# Extreme (Enterasys) IdentiFi

Modified on: Tue, 18 Nov, 2014 at 8:33 AM

---

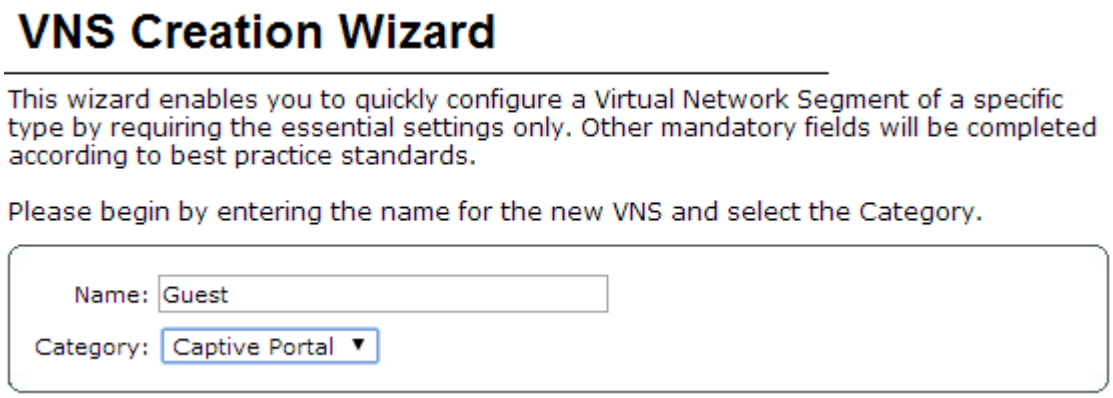
**IMPORTANT NOTICE**: Your controller must be running 09.15 software or above for the integration to work correctly.

Open a web browser and log in to your Extreme IdentiFi controller.


Click on "**VNS**" on the top menu and then "**New...**" "**START VNS WIZARD**" on the left menu and follow the instructions below:

