Profiles

Profiles are the basic building blocks of HotPoint AP configurations. They represent the settings of a virtual machine that can be instantiated on any HotPoint unit. Profiles are a set of configuration that can be applied onto an AP. These configurations include radio parameters, load balancing and rate limit parameters. Each access point under the control of the FWC2050 is capable of supporting 8 profiles per radio, or 16 profiles in total.

Small Networks

For small scale WLAN networks, you can use the basic configuration, and you don't need to create additional profile groups. All APs will belong to the same group and have the same configuration.

Larger Networks

For larger deployments, comprised of different sets of WLAN networks, you will need to use the advanced profile option. Under the Advanced profiles tab, you can create, edit, and delete profile groups. Editing a profile group will take the user to a profile edit page similar to the one under basic setting.

The Delete button, at the bottom of the screen, will delete the selected profile.

Once the creation of the profiles are done, you can go to the Configuration->WLAN Network page to assign profile groups to the APs.

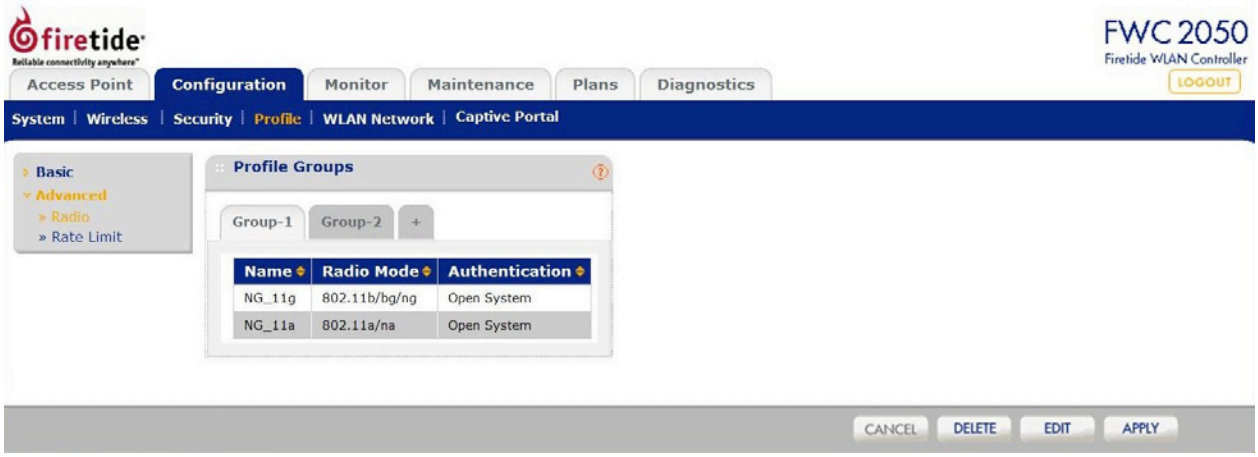
For ease of use, during a profile add, an option is given to the user to clone a profile. Cloning of a profile copies all the settings except the name and SSID.

Configuration templates for Authentication Server Settings in case of LDAP/Radius and MAC ACL list configuration needs to be done separately in their respective pages under Security. Once done, you can assign one of the created security profiles to a particular profile.

