Donyx DRM
User's guide

Table of contents

1. Introduction **3**
1.1. General Information and Functions 3
1.2. System Requirements 4
1.3. System Registration 4
1.4. DRM Client 4
2. User Roles **5**
3. Interface Overview **7**
3.1. Devices 7
3.1.1. Dashboard 7
3.1.2. Device Profile 10
3.1.3. Search and Filters in the **Devices** Section 13
3.1.4. Device settings 14
3.1.5. Editing Multiple Devices 15
3.1.6. Adding a New Device 17
3.2. Events 19
3.2.1. Search and Filters in the **Events** Section 19
3.3. Actions 21
3.3.1. Search and Filters in the **Actions** Section 21
3.3.2. Action Editing 22
3.3.3. New Action 23
3.4. Files 26
3.4.1. Search and Filters in the **Files** Section 27
3.4.2. Viewing File Information 27
3.4.3. Adding a New File 28
3.5. Administration 29
3.5.1. Users 29
3.5.2. Search and Filters in the **Users** Section 29
3.5.3. User Editing 30
3.5.4. New User 31
3.5.5. User Settings 32
3.5.6. Password Reset 33
3.5.7. Settings 34
3.5.8. Notification 38
3.5.9. Logs 42
3.5.10. Security 43
4. Customer Support **44**

1. Introduction

This document describes the **DRM** system, designed for centralized data collection and management of Donyx routers and network servers.

Each router model has its own documentation set. For information on the operation of the devices themselves, please refer to the corresponding user's guide.

1.1. General Information and Functions

The DRM system is designed for centralized configuration management of Donyx routers, enabling monitoring of network equipment and infrastructure status.

The DRM system provides the following core functionality:

- Monitor the status of device groups or individual Donyx routers. The user has access to information such as device status (online/offline), last response time, uptime, and data on CPU usage, LAN interfaces, loopback, routing, etc.
- Centralized firmware update for individual routers or groups of devices within the same hardware series.
- Send reboot and factory reset commands to routers. The built-in scheduler allows for configuring command execution intervals.
- Create rules for generating device backups and system logs.
- Manage configurations of routers connected to the system.

All system operations are performed remotely via a web interface accessible through a browser at drm.donyx.com. The client component is preinstalled in the router firmware.

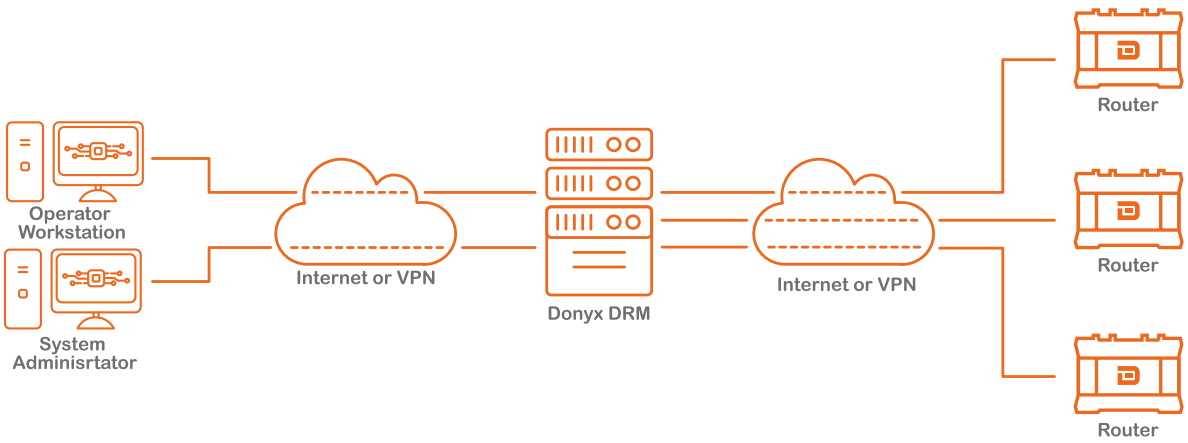


Figure 1. Organization Principle of the Donyx DRM Router Management System

The modular architecture of the Donyx DRM system allows for functionality customization to align with specific business objectives.

1.2. System Requirements

Access to Donyx DRM is provided via a web browser on workstations with Internet connectivity:

- **PC** — running Windows, Linux, macOS, or similar operating systems.
- **Web Browser** — Opera, Firefox, Chrome, Safari, etc. (Internet Explorer is not supported).

1.3. System Registration

There are two ways to register in the Donyx DRM system:

- Go to the self-registration page, fill in the fields, and wait for the email
- Send a request to technical support at support@donyx.com. The email must include the full company name (including legal form), Tax Identification Number (TIN), the employee's full name, phone number and the email address to which the access credentials should be sent.

To create an additional domain for your organization, please contact technical support at support@donyx.com.

1.4. DRM Client

Connecting the router to Donyx DRM is performed via the device's local settings in the *service/drm-client* section. The configuration involves specifying the *Server* address that the router will connect to. Connection integrity is maintained through periodic *Keepalive* messages, and the agent regularly pushes its full status to the server based on the *Force Update* interval.

All communication is secured using the provided *Encryption Key* to ensure data integrity and confidentiality.

Table 1. **Fields in the DRM-client menu**

Field	Description
Disabled	Enables or disables the service.
Server	The address of the Donyx DRM server (*drm.donyx.com*). A UDP port can optionally be specified (default: *11000*).
Force Update	The interval for updating router information on the server.
Keepalive	The interval at which the router sends messages to the server to confirm it is online.
Encryption Key	Pre-shared key (verified via SHA-256).

2. User Roles

The DRM system implements role-based access control for device management. Three roles are available: Administrator, Assistant, and Operator.

Devices are organized into virtual groups. Each group can be assigned one or more Administrators.

Access rights segmentation helps protect the network from unauthorized changes to device operation.

Administrator

The Administrator has unrestricted permissions to perform all actions within the system, including:

- device onboarding;
- software upload for deployment;
- remote command execution;
- device grouping by tags and/or models for improved search and management;
- configuration of device access groups;
- device reboot operations;
- user management within the assigned domain.

Assistant

The Assistant is authorized to perform the following actions:

- Send commands.
- Update firmware.
- Configure settings.
- Customize the status page.
- Create new notifications.
- Change passwords and edit users with the **Operator** role only.



All tasks in the **Actions** menu require Administrator approval.

Assistant does **not** have permission to:

- Delete devices.
- Create users.
- Delete files.
- Delete or modify existing notifications.

Operator

A limited role with view-only access. System menu is view-only. Sections with sensitive data are hidden.

Users can delete their own accounts from the system. This action cannot be undone.

The option is available in the **User Settings** → **Profile** section. To access the section, click the  icon.

3. Interface Overview

3.1. Devices

3.1.1. Dashboard

The **Devices** tab displays information on the status of connected devices, including the total count and the number of devices currently online.

At the top of the section, device information is displayed as blocks.

Click the button to open the list of toggles used to manage block visibility on this page.

You can rearrange the blocks by dragging and dropping them to the desired positions.

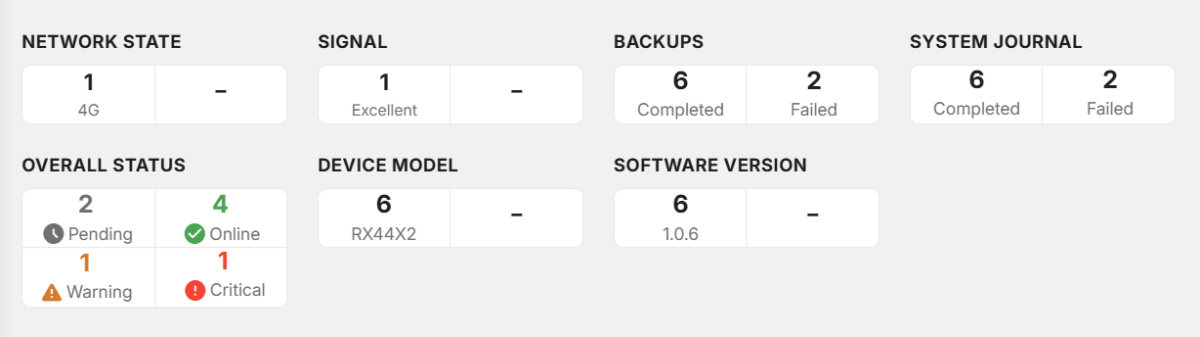


Figure 2. Dashboard

OVERALL STATUS — The status of all connected routers:

Pending	The device has been added to the system but has not yet established a connection or transmitted data.
Online	The device is active and transmitting data regularly. Assigned if the last message from the device was received within the **online→warning** interval (recommended minimum: 15 min).
Critical	No data has been received from the device for an extended period; connection is likely lost. Assigned if the device has not sent messages for longer than the **warning→critical** interval (default: 10080 min, recommended minimum: 15 min).
Warning	The device has not connected recently, but the timeout is not yet critical. Assigned if the last message was received in the interval between **online→warning** and **warning→critical**.

The **online→warning** and **warning→critical** time thresholds can be adjusted to meet specific system requirements. These parameters are located in the **Administration → Settings** section.

SIGNAL — Cellular network signal strength. Displays the number of devices for each signal level:

Excellent	Best possible signal level.
Normal	Standard signal level.
Mid Cell	Acceptable signal level.
Cell Edge	Worst possible signal level.

NETWORK STATE — Data transmission technology. Displays the number of cellular modules for each network mode:

2G	Registered on a 2G network.
3G	Registered on a 3G network.
4G	Registered on a 4G network.
Other	Any other value reported by the device.

DEVICE MODEL — All connected device models. Displays the number of devices for each model:

Example: **RX44X2**	The model name reported by the device.

SOFTWARE VERSION — Firmware version of connected devices. Displays the number of devices for each software version:

Example: **1.1**	Version number of the firmware installed on the router.

BACKUPS — The current status of backup creation. Displays the number of routers for each status:

Completed	Executed successfully.
Failed	Execution error or the deadline has expired.

SYSTEM JOURNAL — The current status of event log generation. Displays the number of routers for each status:

Completed	Executed successfully.
Failed	Execution error or the deadline has expired.

SENSORS — data received from built-in and external sensors, displays the number of devices for each sensor state:

Clicking on a field in this section applies a filter to the device list. To search for a specific device or group by model name, use the search bar.

