Technical Guide

Cross Gateway Roaming

Released: 2018-05-15
Doc Rev. No: R1

Table of Contents

1 Introduction

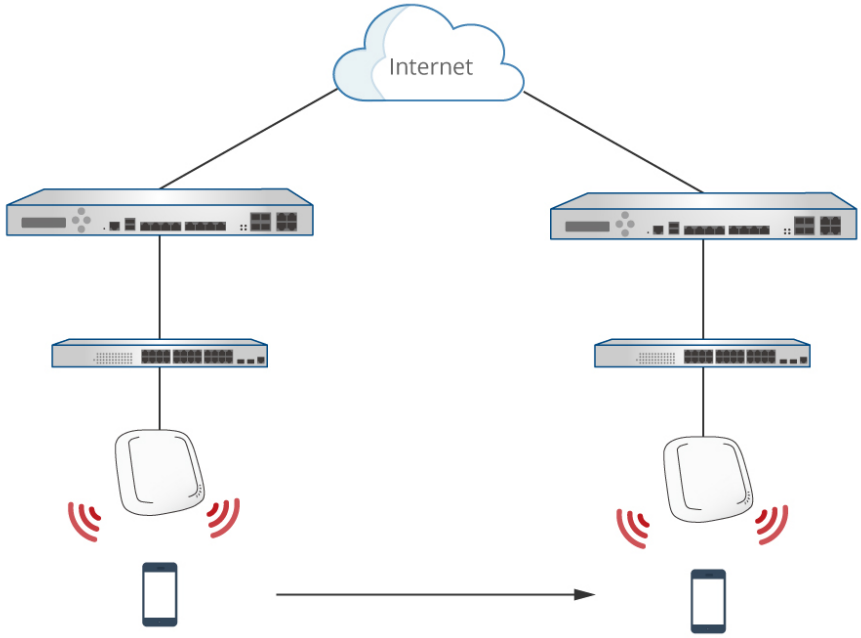
Cross Gateway Roaming is a powerful feature on the Controller that allows an authenticated end user to roam seamlessly within a large network deployment where multiple WLAN controllers are in service at different locations. Note that “authenticated end user” here refers to an end user that has been authenticated by any of the internal/external authentication options on the Controller.

Normally, when a user moves from an edge AP managed by one Controller to another edge AP managed by another Controller, the user would experience network disconnection and have to re-login. However, with Cross Gateway Roaming, the user can stay logged in to the network and continue to enjoy network access without interruption.

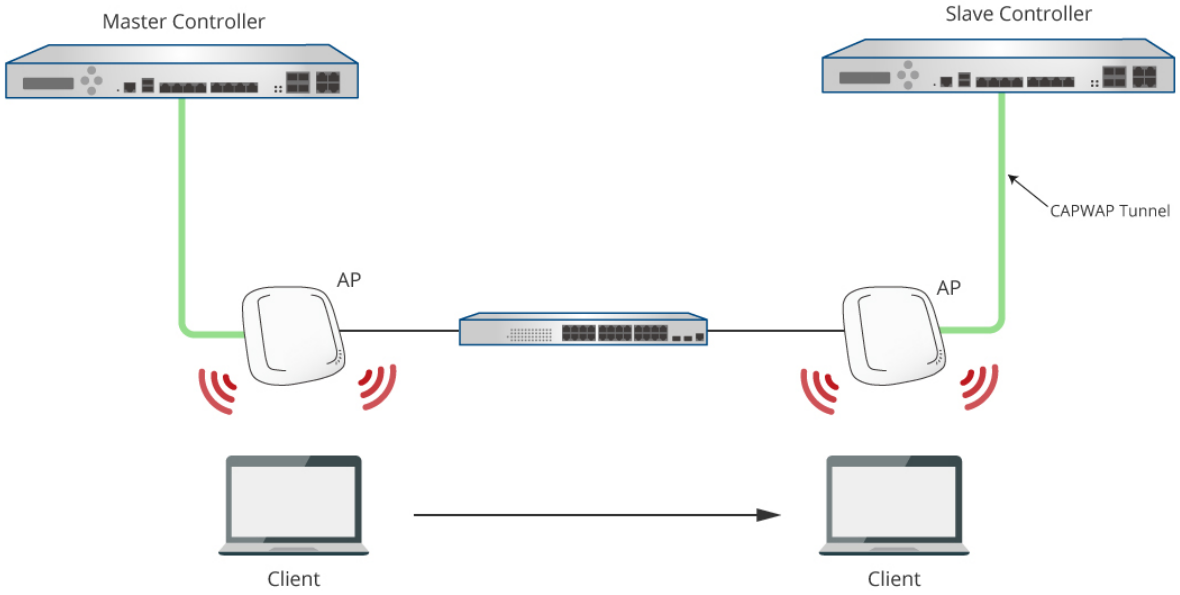
Cross Gateway Roaming adopts a star topology that consists of one Master Node that sits at the center and multiple Slave Nodes that connect to it. One Master Node may connect with up to 15 Slave Nodes. A Controller can be in Master Mode or Slave Mode depending on its Cross Gateway Roaming settings.

This technical guide aims to explain the setup flow of Cross Gateway Roaming on the Controller. Below are two exemplary network deployments that deploy Cross Gateway Roaming so that authenticated users could seamlessly roam within the larger network. For these network deployments, the Master and Slave Controllers could be operating at two adjacent buildings of a company or a hotel, for example, and authenticated users going from one building to the other could stay connected to the Internet. For Network Topology - 2, the Master and Slave Controllers are each managing an Access Point for providing Wi-Fi networks, and CAPWAP tunnels have been built between the Controllers and the Access Points. Note that the SSID on both Access Points have to be the same for Cross Gateway Roaming.

