

RUT850 Hotspot

[Main Page](#) > [RUT Routers](#) > [RUT850](#) > [RUT850 Manual](#) > [RUT850 WebUI](#) > [RUT850 Services section](#) > **RUT850 Hotspot**

The information in this page is updated in accordance with the [RUT850_R_00.01.04](#) firmware version.

□

Contents

- [1 Summary](#)
- [2 General](#)
 - [2.1 External Radius](#)
 - [2.2 Internal Radius](#)
 - [2.3 Without Radius](#)
 - [2.3.1 Users Configuration](#)
 - [2.3.2 Session Templates](#)
 - [2.4 Advertisement](#)
 - [2.5 MAC auth](#)
 - [2.6 SMS OTP](#)
 - [2.7 Walled Garden](#)
- [3 Restricted Internet Access](#)
- [4 Logging](#)
 - [4.1 FTP Upload Settings](#)
 - [4.2 Wifi Log/SMS OTP Log](#)
- [5 Landing Page](#)
 - [5.1 Template](#)
 - [5.2 Custom Landing Page](#)
- [6 Radius Server](#)
 - [6.1 Session Settings](#)
 - [6.2 Users Configuration Settings](#)
 - [6.3 Clients Configuration Settings](#)
- [7 Statistics](#)
- [8 Manage](#)

Summary

Wireless **Hotspots** are essentially Wireless Access Points - they provide network and/or internet access to other WiFi devices. The difference is that Hotspots are a lot more versatile when it comes to managing, monitoring and authenticating the wireless network's users. For example, while Wireless APs can be password protected, with Hotspots you can configure different users with different names, passwords, even data limits and data speeds and more. This chapter is an overview of the **Wireless Hotspot** function in RUT routers.

General

The **General** tab is where most of the Hotspot configurations take place. This section will be divided into six sub-sections - one for each **Authentication mode**, since the chosen **Authentication mode** will define how the Hotspot will be configured in general.

External Radius

External Radius authentication mode uses an external Radius server, to which you have to provide an address to, instead of using the router's internal Radius server.



Field	Value	Description
Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network
Logout address	host ip; default: 1.1.1.1	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Authentication protocol	PAP CHAP; default: PAP	Authentication protocol used to authenticate new connections on the Hotspot
Terms of service	yes no; default: no	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the Landing Page section
RADIUS server #1 RADIUS server #2	ip; default: none	The IP address of the RADIUS server that is to be used for Authenticating your wireless clients
Authentication port	integer [0..65535]; default: 1812	RADIUS server authentication port
Accounting port	integer [0..65535]; default: 1813	RADIUS server accounting port
Radius secret key	string; default: none	The secret key is a password used for authentication with the RADIUS server
UAM port	integer [0..65535]; default: 3990	Port to bind for authenticating clients

UAM UI port	integer [0..65535]; default: 4990	UAM User Interface port
UAM secret	string; default: none	Shared secret between the UAM server and the Hotspot
NAS identifier	string; default: none	NAS-Identifier is one of the basic RADIUS attributes
Swap octets	yes no; default: no	Swaps the meaning of input octets and output as it relates to RADIUS attributes
Location name	string; default: none	Custom location name for your Hotspot
External landing page	yes no; default: no	Enables the use of an external landing page
Landing page address	string; default: none	A custom Hotspot's external landing page
Success URL	string; default: none	A custom redirect URL after successful Hotspot login
Protocol	HTTP HTTPS; default: HTTP	Connection protocol of your Hotspot
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

Internal Radius

Internal Radius is Authentication mode that uses the router's internal RADIUS server for authentication. Teltonika routers' RADIUS server has RFC 2866 RADIUS Accounting and RFC 2869 RADIUS Extensions implemented.



Field	Value	Description
Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network

Logout address	host ip; default: 1.1.1.1	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Terms of service	yes no; default: no	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the Landing Page section
External landing page	yes no; default: no	Enables the use of an external landing page
Landing page address	string; default: none	A custom Hotspot's external landing page
Success URL	string; default: none	A custom redirect URL after successful Hotspot login
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

Information on how to configure Internal radius server can be found [here](#).

Without Radius

Without Radius Authentication doesn't use a Radius server to authenticate users connecting to the Hotspot, instead it gives you the possibility to configure different users with different password and session parameters.



Field	Value	Description
Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF

AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network
Logout address	host ip; default: 1.1.1.1	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Terms of service	yes no; default: no	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the Landing Page section
External landing page	yes no; default: no	Enables the use of an external landing page
Landing page address	string; default: none	A custom Hotspot's external landing page
Success URL	string; default: none	A custom redirect URL after successful Hotspot login
Protocol	HTTP HTTPS; default: HTTP	Connection protocol of your Hotspot
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

Users Configuration

The **Users Configuration** tab is used to create new, unique users that can connect to the Hotspot.