Profile Groups

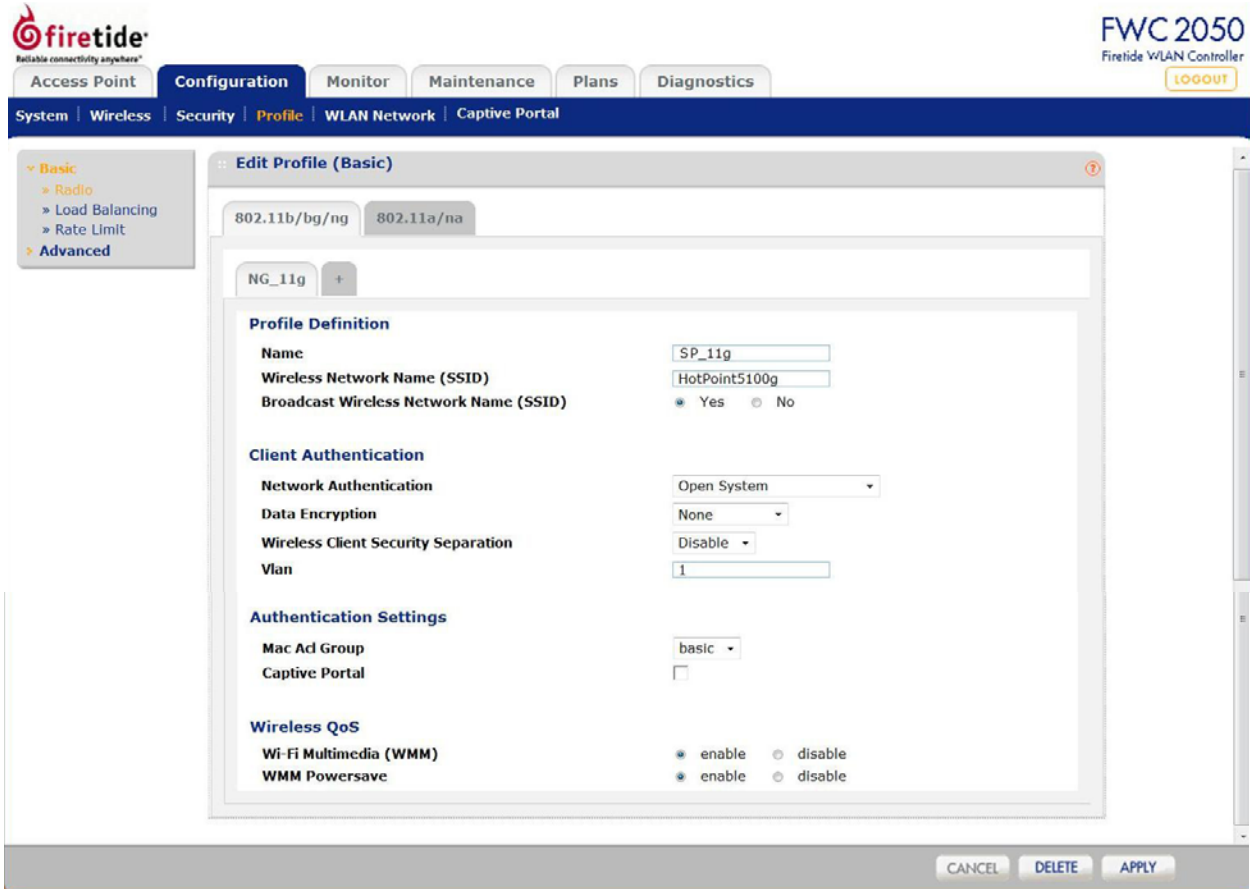
Complex deployments may require multiple sets of profiles. Groups are a way of managing large numbers of profiles. The controller supports configuration of up to 8 distinct set of grouped profiles. Each profile group can contain up to 16 profiles. You can configure these profiles and profile groups without worrying about the state of the APs. Once the APs connect to the controller these profile configuration will be pushed onto the AP. This is the method used to configure the WLAN network offline and then push the configuration once the WLAN network is up and running.

Two groups are defined by default. Additional groups can be created by clicking on the + tab next to the groups, in the Configuration - Profile - Advanced - Radio section, as shown below.



Basic and Advanced - Radio

Settings for Basic and Advanced are similar, except that the Advanced option allows you to configure settings per Group.



Name: Displays user-assigned name of profile.

SSID: Displays the SSID of access point.

Broadcast SSID: Enables broadcasting of the SSID in the clear.

Network Authentication: Displays type of authentication required.

Data Encryption: Displays encryption type.

Wireless Client Security Separation: Controls security among clients connected to AP.

VLAN: Specifies VLAN for traffic to/from this Profile.

MAC ACL Group: Defines MAC address Access Control List preferences.

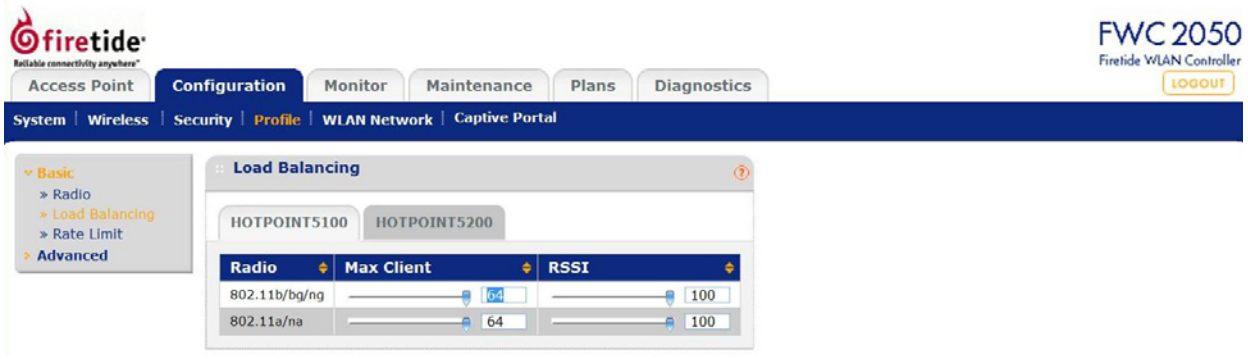
Captive Portal: Defines which, if any, captive portals are being managed.