[Network Topology - 1]



[Network Topology - 2]

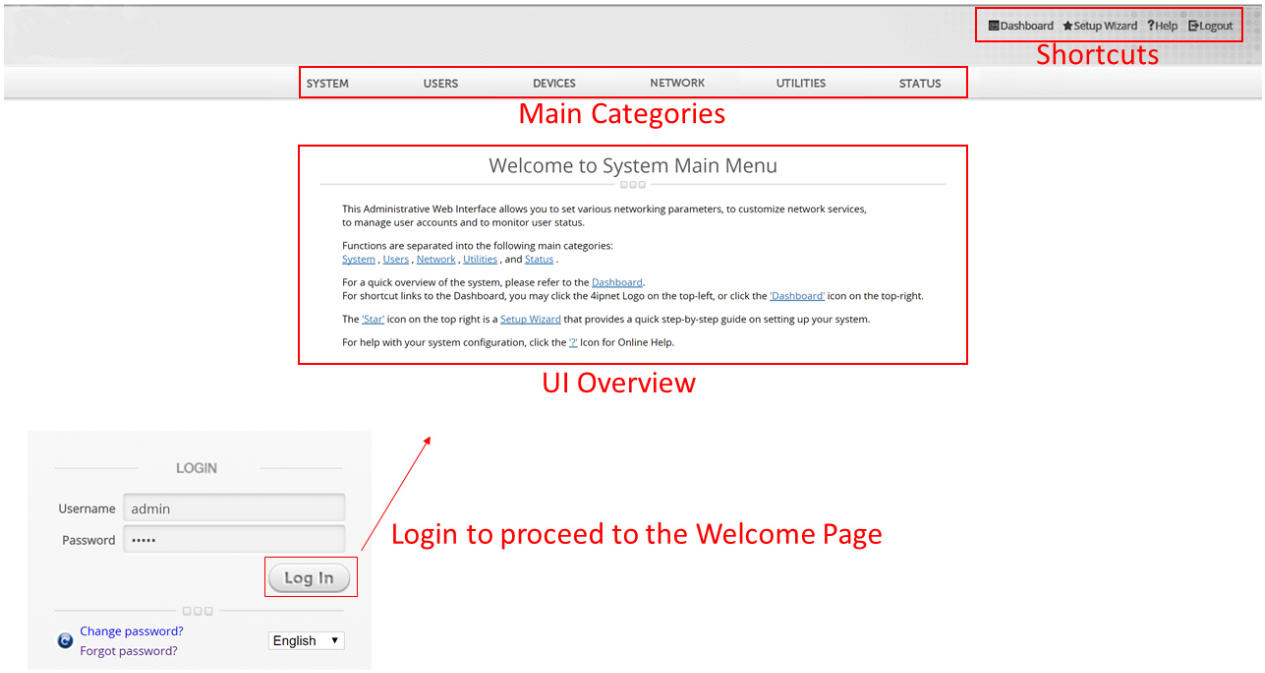


2 Master Controller Configuration

2.1 System – Initial Login

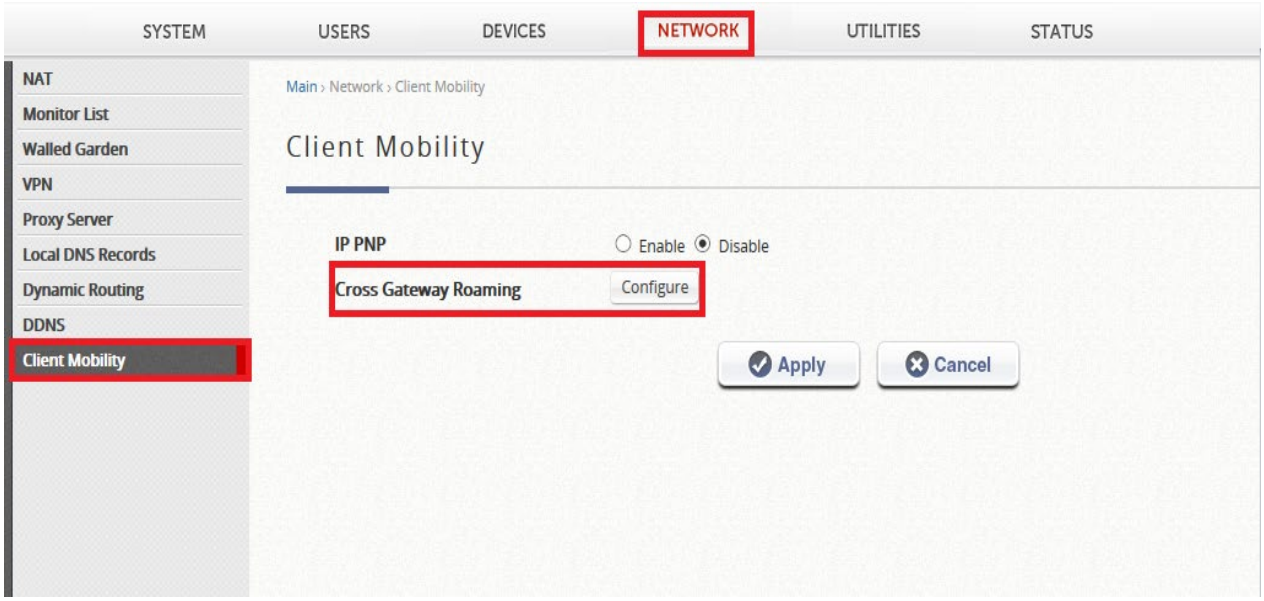
a. Access the Controller's Web Management Interface (WMI) by going to 192.168.1.254 in a web browser. Login to the Controller using the default credentials: admin/admin

Note: Upon first-time login, the admin user will be asked to change the password.

