

SMART EMS

Version:
v3.1.4

Date:
19.07.2024



Contents

1	Introduction	3
1.1	System requirements	3
1.2	Copyright info	3
1.3	Trademark	3
1.4	Contact information	4
2	Changelog	5
3	Login	6
4	Interface overview	7
4.1	Branding	7
4.2	General	7
4.3	List view	9
4.4	Forms	16
4.5	Dialogs	17
5	Using SMART EMS	18
5.1	Devices	18
5.2	Templates	20
5.3	Configs	22
5.4	Firmwares	22
5.5	Logs	22
5.6	Users	23
5.7	Device authentication	25
5.8	Access tags	25
5.9	Labels	25
5.10	Import	25
6	Maintenance	29
6.1	Jobs	29
6.2	Logs	29
6.3	Maintenance schedules	30
6.4	Upload backup	30
6.5	Create backup job	30
6.6	Restore backup job	30
6.7	Create backup for update job	30
6.8	Maintenance mode	30
7	Settings	31
7.1	General	31
7.2	Device types	31
7.3	Logs	32
7.4	Radius	32
7.5	Two-factor authentication	32
7.6	Single Sign-on (SSO)	32
7.7	REST API documentation	33
8	REST API Documentation	34
9	Open source clearance	35

9.1	List actions	35
9.2	Row actions	35
10	Status and license	36
10.1	Requesting license	36
10.2	License expiration	37

1 Introduction

This document intends to provide information and instruction on using the SMART EMS system. Includes information about the product's features and how some of the features are designed to work. The document also provides system requirements and copyright info.

1.1 System requirements

The system is designed to be used by a web browser. In order to ensure the proper functioning of the system, the web browser should support the following standards:

1. HTML 5
2. CSS 3
3. JavaScript support

The application is designed especially for the following web browsers:

1. Edge version 114 and compatible
2. Firefox version 115 and compatible
3. Google Chrome version 114 and compatible
4. Opera version 100 and compatible
5. Safari version 16.5 and compatible

1.2 Copyright info

The copyrights for certain portions of the Software may be owned or licensed by other third parties ("Third Party Software") and used and distributed under license. The Third Party Notices includes the acknowledgements, notices and licenses for the Third Party Software. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in this Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licenses. Copies of those licenses are included in the Third Party Notices. Welotec's warranty and liability for Welotec's modification to the software shown below is the same as Welotec's warranty and liability for the product this Modifications come along with. It is described in your contract with Welotec (including General Terms and Conditions) for the product. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of the Software by sending a request letter to: Welotec GmbH, Zum Hagenbach 7, 48366 Laer, Germany Please include "Source for Welotec VPN Security Suite" and the version number of the software in the request letter. This offer is valid to anyone in receipt of this information.

1.3 Trademark

Welotec is a registered trademark of Welotec GmbH. Other trademarks mentioned in this manual are the property of their companies.

1.4 Contact information

Welotec GmbH

Zum Hagenbach 7, D-48366 Laer

Phone: +49 (0)2554/9130-00

Fax: +49 (0)2554/9130-10

Email: info@welotec.com

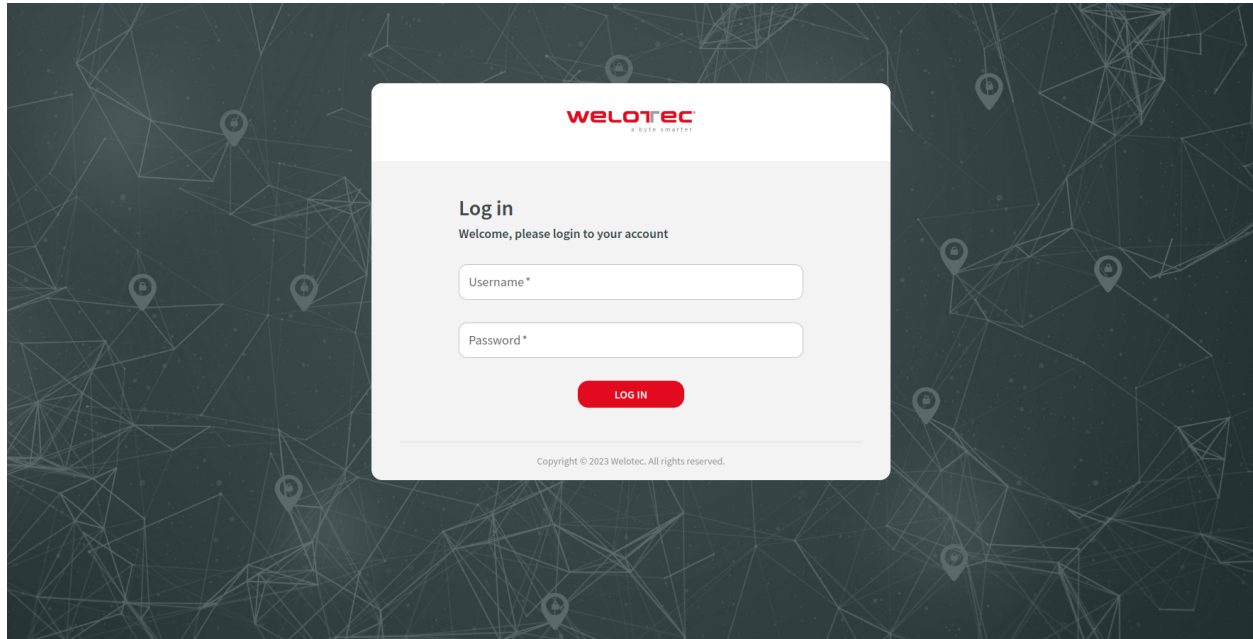
Website: www.welotec.com

2 Changelog

Ver- sion	Date	Log
v3.1.4	11.04.2023	Improve performance of database queries for logs. Add configurable Content-Security-Policy header. TK500v3 device type added
v3.1.3	20.02.2024	Allow router communication on HTTPS port
v3.1.2	22.11.2023	Fix invalid serialization of Edge Gateway config when using communication procedure
v3.1.1	20.11.2023	Fix a valid refresh token being incorrectly rejected for Single Sign-On users
v3.1.0	15.11.2023	Add integration with Microsoft Entra ID using OpenID Connect (Single Sign-On)
v3.0.0	14.07.2023	Initial contents of this document

3 Login

Before using the system you will be asked to authorize yourself. It can be done by providing Username and Password and clicking the “Log in” button.

A screenshot of the Welotec login page. The background is dark grey with a network diagram pattern of white lines and nodes. In the center is a white login card. At the top of the card is the Welotec logo. Below it, the text "Log in" is followed by "Welcome, please login to your account". There are two input fields: "Username *" and "Password *". Below these is a red "LOG IN" button. At the bottom of the card, a small copyright notice reads "Copyright © 2023 Welotec. All rights reserved."/>

welotec
a byte smarter

Log in
Welcome, please login to your account

Username *

Password *

LOG IN

Copyright © 2023 Welotec. All rights reserved.

4 Interface overview

The interface might slightly differ in appearance on different web browsers, due to different ways of rendering the structure of the page.

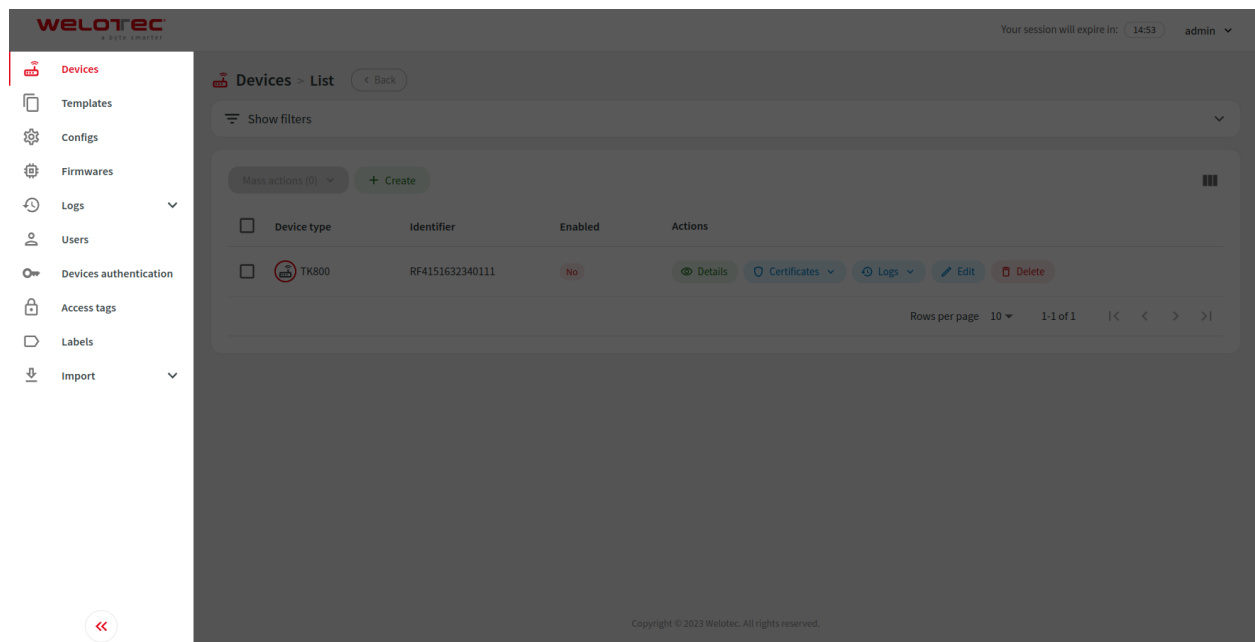
4.1 Branding

The system might be additionally personalized based on your branding needs, therefore screens presented in this document might differ in colour, appearance and branding from the system you are currently using. The structure and general interface of a personalized system remain intact.

