



# Ruijie Easy Gateway 2100-P V2 PoC Guide (V1.2)

## Copyright Statement

Ruijie Networks©2013

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

 ,  ,  ,  ,  ,  
 ,  ,  ,  ,  ,  
 ,  are registered trademarks of Ruijie Networks. Counterfeit is strictly prohibited.

## Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# Preface

*This document providing technical guidance to help engineers testing Easy Gateway products. This document may contain scenario, configuration, command, screenshot image, topology and any related material. This document may not help to solve a similar case due any differences in the real conditions.*

## Audience

- Network Engineers
- Network Administrator

## Obtain Technical Assistance

- Ruijie Networks Websites: <http://www.ruijienetworks.com>
- Ruijie Service Portal: <http://caseportal.ruijienetworks.com>

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

## Related Documents

- RG-EG Implementation Cookbook (V1.0)  
[https://www.ruijienetworks.com/support/documents/slide\\_75371](https://www.ruijienetworks.com/support/documents/slide_75371)
- Ruijie EG Security Gateway datasheet\_EG2100P EG3250  
<https://www.ruijienetworks.com/resources/preview/75394>
- RG-EG2100-P V2 Hardware Installation and Reference Guide  
<https://www.ruijienetworks.com/resources/preview/75320>
- RG-EG Series Gateway Web-Based Configuration Guide, Release 11.9(1)B11S1  
<https://www.ruijienetworks.com/resources/preview/75237>

## Revision History

Date	Change contents	Reviser
2019.09.23	Initial publication V1.0	Ruijie GTAC
2019.09.24	Ruijie Easy Gateway 2100-P V2  PoC Guide (V1.1)  1. Change 3.9.1 Resource Cache Checking as Mobile App Caching  and add it on 2. Test Items Summary;  2. Place 3.2 Login EG's WEB via Cloud to 3.4 Cloud && App  Monitoring section;  3. Change the diagram sequence of section 3.1 Mobile App Quick  Provisioning.	Ruijie GTAC
2021.05.21	Ruijie Easy Gateway 2100-P V2  PoC Guide (V1.2)  Add the L2TP over IPsec VPN	Ruijie GTAC

## 1. Ruijie Easy Gateway Testing List



## 2. Test Items Summary

Category	Test Item	Description	Pass	Fail
1. Mobile App Provisioning	Mobile App Quick Provisioning	EG quick setup via Ruijie Cloud App, and device should online on Cloud		
2. Basic Network Testing	DHCP Sever	Enable service DHCP and create IP Pool Test from laptop or wifi		
	DHCP Client	Only apply on WAN interface		
	WAN Uplink	WAN PPPoE or DHCP as Internet Uplink		
	DNS Proxy	Enable EG as DNS Server		
	Dual WAN Uplink (Optional)	EG support two WAN Uplink to access internet, and load balance		
	Internet Connectivity	Client should connect to Internet successfully		
3. Online Behavior Management	App Blacklist	Block Facebook Keyword : Facebook_Messenger		
		Block Youtube		
	Block User Access	Adding user (Name/IP) to blacklist		

	Block chat / messenger application	Whatsapp		
4. Cloud & App Monitoring	Login EG's WEB via Cloud	Opening EG WEB via Ruijie Cloud Web UI and access successfully		
	Cloud (Web UI) Monitoring	Monitoring EG device and WAN/LAN status on Ruijie Cloud WEB		
	Ruijie Cloud App Monitoring	Monitoring EG device and WAN/LAN status Ruijie Cloud App (IOS or Android)		
5. Authentication Acceleration (EG Offload)	Synchronize Voucher/Account to EG	Using Ruijie Cloud created Voucher to log in with Portal WiFi (SSID)		
	Speed Limit	Using different Voucher Profile with varies speed limit, and create two Voucher code to log-in to get different speed control		
	Seamless Authentication	User can seamless online directly at next time connected WiFi without login again		
	Compatibility test of EG local authentication	Compatibility test of EG local authentication		
6. Internet Access Log Audit	User internet access log checking	User access log (such as visited URL, source/dest IP, MAC, etc.) should send out via HTTP/FTP to Ruijie provided Log Server		
7. IPSEC VPN	IPSEC VPN	The HQ and branch gateway use static IP addresses. The HQ gateway needs to verify the IP address of the branch gateway.		
8. L2TP VPN	L2TP over IPsec	Branch and clients create the L2TP over IPsec VPN with HQ		
9. Resource Cache	Mobile App Caching	Resource cache can reduce bandwidth usage and save users from waiting for access.		

Note: Before PoC, please check whether the EG has been upgrade to the latest version by execute

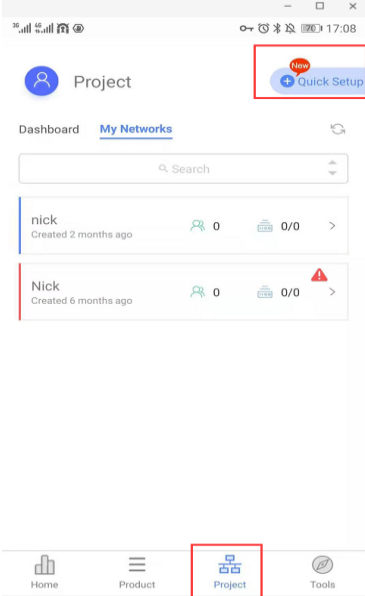
command *“show version detail”*, the example is shown as below:

```

EG#show version detail
System description      : Ruijie EASY GATEWAY(EG2100-P) by Ruijie Networks.
System start time      : 1970-01-01 08:00:00
System uptime          : 0:00:06:50
System hardware version : 2.00
System software version : EG_RGOS 11.9(1)B11S1, Release(06161713)
System patch number    : NA
System software number  : M13125204172019
System serial number    : H1MB0G8002959
System boot version     : 2.2.2.302c1ba(180810)
System core version     : 2.6.32.7efa46adabe6c8
System cpu partition    : 1-3
  
```

### 3. Testing Lists

#### 3.1 Mobile App Quick Provisioning

Testing Project	APP dummy provisioning
Testing Purpose	EG quick setup configuration via Ruijie Cloud App, and online on Ruijie Cloud
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>1. Power on the EG, the AP connect to the EG LAN interface.</li> <li>2. After AP power on, The AP will broadcast the default SSID name to RJ-xxxxxx (xxxxxx is the last six digits of EG2100-P SN)</li> <li>3. Launch Ruijie Cloud APP and Tap Project menu, click Quick Setup to start configuration</li> </ol>  <ol style="list-style-type: none"> <li>4. App will open the EG2100-P initial configuration wizard and log in to the EG2100-P with default account (Username: admin, Password: admin).</li> </ol>



← Quick Setup Guide ...



Ruijie Cloud offers an easy way to set up a network. Firstly, is there a gateway (EG2100-P) in your network?

Yes

No

▶ How to use Ruijie Cloud?  
How to use Ruijie Cloud?

Skip →

← Quick Setup Guide ...



### Easy Gateway

Multi-Function, Easy Management, Low Cost

Please enter the username **admin**

Please enter the password **admin**

Log In

Forgot password? ● ●

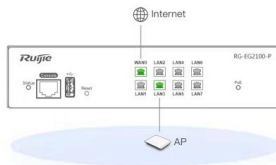
Log in with the default account: **admin/admin**. Complete the Gateway Wizard to configure the WAN port(PPPOE, Static IP or DHCP).

Note: Please ensure that the EG is ready for configuration.

OK. Select WiFi

Skip →

← Quick Setup Guide ...



Power on the device and connect the AP to any port(except WAN) on the gateway.

Note: Gateway must be in the factory default settings, or you need to reset it. (press the Reset button for more than 3 seconds)

Next

← Quick Setup Guide ...



Connect to the WiFi RJ\_XXXXXX after AP and EG are powered on for 3 min.

Next

← Quick Setup Guide ...

Create Network

Set up a new network

Network: |

SSID: @Ruijie-WiFi

Encryption:

Create

Enter the network name and SSID, and select an encryption mode.

Next

Skip →

← Quick Setup Guide ...

My Networks

Dashboard My Networks

% Search

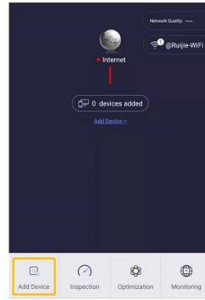
Demo	Created a few seconds ago	0	0/0	>
Office_A	Created 3 minutes ago	0	0/0	>
Office_B	Created 3 minutes ago	0	0/0	>

Tap the network to open its dashboard and add devices.

Next

← Quick Setup Guide

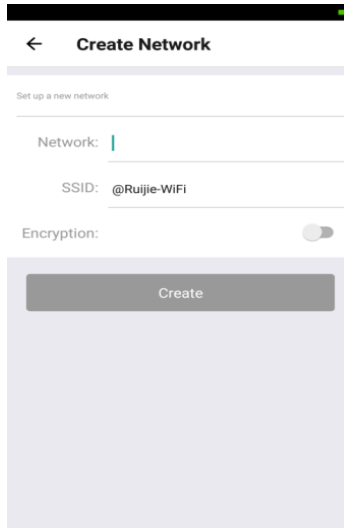
Add Device

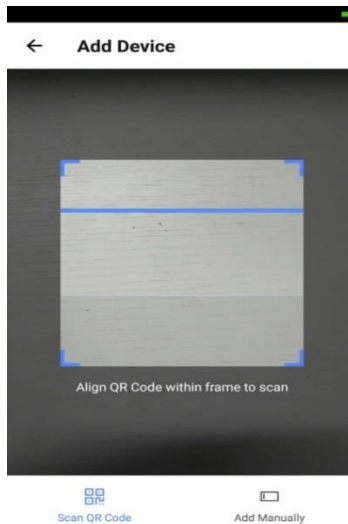
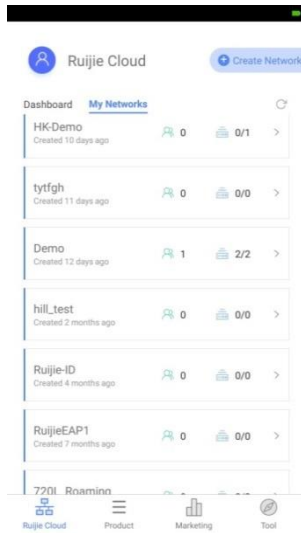


Tap "Add Device" and scan the QR-code on the device.

