User Guide for Aruba Instant (IAP)

There are two methods to configure the Aruba IAP's. The first is via the web based interface (GUI) that sits on the IAP itself. The second is via Aruba Central, a cloud based service where you can manage all your IAP's. Both methods are described below.

To configure via Aruba Instant GUI (Virtual Controller)

Log in to your Aruba (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** : region1.purpleportal.net
    - **URL** : /access/
    - **Port** : 443
    - **Use https** : Enabled
    - **Captive portal failure** : Deny internet
    - **Automatic URL whitelisting** : Disabled
    - **Redirect URL** : https://region1.purpleportal.net/access/?res=success

  Click **OK** to save
- **Auth server 1** : Click the dropdown and choose **New** . Configure with:
    - **Type:** RADIUS
    - **Name** : guestwifi1
    - **IP address** : 54.217.112.62
    - **Auth port** : 1812
    - **Acct port** : 1813
    - **Shared key** : 6n8!5ETGb^nd
    - **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** : 176.34.118.13
    - **Auth port** : 1812
    - **Acct port** : 1813
    - **Shared key** : 6n8!5ETGb^nd
    - **Retype key** : as above

  Click **OK** to save
- **Reauth interval** : 24 hrs

- **Health 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:

  region1.purpleportal.net
  venuewifi.com
  openweathermap.org
  cloudfront.net
  stripe.com

  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	Instagram
facebook.com fbcdn.net akamaihd.net connect.facebook.net	twitter.com twimg.com	linkedin.com licdn.net licdn.com	instagram.com

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

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** : region1.purpleportal.net
  -

  Click **OK** to save.

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

  region1.purpleportal.net
  venuewifi.com
  openweathermap.org
  cloudfront.net
  stripe.com

  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	Instagram
facebook.com fbcdn.net akamaihd.net connect.facebook.net	twitter.com twimg.com	linkedin.com licdn.net licdn.com	instagram.com

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

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

To configure via Aruba Central

Log in to your Aruba Central account at https://portal.central.arubanetworks.com

Under **Wireless Configuration** on the left choose **Networks** .

Click on **Create New** and configure as per below:

- **Type** : Wireless
- **Name (SSID)** : Guest WiFi
- **Primary Usage** : Guest

Click **Next** and configure with the following:

- **Client IP Assignment** : Virtual Controller Assigned

Click **Next** and configure with the following:

- **Splash Page Type** : External
- **Captive Portal Profile** : Choose **New...** and configure with:

  - **Name** : guestwifi
  - **Type** : Radius Authentication
  - **IP or Hostname** : region1.purpleportal.net
  - **URL** : /access/
  - **Port** : 80
  - **Use HTTPS** : Unticked
  - **Captive Portal Failure** : Deny Internet
  - **Automatic URL Whitelisting** : Unticked
  - **Redirect URL** : https://region1.purpleportal.net/access/?res=success

  Click on **Save**
- **WISPr** : Disabled
- **Encryption** : Disabled
- **MAC Authentication** : Disabled
- **Authentication Server 1** : Choose **New...** and configure with:

  - **Name** : guestwifi1
  - **IP Address** : 54.217.112.62
  - **Shared Key** : 6n8!5ETGb^nd
  - **Retype Key** : as above

  All other values should be left at their defaults.

  Click on **Save Server**

- **Authentication Server 2** : Choose **New...** and configure with:

  - **Name** : guestwifi2
  - **IP Address** : 176.34.118.13
  - **Shared Key** : 6n8!5ETGb^nd
  - **Retype Key** : as above

  All other values should be left at their defaults.

  Click on **Save Server**

- **Load Balancing** : Disabled
- **Reauth Interval** : 24 hrs
- **Accounting** : Enabled
- **Accounting Mode** : Authentication
- **Accounting Interval** : 3 min
- **Blacklisting** : Disabled
- **Walled Garden** : Click on 0 **blacklist, 0 whitelist** and configure with:

  Under **Whitelist** click on **New** and enter the below domains, one by one:
  - region1.purpleportal.net
  - cloudfront.net
  - openweathermap.org
  - venuewifi.com
  - stripe.com
- Click on **Ok** to add each one and then add the next until you have all the domains listed.

Click on **Next**

- **Access Rules** : Role Based

Under **Role** click on **New** and enter **Preauth** as the Name. Click **Ok** to add.

Now, under **Access Rules for Selected Roles** click on the **Plus icon**

You will need to add a new rule one by one for each of the following:

- **Access Control** / **Network** / **Any** / **Allow** / **To a Domain Name** : region1.purpleportal.net
- **Access Control** / **Network** / **Any** / **Allow** / **To a Domain Name** : cloudfront.net
- **Access Control** / **Network** / **Any** / **Allow** / **To a Domain Name** : instagram.com
- **Access Control** / **Network** / **Any** / **Allow** / **To a Domain Name** : venuewifi.com
- Access Control / Network / Any / Allow / To a Domain Name : stripe.com

Click on **Save** to each one and then add the next until all are listed.

Finally, add the following rule:

- **Access Control** / **Network** / **Any** / **Deny** / **To All Destinations**

Now, under the **Role** on the left choose **default_wired_port_profile** , and tick the box **Assign Pre-authentication Role** and select **Preauth** .