4.2 General

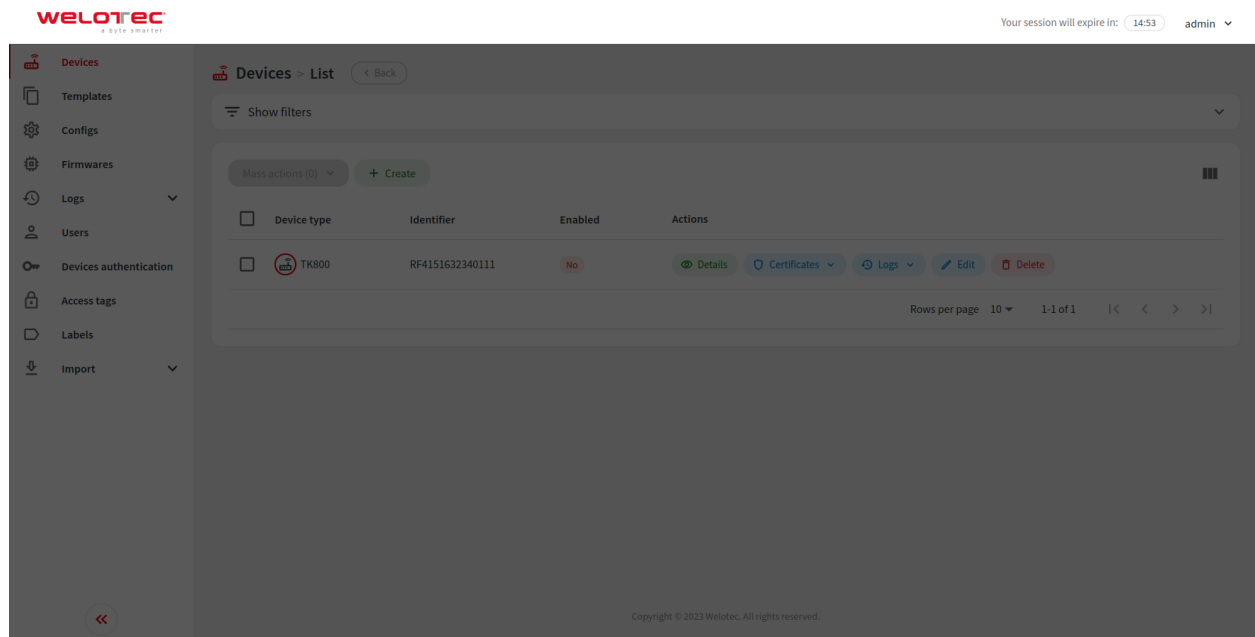
4.2.1 Sidebar

Sidebar is located on the left and holds an expandable menu designed to navigate through the system. Sidebar can also be collapsed to have more space for content.

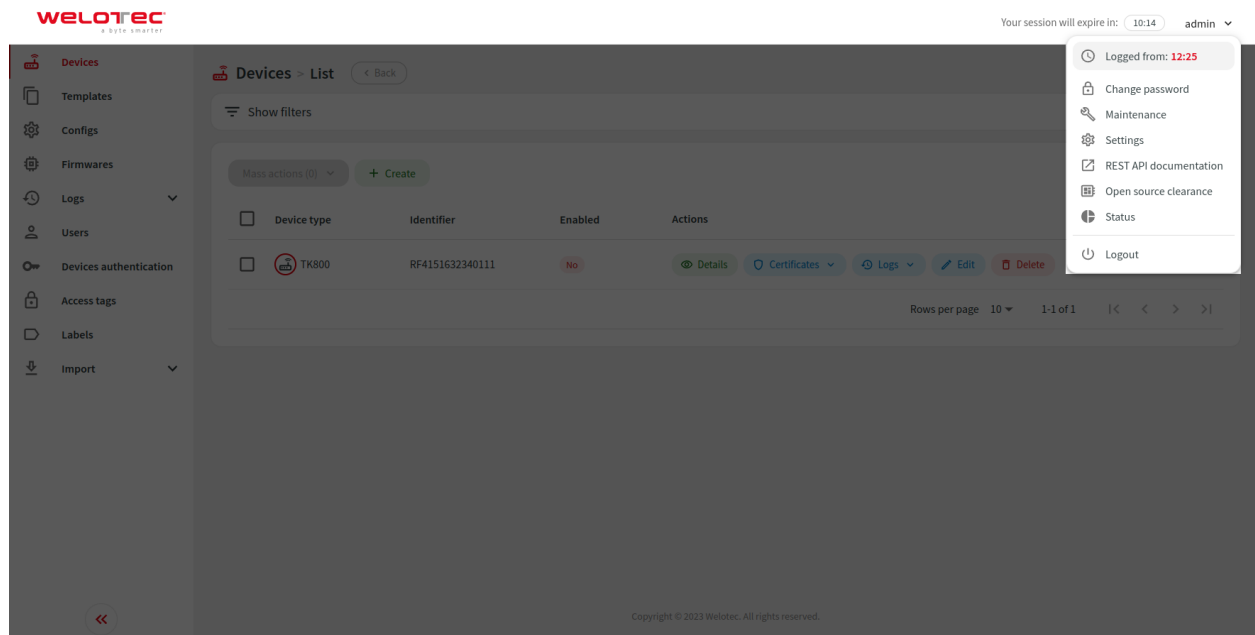


4.2.2 Navbar

Navbar is located at the top and holds information about currently logged-in user and session expiration time.

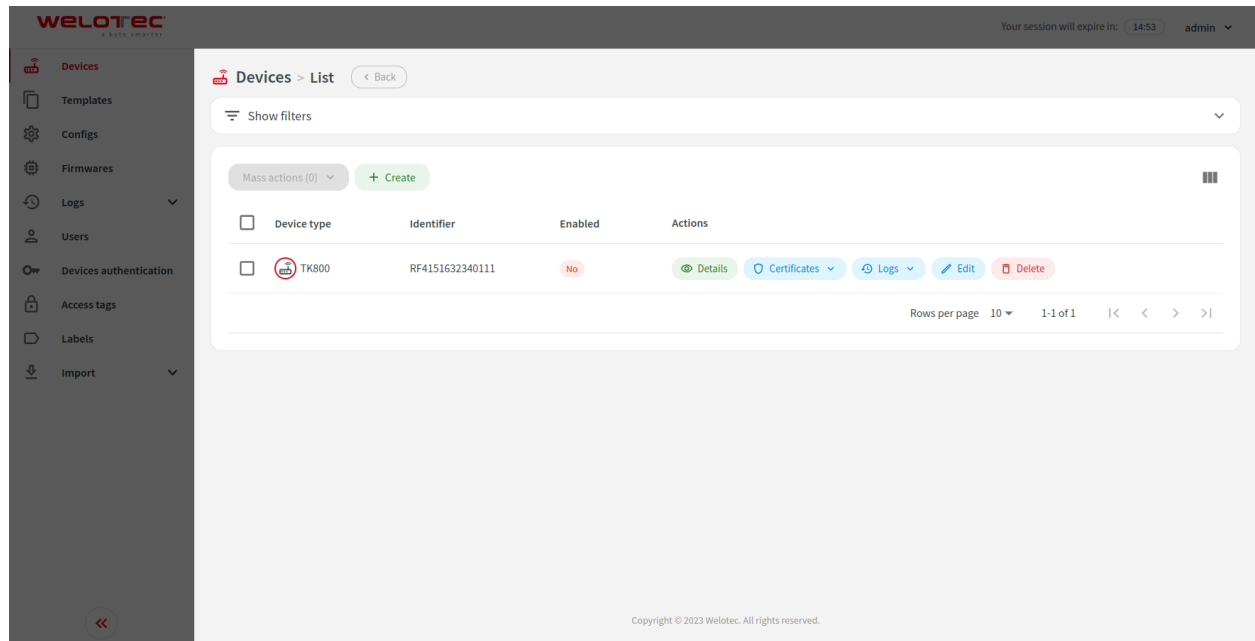


An expandable menu with additional options is available after clicking on the username.