Start

5. Click Start, and set the network SSID. After the network is created, then enter the network and click Add Device to add AP and EG2100-P through scanning the QR code (AP SN/MAC) on the back of the device. **Note: When adding an EG device, you need to enter the WEB management password of the EG device.**



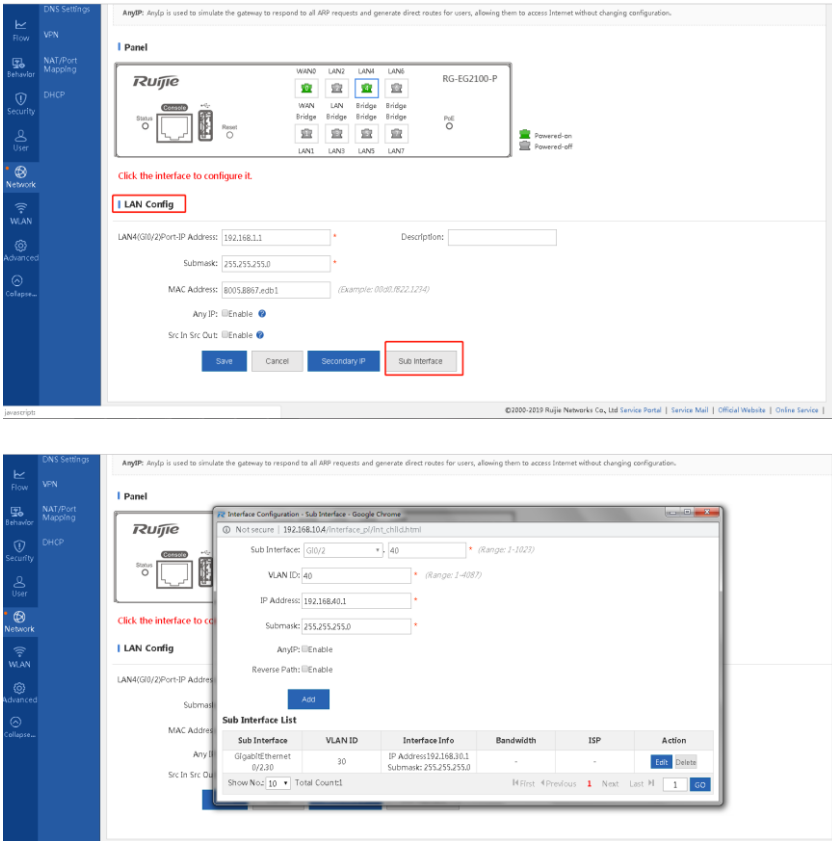


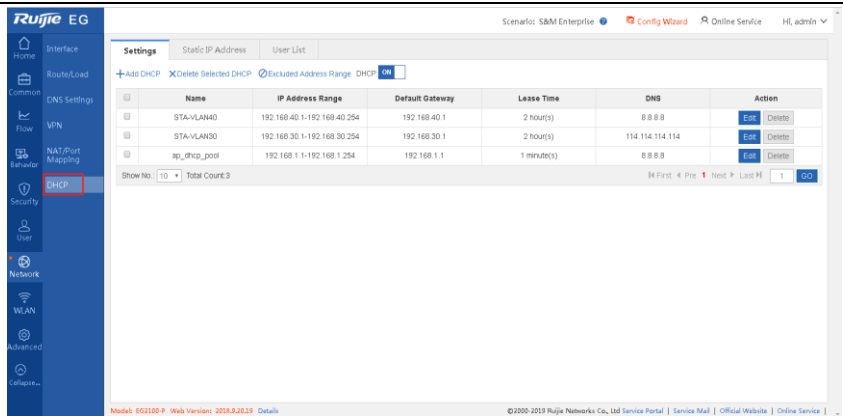
Measured record:

Testing conclusion:

## 3.2 Basic Network Testing

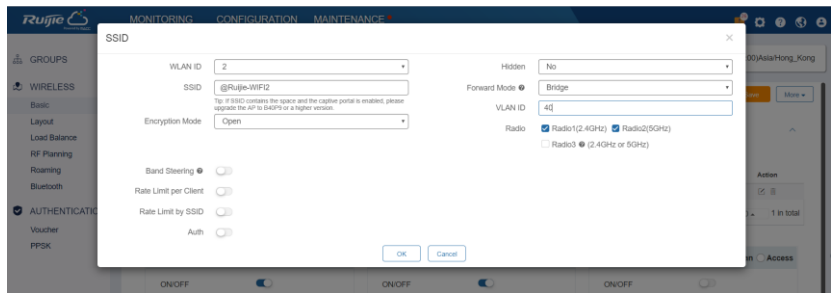
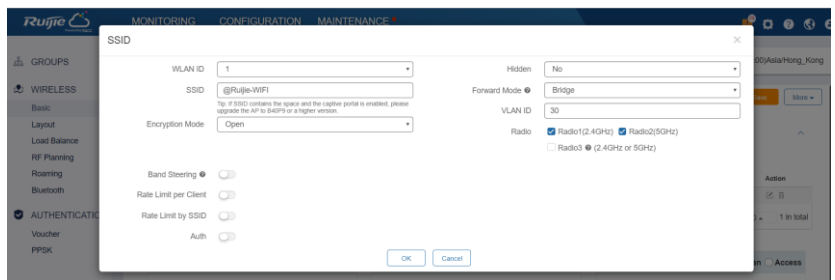
### 3.2.1 DHCP Server

Testing project:	DHCP server												
Testing purpose:	EG as DHCP Server, Clients can get DHCP IP from EG normally												
Testing procedure and expected results:	<p>1. Enable the DHCP server in EG and configure the DHCP pool for AP and STA with different VLANs.</p> <p>Add the sub interfaces with different VLAN in LAN</p>  <p>The screenshot shows the Ruijie EG configuration interface. The top part displays the LAN Config page for LAN4(G0/0/2) with IP Address 192.168.1.1, Submask 255.255.255.0, and MAC Address 8005.8867.fcd1. The 'Sub Interface' button is highlighted. The bottom part shows the Sub Interface Configuration dialog for Sub Interface G0/0/2:40, with VLAN ID 40, IP Address 192.168.40.1, and Submask 255.255.255.0. Below the dialog is a 'Sub Interface List' table:</p> <table border="1"> <thead> <tr> <th>Sub Interface</th> <th>VLAN ID</th> <th>Interface Info</th> <th>Bandwidth</th> <th>ISP</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>GigabitEthernet 0/0/2:40</td> <td>40</td> <td>IP Address: 192.168.40.1 Submask: 255.255.255.0</td> <td>-</td> <td>-</td> <td>Edit Delete</td> </tr> </tbody> </table> <p>Configure the DHCP pool</p>	Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action	GigabitEthernet 0/0/2:40	40	IP Address: 192.168.40.1 Submask: 255.255.255.0	-	-	Edit Delete
Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action								
GigabitEthernet 0/0/2:40	40	IP Address: 192.168.40.1 Submask: 255.255.255.0	-	-	Edit Delete								

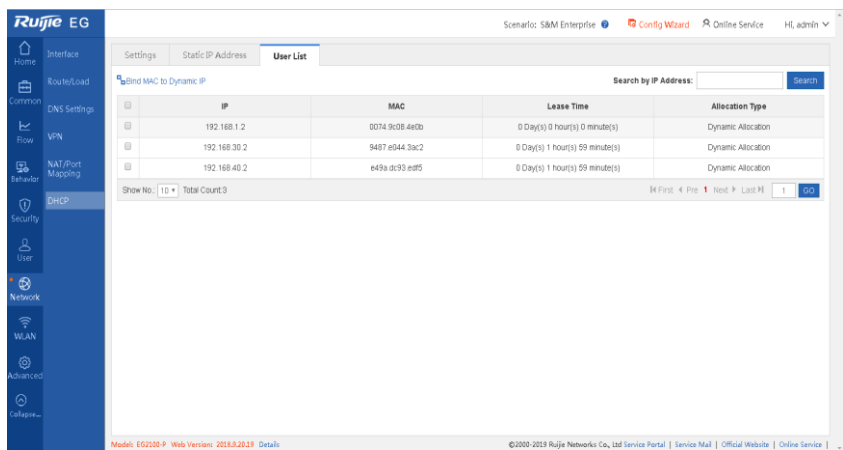


2. AP connect to the EG and configure the STA VLAN, AP and STAs can get the correct IP address.

Configure the STA VLAN via Ruijie Cloud:



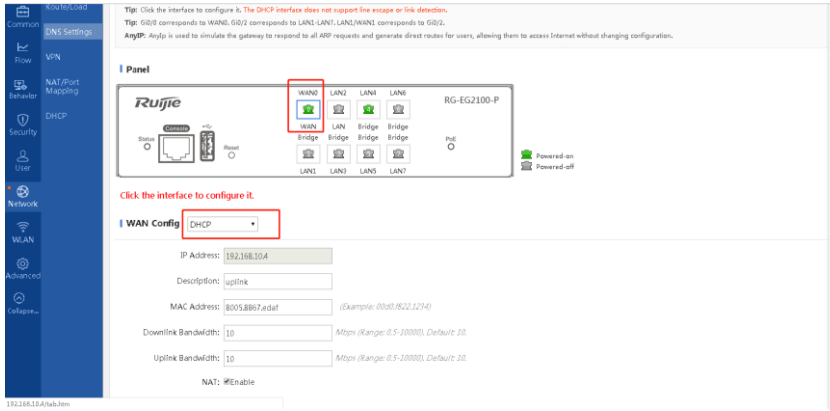
Check the DHCP user list



Measured record:

Testing conclusion:

### 3.2.2 WAN Uplink

Testing project:	WAN uplink (This step is covered during App provisioning, at here you can change WAN Uplink with other ways, such as PPPoE or Static IP)
Testing purpose:	WAN PPPoE, Static or DHCP IP as Internet Uplink
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>1. Configure the EG uplink connection mode (PPPoE/Static/DHCP) and connect it correctly. EG can access the Internet correctly.</li> </ol>  <ol style="list-style-type: none"> <li>2. Connect to EG with wireless and wire user, an access the Internet correctly.</li> </ol>
Measured record:	
Testing conclusion:	

### 3.2.3 Dual WAN Uplink (Optional)

Testing project:	Dual WAN uplink
Testing purpose:	EG support two WAN Uplink to access internet, and load balance
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>1. Configure the EG uplink connection mode (PPPoE/Static/DHCP).</li> <li>2. Add the sub interface with different vlan in the WAN, configure the account info in different sub interface.</li> </ol>

**Panel**

Ruijie RG-EG2100-P

Click the interface to configure it.

**WAN Config** Static IP Address

WAN1(Gi0/1)Port-IP Address:  \*

Submask:  \* Next Hop IP:  \*

Description:

MAC Address: 8005.8867.edd7 (Example: 00d0.1b22.1234)

Downlink Bandwidth: 10 Mbps (Range: 0.5-10000). Default: 10.

Uplink Bandwidth: 10 Mbps (Range: 0.5-10000). Default: 10.

Default Route:  Enable

NAT:  Enable

Src In Src Out:  Enable

Save Cancel **Sub Interface**

### Add the sub interfaces and configure the username/password

▲ Not secure | 172.31.61.20/interface\_pi/int\_child.html

Sub Interface: Gi0/1 | 4 (Range: 1-1023)

VLAN ID: 4 (Range: 1-4087)

Type: PPPoE(ADSL)

Username: test Password: \*\*\*\*

MAC: DC76.5815.C0dE (Format: 0023.AE86.B3E0)

Downlink Bandwidth: 2 Mbps Uplink Bandwidth: 0.5 Mbps

Default Route:  Enable

**Add**

#### Sub Interface List

Interface Configuration - Sub Interface - Google Chrome

▲ Not secure | 172.31.61.20/interface\_pi/int\_child.html

Sub Interface: Gi0/1 | (Range: 1-1023)

VLAN ID: (Range: 1-4087)

Type: DHCP

Downlink Bandwidth: 10 Mbps Uplink Bandwidth: 10 Mbps

Reverse Path:  Enable

**Add**

#### Sub Interface List

Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action
GigabitEthernet 0/1.5	5	Username: ruijie IP Address: 192.168.200.2 Submask: 255.255.255.255	2	Others	<a href="#">Edit</a> <a href="#">Delete</a>
GigabitEthernet 0/1.4	4	Username: test IP Address: 192.168.100.2 Submask: 255.255.255.255	2	Others	<a href="#">Edit</a> <a href="#">Delete</a>

show No.: 10 Total Count: 2 14 First 4 Previous 1 Next Last 1 GO

### 3. Connect the WAN correctly and enable the load balance.

Enable the load balance



### Set the interface's weight

**Tip:** By default, the multi-link load balance regards the bandwidth value as its weight value. Users can change the weight in the following conditions. If the bandwidth usage of an interface is small/large, please increase/decrease its weight so that to increase/decrease the bandwidth usage.

Interface:

Weight:  \* (1~40000000)

Interface	Weight	Action
dialer 1	2000 (Default: 2000)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
dialer 2	2000 (Default: 2000)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.:  Total Count:2

### Configure the default route

**Priority:** The policy-based route and IP-based route both serve packet forwarding. When they exist at the same time, the priority is listed as follows: policy-based route > static route > default route.

