RouterApp

Captive Portal

Used symbols

⚠️ | Danger – Information regarding user safety or potential damage to the router.

❗ | Attention – Problems that can arise in specific situations.

ⓘ Information – Useful tips or information of special interest.

Contents

List of Figures

List of Tables

1. Description of Router App

This module is designed to provide a service called captive portal on routers functioning as a standard Wi-Fi hotspot or as router in a LAN. It means that every customer using this network is redirected to a special web page before a common use of the Internet. It is possible to insert a form for authentication or any information notice. If authentication is required, customer gains access to the Internet after entering the correct login data (username and password). Redirecting to a special web page is only performed for the first access to the Internet.

Captive Portal is typically used on public-access networks (free Wi-Fi hotspots) that require customers to view and interact with before being granted access to the public network. Customers must first contact the operator to provide them authentication data. Use of the *Captive Portal* module is also a way to persuade customers to read and accept the terms of network usage. Last but not least, the captive portal login page is a suitable place for locating advertising banners and other notifications.

For configuration of each router is available web interface of router app, which can be invoked by clicking on the module name on the *Router apps* page of the router web interface. The left part of the module web interface contains the menu with pages for monitoring (*Status*), *Configuration*, *Information* and *Customization* of the router. *Customization* block contains only the *Return* item, which switches this web interface to the interface of the router, see Figure 1.

Figure 1: Web Interface Main Menu

2. Module Configuration

Configuration of *Captive Portal* router app is performed via the form on the *Global*, *Welcome/Ban page* and *QoS* pages in the *Configuration* part of the module web interface.

2.1 Global

First item – *Enable Captive Portal service* is used to activate the module. *Public interface* specifies which interface is dedicated for connecting of clients to the Captive Portal (wlan0/wlan02 for a WiFi AP, eth0 for an Ethernet interface, or combination of all options mentioned before).

Please, note that Multi SSID functionality (one WiFi device can have multiple WiFi APs (SSIDs) is compatible only with firmware 6.3.0 or later!

Enable Exception allows you to use Captive Portal on external WiFi access point via eth0 interface. This exception allows the router to communicate outside the Captive Portal and when the MAC and IP address of the access point are specified, router obtains a way for this communication. This option is enabled only with eth0 interface (or combination containing eth0 interface).

Ticking the *Welcome/Ban page* box the settings for the welcome and ban page is activated. The connection mode can be set to *Reverse Proxy* or to *Redirect*. *Reverse Proxy* mode is used in case of redirecting to a **http** web page, which can contain an active form (some agreement, logging in, ...). In this case internal HTTP server acts like proxy server and forwards all requests to the external destination of HTTP server. It is possible to use any technology for web page dynamic content which is available on the destination server. Beware of access to other domains from index page because access only to specified domain is permitted. It is possible to use *Server Side Includes* technology to achieve some dynamic content. Second possible scripting technology is CGI. Nothing else is available.

For redirecting to a **https** page the *Redirect* mode must be set and used. A page containing an active form cannot be used in this case. Usually, a static web page with automatic redirection to required page is used.

> ⚠️ Some Android OS closing welcome page immediately as soon as internet is reachable so when the redirect mode is used then welcome page is displayed for a very short time. So it is more common to use reverse proxy mode instead of redirect mode for the welcome page.

Fields (*Welcome Page URL*) resp. *Ban Page URL* specifies an URL addresses where the welcome resp. the ban pages are available. A client will be redirected to these pages when accessing the Internet for the first time or when banned respectively. Correct format, in which these pages must be specified, is *http://full.domain.name*. If one of these URL addresses is not specified, the internal pages are used instead. Expected index file name is either *index.(s)html* resp. *ban.(s)html*. There are three internal locations, where router searches for index page in this order:

1. **USB flash disk** – Preferred location. If there is subdirectory *captive_portal* in flash disk root directory with index file, this file is used as welcome page. Flash disk is mounted automatically when service is started.

2. **Router filesystem** – If no USB flash disk is available, internal router filesystem can be used. The main disadvantage of this solution is too little disk space – about 300 kB only.

3. **Default page** – If index file cannot be found on USB flash disk nor on router filesystem, default page is used. 3. It is very simple and unchangeable.