Field	Value	Description
Username	string; default: none	A custom user name used to authenticate clients connecting to the Hotspot
Password	string; default: none	A custom password for the specified user name
Session Template	string; default: unlimited	Session templates define session settings for different users. The unlimited Session Template is a default template with no restrictions. More on Session Template in the next section

Session Templates

A **Session Template** is a set of rules that can be prescribed to a Hotspot user. A default template named **unlimited** is present in the router, but it has no configured restrictions. You can edit the default template or you can create a custom template and configure it.



Field	Value	Description
Idle timeout	integer; default: none	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
Session timeout	integer; default: none	A timeout in seconds after users are automatically disconnected from the Hotspot. The timeout countdown begins when a user is authenticated to the Hotspot and, after an amount of time specified in this field, the user gets disconnected from the Hotspot. 0 means unlimited
Download bandwidth	integer; default: none	Maximum download bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s, Gbit/s
Upload bandwidth	integer; default: none	Maximum upload bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
Download limit	integer; default: none	A received data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Download limit is specified in MB
Upload limit	integer; default: none	A sent data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Upload limit is specified in MB
Period	Month Week Day; default: Month	The beginning of the period during which the restriction specified in this section will apply. After the period is over, all specified limits are reset
Start day Start hour	integer [1..31] Monday..Sunday integer [1..24]; default: day 1	Specifies which day of the month, week or hour of the day the limits will be reset

Advertisement

The **Advertisement** Authentication mode doesn't use any kind of actual authentication. Instead when a user connects to the Hotspot he first gets redirected to a specified advertisement page. After that the user is free to use the Hotspot.



Field	Value	Description
-------	-------	-------------

Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Advertisement address	host ip; default: none	The address of the advertisement page that newly connected users will be redirected to
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

MAC auth

MAC auth Authentication mode authenticates users by their MAC address. A list of accepted or unaccepted MAC addresses can be configured in the router's WebUI's Wireless section under Interface Configuration->[MAC Filter](#)



Field	Value	Description
Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF
AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network

Logout address	host ip; default: 1.1.1.1	An address that can be used by users to logout from the Hotspot session
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Terms of service	yes no; default: no	If enabled, users have to agree to the Terms of service before logging in. Custom Terms of service can be defined in the Landing Page section
Password protection	yes no; default: no	Enables Hotspot password protection
Password	string; default: none	A password used to authenticate connecting clients to the Hotspot
Website access link	Link Auto redirect Custom address; default: Link	Requested website access mode
Protocol	HTTP HTTPS; default: HTTP	Connection protocol of your Hotspot
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

SMS OTP

With **SMS OTP** Authentication mode connecting users are prompted to enter their phone number. After that, the router sends an SMS message containing a code to the specified number. Users then authenticate themselves to the Hotspot using this code.



Field	Value	Description
Configuration profile	Custom Cloud4wi Hotspotsystem; default: Custom	If not set to Custom , Configuration profile selections will automatically fill all the fields in accordance with the chosen profile. It also automatically adds an exception for the chosen service in the Walled Garden section. Used only with External radius Authentication mode.
Enable	yes no; default: no	Toggles Wi-Fi Hotspot ON or OFF

AP IP	ip; default: 192.168.2.254/24	Access Point IP address defines the IP address of your Hotspot's network
Authentication mode	External radius Internal radius Without radius Advertisement MAC auth SMS OTP; default: Without radius	Authentication mode defines how users will connect to the Hotspot
Protocol	HTTP HTTPS; default: HTTP	Connection protocol of your Hotspot
HTTPS to landing page redirect	yes no; default: no	Redirects HTTP pages to landing page
SSL key file	.key file; default: none	SSL key file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
SSL certificate file	.crt file; default: none	SSL certificate file used for authentication. This field becomes visible only if HTTPS to landing page redirect is enabled
Use custom DNS	yes no; default: no	Enables the use of custom DNS servers instead of your regular DNS
DNS server 1 DNS server 2	ip; default: none	Additional DNS servers that are to be used by the Hotspot. These fields become visible only if Use custom DNS is enabled

Walled Garden

You can configure a list of addresses that users connected to the Hotspot will be able to reach without any authentication. By default this list is empty. Click the **Add** button to add a new address.



Field	Value	Description
Enable	yes no; default: yes	Enables or disables an entry of the list
Address	host ip; default: none	An address that users connected to the Hotspot can reach without authentication
Port	integer [0..65535]; default: none	Specifies the port through which the user can connect to the provided address. This field becomes visible only if Allow subdomains is disabled
Allow subdomains	yes no; default: no	If checked, users can connect to the specified address and all of its subdomains

Restricted Internet Access

The **Restricted Internet Access** page provides you with the possibility to restrict internet access on Hotspot on specified hours. Blue squares represent restricted access, white squares - allowed access. Bellow is an example of a configuration that restricts internet access outside of working hours.