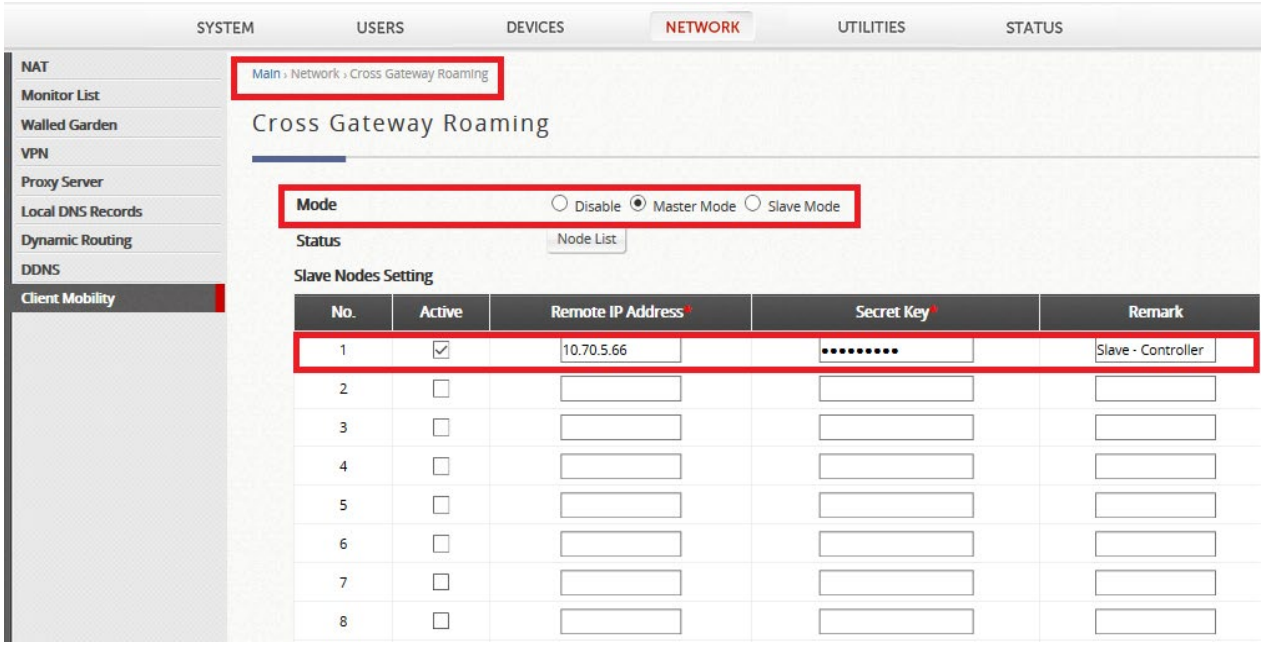


2.2 Enabling Cross Gateway Roaming

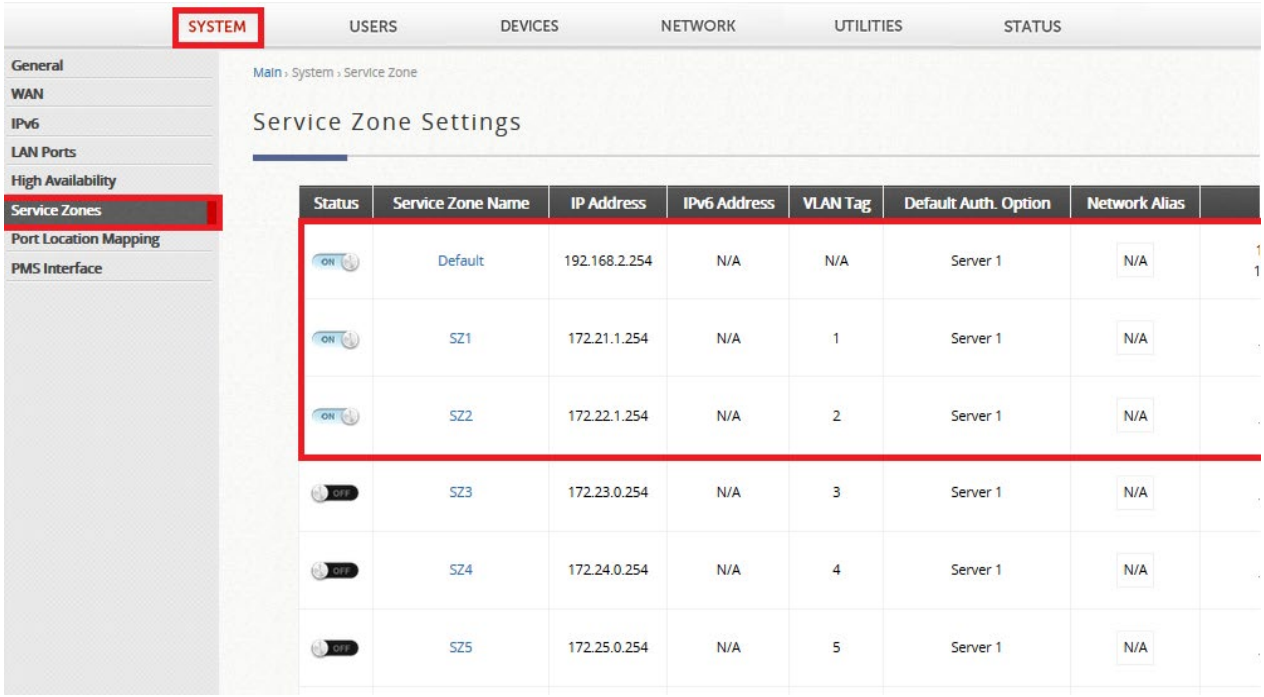
a. Go to *Network > Client Mobility > Cross Gateway Roaming*



b. Set this Controller to be in "Master Mode" and inform the Controller where the Slave Controller by providing the IP address of the Slave Controller. Also set up a security key for communication between the two Controllers.

