https://wiki.teltonika-networks.com/view/RUT300_Administration

RUT300 Administration

The information in this page is updated in accordance with firmware version **RUT30X_R_00.07.07.1**.

□

Contents

- 1 Summary
- 2 General
- 3 Date & Time
  - 3.1 Summary
  - 3.2 General
  - 3.3 NTP
    - 3.3.1 Time Synchronization
    - 3.3.2 Time Servers
    - 3.3.3 NTP Server
  - 3.4 NTPD
- 4 User Settings
  - 4.1 Change Password
  - 4.2 System Users
    - 4.2.1 Summary
    - 4.2.2 Groups
      - 4.2.2.1 Group Settings (edit group)
        - 4.2.2.1.1 Examples
    - 4.2.3 Users
      - 4.2.3.1 User Settings (edit user)
    - 4.2.4 Add New User
- 5 Access Control
  - 5.1 General
  - 5.2 PAM
    - 5.2.1 Modify PAM Auth
  - 5.3 Security
- 6 Recipients
- 7 Certificates
  - 7.1 Certificate Generation
    - 7.1.1 Generation Parameters
    - 7.1.2 Certificate Signing
  - 7.2 Certificate Manager
    - 7.2.1 Certificate Import
    - 7.2.2 Certificates, Keys & Requests
  - 7.3 Root CA

- 8 Profiles
  - 8.1 Summary
  - 8.2 Configuration Profiles
  - 8.3 Scheduler
    - 8.3.1 General Configuration
    - 8.3.2 Profile Scheduler Instances
      - 8.3.2.1 Profile Scheduler Instance Configuration
      - 8.3.2.2 Profile Scheduler Instance Example
- 9 Storage Memory Expansion
  - 9.1 USB
    - 9.1.1 Memory Expansion
    - 9.1.2 Enabling memory expansion
    - 9.1.3 Disabling memory expansion
  - 9.2 SSHFS

Summary

This page is an overview of the **Administration** section of RUT300 devices.

General

The **General** section is used to set up some of device managerial parameters, such as changing device name. For more information on the General section, refer to figure and table below.

Field	Value	Description
General Settings		
Language	English | Turkish* | Spanish* | Portuguese* | German* | Japanese*; default: **English**	Changes the router's WebUI language.
Configuration Mode	Basic | Advanced; default: **Basic**	Mode determines what options and configurations are shown. In Basic mode only the essential configurations are shown. In Advanced mode there is greater freedom to configure and access more options.
Device name and hostname		
Device name	string; default: **RUT300**	Device model name.
Hostname	string; default: **Teltonika-RUT300.com**	Device hostname. This can be used for communication with other LAN hosts.
LED Indication		
Enable	off | on; default: **on**	Manages signal strength, LAN and connection status indication LEDs.
Reset Button Configuration		
Min time	integer [0..60]; default: **none**	Minimum time (in seconds) the button needs to be held to perform an action.

Max time	integer [1..60]; default: **none**	Maximum time (in seconds) the button can be held to perform an action, after which no action will be performed.

* Different language packages can be downloaded separately from the **System → Package Manager** page.

Date & Time

Summary

Network Time Protocol (**NTP**) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. This chapter is an overview of the NTP section for RUT300 devices.

General

The **Time Synchronization** section lets you select time zone and synchronize the time.

The figure below is an example of the Time Synchronization section and the table below provides information about the fields contained in that section:

Field	Value	Description
Current system time	time; default: **none**	Current local time of the device.
Sync with browser	-(interactive button)	Click to synchronize device time and time zone to browsers, if your device time or time zone is not correct.
Time zone	time zone; default: **UTC**	The device will sync time in accordance with the selected time zone.

NTP

This section is used to configure NTP client, server and time servers.

Time Synchronization

This section is used to configure the device's time settings.

