Alcatel-Lucent Instant (IAP)

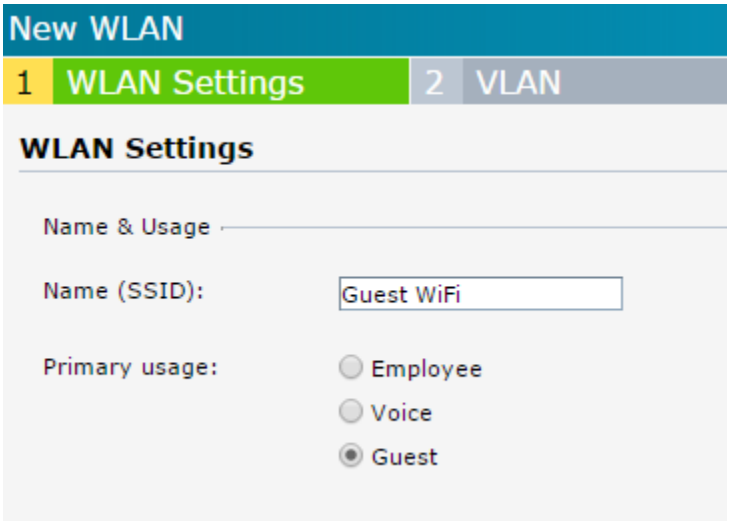
Modified on: Thu, 7 May, 2015 at 7:58 PM

Log in to your Alcatel-Lucent (Master) IAP

Under **Network** at the top left, click on **New**

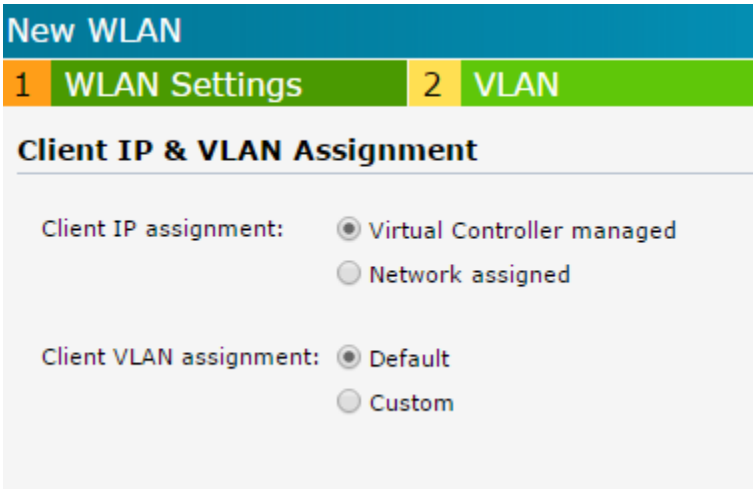
Configure with:

- **Name (SSID)**: Guest WiFi (or whatever you wish)
- **Primary usage**: Guest



Click **Next** and configure with:

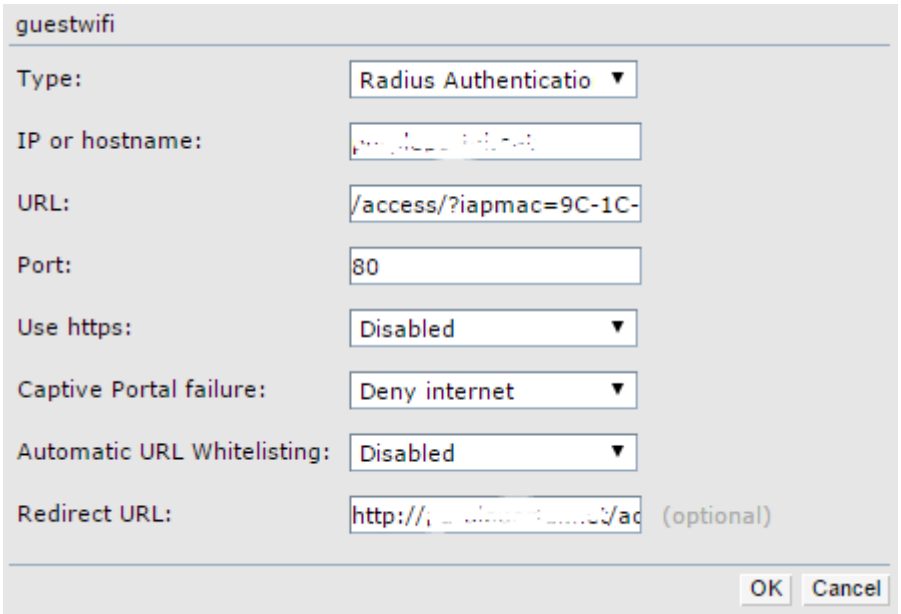
- **Client IP assignment**: Virtual Controller managed
- **Client VLAN assignment**: Default (unless you have a custom VLAN set up)