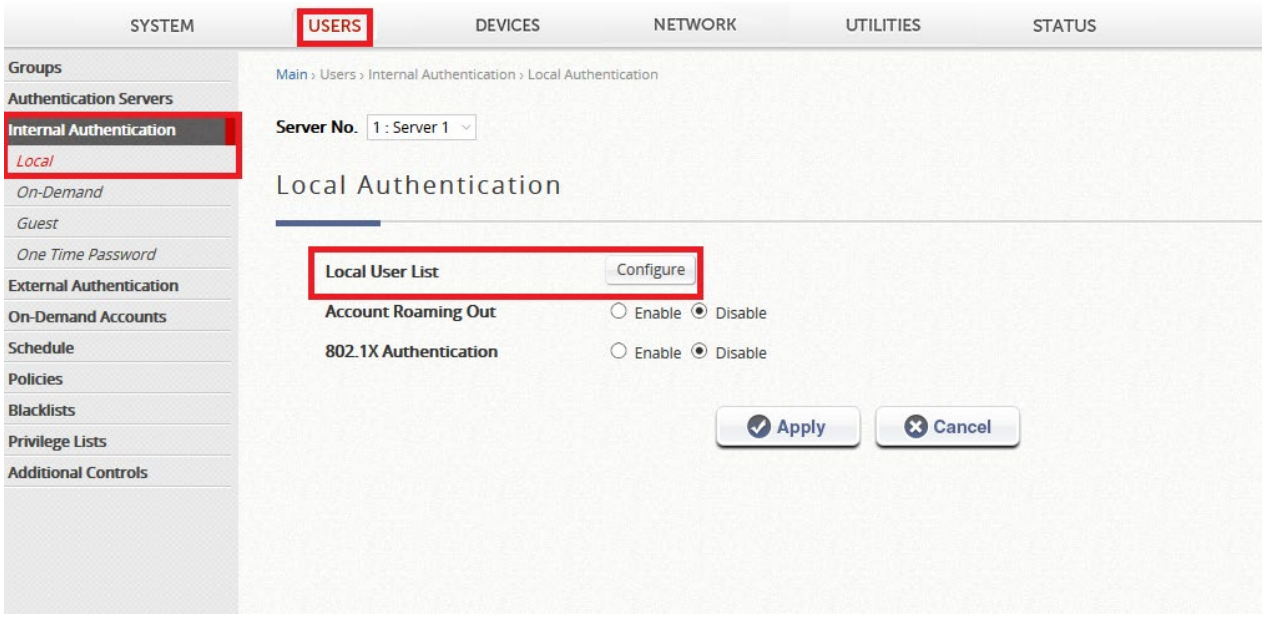


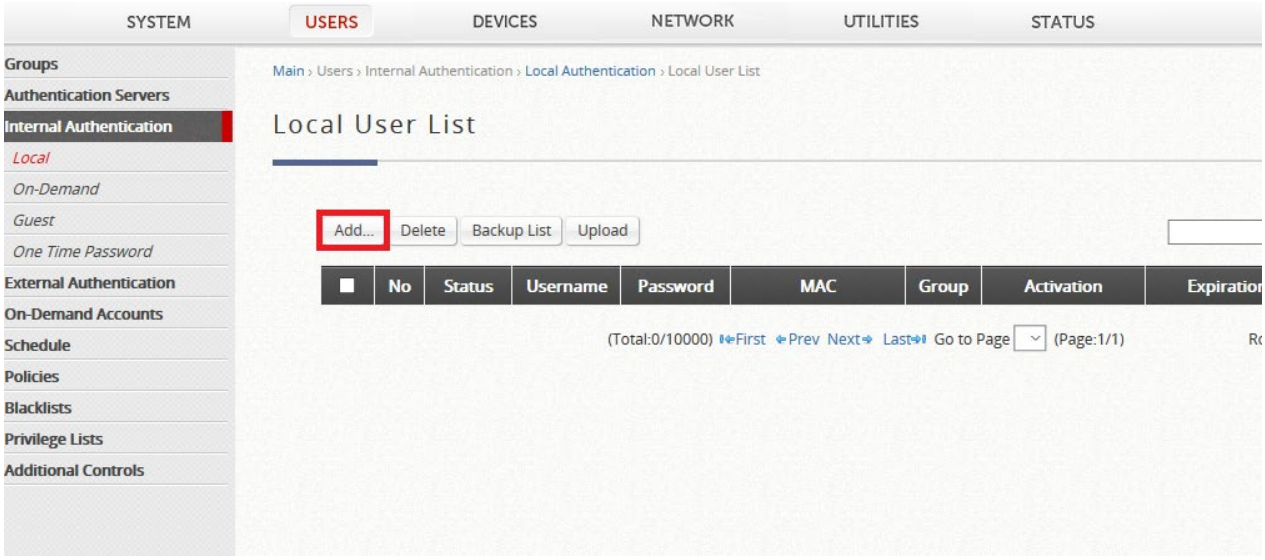
c. Go to *System > Service Zone* to enable the Service Zones that will be providing services.

