

# Captive Portal and Internal RADIUS Server Setup

## HOW TO GUIDE



June 2015

© 2015 ZIH Corp. All rights reserved. Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are property of their respective owners.

# Overview

Zebra markets two separate product lines in the WLAN Portfolio: WiNG, for large enterprises with complex distributed network deployments, and WiNG Express, for small to mid-size companies that need an easily managed, cost effective wireless network solution with enterprise-class features to support their business activities. Both of these architectures have the same operating system at their core – WiNG 5. While WiNG Express is perfect for many of our customers, it can be tricky to understand when customer requirements demand a more extensive feature set.

## 1. CAPTIVE PORTAL

Captive portals provide secure authenticated or un-authenticated access to Wireless LANs using standard Web browsers. Captive portals function by capturing and redirecting a wireless user's Web browser session to a landing page where the user must enter their credentials, accept terms and agreement or supply specific information before being permitted access to the Wireless network.

Captive portals can be utilized for multiple applications including guest / visitor access, hotspots or BYOD and are now common in most enterprise environments. Captive portals have become a very popular means for authenticating guest / visitor users as they provide administrators with the means for implementing authentication without deploying 802.1X or distributing pre-shared keys. More recently captive portals have also become a popular mechanism for on-boarding devices for secure guest access applications by re-directing corporate or guest / visitor user's web-browser sessions to a service which can quickly provision the device to connect to a secure network.

WiNG Express provides Captive Portal operation for Hotspots and Guest Access for visitors. This service is completely flexible and permits content customization, according to type or deployment conditions.

The Captive Portal operation is controlled using embedded captive portal policies which are assigned to respective guest Wireless LANs that are performing the capture and redirection. Each captive portal policy defines:

1. The captive portal type (authenticated vs. non-authenticated).
2. The captive portal connection mode (HTTP or HTTPS).
3. The authentication method (internal, external).
4. Login, welcome, failed and terms of condition web page source and customization.

When enabling captive portal services in a WiNG Express network, there are two main choices that need to be made. The first choice is to determine if and how the captive portal authenticates the users, a terms and conditions page is presented. The second choice determines where in the network the captive portal pages are hosted. Captive portal pages can be hosted on the WiNG Express Virtual Controller, Access Points, external HTTP server or an external appliance providing secure guest access provisioning.

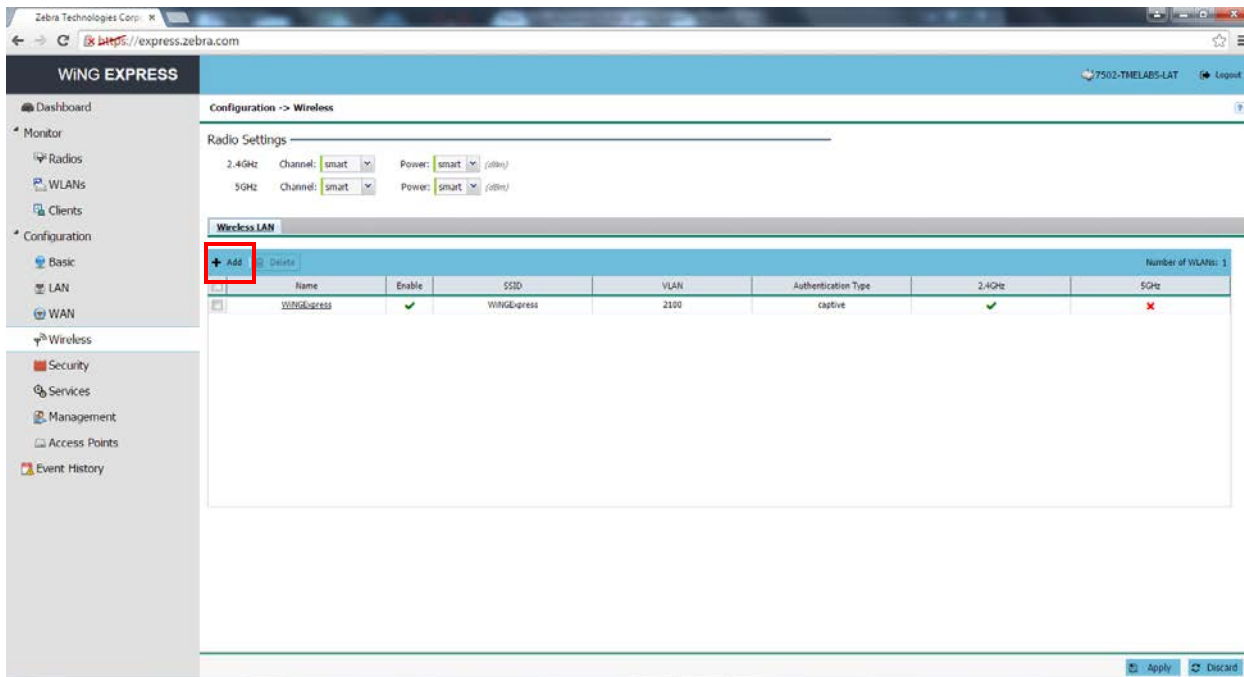
The choice as to how authentication is performed, where the captive portal pages are hosted and which devices perform the capture and redirection will largely depend on the specific type of deployment.

The following steps describe how to configure Captive Portal services using WiNG Express devices.

## 2. GUEST WLAN CONFIGURATION

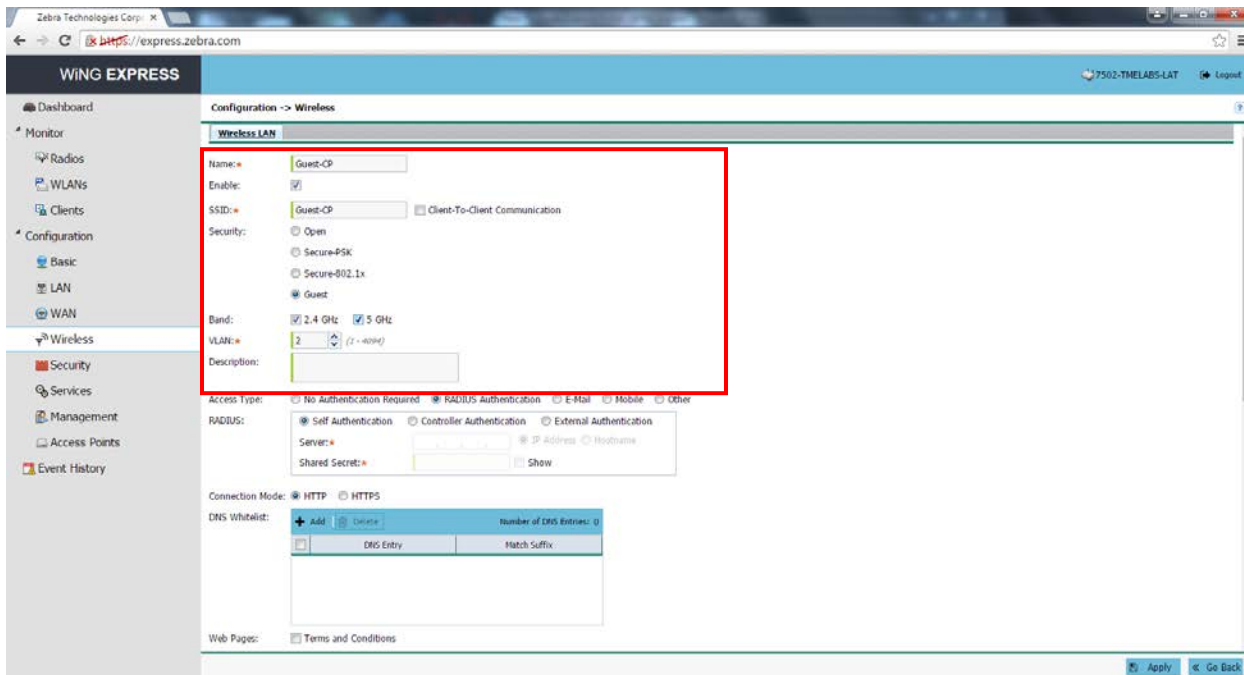
To create a new Guest WLAN service, select Configuration->Wireless options at WiNG Express GUI.

Click in "Add" to create a new Wireless LAN service.