Field	Value	Description

Enable NTP Client	off | on; default: **on**	Turns NTP on or off.
Save time to flash	off | on; default: **off**	Saves last synchronized time to flash memory.
Force Servers	off | on; default: **off**	Forces unreliable NTP servers.
Update interval (in seconds)	integer; default: **86400**	How often the device will update the time.
Offset frequency	integer; default: **0**	Adjusts the minor drift of the clock so that it will run more accurately.
Count of time synchronizations	integer; default: **none**	The amount of times the device will perform time synchronizations. Leave empty in order to set to infinite.

Time Servers

This section is used to specify which time servers the device will use for time synchronization. To add more time servers to the list, click the 'Add' button.

Field	Value	Description
Hostname	ip | url; default: **0.openwrt.pool.ntp.org**	NTP servers that this device uses to sync time.

NTP Server

The device can also act as an **NTP Server**, providing clock synchronization to other devices in the network. From this section you can turn this feature on or off:

NTPD

The **NTPD** program is an operating system daemon that synchronizes the system clock to remote NTP time servers or local reference clocks. NTPD includes the ability to use this to keep your clock in sync and will run more accurately than a clock on a device not running NTPD. NTPD will also use several servers to improve accuracy. It is a complete implementation of NTP version 4 defined by RFC-5905, but also retains compatible with version 3 defined by RFC-1305 and versions 1 and 2, defined by RFC-1059 and RFC-1119, respectively.

Note: NTPD is additional software that can be installed from the **System → Package Manager** page.

Field	Value	Description
Enable NTPD	off | on; default: **off**	Turns NTPD on or off.
Enable NTP config from file	off | on; default: **off**	Run NTPD with uploaded configuration file.

NTP configuration file	.conf file; default: **none**	Upload a custom configuration file.
Server	ip | url; default: **0.openwrt.pool.ntp.org**	NTP servers that this device uses to sync time.
Enable Server	off | on; default: **off**	Enables NTPD server to make the router act as an NTP server so that it can provide time synchronization services for other network devices.

User Settings

Change Password

The **User settings** section is used to change the password of the current user.

System Users

Summary

The **System Users** page is used to add new user accounts that can access the device with different user credentials than the default ones. The newly added users can be assigned to one of two groups, either of which can be modified to limit WebUI read/write access rights for users belonging to each specific group.

This page is unrelated to SSH users. By default, there is one SSH user named "root" and it shares the same password as the default WebUI user named "admin".

This manual page provides an overview of the Users page in RUT300 devices.

If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should **turn on "Advanced WebUI" mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.

Groups

The **Groups** section lists available user groups of which there are three:

- **root** - highest level of authority. Key elements that define this group:
  - has unlimited read/write access;

- additional users cannot be added to this group;
- access rights for this group cannot be modified.

- **admin** - second highest level of authority. Key elements that define this group:
  - limited read access; by default, users belonging to this group cannot view these pages:
    - System → Users.
  - unlimited write access by default;
  - access rights can be modified.

- **user** - lowest level of authority. Key elements that define this group:
  - no write access;
  - limited read access; by default, users belonging to this group cannot view these pages:
    - System → Users;
    - System → Firmware;
    - System → Reboot.
  - access rights can be modified.

Additional note: you can view and/or edit settings for each group by clicking the 'Edit' button next to them. More on information on how to edit group access settings is located in the following section of this manual page.

Group Settings (edit group)

A group's parameters can be set in its **Group Settings** page. To access the Groups Settings page, click the 'Edit' button next to the group's name. Below is an example of the Group Settings section:

Field	Value	Description
Write action	Allow | Deny; default: **Allow**	Specifies whether to allow or deny write actions for users in the group. Write actions consist of changing configurations and performing certain actions (such as clicking buttons). This field directly correlates with the "Write access" field below it, because the selected write action will apply to pages specified in that field.
Write access	path(s) to page(s); default: • **system/multiusers/change_password**	Path(s) to the page(s) to which the selected "Write action" will be applied. Click the plus symbol to add multiple entries.

