https://wiki.teltonika-networks.com/view/RUT140_Hotspot

RUT140 Hotspot

The information in this page is updated in accordance with firmware version **RUT14X_R_00.07.07.1**.

□

Contents

- 1 Summary
- 2 General
  - 2.1 Hotspot Instances
    - 2.1.1 General Settings
      - 2.1.1.1 General
      - 2.1.1.2 Advanced
      - 2.1.1.3 Radius
      - 2.1.1.4 Walled Garden
      - 2.1.1.5 URL Parameters
      - 2.1.1.6 User Scripts
- 3 Local Users
- 4 Landing Page
  - 4.1 General Settings
  - 4.2 Themes
    - 4.2.1 Images
    - 4.2.2 Style Settings
    - 4.2.3 View Settings
    - 4.2.4 Custom Theme
- 5 User Groups
- 6 User Management
- 7 Hotspot 2.0
  - 7.1 Hotspot 2.0 Configuration
    - 7.1.1 General Setup
    - 7.1.2 OSU Provider
    - 7.1.3 WAN Metrics
  - 7.2 Venue Name Information
  - 7.3 3GPP Cellular Network Information
  - 7.4 Network Access Identifier (NAI) Realm Information
  - 7.5 Operator Friendly Name
  - 7.6 Connection Capability

Summary

On Teltonika Networks devices a **Hotspot** is a service that provides authentication, authorization and accounting for a network. This chapter is an overview of the Hotspot section for RUT140 devices.

General

Hotspot Instances

The **Hotspot Instances** section displays the main parameters of your Hotspot. By default, a Hotspot instance does not exist on the device. To create a new instance and begin configuration:

1. select an 'Interface';
2. click the 'Add' button;

After this, a new Hotspot configuration window will appear.

General Settings

The **General Settings** window is where most of the Hotspot configuration takes place. Look to the sub-sections below for information on configuration fields found in the General Settings sections.

General

Field	Value	Description
Configuration profile	Cloud4wi | Default | Hotspotsystems | Purple portal; default: **Default**	Pre-configures Hotspot settings according to the selected service provider.
Enable	off | on; default: **on**	Turns the Hotspot instance on or off.
Hotspot Network	ip/netmask; default: **192.168.2.0/24**	IP address and subnet of the Hotspot network.
IP Address	ip; default: **192.168.2.254**	Defines the IP address of your Hotspot router in network.
Authentication mode	Local users | Radius | MAC authentication | Single sign-on; default: **Local users**	Authentication mode defines how users will connect to the Hotspot.
Local users: Allow signup	off | **on**; default: **off**	Allows users to sign up to hotspot via landing page.

Local users: Expiration time	integer; default: **0**	User credential expiration time. Applies to users who signed up via landing page.
Local users: Users group	user group; default: **default**	The user group to which users signed up via landing page should be assigned to.
Radius: Enable MAC authentication	off | on; default: **off**	Enable MAC address authentication.
MAC authentication: Require password	off | on; default: **off**	Enables password requirement for MAC authentication.
MAC authentication: MAC auth password	string; default: **none**	Password for MAC authentication.
MAC authentication / Single sign-on: User group	select; default: **default**	Specifies the group of dynamically created users.
Landing Page	Internal | External; default: **Internal**	Location of the landing page.
UAM Port	integer; default: **3990**	Port to bind for authenticating clients.
Password encoding	off | on; default: **none**	Password encoding with the challenge.
Landing page address	url; default: **none**	External landing page address (http://www.example.com).
UAM Secret	string; default: **none**	Shared secret between uamserver and hotspot.
Success page	Success Page | Original URL | Custom; default: **Success page**	Location to return to after successful authentication.
Custom	url; default: **none**	Address must contain protocol (http://www.example.com).