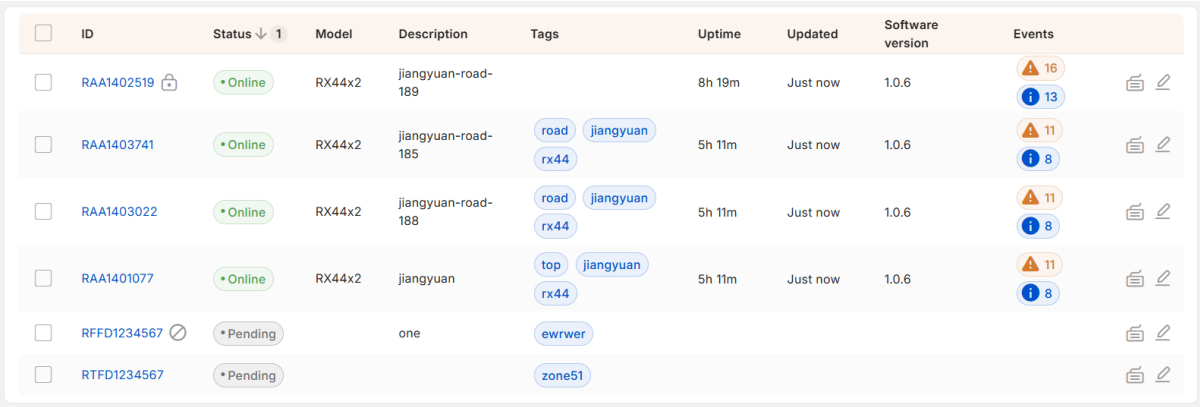
The icon indicates that data encryption is enabled for transmitted traffic.

The icon indicates that the device is denied access to the system.

This section allows monitoring device status. Device status information is updated upon interface changes or at a specified frequency (configured via the router's web interface).

At the bottom of the section, information about connected devices is displayed in a table format.

Clicking the **Columns** button opens a list of toggles to control the visibility of columns in this table.



ID	Status	Model	Description	Tags	Uptime	Updated	Software version	Events
RAA1402519	Online	RX44x2	jiangyuan-road-189		8h 19m	Just now	1.0.6	16 13
RAA1403741	Online	RX44x2	jiangyuan-road-185	road jiangyuan rx44	5h 11m	Just now	1.0.6	11 8
RAA1403022	Online	RX44x2	jiangyuan-road-188	road jiangyuan rx44	5h 11m	Just now	1.0.6	11 8
RAA1401077	Online	RX44x2	jiangyuan	top jiangyuan rx44	5h 11m	Just now	1.0.6	11 8
RFFD1234567	Pending		one	ewrwer				
RTFD1234567	Pending			zone51				

Figure 3. Device Table View

Selecting one or more devices in the list activates buttons for the following group operations:

- **Action** — Assigns a new action to all selected devices. Clicking this button redirects to the **Actions** section for further configuration.
- **Edit** — Enables simultaneous (bulk) modification of parameters for the selected devices. This function allows for editing descriptions, tags, or changing the block status.

Clicking the **Download** button downloads a CSV file containing information on all devices in the domain.
Additionally, device descriptions and interface data are downloaded in JSON format. The file format is compatible with most spreadsheet editors (Microsoft Excel, LibreOffice Calc, etc.), allowing for data analysis.

The exported file is intended exclusively for analytics and is not suitable for the **Multiple add** function (bulk device import)!

3.1.2. Device Profile

Clicking on the router identifier displays detailed information about the device's status.

The time displayed in the **Updated** field indicates when the DRM system last received information from the router.

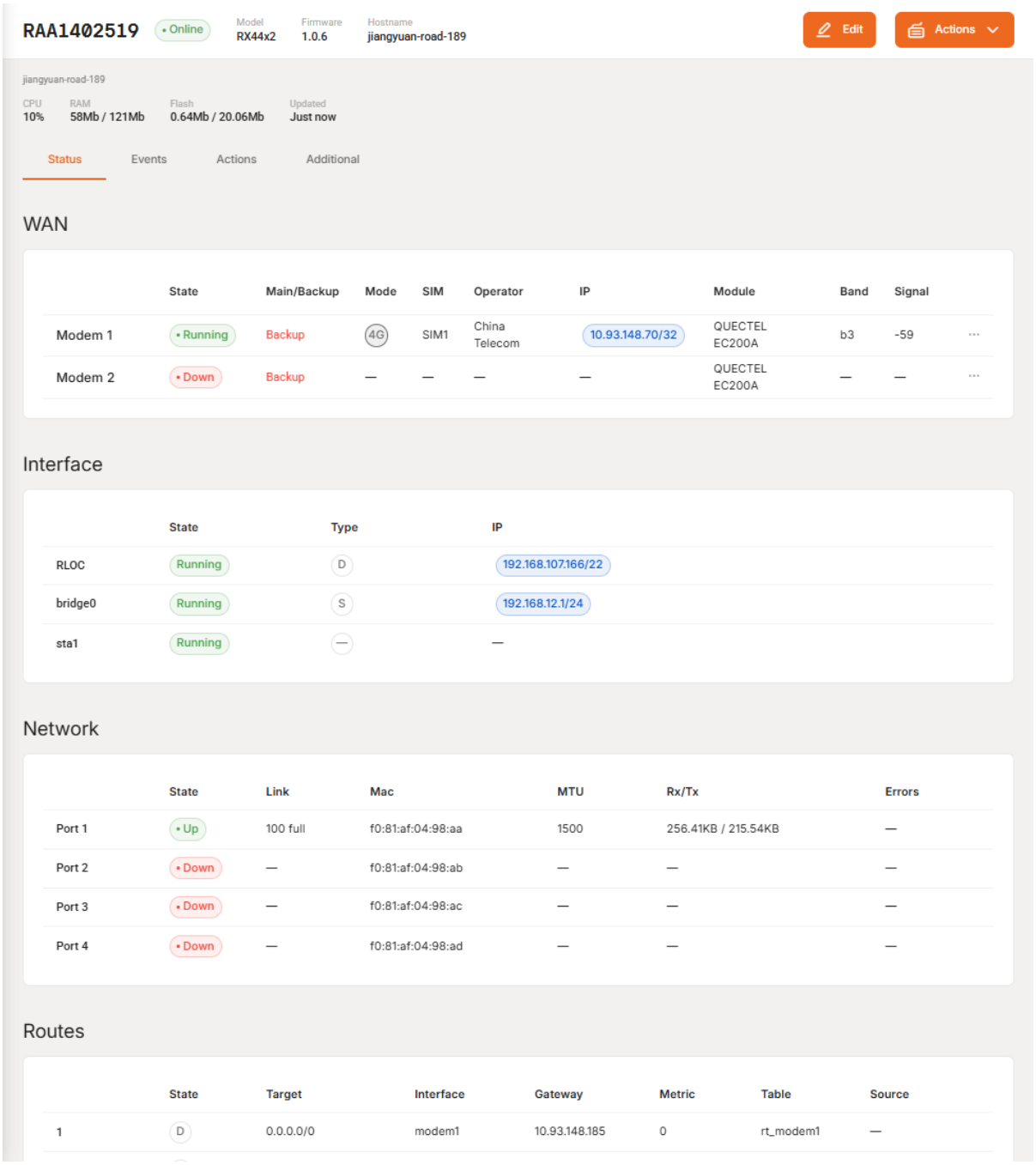


Figure 4. Device Profile View

The section displays general device information, including the router model, firmware version, hostname, assigned tags, CPU status, interface and routing details, flash storage usage, and RAM utilization. Depending on the enabled services, additional blocks for tunnels and other interfaces may also be displayed.

The availability of specific fields depends on the device hardware configuration and the supported hardware features, modules, and sensors.

- **WAN**

Modem connection parameters:

- Current modem connection status.
- Role of the modem in the system.
- Cellular network technology currently in use.
- Active SIM slot number.
- Cellular operator name to which the modem is connected.
- IP address assigned by the operator for internet access.

Hardware and signal information:

- Model and firmware version of the embedded modem module.
- Frequency band currently used by the modem.
- Cellular signal strength (typically displayed as a bar, percentage, or in dBm).
- Unique International Mobile Equipment Identity (IMEI) of the modem.
- Unique Integrated Circuit Card Identifier (ICCID) of the SIM card.
- Unique International Mobile Subscriber Identity (IMSI) linked to the SIM card.

Usage statistics:

- Volume of data received (Rx) and transmitted (Tx) via the modem during the current session.
- Uptime since the last successful network connection.

- **Interface**

Information about configured network interfaces:

- Service interface names (e.g., *lan*, *loopback*, *wan*).
- Interface status.
- Connection type.
- Interface IP address.

- **Routes**

Information about the routing table used by the router:

- Route status.
- Destination network address or host IP.
- Network interface used for routing.
- Next hop gateway IP address.
- Route priority (metric).
- Routing table identifier.
- Routing source IP address.

The list of interfaces depends on the services enabled or disabled on the router. Therefore, this section may contain additional information (blocks describing other interfaces, tunnels, etc.).

Additionally, editing the selected device and assigning a new action to it are available within this section.

3.1.3. Search and Filters in the Devices Section

In the **Devices** section, the table supports sorting by any column and data display management:

- **Sorting:** To sort the list, click the header of any column. Selected columns are marked with numbers indicating sorting priority.
- **Quick Search:** To find a device, enter text in the search field. The search is performed based on matches in the *Identifier*, *Model*, *Description*, *Tags*, and *ICCID* columns.
- **Filters:** Use drop-down lists and the filter panel to select records by specific tags or event types.

These tools can be combined. For example, it is possible to find all devices with the tag "DEPOT" that contain the street name in the description, and sort them by the date of the last event.

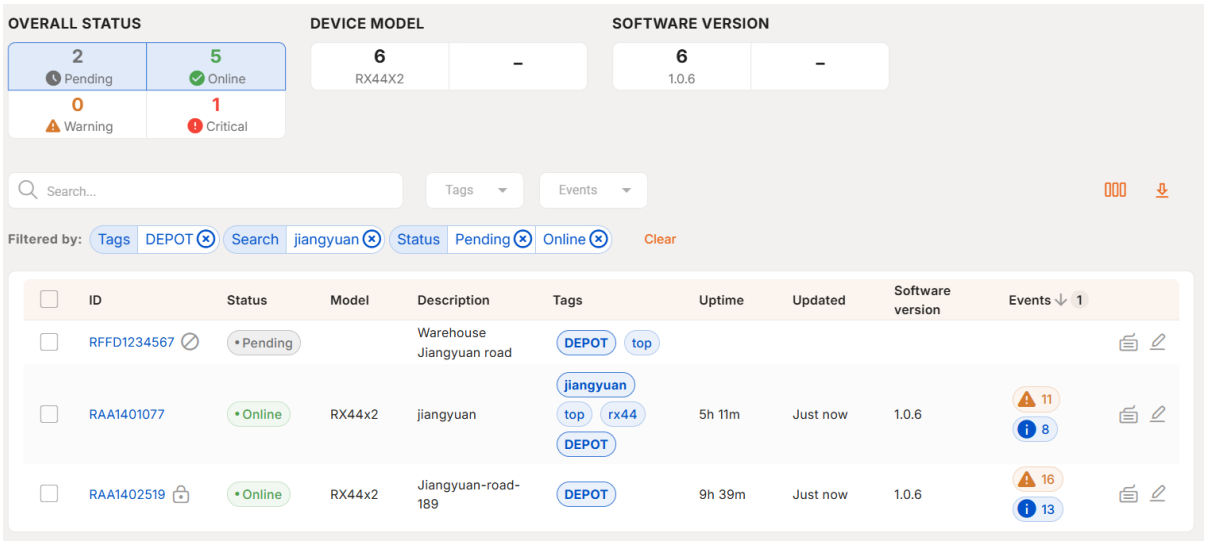


Figure 5. Filtering by Parameters Example

Filters affect data display only within the sections where they are applied.

