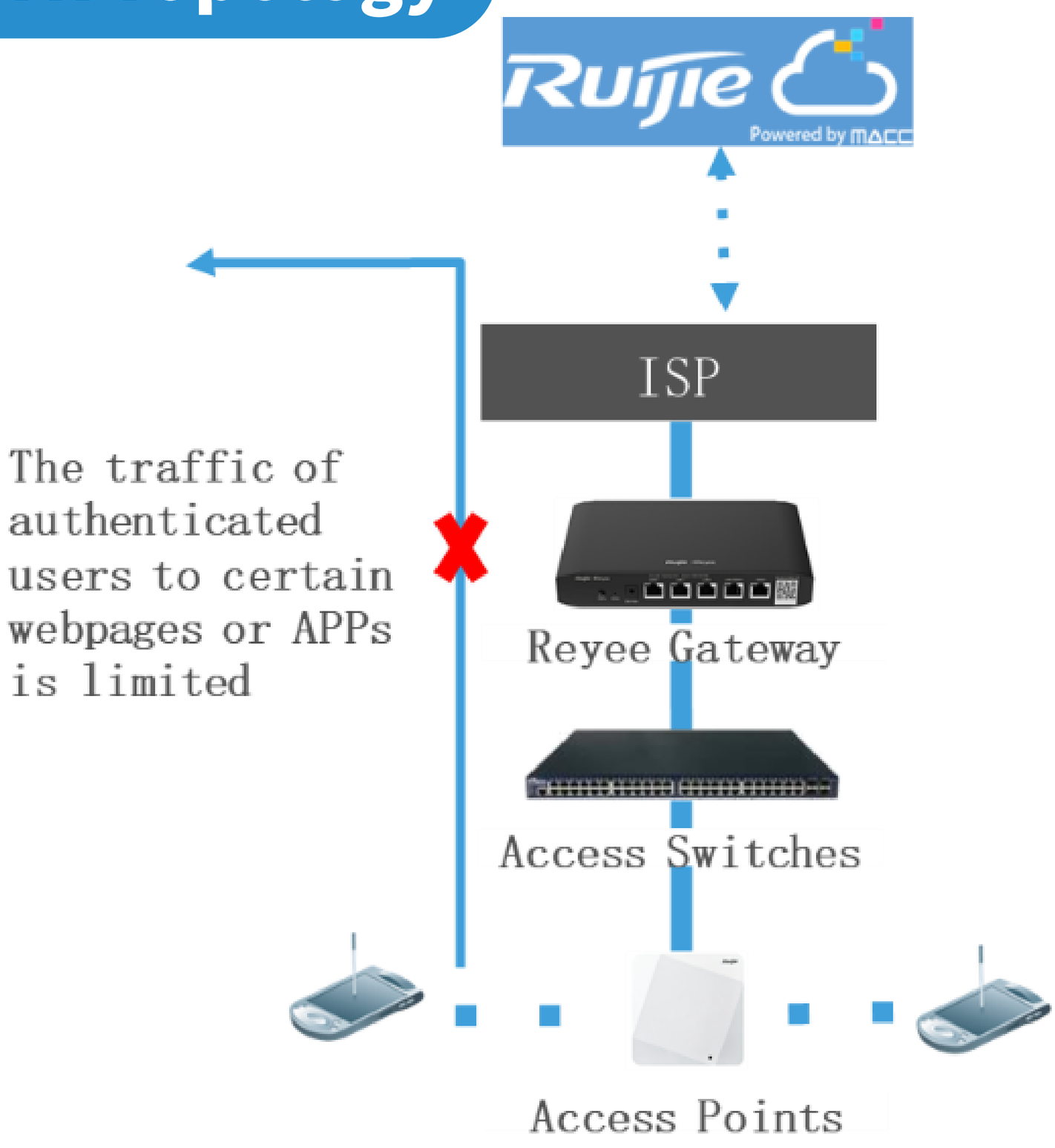
How to manage the access behavior of the authenticated users on Reyee EG?