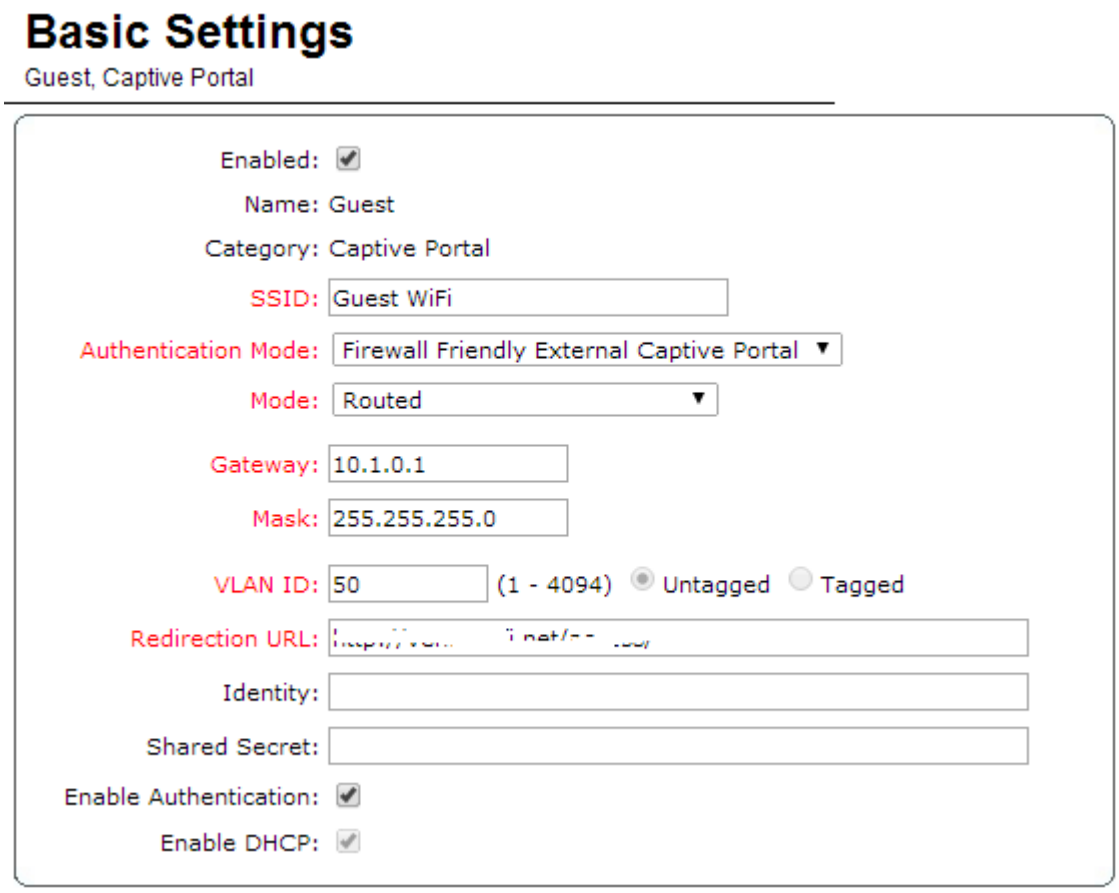
**Name**: Guest

**Category**: Captive Portal



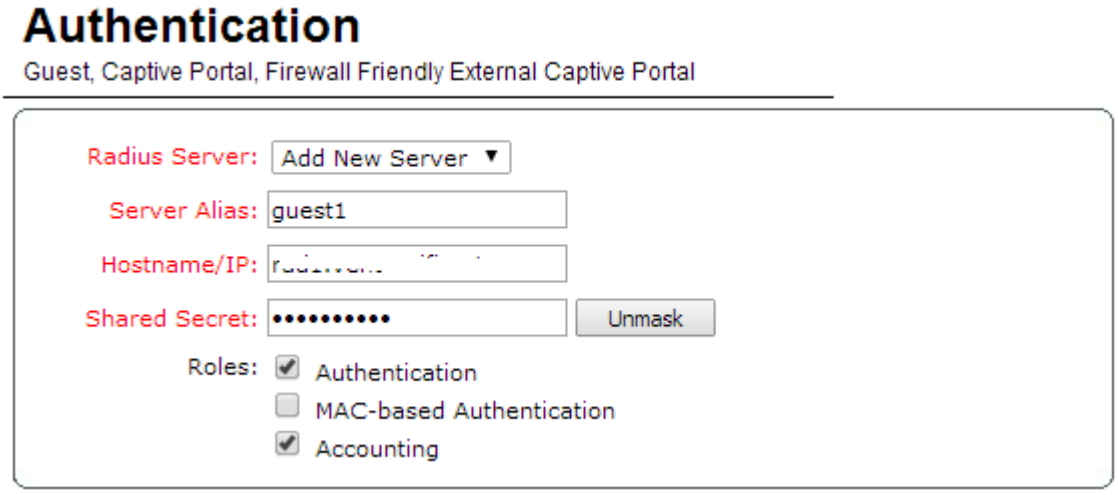

Click **Next** to continue

- **Enabled**: Ticked
- **SSID**: Guest WiFi (or whatever you like)
- **Authentication Mode**: Firewall Friendly External Captive Portal
- **Mode**: Routed
- **Gateway**: 10.1.0.1
- **Mask**: 255.255.255.0
- **VLAN ID**: 50 (choose another if you already use VLAN 50) and ensure Untagged is ticked
- **Redirection URL**: *insert access_url here*
- **Enable Authentication**: Ticked
- **Enable DHCP**: Ticked



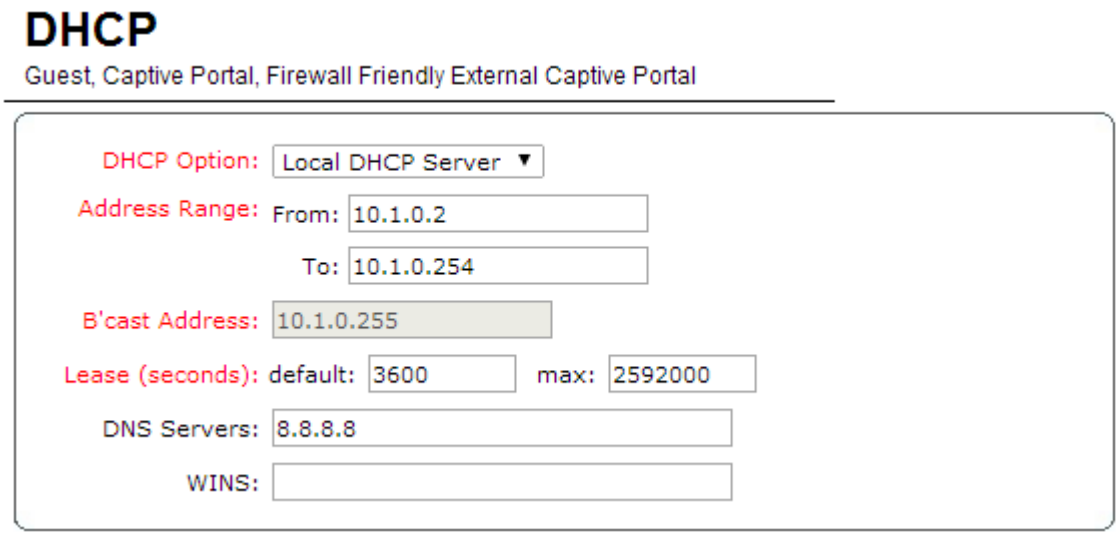

Click **Next** to continue

- **Radius Server**: Add New Server
- **Server Alias**: guest1
- **Hostname/IP**: *insert radius_server here*
- **Shared Secret**: *insert radius_secret here*
- **Roles**: Tick both Authentication and Accounting



Click **Next** to continue

- **DHCP Option**: Local DHCP Server
- **Address Range**: 10.1.0.2 - 10.1.0.254
- **Lease**: default = 3600, max = 2592000
- **DNS Servers**: 8.8.8.8