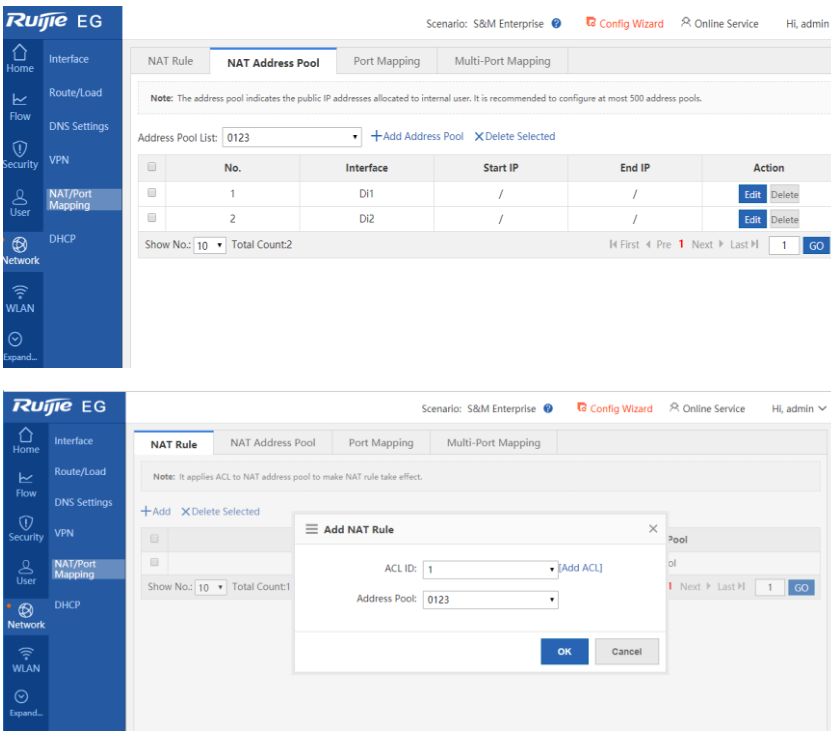
**IP-Based Route:** It can transmit packet according to the specified path and includes static route, address database and default route. Among them, the default route has the lowest priority.

+ Add Static Route + Add Default Route Filter Criteria:

Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
0.0.0.0	0.0.0.0		dialer 1	Primary Route	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
0.0.0.0	0.0.0.0		dialer 2	Primary Route	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.:  Total Count:2

### Add the NAT outside interface and NAT rule

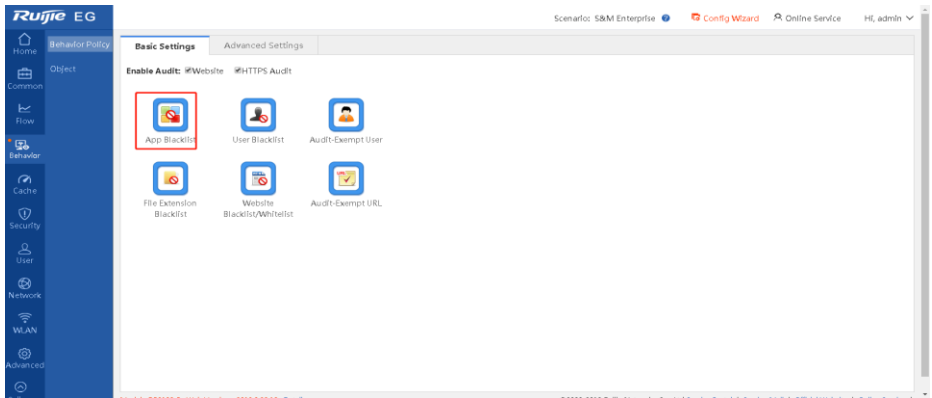
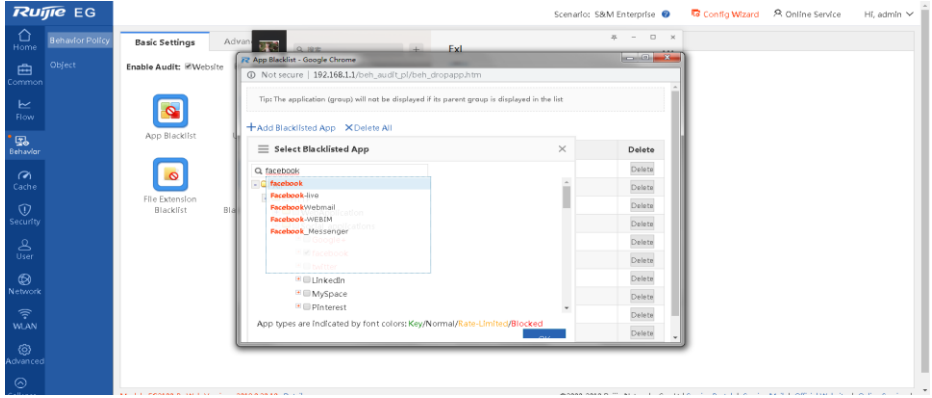
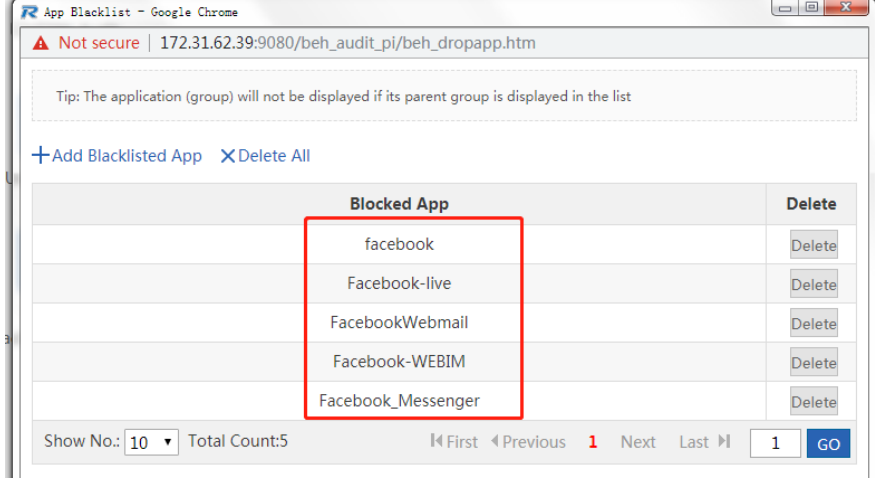
	 <p>4. Monitor the load balance in Traffic Monitoring</p>
Measured record:	
Testing conclusion:	

### 3.2.4 Internet Connectivity

Testing project:	Internet connectivity
Testing purpose:	Client should connect to Internet successfully
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>1. Make sure the EG uplink connection is ok.</li> <li>2. The AP access to the EG, obtains an ip address from the EG, and releases the SSID. The STAs can browse the webpage and the video.</li> <li>3. The PC accesses the EG to obtain an IP address, and can browse the webpage and the video normally.</li> </ol>
Measured record:	
Testing conclusion:	

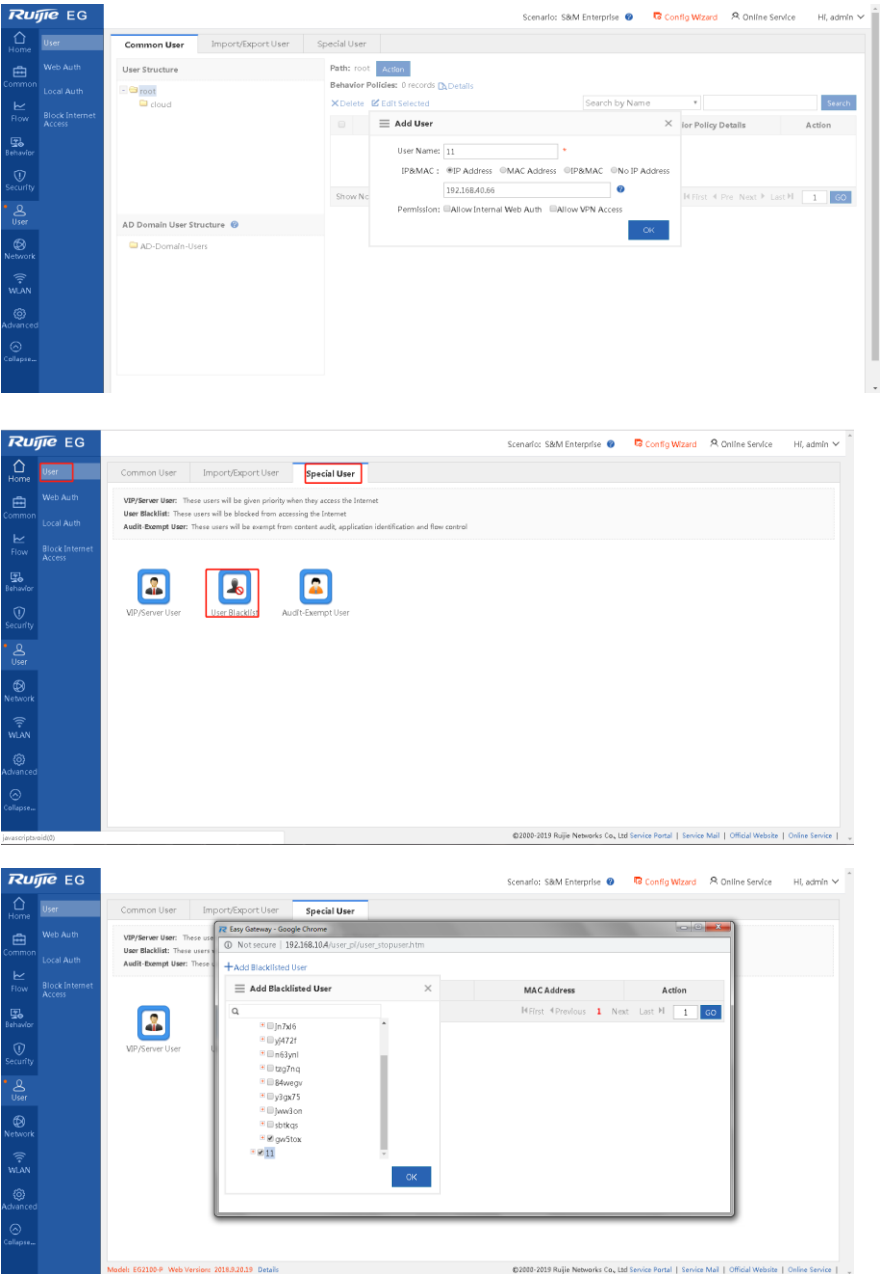
### 3.3 Online Behaviour Management

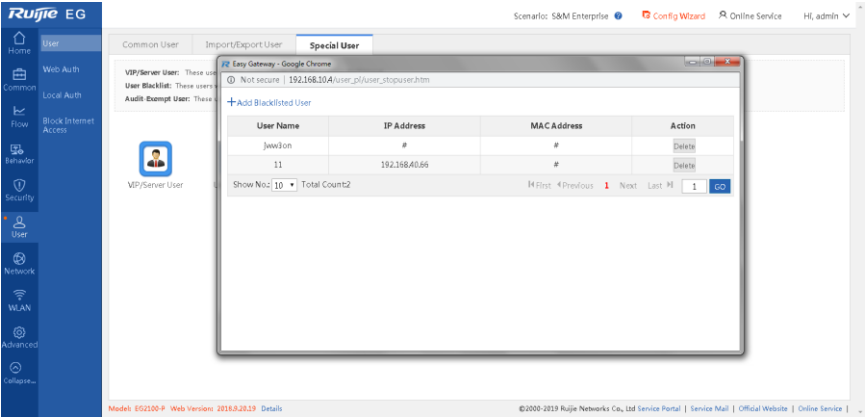
#### 3.3.1 Block Facebook/Youtube Access

Testing project :	Block access
Testing purpose :	Block Facebook access
Testing procedure and results:	<p>1. Add the Facebook Applications to App Blacklist</p>    <p>2. STA connect to EG access to the Facebook with APP and Website, it will be</p>

	blocked, other websites can be accessed successfully.
Measured record:	
Testing conclusion:	