Logging

The Hotspot **Logging** section is used to send Hotspot or Wireless information to an FTP or Syslog server. 

Field	Value	Description
Enable	yes no; default: no	Enables or disables whole logging section's functionality



Field	Value	Description
Enable	yes no; default: no	Toggles logging to Syslog ON or OFF
Server address	host ip; default: " "	Syslog server address
Port	integer [0..65535]; default: " "	Syslog server port
Protocol	UDP TCP default: TCP	Protocol of the syslog server
Prefix text	string; default: " "	Prefix custom text to streamed messages
Protocol filter	UDP TCP Any; default: Any	Filter log messages depending on protocol
Port filter	integer [0..65535]; default: " "	Filter log messages depending on port of port range



Field	Value	Description
Enable	yes no; default: no	Toggles logging to FTP ON or OFF
Server address	host ip; default: your.ftp.server	FTP server address.
User name	string; default: username	User name used for authentication when logging into an FTP server
Password	string; default: password	Password used for authentication when logging into an FTP server
Port	integer [0..65535]; default: 21	FTP server port
File name extras	No extra information MAC address Serial number Custom string; default: No extra information	Extra information to be added to the log filename



FTP Upload Settings

Here you can configure your timing settings for the log upload via FTP feature.



Field	Value	Description
Mode	Fixed Interval; default: Fixed	The scheduling mode to be used for uploading to FTP server
Hours	time; default: 8 hours	Time interval when the uploads will take place
Minutes	time; default: 15 minutes	Time interval when the uploads will take place
Days	time; default: Monday, Tuesday, Wednesday, Thursday, Friday	On which day upload will take place

Wifi Log/SMS OTP Log

WiFi and SMS OTP logs show information about connections to your WiFi Hotspot. FTP logging has to be enabled.  

Landing Page

This section is used to define how your Hotspot's Landing Page will look like.



Template

This is a template based on the default landing page. You can edit its HTML code to make it look however you want!



Custom Landing Page

Radius Server

This section is used to configure your **Radius Server** for use with [Internal radius](#) Authentication mode



Field	Value	Description
Enable	yes no; default: no	Toggles Radius Server ON or OFF
Remote access	yes no; default: no	Toggles remote access to the Radius Server ON or OFF.
Accounting port	integer [0..65535]; default: 1813	Radius server accounting port
Authentication port	integer [0..65535]; default: 1812	Radius server authentication port

Session Settings

A **Session Template** is a set of rules that can be prescribed to a Hotspot user. A default template named **unlimited** is present in the router, but it has no configured restriction. You can edit the default template or you can create a custom template and configure it.



Field	Value	Description
Idle timeout	integer; default: none	A timeout in seconds after which idle users are automatically disconnected from the Hotspot. 0 means unlimited
Session timeout	integer; default: none	A timeout in seconds after users are automatically disconnected from the Hotspot. The timeout countdown begins when a user is authenticated to the Hotspot and, after an amount of time specified in this field, the user gets disconnected from the Hotspot. 0 means unlimited
Download bandwidth	integer; default: none	Maximum download bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
Upload bandwidth	integer; default: none	Maximum upload bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Kbit/s, Mbit/s or Gbit/s
Download limit	integer; default: none	A received data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Download limit is specified in MB
Upload limit	integer; default: none	A sent data limit that the users assigned to this template can reach. After the data limit is reached, the user will lose data connection. Upload limit is specified in MB
Period	Month Week Day; default: Month	The beginning of the period during which the restriction specified in this section will apply. After the period is over, all specified limits are reset
Start day Start hour	integer [1..31] Monday..Sunday integer [1..24]; default: day 1	Specifies which day of the month, week or hour of the day the limits will be reset

Users Configuration Settings

The **Users Configuration** tab is used to create new, unique users that can connect to the Hotspot.



Field	Value	Description
Username	string; default: none	A custom user name used to authenticate clients connecting to the Hotspot
Password	string; default: none	A custom password for the specified user name
Session Template	string; default: unlimited	Session templates define session settings for different users. The unlimited Session Template is a default template with no restrictions. More on Session Template in the next section

Clients Configuration Settings



Field	Value	Description
Enable	yes no; default: yes	Toggles Clients Configuration ON or OFF
Client name	string; default: none	A custom user name used to authenticate clients connecting to the Hotspot
IP address	ip; default: none	The IP address of the client
Netmask	integer [0..32]; default: none	The netmask of the client
Radius shared secret	string; default: none	Radius shared secret used for communication between the client/NAS and the radius server

Statistics

The **Statistics** page shows statistics about connections to the hotspot. **Reminder: Statistics page becomes visible only when device is connected to the hotspot.**



Manage

With the help of the **Manage** page you manage the users that are connected to your Hotspot. To reach the **Manage** window, go to Services->Hotspot. The **Manage** button will be located next to your Hotspot instance.