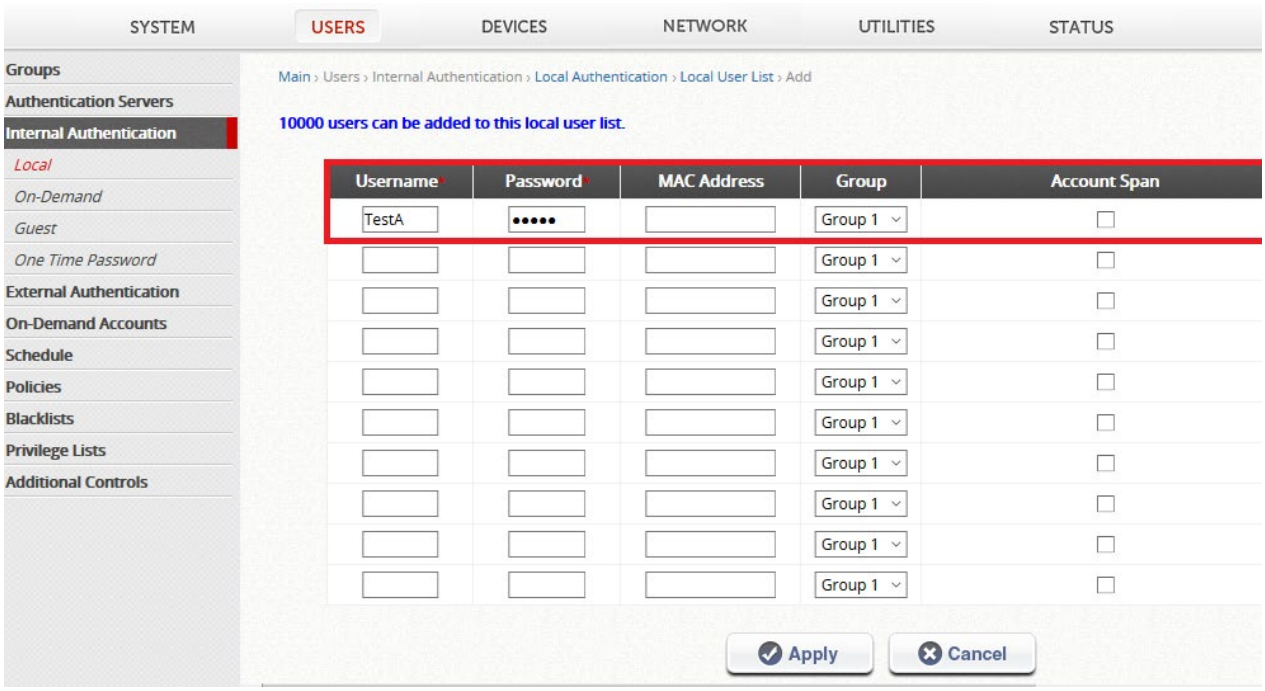


Default Service Zone: 192.168.2.254/255.255.255.0
Service Zone 1: 172.21.1.254/255.255.255.0
Service Zone 2: 172.22.1.254/255.255.255.0

d. For demonstration purpose, a Local account (Local Authentication) will be used. However, as mentioned previously, accounts of other authentication types can also be used. Go to *Users > Internal Authentication > Local* to set up a Local account.







e. Take an AP to connect to the Master Controller by establishing a CAPWAP tunnel. Perform the necessary steps to achieve this, such as configuring CAPWAP settings on both the Controller and the AP and applying a Template to the AP, where the Template has one VAP with Complete Tunnel enabled. This completes the set up for Cross Gateway Roaming on the Master Controller.

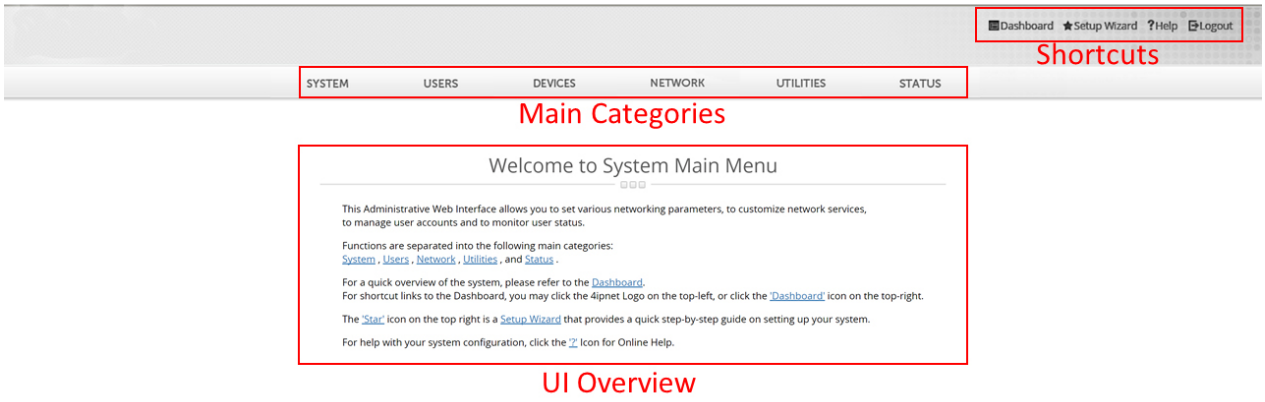
3 Slave Controller Configuration

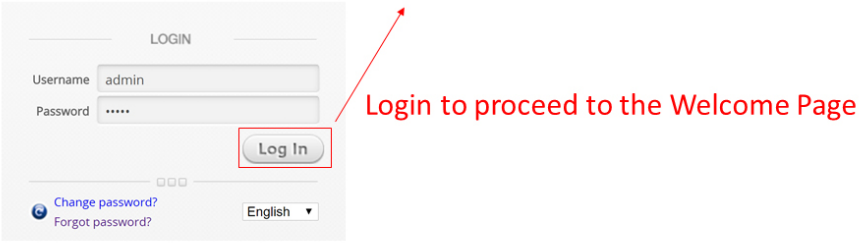
3.1 Enabling Cross Gateway Roaming

a. Access the Controller's Web Management Interface (WMI) by entering 192.168.1.254 in a web browser.