Click **Next** to continue

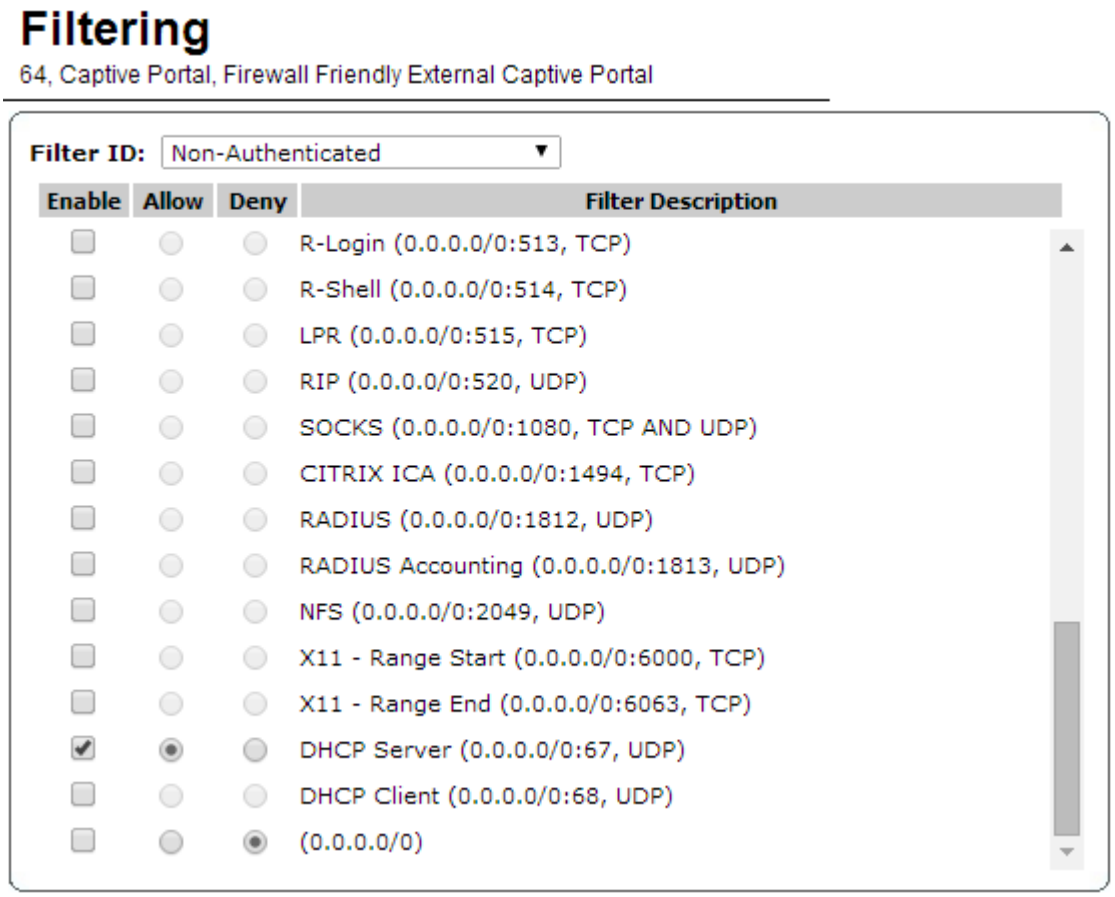
From the Filter ID drop down list, select **Non-Authenticated**.

Tick the **Enable** and then **Allow** box for each of the following:

- DNS (0.0.0.0/0:53, UDP)
- DHCP Server (0.0.0.0/0:67, UDP)

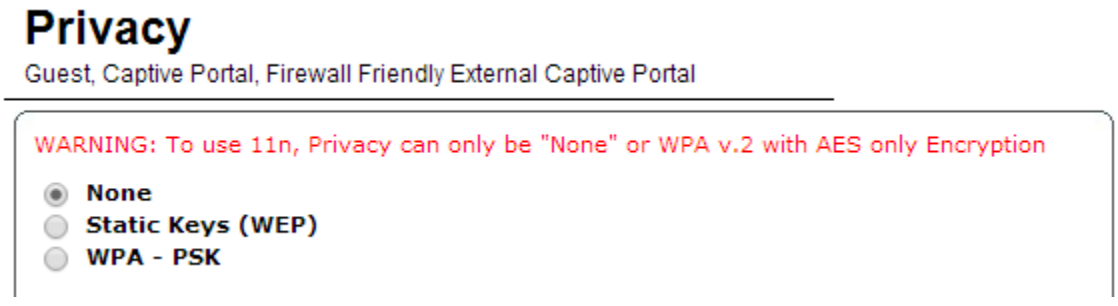
And tick the **Enable** and then **Deny** box for:

- (0.0.0.0/0)