Figure 2: Global configuration form

In the another part of the configuration form on the *Global* page customers authentication can be enabled/disabled before enabling access to the Internet using *Require authentication* checkbox. If authentication is required, it is necessary to set login data using *Username* and *Password* items. This authentication makes sense only if internal welcome page is used (i.e. *Welcome Page URL* field is blank). Method you can create a page with an authentication form is described in chapter *4 How to Create Own Welcome Page*. If external welcome page is used, authentication can be implemented independently and totally on remote HTTP server and then should be disabled here.

Next section of this form allows user to configure sending of statistical data to selected server. Sending statistics is activated by ticking the box *Send statistics*. It is necessary to specify the address of the server to which the data will be sent (*Server Address*). Sending period (*Send Period*) and data format (*Data Format*) can be configured as well. If the *Data Format* is set to *Extended*, the AP MAC and AP IP addresses are reported by a POST request.

Statistical data are sent from the router app via HTTPS using POST method. Data are divided into three messages: cust-list (message about connected customers), domain-list (list of visited domains) a utilization-list (list of used services). These messages are described in detail in Attachment A on page A1.
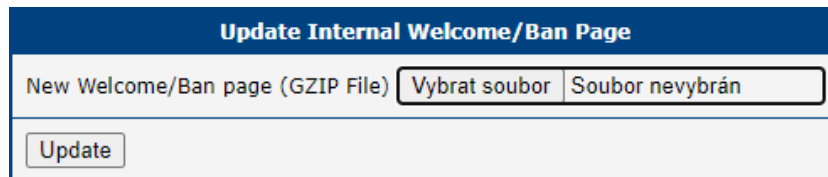
In the last part of the *Global* configuration form *Automatic disconnect after* item for automatic disconnection of a customer is available. Every customer is automatically disconnected when specified time expires. It is possible to choose from the following two ways of disconnection:

- **Inactivity** – Disconnection is performed if no data is transferred from/to customer for a specified time. Beware of applications which transfer data on background without customer intervention and which can cause long connection times.

- **Using** – Customer is disconnected after a set period of time, even though data transfer is in progress.

In some cases it may be desirable to delay the reconnection of a customer after he was automatically disconnected. This is done using the *Customer reconnect delay* field, where it is possible to specify the period (time) during which the customer will be temporarily banned. Zero value disables this function, so reconnection can be made without delay. Customers are recognized according to WiFi MAC address.

2.2   Welcome/Ban Page

There is available only *New Welcome/Ban Page (GZIP file)* item in the configuration form on the *Welcome/Ban page* page. This item allows you to select and subsequently upload a new welcome and ban pages using *Select file* and *Update* buttons. File format has to be TAR/GZIP. If USB flash disk is connected, file is unpacked here. Otherwise file is unpacked in router filesystem.

Figure 3: Welcome/Ban page configuration form

2.3   QoS

This configuration form allows you to limit the transfer rate and volume of data for every customer. Transfer rate limit is activated using the *Limit transfer rate* checkbox. Items *Total max. download rate* and *Total max. upload rate* set the maximum transmission rates for download, resp. upload within access technology used on the wireless side. Recommended values are about 10 % below technology maximum. *Customer max. download rate* and *Customer max. upload rate* specifies the maximum download and upload transfer rate for individual customers on WiFi side. If this value is multiplied by the number of simultaneously connected customers, the resulting value should not be higher than the total rate (*Total max. download/upload rate*).