I. Applicable Scenario

The solution introduced here can be applied to the scenario that you want to prohibit some authenticated visitors or users from accessing some websites or APPs. This article describes how to simply add some control policies on Reyee EG to manage the access behavior of Ruijie cloud authenticated users.

II. Network Topology



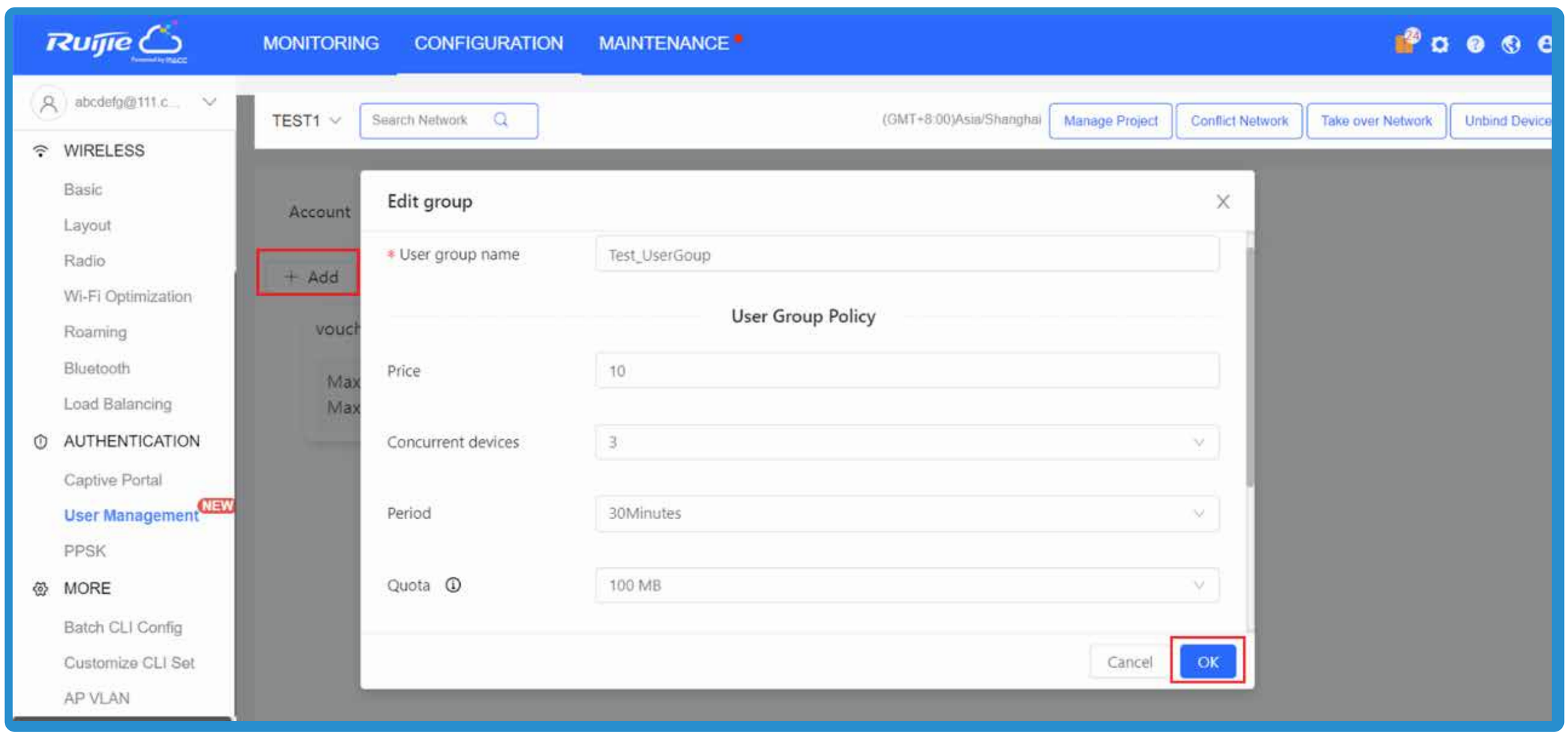
III. Configuration Notes

1. Customize the user groups on Cloud and print accounts or voucher codes that are used for authentication.
2. Create the portal template and synchronize it to the EG local eWeb on Cloud.
3. Configure the access control policies after clients finished the authentication.

