

Save

SYSLOG Server2

Create

Important — integration complete

That's it. Useroam Cloud Hotspot and the legal 5651 syslog integration are now fully configured on your Ruijie / Reyee gateway. Remember to update the Useroam panel whenever the device serial number or WAN IP address changes, otherwise the integration will stop working. For assistance during the process, contact our technical team at **destek@useroamteknoloji.com**.

Login with WhatsApp — firewall allowlist (walled garden)

For the **Login with WhatsApp** flow to work while the guest is still behind the captive portal (before internet access is granted), the following addresses **must be allowed** in your firewall or walled-garden configuration. Without these rules the WhatsApp login screen will not open and the automatic login based on delivery confirmation will not work.

Domains to allow (FQDN)

- *.wa.me
- *.whatsapp.com
- *.whatsapp.net
- g.whatsapp.net
- mmg.whatsapp.net
- fbsbx.com
- *.useroam.com

IP addresses to allow

- 157.240.0.0 — Meta / Facebook network block
- 31.13.0.0 — Meta / Facebook network block
- 104.247.174.120 — Useroam panel

Note: 157.240.0.0 and 31.13.0.0 are typically /16 network blocks (Meta infrastructure); we recommend defining them as blocks in the firewall (157.240.0.0/16, 31.13.0.0/16). 104.247.174.120 is the Useroam panel IP (/32). Use the domain list if your firewall supports FQDN-based filtering; otherwise use the IP blocks.

Revizyon #1

tugay tarafından 10 Ağustos 2026 22:55:57 oluşturuldu

tugay tarafından 10 Ağustos 2026 22:55:57 güncellendi