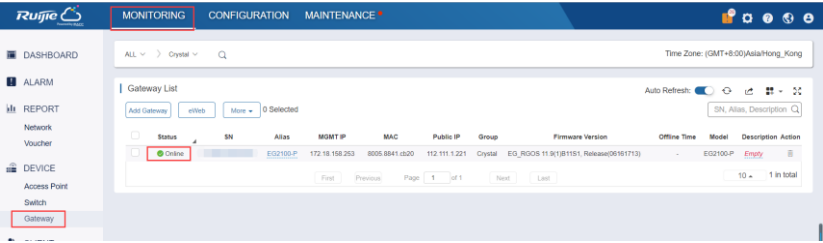
### 3.3.2 Block User Access

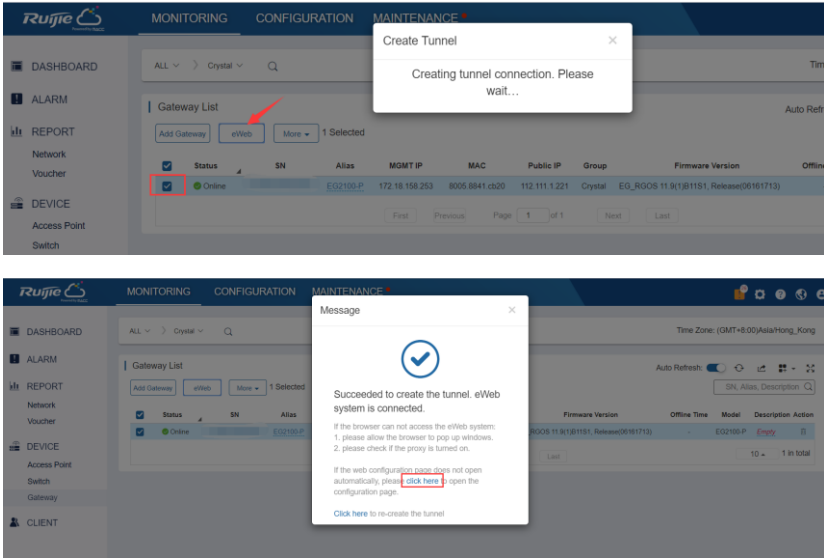
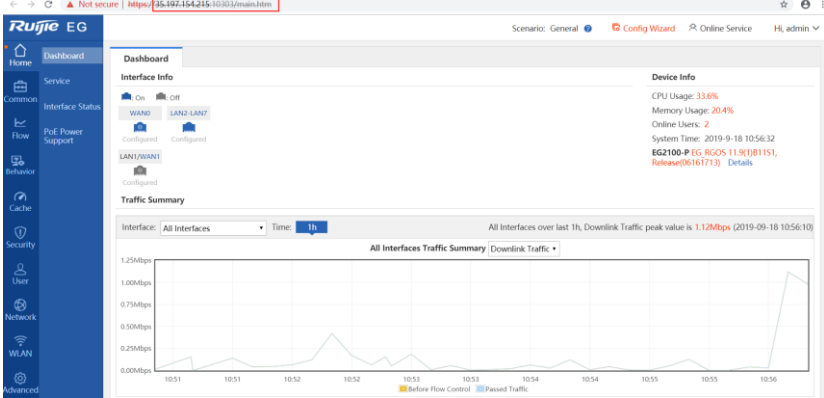
Testing project:	Blacklist
Testing purpose:	Add user(Name/IP) to blacklist
Testing procedure and expected results:	<p>1. Add the users with name or IP range, then add the user to blacklist.</p> 

	 <p>2. STA connect to EG with the user in blacklist and try access to the internet, he will be blocked.</p>
Measured record:	
Testing conclusion:	

### 3.4 Cloud & App Monitoring

#### 3.4.1 Login EG WEB via Cloud

Testing project:	EG WEB configuration
Testing purpose:	Cloud open EG WEB and access successfully
Testing procedure and expected results:	<p>4 Make sure the EG online on Cloud.</p>  <p>5 Connect the eWeb in Ruijie Cloud, it will create the tunnel to EG from Ruijie Cloud.</p>

	 <p>6 Now you can configure the EG by eWeb from Ruijie Cloud.</p> 
Measured record:	
Testing conclusion:	

### 3.4.2 Cloud Monitoring

Testing project:	Monitoring(Ruijie cloud)
Testing purpose:	EG overview status and WAN/LAN status can be monitoring on Ruijie Cloud WEB
Testing procedure and expected results:	1. Ruijie cloud can monitor the device status, including device details, traffic information, current user, interface status and alarm. The CWMP interface can work normally.

**Ruijie** MONITORING CONFIGURATION MAINTENANCE

Diagnose Tool eWeb Telnet More

Update Time: 2019-09-18 11:01:38

WLAN LAN Disconnected Disabled

PPPoE Static IP DHCP P2E Anomalous Copper SFP

Basic  
 Alias: EG2100-P  
 MGMT Password: \*\*\*\*\*  
 Device Model: EG2100-P  
 SN: \*\*\*\*\*  
 MAC: 8005.8841.d200  
 Firmware Version: EG\_R00S 11.9(1)B151; Release(20161113)  
 MGMT IP: 172.18.158.253  
 Description: /

Overview WAN LAN Config PoE Alarm Tunnel

Port	Physical Port	PoE-capable	PoE Status	Power	PD class
port0	GG0	Enable	Off	0.0W	Unknown
port1	GG1	Enable	Off	0.0W	Unknown
port2	LAN 2	Enable	Off	0.0W	Unknown
port3	LAN 3	Enable	Off	0.0W	Unknown
port4	LAN 4	Enable	Off	0.0W	Unknown
port5	LAN 5	Enable	Off	0.0W	Unknown
port6	LAN 6	Enable	On	3.1W	3
port7	LAN 7	Enable	Off	0.0W	Unknown

**Ruijie** MONITORING CONFIGURATION MAINTENANCE

Diagnose Tool eWeb Telnet More

Update Time: 2019-09-18 11:01:38

WLAN LAN Disconnected Disabled

PPPoE Static IP DHCP P2E Anomalous Copper SFP

Basic  
 Alias: EG2100-P  
 MGMT Password: \*\*\*\*\*  
 Device Model: EG2100-P  
 SN: \*\*\*\*\*  
 MAC: 8005.8841.d200  
 Firmware Version: EG\_R00S 11.9(1)B151; Release(20161113)  
 MGMT IP: 172.18.158.253  
 Description: /

Overview WAN LAN Config PoE Alarm Tunnel

CPU & Memory Usage Device Status Connectivity

CPU Usage: 18.0% Memory Usage: 19.9%

Online Status: Online Clients: 2 Sessions: 37

Connectivity: Last 24 Hours Last 7 Days

2019-09-17--2019-09-18 Rate Summary

2019-09-17--2019-09-18 Client Summary

https://cloud-as.ruijienetworks.com/admin3?sessionId=975873263f68EEA2FC26A9D3637E0F

**Ruijie** MONITORING CONFIGURATION MAINTENANCE

Diagnose Tool eWeb Telnet More

Update Time: 2019-09-18 11:01:38

WLAN LAN Disconnected Disabled

PPPoE Static IP DHCP P2E Anomalous Copper SFP

Basic  
 Alias: EG2100-P  
 MGMT Password: \*\*\*\*\*  
 Device Model: EG2100-P  
 SN: \*\*\*\*\*  
 MAC: 8005.8841.d200  
 Firmware Version: EG\_R00S 11.9(1)B151; Release(20161113)  
 MGMT IP: 172.18.158.253  
 Description: /

Overview WAN LAN Config PoE Alarm Tunnel

2019-09-17--2019-09-18 Rate Summary

2019-09-17--2019-09-18 Client Summary

2019-09-17--2019-09-18 CPU/Memory Summary

2019-09-17--2019-09-18 Session Summary

https://cloud-as.ruijienetworks.com/admin3?sessionId=975873263f68EEA2FC26A9D3637E0F

**Ruijie** MONITORING CONFIGURATION MAINTENANCE

Diagnose Tool eWeb Telnet More

Update Time: 2019-09-18 11:01:38

WLAN LAN Disconnected Disabled

PPPoE Static IP DHCP P2E Anomalous Copper SFP

Basic  
 Alias: EG2100-P  
 MGMT Password: \*\*\*\*\*  
 Device Model: EG2100-P  
 SN: \*\*\*\*\*  
 MAC: 8005.8841.d200  
 Firmware Version: EG\_R00S 11.9(1)B151; Release(20161113)  
 MGMT IP: 172.18.158.253  
 Description: /

Overview WAN LAN Config PoE Alarm Tunnel

Top 10 Applications by Traffic

No.	Application	Traffic
1	DNS	0.00 B + /377.00 B +
2	SYNACK	0.00 B + /0.00 B +

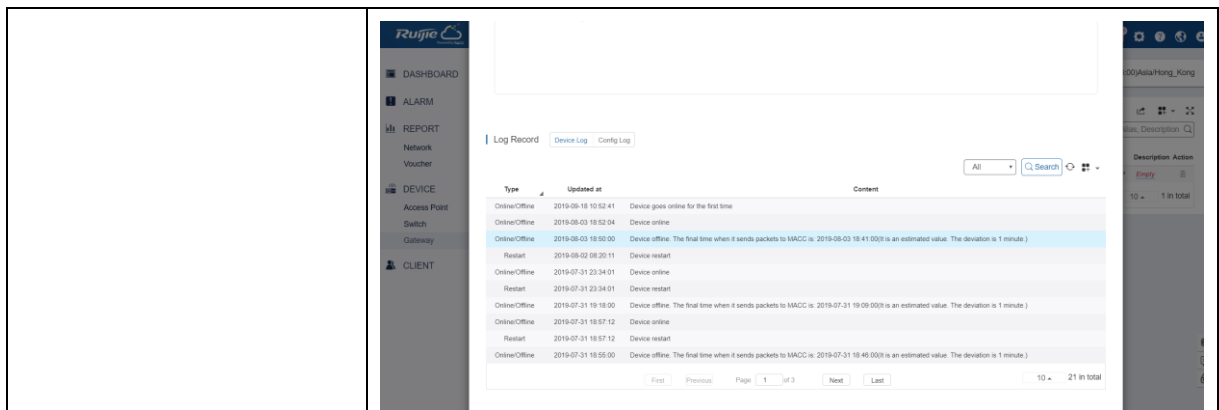
Top 10 Users by Traffic

No.	Username	Traffic
1	192.168.1.3	0.00 B + /377.00 B +

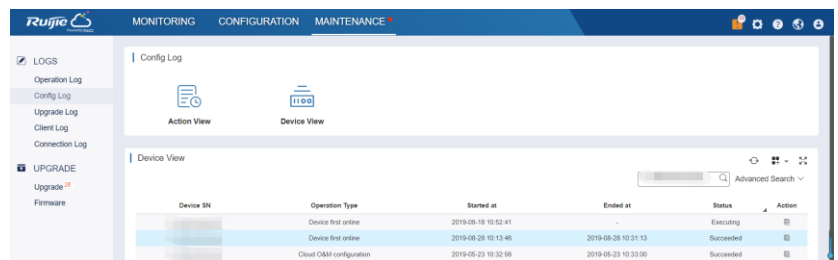
Log Record Device Log Config Log

All Search

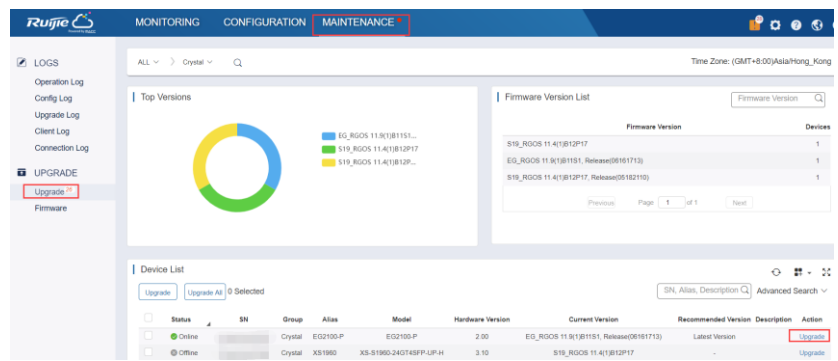
Type	Updated at	Content
Online/Offline	2019-08-18 10:52:41	Device goes online for the first time
Online/Offline	2019-08-03 18:52:04	Device online
Online/Offline	2019-08-03 18:50:00	Device offline. The final time when it sends packets to MACC is: 2019-08-03 18:41:00(0) is an estimated value. The deviation is 1 minute.)
Restart	2019-08-02 08:20:11	Device restart
Online/Offline	2019-07-31 23:34:01	Device online
Restart	2019-07-31 23:34:01	Device restart
Online/Offline	2019-07-31 19:19:00	Device offline. The final time when it sends packets to MACC is: 2019-07-31 19:09:00(0) is an estimated value. The deviation is 1 minute.)
Online/Offline	2019-07-31 18:57:12	Device online
Restart	2019-07-31 18:57:12	Device restart
Online/Offline	2019-07-31 18:55:00	Device offline. The final time when it sends packets to MACC is: 2019-07-31 18:46:00(0) is an estimated value. The deviation is 1 minute.)