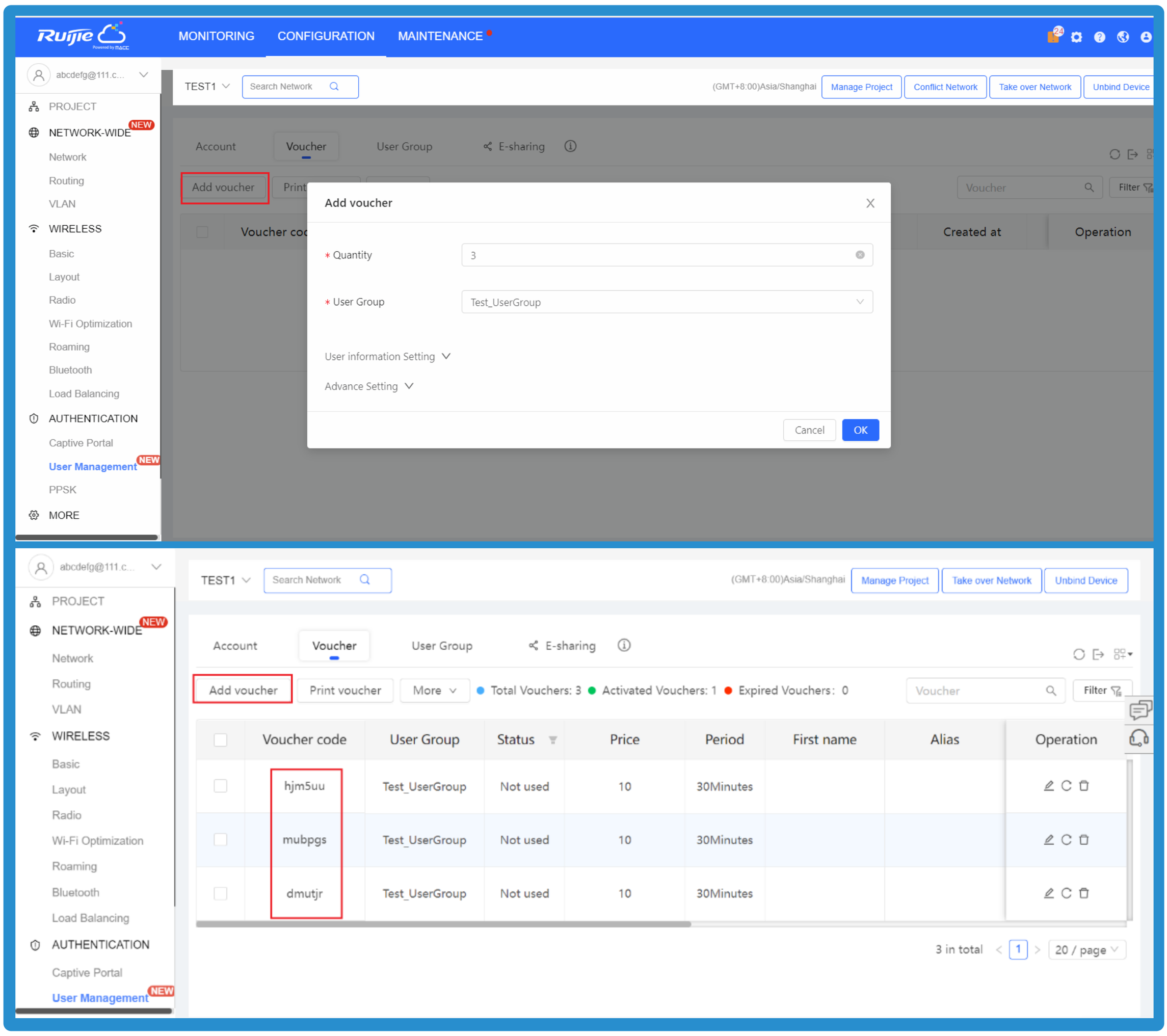
IV. Configuration Steps

1 Create a user group and add voucher codes.

As shown in the below picture, select the project and create a new user group and customize the Price, Concurrent devices, and Period, etc.