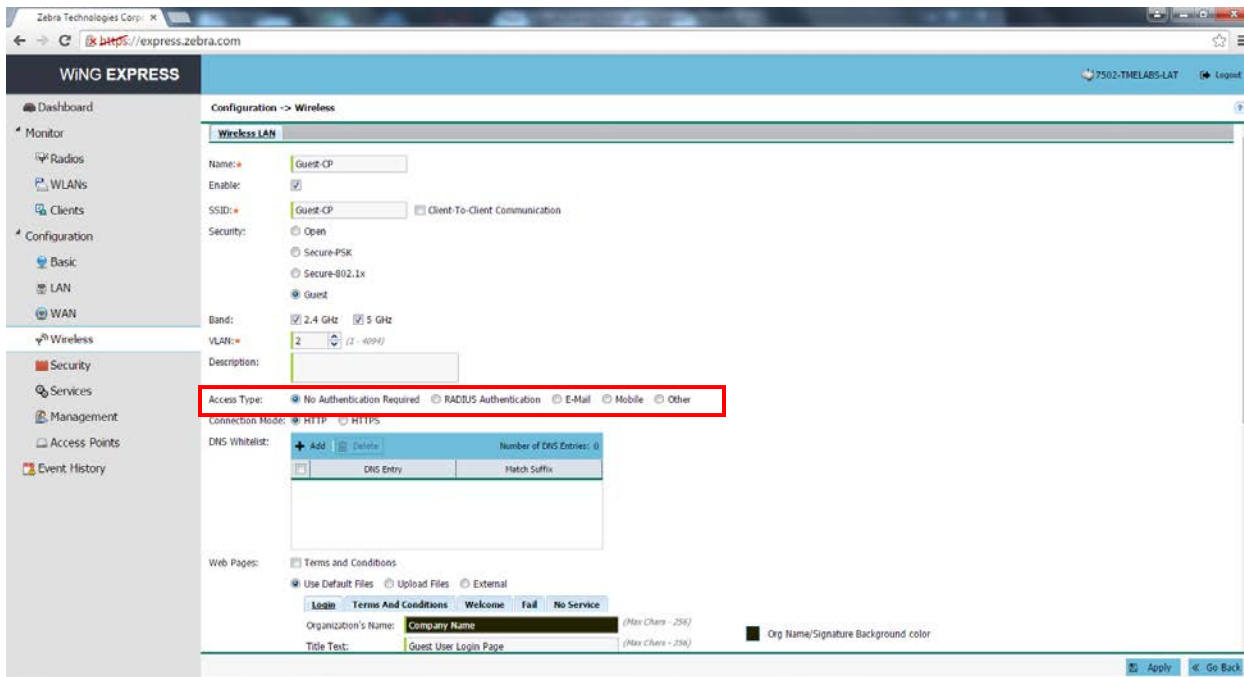
You will be guided to a new sub-menu. To enable a Guest WLAN service, the following settings shall be configured:

Option	Description
Name	Guest WLAN service name
Enable	Click to get Guest WLAN enabled
SSID	Guest WLAN SSID. If a local RADIUS authentication is part of your WLAN service, please type the same SSID name configured at RADIUS group
Security	Select "Guest" to enable WLAN Guest services
Band	Radio band which this service will be provided. If your WiNG Express device is a dual-band radio supported model, it is suggested to enable both bands to enable service offload
Service Time	Date and time which subscriber is allowed to access WLAN Guest service
VLAN	Guest WLAN service VLAN
Description (optional)	Short description for Guest WLAN service



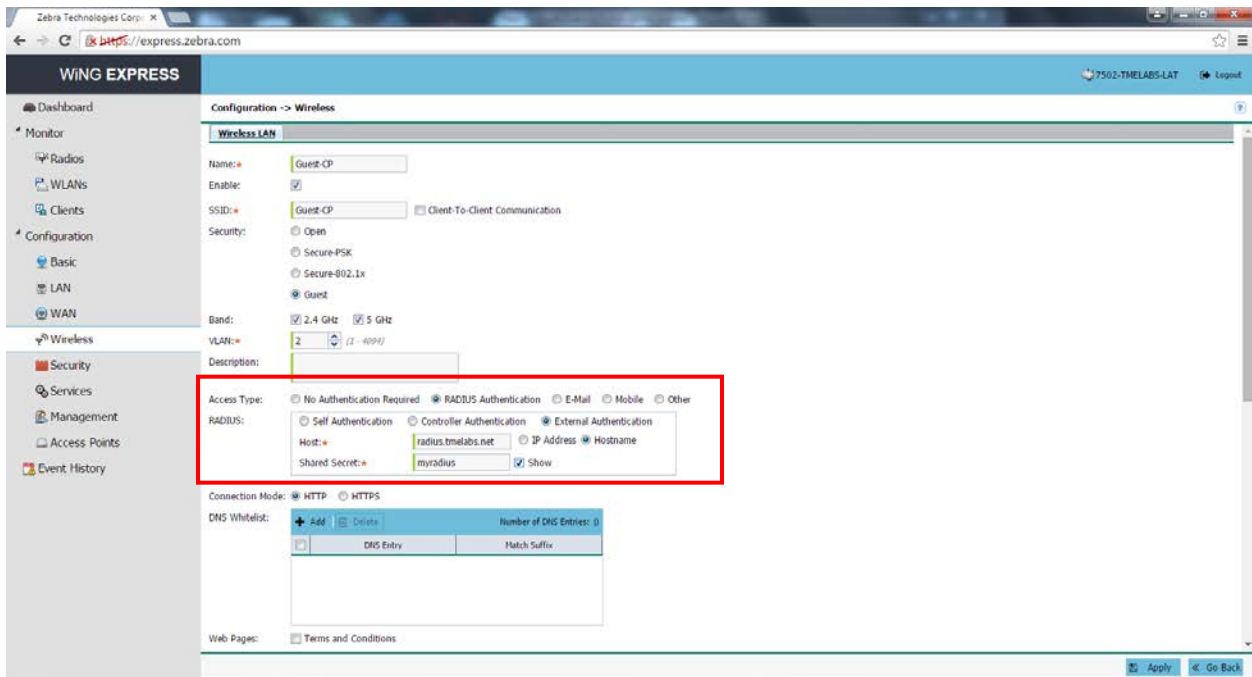
A Guest WLAN allows different Access Types for subscriber authentication. Those options permit that Guest WLAN service can be configured according to your network requirements or architecture design.

Option	Description
No Authentication Required	Select this option if your Guest WLAN does not require RADIUS authentication
RADIUS Authentication	Enable if Guest WLAN required RADIUS authentication
E-Mail	Select if your service requires e-mail validation (this information shall be configured at RADIUS user database/information)
Mobile	Select if your service requires mobile number validation (this information shall be configured at RADIUS user database/information)
Band	Radio band which this service will be provided. If your WiNG Express device is a dual-band radio supported model, it is suggested to enable both bands to enable service offload
Service Time	Date and time which subscriber is allowed to access WLAN Guest service
VLAN	Guest WLAN service VLAN
Description (optional)	Short description for Guest WLAN service



If RADIUS Authentication option is selected, WiNG Express supports three different modes of RADIUS setup:

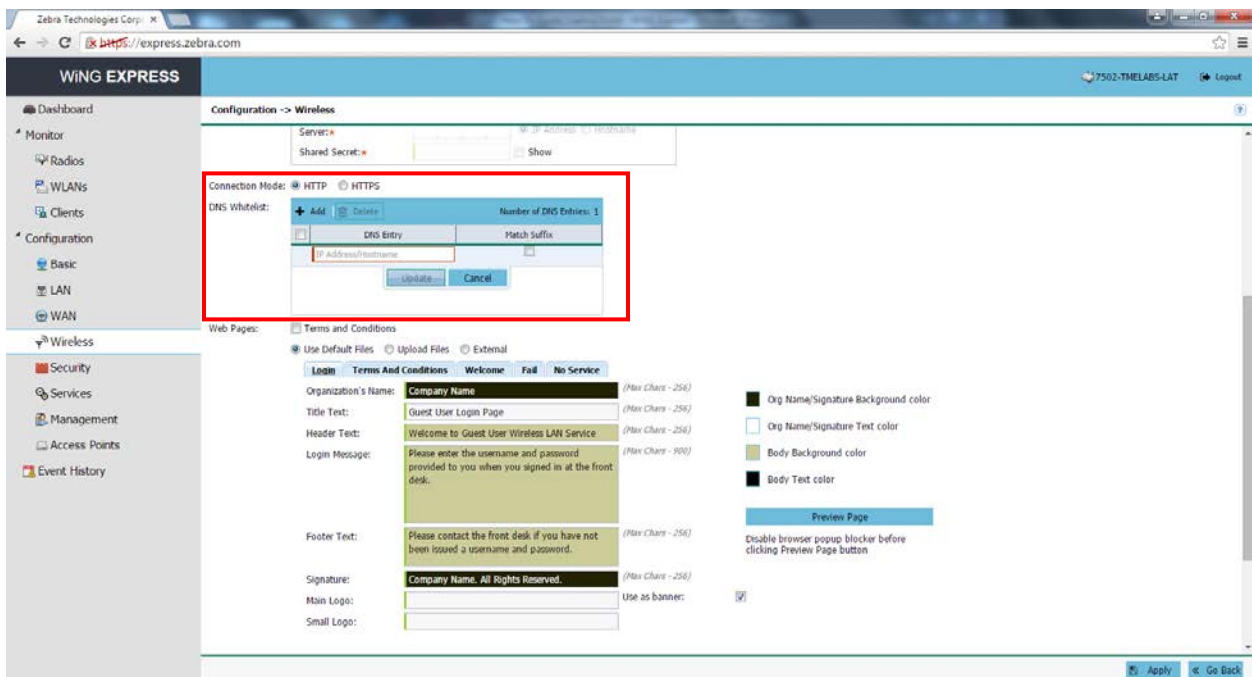
Option	Description
Self Authentication	Select this option if your WiNG Express Access Point will authenticate Guest WLAN subscribers. Recommended in stand-alone or independent Access Point setup
Controller Authentication	Select this option if you have a WiNG Express Virtual Controller set in your network
External Authentication	Select this option if an external RADIUS server will authenticate Guest WLAN subscribers. Type the IP address or Hostname and RADIUS secret to enable WiNG Express device to forward RADIUS authentication



If your Captive Portal service shall be provided over HTTP or HTTPS mode, please select the proper protocol at Connection Mode options.