3.1.4. Device settings

To open device settings, click the icon.

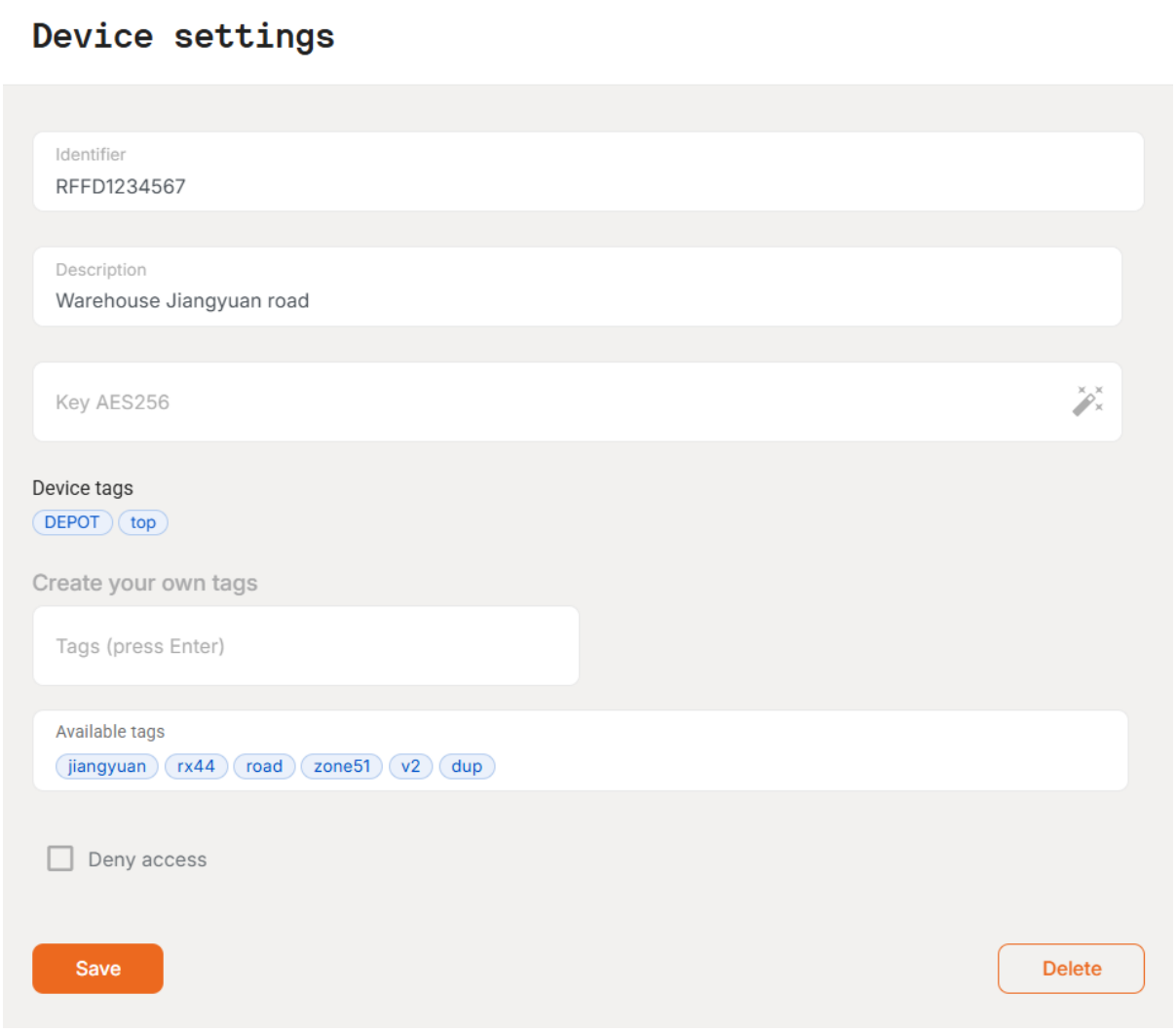


Figure 6. Device Settings View

A description of the fields within the **Device settings** menu is provided in the table below.

Table 2. **Fields in the Device settings menu**

Field	**Description**
Identifier	Device serial number.
Description	Device comment or description.
AES256 Key	256-bit key.
Tags	Labels for quick sorting and searching. Maximum length per tag is 25 characters.

Access for selected devices can be restricted using the **Deny access** checkbox. Upon blocking, the device's status changes to *Critical* after the **warning→critical** time interval, which is configured in the

Administration → **Settings** section. A blocked device is marked in the table with the ⊘ icon.

After completing the fields, click **Save**.

To delete a device, click the **Delete** button, wait for it to turn red, and click it again to confirm. Upon deletion, the device is removed from the system and can no longer exchange data with the application.

3.1.5. Editing Multiple Devices

To edit parameters for several devices simultaneously, select them from the list using the checkboxes.

Once at least one device is selected, the Edit button appears above the table. Click it to open the editing form.

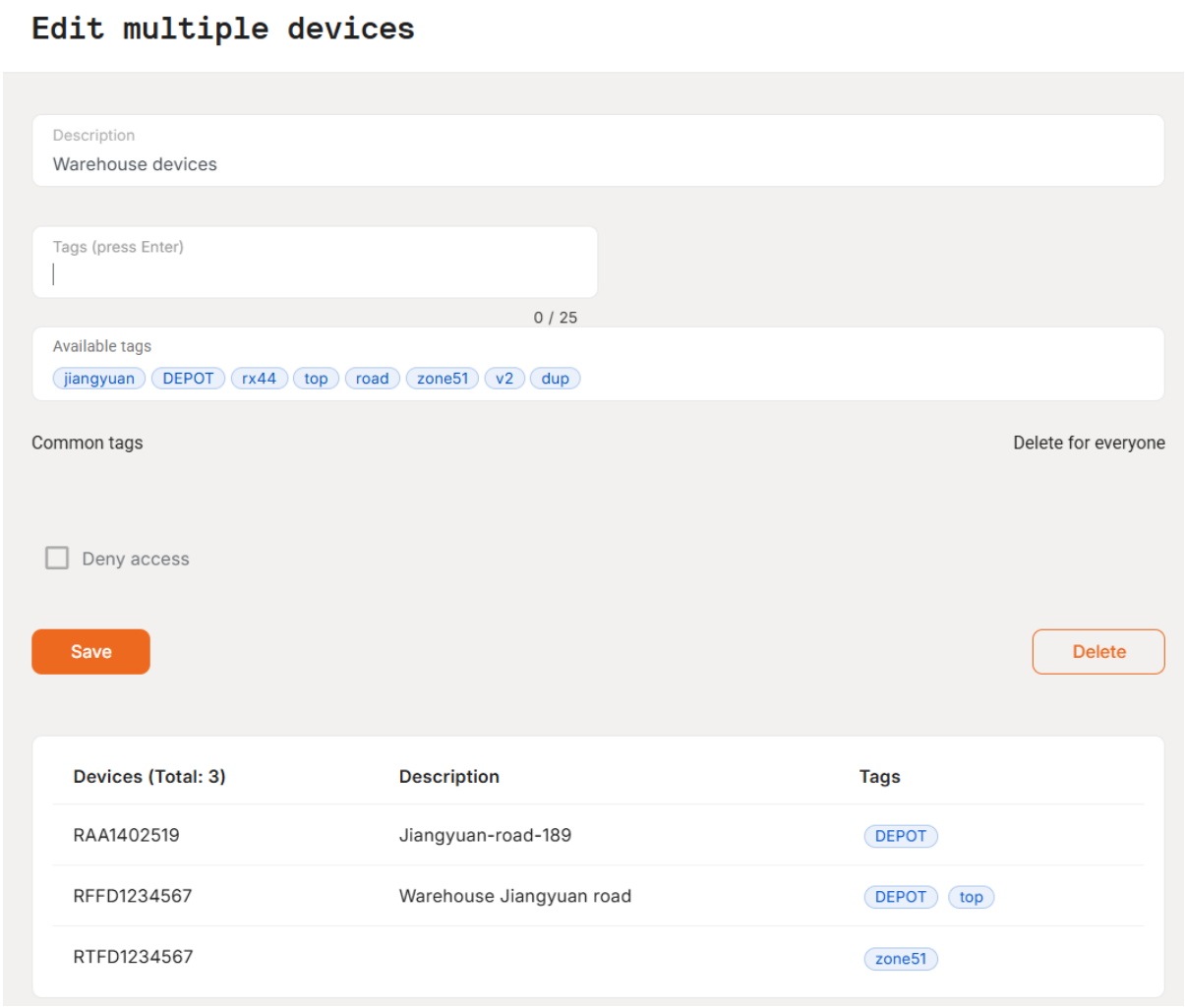


Figure 7. Edit Multiple Devices View

Table 3. **Fields in the Edit multiple devices menu**

Field	Description
Description	A comment field to facilitate device identification (e.g., device location).
Tags	A field for assigning tags used for quick filtering and grouping.
Devices	Serial numbers of the selected devices and their total count.

Access for selected devices can be restricted using the **Deny access** checkbox. Upon blocking, the device's status changes to *Critical* after the **warning→critical** time interval, which is configured in the **Administration → Settings** section. A blocked device is marked in the table with the ⊘ icon.

When editing multiple devices simultaneously, the **Deny access** checkbox is unchecked by default.

After completing the fields, click **Save**.

To delete the selected devices, click the **Delete** button, wait for it to turn red, and click it again to confirm. Upon deletion, the devices are removed from the system and can no longer exchange data with the application.

3.1.6. Adding a New Device

The function to add new devices is restricted to users with the **Administrator** role.

To add a new device, click the + Add device icon located at the top of the **Devices** section.