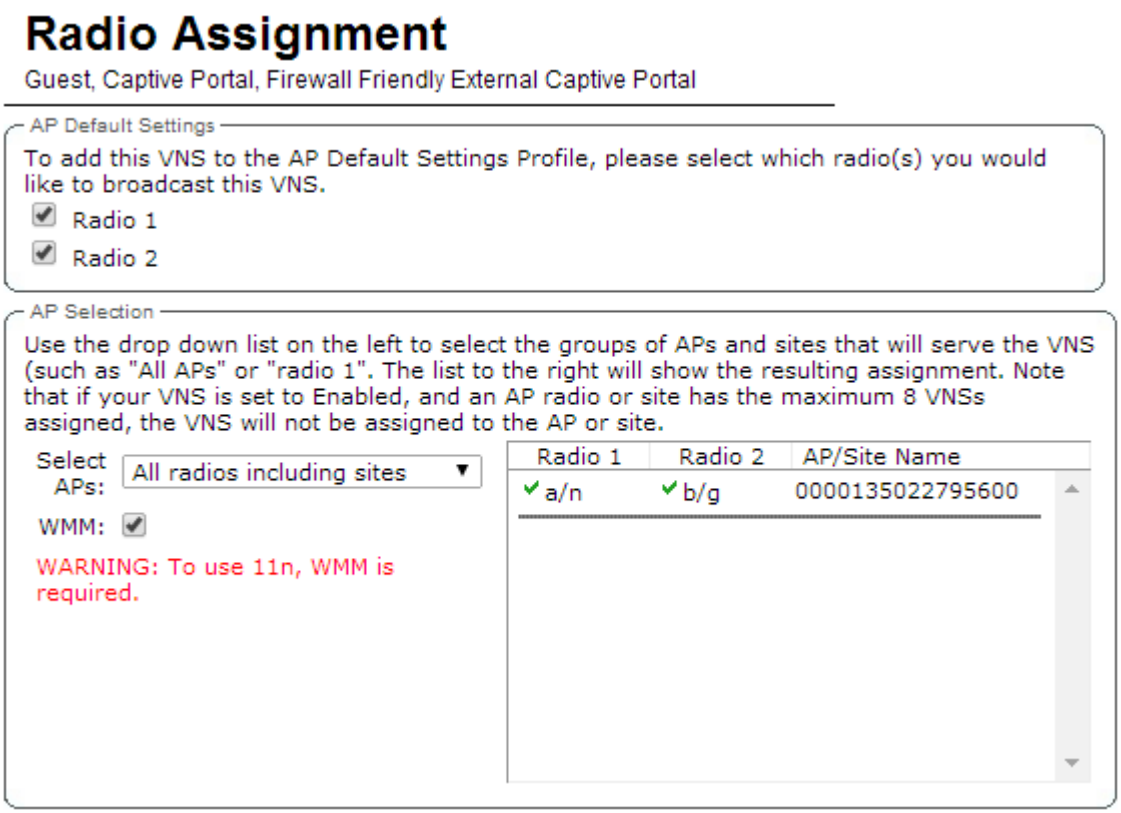

Click **Next** to continue

Set the **Privacy** to **None**

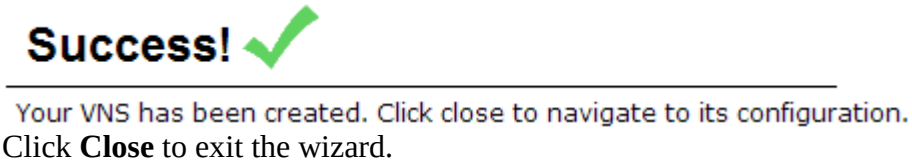



Click **Next** to continue

- **Select APs**: Select All radios including sites (unless you want to apply the guest access to a particular AP/site, in which case select what you need).

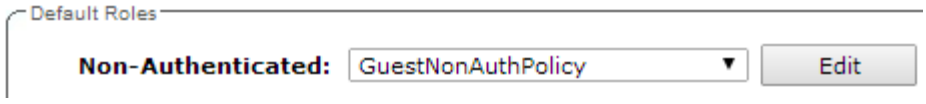



Click **Next** to continue and then **Finish** to confirm.