Click **Next** and configure with:

- **Splash page type**: External
- **Captive portal profile**: Click the dropdown and choose **New**. Configure with:

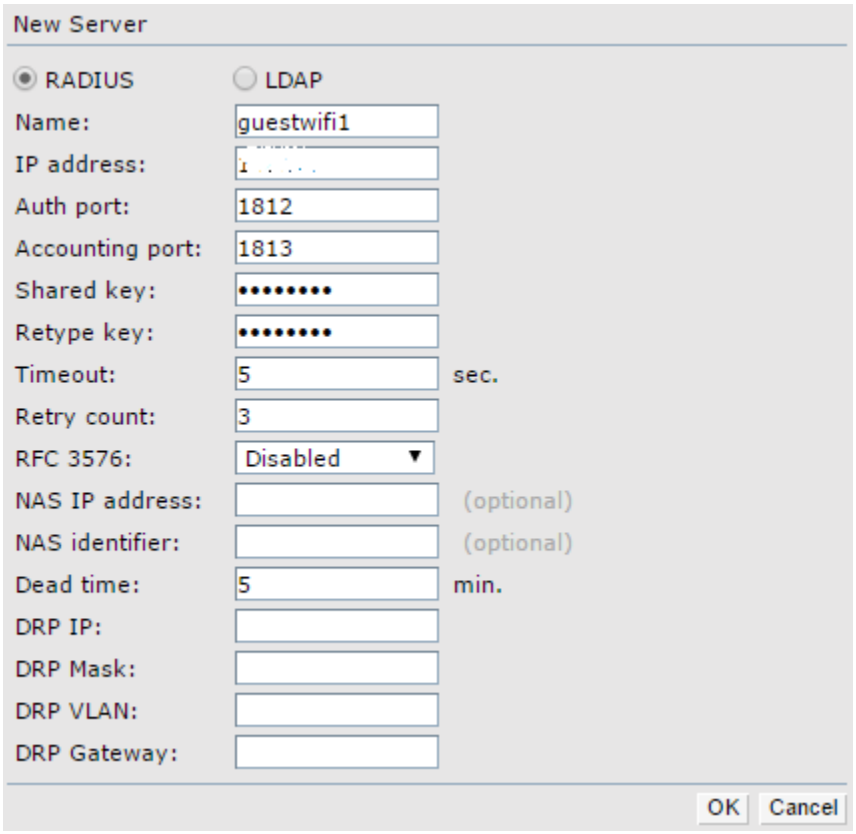
  - **Name**: guestwifi
  - **Type**: Radius Authentication
  - **IP or hostname**: *insert access_domain here*
  - **URL**: /access/?iapmac=<ap-mac> (i.e. /access/?iapmac=00-0B-86-6E-C5-F8)
  - **Port**: 80
  - **Use https**: Disabled
  - **Captive portal failure**: Deny internet
  - **Automatic URL whitelisting**: Disabled
  - **Redirect URL**: *insert redirect_url here*



Click **OK** to save

- **Auth server 1**: Click the dropdown and choose **New**. Configure with:

    - **Type:** RADIUS
    - **Name**: guestwifi1
    - **IP address**: *insert radius_server_ip here*
    - **Auth port**: 1812
    - **Acct port**: 1813
    - **Shared key**: *insert radius_secret here*
    - **Retype key**: as above



Click **OK** to save

- **Auth server 2**: Click the dropdown and choose **New**. Configure with

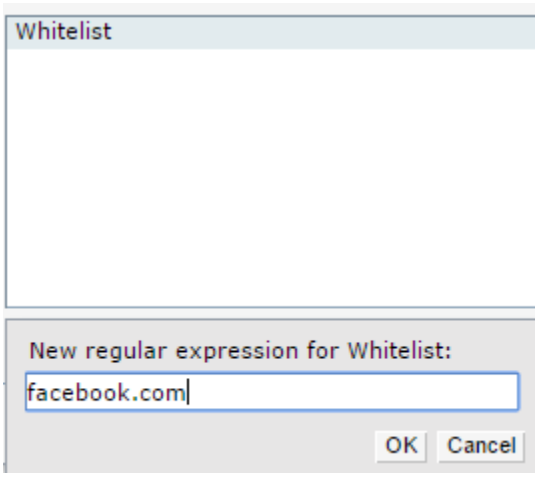
    - **Type:** RADIUS

    - **Name**: guestwifi2
    - **IP address**: *insert radius_server2_ip here*
    - **Auth port**: 1812
    - **Acct port**: 1813