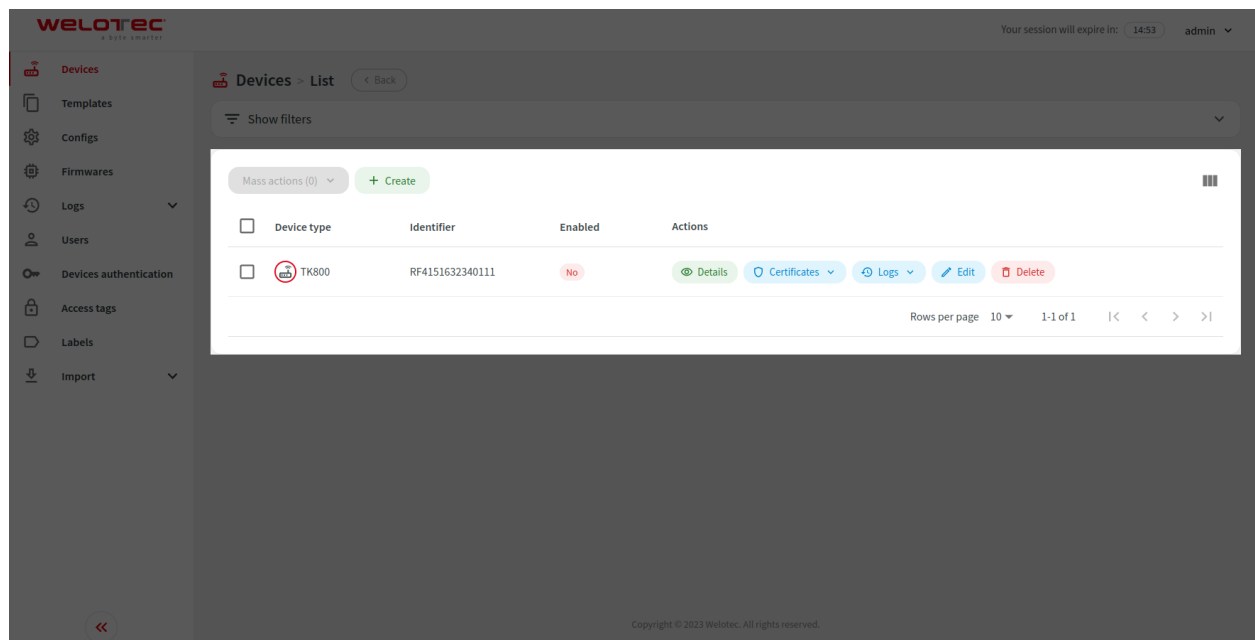
4.2.3 Content

General content is located in the middle and presents selected information.



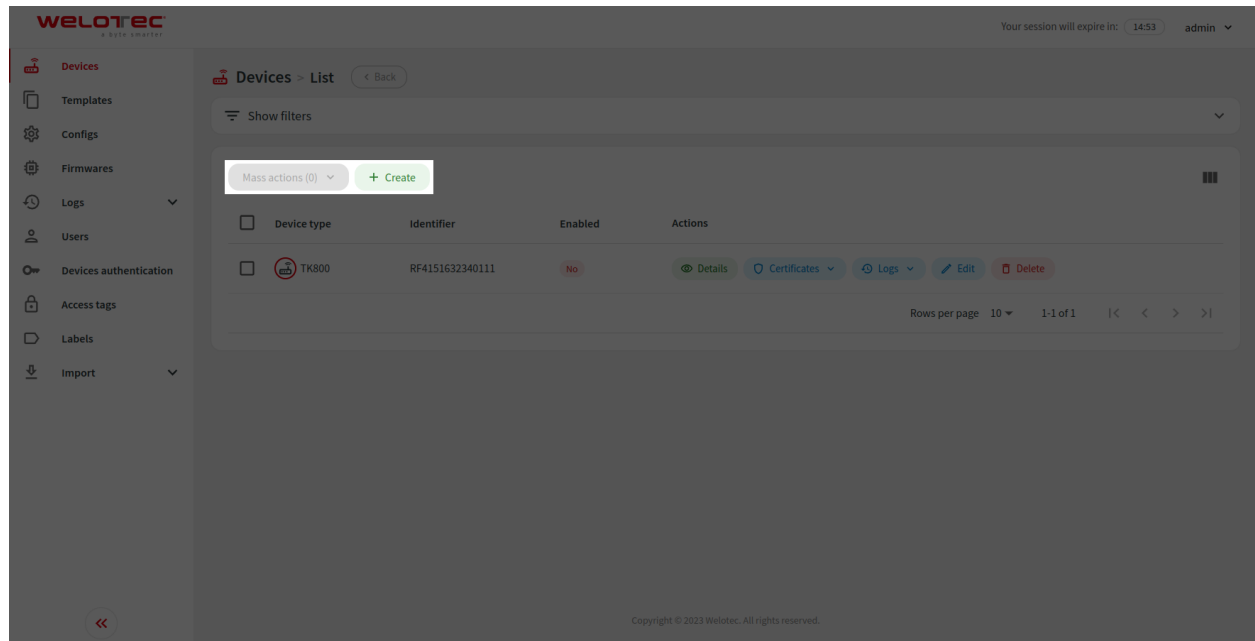
4.3 List view

Inside the content area you can often find a table with columns and rows that presents a list of selected data.



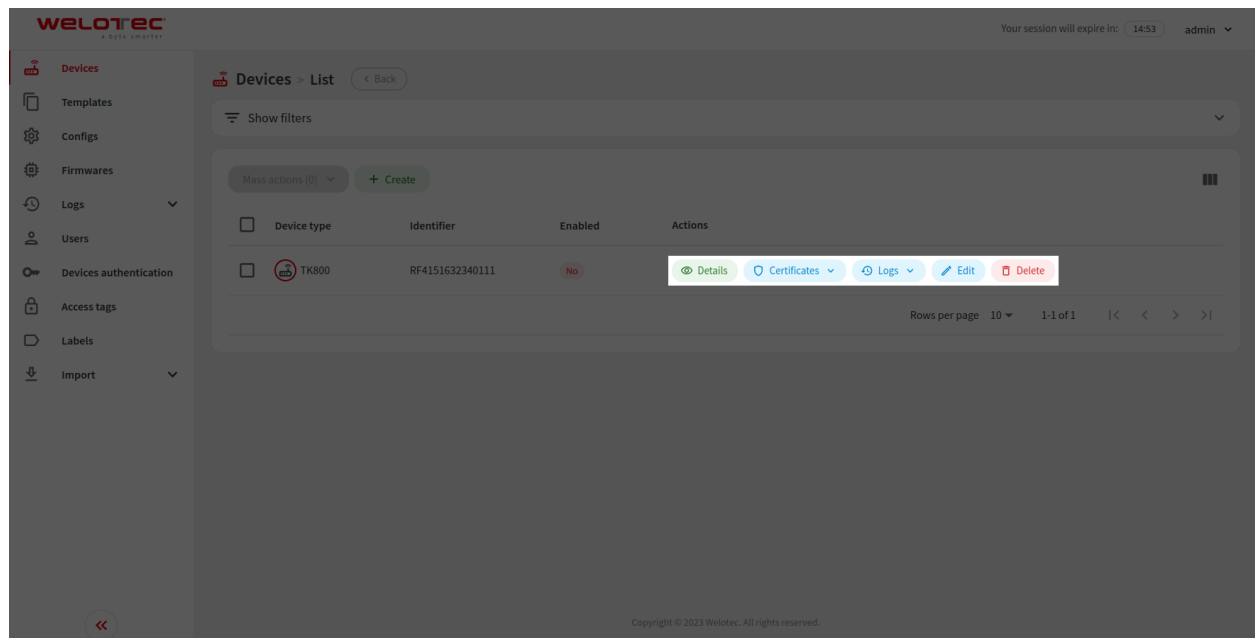
4.3.1 List actions

Most lists allow you to perform actions related to visible data i.e. create, mass actions or export.



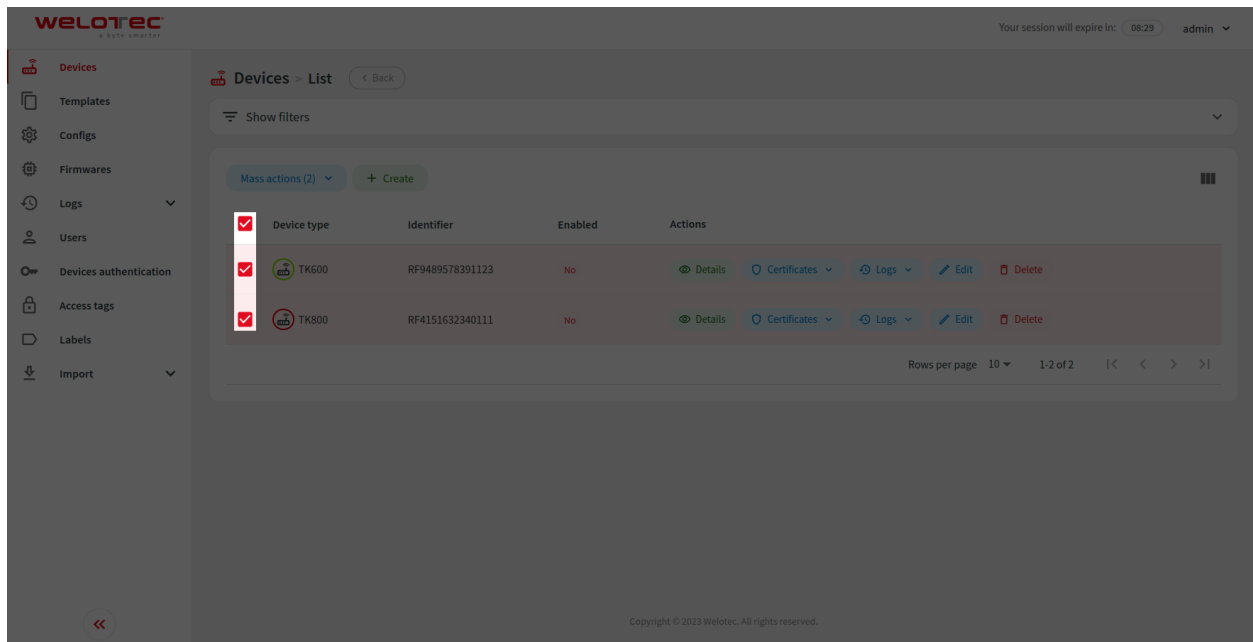
4.3.2 Row actions

In most cases you can also perform actions related to a specific row i.e. edit or delete. Some actions may be disabled, please hover over the disabled button to see a tooltip with detailed information.