Wi-Fi Multimedia (WMM): Enables WMM mode. Select this option to ensure that applications that require better throughput and performance are provided special queues with higher priority. WMM defines the following four queues in decreasing order of priority:

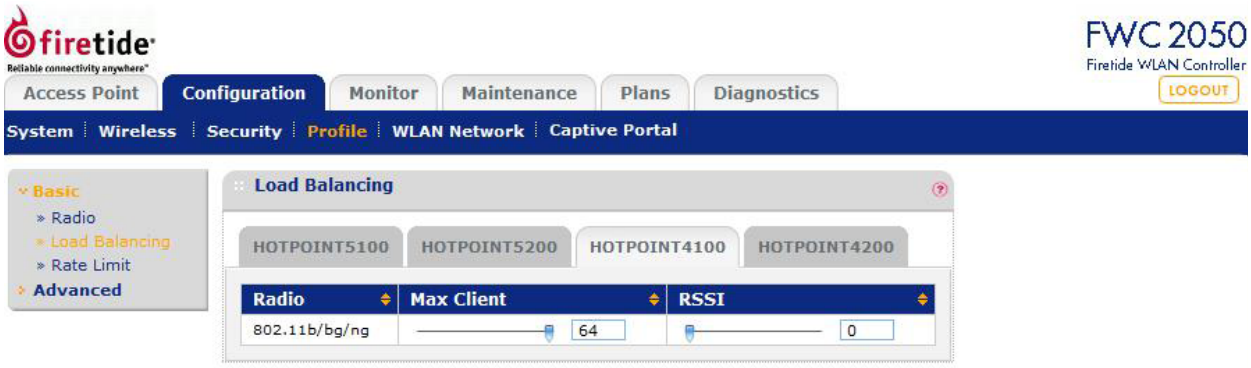
- **Voice:** The highest priority queue, minimum delay; ideal for VOIP and streaming media.
- **Video:** The second highest priority queue, low delay. Video applications are routed to this queue.
- **Best Effort:** The medium priority queue, medium delay. Most IP applications use this queue.
- **Background:** Low priority queue with high throughput. Applications which are not time-sensitive but require high throughput can use this queue.

With WMM enabled, QoS prioritization and coordination of wireless access is on. Disabling WMM will deactivate QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point.

WMM Powersave: Enables Powersave option for WMM.



or



Max Client: The maximum number of clients the that can connect to this profile.

RSSI: Defines the weakest signal that the APs in this profile will accept.

The controller supports balancing of load on the APs it manages. This is based on the number of clients connected to APs as well as signal quality of clients. At the time a client discovers APs (using probe requests) or sends association frames, AP decides whether to accept a client or not based on the number of clients already connected or the signal strength of the clients.

The two configurations are:

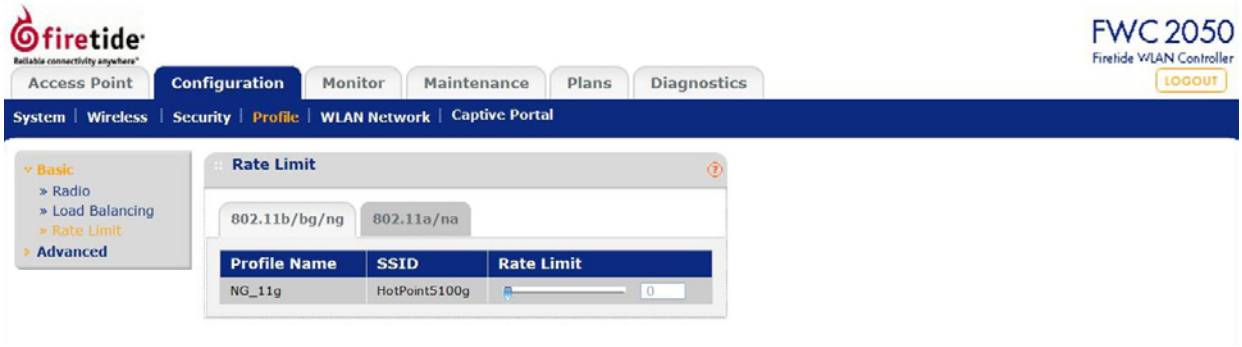
Max Clients: The maximum number of wireless clients that can connect to each radio of Access Point at one time. A value of 64 can be selected to specify to allow maximum supported by Access Point.