Read action	Allow | Deny; default: **Deny**	Specifies whether to allow or deny read actions for users in the group. Read actions consist of viewing pages on the WebUI. This field directly correlates with the "Read access" field below it, because the selected read action will apply to pages specified in that field.
Read access	path(s) to page(s); default: • **services/mobile_utilities/sms/send** • **services/packages** • **system/multiusers/** • **system/flashops/** • **system/backup** • **system/admin/access_control** • **system/cli** • **system/uscripts** • **system/wizard** • **services/packages/upload** • **network/**	Path(s) to the page(s) to which the selected "Read action" will be applied. Click the plus symbol to add more entries.

Examples

The easiest way to master the syntax is to navigate to page that you want to generate a path for and the copy the path from the URL of that page.

For example, to specify the path to the Network → Mobile page, navigate to the page, copy the page's URL address **starting from the symbol "#"** and paste it into one of the access fields:

However, the VPN window contains links to many different types of VPN pages. If you want to specify only one of them, you can do it as well. For example, to to specify the path to the IPsec page, **add "/ipsec" to the path string**:

`services/vpn/`**`ipsec`**

An **asterisk (*)** in the path string means that the every page from that point on is included in that path. For example, to generate a path that includes pages in the Services menu tab:

`services/*`

Or to simply include everything in the entire WebUI (**if this path is combined with *Read action: Deny*, users from that group will not be able to login to the WebUI**):

`*`

Users

The **Users** section lists all created users and provides the possibility to change their passwords and the group they belong to (with the exception of the default user "admin" which always belongs to the *root* group).

By default, there is only one user called "admin":

User Settings (edit user)

Each user's password and group parameters can be set in their **User Settings** pages. To access the User Settings page, click the 'Edit' button next to the user's name.

However, you may want to add a new user at first. This can be done from the Add New User section below:

1. create a username;
2. create a password for the user (must contain at least 8 characters, including at least one upper case letter and one digit);
3. click the 'Add' button;
4. click the 'Edit' next to newly added user.

Below is an example of a newly added user's settings page:

Field	Value	Description
Username	string; default: **none**	Displays the user's name.
New password	string; default: **none**	• Create a new password for the user. The password must contain at least 8 characters, including at least one upper case letter and one digit. • Another option is to use the 'Dice' icon, which generates random passwords.
Confirm new password	string; default: **none**	Repeat the new password.
Group	admin | user; default: **user**	The group to which the user belongs.
Enable SSH access	off | on; default: **off**	Enables SSH access (only for 'root' users).

Add New User

The **Add New User** section is used to create additional users that can access the WebUI. After a new user is added, it will appear in the Users section.

Field	Value	Description
Username	string; default: **none**	A custom name for the new user.
Password	string; default: **none**	• A password for the new user. The password must contain at least 8 characters, including at least one upper case letter and one digit. • Another option is to use the 'Dice' icon, which generates random passwords.

Access Control

General

The **Access Control** page is used to manage remote and local access to device.

Important: turning on remote access leaves your device vulnerable to external attackers. Make sure you use a strong password.

SSH

Field	Value	Description
Enable SSH access	off | on; default: **on**	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	off | on; default: **off**	Turns SSH access from remote networks (WAN) on or off.
Port	integer [0..65535]; default: **22**	Selects which port to use for SSH access.
Enable key-based authentication	off | on; default: **off**	Use public keys for authentication.

WebUI

Field	Value	Description
Enable HTTP access	off | on; default: **on**	Turns HTTP access from the local network (LAN) to the device WebUI on or off.
Enable HTTPS access	off | on; default: **on**	Turns HTTPS access from the local network (LAN) to the device WebUI on or off.