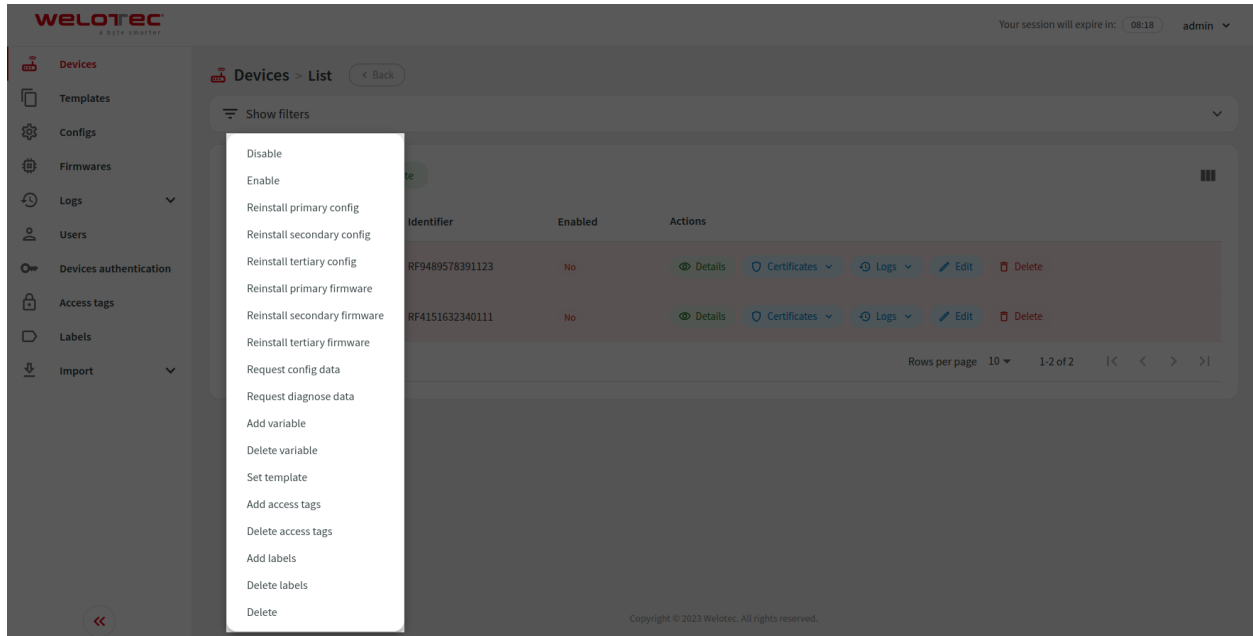


4.3.3 Mass actions

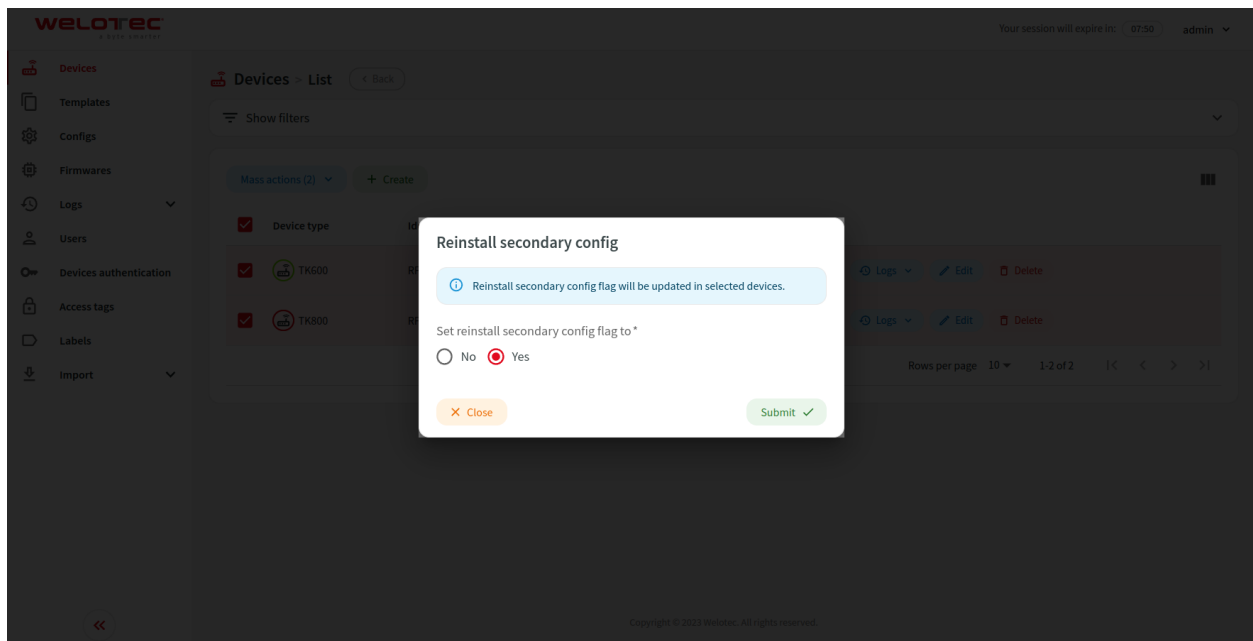
Mass actions give you the possibility to perform an operation on multiple selected rows (i.e. multiple devices). You can select rows using checkboxes in the first column in the table. You can also use the checkbox in the header of a table to select all visible rows.



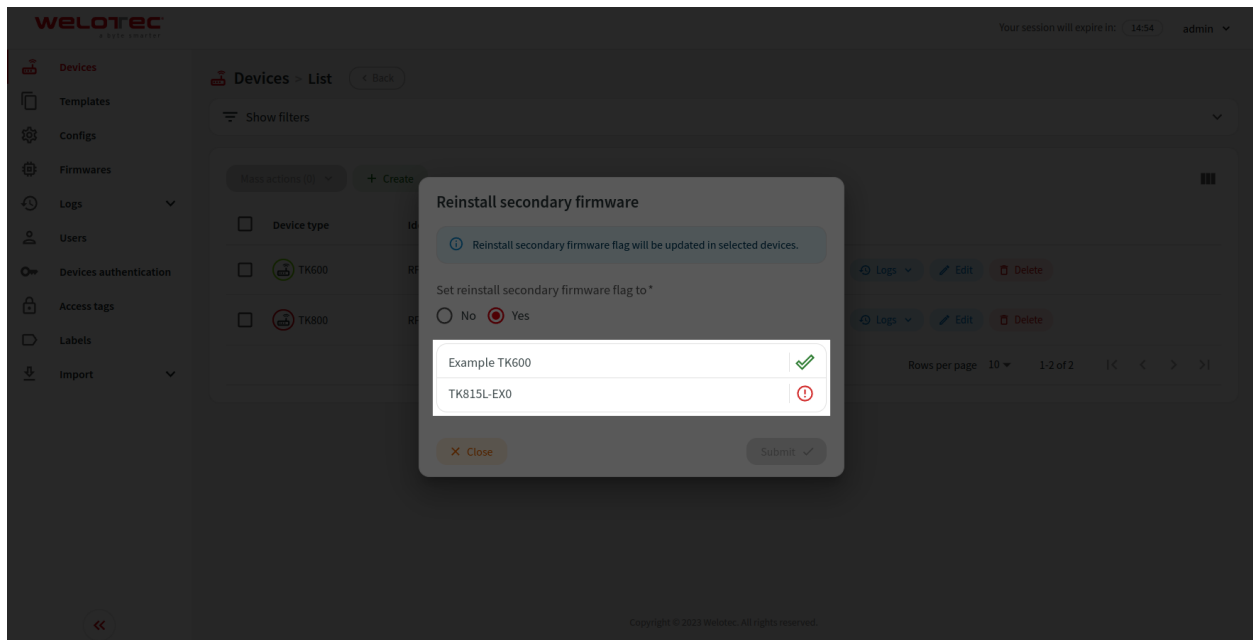
When at least one row is selected “Mass actions” button becomes usable. Clicking on the “Mass actions” button will expand possible mass actions.



Choosing one will open a confirmation dialog. Some mass actions (i.e. “Reinstall secondary config”) require you to provide additional information. When ready you can click “Submit” to execute the selected mass action.

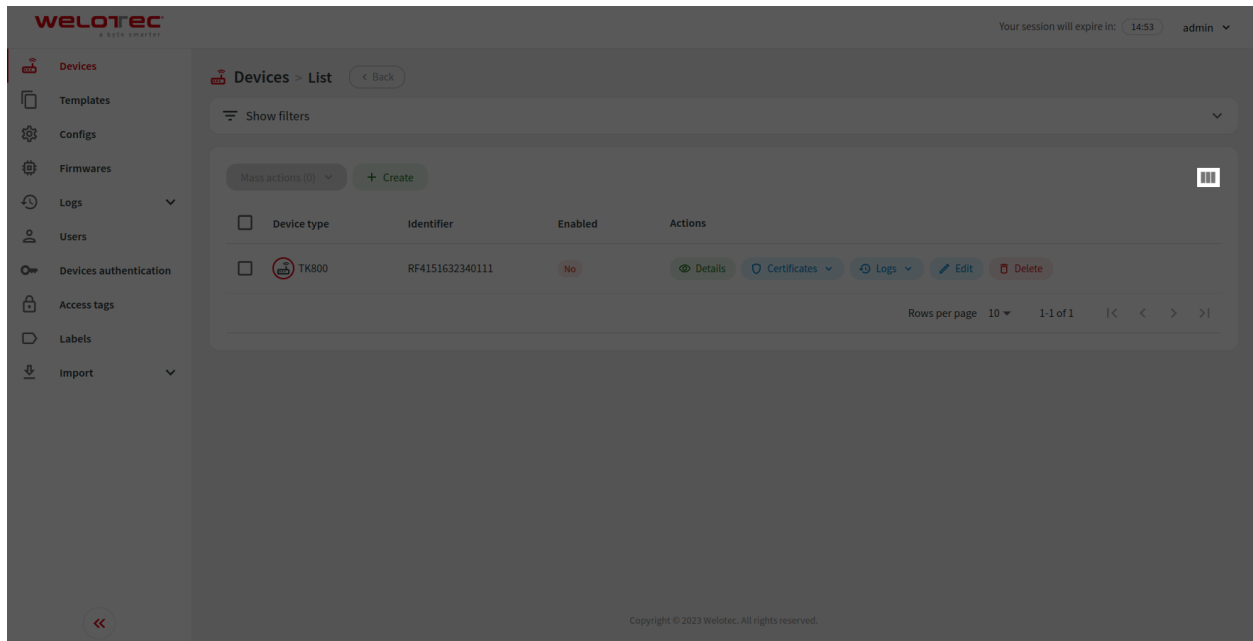


You will get feedback from the system about the status of executed action for each row. Each action can be executed successfully, executed with warnings, executed with errors or skipped. You can hover over the status icon to get a tooltip with detailed information.