Figure 4: QoS configuration form

There is also *Use predefined values for* select box, which allows you to fill the above mentioned items automatically by predefined values for specific connection technology. Predefined total values are 10 % below technology limit. Predefined customer values are calculated for three simultaneously connected customers. Default predefined values is usually necessary to easily customize according to the specific conditions that the result is optimal for your situation.
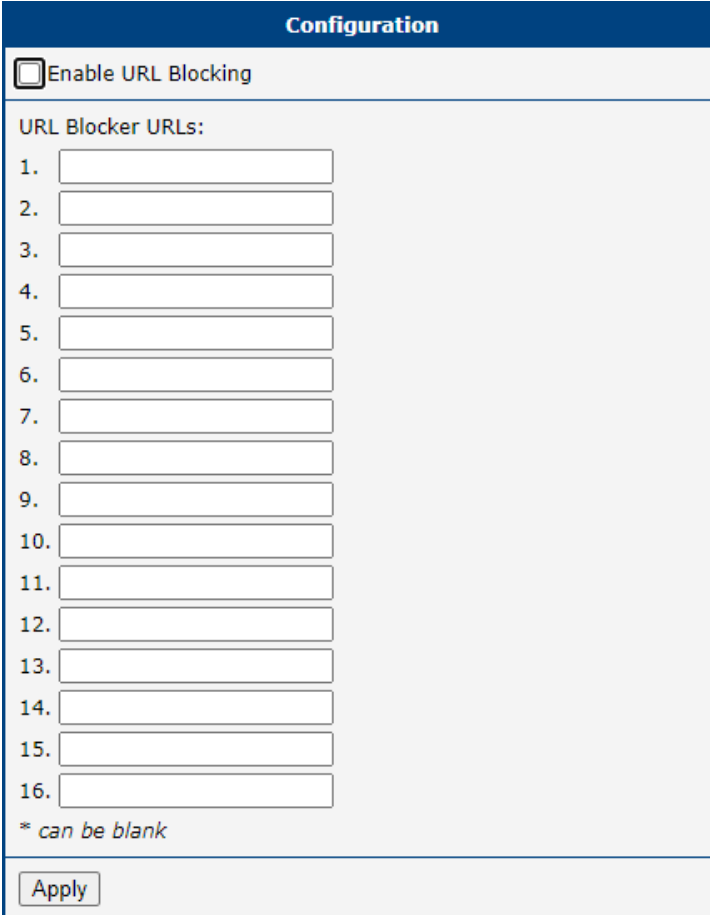
In the second part of the *QoS* configuration form, the maximal amount of incoming or outgoing data for every customer can be set. This function is activated by ticking the *Disconnect customer after transfer* checkbox. *Download volume* and *Or upload volume* items specify maximal download/upload data amount for every single customer. When one of these limits is reached, the access for the customer is prohibited for the time specified in *Ban for period* field. Only wireless side is limited, internal communication on WiFi side is unlimited. Limit overrun is checked once per minute.

The download/upload speed can be limited by setting in the last part of the *QoS* configuration form. This

function is activated by ticking the *Limit customer's download/upload speed* checkbox. *After download* and *Or after upload* fields specify the amount of data after which the speed will be reduced to the values declared in *Restrict download speed to* and *Restrict upload speed to* fields. This limitation is made for the time entered in the *Restrict speed for period* field.

2.4   URL Blocker

By ticking *Enable URL Blocking* you could set up to 16 domains to be inaccessible/blocked.