- **Shared key**: *insert radius_secret here*
- **Retype key**: as above

Click **OK** to save

- **Reauth interval**: 24 hrs
- **Accounting**: Enabled
- **Accounting mode**: Authentication
- **Accounting interval**: 3 min
- **Blacklisting**: Disabled
- **Walled garden**: Click the link "Blacklist: 0 Whitelist: 0" and you will see the below screen:



Under **Whitelist** Click **New** and add all the below domains one by one until all are in the list:

insert access_domain here

www.google.com
www.google.co.uk

google-analytics.com

venuewifi.com

openweathermap.org

cloudfront.net

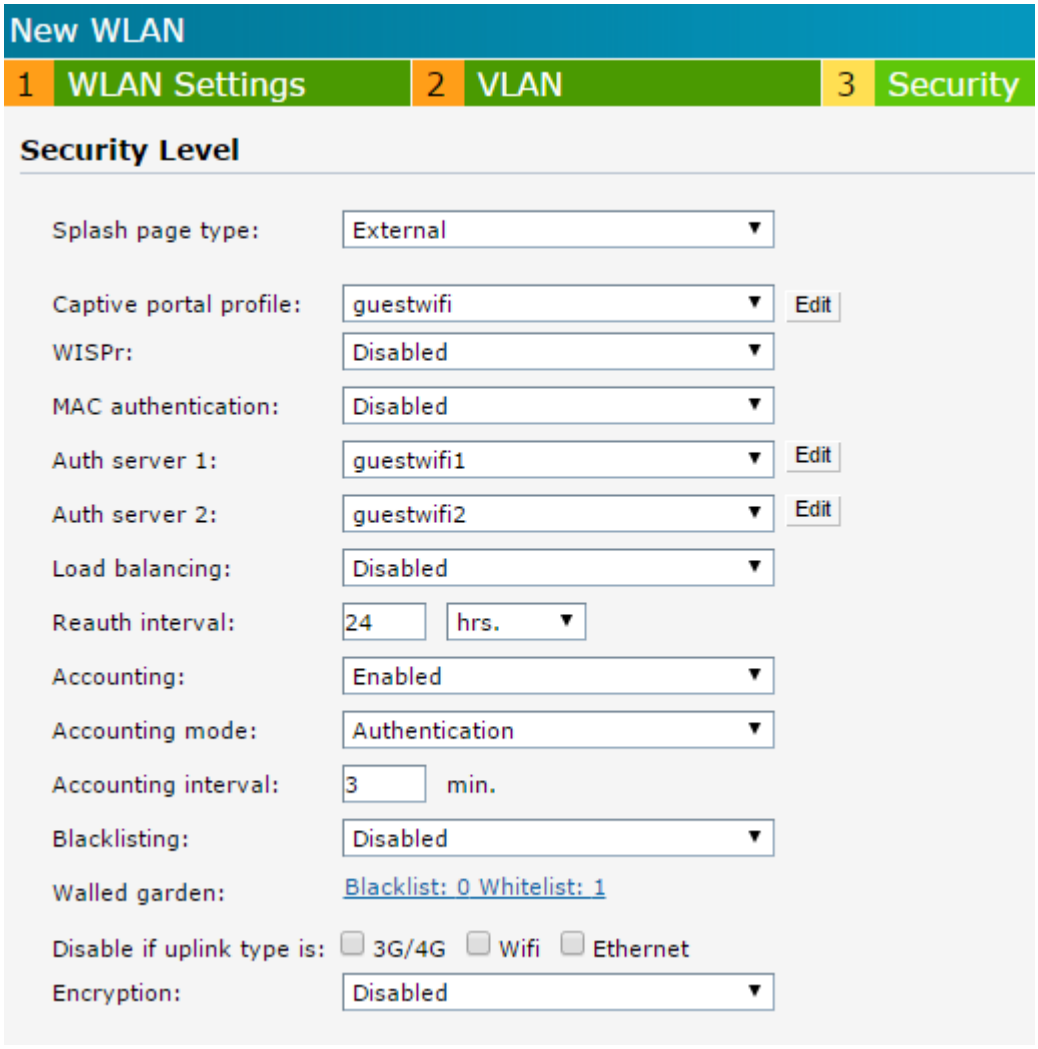
If you wish to support social network logins, you also need to add the domains below for each network you plan to support