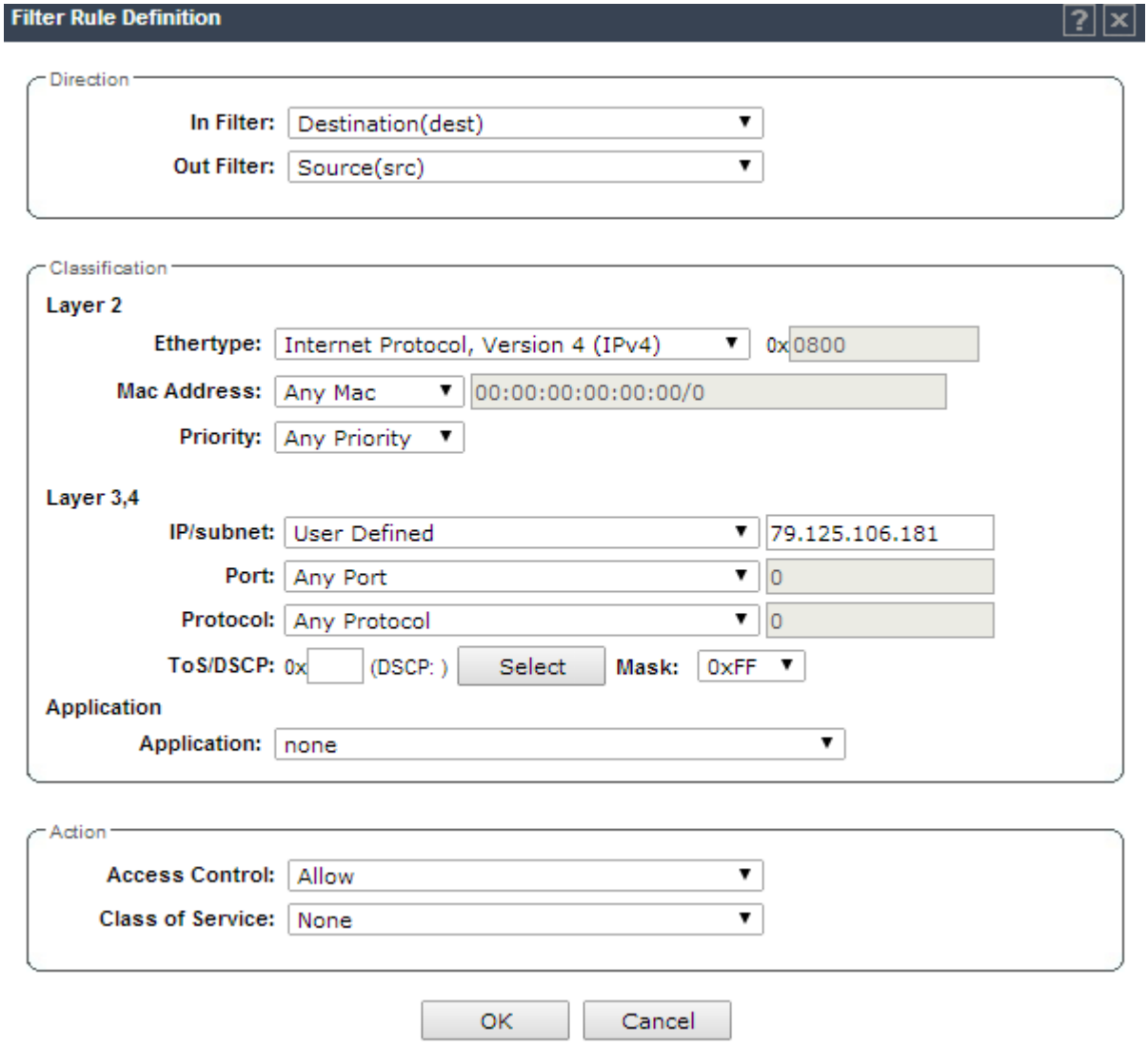

Click **Close** to exit the wizard.

Now, on the page you are returned to, under **Default Roles**, click the **Edit** button beside **GuestNonAuthPolicy**




Click on the **Policy Rules** tab and then click **Add** at the bottom. Leave all the boxes at their defaults but set the following:

- **Layer 3,4 IP/subnet**: User Defined = *insert walled_garden_ip here*
- **Access Control**: Allow




Click **OK** to Save and then click on **Add** again to add another Rule. This time, set the following:

- **Layer 3,4 IP/subnet**: User Defined = *insert walled_garden2_ip here*
- **Access Control**: Allow

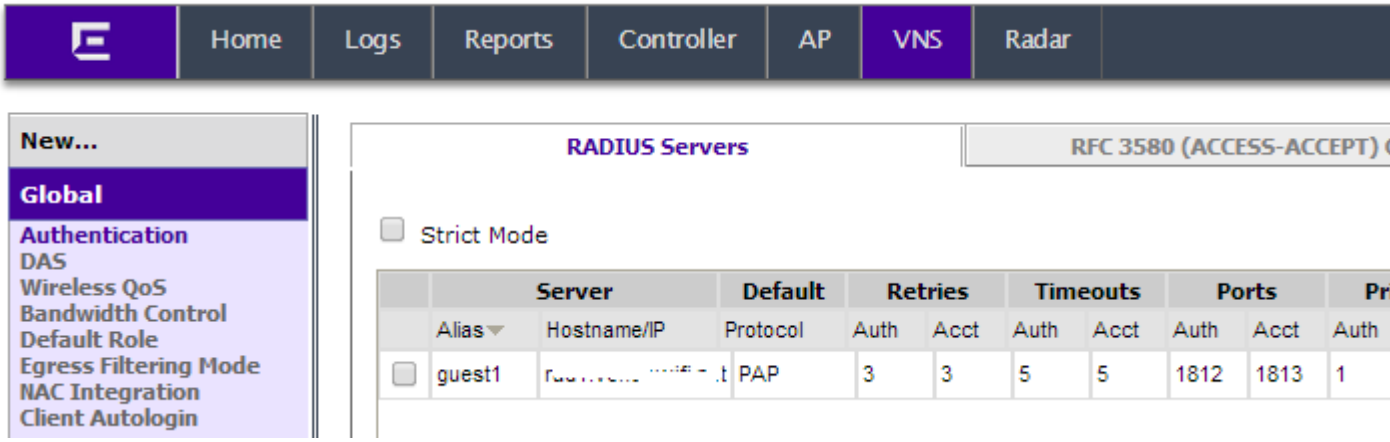
Click **OK** to Save and then click on **Add** again to add another Rule. This time, set the following:

- **Layer 2 Ethertype**: Address Resolution Protocol (ARP)
- **Access Control**: Allow