Optionally, when Open-Garden pages (e.g. Promotions, Corporate Portal, Advertisements, etc) can be allowed to be accessed by WLAN subscribers without authentication, a DNS Whitelist shall be configured to avoid Captive Portal redirect issues.

To configure a DNS Whitelist, click in "Add" and select all IP addresses or DNS entries which are not being intercepted by WiNG Express Captive Portal. If an entry has flexible URL or hostnames (suffixes), select "Match Suffix" box to avoid redirection issues.

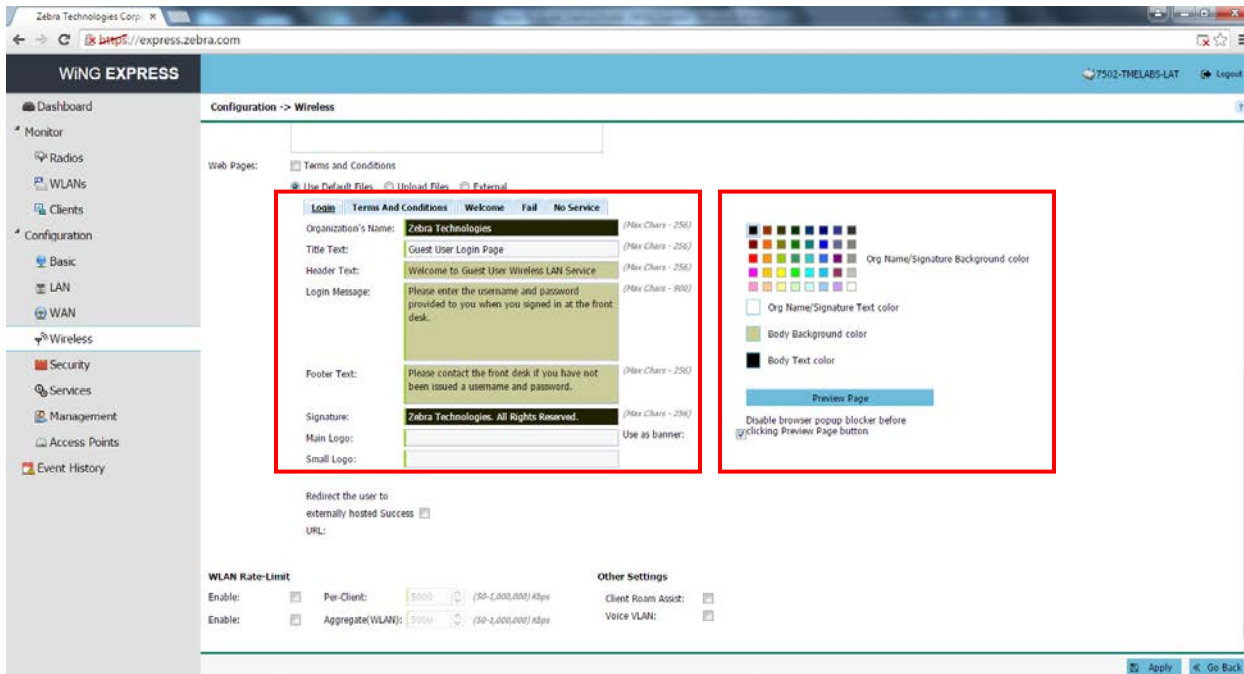


Once authentication type is enabled, Captive Portal pages shall be configured in order to provide the expected content to be displayed to your subscribers during authentication process.

WiNG Express Captive Portal services support the following options:

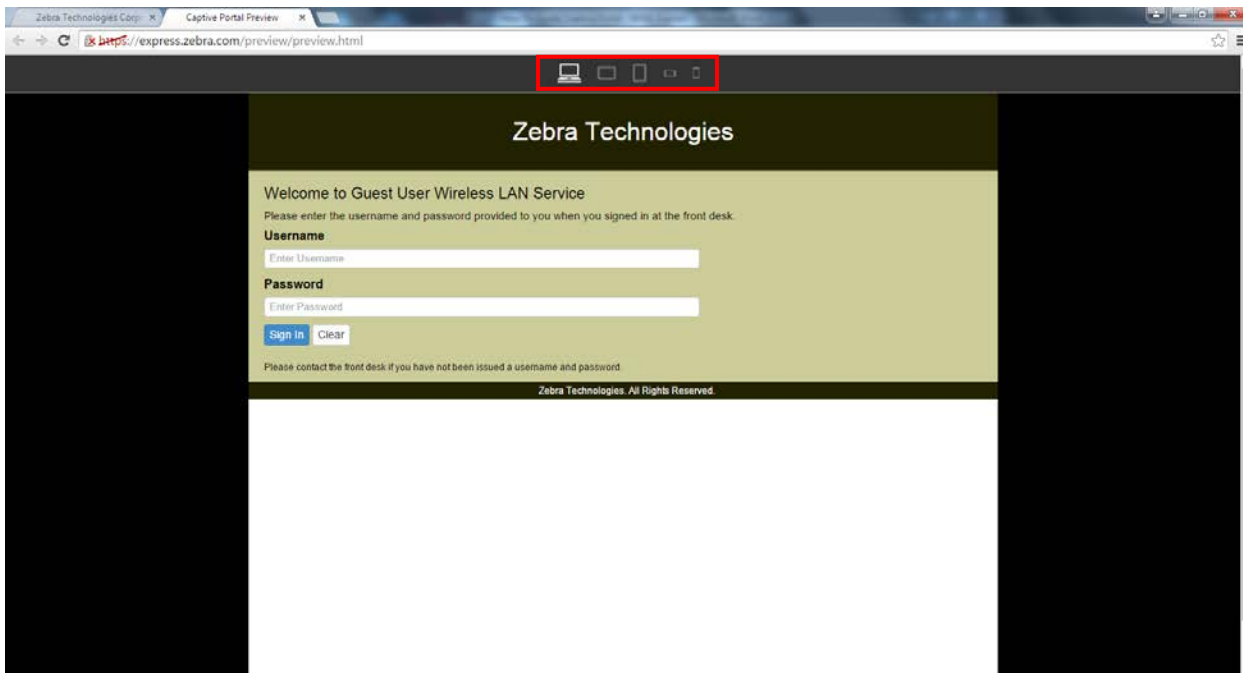
Option	Description
Use Terms and Conditions	To display Service Terms and Conditions, select the box to have the terms displayed in Main Captive Portal user authentication page
Use Default Files	Select this option if you will use embedded WiNG Express Captive Portal
Upload Files	Select this option if you want to send customized pages to WiNG Express device. A WiNG Express device supports standard HTML formats and basic javascript components. Files can be uploaded via FTP, TFTP or HTTP.
External	Select this option if your Guest WLAN service pages are provided from an external server.

If your option is to use Default Files, WiNG Express supports that Captive Portal pages has text and content customization, as like as webpage format (Company Logo, Colors, etc) can be customized in accordance with your Corporate design template.

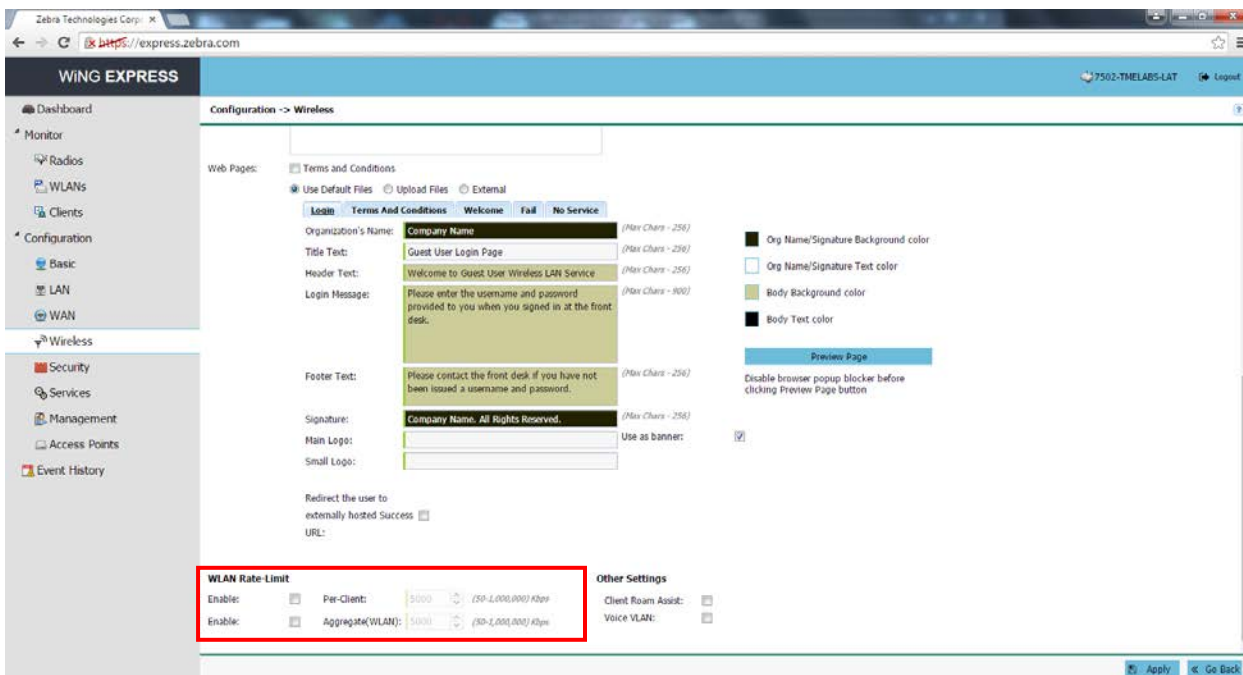


To have a preview of customization process, select the "Preview Page" button above of color pan. Please make sure that your browser is with popup blocker option disabled.