2. Ruijie Cloud support grouping function, report log function is normal



3. Ruijie Cloud can upgrade the device version.



Measured record:	
Testing conclusion:	

### 3.4.3 Ruijie Cloud App Monitoring

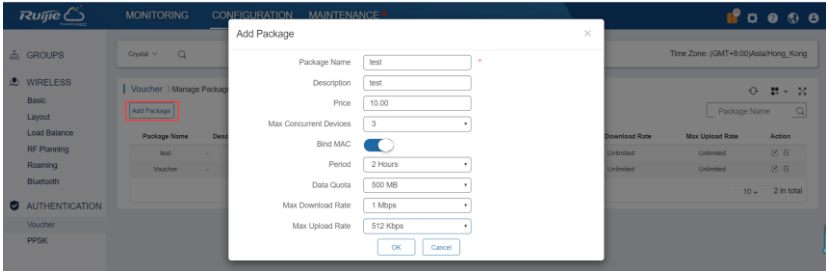
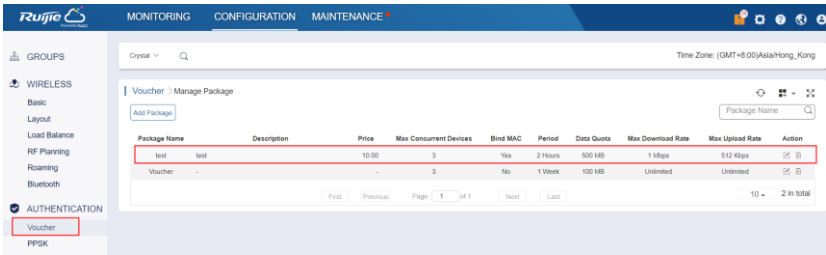
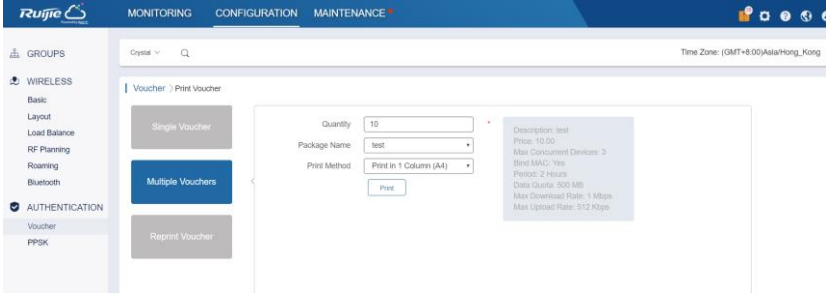
Testing project:	Monitoring(Ruijie cloud APP)
Testing purpose:	Ruijie Cloud App(IOS or Android) monitoring EG status(IOS and Android)
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>1. Ruijie cloud can monitor the device info, system status, clients status, applications status and log.</li> <li>2. Using the Ruijie Cloud APP to add, delete, and configure devices. You can synchronize them under the same account of the Ruijie Cloud.</li> <li>3. Support IOS or Android version.</li> </ol>



Measured record:	
Testing conclusion:	

### 3.5 Authentication Acceleration (EG Offload)

#### 3.5.1 Synchronize Voucher/Account to EG

Testing project:	Synchronize Voucher/Account to EG																														
Testing purpose:	Use Cloud Voucher Code to log in with Portal WiFi (SSID)																														
Testing procedure and expected results:	<p>1. EG is installed and online on the Ruijie Cloud, the Ruijie Cloud operates the voucher user (addition and deletion), which can be correctly synchronized to the EG.</p> <p>Create the package</p>  <p>Testing procedure and expected results:</p>  <table border="1"> <thead> <tr> <th>Package Name</th> <th>Description</th> <th>Price</th> <th>Max Concurrent Devices</th> <th>Bind MAC</th> <th>Period</th> <th>Data Quota</th> <th>Max Download Rate</th> <th>Max Upload Rate</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>test</td> <td>test</td> <td>10.00</td> <td>3</td> <td>Yes</td> <td>2 Hours</td> <td>500 MB</td> <td>1 Mbps</td> <td>512 Kbps</td> <td>✕ 📄</td> </tr> <tr> <td>Voucher</td> <td>-</td> <td>-</td> <td>3</td> <td>No</td> <td>1 Week</td> <td>100 MB</td> <td>Unlimited</td> <td>Unlimited</td> <td>✕ 📄</td> </tr> </tbody> </table> <p>Print voucher</p> 	Package Name	Description	Price	Max Concurrent Devices	Bind MAC	Period	Data Quota	Max Download Rate	Max Upload Rate	Action	test	test	10.00	3	Yes	2 Hours	500 MB	1 Mbps	512 Kbps	✕ 📄	Voucher	-	-	3	No	1 Week	100 MB	Unlimited	Unlimited	✕ 📄
Package Name	Description	Price	Max Concurrent Devices	Bind MAC	Period	Data Quota	Max Download Rate	Max Upload Rate	Action																						
test	test	10.00	3	Yes	2 Hours	500 MB	1 Mbps	512 Kbps	✕ 📄																						
Voucher	-	-	3	No	1 Week	100 MB	Unlimited	Unlimited	✕ 📄																						

Time Zone: (GMT+8:00)Asia/Hong\_Kong

Total Vouchers: 12 Activated Vouchers: 0 Depleted Vouchers: 2

Voucher Code	Name/Ref	Package Name	Price	Period	Created at	Expired at	Devices	Bind MAC	Data Usage	Max Download Rate	Max Upload Rate	Status
spewr5	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
jhrig	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
bdcto	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
yypp	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
enful	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
g2avt	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
phump	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
nmyqk	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
x7muc	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated
mflvk	-	test	10.00	2 Hours	2019-09-18 11:08:45	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 Kbps	Not Activated

### Enable the auth integration with Cloud

Note:

- Bridge mode is not supported.
- Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
- You can configure username and password on the User page.
- You can view AD domain user information on the User page.
- Users who fail single sign-on will be matched with the other policies.
- Please disable flow control if you want to configure rate limit on cloud accounts for Auth integration with Cloud. Otherwise, rate limiting may not function accurately.

Auth Integrator with Cloud

Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
No Record Found							

### Show the users synced from Cloud

User Structure

- root
  - cloud
- AD Domain User Structure
  - AD-Domain-Users

Name	IP/MAC Address	Behavior Policy Details	Action
gw5ta	Null		Edit Delete
sbkkg	Null		Edit Delete
jww3on	Null		Edit Delete
y3g75	Null		Edit Delete
84wgr	Null		Edit Delete
tzg7nq	Null		Edit Delete
n63ynl	Null		Edit Delete
y472f	Null		Edit Delete
Jn7w6	Null		Edit Delete
m7xae	Null		Edit Delete

2. Enable the local authentication on EG, The users can connect to external network by voucher authentication  
Add the authentication IP range

**Auth Policy**

Note: 1. Bridge mode is not supported.  
 2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.  
 3. You can configure username and password on the User page.  
 4. You can view AD domain user information on the User page.  
 5. Users who fail single sign-on will be matched with the other policies.  
 6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

Enable:

Policy Name: test

Policy Type:  Account  Single Sign-On  Voucher

IP Range: 192.168.30.2-192.168.30.253

Save

**Auth Policy**

Note: 1. Bridge mode is not supported.  
 2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.  
 3. You can configure username and password on the User page.  
 4. You can view AD domain user information on the User page.  
 5. Users who fail single sign-on will be matched with the other policies.  
 6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

Auth Integration with Cloud:

Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
test	192.168.30.2-192.168.30.253	Account Auth	Voucher	Enable	Active		Edit Delete

Show No: 10 Total Count: 1

Show the online info

**Online Info**

Note: If a mobile number is registered for SMS authentication, the mobile number will be displayed as the username.

Search by Username: gw5tox Search Force Offline

User Name	IP	Type	Uptime	Action
gw5tox	192.168.30.2	Account Auth	2019-2-27 14:15:19	Force Offline

Show No: 10 Total Count: 1

This voucher status is **Activated**

**Vouchers**

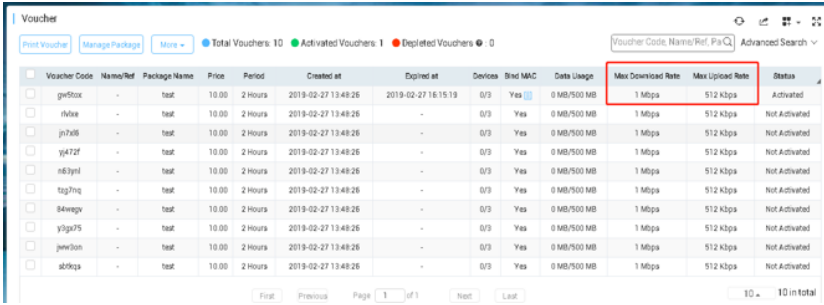
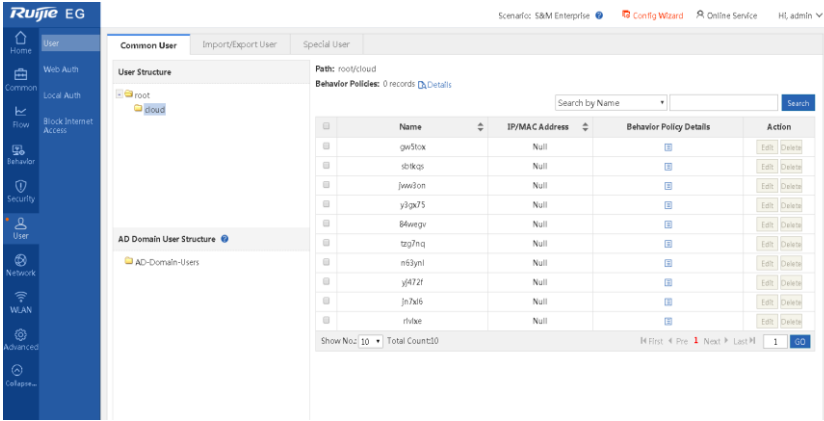
Total Vouchers: 10 Activated Vouchers: 1 Expired Vouchers: 0

Voucher Code	Name/Ref	Package Name	Price	Period	Created at	Expired at	Devices	Bind MAC	Data Usage	Max Download Rate	Max Upload Rate	Status
gw5tox	-	test	10.00	2 Hours	2019-02-27 13:48:26	2019-02-27 16:15:19	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Activated
rhvze	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
gn7x6	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
yp472f	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
n83ym	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
tdq7nq	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
8dwegv	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
y3gv75	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
pw63on	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated
abtkqa	-	test	10.00	2 Hours	2019-02-27 13:48:26	-	0/3	Yes	0 MB/500 MB	1 Mbps	512 kbps	Not Activated

Measured record:

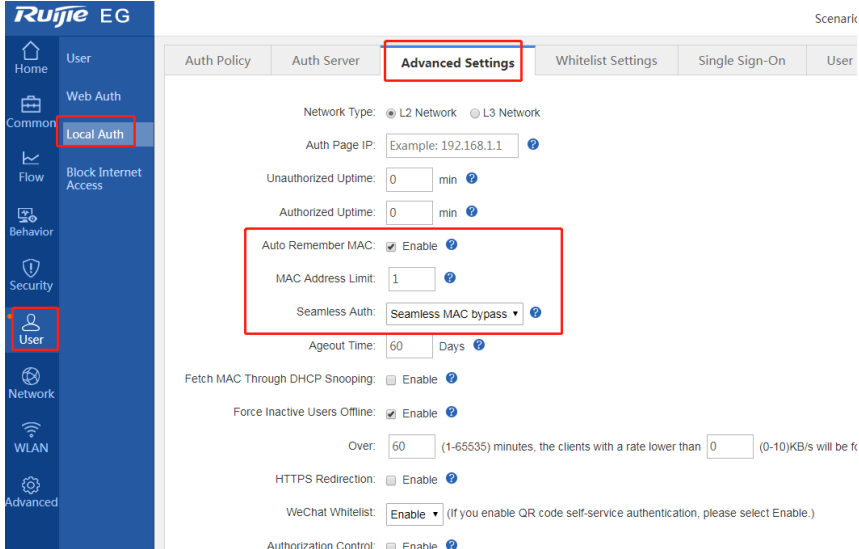
Testing conclusion:	
---------------------	--

### 3.5.2 Speed Limit

Testing project:	Voucher
Testing purpose:	Different Voucher Profile with different speed limit
Testing procedure and expected results:	<p>1. Configure the different voucher profile with different speedlimit on Ruijie Cloud. Configure the speed limit</p>  <p>2. Sync the voucher account to EG.</p>  <p>3. STA access with different voucher code and check the speed test result whether the same as Voucher profile configured.</p>
	Measured record:
Testing conclusion:	

### 3.5.3 Seamless Authentication

Testing project:	Seamless
------------------	----------

Testing purpose:	Enable and disable Seamless
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>EG is installed and online on the Ruijie Cloud, the Ruijie Cloud operates the Voucher user (addition and deletion), which can be correctly synchronized to the EG.</li> <li>Enable and disable seamless on EG. Close means disable seamless, seamless MAC bypass means enable seamless with MAC</li> </ol>  <ol style="list-style-type: none"> <li>Test the seamless with different STAs, record the result. First time STA login to online, then next time STA come back the network (or you can kick out the user on EG), he will be online automatically.</li> </ol>
Measured record:	
Testing conclusion:	

### 3.5.4 Compatibility test of EG local authentication

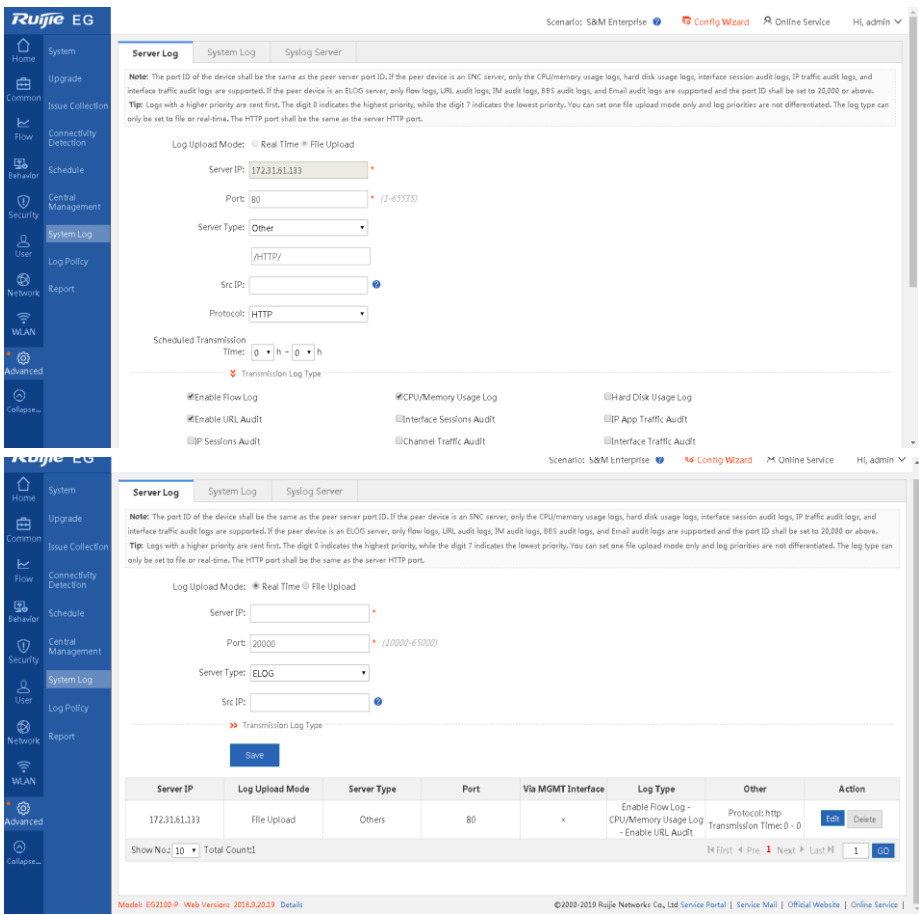
Testing project:	Compatibility
Testing purpose:	Compatibility with STAs
Testing procedure and expected results:	<ol style="list-style-type: none"> <li>Configure the captive portal template on Cloud and synchronize it to EG</li> <li>The user can select login options and customize the portal page</li> <li>Enable local auth on EG, including account, voucher and one-click authentication</li> <li>Use different STAs including laptop and mobile phone (iOS and Android), and make sure the portal page pops up automatically and is consistent with the template on Cloud</li> </ol>
Measured record:	

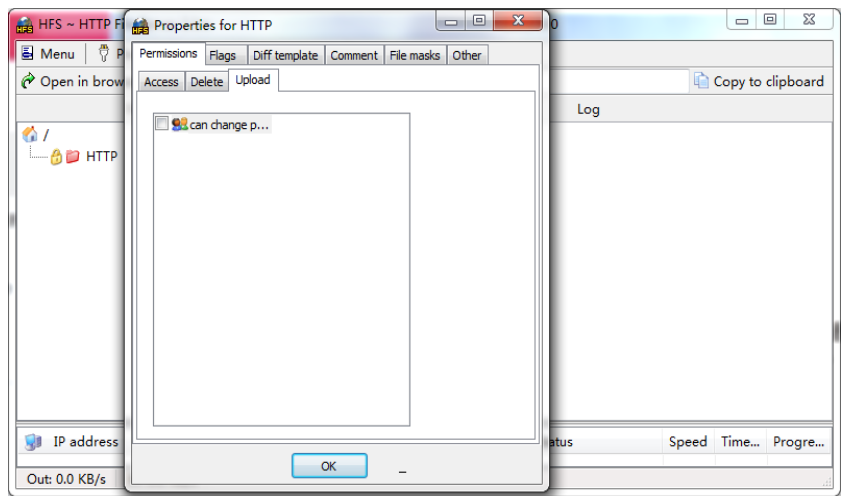
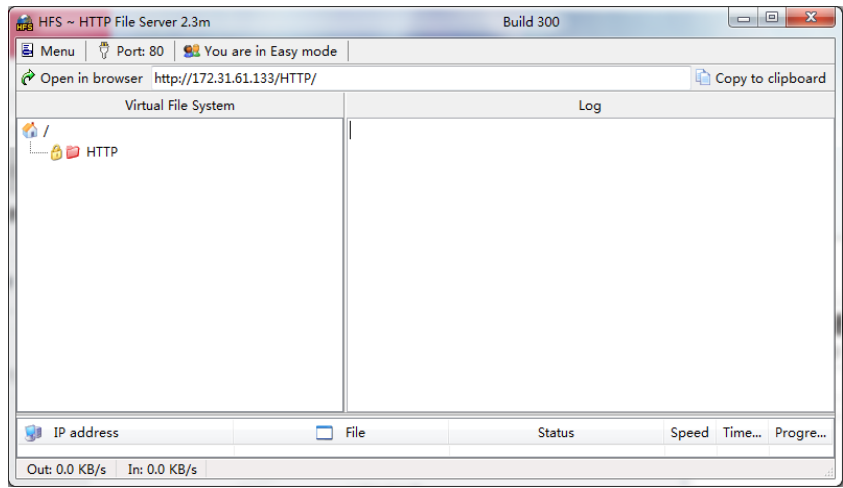
	Phone Model	OS and version	Browser	Result
	Iphone X	IOS 12.2	Safari	
	Samsung S10	Android 9.0	Chrome	
Measured record:				
Testing conclusion:				

## 3.6 User Access Log Audit

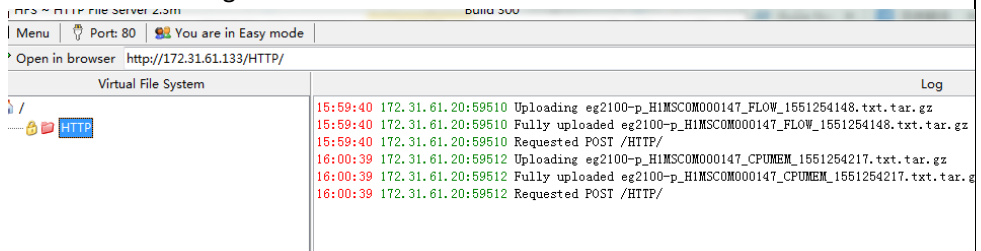
### 3.6.1 User access log checking

Testing project:	Log audit
Testing purpose:	User access log (such as visited URL, source/dest IP, etc.) should send out via HTTP to Log Server

Testing procedure and expected results:	1. Enable the log policy on EG and set the log level.															
	 <table border="1"> <thead> <tr> <th>Server IP</th> <th>Log Upload Mode</th> <th>Server Type</th> <th>Port</th> <th>Via MGMT Interface</th> <th>Log Type</th> <th>Other</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>172.31.61.133</td> <td>File Upload</td> <td>Others</td> <td>80</td> <td>x</td> <td>Enable Flow Log - CPU/Memory Usage Log - Enable URL Audit</td> <td>Protocol:http Transmission Time:0 - 0</td> <td>Edit Delete</td> </tr> </tbody> </table>	Server IP	Log Upload Mode	Server Type	Port	Via MGMT Interface	Log Type	Other	Action	172.31.61.133	File Upload	Others	80	x	Enable Flow Log - CPU/Memory Usage Log - Enable URL Audit	Protocol:http Transmission Time:0 - 0
Server IP	Log Upload Mode	Server Type	Port	Via MGMT Interface	Log Type	Other	Action									
172.31.61.133	File Upload	Others	80	x	Enable Flow Log - CPU/Memory Usage Log - Enable URL Audit	Protocol:http Transmission Time:0 - 0	Edit Delete									
	2. Configure the log server (HTTP).															



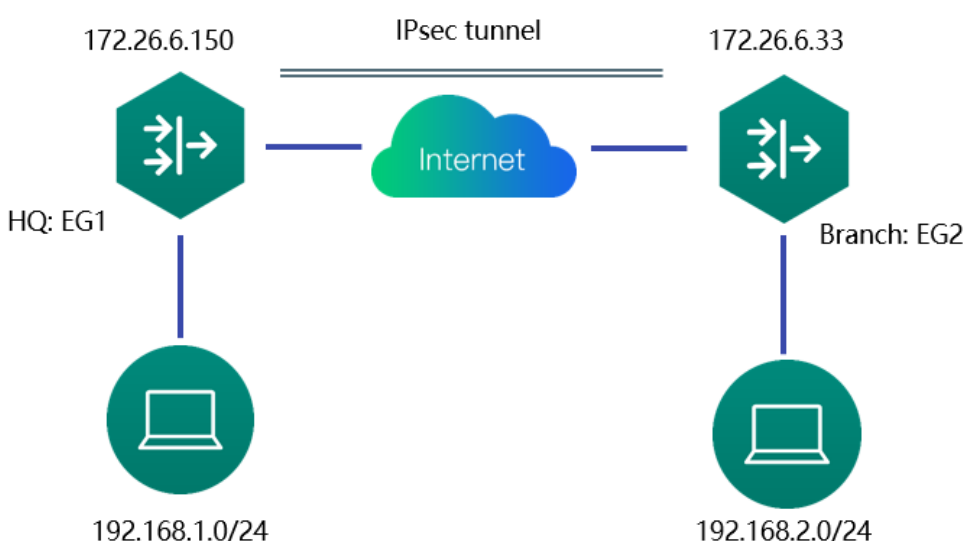
3. Monitor the log content on server.