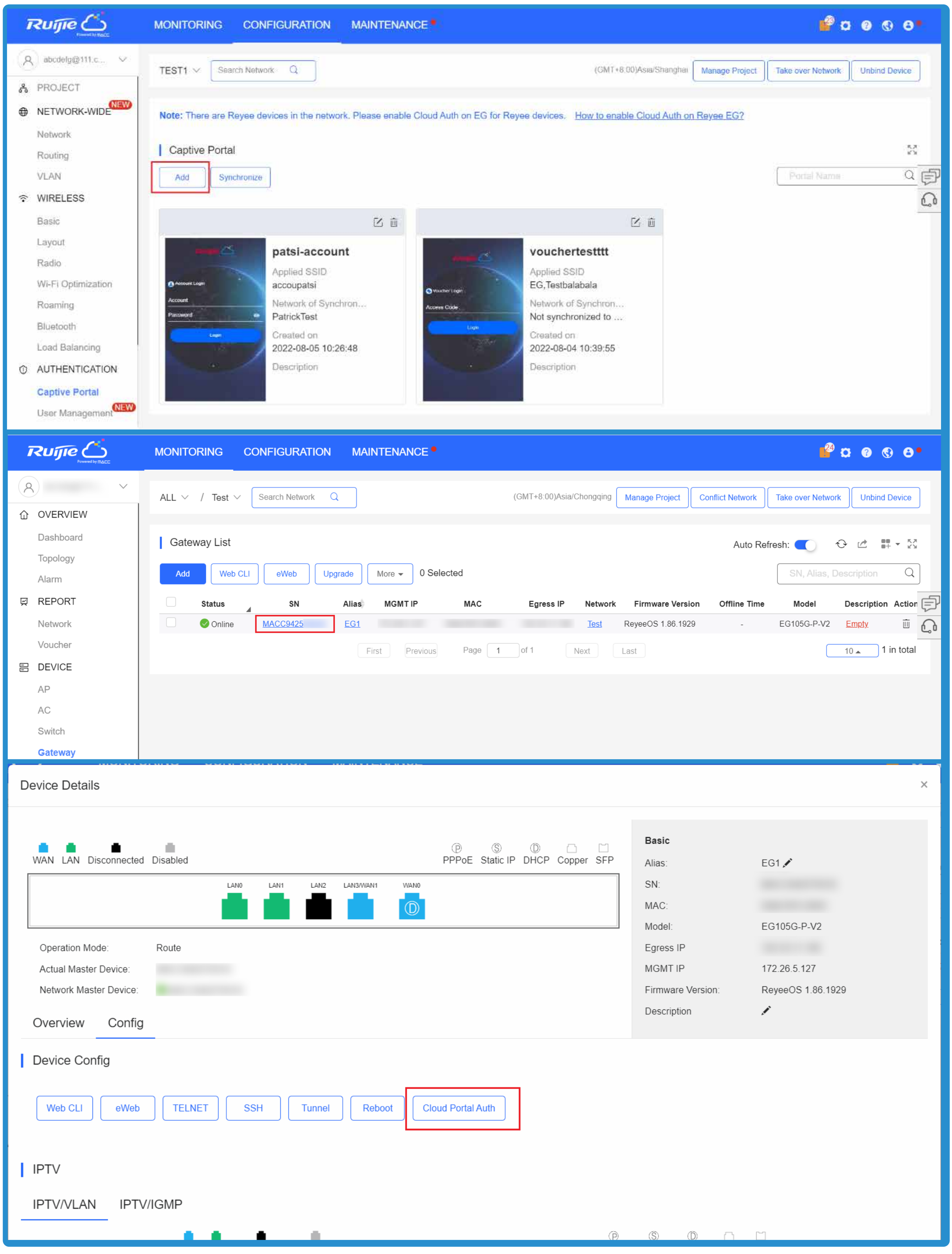
Then, add voucher codes or accounts for clients who need to be authenticated. For example, three new voucher codes have been created here.