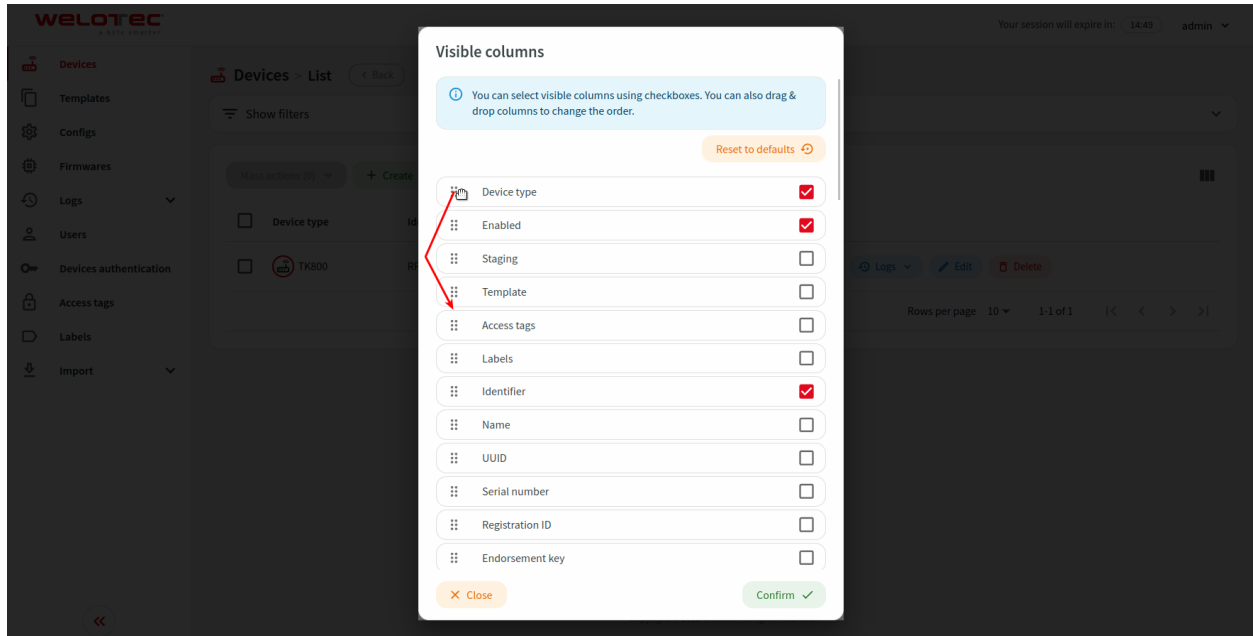


4.3.4 Visible columns

Lists that may have plenty of columns have the possibility to adjust them. Please click the “Adjust visible columns” button.

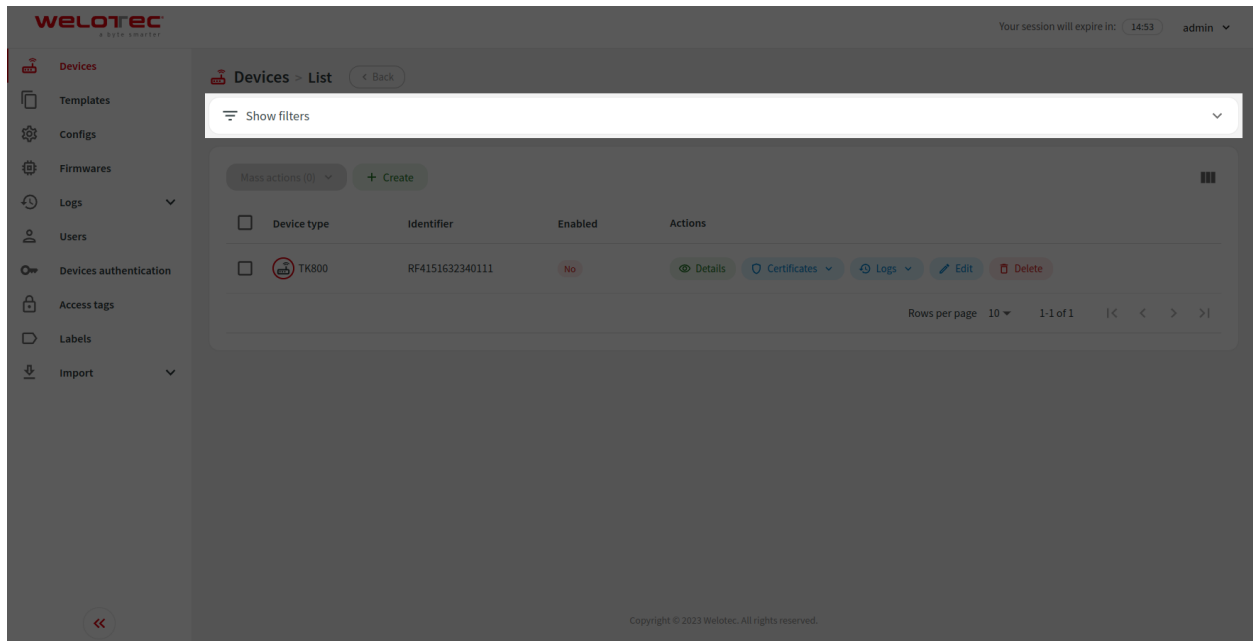


Visible columns dialog will be shown. It will allow you to select visible columns and adjust their order by using the drag & drop technique. Afterward please the changes by clicking the “Confirm” button. You can also reset visible columns to defaults by clicking the “Reset to defaults” button.