Click **OK** to Save

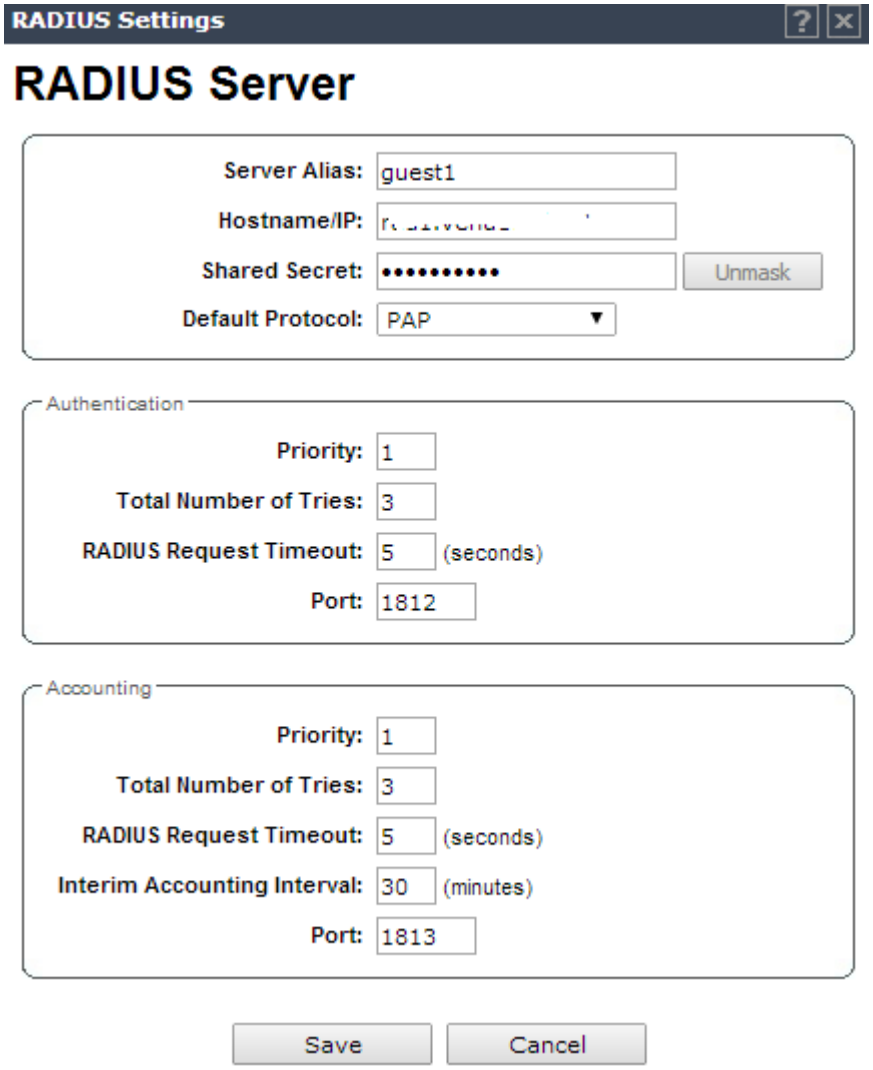
Important: You need to select each the bottom three entries you just added and click the **Top** button to move them to the top of the list.

Next, under **Global** on the left, choose **Authentication**.



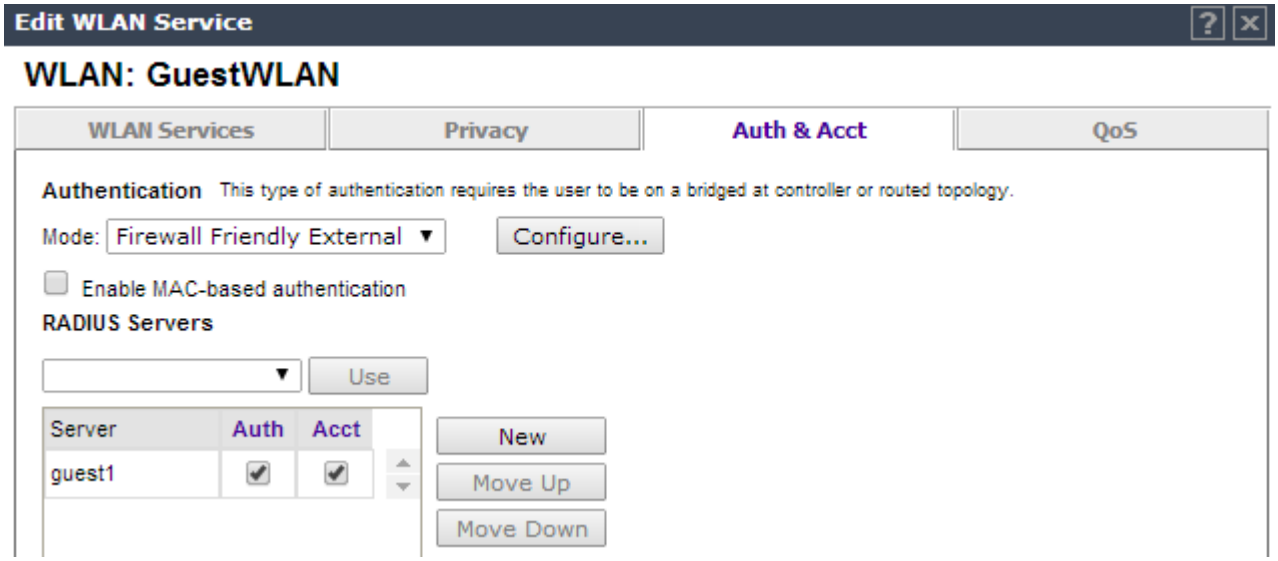

Click on **guest1** and change the following:

- **Default Protocol**: PAP



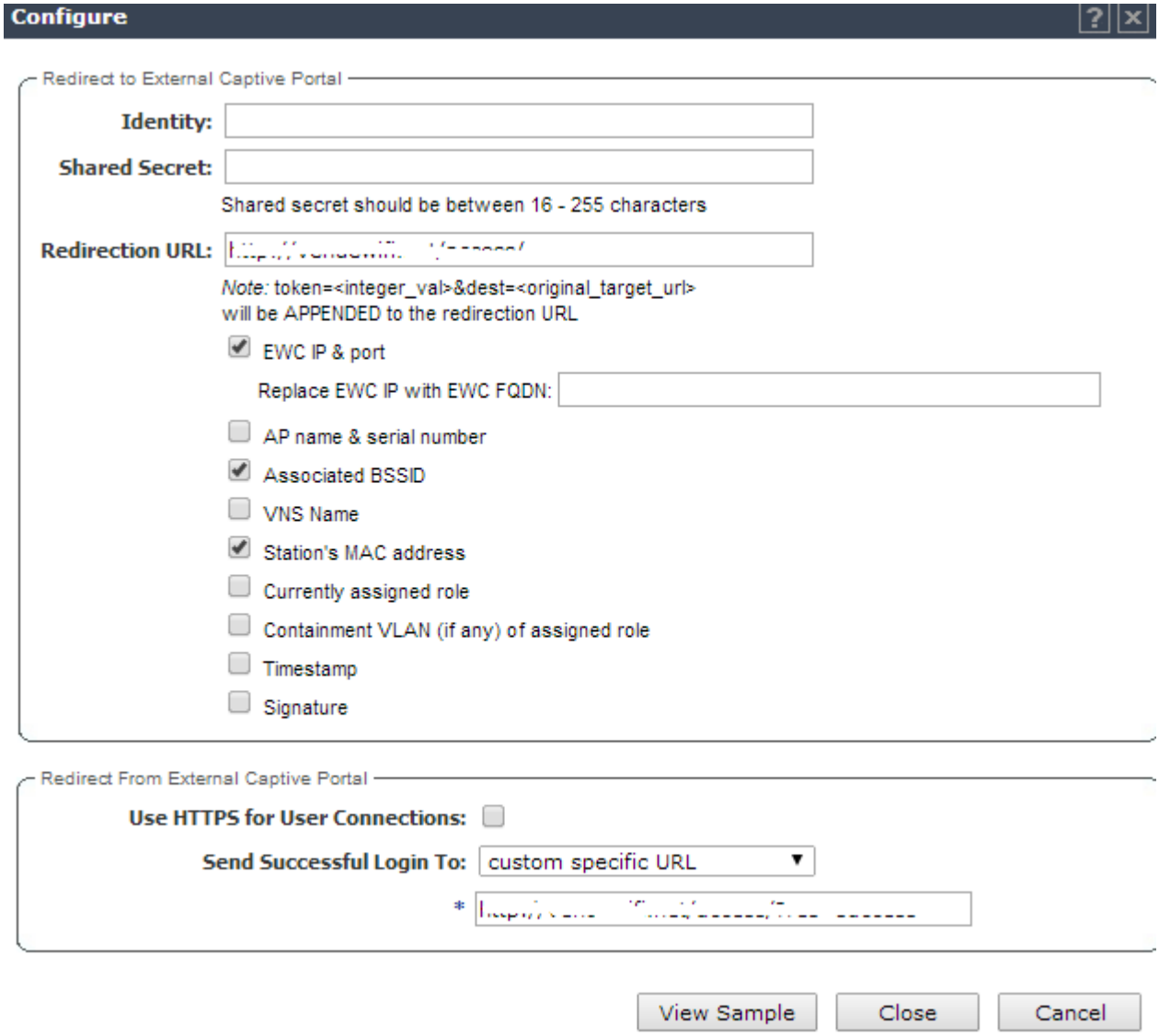

Click on **Save** to continue

Next, click on **WLAN Services** on the left and then click on **GuestWLAN**




Under the **Auth & Acct** tab click on **Configure...** and then set the following:

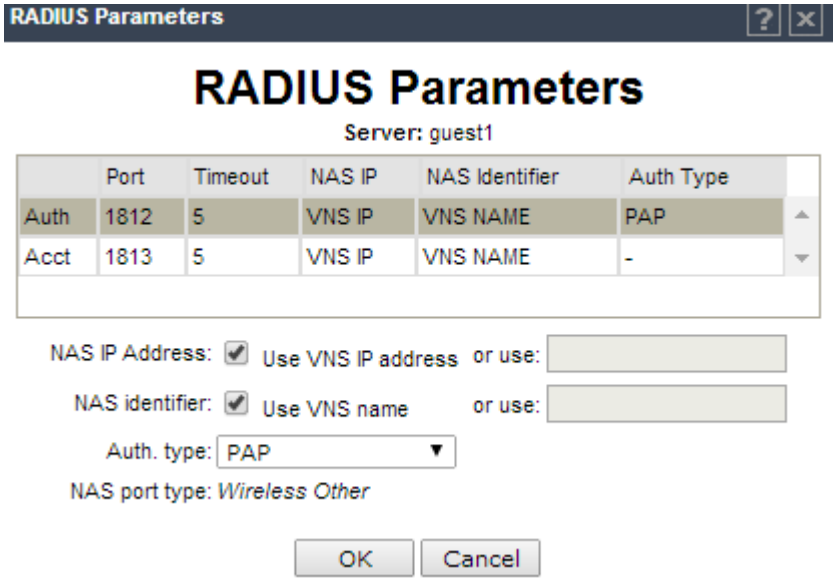
- **EWC IP & Port**: Ticked
- **Associated BSSID**: Ticked
- **Station's MAC address**: Ticked
- **Use HTTPS for User Connections**: Unticked
- **Send Successful Login To:** custom specific URL: *insert redirect_url here*