IV. Configuration Steps

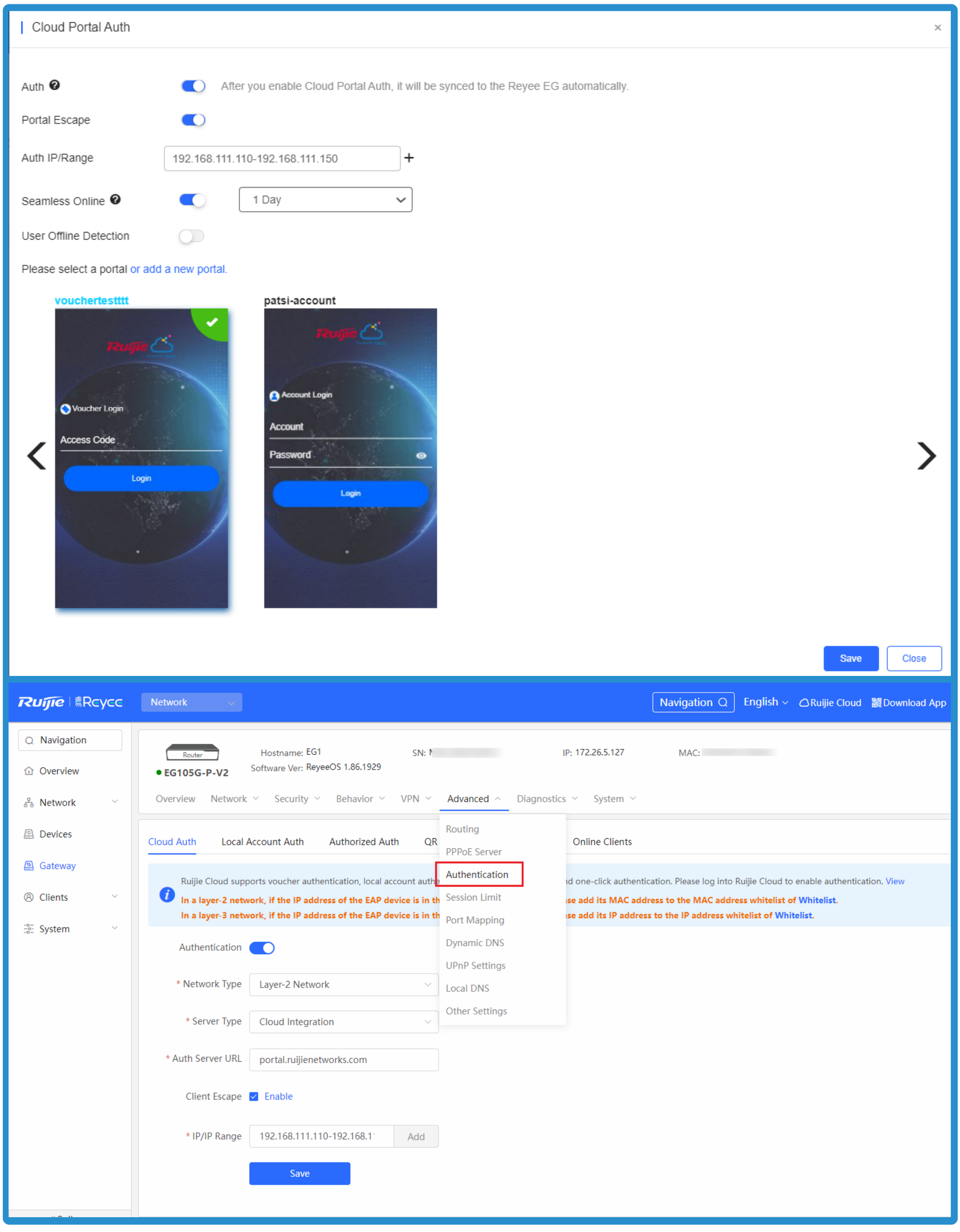
② Synchronize the captive portal from Cloud to EG local EWEB.