A new page is displayed that allow you having a preview in all supported view formats (PC, Tablet, Mobile).

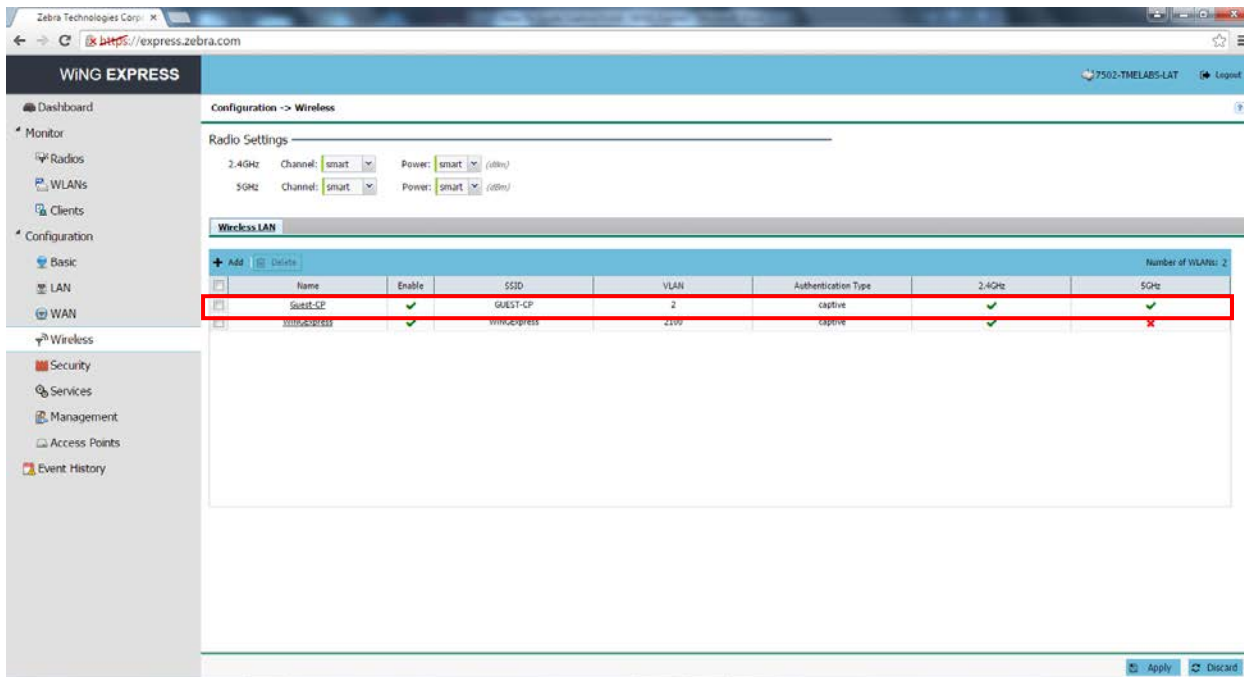
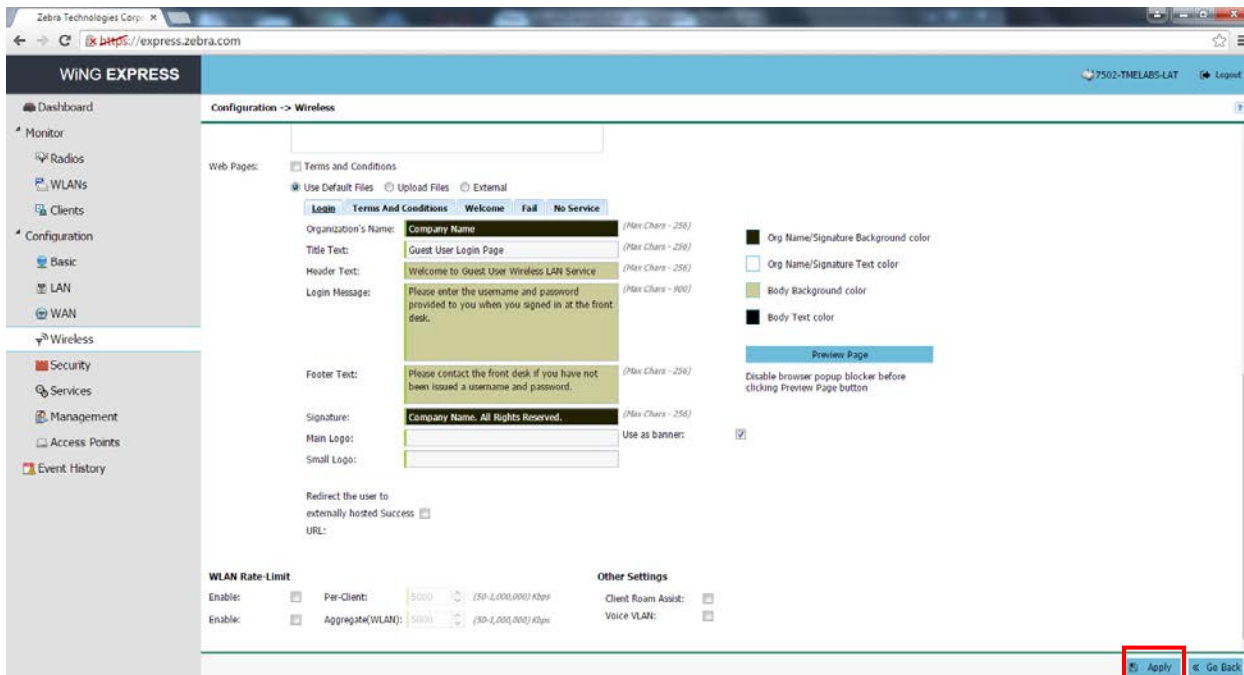


Finally, if the Guest WLAN service shall have Rate-Limit settings enabled (per user or per aggregate WLAN), select the required bandwidth limitation to be applied with the proper bandwidth size to be used in Traffic Shaping services.



After making all required settings, please click at “Apply” button. The Guest WLAN service will be displayed as a “captive” Authentication Type into Wireless LAN list.





## WORKING WITH CUSTOMIZED PAGES

WiNG Express devices supports that customized HTML pages can be uploaded, in order to modify default Captive Portal pages according to customer requirements or to service policies. The Access Point supports LightHTTP service, which is possible to handle Captive Portal pages based on CSS.

WiNG Express Captive Portal service is composed by the following files: acknowledgement.html; agreement.html; agreement\_view.html; fail.html; login.html; noservice.html; tc.html; welcome.html and cp\_style.css

Below you can describe the structure of welcome.html default file, where is possible to select and configure all necessary fields to be selected for a customized page.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta name="viewport" content="width=device-width, maximum-scale=1.0, user-scalable=yes" />
  <title>Guest User Login Page </title>
  <link rel="stylesheet" type="text/css" href="cp_style.css" />
</head>

<body>

<div id="main" style="background-color:#222200; color:#ffffff">
  <!-- header start -->
  <header>
    <div class="org">
      <p class="name">Zebra Technologies</p>
    </div>
  </header>
  <!-- header end -->

  <!-- content -->
  <div class="bd" style="background-color: #cccc99; color: #000000;">

    <div class="message">
      <p class="title">Welcome to Guest User Wireless LAN Service</p>

      <p class="subtitle show">Please enter the username and password provided to you
when you signed in at the front desk.</p>
    </div>

    <div class="form">
      <form name="frmLogin" id="frmLogin" action="/cgi-bin/hslogin.cgi" method="POST"
onReset="return clear()">
        <div class="normal-login show">
          <dl>
            <dt>Username</dt>
            <dd><input class="control" name="f_user" id="f_user" type="text"
placeholder="Enter Username"></dd>
          </dl>
        </div>
      </form>
    </div>
  </div>
</div>
```

```
        <dt>Password</dt>
        <dd><input class="control" name="f_pass" id="f_pass"
type="password" placeholder="Enter Password"></dd>
    </dl>
    <input size="64" name="f_hs_server" id="f_hs_server" type="hidden">
    <input name="f_Qv" id="f_Qv" type="hidden">

    <input name="submit" value="Sign In" type="submit" class="btn primary">
    <input name="reset" value="Clear" type="reset" class="btn default">
    </div>
    </form>
</div>
<div class="info">
    <p class="subtitle show">Please contact the front desk if you have not been
issued a username and password.</p>
</div>
</div>
<!-- content end -->

<!-- Org footer -->
<footer>
    <div class="org footer">
        <p class="copyright">Zebra Technologies. All Rights Reserved.</p>
    </div>
</footer>
<!-- Footer -->
</div>
<script>
// function to get the query parameter value from URL query string.
function getQueryVariable(variable) {
    var query = window.location.search.substring(1);
    var vars = query.split(/[?&]/);
    for (var i=0;i<vars.length;i++) {
        var pair = vars[i].split("=");
        if (pair[0] == variable) {
            if (pair[0] == "Qv") {
```

```

        return vars[i].substr(3, vars[i].length);
    }
    return pair[1];
}
}
return "";
}

if (navigator.userAgent.indexOf('iPhone') != -1) {
    addEventListener('load', function() {
        setTimeout(hideURLbar, 0);
    }, false);
}

function hideURLbar() {
    window.scrollTo(0, 1);
}

function clear(){
document.getElementById('f_user').value = "";
document.getElementById('f_pass').value = "";
return true;
}

var hs_server = "NONE";
var port = 880;
var postToUrl = "/cgi-bin/hslogin.cgi";
hs_server = getQueryVariable("hs_server");
Qv = getQueryVariable("Qv");
postToUrl = ":" + port + postToUrl;

document.forms['frmLogin'].elements['f_hs_server'].value = hs_server
document.forms['frmLogin'].elements['f_Qv'].value = Qv
document.getElementById("frmLogin").action = "http://" + hs_server + postToUrl;
</script>

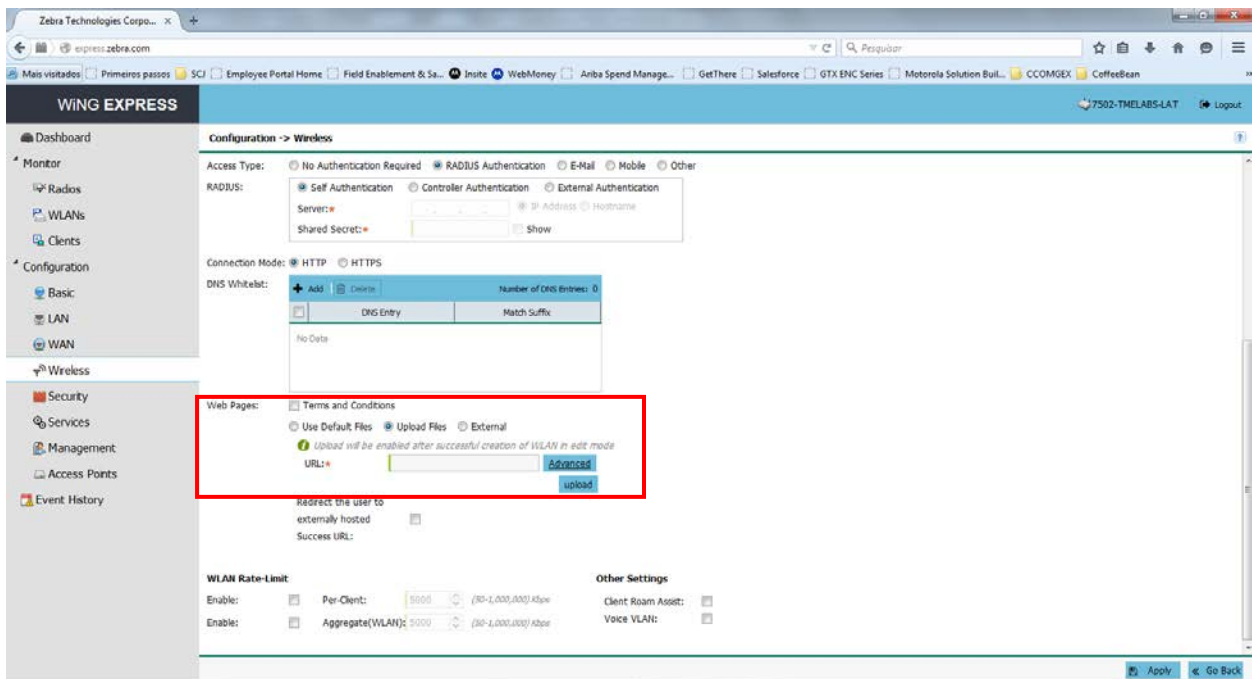
```

</body>

</html>

Once making all adjusts, the HTML and CSS files can be uploaded to a WiNG Express device, using TFTP, FTP or HTTP services.

To upload the files, select “Configuration -> Wireless”. Go to “Web Pages” option and select “Upload Files”.



Before starting file transfer process, click in “Advanced” button. Once selected, you will be able to add all information for server host.

Option	Description
Protocol	Select which protocol is being used for file transfer process (FTP, TFTP or HTTP). <b>Make sure that your host has the proper server enabled and configured.</b> If the server is enabled in a different port, you can select service port at the field “Port”.
Host	Server hostname or IP Address
Username	Server Username
Password	Server Password
Path	Server Path and filename

After completing all information above, click in “Upload”.

### 3. DHCP SERVER AND NAT CONFIGURATION

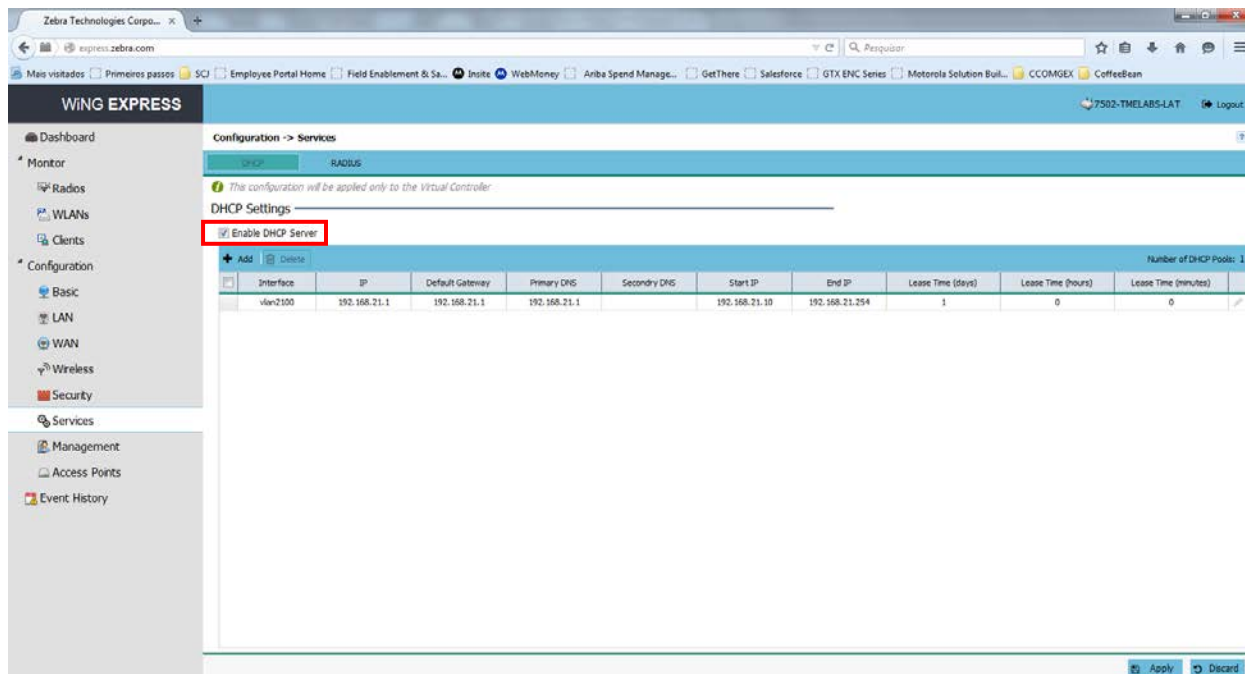
In order to enable Captive Portal and Hotspot services over a WiNG Express device, is required also to define the DHCP scope with IP address range to be allocated to all hotspot subscribers. In addition, if necessary, a NAT service shall be enabled over hotspot VLAN interface.

#### 3.1 DHCP SERVICE CONFIGURATION

To make sure that DHCP server is enabled into Express AP, select “Configuration-> Services”. If DHCP service is not enabled, please select the checkbox “Enable DHCP Server”.

Click in “Apply” button on the bottom right screen to commit and save the configuration.

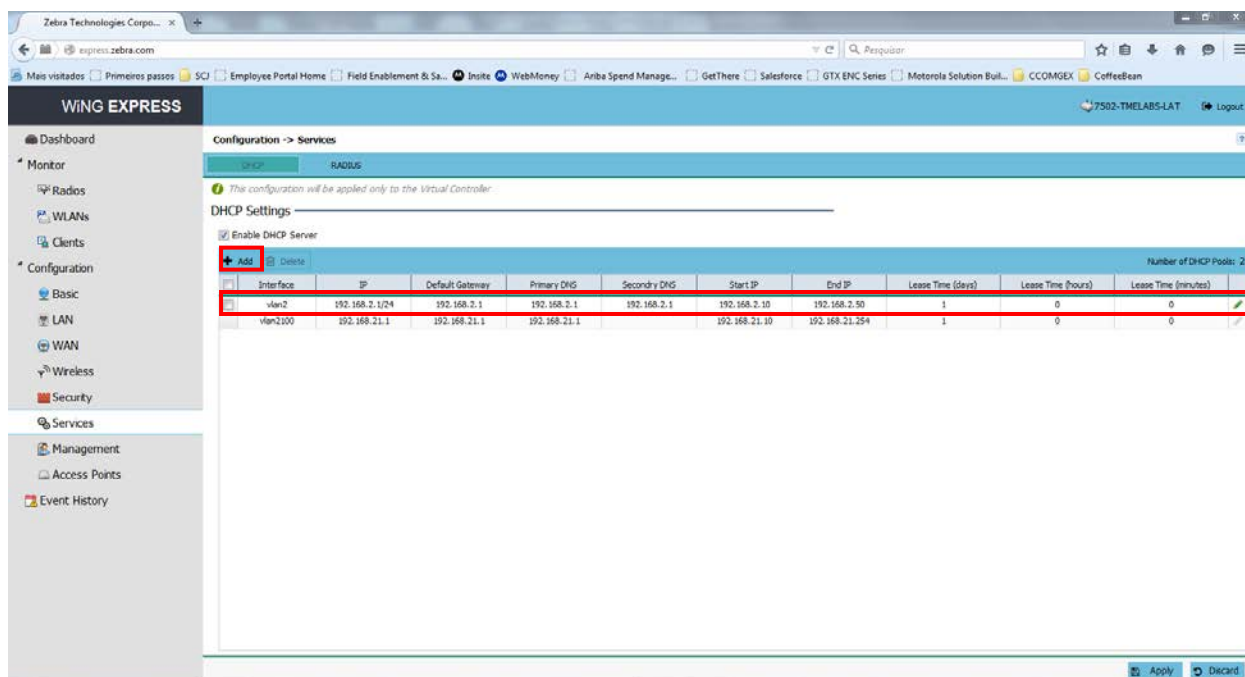
After enabling the DHCP Server, you will be able to add DHCP addresses scopes for hotspot configuration. You will be aware that a scope for VLAN 2100 is already present. This interface is built by default by WiNG Express OS to support AP management.



To add the address scope for hotspot service, click in "Add" button. You will notice that hotspot VLAN will be highlighted for DHCP scope configuration.

**Make sure that hotspot VLAN has an IP address properly configured over Access Point level, selecting "Configuration -> Access Points -> <Access Point Name>"**

Select the desired range (Start IP, End IP) to be provided to subscribers, as long as the DNS servers to be offered to DHCP users. A common usecase is to select VLAN IP address as service Default Gateway and DNS servers to be offered, in order to ensure the use of same DNS server address configured at WiNG Express WAN interface.



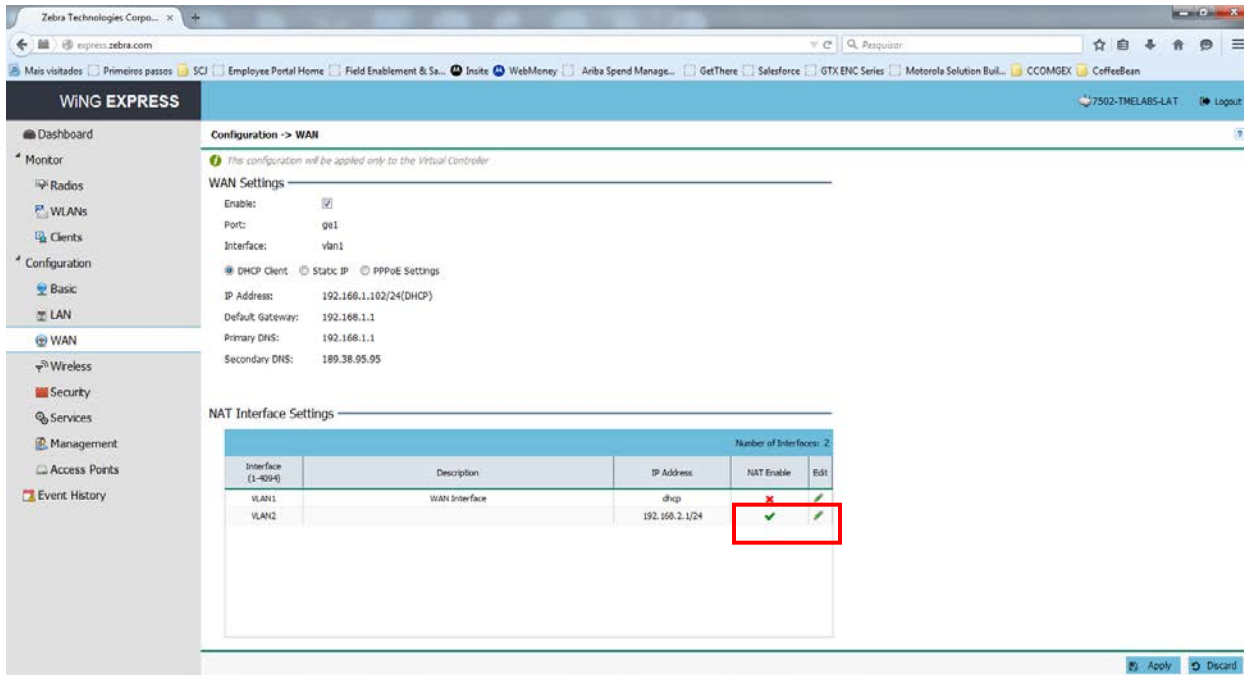
After making all required settings, please click at "Apply" button.