Click on **Close** to save

Next, click on the **guest1** under Server and choose the **Configure** button just to the right. Set the following:

- **Auth type: PAP**

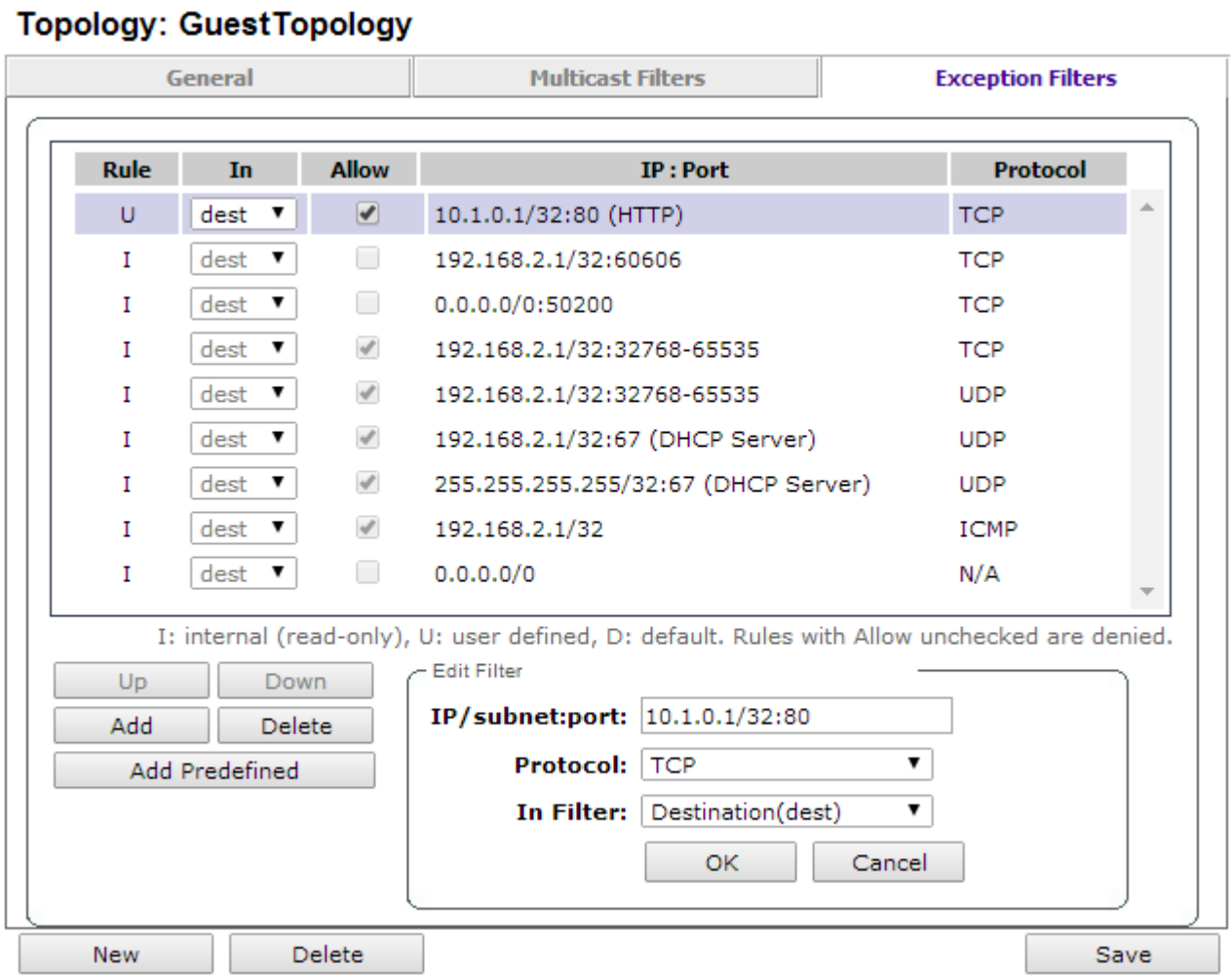



Click on **OK** to save

Finally, click on **Network** on the left and then **Topologies**. Click on the **GuestTopology** entry and then choose the **Exception Filters** tab.

Click on the **Add** button. Enter the following:

- **IP/subnet:port**: 10.1.0.1/32:80
- **Protocol** TCP
- **In Filter**: Destination (dest)




Click **OK** to save.