Redirect to HTTPS	off | on; default: **off**	Redirects connection attempts from HTTP to HTTPS.
Enable remote HTTP access	off | on; default: **off**	Turns HTTP access from remote networks (WAN) to the device WebUI on or off.
Port	integer [0..65535]; default: **80**	Selects which port to use for HTTP access.
Enable remote HTTPS access	off | on; default: **off**	Turns HTTPS access from remote networks (WAN) to the device WebUI on or off.
Port	integer [0..65535]; default: **443**	Selects which port to use for HTTPS access.
Ignore private IPs on public interface	off | on; default: **on**	Prevent access from private (RFC1918) IPs on an interface if it has an public IP address.
Certificate files from device	off | on; default: **on**	Choose this option if you want to select certificate files from device. Certificate files can be generated in Certificates section.
Server certificate	.crt; default: **uhttpd.crt**	Server certificate file.
Server key	.key; default: **uhttpd.key**	Server key file.

CLI

Field	Value	Description
Enable CLI	off | on; default: **on**	Turns CLI access from the local network (LAN) on or off.
Enable remote CLI	off | on; default: **off**	Turns CLI access from remote networks (WAN) on or off.
Port range	range of integers [0..65534]-[1..65535]; default: **4200-4220**	Selects which ports to use for CLI access.
Shell limit	integer [1..10]; default: **5**	Maximum number of active CLI connections.

Telnet

Field	Value	Description
Enable Telnet access	off | on; default: **on**	Turns Telnet access from the local network (LAN) on or off.
Enable remote Telnet access	off | on; default: **off**	Turns Telnet access from remote networks (WAN) on or off.
Port range	integer [0..65535]; default: **23**	Selects which port to use for Telnet access.

PAM

Note: PAM is additional software that can be installed from the **System → Package Manager** page.

Modify PAM Auth

Field	Value	Description
Enable	off | on; default: **on**	Turns the PAM auth on or off.
Module	TACACS+ | Radius | Local; default: **Local**	Specifies the PAM module that implements the service.
Type	Required | Requisite | Sufficient | Optional; default: **Optional**	Determines the continuation or failure behavior for the module
TACACS+/Radius: Server	ip4 | ip6; default: **none**	The IP address of the RADIUS server
TACACS+/Radius: Secret	string; default: **none**	RADIUS shared secret
TACACS+/Radius: Port	integer [0..65535]; default: **49**/**1812**	RADIUS server authentication port
Radius: Timeout	integer [3..10]; default: **3**	Timeout in seconds waiting for RADIUS server reply.

Security

The **Security** tab provides the possibility to enable/disable blocking IP's service and delete blocked devices from the list.

IP Block Settings

Field	Value	Description
Enable	off | on; default: **on**	Enable or disable blocking IP's if they have reached the set amount of failed times.
Type	Timed blocking | Permanent blocking; default: **Timed blocking**	You can choose an option of a blocking type.
Fail count	integer [1..1000]; default: **10**	An amount of times IP address can try to access SSH or WebUI before being blocked.
Clean after reboot	off | on; default: **off**	If enabled, blocked loging attempts list will be cleared on device reboot.

Login Attempts

Field	Value	Description
Source	IP address	Shows the IP address from which the connection failed.
Destination	IP address	Shows yours device IP adress
Port (protocol)	Port number	Shows the port number from which the connection failed.
Status	Attempt count | Blocked	Shows the number of failed attempts to connect to device. Indicates whether the source address is blocked or not.
Reset	Check box	Allows you to select multiple IP addresses.
Actions	-(interactive button)	Allows you to select multiple IP addresses.
Unblock all	-(interactive button)	Deletes instance.
Unblock selected	-(interactive button)	Unblocks selected source adresses from the list.

Recipients

The **Recipients** section is used to configure email users, which can later be used along with email related services, such as Events Reporting.

Certificates

The **Certificates** page is used for convenient TLS certificate and key generation and management. Generated files can be exported and used on other machines or locally on this device with functions that use TLS/SSL, such as MQTT, OpenVPN, IPsec and others.

Certificate Generation

The **Certificate Generation** tab provides the possibility to generate TLS certificates required for secure authentication and communication encryption used by some of the devices services.

There are five distinct generation methods (denoted by the selected 'File Type').