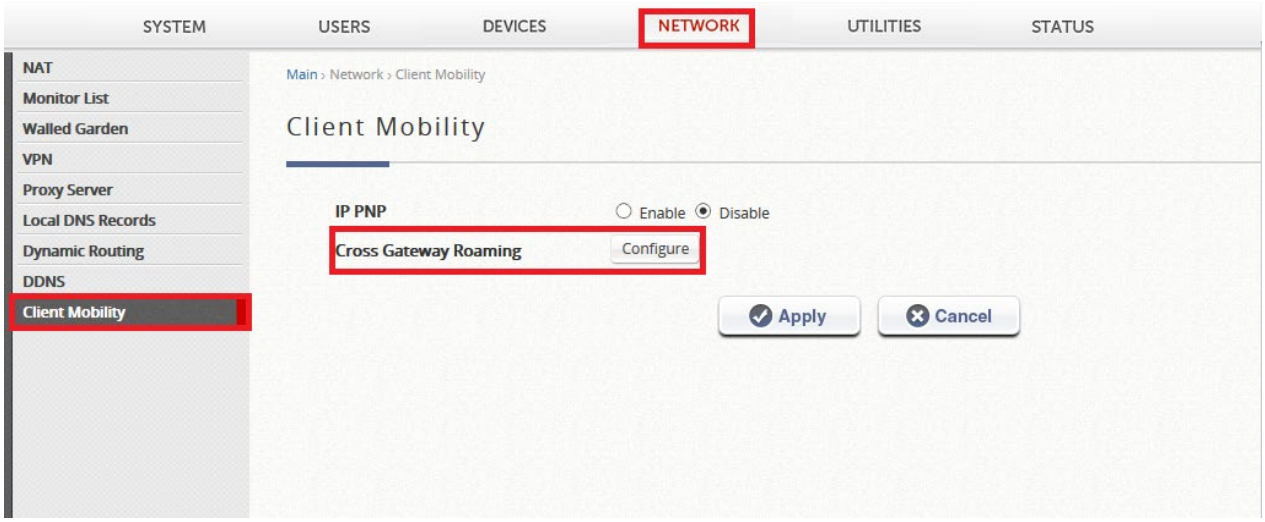
b. Login to the Controller using the default credentials: admin/admin

Note: Upon first-time login, the admin user will be asked to change the password.

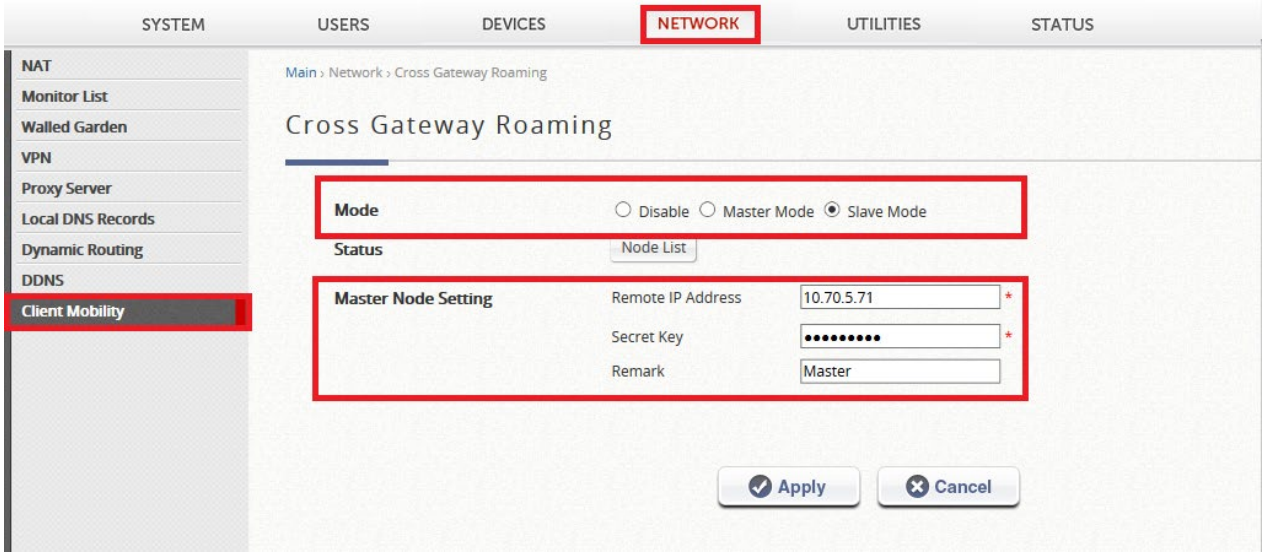




c. Go to *Network > Client Mobility > Cross Gateway Roaming*



d. Set this Controller to be in "Slave Mode" and enter the same security key.



e. Click on "Node List" to verify the set up

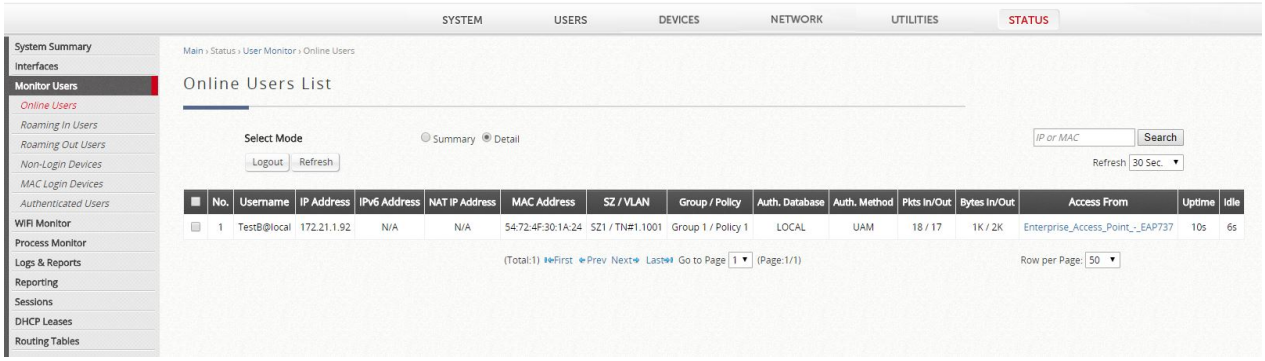
** From this figure, Cross Gateway Roaming has been established between the Master and Slave Controllers. Service Zones enabled on the Master Controller will be displayed.