Figure 5: URL Blocker form

3. Status Overview

3.1 Global Overview

An overview of the current status can be viewed by clicking on the *Overview* item in the main menu of module web interface, see the figure 6. At the beginning of this page is a list of services and information about whether the corresponding service is active or not.
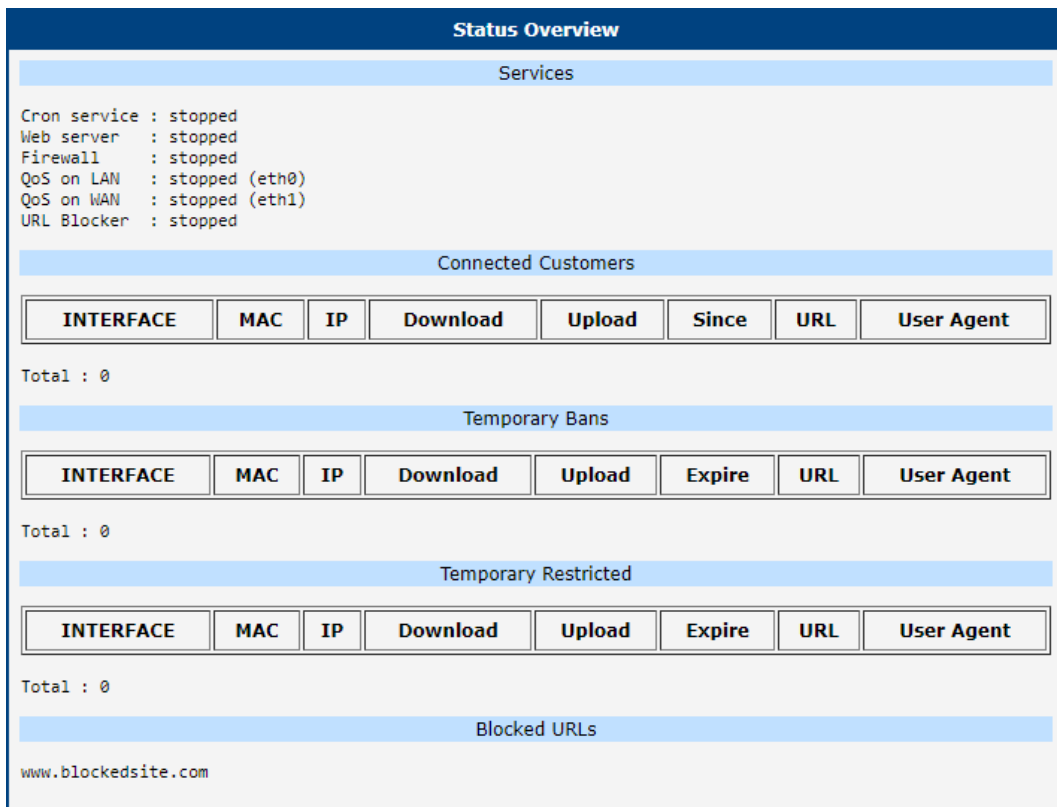
Figure 6: Global overview page

These are the following services:

Service	Description
Cron service	Service, which automatically runs a command respectively process (script, program, etc.) at a certain time.
Web service	Service that allows interaction of two machines on a network.
Firewall	Manages and secures traffic between networks.
QoS on LAN	Services used for management of data flows in LAN network.
QoS on WAN	Services used for management of data flows in WAN network.

Table 1: Available services

Below is a table that shows information about connected users. There are successively these parameters:

Parameter	Description
MAC	MAC address of the customer
IP	IP address of the customer
Download	The volume of downloaded data
Upload	The volume of sent data
Since	Time from which the user is connected
URL	Requested URL
User agent	A string consisting of the following parts: browser name and version (used by the customer), operating system and some other components installed with browser or operating system.

Table 2: Connected customers

At the end of the *Overview* page is a table in which is information about customers, who are temporarily banned. These are the same parameters as in the case of connected customers (table above). Only *Since* item is replaced by the *Expire* item, which informs about the time when temporary ban expires.

3.2   Log Pages

Users Log page contains information about access history of Captive Portal users, see the figure 7. This page displays information about currently logged in users, timestamp of users login and logout and users with restricted access.

Users Log

Current Users

00:34:da:52:e6:2c (192.168.2.2) is NOT logged in

Login

2018-10-10 11:28:01 login: 192.168.2.2 (00:34:da:52:e6:2c) Android 6.0; Mobile; Firefox/62.0 has been successfully logged in
2018-10-10 11:30:43 login: 192.168.2.2 (00:34:da:52:e6:2c) Android 6.0; Mobile; Firefox/62.0 has been successfully logged in

Logout

2018-10-10 11:30:01 logout: 192.168.2.2 has been logged out
2018-10-10 11:33:01 logout: 192.168.2.2 has been logged out

Restrict

2018-10-10 11:30:01 restrict: 192.168.2.2 (00:34:da:52:e6:2c) has been restricted
2018-10-10 11:33:01 restrict: 192.168.2.2 (00:34:da:52:e6:2c) has been restricted

Figure 7: Information about users' access

Connection Log page contains the log of internal router's web server. Page *System Log* displays the whole router's system log, not just the module one.

4. How to Create Own Welcome Page

Welcome page is a special page, which is displayed to every customer, who tries to access the Internet for the first time. Any URL from customer browser is redirected to welcome page.[1] This page has to be named *index.shtml* or *index.html*. There should always be link on welcome page which enables full internet access to customer. This link should look like:

```
<p>You can continue <a href="/captive\_portal/index2.sh">here</a>...</p>
```

Internal page /captive_portal/index2.sh will enable access to internet for customer's IP address and then redirect customer browser to original URL.

Depending on other settings there are more alternatives, what welcome page is returned to customer.

4.1 Simple Page

Unless authentication (*Require authentication*) nor reconnect delay (*Customer reconnect delay*) is enabled in the *Global* configuration form, customer is redirected to a simple page that might look as it is shown in the example above (file name is *index.shtml* or *index.html*). Page can contain anything. Only mandatory object is link to enable full access. Without it customer never get direct and full access to internet and only access to internal or external web server will be available.

4.2 Login Page

If authentication is enabled (*Require authentication*) in the *Global* configuration form, customer is redirected to a page named *login.shtml* or *login.html*. There should be some form where customer can fill in username and password and submit it to web server for authentication. There are two possibilities how to submit authentication data:

1. **Plain text** – Easier solution whose disadvantage is the transfer of authentication data in unencrypted form. Submit link should look like:

   ```
   /captive\_portal/index2.sh?auth\_name=user\&auth\_pass=secr
   ```

2. **Hash text** – More complicated solution, however username and password are transferred encrypted. Submit link should look like:

   ```
   /captive\_portal/index2.sh?auth\_hash=a621b9c2130bdf72ebc81a
   ```

---

[1]Only HTTP protocol is redirected, HTTPS is blocked entirely in this phase.

Hash is calculated as MD5 sum over "salt" + username + password, where *salt* is randomly generated value accessible on server side through SSI (Server Side Includes) and environment variable CP_AUTH_SALT.

4.3   Ban Page

If reconnect delay is enabled (*Customer reconnect delay*) in the *Global* configuration form and customer tries access to the Internet during temporary ban period, he (customer) is redirected to a page named *ban.shtml* or *ban.html*. It is possible to use SSI and environment variable CP_BAN_LEFT which contains number of seconds to ban expiration. Ban page shouldn't contain link to enable internet access which wouldn't be even so applicable.

4.4   Customized Original URL

A link that allows the customer to have full access to the Internet can be extended by parameter in this form: origin_url. In this way, customer can be redirected to a different URL than he originally requested. The example below shows a situation in which the customer is not redirected to the originally requested URL, but to http://full.domain.name/.

```
/captive\_portal/index2.sh?origin\_url=http\%3A\%2F\%2Ffull.domain.name\%2F
```

Notice of escaping control characters in parameter value. This parameter (origin_url) must be the last.

4.5   External Welcome/Ban Page

If you use an external welcome/ban page, then you need to run *index2.sh* shell script as described for the internal welcome/ban page. There are basically two options on how to run the *index2.sh* script: run it after button press (authentication action) or run it automatically after each web page refresh. Below is an example of html code to run the *index2.sh* script from an external page.

```
<meta http-equiv="refresh" content="1;url=http://127.0.0.1/captive_portal/
index2.sh?origin_url=*****">
- Replace * with an URL of your web page.
```

HTTP GET Welcome page request to the external server contains origin URL and information about AP/STA client as show below.

```
GET /?origin_url=<URL>&client_mac=04:f1:28:XX:XX:XX&client_ip=192.168.3.10
&ap_mac=00:22:88:XX:XX:XX&ap_ip=192.168.3.1&ap_ssid=v3L HTTP/1.1|Host:...
```

4.6   Example

Complex example how to create welcome page is in `WelcomePageExample.tar.gz` file, which is available on Captive Portal webpage. This example uses SSI technology for creating dynamic content. The archive contains the following files (in alphabetical order):

- ban.shtml – This page is returned when customer is temporarily banned.

- example.jpg – Common picture for all pages.

- footer.shtml – Common footer included in all pages.

- header.shtml – Common header included in all pages.

- index.shtml – The main welcome page for situations in which authentication of customers **is not required**.

- login.shtml – The main welcome page for situations in which authentication of customers **is required**.

- md5.js – Auxiliary javascript function for calculating MD5 sum when authentication is required.

The whole archive can be uploaded to the router using the form on the *Welcome page* page of the web interface of this module. Example is very small and therefore it can be used as an internal page located in the router filesystem.

5. Information

5.1 licenses

Summarizes Open-Source Software (OSS) licenses used by this module.

Captive Portal Licenses		
Project	**License**	**More Information**
hiawatha	GPLv2	License
openssl	OpenSSL	License

Figure 8: licenses

6. Related Documents

You can obtain product-related documents on *Engineering Portal* at *icr.advantech.com* address.

To get your router's *Quick Start Guide*, *User Manual*, *Configuration Manual*, or *Firmware* go to the *Router Models* page, find the required model, and switch to the *Manuals* or *Firmware* tab, respectively.

The *Router Apps* installation packages and manuals are available on the *Router Apps* page.

For the *Development Documents*, go to the *Development* page.

Attachment A: Statistics Distribution Protocol

Statistical data are sent from the router app via HTTPS using POST method. Data are divided into three messages: cust-list (message about connected customers), domain-list (list of visited domains) a utilization-list (list of used services). The period of the data distribudion and the server address can be set in the global configuraion page of the module. Please, note that this module is compatible only with router's firmware 4.0.0 or later.

Cust-list: list of connected customers

```
POST /cust-list.php HTTP/1.1
User-Agent: CaptivePortal
Host: Host IP address
Accept: */*
Content-Length: Message length
Content-Type: application/x-www-form-urlencoded

ap_mac[$i]=$AP_MAC&ap_ip[$i]=$AP_IP&timestamp[$i]=$NOW&connected[$i]
=2&mac[$i]=$MAC&ipaddr[$i]=$IP&download[$i]=0&upload[$i]=0&since[$i]=$NOW&url[$i]
=$3&useragent[$i]=$4&...
```

Fields description:

ap_mac[1] - MAC address of the access point
ap_ip[1] - IP address of the access point
timestamp - data timestamp [unix format date +%s]
connected - 0...customer disconnected
      1...customer connected - already connected (updted the entry in DB)
      2...customer connected - newly connected (new entry in DB)
mac - MAC address of the customer
ipaddr - IP address of the customer
download - total amount of downloaded data
upload - total amount of uploaded data
since - connected to the captive portal from [unix format date +%s]
useragent - type of the web browser

---

[1]If the *Data Format*, in the *Global Configuration*, is set to *Extended*.

Domain – list: list of visited domains

```
POST /domain-list.php HTTP/1.1
User-Agent: CaptivePortal
Host: Host IP address
Accept: */*
Content-Length: Message length
Content-Type: application/x-www-form-urlencoded
```

```
ap_mac[$i]=AP_MAC&ap_ip[$i]=$AP_IP&year[$i]=$YEAR&month[$i]
=$MONTH&day[$i]=$DAY&time[$i]=$TIME&domain[$i]=$DOMAIN&ip[$i]=$IP&...
```

Fields description:

ap_mac[1] - MAC address of the access point
ap_ip[1] - IP address of the access point
year - year of domain visiting
month - month of domain visiting
day - day of domain visiting
time - time of domain visiting [hh:mm:ss]
domain - visited domain
ip - IP address of the customer visiting the domain

Utilization-list: list of used services

```
POST /utilization-list.php HTTP/1.1
User-Agent: CaptivePortal
Host: Host IP address
Accept: */*
Content-Length: Message length
Content-Type: application/x-www-form-urlencoded
```

```
ap_mac[$i]=$AP_MAC&ap_ip[$i]=$AP_IP&timestamp[$i]=$NOW&netpool[$i]
=$W_NETWORK&category[$i]=2&rxbytes[$i]=RXBYTES&txbytes[$i]=$TXBYTES&...
```

Fields description:

ap_mac[1] - MAC address of the access point
ap_ip[1] - IP address of the access point
timestamp - data timestamp [unix format date +%s]
netpool - monitored network (WLAN, LAN)
category - service type 1 – other; 2 – http, https; 3 – ftp; 4 – smtp;
     5 – imap, imapv3, imaps, pop3, pop3s
rxbytes - amount of received data for the category
txbytes - amount of sent data for the category

---

[1]If the *Data Format*, in the *Global Configuration*, is set to *Extended*.