1. **Simple** - generates and signs a set of 2048 bit certificate and key files that include:
   - Certificate Authority (CA)
   - Server certificate & key
   - Client certificate & key
   - DH Parameters

   The CA file generated with this option automatically signs the certificates. In short, this option is used for convenience as it doesn't let the user set any additional parameters for the certificate files. Therefore, it should be used only when no other specific requirements are expected.
2. **CA** - generates a Certificate Authority (CA) file. A CA is a type of certificate file that certifies

the ownership of a public key by the named subject of the certificate. In other words, it assures clients that they are connecting to a trusted server and vice versa.
3. **Server** - generates a server certificate and key. A server certificate validates a server's identity to connecting clients, while a key is responsible for encryption.
4. **Client** - generates a client certificate and key. A client certificate validates a client's identity to the server that it's connecting to, while a key is responsible for encryption.
5. **DH Parameters** - generates a Diffie-Hellman (DH) parameters file. DH parameters are used in symmetric encryption to protect and define how OpenSSL key exchange is performed.

Generation Parameters

Generating each type of file requires setting some parameters. This section provides an overview for parameters used in Simple and TLS certificate generation.

Simple file parameters

Field	Value	Description
Hosts	string; default: **none**	Appends hostnames to certificates.
IP addresses	IPv4 address; default: **none**	Appends IPv4 addresses to certificates.

TLS parameters or simply parameters that apply to each (CA, Server, Client, DH) file type are the size and common name of the generated file(s).

Field	Value	Description
Key Size	integer; default: **2048**	Generated key size in bits. Larger keys provide more security but take longer to generate. A 2048 bit is the preferred option.
Name (CN)	string; default: **cert**	Common Name (CN), aka Fully Qualified Domain Name (FQDN) is a parameter that defines the name of the certificate. It should be chosen with care as it is not only used for easier management. For example, the Common Name should typically hostname of the server. It may also be used to differentiate clients in order to apply client-specific settings.

Subject information is not mandatory but can be used as user-friendly way to identify the ownership of certificate files by including such information as the owner's location and company name.

The **Sign the certificate** slider control whether the certificate will be signed automatically or

manually after the generation is complete.

Field	Value	Description
Days Valid	integer; default: **3650**	Length of the signature's validity.
CA File Name	filename; default: **none**	Selects which CA file will be used to sign the generated certificate.
CA key	filename; default: **none**	Selects which CA key file will be used to sign the generated certificate.
Delete Signing Request	off | on; default: **off**	Generation creates additional 'signing request' files (which appear under the Certificate Manager tab) that are later used to sign the generated certificates. When this option is set to 'on', the device deletes the signing request files after the signing process is complete.

A **Private Key Decryption Password** is a parameter used to decrypt private keys protected by a password.

Certificate Signing

The **Certificate Signing** section is used to validate (sign) unsigned certificates.

Field	Value	Description
Signed Certificate Name	string; default: **none**	Name of the signed certificate.
Type of Certificate to Sign	Certificate Authority | Client Certificate | Server Certificate; default: **Certificate Authority**	Specifies what type of file will be signed.
Certificate Request File	file; default: **none**	Specifies the signing request file linked to the certificate.
Days Valid	integer; default: **none**	Length of the signature's validity.
Certificate Authority File	filename; default: **none**	Selects which CA file will be used to sign the generated certificate.
Certificate Authority Key	filename; default: **none**	Selects which CA key file will be used to sign the generated certificate.
Delete Signing Request	off | on; default: **off**	Generation creates additional 'signing request' files (which appear under the Certificate Manager tab) that are later used to sign the generated certificates. When this option is set to 'on', the device deletes the signing request files after the signing process is complete.
Hosts	string; default: **none**	Appends hostnames to certificates.

IP addresses	IPv4 address; default: **none**	Appends IPv4 addresses to certificates.
Sign	- (interactive button)	Signs the certificate on click.

Certificate Manager

The **Certificate Manager** page displays information on all certificate and key files stored on the device and provides the possibility export these files for use on another machine or import files generated elsewhere.