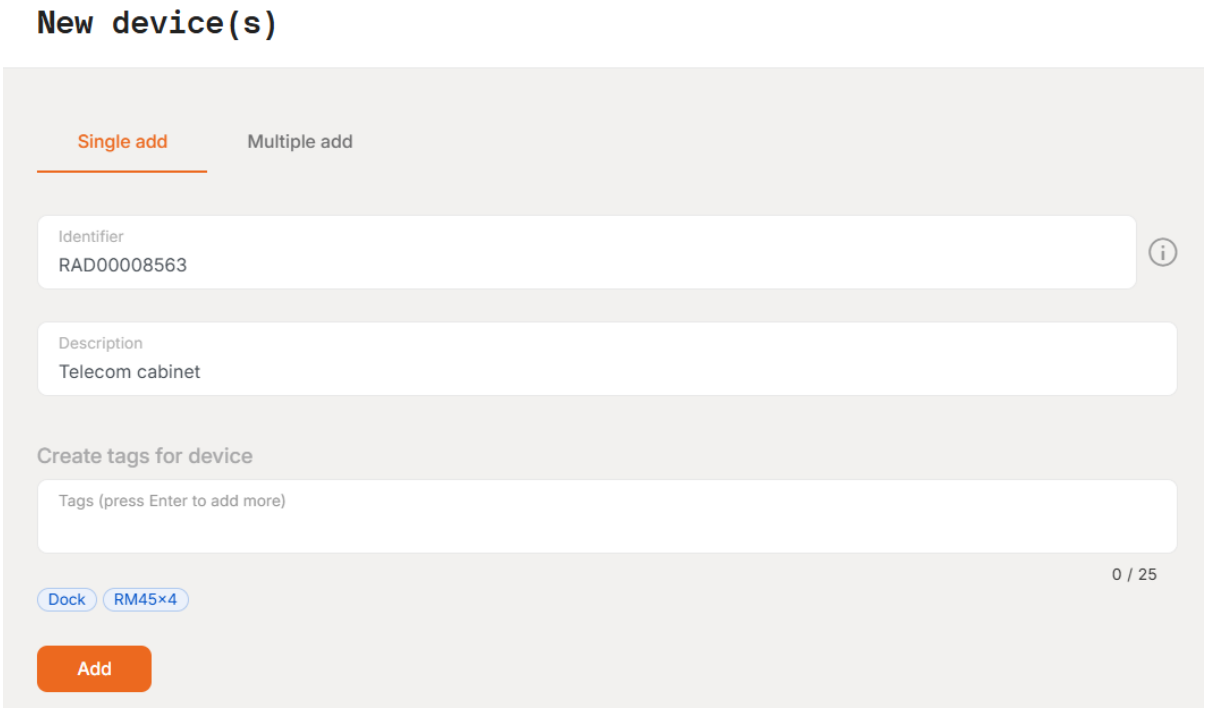


Figure 8. Add New Device View

Single Add

To add devices individually, complete the following fields in the displayed menu:

- Identifier — The serial number of the device (typically located on the back panel). This is a mandatory parameter.
- Description — Explanatory information to assist in identifying the device. This is an optional parameter.
- Tags — Tags assigned for quick search or grouping of the device. This is an optional parameter.

After completing the required fields, click **Add**.

Multiple Add

The system provides a feature for bulk device import using a file containing a list of identifiers. The file must be in CSV format with UTF-8 encoding. The following fields are supported: *IDENT;TAGS;DESCR*.

Table 4. **Field descriptions for bulk device import**

Field	Description
IDENT	Device identifier (Serial Number).
TAGS	Comma-separated list of tags. Tags must consist of 3 to 25 Latin letters, digits, or the following symbols: _, **-**. Spaces within tags are not permitted (they will be automatically removed during import).
DESCR	Device description. Cyrillic characters are permitted.

Example content of the import file (.csv)

```
RAB0402519;DEPOT,access;Testing X-series
RFGG1000107;;
RAA00008563;;Testing S-series
RAGH1000100
```

After uploading the file, click **Add from file**.

3.2. Events

The **Events** tab displays alerts generated by the services, sensors, and other devices connected to the router. The system records audit information regarding the alert reception time and the user who processed it.

Events are categorized into two sections: **New** contains events requiring attention, while **All events** displays all occurrences related to connected devices.

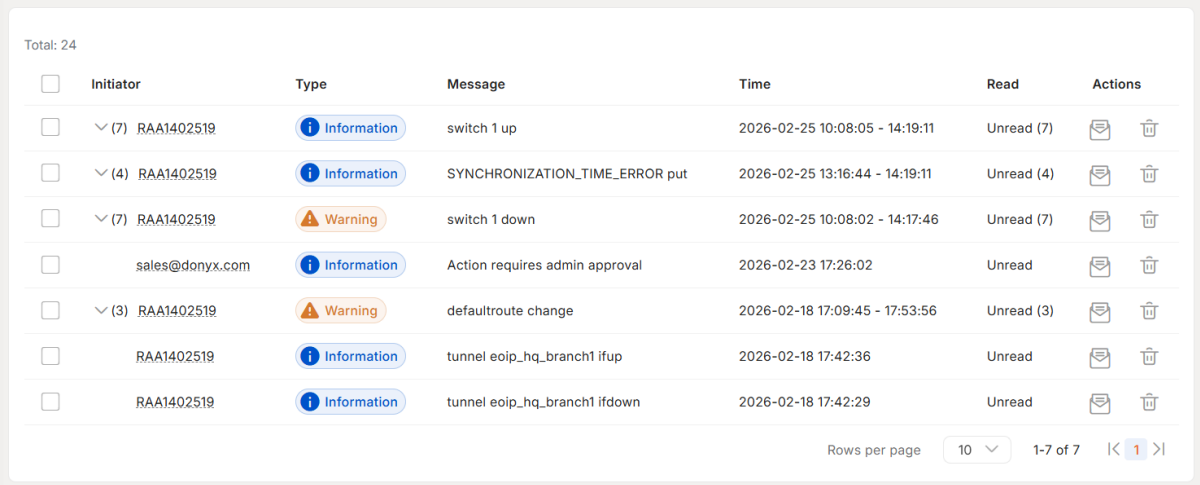


Figure 9. Events View

An event is marked as read by clicking the envelope icon in the **Action** column.

Similar events for specific devices are collapsed into blocks. To expand the list, click the **V** symbol next to the device.

Clicking the button allows for downloading a file containing event information from devices, users, or the system.The file is compatible with most spreadsheet applications and can be used for analysis.

Each event type is indicated by a corresponding icon: Warning, Information, Error.

3.2.1. Search and Filters in the Events Section

The **Events** section provides comprehensive search and filtering capabilities for monitoring system activity.

Two search methods are available: exact match and filter-based search. Filter-based search utilizes **OR** logic; if multiple tags are specified, the table displays all records containing at least one match. The *Filtered by* row indicates the currently active keywords.

Search functionality is supported for the *Initiator* and *Message* columns. For the *Read* column, search is performed based on the user who marked the event as read.

Interactive filtering is also available: clicking a specific value in the *Initiator* or *Type* columns automatically filters the table by that value. Simultaneous filtering across both columns is supported.

Additionally, the button enables table filtering by a specified time interval.

Search and filtering tools can be used concurrently.

Filters affect data display only within the sections where they are applied.

3.3. Actions

New actions are created in the **Devices** section after selecting one or more devices.

The **Actions** section stores the history of all operations performed on the devices. This includes configuration changes as well as service commands, such as backup creation or system log retrieval.

Clicking the button enables the download of a file containing information about actions performed on individual devices or groups at various times. The file format is compatible with most spreadsheet applications (Microsoft Excel, LibreOffice Calc, etc.), which facilitates data analysis.

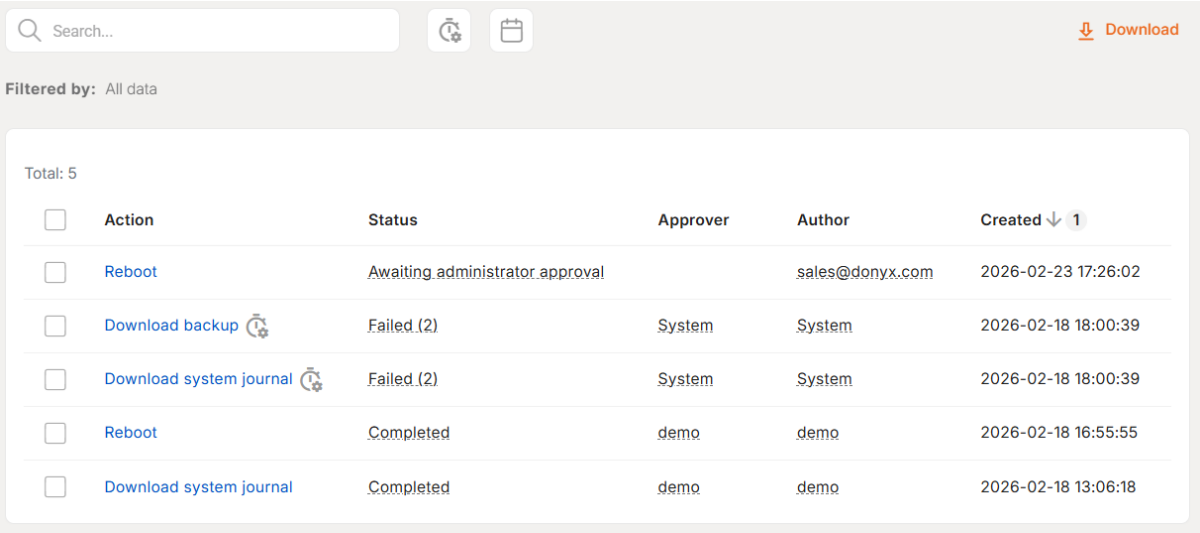


Figure 10. Actions View

Table 5. **Fields in the Actions section**

Field	Description
Action	Action type according to Section New Action.
Status	Current status of the command.
Approver	The name of the user who confirmed the action. If the action is routine, the field will display *System*.
Author	The name of the user who initiated the action. If the action is routine, the field will display *System*.
Created	Date and time the command was added to the execution queue.

3.3.1. Search and Filters in the Actions Section

In the **Actions** section, the table supports sorting by any column and data display management:

- **Sorting:** To sort the list, click the header of any column. Selected columns are marked with numbers indicating sorting priority.
- **Quick Search:** To find a device, enter text in the search field. The search is performed based on matches in the *Action*, *Approver*, and *Author* columns.

The button enables filtering the table by time interval, while the button filters for routine actions.

Furthermore, clicking on a specific value in the **Status**, **Approver**, or **Author** column filters the table accordingly. Simultaneous filtering by all three columns is supported.

These tools can be combined.

Filters affect data display only within the sections where they are applied.

3.3.2. Action Editing

To perform operations on an action, click the specific entry in the list.

The **Actions** menu provides the following functions:

- **Repeat** — Re-adds the selected action to the execution queue.
- **Delete** — To remove an action, click the **Delete** button, wait for it to turn red, and click it again.
- **Approve** — Authorizes actions initiated by users with the **Assistant** role. To confirm the action, click the **Approve** button.