** Important: When using Cross Gateway Roaming, please make sure the IP address ranges assigned to the Service Zones on both Controllers do not overlap. For instance, the default IP address range of the Default Service Zone is 192.168.1.254/255.255.0.0. Thus, only one Controller can have such IP address range, and the other one has to use a different IP address range to prevent IP address conflicts.

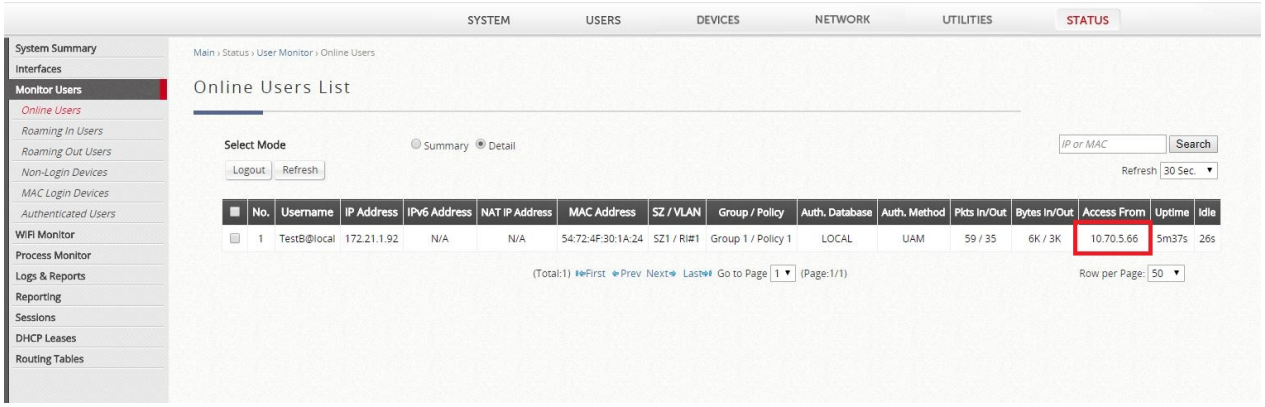
4 Logs

4.1 Login from Master Controller

a. Take a client to login to the network managed by the Master Controller (10.70.5.71), and then verify whether the client has successfully logged in by going to *Status > Monitor Users > Online Users* on the Master Controller. Here, the client is accessing from an EAP737 that is managed by the Master Controller using CAPWAP.

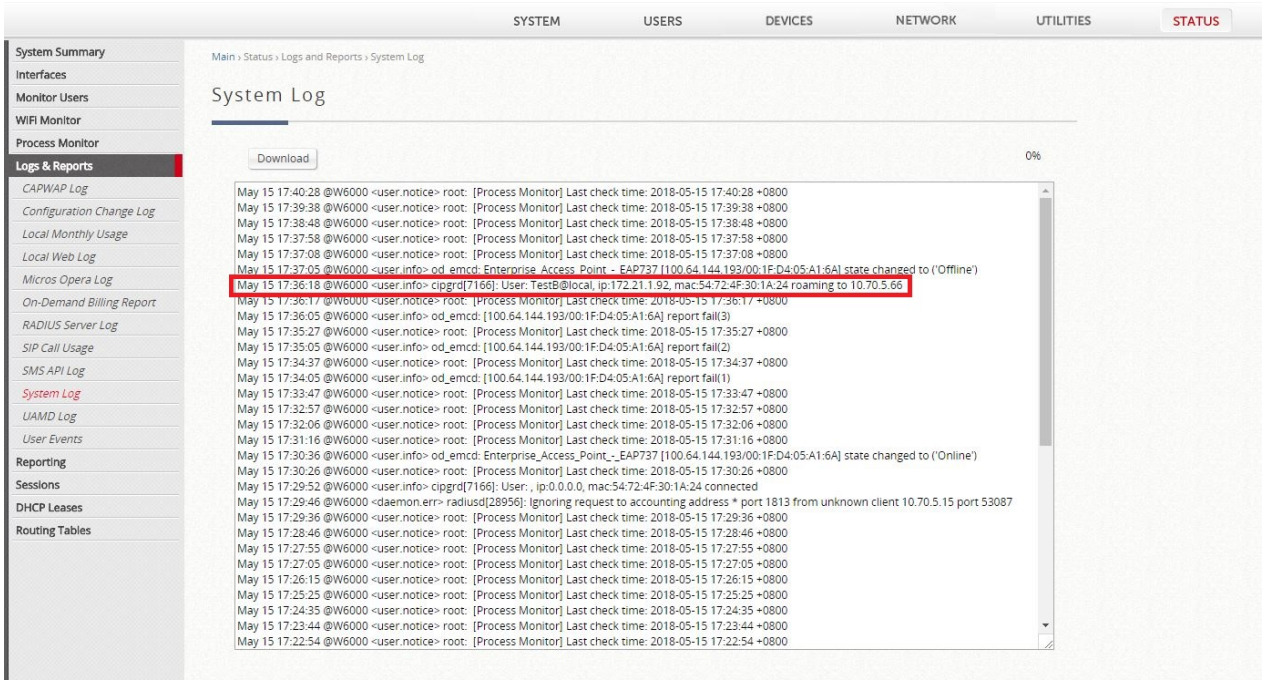


b. Take the client to roam to the network managed by the Slave Controller (10.70.5.66), and then check the “Online User list” on the Master Controller again. Notice that the client is now accessing from the Slave Controller.