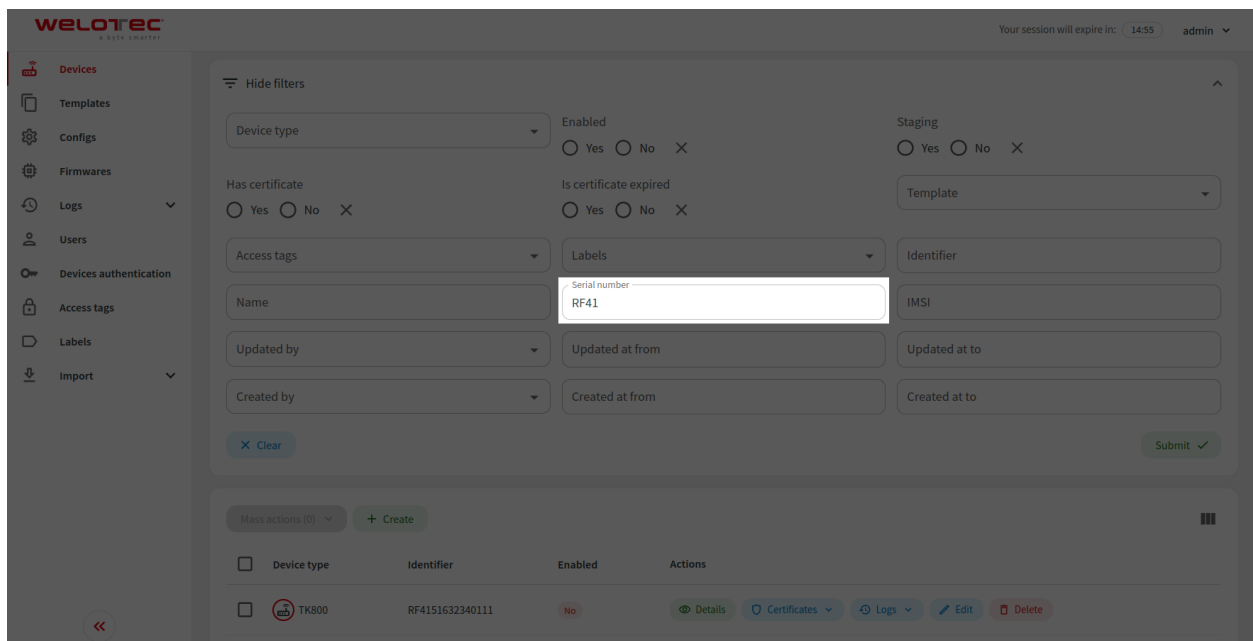


4.3.5 Filtering list results

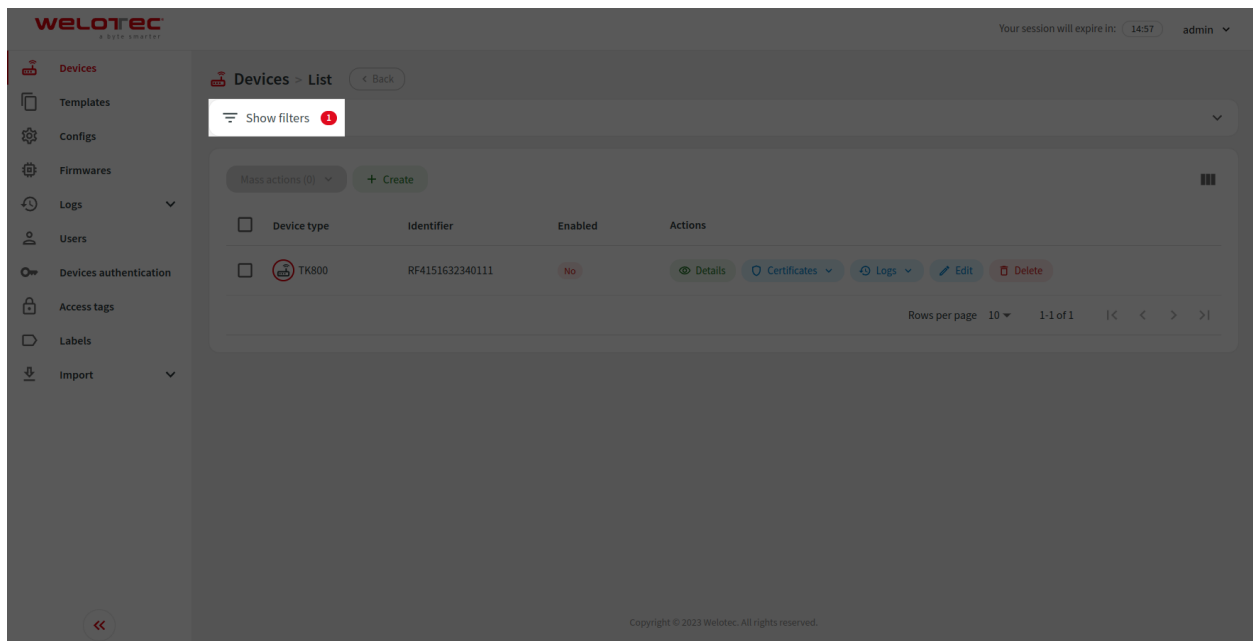
Visible results on the list can be filtered according to available filters. You can find an expandable “Show filters” section.



You can use a specific filter by filling in or choosing the proper value in related input and clicking “Submit”. You can also reset all filters by clicking “Clear”.

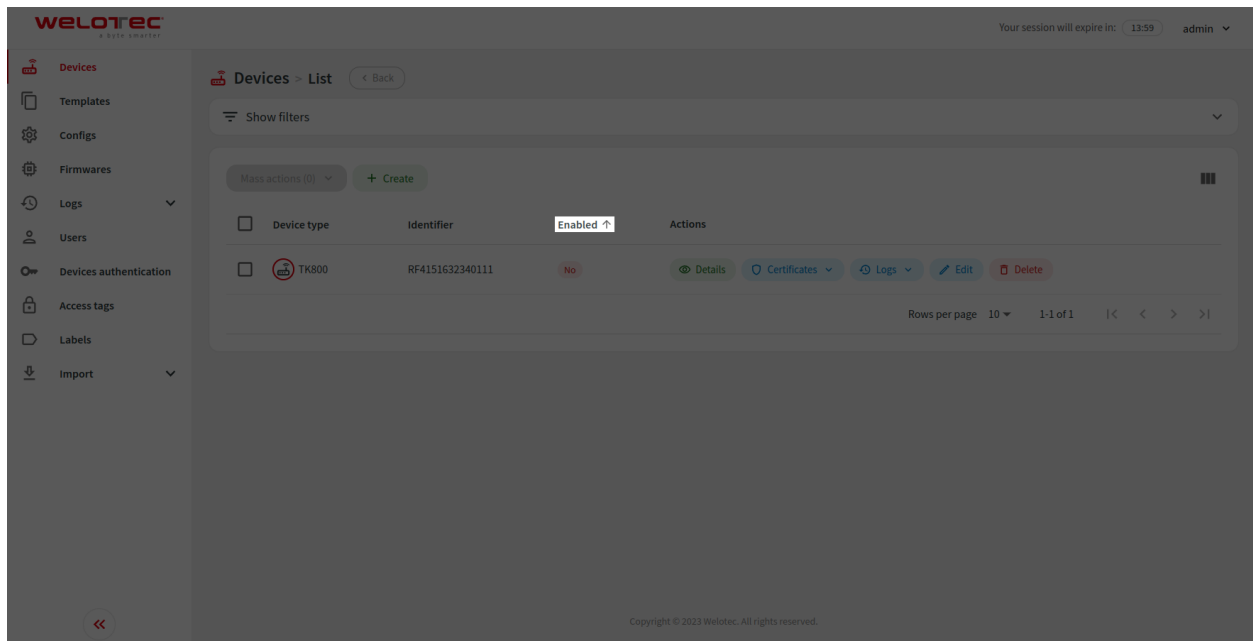


There is an additional indicator (a badge) on the “Show filters” section in case any of the available filters are currently active.



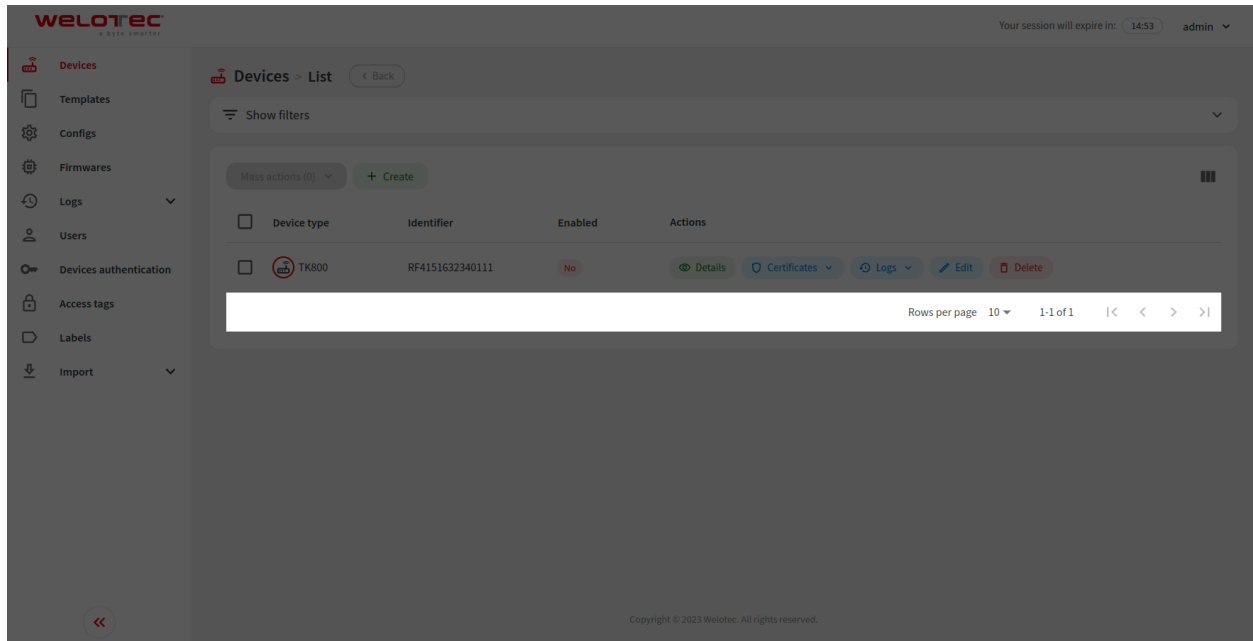
4.3.6 Sorting list results

You can also sort visible results by clicking on the desired column. The second click on the same column will reverse the sorting order.



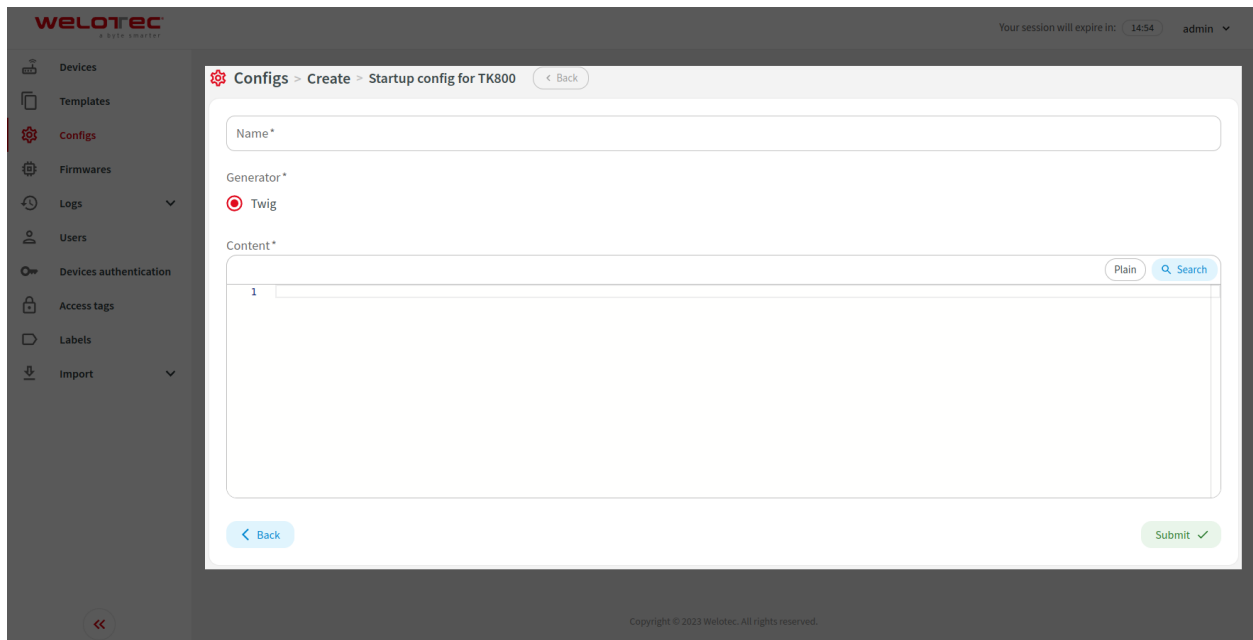
4.3.7 List pagination

Visible results are divided into pages. You can go to a specific page by using the proper button below list results.



