Generate RMS Connect link API example

□

Contents

Introduction

Using the RMS API allows users to automate tasks and integrate RMS into their solutions. In this guide, an example will be provided that step-by-step shows a way to apply the RMS API to create and fetch RMS Connect links.

Such an application could be used to integrate RMS connect link generation into your solution, which would allow you to access devices faster and from a native device control solution.

All documentation of the RMS API can be found here - https://developers.rms.teltonika-networks.com/

This example only includes using Personal Access Tokens to use the API. The RMS API also allows for Application Authentication, used specifically in applications that can use RMS as an OAuth provider.

Two-Factor Authentication

Firstly, to create a Personal Access Token, your account must have Two-Factor Authentication enabled.

This can be done by going to your RMS Account settings and then the Security page. Any Authentication type (other than None) is viable.

Once Two-Factor authentication is enabled, you can then head over to the API → Access tokens page of your Account settings to begin creating a Personal Access token.

Add a new access token

Once there, simply press Add new access token.

Next, input a name for this access token and select the necessary Scopes. Scopes are permissions – what the access token will be capable of doing in your account. For this example, we will be selecting these scopes:

- **devices:read**
- **device_remote_access:read**
- **device_remote_access:write**

This will give the specific RMS API token the rights to read information about devices, and create and read information about RMS connect devices. After selecting the necessary scopes, press Save Personal Access Token – you will be shown a table containing your Personal Access Token. WARNING: This is the only time the created access token will be shown, make sure to copy it, as you will not be able to see it again.

Now that we have the access token, we can now use the RMS API. All information about each API endpoint can be found in the **API reference**.

There are multiple ways to use an API, for this example, we will be using Postman.

Setting up Postman

To start using post efficiently you can download the RMS API Reference YAML file which you will be able to upload to your Postman desktop application by simply clicking the import button in the desktop app and then uploading the downloaded YAML file.

Adding RMS API access token to Postman

After that, you will be able to set authorization for RMS API from Postman. To do this:

1. Click on the API button;
2. Select "RMS API" from the list;
3. Go to the "Authorizations" tab;
4. Select **Type** as "Bearer Token";
5. Enter your saved **RMS API token** to the **Token** field;

Setting up authorization for API calls

This will allow us to copy in Bearer token in one place, which API calls will be able to inherit. To set this up, whenever you open a new API call, go to the **Authorization** tab and select the **Type** as "**Inherit from parent**".

Searching for API calls

To follow this configuration example more easily, you can search for all of the API calls in the list:

Getting the device ID in RMS

To get the ID of the device, for which we will want to generate RMS connect remote accesses and generate links for them, we first need to execute **GET /devices** API call called **Get all device** in the "Postman" collection list.

To get the RMS device ID we need to make this call with API call keys: **fields** and **q**. **Fields** will make it so that the response will only contain fields which we entered and **q** will make it so that only the device with entered serial number we entered is outputted.

The parameters and the response can be seen in the following image:

Field "id" in the response string is the device ID in RMS.

Adding a new remote device

This section will tell you how to a new remote device to RMS Connect.

To add a new remote device we will need:

- Device ID of Teltonika Networks device in RMS;
- LAN IP address of the device we will be creating the remote to;
- The port that is used to reach that service;
- Name of the protocol. The currently supported protocols are:
    - HTTPS
    - HTTP
    - SFTP
    - RDP
    - SSH
    - Telnet

The call needed to add a remote access device/service is **Post /devices/remote/access** and can be found by name **Create a remote access configuration** in the collection list. This API call only needs to have a quest body and no keys. An example request body to add remote access to the router WebUI and the response after sending the call:

This will create a remote access configuration for which we will be able to generate RMS Connect links to access the devices and/or services remotely.

NOTE: It is recommended to use unique names for each remote access configuration within each router to allow for better management of remote access configurations.

Getting the remote access ID

After the creation of the remote access configuration, it was assigned a unique ID, which we need to know, to be able to generate links to that specific remote access.

For this process API call **GET /devices/remote-access** and in the API call collection it is called **Get all device's remote access configurations**. To get the remote access ID for the newly created remote access configuration, the best way would be to filter by the device ID and the name of your new remote access configuration.

An example of the API call can be seen below, the remote access id will be shown in the field called "id".

Generation of RMS Connect link

When the remote access ID is known, we can generate the remote access link with the RMS API call **POST /devices/connect** that in the API collection is called **Start an RMS Connect session**. This call will require both the variable keys and the request body.

The only key required is **access_id** which will be used to identify for which remote access configuration the link will be created.

The request body needs to contain the **duration** in seconds for how long the link will be available. There is no limit to the maximum value but note, that the time standard has some limits.

After this call is completed the RMS connect link is now generated.

Getting the remote access link

After the link has been created, we can use the RMS API call **GET /devices/connect/:access_id/sessions** which in the API collection is called **Get RMS Connect sessions**. This call will display all of the links that are generated from the specified remote access ID. Field **Active** will make it so only active links are outputted for the **access_id** that is provided.

Congratulations, you can now access your remote device using the link you generated using RMS API.