Advanced

Field	Value	Description
Additional interfaces	Available interfaces; default: **none**	Choose additional the interfaces you want to attach to this hotspot instance.
Enable MAC blocking	off | on; default: off	Blocks access to MAC addresses that have reached set amount of failed login attempts.
Logout address	ip; default: **1.0.0.0**	IP address to instantly logout a client accessing it.
Protocol	HTTP | HTTPS; default: **HTTP**	Protocol to be used for landing page.
Enable TOS	off | on; default: **off**	Enables Terms of Service (ToS) requirement. Client device will be able to access the Internet only after agreeing ToS.
Trial access	off | **on**; default: **off**	Enables trial internet access for a specific group.
Group	User group; default: **default**	Specifies the group of trial users.
Subdomain	string; default: **none**	Combined with Domain to make a DNS alias for the Hotspot IP address.

Domain	string; default: **none**	Combined with Subdomain to make a DNS alias for the Hotspot IP address.
HTTPS to landing page redirect	off | **on**; default: **off**	Redirect initial pre-landing page HTTPS requests to hotspot landing page.
Certificate files from device	off | on; default: **off**	Specified whether to upload key & certificate files from computer or to use files generated on this device via the *System* → *Administration* → ***Certificates*** page.
SSL key file	key file; default: **none**	Upload/select SSL key.
SSL certificate file	certificate file; default: **none**	Upload/select SSL certificate.
Primary DNS server	ip; default: **8.8.8.8**	Additional DNS servers that are to be used by the Hotspot.
Secondary DNS server	ip; default: **8.8.4.4**	Additional DNS servers that are to be used by the Hotspot.

Radius

Radius authentication mode uses an external RADIUS server, to which you have to provide an address to, instead of using the router's Local Authentication. If you are using Local authentication, this section is not visible.

Field	Value	Description
RADIUS server #1	ip; default: **none**	The IP address of the RADIUS server #1 that is to be used for Authenticating your wireless clients.
RADIUS server #2	ip; default: **none**	The IP address of the RADIUS server #2 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.
NAS identifier	string; default: **none**	NAS-Identifier is one of the basic RADIUS attributes.
Radius secret key	string; default: **none**	The secret key is a password used for authentication with the RADIUS server.
Swap octets	off | on; default: **off**	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.
Location ID	string; default: **none**	Custom location ID for your Hotspot.

Walled Garden

You can add a list of addresses that users connected to the Hotspot will be able to reach without any authentication. By default this list is empty. Simply write addresses into the Address List.

Format of address is **website.com** (does not include https://www).

Field	Value	Description
Address list	domain names (one record per line); default: **none**	List of addresses the client can access without first authenticating. One record per line. See placeholder for accepted formats.

URL Parameters

The **URL parameters** section becomes visible when **Landing page** is selected as **External** in General settings section.

Field	Value	Description
UAM IP	string; default: **none**	The IP Address of the Captive Portal gateway.
UAM port	string; default: **none**	The port on which the Captive Portal will serve web content.
Called	string; default: **none**	The MAC address of the IP Address of the Captive Portal gateway.
MAC	string; default: **none**	The MAC address of the client trying to gain Internet access.
IP	ip default: **none**	The IP Address of the client trying to gain Internet access.
NAS id	string; default: **none**	An identification for the Captive Portal used in the RADIUS request.
Session id	string; default: **none**	The unique identifer for session.
User url	string; default: **none**	The URL which the user tried to access before he were redirected to the Captive Portal's URL's pages.
Challenge	string; default: **none**	A challenge that should be used together with the user's password to create an encrypted phrase used to log on.
Custom 1	string; default: **none**	Add custom name and custom value which will be displayed in url parameters.
-	SSID | Hostname | FW version | --Custom--; default: **SSID**	-
Custom 2	string; default: **none**	Add custom name and custom value which will be displayed in url parameters.
-	SSID | Hostname | FW version | --Custom--; default: **SSID**	-

User Scripts

In this section you can add custom **Scripts** that will be executed after a session is authorized in the **Session up** section, after session has moved from authorized state to unauthorized in the **Session down** section and after a new user has been signed up in the **User signup** section.

Field	Value	Description
Session up	bash script; default: **none**	Script executed after a session is authorized. Executed with the environment variables (Please refer to the wiki).
Session down	bash script; default: **none**	Script executed after a session has moved from authorized state to unauthorized. Executed with the environment variables (Please refer to the wiki).
User signup	bash script; default: **none**	Script executed after a new user has been created during signup process. Executed with the environment variables (Please refer to the wiki).