Table 6. **Fields in the Action menu**

Field	Description
Type	Category of the executed command according to Table Description of available actions.
Author	The name of the user who initiated the action.
Approved	The name of the user who approved the action.
Command	Syntax of the user command sent to the device.
Postponed until	The scheduled start time for actions deferred for future execution.
Runs until	The expiration time for the scheduled command.
Files	Attached files associated with the action.
Result	Final execution status on devices. To view a detailed report, click on the specific device entry.
Pending	List of devices targeted by the action.

3.3.3. New Action

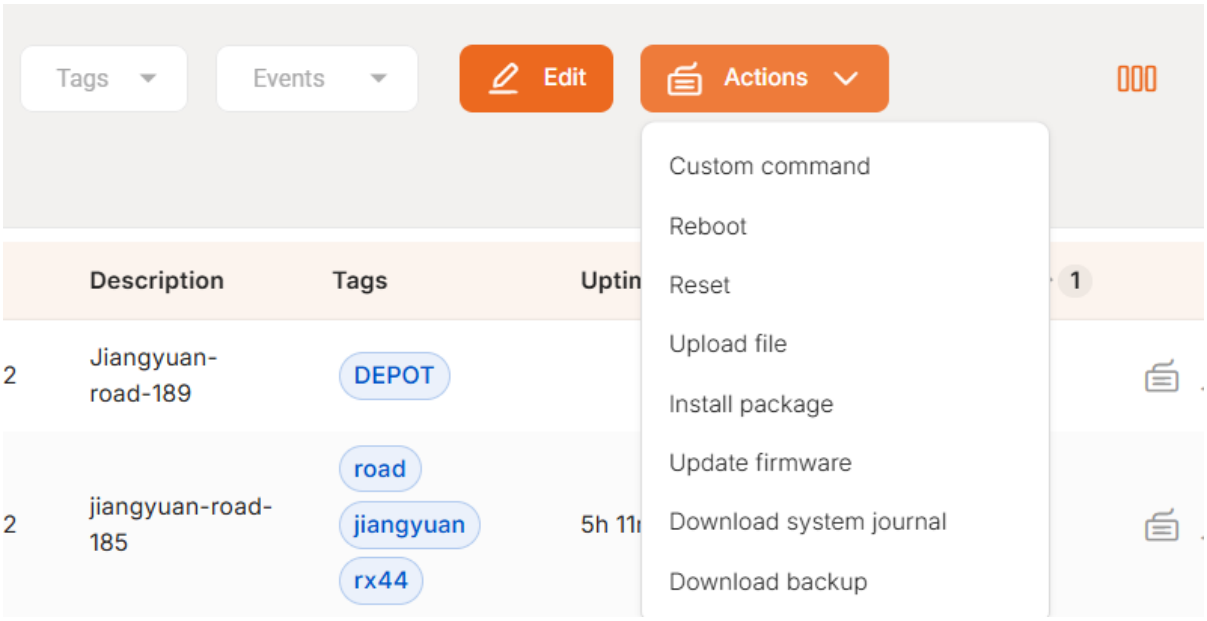


Figure 11. Add New Action View

To add a new action to the execution queue, select the routers in the **Devices** section using the checkboxes and click the Actions button. If an action needs to be assigned to a single device, click the button next to it.

The ability to create new actions depends on the account role:

- **Administrator:** Users with this role can create and execute actions directly. These actions are performed immediately (or at the scheduled time) without additional verification.
- **Assistant:** Users with this role can also create actions, but they do not start automatically. Execution requires mandatory confirmation (approval) from an Administrator.

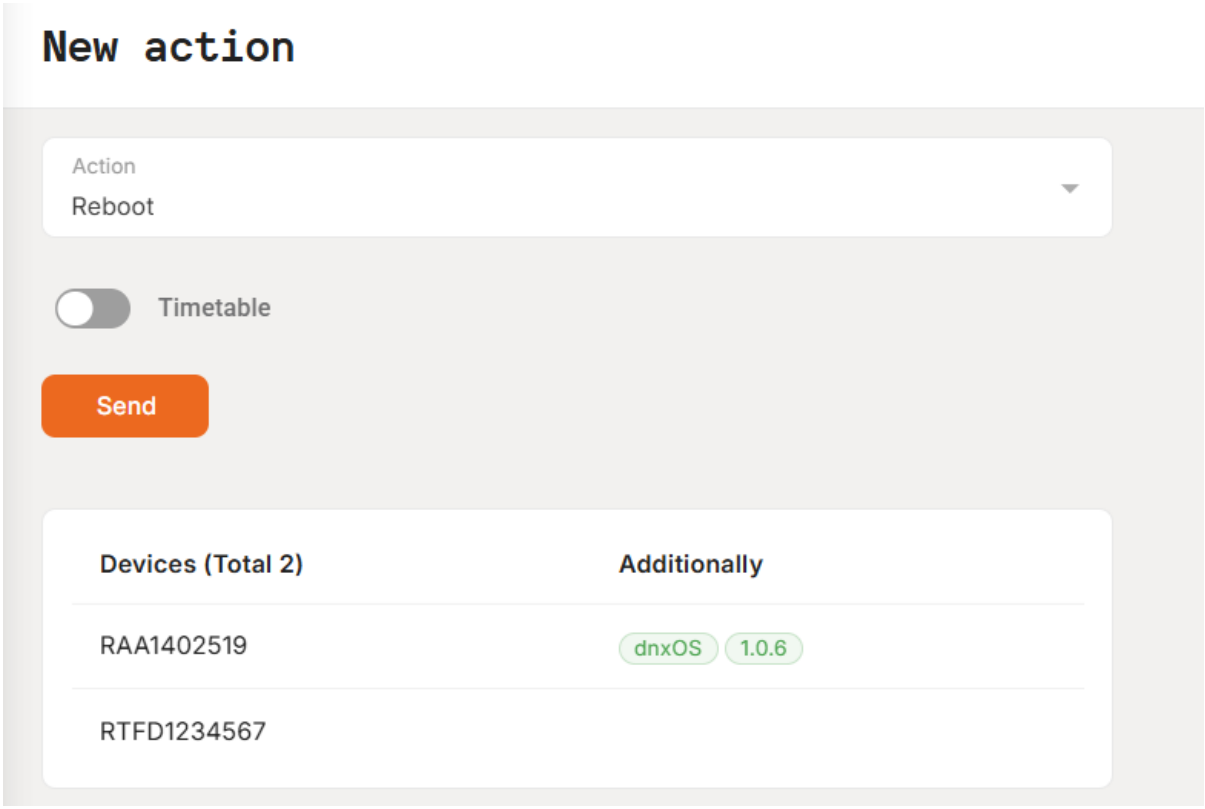


Figure 12. New Actions View

Table 7. **Fields in the New action menu**

Field	Description
Action	Select the command type to be executed from the drop-down list.
Select/choose file	This field appears if the selected action requires a file (e.g., a firmware image).
Timetable	By default, the action is executed immediately upon creation (and approval). To schedule the operation for a specific time, move the toggle to the right. This activates the following fields: • **Postpone until:** Specify the earliest time the action should start. • **Run until:** Specify the time by which the device must complete the command. This is used for devices that may be temporarily offline.
Devices	An informational field displaying the count and serial numbers of all target devices. It also provides additional details, such as hardware series and OS type.

Downloading files to routers, installing packages, and updating firmware requires that the corresponding files be pre-uploaded to the system in the *Files* section.

After completing the required fields, click **Send**.

The list of actions sent to the devices is displayed in the *Actions* section.

Table 8. **Description of available actions**

Action	Description
Custom command	A user shell command for the router software shell. The input field is limited to 252 characters.

Reboot	Power reboot of the selected devices.
Reset	Resets the device to factory settings.
Upload file	Uploads files to the device that are not firmware images or application packages.
Install package	Installation of application packages.
Update firmware	Firmware update for the selected devices (requires selection of a firmware file).
Download system journal	Generates and downloads the device system log.
Download backup	Generates and downloads a backup of the device configuration.

The ☆ button allows for creating a shortcut from a custom shell command. To do this, enter a name for the shortcut in the displayed field. Commands can be deleted in the **Administration** → **Settings** → **User actions list** section.

Adding a created shortcut to the **Action** dropdown list is performed in the user settings located in the top right corner of the web interface.

Note that the **Action** dropdown list can display a maximum of ten actions.

3.4. Files

The **Files** section contains information about files and scripts (such as certificates) stored in the system.

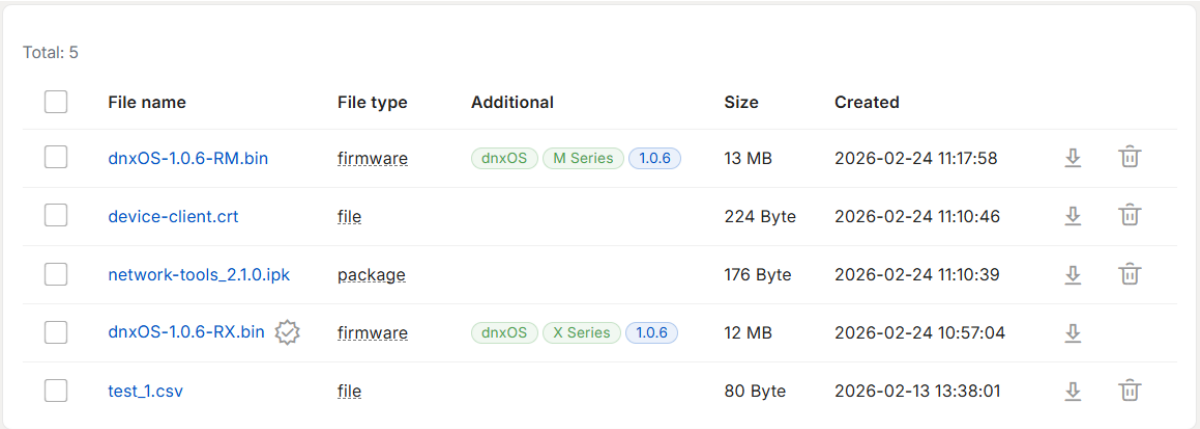


Figure 13. **Files View**

Table 9. Fields in the **Files** menu

Field	Description
File name	The name of the file.
File type	The category of the file (e.g., firmware).
Additional	Metadata identifying the file category, such as the operating system type, software version, or the hardware platform for which the file is intended.
Size	The file size.
Created	The date and time the file was added to the system.

The icon marks official software versions.

The and buttons allow you to download or delete a file. To perform a deletion, click the icon twice.

Official software version files cannot be deleted.

3.4.1. Search and Filters in the Files Section

In the **Files** section, the table supports sorting by any column and data display management:

- **Sorting:** To sort the list, click the header of any column. Selected columns are marked with numbers indicating sorting priority.
- **Quick Search:** To find a device, enter text in the search field. The search is performed based on matches in the *File name* and *File type* columns.