Measured record:	
Testing conclusion :	

## 3.7 IPSEC VPN

### 3.7.1 Establish VPN

Testing project:	Establish VPN
Testing purpose:	The HQ and branch gateways use static IP addresses. The HQ gateway needs to verify the IP address of branch gateway.
Testing procedure and expected results:	<p>1. Check the network topology.</p>  <p>The diagram illustrates a network topology for an IPsec VPN. On the left, a green hexagonal gateway icon labeled 'HQ: EG1' with IP address '172.26.6.150' is connected to a green circular laptop icon representing the HQ network '192.168.1.0/24'. On the right, a similar green hexagonal gateway icon labeled 'Branch: EG2' with IP address '172.26.6.33' is connected to a green circular laptop icon representing the Branch network '192.168.2.0/24'. A blue cloud labeled 'Internet' is positioned between the two gateways. A double-line connection labeled 'IPsec tunnel' spans across the Internet cloud, connecting the two gateways.</p> <p>2. Configure the branch.</p> <ol style="list-style-type: none"><li>1) Complete wizard-based setup to meet basic Internet access requirements of users in the HQ and branch. If the users can access the Internet, check whether the next hop address is configured on the WAN interface.</li><li>2) Configure IPsec for the branch. Choose Network &gt; VPN and click Configure. Select Branch, and click Next.</li></ol>



☰ Welcome to VPN Config Wizard



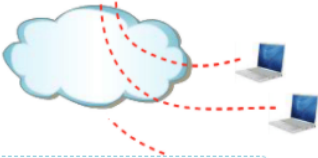
Select a Position:

**Headquarter**

Set the current device as Headquarter device and connect the terminal devices to it.

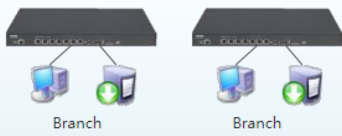


Internet



**Branch**

Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.



/ Network Position

2 Configure Branch

3 Connect to HQ

Back Next

☰ Welcome to VPN Config Wizard



Enter Basic Information.

VPN Type: IPsec

HQ Public IP/Domain Name: 172.26.6.150 \* +IP/URL ?

Pre-shared Key: \*\*\*\*\* \*

Interface: Gi0/0 ?

Network Config Wizard

Local Network		HQ Network		
192.168.2.0	255.255.255.0	192.168.1.0	255.255.255.0	+
				×

>> Advance Settings

/ Network Position

2 Configure Branch

3 Connect to HQ

Back Next

**Welcome to VPN Config Wizard**

Auth:  Enable ?

Negotiation Mode: Main Mode

IKE Policy: Encryption Algorithm: DES Hash Algorithm: SHA DH Group: group1 Lifetime: 86400 ?

Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding)

Secrecy: Disable

IPSec Lifetime: 3600 second(s) ?

DPD Type: on-demand DPD Interval: 30 second(s) ?

Back Next

Network Position

**2 Configure Branch**

3 Connect to HQ

3. Configure the HQ.

- 1) Complete wizard-based setup to implement basic Internet access service of the HQ router.
- 2) Configure IPsec for router A in the HQ.

Choose Network > VPN and click Configure. Select Headquarter, and click Next.

**Welcome to VPN Config Wizard**

Select a Position:

**Headquarter**  
Set the current device as Headquarter device and connect the terminal devices to it.

**Branch**  
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

Internet

Branch

Branch

Back Next

Network Position

Branch Type


VPN Type


Finish

Select Branch, and click Next.

☰ Welcome to VPN Config Wizard

Select a Branch Type:

Mobile User 

Branch 

Network Position

2 Branch Type

3 VPN Type


4 Finish

Back Next

Select IPsec, and click Next.

☰ Welcome to VPN Config Wizard

Recommended VPN Types:  
*You can change the VPN type.*

Branch   L2TP  IPsec  L2TP IPsec

**i** PPTP/L2TP: Support access authentication without data encryption.  
IPsec: Support data encryption.  
L2TP IPsec: Support access authentication and data encryption.

Network Position

2 Branch Type

3 VPN Type

4 Configure IPsec

5 Finish

Back Next

☰ Welcome to VPN Config Wizard

Configure IPSec Parameter

Pre-shared Key:  \* ?

Local ID ? :  Enable

Network Config Wizard

Local Network		The branch network		Outbound Interface	
<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.2.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="Gi0/0"/>	<input type="button" value="+"/>
					<input type="button" value="X"/>

>> Advance Settings

/ Network Position

2 Branch Type

3 VPN Type

4 Configure IPSec

5 Finish

Back

Next

☰ Welcome to VPN Config Wizard

> Advance Settings

IKE Policy: Encryption Algorithm Hash Algorithm DH Group Lifetime  
    ?

Transform Set 1:

Transform Set 2:  ?

PFS(Perfect

Forwarding

Secrecy:

IPSec Lifetime:  second(s) ?

DPD Type:  DPD Interval:  second(s) ?

/ Network Position

2 Branch Type

3 VPN Type

4 Configure IPSec

5 Finish

Back

Next

☰ Welcome to VPN Config Wizard

The VPN is created.

**Then:**

View branch configuration. [View](#)

1 Network Position  
2 Branch Type  
3 VPN Type  
4 Configure IPSec  
5 **Finish**

Back Finish

#### 4. Verification

- 1) Choose Network > VPN, and click the Topo tab to view the configuration.

VPN

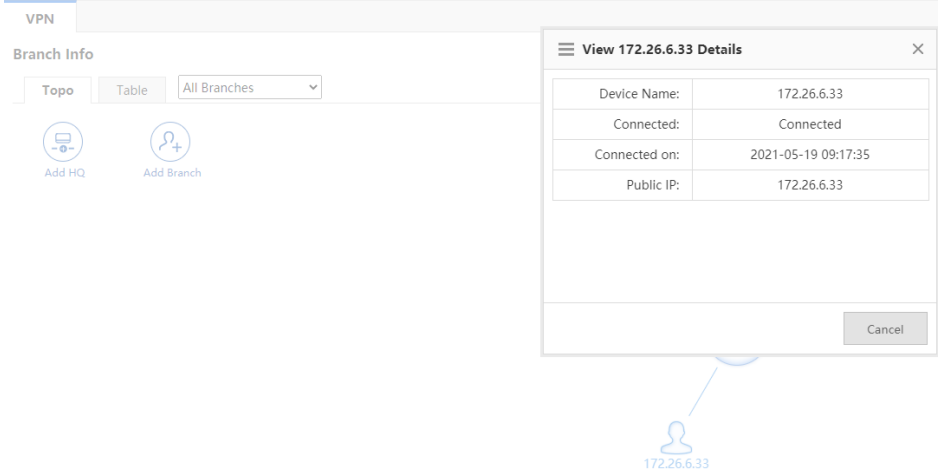
Branch Info

Topo Table All Branches

Add HQ Add Branch

Ruijie (local device)  
IP: 172.26.6.150

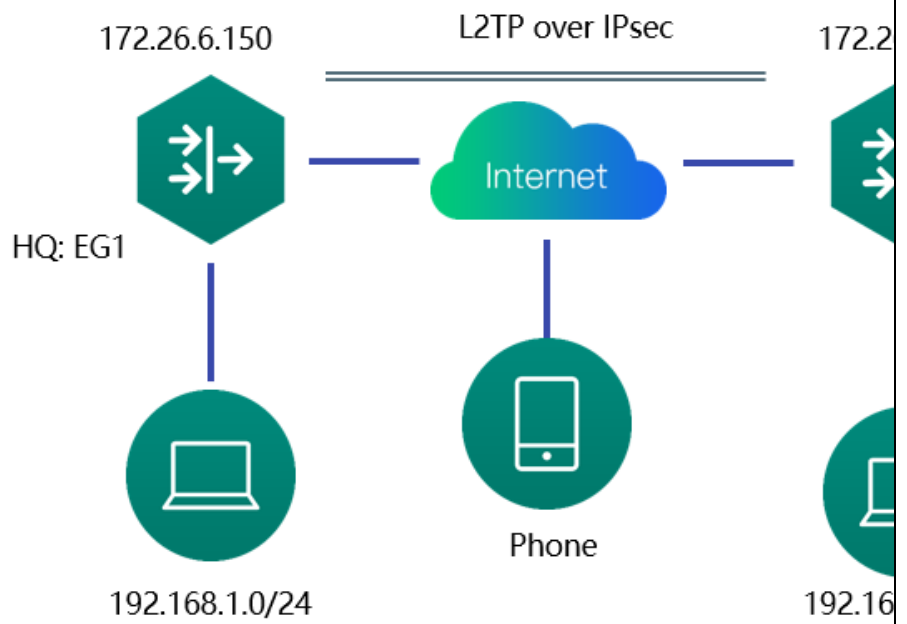
172.26.6.33

	
Measured record:	
Testing conclusion :	

### 3.8 L2TP over IPsec VPN

#### 3.8.1 Establish VPN

Testing project:	Establish VPN
Testing purpose:	Branch and clients create the L2TP over IPsec VPN with HQ.
Testing procedure and expected results:	1. Check the network topology.



2. Configure the branch.

1) Complete wizard-based setup to meet basic Internet access requirements of users in the HQ and branch. If the users can access the Internet, check whether the next hop address is configured for the WAN interface.

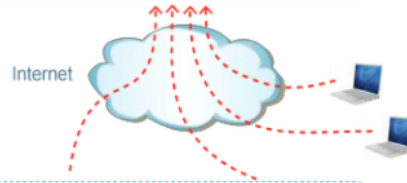
2) Configure IPsec for the branch.

Choose Network > VPN and click Configure. Select Branch, and click Next.

☰ Welcome to VPN Config Wizard

Select a Position:

**Headquarter**  
Set the current device as Headquarter device and connect the terminal devices to it.



**Branch**  
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.



☰ Welcome to VPN Config Wizard

Enter Basic Information.

VPN Type:  ▾

HQ Public IP/Domain Name:  \* +IP/URL ?

Pre-shared Key:  \*

User Name:  \*

Password:  \*

HQ Network:  -  +

» Advance Settings



☰ Welcome to VPN Config Wizard

Auth:  Enable ?

IKE Policy: Encryption Algorithm Hash Algorithm DH Group Lifetime  
DES SHA group1 86400 ?

Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding

Secrecy: Disable


IPSec Lifetime: 3600 second(s) ?

DPD Type: on-demand DPD Interval: 30 second(s) ?

Keepalive Interval: 60 second(s)

Allow HQ to Access

☰ Welcome to VPN Config Wizard

 Connecting...

☰ Welcome to VPN Config Wizard

Connect operation succeeded. You can now access the headquarter network.

3) Configure the HQ.

Complete wizard-based setup to implement basic Internet access service of the HQ router.

Configure L2TP IPsec for router A in the HQ.

Choose Network > VPN and click Configure. Select Headquarter, and click Next.

☰ Welcome to VPN Config Wizard

Select a Position:



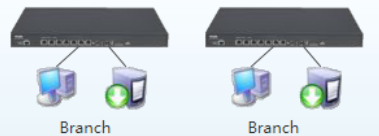
Headquarter

Set the current device as Headquarter device and connect the terminal devices to it.



Branch


Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.




Select Mobile User, and click Next.

☰ Welcome to VPN Config Wizard

Select a Branch Type:

Mobile User 

Branch 

Select L2TP IPsec, and click Next.