Certificate Import

The **Certificate Import** section provides the possibility to import certificates and files generated on another machine. To upload such a file simply click 'Browse' and locate the file on your computer, it should then start uploading automatically.

Certificates, Keys & Requests

The **Certificates**, **Keys** and **Requests** section display files generated on or imported to the device along with the most important information related to them.

By default, the lists are empty. A set certificates generated using 'Simple' file type would look something like this:

The 'Export' buttons are used to download the files from the device onto your local machine. The 'X' buttons located to the right of each entry are used to delete related files.

Root CA

The **Root CA** section is used to add a root CA certificate file to the device. There is a default file already preloaded on the device which will be overwritten by any uploaded file. The certificates must be in .pem format, maximum file size is 300 KB. These certificates are only needed if you want to use HTTPS for your services and the default file should be sufficient in most cases.

Profiles

Summary

Configuration **profiles** provide a way to create multiple distinct device configuration sets and apply

them to the device based on current user requirements. This chapter is an overview of the Profiles page in RUT300 devices.

Configuration Profiles

This section displays user defined **configuration profiles**:

To create a new profile, configure the device in accordance with your needs, go to this page, enter a custom name for the profile and click the 'Add' button. You can also choose to create a profile without any previous configurations. A new profile with the given name will appear in the "configuration profiles" list:

The 'Apply' button applies the adjacent configuration on the device.

Scheduler

The **Profile Scheduler** provides a possibility to set up a schedule of when the device should use one profile configuration or another.

Check Profile Scheduler Instance Example to get a better understanding at how Profile Scheduler Instances works.

General Configuration

The **General Configuration** section is used to enable the Scheduler itself. Created instances won't work unless this option is turned on.

Profile Scheduler Instances

The **Profile Scheduler Instances** section allows you to create profile Instances to be enabled during specific time intervals. To add a new Instance click **Add** button.

Note: new Instance can only be created if there is at least one custom profile created.

Profile Scheduler Instance Configuration

This page is used to configure profile, time and day of selected scheduler instance. Refer to the

figure and table below for information on the Profile Scheduler Instance Configuration fields:

Field	Value	Description
Enable	off | on; default: **off**	Enable selected instance for scheduler.
Profile	profiles; default: **none**	Select profile which will be applied during specified time interval.
Interval Type	Weekdays | Month Days; default: **Weekdays**	Depending on your needs select whether you want to configure weekdays or specific month days.
Start Time	time; default: **12:00**	Enter time of the start of interval in which scheduler will switch profiles.
End Time	time; default: **12:00**	Enter time of the end of interval in which scheduler will switch profiles back.
Interval Type: Weekdays		
Start Day	Weekday [Monday..Sunday]; default: **Sunday**	Select a day of the start of interval in which scheduler will switch profiles.
End Day	Weekday [Monday..Sunday]; default: **Sunday**	Select a day of the end of interval in which scheduler will switch profiles back.
Interval Type: Month Days		
Start Day	Day of month [1..31]; default: **1**	Select a day of the start of interval in which scheduler will switch profiles.
End Day	Day of month [1..31]; default: **1**	Select a day of the end of interval in which scheduler will switch profiles back.
Force last day	off | on; default: **off**	Force intervals to accept last day of month as valid option if selected day doesn't exist in ongoing month.

Profile Scheduler Instance Example

Scheduler will use *profile instance* if it is enabled **and** it's time interval matches device's date, otherwise *default* profile will be used.

Example - we have 3 profiles in total:

- default
- Profile A
- Profile B

We create profile instances for Profiles A and B:

- Profile A: 08:00 - 11:00
- Profile B: 13:00 - 20:00

During 11:00 - 13:00 and 20:00 - 08:00 *default* profile will be used.

Storage Memory Expansion

USB

The **Storage Memory Expansion** function provides the possibility to expand the device's flash memory with a USB mass storage device.