4.4 Forms

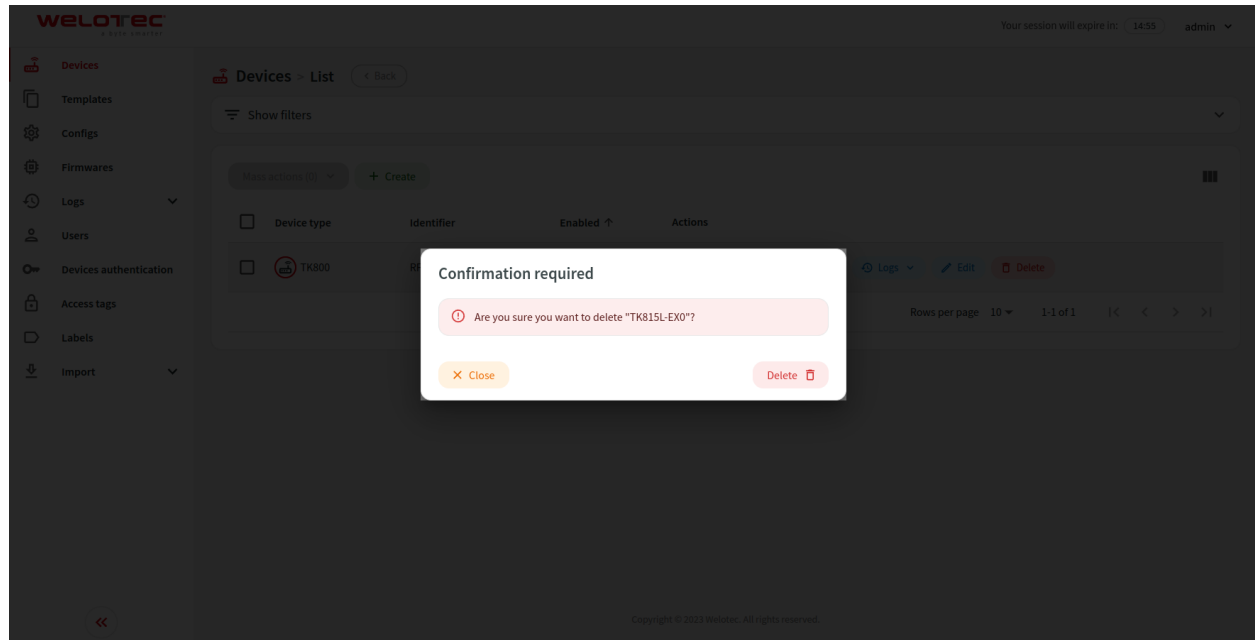
In order to input or change data you will use forms (i.e. to edit or create a device). Such a form consists of inputs that may need filling. When you edit or create information you can click “Submit” to store or update them in our system.



4.5 Dialogs

Modal dialogs appear on top of the content and move the system into a special mode requiring user interaction. This dialog disables the main content until the user explicitly interacts with the modal dialog.

An example use of such dialog is a delete action. In order to perform this action you have to confirm your decision. There are some cases in which deleting some information might lead to additional consequences, you will be informed about them on the delete confirmation screen.



5 Using SMART EMS

5.1 Devices

This section allows you to manage existing devices. Please be aware that by default only a few selected columns are visible, you can adjust them by using the visible columns functionality.

5.1.1 Mass actions

You can perform the following mass actions:

1. Disable
2. Enable
3. Reinstall primary config
4. Reinstall secondary config
5. Reinstall tertiary config
6. Reinstall primary firmware
7. Reinstall secondary firmware
8. Reinstall tertiary firmware
9. Request config data
10. Request diagnose data
11. Add variable
12. Delete variable
13. Set template - Please refer to *Applying a template* section for more information
14. Add access tags
15. Delete access tags
16. Add labels
17. Delete labels
18. Delete

5.1.2 Row actions

You can perform the following extra actions on a single row:

1. Details - Open details about a device. Please refer to the *Details* section for more information.
2. Certificates - Expandable group of actions connected to certificate management. Visible only for devices that support certificates.
 1. Upload separate files - Opens a dialog that allows you to upload a public key, private key and CA certificate.
 2. Upload single file (.p12, .pfx) - Opens a dialog that allows you to upload a public key, private key and CA certificate as a single PKCS #12 file.
 3. Delete certificate - Delete certificates after they are uploaded as separate files or a PKCS #12 file.

4. Download certificate - Download public key as .crt file.
 5. Download private key - Download private key as .key file.
 6. Download CA certificate - Download CA certificate as .crt file.
 7. Download .p12 - Download PKCS #12 file containing public key, private key and CA certificate.
3. Logs - Expandable group of actions connected with logs. Visible only for devices that support logs.
1. Communication logs - View communication logs for the selected device
 2. Device commands - View device commands for the selected device
 3. Config logs - View config logs for the selected device
 4. Diagnose logs - View diagnose logs for the selected device

5.1.3 Applying a template

The template contains a common setup for many devices. When applying a template you can choose what parts of a template will be overwritten in a device. You can select from the following options:

- Device description
- Variables
- Access tags
- Labels

Overwriting means that i.e. in case of variables, existing ones will be removed and variables from the template will be copied into the device.

While applying a template you can also choose to reinstall configs and firmwares that are supported in this template.

Applying a template to a specific device also means that the communication protocol will use configs and firmwares directly from the applied template.

After applying a template to a device, you can change the device description, variables, access tags and labels. This will not affect the template itself or other devices using the same template. The same rule applies from the template perspective. You can change the device description, variables, access tags and labels in the template. For the changes to be transferred to devices, you have to apply the template to a device. Changing config or firmware in the template will affect all devices that are using this template.

Templates support versions. Each template can have one version assigned to “Staging” and one version assigned to “Production”. Devices that have the “Staging” flag set to true will use the “Staging” version of a template. In case the “Staging” version does not exist, such a device will use the “Production” version.

5.1.4 Details

The screen provides detailed information about a single device. The contents of this screen may differ between devices because they may support different functionalities.

You have access to similar actions as described in the “Row actions” section. You can additionally use the “Configs” button which allows you to view generated config for this device. It is only visible for devices that support at least one config.

This section allows you to manage existing templates.

5.2.1 Row actions

You can perform the following extra actions on a single row:

1. Details - Open details about a template. Please refer to the *Details* section for more information.

5.2.2 Details

The screen provides detailed information about a single template.

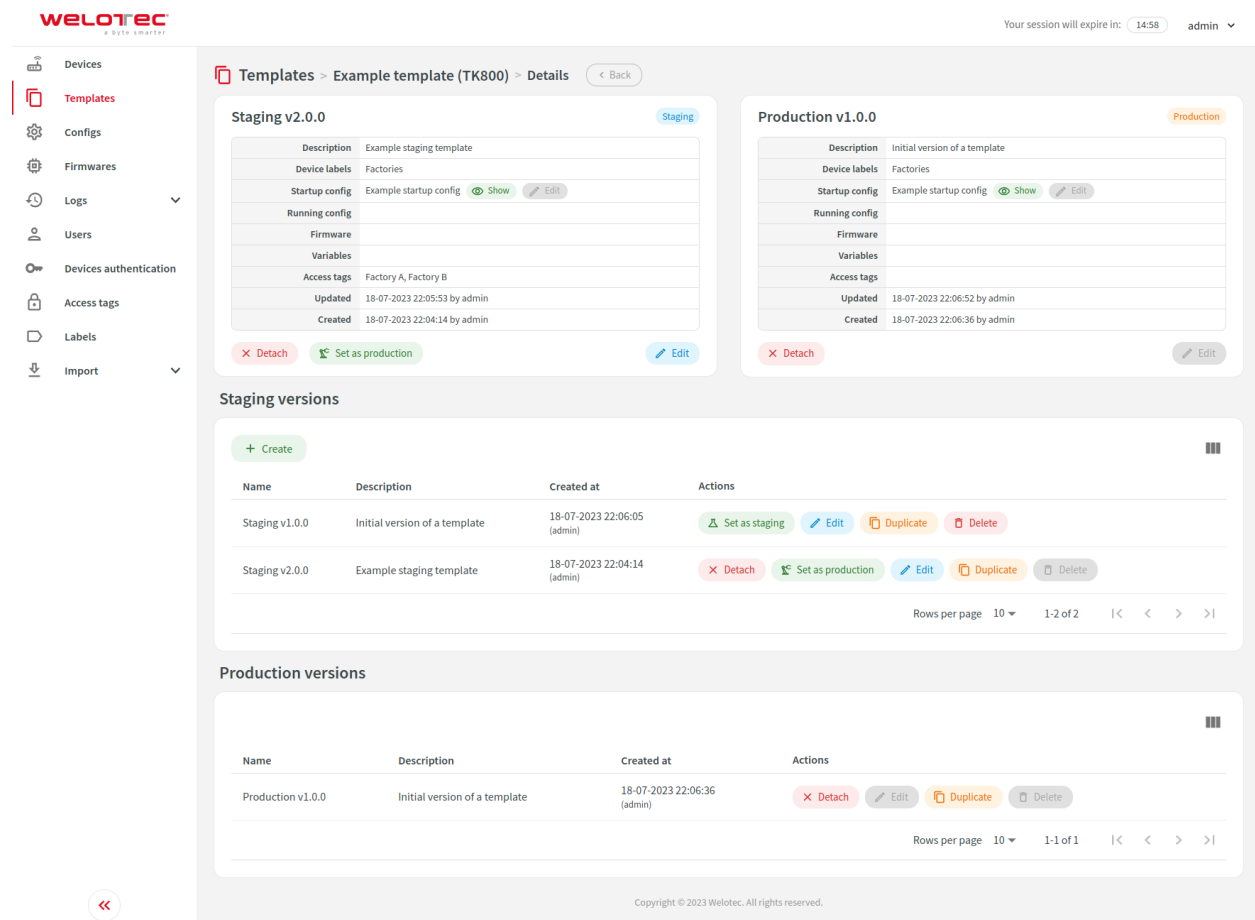
Templates can have multiple versions. Each template can have one version assigned as “Staging” and one version assigned as “Production”. Please refer to the *Applying a template* section for more information about using a template with a device.