RSSI: The minimum signal quality in percentage (0 - 100) % expected from the wireless clients that connect to the Access Points. A value of 0 means this check is not enforced and load balancing is disabled.

Setting the Max. number of clients to a low value (compared to the total number of client in an office/floor) is recommended when there are several APs and the administrator would like a good distribution of clients between the access points.

Setting the RSSI to a high percentage would mean that only clients near to APs will be permitted to associate to the APs and is good in situation where the throughput expectation is high. In scenarios, where the clients can be expected to be far away (or the number of APs is less), this should be set to a lower value.

Basic and Advanced - Rate Limiting



The Rate Limiting feature can be configured differently for each BSSID in security profile group. Rate limiting is done per BSSID and is configured as a percentage of available bandwidth. Available bandwidth is determined by the number of errors occurring during transmission and the amount of time a packet spends in the transmission queue.

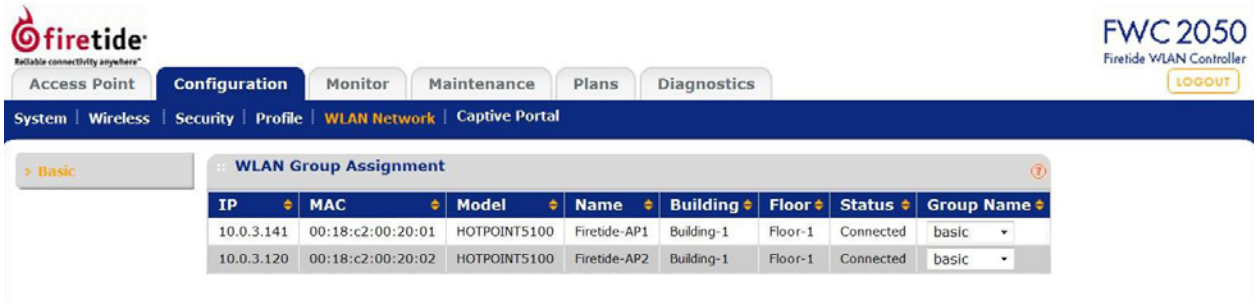
The available bandwidth is distributed among the BSSIDs configured on the Access Points as a specified percentage. The percentage configured for a BSSID is shared among all the clients connected to it. The total of the percentages distributed among the BSSIDs can be up to 100%.

Rate Limiting can be disabled by setting the limit to 0%. This can be useful for having BSSIDs for management/administration/testing.

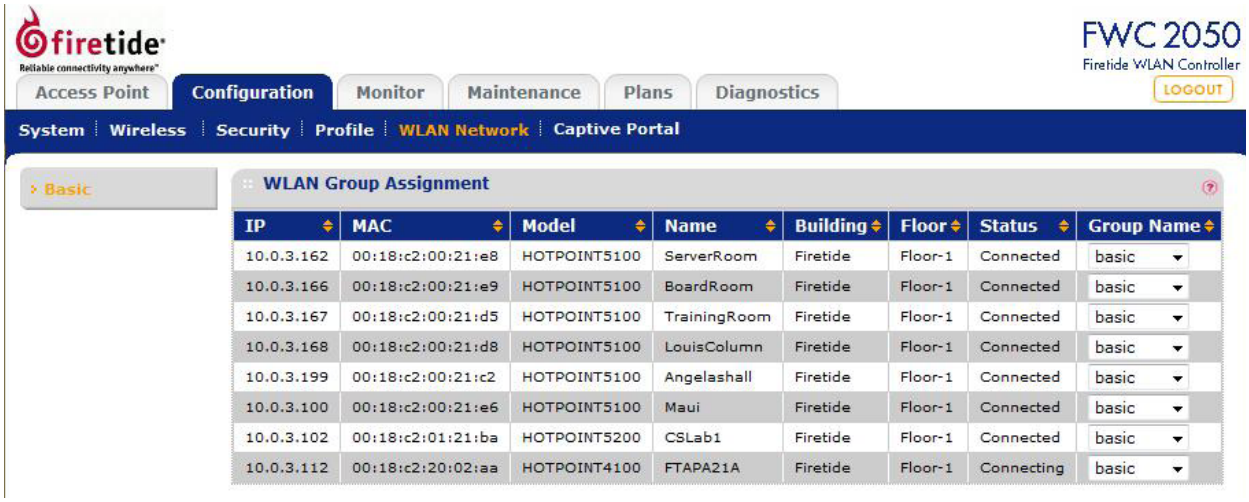
Rate Limit: The slider bar and value specify configured rate limit values.