Memory Expansion

You can **expand the flash memory** of this device with a USB Mass Storage Device (MSD) and use the extra memory to install additional software packages. This section provides instruction on how to do just that. However, there are a few prerequisites and warnings to take note of before using memory expansion.

To be eligible for memory expansion, the USB MSD must meet the following restrictions.

- The MSD must be the last one (chronologically) inserted.
- If you are using a USB hub, the target MSD must be the last one attached to the hub.
- **No important data on the MSD as it will be wiped during expansion setup!**

When expansion is enabled, **do not detach the USB device as this will delete the data stored on it**. Changes made to the device configuration while expansion was enabled will disappear after it is disabled.

Enabling memory expansion

To successfully expand the flash memory of your device follow the steps described below.

1. Attach a USB Mass Storage Device (MSD) to the USB connector on the device and go to the Services → Storage Memory Expansion page.
2. Set the 'Enable storage expansion' slider to 'on' and click 'Save & Apply'.
3. You will see a pop-up asking for confirmation. Take note that if you continue from this point on:
   - your **USB device's memory will be wiped** and formatted to ext2 format;
   - your device's **current configuration will be backed up** and restored to this point if the USB drive is removed or memory expansion is disabled;
   - the entire procedure **may take a very long time** and includes a reboot at the end; exact time will vary depending on the size of the MSD (larger size will take longer; for example, using a 128 GB drive will take about 2 hours to fully set up, while a 16 GB will only take about 5 minutes).

   Click 'Continue' to proceed.
4. If all is in order you should see a 'Formatting MSD...' message on the screen. This indicates that the MSD is being formatted and integrated with the system. This procedure can take a long time and ends with a reboot of the device.

5. Your device's flash memory will be expanded once the reboot has finished. In order to check, log in to the WebUI and look to the 'System' widget in the 'Overview' page. Hover your mouse cursor over the 'FLASH' memory indicator; you should see an increase to the device's flash memory.

Disabling memory expansion

To successfully disable memory expansion follow the steps described below.

1. Go to the Services → Storage Memory Expansion page.
2. Set the 'Enable storage expansion' slider to 'off' and click 'Save & Apply'.

3. You will see a pop-up asking for confirmation. Take note that if you continue from this point on:
    - your **USB device's memory will be wiped** and formatted to NTFS format;
    - your **device's configuration will be restored** to the point it was before memory expansion;
    - the entire procedure **will take up to 2 minutes** including a reboot.

   Click 'Continue' to proceed.

4. If all is in order you should see a 'Formatting MSD...' message on the screen. This indicates that the MSD is being formatted and detached from the system. This procedure can take up to a couple of minutes and ends with a reboot of the device.

5. Your device's flash memory will be restored to normal once the reboot has finished. In order to check, log in to the WebUI and look to the 'System' widget in the 'Overview' page. Hover your mouse cursor over the 'FLASH' memory indicator; you should see your device's flash memory return to its regular size.

SSHFS

SSHFS is a tool, which allows you to mount a remote filesystem (in remote SSH server) to your RUT300 device using SSH. This service is safe to use as it authenticates connections and encrypts them.

SSHFS configuration consists of setting up authentication, port and mount information parameters. Below is an example oh the SSHFS configuration page.

Field	Value	Description
Enable	off | on; default: **off**	Turns the SSHFS service on or off.
Hostname	string; default: **none**	Hostname of the remote SSH server.
Port	integer [0..65535]; default: **none**	Port of the remote SSH server.

Username	string; default: **none**	Username of the remote SSH server.
Password	string; default: **none**	Password of the remote SSH server.
Mount Point	filepath; default: **/sshmount**	Mount point of remote file system **in the RUT300**. Remote file system has to be mounted at root **/** level. By default the remote file system will be mounted on **/sshmount**, directory will be automatically created if does not exist yet.
Mount Path	filepath; default: **/home/**	Mount path **in the remote SSH server**. For example, if SSH server is hosted on Ubuntu operating system, the Mount Path could look like this (depending on your needs): **/home/username/**