Local Users

The **Local Users** section is used to create and manage users that can connect to the Hotspot. The elements comprising the Local Users page are explained in the list and figure below.

1. Entering a Username, Password and clicking the 'Add' button creates a new user.
2. The 'Group' dropdown menu assigns a user to another group.
3. The 'Edit' button lets you change a user's password or assign the user to another group.
4. The 'Delete[X]' button deletes a user.

Landing Page

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

General Settings

General Settings section lets you choose the authentication protocol and theme that will be used in the Landing Page. You can download more themes using the Package Manager

Themes

The **Themes** section displays all available Landing Page themes. In order to download a theme, click the 'Download' button, in order to edit a theme, click the 'Edit' button next to it.

Images

The **Images** section allows you to upload custom images to different objects.

Style Settings

Pressing 'Edit' button next to style settings lets you edit how your landing page will look visually using CSS syntax.

View Settings

In **View Settings** you can access and modify default templates for various parts of landing page and edit their HTML code.

Custom Theme

To use custom theme you can download default theme and edit it's content. Then use 'Browse' button to upload it.

User Groups

User Groups provides the possibility to set different connection limits for different users. A group called 'default' is already created and does not have any limitations set by default. You can

1. create a new group by entering a custom Name and clicking 'Add'
2. or configure the existing rule by clicking the 'Edit' button next to it.

A group's settings page will look similar to this:

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.)
Time limit	integer; default: **none**	Disables hotspot user after time limit in sec is reached. (0, meaning unlimited)
Download bandwidth	integer; default: **none**	Maximum download bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Mbit/s.

Upload bandwidth	integer; default: **none**	Maximum upload bandwidth that the users assigned to this template can achieve. Bandwidth can be specified in Mbit/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.
Warning	integer; default: **none**	Send an SMS warning to hotspot user after warning value of download or upload data in MB is reached. Only works with SMS OTP authentication.
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	integer [1..31] | Monday..Sunday | integer [1..24]; default: **1**	Choices changes depending on what 'Period' was chosen. Specifies which day of the month, week or hour of the day the limits will be reset.

User Management

The **User sessions** tab displays the status and session statistics of currently logged in users. You can also "kick" (deauthenticate) a user by clicking the 'Logout' button next to it.

The **Registered Hotspot Users** tab displays the data of unique users that have registered to the hotspot before.

Hotspot 2.0

The **Hotspot 2.0** displays available WiFi interfaces. In order to begin configuring an interface click the 'Edit' button next to it:

After this you should be redirected to the configuration page for that interface.

Hotspot 2.0 Configuration

The main **configuration parameters** of a Hotspot 2.0 interface will be discussed in this section.

A Hotspot 2.0 interface requires WPA2-EAP encryption. You can configure it in the *Network → Wireless* page (click 'Edit' next to an interface and find the Wireless Security section).

General Setup

Field	Value	Description
Enable	off | on; default: **off**	Turns Hotspot 2.0 for this interface on or off.
Internet access	off | on; default: **off**	Is used to inform the client device whether internet access is available.
Access Network Type	Private network | Private network with guest access | Chargeable public network | Free public network | Personal device network | Emergency services only network | Test or experimental; default: **Private network**	The access network type present in beacon and probe response frames. Mobile devices can use this information when selecting a hotspot.
HESSID	mac; default: **none**	Homogeneous ESS identifier (optional). This shall be identical to one of the BSSIDs in the homogeneous ESS.
Roaming consortium OI	3 or 5 octet hexstring; default: **none**	Only first three entries are available through Beacon and Probe Response frames.
Network authentication type	Not configured | Acceptance of terms and conditions | On-line enrollment supported | http/https redirection | DNS redirection; default: **Not configured**	Type of authentication used on this network.
Redirect URL	url; default: **none**	Http/https redirection link.
IP Address type availability	Address type not available | Public IPv1 address available | Port restricted IPv4 address available | Single NATed IPv4 address available | Double NATed IPv4 address available | Port restricted IPv4 address and single NATed IPv4 address available | Port restricted IPv4 address and double NATed IPv4 address available | Availability of the address type is not known; default: **Availability of the address type is not known**	Provides information about the IP address version and type that would be available to a mobile device after it authenticates to the network.
Domain name	domain name; default: **none**	The Domain Name ANQP-element provides a list of one or more domain names of the entity operating the hotspot network.
Venue group	various; default: **Unspecified**	Describes the venue in which the hotspot is located.
Venue type	various; default: **Unspecified**	Describes the venue in which the hotspot is located.