☰ Welcome to VPN Config Wizard

Recommended VPN Types:

*You can change the VPN type.*

Mobile User 

PPTP

L2TP IPsec



PPTP/L2TP: Support access authentication without data encryption.

IPsec: Support data encryption.

L2TP IPsec: Support access authentication and data encryption.

Enter the basic information, client IP range and DNS

☰ Welcome to VPN Config Wizard

**Enter Basic Information**

Client IP Range:  ~  \*

*Please make sure that the IP addresses are not in use in the LAN.*

HQ Domain Name:

Primary DNS Server:

Secondary DNS Server:

*If a mobile user wants to access the LAN through the domain name, a DNS server address should be configured which is usually the same with the address of the LAN DNS server.*

» Advance Settings

**Enable the branch and add the branch network**

☰ Welcome to VPN Config Wizard

*LAN DNS server.*

» Advance Settings

Local Tunnel IP:  \*

Local Tunnel Mask:  \*

L2TP Keepalive

Interval:  second(s).

L2TP Verification Code:  Enable

Allow HQ to Access

Branch:  Enable ?

Branch Tunnel IP	The branch network		
<input type="text" value="100.1.1.2"/>	<input type="text" value="192.168.3.0"/>	<input type="text" value="255.255.255.0"/>	+ ×

**Add the account**

☰ Welcome to VPN Config Wizard

Save Account on

Local Device  Other System ?

**Add Branch** User Name:  Password:

Type:	User Name	Action
	test	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.:  Total Count: 1   1

☰ Welcome to VPN Config Wizard

Pre-shared Key:  \* ?

Local ID ? :  Enable

⌵ Advance Settings

Interface:  Gi0/0 ?

IKE Policy: Encryption Algorithm  Hash Algorithm  DH Group  Lifetime  ?

Transform Set 1:

Transform Set 2:  ?

PFS(Perfect

Forwarding

Secrecy:

☰ Welcome to VPN Config Wizard

The VPN is created.

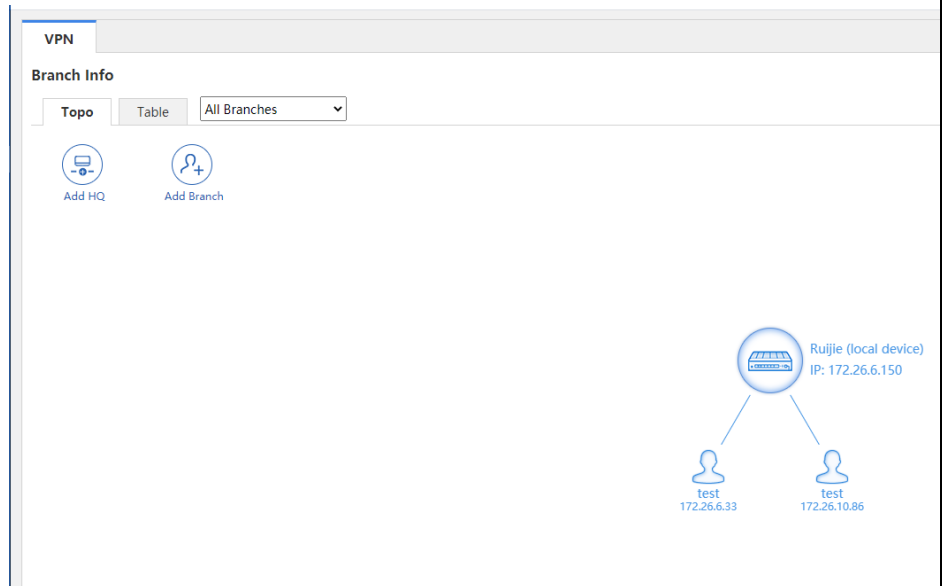
Then:

View branch configuration. [View](#)

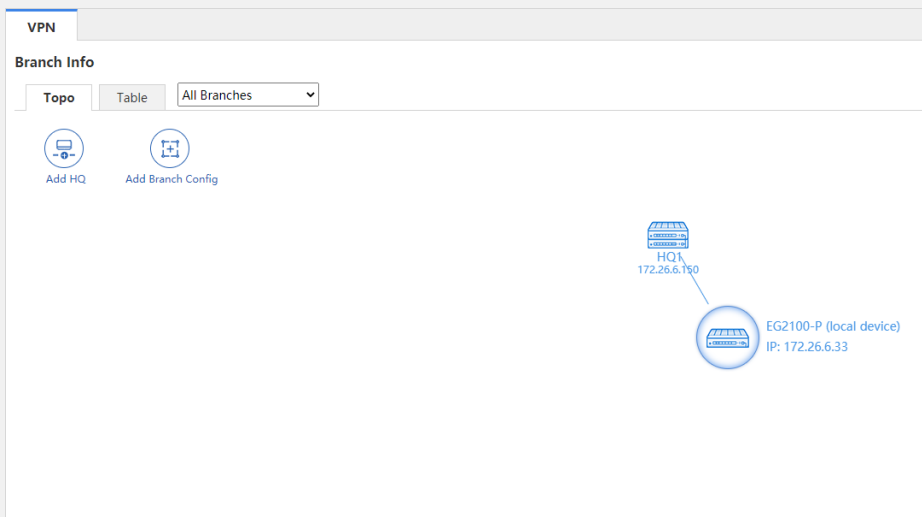
#### 4) Verification

Choose Network > VPN, and click the Topo tab to view the configuration.

HQ review

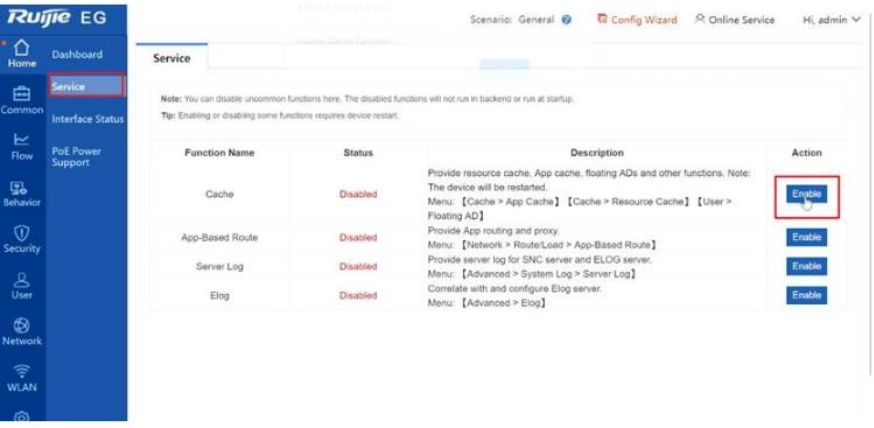


Branch review

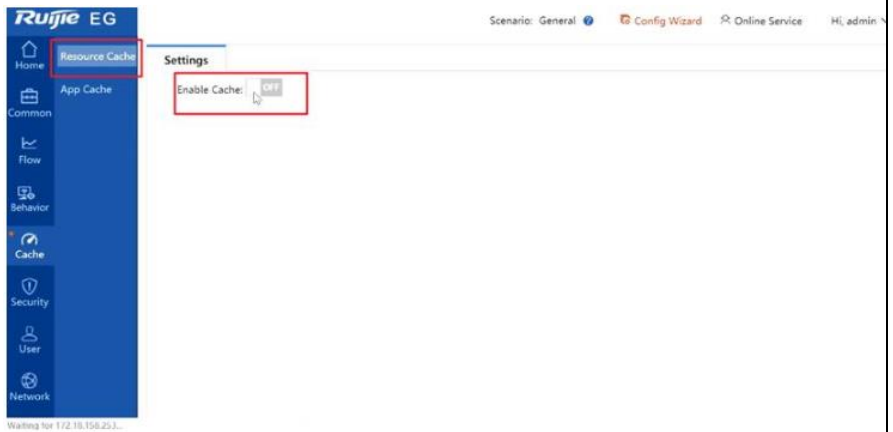
	
Measured record:	
Testing conclusion:	

### 3.9 Resource Cache

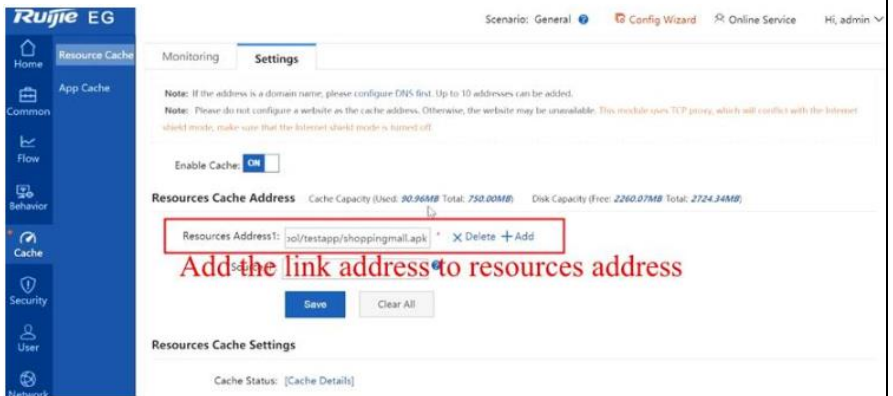
#### 3.9.1 Mobile App Caching

Testing project:	Mobile App Caching
Testing purpose:	<p>Resource cache refers to synchronizing resource from the specified server to a device. Afterwards, users can get the resource directly from the device without crossing WAN.</p> <p>Resource cache can reduce bandwidth usage and save users from waiting for access.</p>
Testing procedure and results:	<p>1. Enable the cache function, the device will be restarted:</p> 

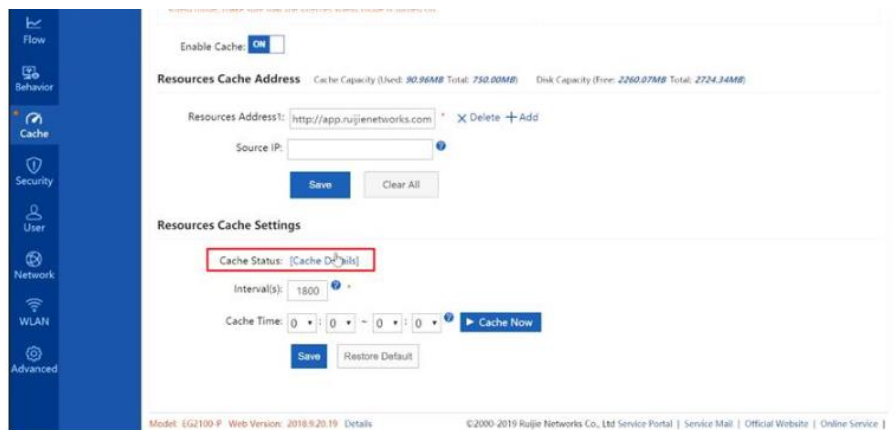
2. Enable resource cache:



3. Paste the download link of the resource to the "Resources Address1":



4. Check the cache file:



Resource Name	Resource Size	Cache Time:
app.rujietworks.com/	error	2019-05-31 11:14:43
app.rujietworks.com:50090/tool/testapp/shoppingmall.apk	90.96MB	2019-05-31 11:14:15

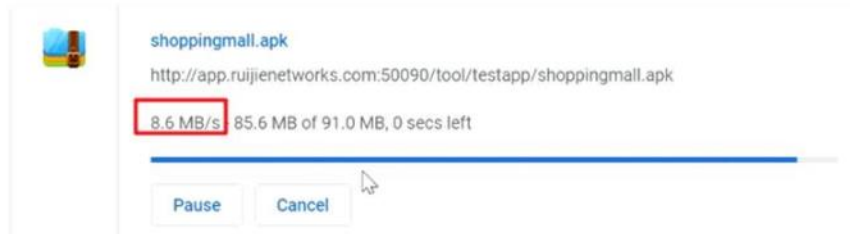
Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO



5. Verification

1) Download the file via browser:

Today



2) The file is downloaded within the LAN.



Measured record:

Testing conclusion: