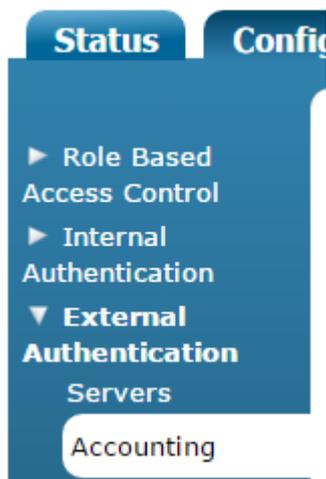


ADTRAN Bluesocket

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

Create Accounting Server

Name	<input type="text" value="guest1"/>
Enabled	<input checked="" type="checkbox"/>
IP Address	<input type="text"/>
Port	<input type="text" value="1813"/>
Shared Secret	<input type="text" value="....."/>
Shared Secret Confirmation	<input type="text" value="....."/>
Timeout	<input type="text" value="5"/>
Retries	<input type="text" value="5"/>
Interim Updates Enabled	<input checked="" type="checkbox"/>
Interim Update Interval In Seconds	<input type="text" value="300"/>
<input type="button" value="Create Accounting Server"/>	

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

Create Authentication Server

Type	RadiusWebAuthServer ▼
Name	guest1
Accounting Server	guest1 ▼
IP Address	0.0.0.0
Port	1812 <i>Typically, the port should be 1812 or 1642</i>
Shared Secret/Password	••••••
Shared Secret/Password Confirmation	••••••
Timeout Weight	1 <i>Current total weight is 0, and current total weight is 0. Set the weight of the timeout for this server. Each server's timeout will be computed based on the total weight.</i>
Maximum Number of Simultaneous Users Allowed to Authenticate at Once	0 <i>Blank or 0 = no limit.</i>
Precedence	Highest ▼
Authentication Rules	
Role	Guest ▼
Append Auth Rule	
<input type="button" value="Create Authentication Server"/>	

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

Create Login Form

Name	<input type="text" value="guest"/>
Authentication Method	
Hotspot account	<input type="text" value="▼"/>
Allow User Logins	<input checked="" type="checkbox"/>
Allow Guest Logins	<input type="checkbox"/>
Default Language	<input type="text" value="English"/>
Redirect Clients To An External URL	<input checked="" type="checkbox"/>
Redirection To An External Cap	
Base URL of External Server	<input type="text" value="http://www.example.com/"/>
<i>Please ensure that the external server is reachable and that the URL is correct. The URL should be in the format: http://www.example.com/which_form=reg&source=CLIENT_IP&bs_name=CLIENT_IP</i>	
Client's Access Point MAC Address	<input type="text" value="blue_ap"/>
Client's Access Point Name	<input type="text" value="blue_ap_name"/>
vWLAN IP Address	<input type="text" value="blue_controller"/>
Client's Original URL	<input type="text" value="blue_destination"/>
Client's MAC Address	<input type="text" value="blue_mac"/>
Client's IP Address	<input type="text" value="blue_source"/>
Client's Access Point SSID	<input type="text" value="blue_ssid"/>
Client's VLAN ID	<input type="text" value="blue_vlan"/>
AP Status	<input type="text"/>
Double Encoding of URI Parameters	<input type="checkbox"/>
Include RADIUS Option Vendor option	<input type="checkbox"/>
<input type="button" value="Create Login Form"/>	

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.

Create Destination Group

Name

Destinations

1 items selected Remove all <input type="text" value=""/>		Add all
- facebook		+ Any

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**

Edit Role

Name

Firewall Rules

Network traffic is checked against the following policies.

If the service, direction, and destination match, the action is taken and checked.

There are several implicit policies that apply to this role (after the configuration is complete):

DHCP is allowed to the AP

DNS is allowed to the DNS servers that the client is given

Unless previously allowed by a configured rule, HTTP traffic is redirected to the vWLAN

HTTP, HTTPS and ICMP are allowed only to the vWLAN

If no rule matches, the traffic is denied.

In most cases, you should not have to configure any firewall rules for the role.

Policy	Service	Direction	Destination	
 <input type="text" value="Allow"/>	<input type="text" value="Any"/>	<input type="text" value="Both Ways"/>	<input type="text" value="guest"/>	

[Append Firewall Rule](#)

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

Create SSID

Name/ESSID	<input type="text" value="Guest WiFi"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Convert Multicast/Broadcast Network Traffic To Unicast	<input type="text" value="Convert multicast to unicast"/>
Authentication	<input type="text" value="Open System"/>
Cipher	<input type="text" value="Disabled"/>
Login Form	<input type="text" value="guest"/>
Role	<input type="text" value="Un-registered"/>
Standby SSID	<input type="checkbox"/>
	<input type="button" value="Create SSID"/>

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.