As shown in the blow pictures, add a new captive portal firstly on the Cloud, then synchronize that to the EG local eWeb in the ‘Cloud Portal Auth’ page.



In this page, you may customize the IP range for the authenticated users and enable the ‘Seamless Online’, ‘Portal Escape’ and ‘User Offline Detection’ feature here. After click ‘Save’ button, the selected captive portal template will be synchronize to the local EG eWeb. You can enter the ‘Authentication’ menu and confirm whether the portal was synchronized correctly.

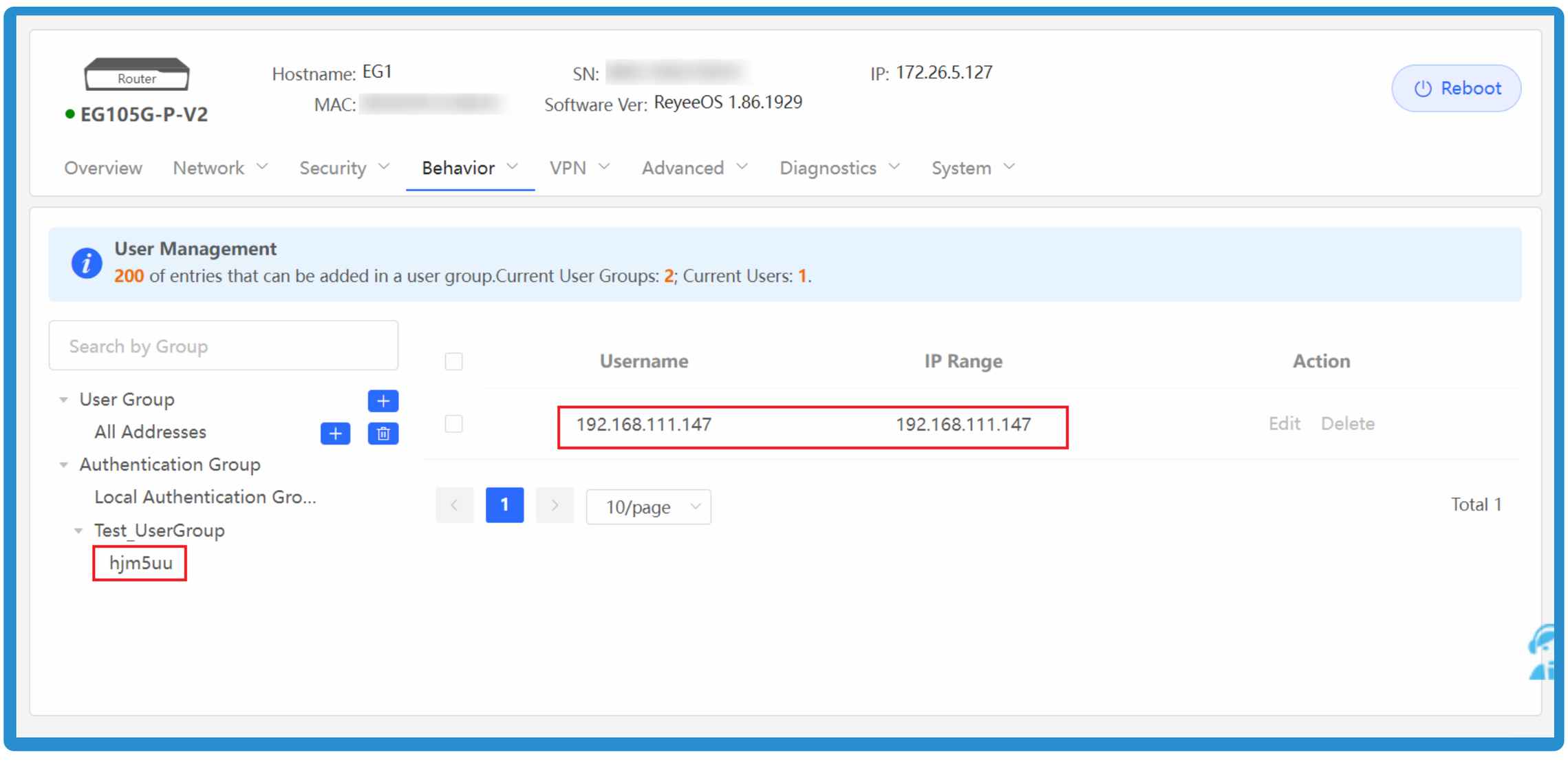
IV. Configuration Steps



3 Reyee EG identifies the client account after completing the authentication.

As shown in the below pictures, when clients connect to the SSID and get an address in the authenticated IP range, they need to input the voucher code that was created on Cloud before finishing the authentication. On the User Management page of EG eWeb, the account used by the authenticated user will be displayed in the authentication group.