## 3.2 NAT CONFIGURATION

In order that hotspot service ensures the proper connectivity and to route subscribers to Internet, a NAT service shall be enabled once WAN interface is connected to a different LAN segment (DSL router, LAN router, PPPoE client, etc).

Once selected, WiNG Express OS will enforce NAT service to the selected VLAN.

In order to enable NAT service, go over the hotspot VLAN, click in “Edit” and select “NAT Enable” checkbox.



After making all required settings, please click at “Apply” button.

## 4. INTERNAL RADIUS SERVER (LOCAL AUTHENTICATION)

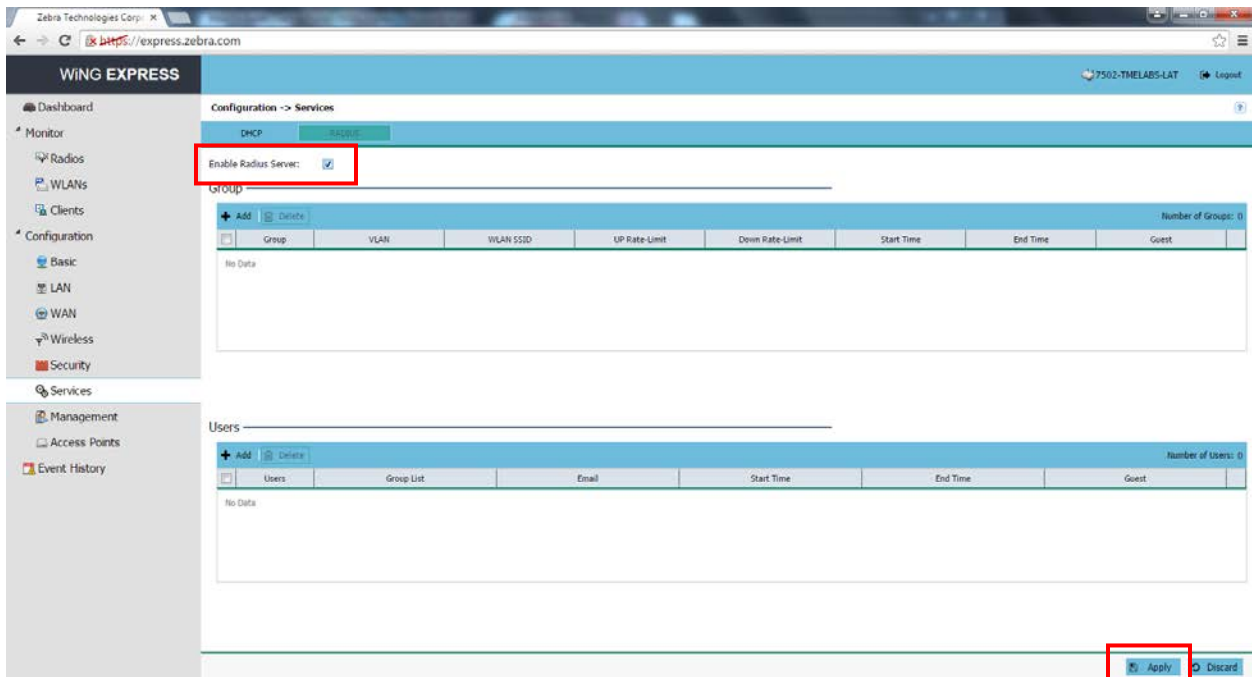
WiNG Express devices supports local RADIUS server to simplify a hotspot or Guest WLAN service to visitors. However, this service is not enabled by default.

If your Guest service does not require local authentication, please skip this step.

WiNG Express devices supports internal RADIUS configuration in two modes: site and system levels. A device configured in site level corresponds when the Access Point itself is configured to support RADIUS service; the hotspot subscribers are authenticated locally.

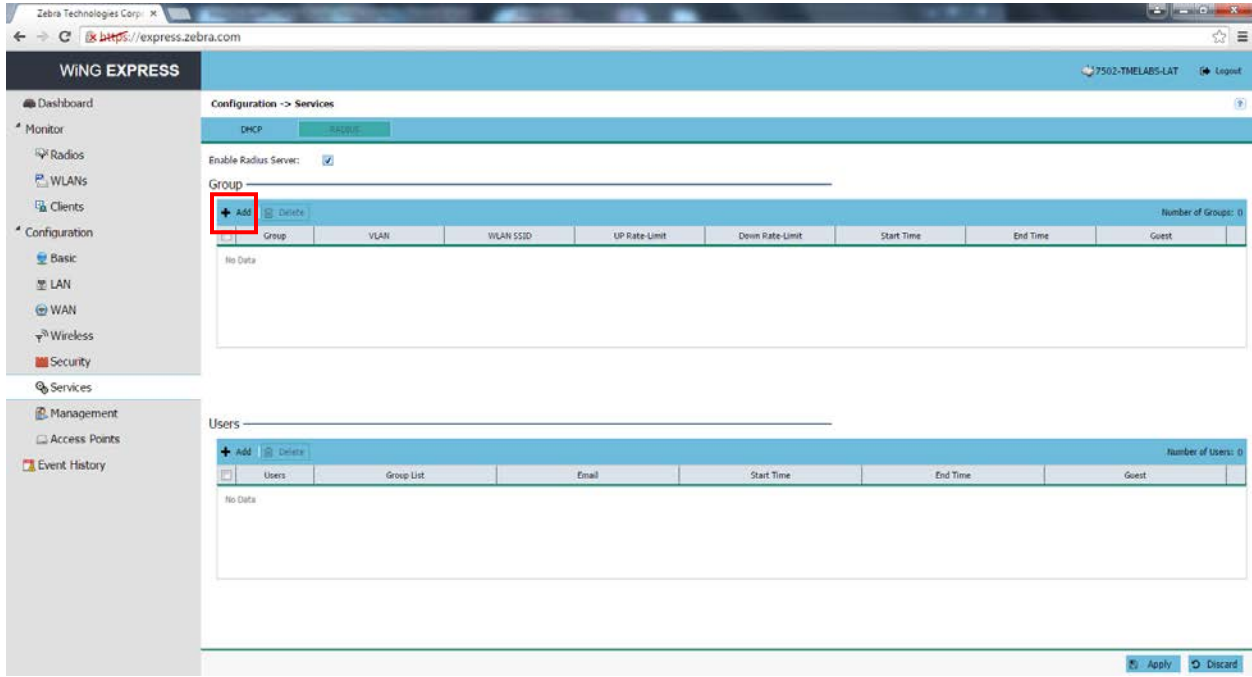
System level configuration corresponds when the Express Virtual Controller (VC) is responsible to provide RADIUS authentication to the subscribers connected to all Access Points managed by this VC.

To configure the RADIUS server, go to Configuration->Services at WiNG Express GUI. You may find two tabs over the main configuration screen: DHCP and RADIUS. Select RADIUS to proceed with the necessary configuration. Select “Enable RADIUS Server” and click into “Apply” button to proceed with service activation.



Once activated, a RADIUS server in WING Express device requires two separate configurations: RADIUS User Group and RADIUS subscribers. The User Group provides all global policies that shall be applied to certain group of users (e.g. Guests, Public Services, Users, etc), like rate-limit, pre-defined schedule or allowed period to permit those users to be authenticated. Additionally, service VLAN and your correspondent SSID are being configured into the RADIUS group.

To create a new group, please select “Add” button. You will be guided to the further configuration sub-menu.





RADIUS user group provides the following settings:

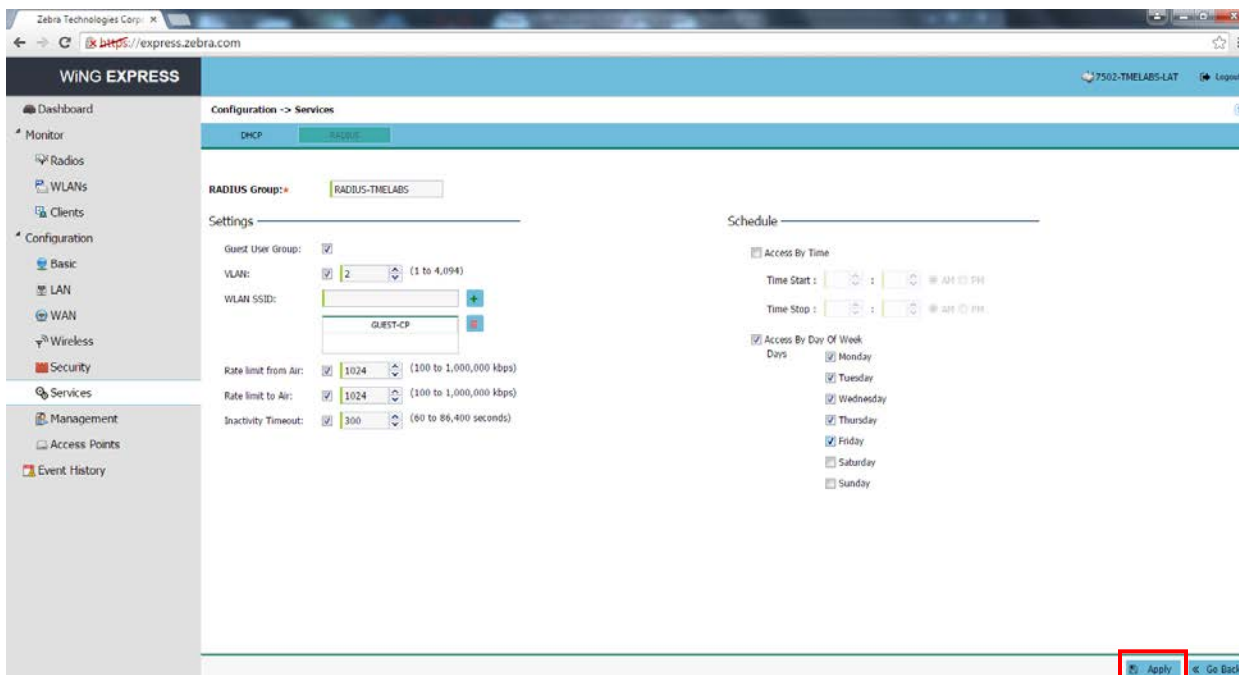
Option	Description
RADIUS Group	Group Name
Guest User Group	Enables RADIUS group for Guest Services
VLAN	Service VLAN
WLAN SSID	All Wireless SSIDs that supports this RADIUS group. To enable the correspondent WLAN, please type the SSID name and select the “+” signal. To remove a Guest WLAN in the list, just select the proper SSID name and click to the red trash can.
Rate limit from and to air	Bandwidth limitation (per user) for service shaping issues.