Facebook	Twitter	LinkedIn	Google	Instagram
facebook.com	twitter.com	linkedin.com	googleusercontent.com	instagram.com

fbcdn.net akamaihd.net connect.facebook.net	twimg.com	licdn.net licdn.com	googleapis.com accounts.google.com gstatic.com	

Press **OK** when all the domains have been added to save

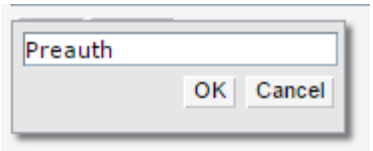
Your settings should now appear like so:



Click **Next** and configure with:

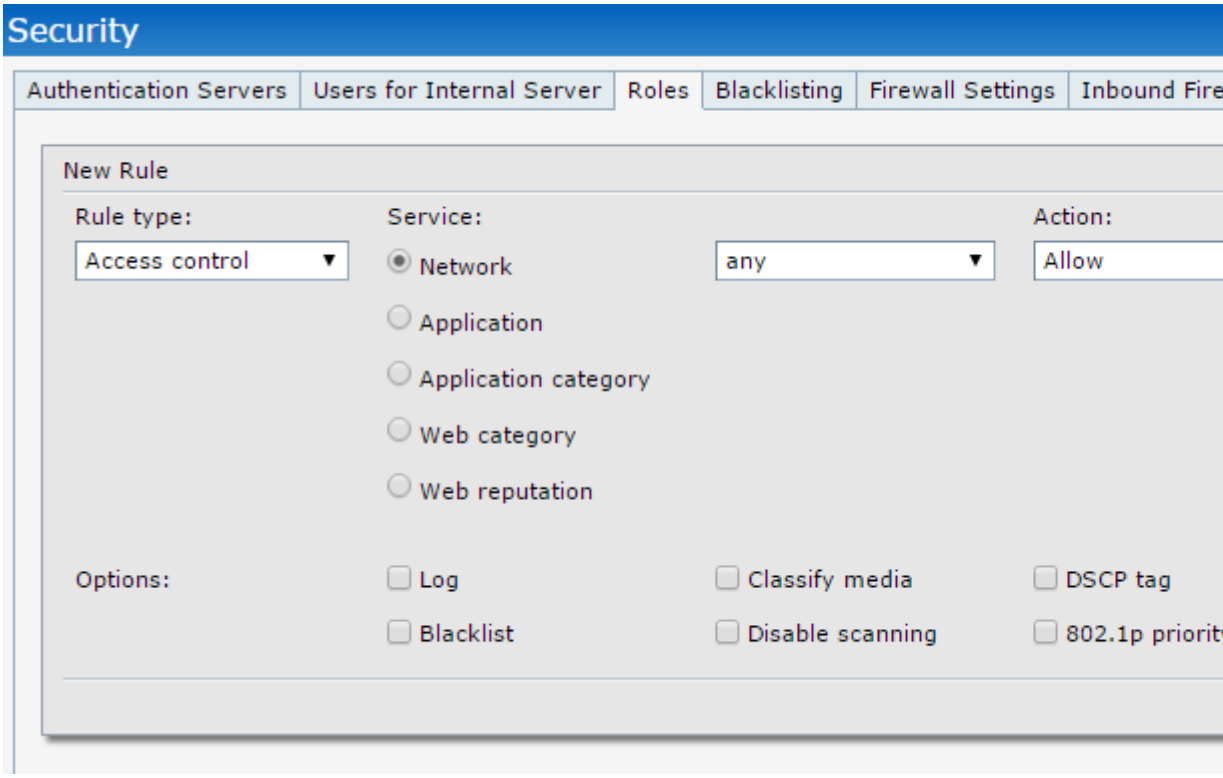
- **Access Rules**: Role-based

  Under **Roles** click **New** and enter **Preauth** as the name



Under **Access Rules for Preauth** click **New** and add the following rule:

- **Rule type**: Access control
- **Service**: Network - any
- **Action**: Allow
- **Destination**: to domain name
- **Domain name**: *insert access_domain here*



Click **OK** to save.