The button allows for filtering the table to display only official software versions.

Furthermore, clicking on a specific value in the **File type**, or **Additional** column filters the table accordingly. Simultaneous filtering by all three columns is supported. These tools can be combined.

3.4.2. Viewing File Information

Detailed information about an uploaded file is accessed by clicking the specific entry in the list.

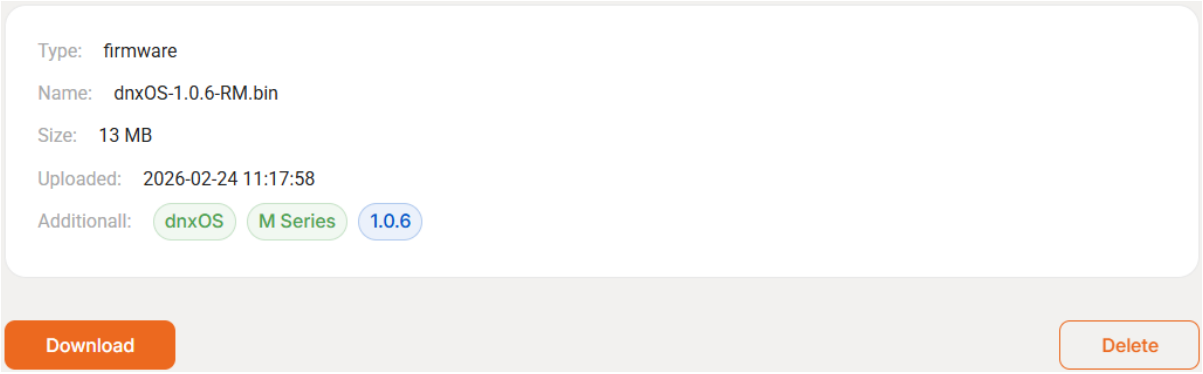


Figure 14. File Information View

Table 10. **Fields in the File menu**

Field	Description
Type	The category of the file.
Name	The name of the file.
Size	File size in bytes.
Additional	Metadata identifying the file category, such as the operating system type, software version, or the hardware platform for which the file is intended.
Uploaded	The date and time the file was added to the system.

The **Download** button allows for downloading the file.

To delete a file, click the **Delete** button, wait for it to turn red, and click it again.

Official software version files cannot be deleted.

3.4.3. Adding a New File

The addition of new files is restricted to users with the **Administrator** role.

To add a new file, navigate to the *Files* section, click the 

icon at the top of the screen, and select the file from the system explorer.

If multiple files with identical names are uploaded, the system will retain only one file (the most recently uploaded version overwrites the existing one).

The maximum size for an uploaded file is 25 MB.

3.5. Administration

3.5.1. Users

Access to this section is restricted to users with the **Administrator** and **Assistant** roles.

The **Users** section contains information about system users. This section allows for adding new users, as well as editing or deactivating existing profiles.

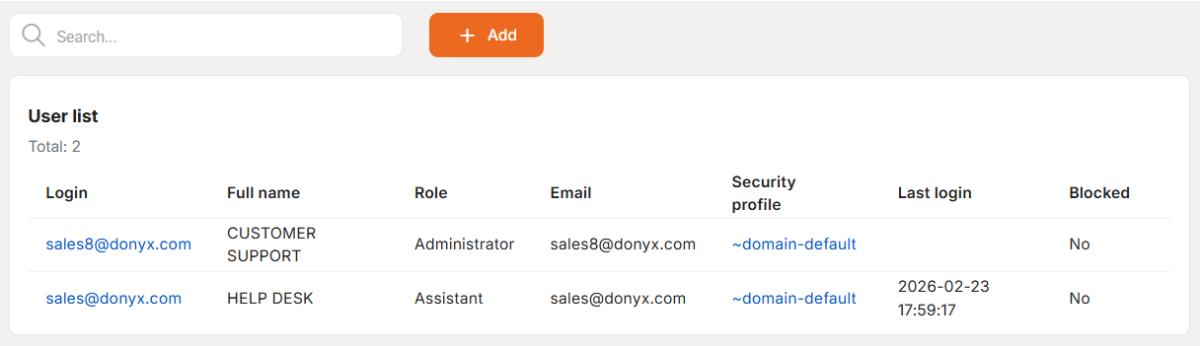


Figure 15. Users View

Table 11. **Fields in the Users section**

Field	Description
Login	The username specified during registration.
Full name	The user's first and last name.
Role	Access role. See the User Roles section of this guide.
Email	The contact email address provided during registration.
Security profile	The security profile assigned to the user.
Last login	The date and time of the user's most recent login.
Blocked	Current user status (*yes* / *no*).

3.5.2. Search and Filters in the Users Section

In the **Users** section, the table supports sorting by any column and data display management:

- **Sorting:** To sort the list, click the header of any column. Selected columns are marked with numbers indicating sorting priority.
- **Quick Search:** To find a device, enter text in the search field. The search is performed based on matches in the *Full name*, *Role*, *Email*, *Security profile*, and *Blocked* columns.

3.5.3. User Editing

Selecting a specific user from the list opens a page for editing their profile information.

Table 12. **Fields in the Edit user menu**

Field	Description
Login (not editable)	The username selected during registration. The login must be unique within the system and cannot be modified after creation.
Full name	The user's first and last name.
Email	The contact email address.
Phone	The contact telephone number.
Security profile	Permissions for executing specific actions. Information regarding the last use of DRM is available under the security profile.
Role	Access role. See the User Roles section of this guide.
Password *	The password entered during registration.

* Passwords must be at least 10 characters long and consist of Latin letters (A-Z, a-z), digits (0-9), and special characters: %, *,) , ?, @, #, $, ~. The use of more than two identical consecutive characters is not permitted.

Access for a selected user can be restricted using the **Blocked** checkbox.

If a security profile or role is modified, the system automatically activates and temporarily locks the **Password expired** option. This restriction is automatically lifted once the user updates the password.

After a security profile or role change, the user will be required to change their password upon the next login.

After completing the fields, click **Save**.

To delete a user, click the **Delete** button, wait for it to turn red, and click it again.

3.5.4. New User

The addition of new users is restricted to accounts with the **Administrator** role.

To add a new user, navigate to the **Users** section and click the 

icon at the top of the screen.

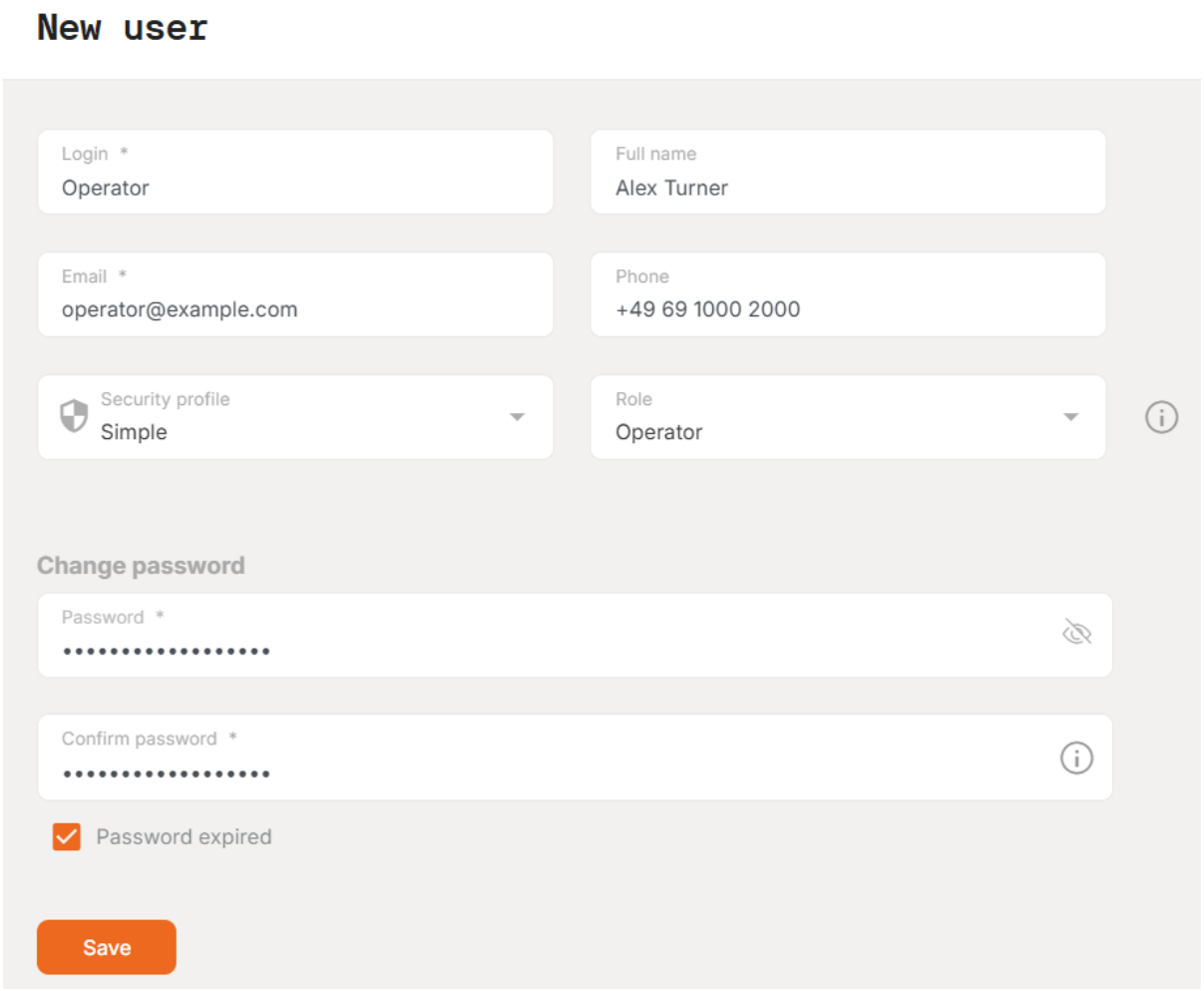


Figure 16. Add New User View

To add a new user, complete the corresponding fields in the displayed menu.

Table 13. **Fields in the New User menu**

Field	Description
Login	A unique identifier for accessing the system. The login must be unique within the domain and cannot be modified after the user profile is created.
Full name	The user's first and last name.
Email	The contact email address.
Contact phone	The contact telephone number.

Security profile	Permissions for executing specific actions.
Role	Access role. See the User Roles section of this guide.
Password *	The user's password.

* Passwords must be at least 10 characters long and consist of Latin letters (A-Z, a-z), digits (0-9), and special characters: %, *,) , ?, @, #, $, ~. The use of more than two identical consecutive characters is not permitted.

After completing the fields, click **Save**.