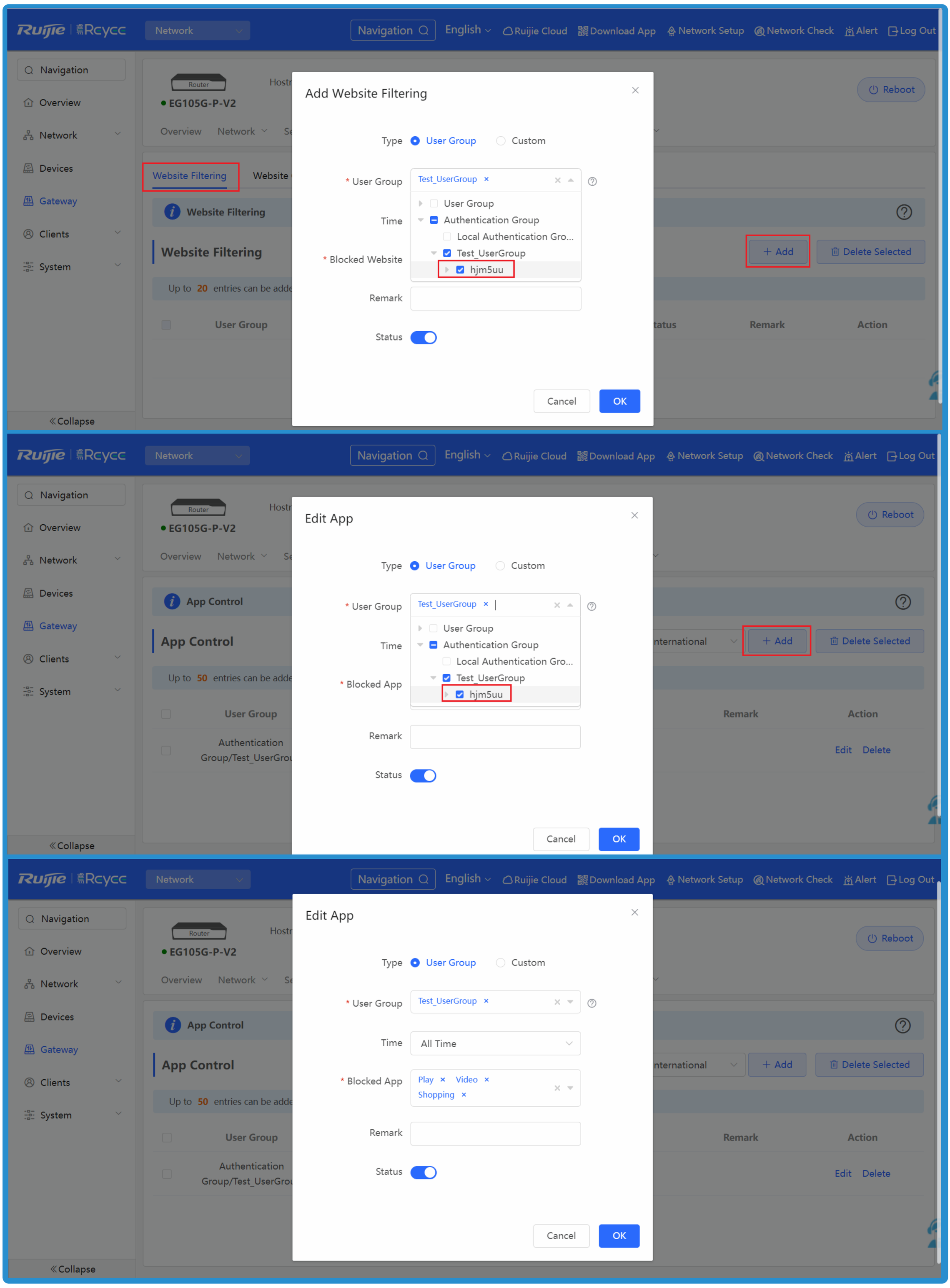
IV. Configuration Steps



4 Create control policies for the authenticated users.

As shown in the below pictures, taking blocking customers from accessing websites and APPs as an example, you can enter the ‘Website Management’ and ‘App Control’ page of EG, and chose the blocked websites and blocked APPs for the authenticated users. In this test, Play, Video, and Shopping were selected as the blocked group.