Inactivity timeout	Minimum timeout for authentication session. If user device is in standby mode, for example and exceeds the configured Inactivity timeout session, the subscriber shall have to get a new authentication session.

The minimum configuration below is mandatory to get RADIUS group configured:

- Group Name
- Guest User Group
- VLAN
- WLAN SSID

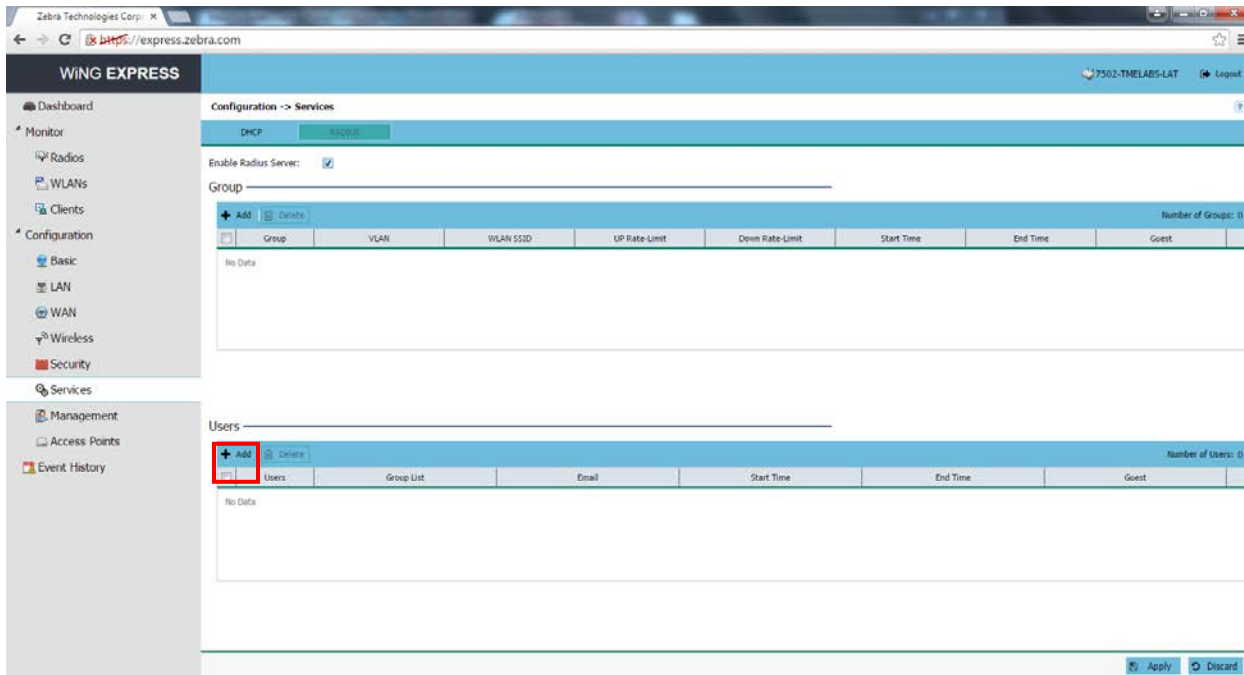
All other settings are optional and can be included or excluded after group configuration.

After making all required settings, please click at “Apply” button.



After configured the user group, the RADIUS users can be created to enable subscriber authentication.

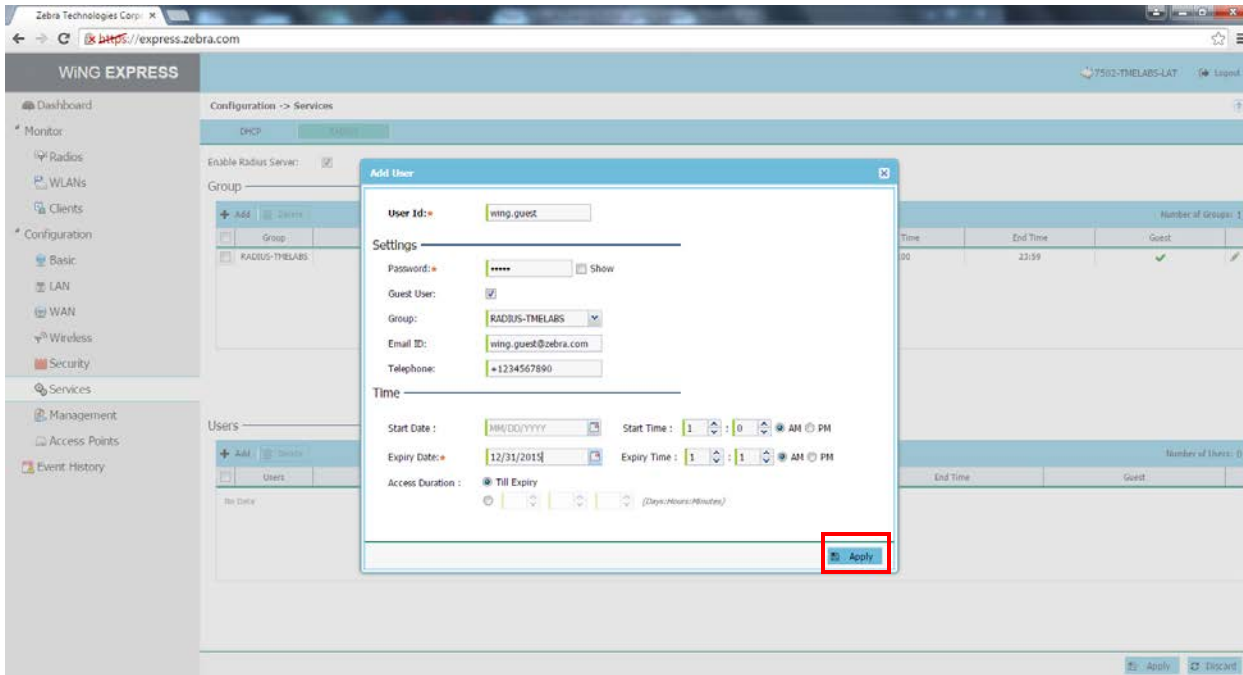
Click in “Add” to create a new user. Once clicked a pop-up menu will be displayed to enable adding all user settings.



To add the new user, all settings below shall be configured to enable subscriber authentication.

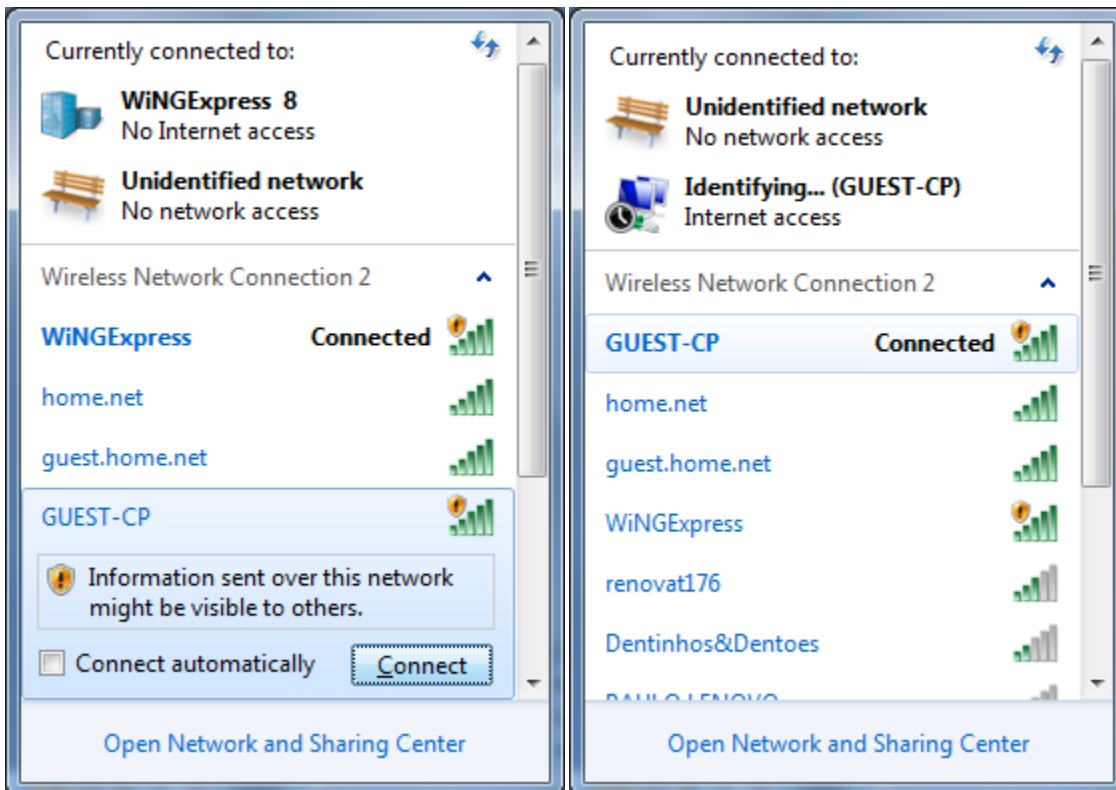
Option	Description
User Id	RADIUS username. This username shall be provided to WLAN subscriber.
Password	Guest service password. To show the configured password, click at “show” option. To get proper service authentication, subscriber has to type the configured password when required.
Guest User Group	Guest WLAN subscriber
	RADIUS User Group settings
Email ID and Telephone	User contact information
Service Time	Date and time which subscriber is allowed to access WLAN Guest service.

After making all required settings, please click at “Apply” button.

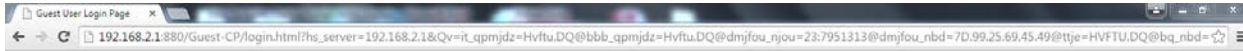


## 5. TESTING YOUR GUEST WLAN

To validate that Guest WLAN service is activated and working properly, select and connect to the configured WLAN Service, using a Guest device (PC, Mobile, Tablet)



Once connected, you will be redirected to the Captive Portal page configured for this Guest WLAN service. If RADIUS authentication (self, controller or external) is required, please use a previous configured subscriber username and password. Once authenticated, you will be redirected to the welcome page.



**Zebra Technologies**

Welcome to Guest User Wireless LAN Service

Please enter the username and password provided to you when you signed in at the front desk.

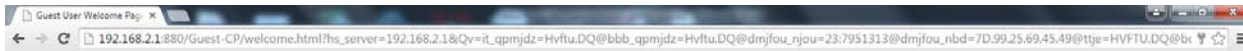
**Username**  
Enter Username

**Password**  
Enter Password

[Sign In](#) [Clear](#)

Please contact the front desk if you have not been issued a username and password.

Zebra Technologies. All Rights Reserved.



**Zebra Technologies**

Welcome. You are now connected to the Internet.

Status	Connected
Time Remaining	2 Days, 1 Hrs, 44 Mins

Click [Disconnect](#) to end this session.

Zebra Technologies. All Rights Reserved.