3.5.5. User Settings

The user settings section is located in the top-right corner of the web interface. To access the section, click the icon.

User profile data is managed in the **Profile** sub-section. The following fields are available for modification:

- Full name.
- Email address.
- Contact phone number.
- New password. The password can only be changed once every 5 minutes.

This section also allows users to delete their own account.

After completing the fields, click **Save**.

The **Settings** sub-section allows for configuring which operations, including saved user commands, appear in the **Action** dropdown menu within the *Devices* section.

A maximum of ten actions can be selected for display in the **Action** dropdown list.

The web interface theme is toggled via the icon.

3.5.6. Password Reset

Clicking the **Forgot password** button on the authorization page opens a form for entering the login and email address. Upon correct completion of the form, a message containing a temporary password is sent to the specified email address. All domain administrators for the respective user are notified of this event.

After authenticating with the temporary password, the user is redirected to a page where a new permanent password must be configured for further system operation.

A temporary password remains valid for **10 minutes**, after which it cannot be used for login. In the event of expiration, the reset form must be resubmitted. The old password remains valid until the new permanent password is successfully established.

If it is necessary to reset the password for the sole administrator and the registered email is unavailable, the reset is performed by contacting technical support at the address specified in the **Customer Support** section of this manual.

3.5.7. Settings

The **Settings** section allows for defining router status update intervals and configuring parameters for backups and system logging.

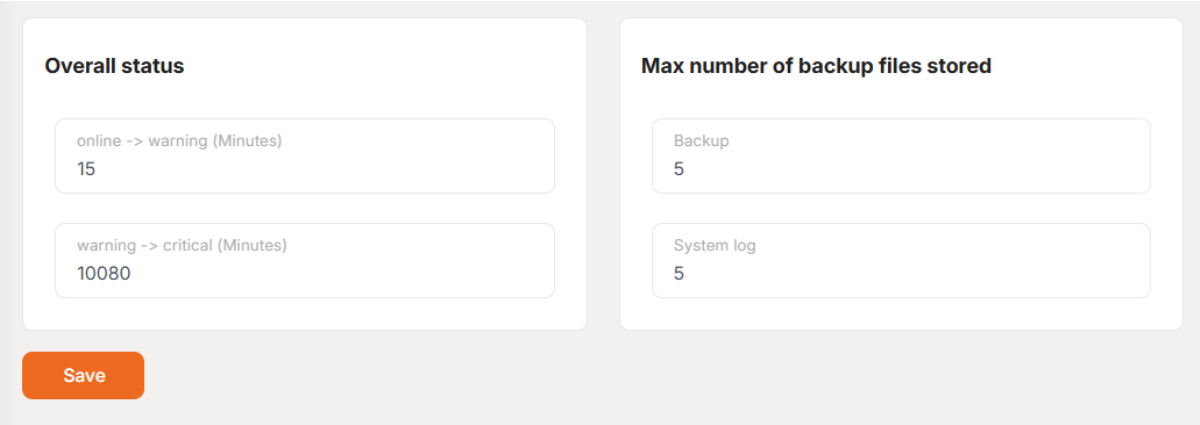


Figure 17. Settings View

In the **Overall status** block, the time intervals (**online→warning** and **warning→critical**) are configured to determine how long a device remains in the *Online* status and when it transitions to *Critical*. These parameters are used to calculate the data displayed in the **OVERALL STATUS** information block within the **Devices** section.

It is recommended not to set the **online→warning** and **warning→critical** intervals to less than 15 minutes, as the default information update period between DRM and the router is 10 minutes (configured in the router settings under the **DRM Client** section).

The **Max number of backup files stored** block defines the quantity of configuration backups and system logs retained on the device. Reductions to this value are applied upon the storage of a new backup file.

Device backup

The **Device backup** block allows for viewing and editing existing backup rules, as well as creating new ones.

To edit an existing rule, click its name in the table. To configure a new backup rule, click the **Add** button and complete the required fields.

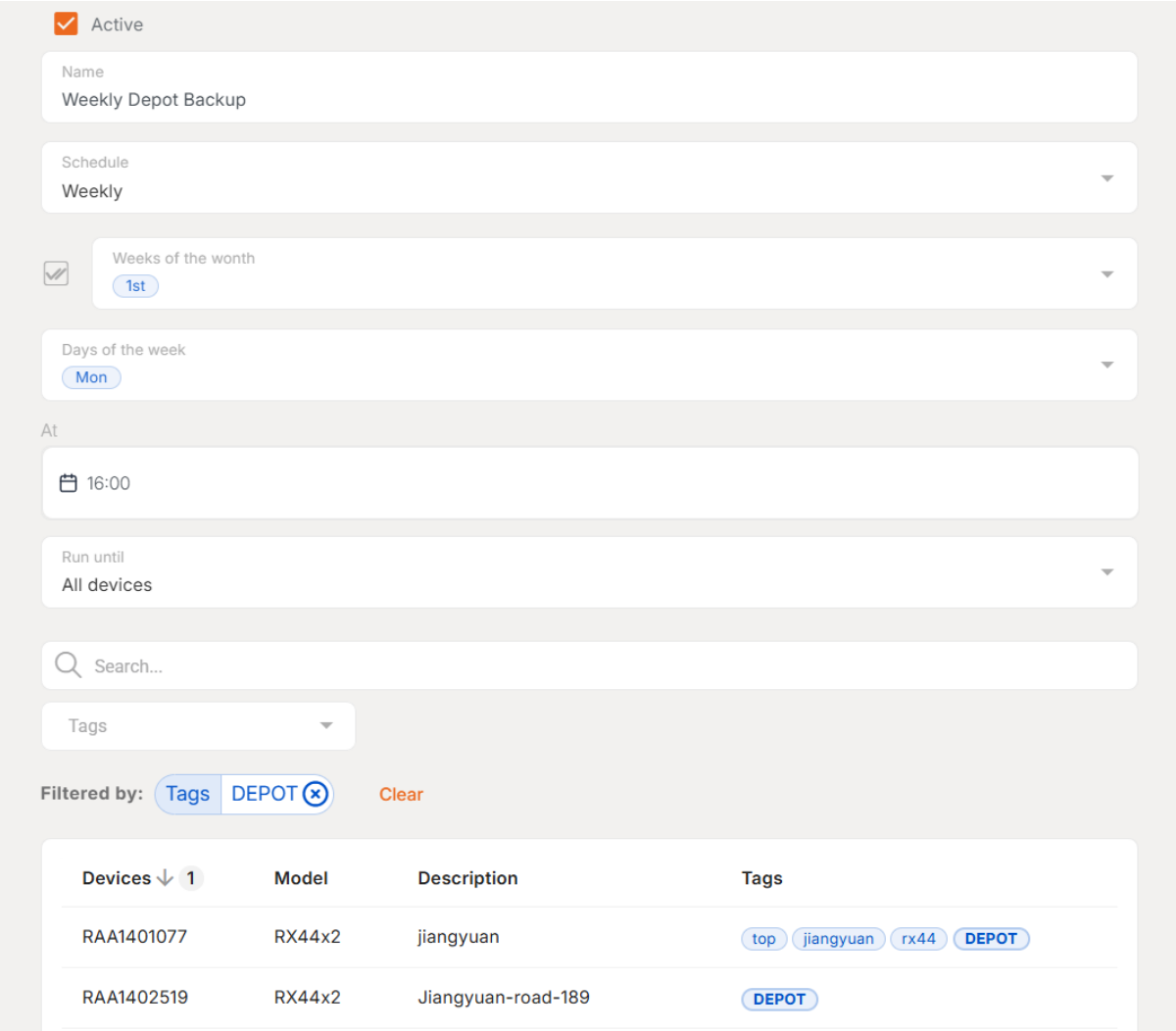


Figure 18. Device Backup Rule Configuration View

Table 14. **Fields for backup rule configuration**

Field	Description
Active	Checkbox to enable or disable the rule.
Name	A unique name for the rule.
Schedule	Defines the backup frequency. Select the preferred interval (*Daily* or *Weekly*) and the start time.
Run until	Target devices for the backup. The rule can be applied to all devices in the system, a specific group, or devices filtered by their assigned tags.

The selection of a device group for backups is performed using the search bar and filter, which identify the required devices based on specified parameters such as tags or models.

After completing the fields, click **Save**.

Multiple tasks of the same type can be applied to a single device. To ensure correct operation, it is recommended to assign no more than one task of each type per device. Assigning multiple identical tasks may result in configuration conflicts and redundant operations.

Backups can be downloaded in the **Devices** section by clicking the specific device identifier (within the *Actions* and *Additional* tabs), as well as in the **Actions** section.

Device system log

The **Device system log** block allows for viewing existing log generation rules and creating new ones.

To create a rule for generating device log files, click the **Add** button and complete the required fields.

