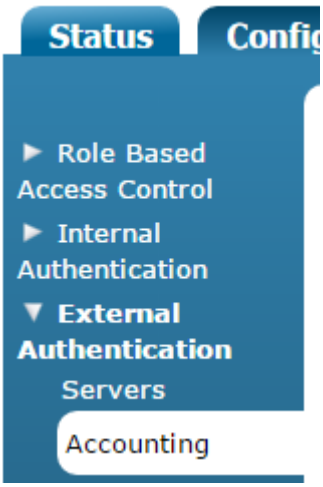
ADTRAN Bluesocket

Modified on: Wed, 29 Apr, 2015 at 8:18 AM

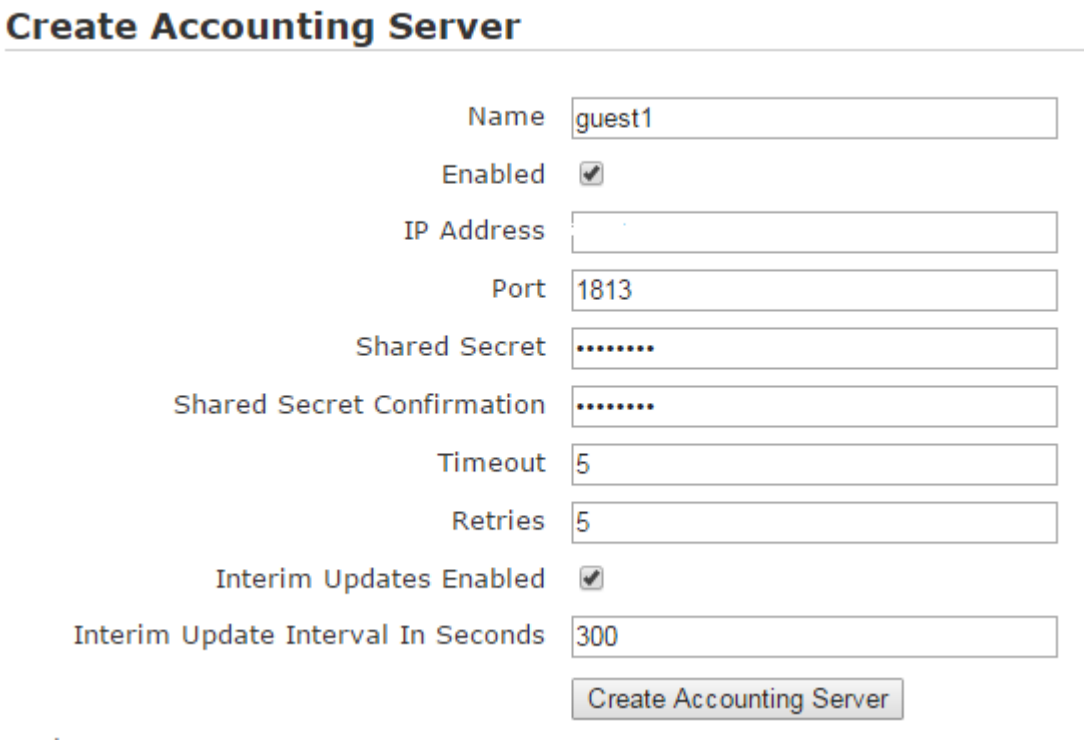
Please log in to your Bluesocket WLAN controller

At the top click on **Configuration** and then on the left, under **External Authentication** click on **Accounting**



Click on **Create Accounting Server** and enter the following:

- **Name**: guest1
- **Enabled**: Ticked
- **IP Address**: *insert radius_server_ip here*
- **Port**: 1813
- **Shared Secret**: *insert radius_secret here*
- **Shared Secret Confirmation**: as above
- **Timeout**: 5
- **Retries**: 5
- **Interim Updates Enabled**: Ticked
- **Interim Update Interval**: 300



Click **Create Accounting Server**

Click on **Create Accounting Server** again and enter the following:

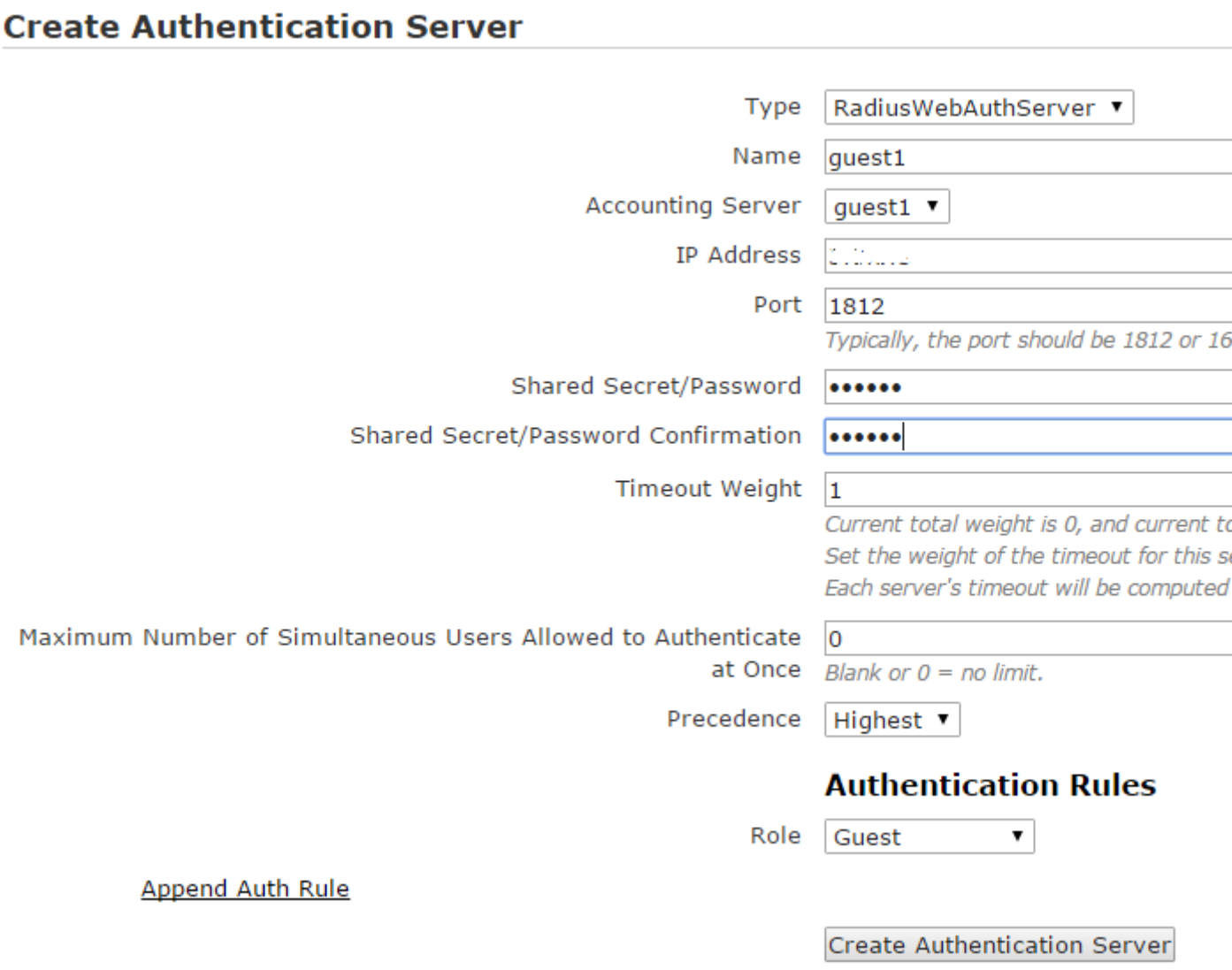
- **Name**: guest2
- **Enabled**: Ticked
- **IP Address**: *insert radius_server2_ip here*
- **Port**: 1813
- **Shared Secret**: *insert radius_secret here*
- **Shared Secret Confirmation**: as above
- **Timeout**: 5
- **Retries**: 5
- **Interim Updates Enabled**: Ticked
- **Interim Update Interval**: 300

Click **Create Accounting Server**

Next, on the left, under **External Authentication** click on **Servers**. Click on **Create Authentication Server** and enter the following:

- **Type**: RadiusWebAuthServer

- **Name**: guest1
- **Accounting Server**: guest1
- **IP Address**: *insert radius_server_ip here*
- **Port**: 1812
- **Shared Secret**: *insert radius_secret here*
- **Shared Secret Confirmation**: as above
- **Timeout Weight**: 1
- **Precedence**: Highest
- **Role**: Guest



Click on **Create Authentication Server**.

Click on **Create Authentication Server** again and enter the following:

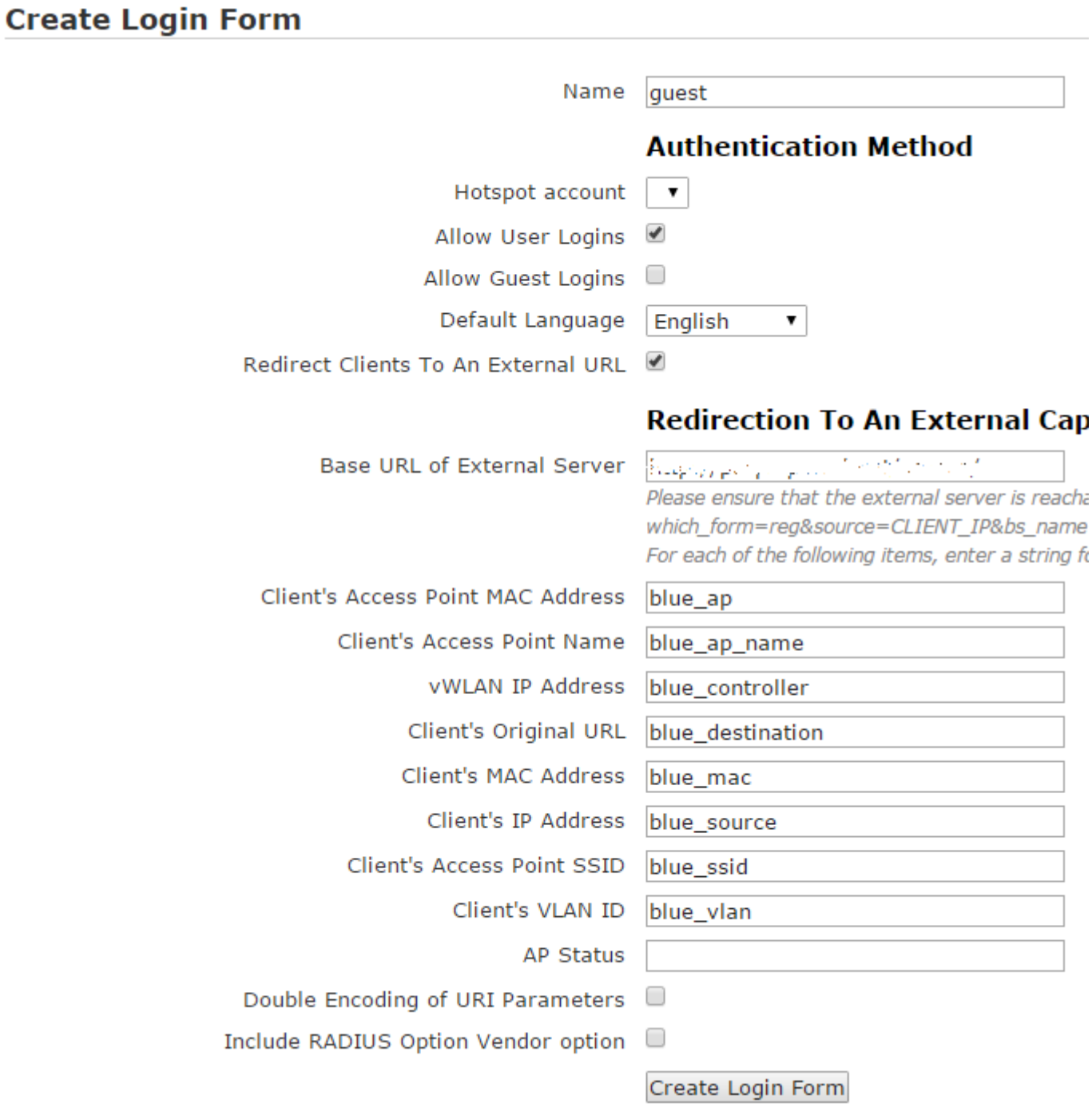
- **Type**: RadiusWebAuthServer

- **Name**: guest2
- **Accounting Server**: guest2
- **IP Address**: *insert radius_server2_ip here*
- **Port**: 1812
- **Shared Secret**: *insert radius_secret here*
- **Shared Secret Confirmation**: as above
- **Timeout Weight**: 1
- **Precedence**: Lowest
- **Role**: Guest

Click on **Create Authentication Server**.

Next, on the left under **Captive Portal**, click on **Forms**. Click **Create Login Form** and enter the following:

- **Name**: guest
- **Allow User Logins**: Ticked
- **Allow Guest Logins**: Unticked
- **Redirect Clients to an External URL**: Ticked
- **Base URL of External Server**: *insert access_url here*
- **Clients Access Point MAC Address**: blue_ap
- **Client's Access Point Name**: blue_ap_name
- **vWLAN IP Address**: blue_controller
- **Client's Original URL**: blue_destination
- **Client's MAC Address**: blue_mac
- **Client's IP Address**: blue_source
- **Client's Access Point SSID**: blue_ssid
- **Client's VLAN ID**: blue_vlan
- **Double Encoding of URI Parameters**: Unticked
- **Include RADIUS Option Vendor option**: Unticked



Click on **Create Login Form**.

Next, on the left, under **Role Based Access Control** click on **Destinations**. Click on **Create Destination Hostname** and enter:

- **Name**: guestportal
- **Address**: *insert access_domain here*

Click on **Create Destination**. Now, for each of the below entries, create another destination hostname until you have added each one:

- **Name**: google1
- **Address**: www.google.co.uk

- **Name**: google2
- **Address**: www.google.com

- **Name**: google3
- **Address**: google-analytics.com

- **Name**: venuewifi
- **Address**: *.venuewifi.com

- **Name**: owm
- **Address**: *.openweathermap.org

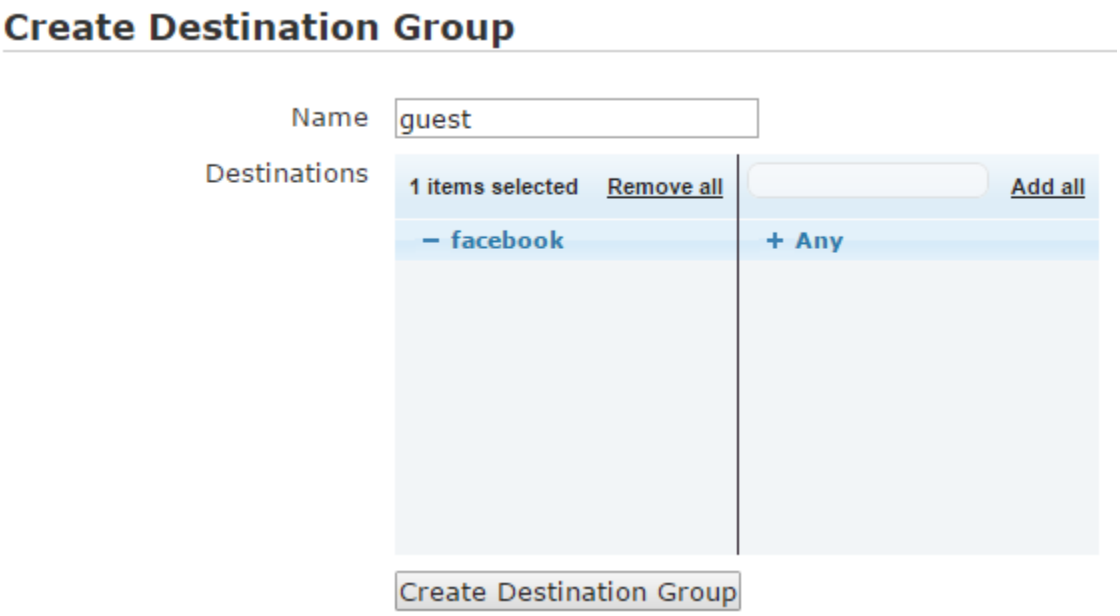
- **Name**: cloudfront
- **Address**: *.cloudfront.net

If you wish to support social network logins, you also need to add the destinations below for each network you plan to support, in the same way you did above. You can enter anything in the "Name" field.

Facebook	Twitter	LinkedIn	Google	Instagram
facebook.com		linkedin.com	*.googleusercontent.com	
*.facebook.com	twitter.com	*.linkedin.com	*.googleapis.com	instagram.com
*.fbcdn.net	*.twitter.com	*.licdn.net	accounts.google.com	*.instagram.com
*.akamaihd.net	*.twimg.com	*.licdn.com	*.gstatic.com	
connect.facebook.net				

Next, on the left, click on **Destination Groups**. Click on **Create Destination Group**.

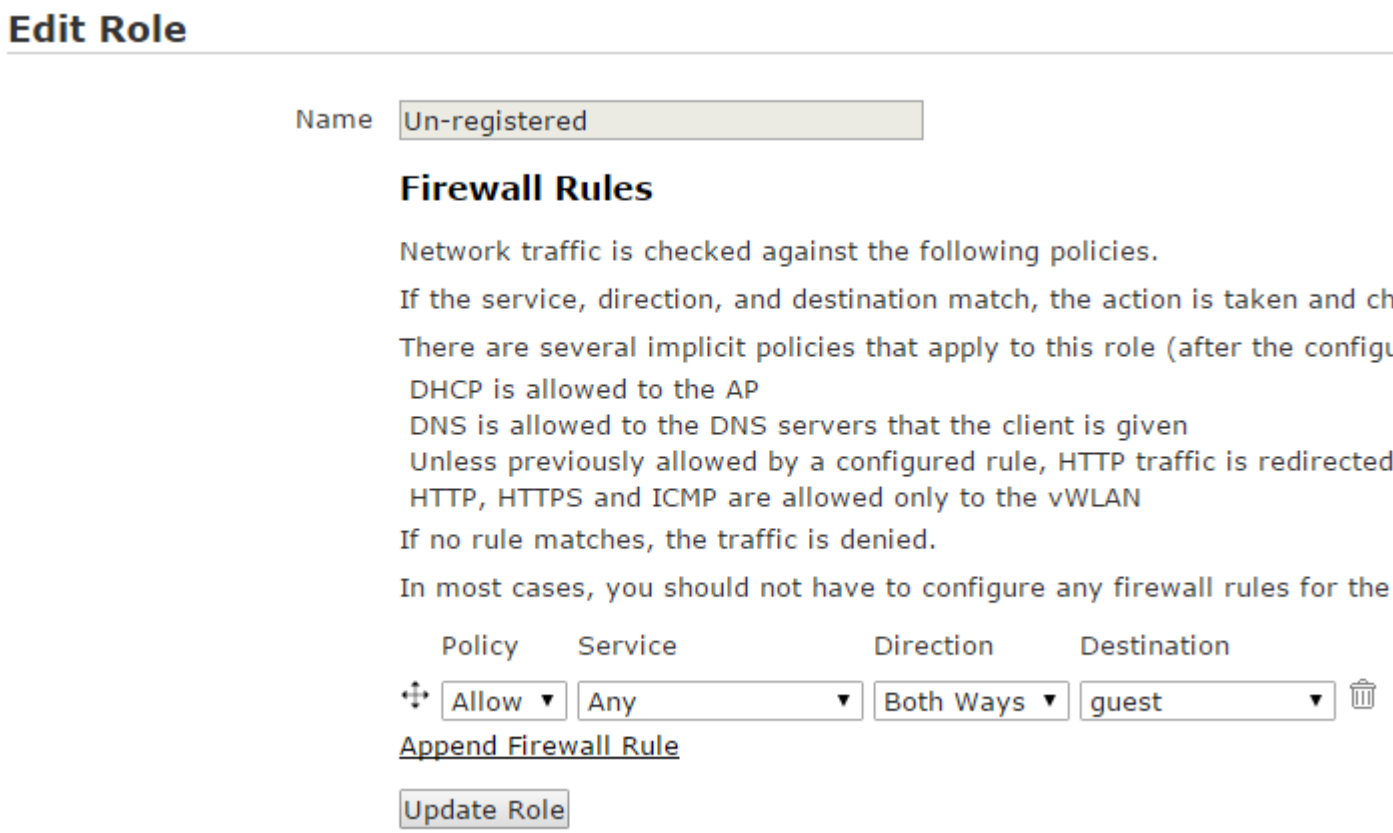
- **Name**: guest
- **Destinations**: Click the + sign beside each domain on the right hand list to add all of these to the left list. Be sure not to add the "Any" rule.



Click **Create Destination Group**

Next, on the left, click on **Roles**. Click on the **Un-registered** role. At the bottom, click on **Append Firewall Rule** and choose:

- **Policy**: Allow
- **Service**: Any
- **Direction**: Both Ways
- **Destination**: under "Destination Groups" choose **guest**



Click **Update Role**.

Next, on the left, click on **Roles**. Click on the **Guest** role. Under the **Post Login Redirection** section, enter:

URL Redirect: *insert redirect_url here*

Click **Update Role** to save.

Next, on the left, under **Wireless** click on **SSIDs**. Click on **Create SSID** and enter the following:

Name: Guest WiFi (or whatever you wish)

Broadcast SSID: Ticked

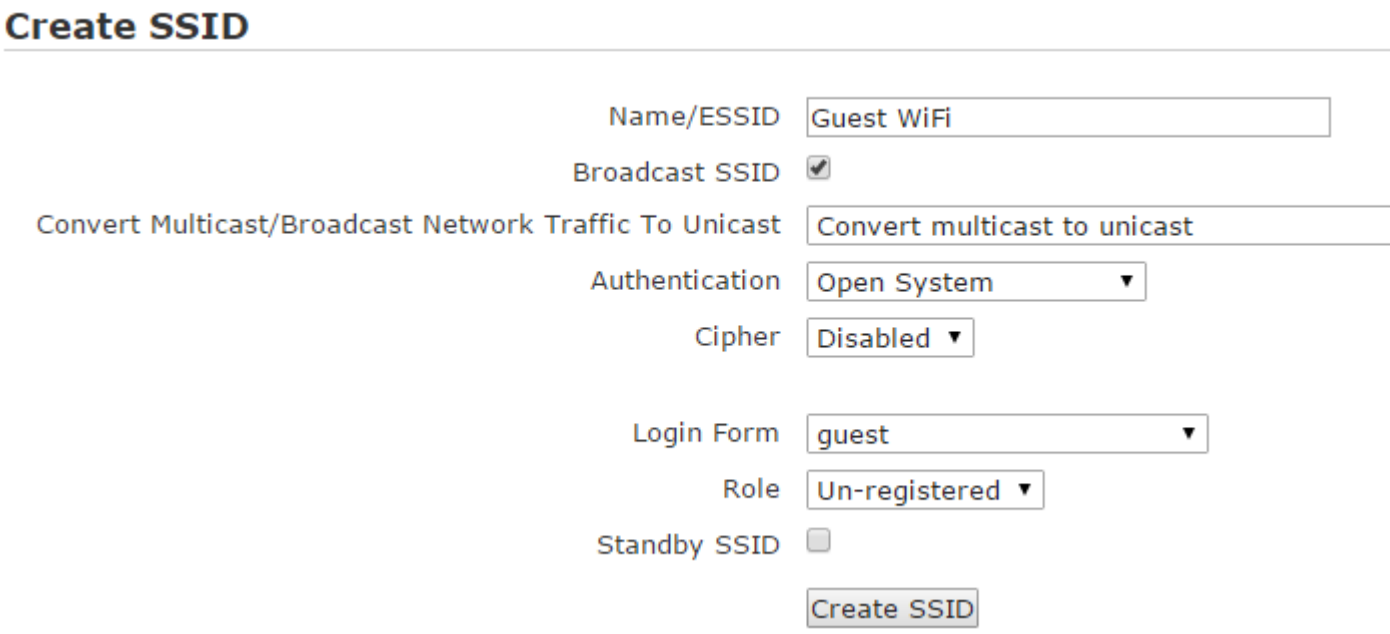
Authentication: Open System

Cipher: Disabled

Login Form: guest

Role: Un-registered

Standby SSID: Unticked



Click on **Create SSID**.

Finally, you need to apply this new configuration to your AP's in the usual way. For example, go to the **Status** tab at the top and choose **Access Points**. Highlight the ones you are using and click the **Apply** button.