You need to add a rule (just like you did above), for all the below domains:

insert access_domain here

www.google.com
www.google.co.uk

google-analytics.com

venuewifi.com

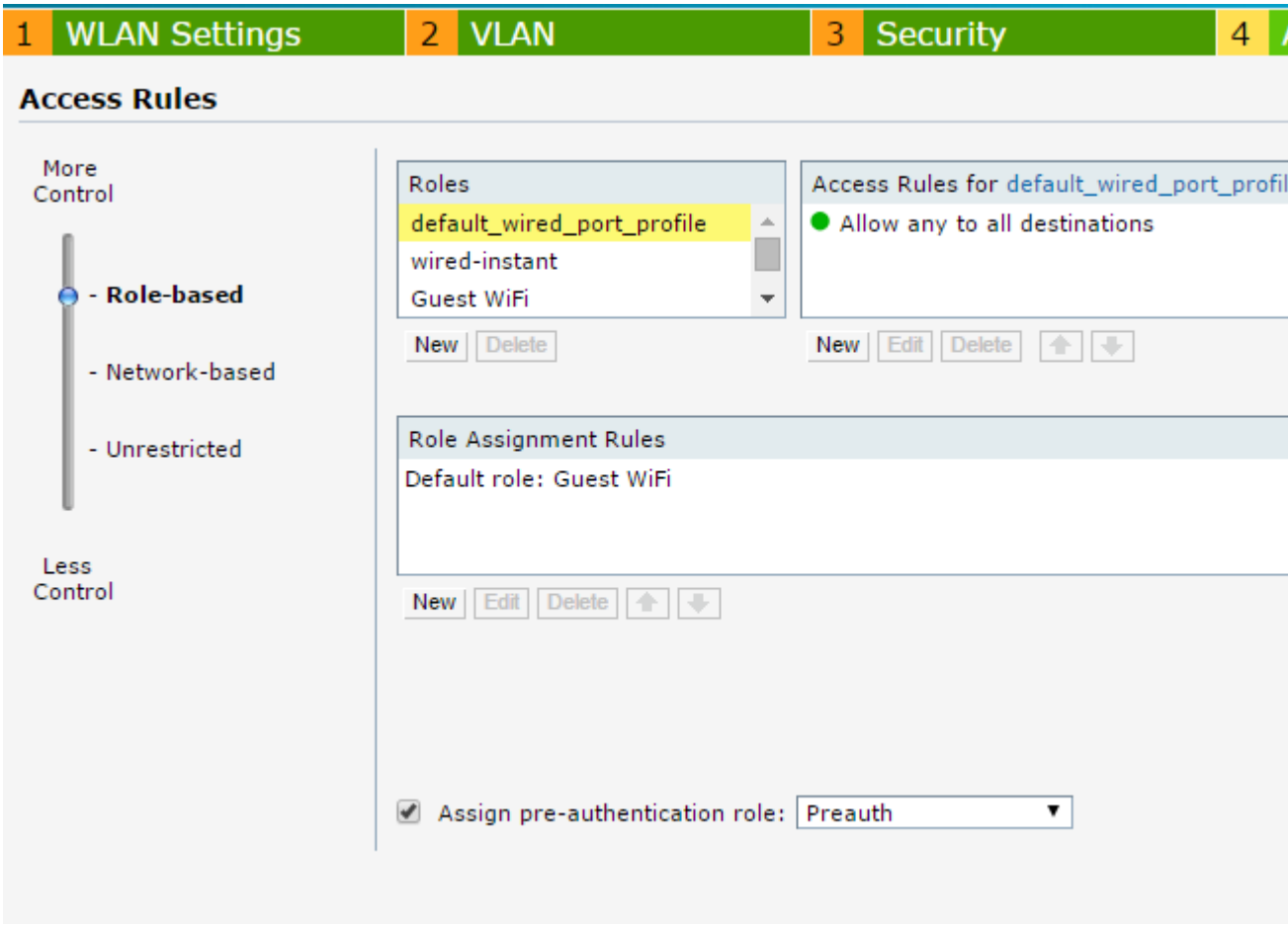
openweathermap.org

cloudfront.net

If you wish to support social network logins, you also need to add a rule for the domains below for each network you plan to support

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

- **Assign pre-authentication role**: select **Preauth**



Click **Finish** to complete the set up.