OSU Provider

Field	Value	Description
OSU ssid	string; default: **none**	Informs client devices about the SSID used for OSU connections.
OSU server URL	url; default: **none**	Is used to inform the client device whether internet access is available.
Name language code	string; default: **none**	Two or three character language code (ISO-639).
OSU friendly name	string; default: **none**	User-friendly name of an OSU service provider.
OSU NAI	string; default: **none**	OSU network access identifier.
OSU method list	OMA-DM | SOAP-XML; default: **none**	Configures the supported OSU method(s) of the OSU provider.
Description language code	string; default: **none**	Two or three character language code (ISO-639).
Description	string; default: **none**	OSU service description.

WAN Metrics

Field	Value	Description
Link Status	Link up | Link Down; default: **Link up**	Provides information about the WAN link that connects the hotspot to the Internet.
Downlink Speed	integer [1..4294967295]; default: **none**	Maximum downlink speed in Kbps.
Uplink Speed	integer [1..4294967295]; default: **none**	Maximum uplink speed in Kbps.

Venue Name Information

The **Venue Name Information** is used to configure one or more Venue Name values for Venue Name ANQP information. To add a new Venue configuration, click the 'Add' button.

You should see a new entry appear in the Venue Name Information list.

Field	Value	Description
Language Code	string; default: **none**	Two or three character language code (ISO-639).
Venue Name	string; default: **none**	Name of this venue.

Venue URL Information	url; default: **none**	Venue URL to provide additional information corresponding to Venue Name information (the URL should contain protocol).

3GPP Cellular Network Information

The **3GPP Cellular Network Information** section is used to uniquely identify mobile network operators. To add a new mobile operator instance, click the 'Add' button.

You should see a new entry appear in the 3GPP Cellular Network Information list.

Field	Value	Description
Mobile Country Code	integer; default: **none**	Mobile country code (3 decimal digits).
Mobile Network Code	integer; default: **none**	Mobile network code (2 or 3 decimal digits).

Network Access Identifier (NAI) Realm Information

The **Network Access Identifier (NAI) Realm Information** parameters provide information for stations using interworking network selection to allow automatic connection to a network based on credentials. To add a new NAI Realm Information configuration, click the 'Add' button.

You should see a new entry appear in the Network Access Identifier (NAI) Realm Information list.

Field	Value	Description
NAI Realm	url; default: **Link up**	The NAI Realm provides a list of NAI realms corresponding to the Home SPs that can authenticate a client device.
EAP Method	EAP-TLS | EAP-TTLS | PEAP | EAP-FAST; default: **Undefined**	Identifies the EAP method supported by that NAI realm for authentication.
Authentication Parameter	Undefined | Non EAP PAP | Non EAP CHAP | Non EAP MSCHAP | Non EAP MSCHAPV2 | Credential certificate | Credential username/password; default: **Undefined**	EAP method authentication parameter.

Operator Friendly Name

The client device may obtain the **Operator Friendly Name** via GAS/ANQP queries to assist the user during manual hotspot selection. To add a new Operator Friendly Name configuration, click the 'Add' button.

You should see a new entry appear in the Operator Friendly Name list.

Field	Value	Description
Language Code	string; default: **Link up**	Two or three character language code (ISO-639).
Operator's Name	string; default: **none**	Provides a friendly name for the Hotspot Operator.

Connection Capability

The **Connection Capability** section provides information on the status of commonly used communication protocols and ports. To add a new protocol/port configuration, click the 'Add' button.

You should see a new entry appear in the Connection Capability list.

Field	Value	Description
Protocol	ICMP | TCP | UDP; default: **ICMP**	Network protocol type.
Port Number	integer [0..65535]; default: **none**	TCP/UDP port number.
Status	Closed | Open | Unknown; default: **Closed**	Status to be displayed for the selected protocol/port combination.