WLAN Network

This screen allows you to assign each AP to a group.

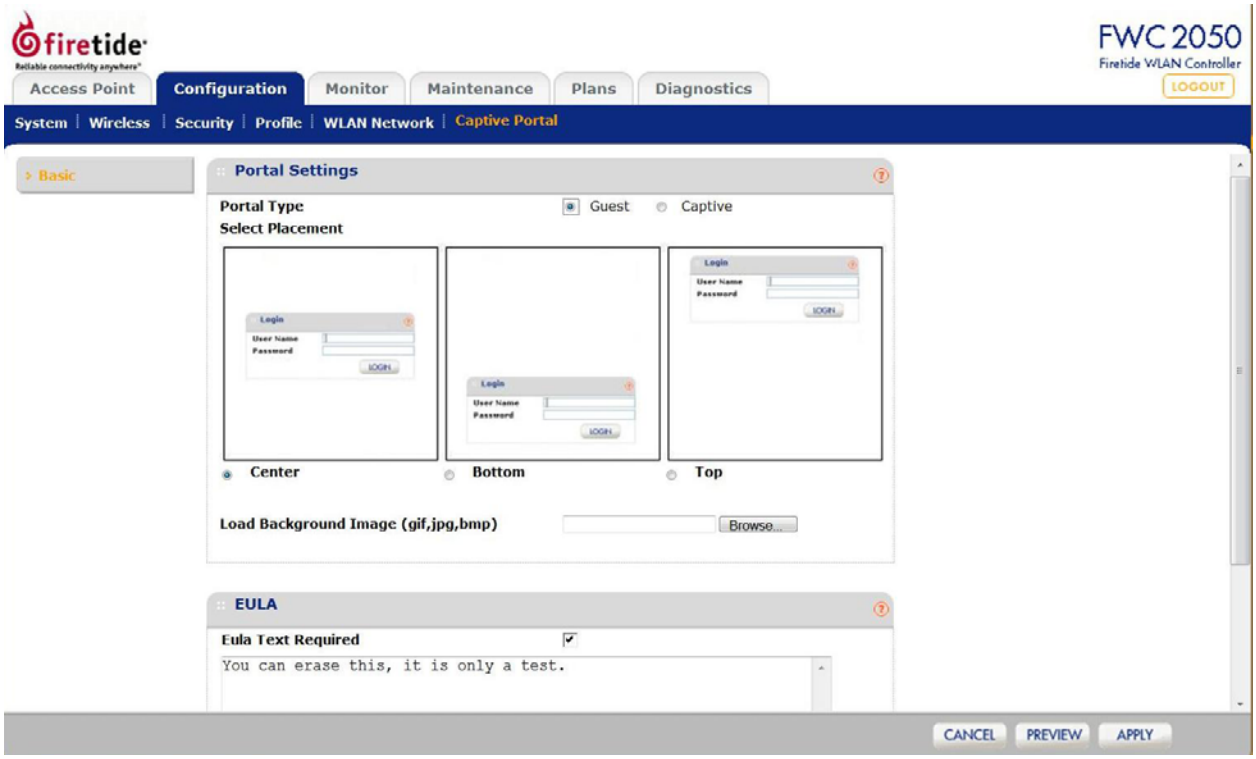


or



Captive Portal

The Captive Portal allows you to require the user to log in, and optionally accept a EULA, in order to use the wireless service.



Portal Type: Portals can be guest (open to all) or require an ID and password. In Guest mode, the user must enter an email address to gain access. In Captive mode, the user must enter a user name and password. These values are defined as shown in "Maintenance" on page 35.

Select Placement: Allows you to position the login in a location compatible with the background image.

Load Background Image: Allows you to place an image with logos, etc as required for your application.

EULA Text Required: You can optionally require a EULA. Enter the EULA text in place of the 'test' text, and tick the enable box.