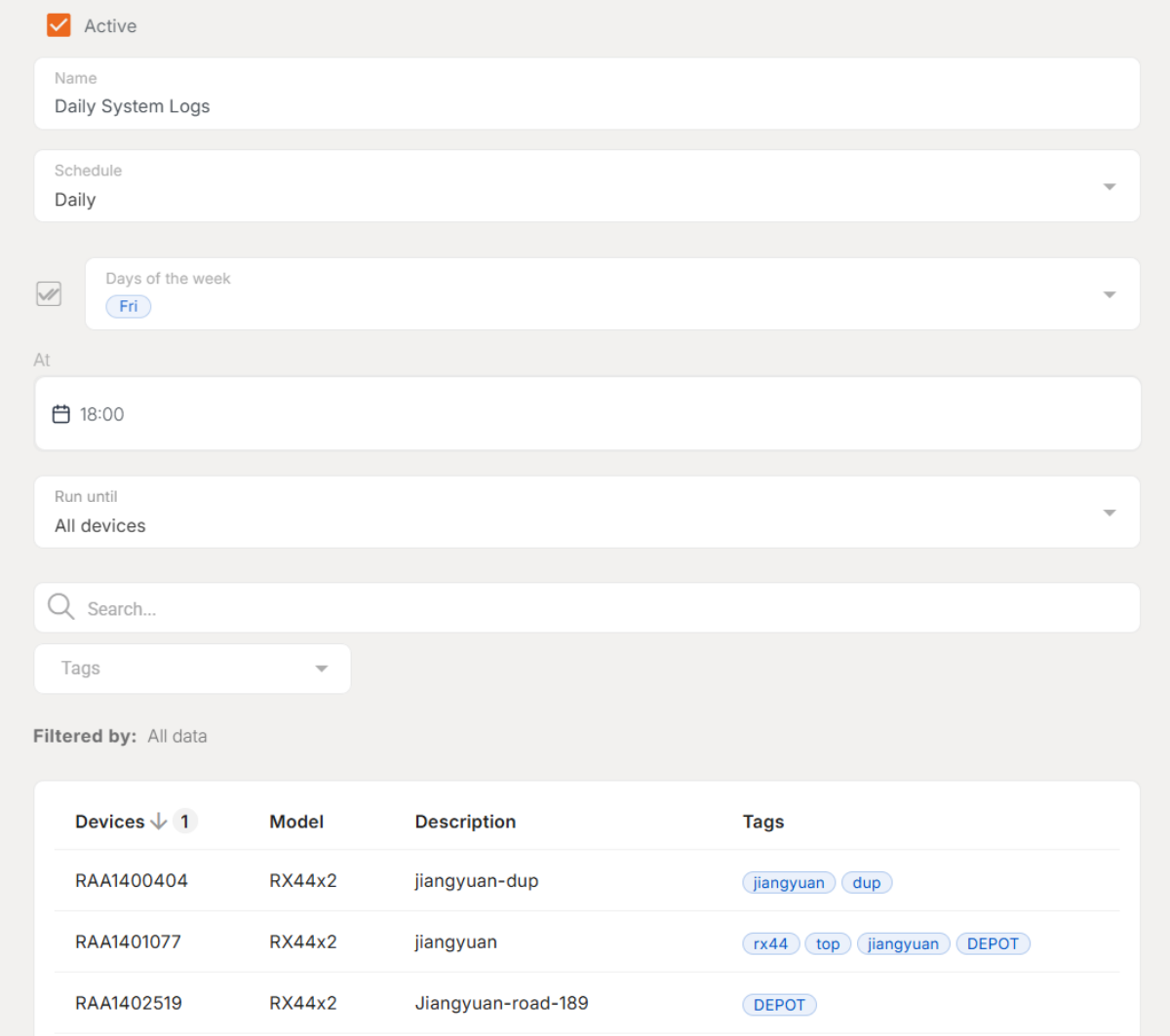


Figure 19. Device System Log Rule Configuration View

Table 15. **Fields for system log rule configuration**

Field	Description
Active	Checkbox to enable or disable the rule.
Name	A unique name for the rule.
Schedule	Defines the frequency of log generation. Select the preferred interval (*Daily* or *Weekly*) and the start time.
Run until	Target devices for log generation. The rule can be applied to all devices in the system, a specific group, or devices filtered by their assigned tags.

The selection of a device group for system log creation is performed using the search bar and filter, which identify the required devices based on parameters such as tags or models.

After completing the fields, click **Save**.

Multiple tasks of the same type can be applied to a single device. To ensure correct operation, it is recommended to assign no more than one task of each type per device. Assigning multiple identical tasks may result in configuration conflicts and redundant operations.

Device system log can be downloaded in the **Devices** section by clicking the specific device identifier (within the *Actions* and *Additional* tabs), as well as in the **Actions** section.

User actions list

The **User actions list** block provides management for created and saved shell commands used for device operations.

To create a new command, click the **Add** button and complete the required fields.

Table 16. **Fields for custom action configuration**

Field	Description
Type	The name or category for the command.
Command	The script or technical command to be executed on the device.

After completing the fields, click **Save**.

Analyzed events

The **Analyzed events** block allows for managing which router events the system analyzes and records. Toggles are used to enable or disable analysis for each specific event type.

Event analysis applies only to new occurrences. Monitoring begins from the moment a specific event type is enabled; historical events are not analyzed.

3.5.8. Notification

The **Notification** section contains a list of user-defined rules for sending device alerts.

The toggle switch adjacent to the rule name enables or disables notification activity. To activate a rule, move the toggle to the right.

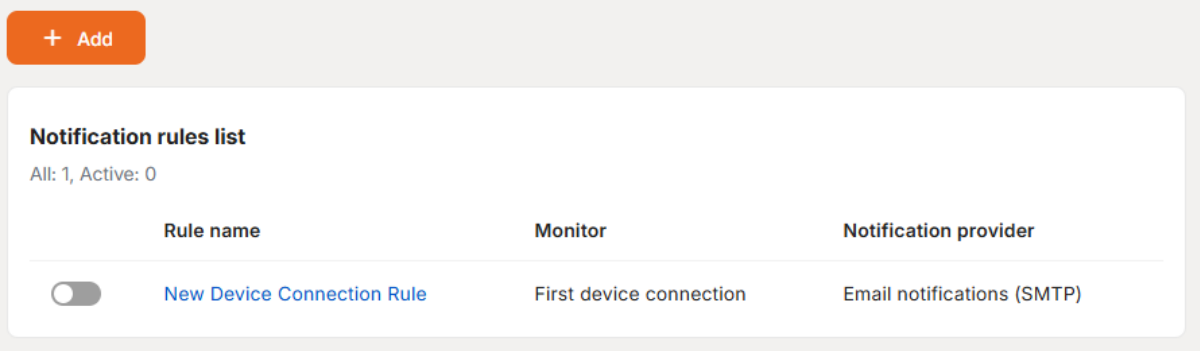


Figure 20. Notifications View

To create a notification rule, click the + Add icon and complete the required fields.

Table 17. **Notification rule configuration fields**

Field	Description
Name	The name assigned to the rule.
Monitor	The type of event to be monitored. Select one of the following options: • **First device connection:** Notifies upon the initial connection of a new device. Used to track the addition of new hardware. • **Device sent a new event:** Notifies when a new event (e.g., action or system event) is registered on the device. • **Device status update:** Notifies when a device's status changes (e.g., to *Warning* or *Critical*). • **User action on device:** Notifies when a specific user action is performed. • **Firmware update required:** Notifies when a new firmware version becomes available for the device.
Event notification	Selection of the specific event trigger. This parameter refines the **Monitor** setting: • **Device sent a new event:** *command* — confirmation of command execution; *event* — any informational event. • **User action on device:** *put* — addition of a new device; *update* — device editing (updating descriptions, managing tags, changing encryption keys); *delete* — device removal.
Notification by timer	Selection of the specific timer trigger. This parameter refines the **Monitor** setting.
Informational status	Selection of the status level that triggers the notification. This parameter refines the **Monitor** setting: • **Device status update:** *critical* — a severe failure occurred; *warning* — a non-critical issue occurred.

Notification provider	Selection of the notification delivery channel. Choose from the available options in the dropdown list or create a new one.

Notification rules are global and can be created or edited by all users within the domain.

Notification Provider

A new delivery method is created by clicking the **+** icon in the left part of the field and completing the required parameters.

Table 18. **Fields for creating notification provider**

Field	**Description**
Provider name	The name of the notification delivery method.
Provider template	Selection of the delivery protocol template. Available options: • *smtp*: Sending notifications via email using an SMTP server. Requires configuration of server parameters (address, port, credentials). • *telegram*: Sending notifications to the Telegram messenger. Requires integration with a Telegram bot (bot token).
Language	The language in which notifications will be generated.

An asterisk (*) next to a field name denotes a required parameter. Configuration cannot be completed unless all mandatory fields are populated.

Sending email notifications via an SMTP server

To configure email notifications via an SMTP server, select the *smtp* template and complete the required fields.

Table 19. **Fields for configuring notifications via SMTP**

Field	Description
Provider name	The name assigned to this configuration.
Provider template	Indicates that this configuration is intended for sending notifications via SMTP.
Language	The language in which notifications will be generated.
Hostname	Required. The SMTP server address.
Port	Required. The SMTP server port. Typically, port *25* is used for unencrypted connections, while ports *465* or *587* are used for secure connections (SSL/TLS).
Username	The username for authentication on the SMTP server. This may be an email address or another identifier depending on server requirements.
Password	The password for authentication on the SMTP server.
Sender email	Required. The email address from which notifications will be sent.
Custom email subject	The subject line for the notification email.
Recipients	Required. The email address(es) of the notification recipient(s). Multiple addresses may be separated by a comma or semicolon.
CC	Email address(es) for sending a carbon copy (CC) of the email. Multiple addresses may be separated by a comma or semicolon.
BCC	Email address(es) for sending a blind carbon copy (BCC) of the email. Recipients in this field are not visible to other recipients.

For the correct operation of notifications through the SMTP servers of certain email providers, additional account security settings may be required (such as generating an application-specific password or enabling access for third-party clients).

The **Check** button is used to verify the validity of the entered data, such as the availability of the SMTP server. If the parameters are configured correctly, a test notification will be sent to the specified email address.

After completing the fields, click **Save**.

Sending notifications to the Telegram messenger

To configure notification delivery to Telegram, select the *telegram* template and complete the corresponding fields.

Table 20. **Fields for configuring notifications via Telegram**

Field	Description
Provider name	The name assigned to this configuration.
Provider template	Indicates that this configuration is intended for sending notifications via Telegram.
Language	The language in which notifications will be generated.
Telegram bot token	Required. The unique access key for the Telegram bot. To obtain it, create a new bot or select an existing one through the official *@BotFather* bot in Telegram. Copy the token and paste it into this field.
Telegram chat ID	Required. The unique identifier of the chat for receiving notifications. To obtain the chat ID: 1. Send any message to the bot in Telegram. 2. Ensure the **Telegram bot token** field is already populated. 3. Click the hint link provided in the interface (the token will be inserted automatically). 4. In the displayed text, locate the *chat* block and copy the numerical value specified next to *id*.
Message thread ID	Allows for sending notifications to a specific message thread within a chat. If not specified, messages are sent to the main chat. Useful for grouping notifications by topic.
Send silently	If enabled, users receive notifications without an audible alert.
Protect content	If enabled, incoming messages are protected from being saved or forwarded to other chats, enhancing notification confidentiality.

The **Check** button is used to verify the validity of the entered data, such as the bot token and chat ID. If the parameters are configured correctly, a test notification will be sent to the specified Telegram chat.

After completing the fields, click **Save**.

3.5.9. Logs

The **Logs** section maintains a record of user activity, displaying operations performed by system users within the domain.

Table 21. **Fields in the Logs section**

Field	Description
Initiator	The user who performed the action.
Activity	A brief description of the action.
Status	The result of the operation.
Created time	The date and time the action was recorded.
Initiator IP	The IP address from which the user performed the action.
Info	Technical details of the action. This may include simple commands (e.g., *reboot*) or complete configuration parameters.

The **Logs** section supports two search methods: exact match search and filter-based search. The filter-based search operates using **OR** logic; if multiple tags are specified, all entries containing at least one of the tags are displayed. The **Filtered by** line indicates the currently applied keywords.

The table supports sorting by any column. The button enables filtering events by date. Selecting a time interval displays actions only for that specific period.

Clicking the **Download** button allows for downloading the log as a CSV file.

3.5.10. Security

The **Security** section displays the list of security profiles available for viewing by the Administrator.

The information presented in this section is not editable. To modify a security profile, please contact the domain creator or technical support at the email address provided in the **Customer Support** section of this manual.

4. Customer Support

Website	donyx.com
Email	support@donyx.com