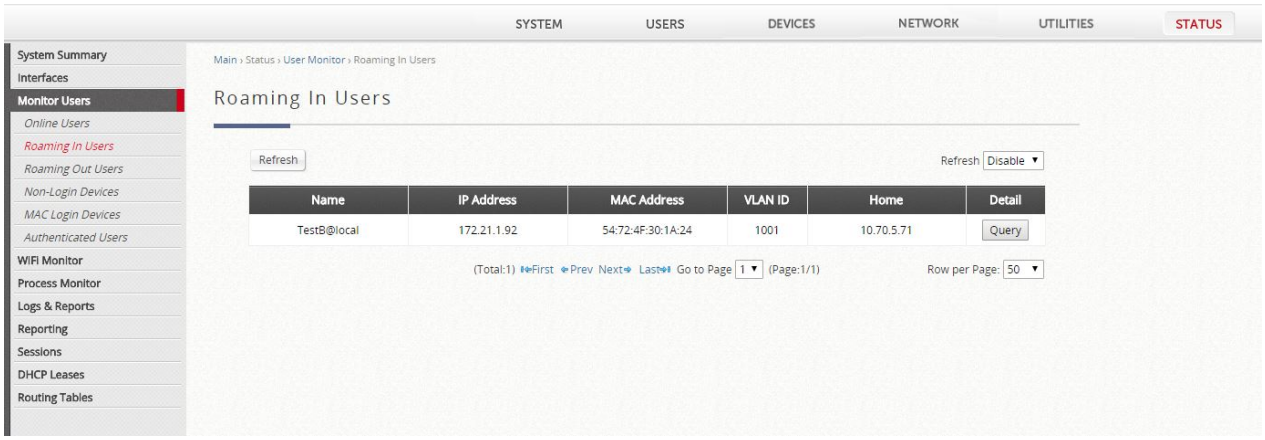


c. In the System Log of the Master Controller (*Status > Logs & Reports > System Log*), the following message will be displayed:

May 15 17:36:18 @W6000 <user.info> cipgrd[7166]: User: TestB@local, ip:172.21.1.92, mac:54:72:4F:30:1A:24 roaming to 10.70.5.66

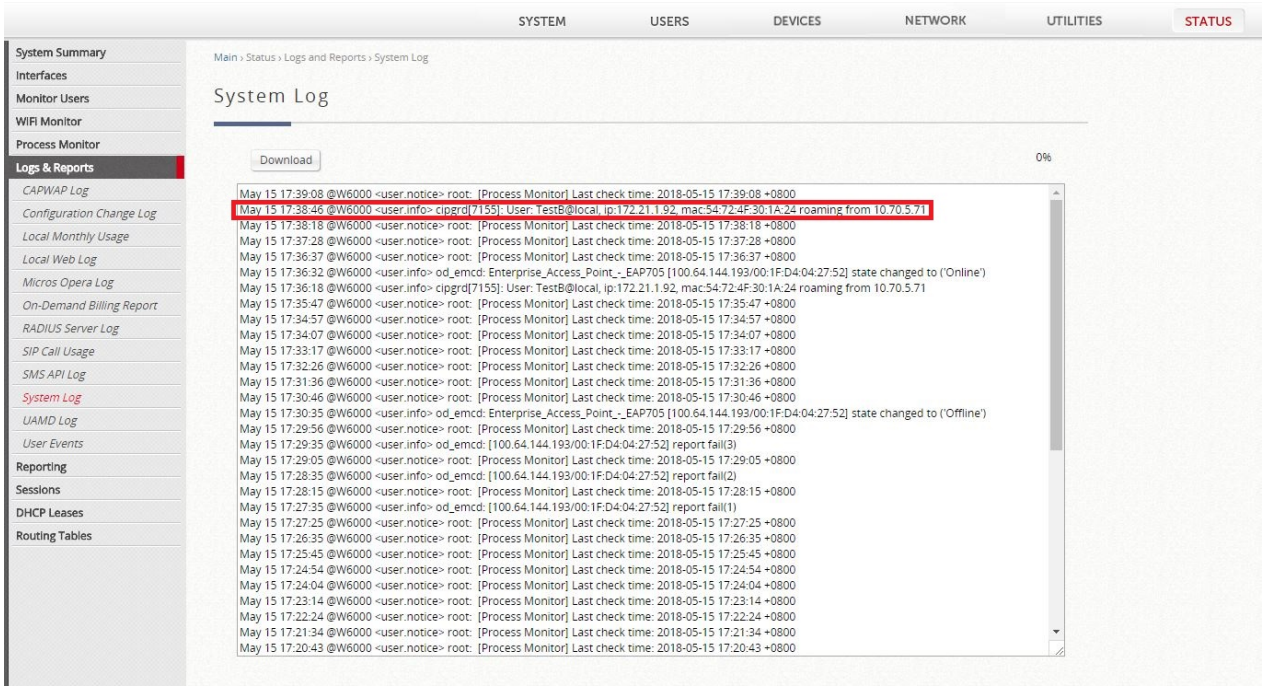


d. For the Slave Controller, the client will appear in "Roaming In Users" (*Status > Monitor Users > Roaming In Users*).



e. For In the System Log of the Slave Controller (*Status > Logs & Reports > System Log*), the following message will be displayed:

May 15 17:38:46 @W6000 <user.info> cipgrd[7155]: User: TestB@local, ip:172.21.1.92, mac:54:72:4F:30:1A:24 roaming from 10.70.5.71



5 Remarks

Please contact Technical Support Team for additional inquiries.