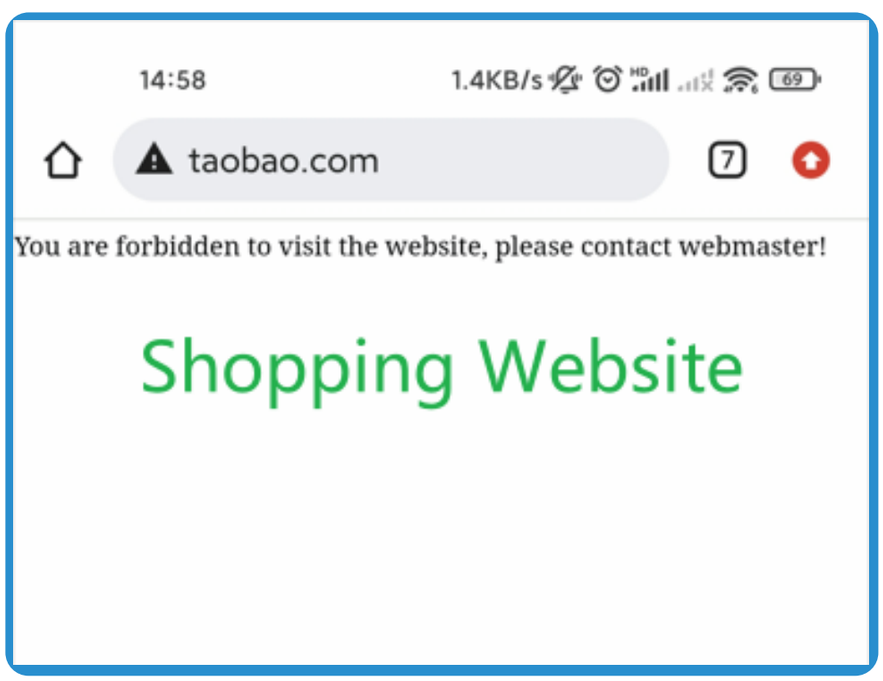
IV. Configuration Steps



V. Verification

As shown in the below pictures, the authenticated users won’t able to access the blocked websites and APPs after the control policies taking effect.

V. Verification



Official Website ⋙ https://www.ruijienetworks.com

Community ⋙ https://community.ruijienetworks.com

Facebook ⋙ Ruijie Tech Support

YouTube ⋙ Ruijie Networks

Official Website

Community

Facebook

YouTube Training