When using the “Set as staging” or “Set as production” buttons a dialog will be shown with the possibility to reinstall supported configs and firmwares for all connected devices. For the “Staging” version this will only affect devices that have this template selected and their “Staging” flag is set to true.

A similar possibility is presented when editing the currently selected “Staging” version. When changing configs or firmwares you will see an option to change the connected reinstall flag.

You can also quickly show or edit selected config in the “Staging” version by using buttons in corresponding rows.

The selected “Production” version is not editable to avoid accidental modification of the production environment and keep track of past versions.



WELOTEC BYE SMARTER

Your session will expire in: 14:58 admin

Templates > Example template (TK800) > Details < Back

Staging v2.0.0 Staging

Description	Example staging template
Device labels	Factories
Startup config	Example startup config Show Edit
Running config	
Firmware	
Variables	
Access tags	Factory A, Factory B
Updated	18-07-2023 22:05:53 by admin
Created	18-07-2023 22:04:14 by admin

[Detach](#) [Set as production](#) [Edit](#)

Production v1.0.0 Production

Description	Initial version of a template
Device labels	Factories
Startup config	Example startup config Show Edit
Running config	
Firmware	
Variables	
Access tags	
Updated	18-07-2023 22:06:52 by admin
Created	18-07-2023 22:06:36 by admin

[Detach](#) [Edit](#)

Staging versions

Name	Description	Created at	Actions
Staging v1.0.0	Initial version of a template	18-07-2023 22:06:05 (admin)	Set as staging Edit Duplicate Delete
Staging v2.0.0	Example staging template	18-07-2023 22:04:14 (admin)	Detach Set as production Edit Duplicate Delete

Rows per page 10 1-2 of 2 |< < > >|

Production versions

Name	Description	Created at	Actions
Production v1.0.0	Initial version of a template	18-07-2023 22:06:36 (admin)	Detach Edit Duplicate Delete

Rows per page 10 1-1 of 1 |< < > >|

Copyright © 2023 Welotec. All rights reserved.

5.3 Configs

This section allows you to manage existing configs.

5.3.1 Row actions

You can perform the following extra actions on a single row:

1. Show - Open a dialog with the contents of the selected config.
2. Duplicate - Duplicate selected config.

5.3.2 Content with variables

The content supports variables. This allows you to use a single config for multiple devices (through templates).

There are many predefined variables for every device that supports variables. You can also define custom variables in a device. You can view both defined and predefined variables on the device details screen.

Variables are available inside content as a Twig or PHP (deprecated) variable.

5.3.3 Generators

SMART EMS currently supports two ways of generating configs.

1. Twig config generator - Config is generated using the Twig template engine.
2. PHP config generator - Config is generated by evaluating PHP code (deprecated).

Config generators can be enabled or disabled via Settings. By default PHP config generator is disabled.

You can find more information about the Twig template engine here [Twig](#).

5.4 Firmwares

This section allows you to view a manage existing firmwares.

5.4.1 Row actions

You can perform the following extra actions on a single row:

1. Download - Download uploaded firmware.
2. Show URL - Open a dialog with the external URL of the selected firmware.
3. Duplicate - Duplicate selected firmware.

5.5 Logs

5.5.1 Login attempts

This section allows you to view a list of login attempts.

5.5.2 Device failed login attempts

This section allows you to view a list of device failed login attempts.

5.5.3 Communication logs

This section allows you to view a list of device failed login attempts. Please be aware that by default only a few selected columns are visible, you can adjust them by using the visible columns functionality.

Row actions

You can perform the following extra actions on a single row:

1. Show message - Open a dialog with the contents of a message of the selected communication log.
2. Show content - Open a dialog with the contents of a request or response that is connected to the selected communication log.

5.5.4 Device commands

This section allows you to view a list of device commands. Please be aware that by default only a few selected columns are visible, you can adjust them by using the visible columns functionality.

5.5.5 Config logs

This section allows you to view a list of config logs. Please be aware that by default only a few selected columns are visible, you can adjust them by using the visible columns functionality.

Row actions

You can perform the following extra actions on a single row:

1. Show content - Open a dialog with the contents of the selected config log.
2. Communication logs - Redirects to communication log screen with rows associated with selected config log.

5.5.6 Diagnose logs

This section allows you to view a list of diagnose logs.

Row actions

You can perform the following extra actions on a single row:

1. Show content - Open a dialog with the contents of the selected diagnose log.

5.6 Users

This section allows you to manage existing users.

5.6.1 Row actions

You can perform the following extra actions on a single row:

1. Enable - Allows you to enable the selected user.
2. Disable - Allows you to disable the selected user.
3. Change password - Allows you to change password for the selected user.
4. Reset secret - Allows you to reset secret for the selected user. Only available when two-factor authentication is enabled in the system.
5. Reset login attempts - Allows you to reset login attempts for the selected user. Only visible when the user exceeded the configured limit for failed login attempts.

5.6.2 Access restrictions

Administrator permissions

Users with administrator permissions have access to all functionalities and see all data.

SMART EMS permissions

Users with SMART EMS permissions are restricted to the following screens:

1. Devices
2. Templates
3. Configs
4. Firmwares
5. Logs
 1. Communication logs
 2. Device commands
 3. Config logs
 4. Diagnose logs

This user has limited access to devices based on access tags. Users with SMART EMS permissions will have access to a device when at least one access tag that he has assigned is also assigned to a device.

Templates, firmwares, configs and logs are also limited to only those that are connected to visible devices. User with SMART EMS permissions will not be able to change templates, firmwares and configs that are also used in devices that he does not have access.

Disabled users

Disabled users will not be able to log in to the system. They will be informed that their account is disabled on the login screen.

5.7 Device authentication

This section allows you to manage existing devices authentication.

5.7.1 Access restrictions

Permitted devices

Device authentication has to be restricted to one or more device types. This will allow the device authentication to be used only for permitted device types.

Disabled users

Disabled device authentication will not be able to log in to the system. The system will respond with a 401 Unauthorized response status code.

5.8 Access tags

This section allows you to manage existing access tags.

Access tags are used to restrict access for users with SMART EMS permissions. Please refer to the *SMART EMS permissions* section for more information.

5.9 Labels

This section allows you to manage existing labels.

Labels are intended to be used as a way to freely group devices.

5.10 Import

5.10.1 Devices

This section allows you to import devices using an Excel file. The process is divided into steps.

Step 1

Form with the possibility to upload an import Excel file. You can find more information about the expected column structure on the screen.

WELOTEC

A B2B2C SMARTER

Your session will expire in: 14:38

admin

Devices

Templates

Configs

Firmwares

Logs

Users

Devices authentication

Access tags

Labels

Import

Devices

History

Import > Create

< Back

First row is skipped and designed to describe column names. Router import file should have following columns: Name, Serial number, IMSI, Device type, Template name, Access tags, Labels and Variables (multiple columns). Access tags and labels should be separated using comma (","). Each variable is represented as a pair of columns. First column is variable name and second is variable value. You can use multiple pairs of columns to import multiple variables for one router. Please note that order of columns is important and the import is limited to 10000 rows. You can download example import devices file using button below.

Download example import file

File

Click to choose a file

Click to choose a file

< Back

Submit

Copyright © 2023 Welotec. All rights reserved.

Step 2

The uploaded file is parsed and you are presented with rows that will be imported. Each row also includes a status which can be “Valid”, “Warning” or “Invalid”. Please click on the status icon to see more detailed information.

You can adjust imported rows by changing the data using inputs in columns or using mass actions.

After the imported rows data is ready, please click “Start import”. A dialog will be shown with an option to decide whether variables and access tags should be overwritten from selected templates. After clicking “Submit” the import process will start.

WELOTEC

A B2B2C SMARTER

Your session will expire in: 14:40

admin

Devices

Templates

Configs

Firmwares

Logs

Users

Devices authentication

Access tags

Labels

Import

Devices

History

Import > import-devices-example-file.xlsx > Details

< Back

Start import

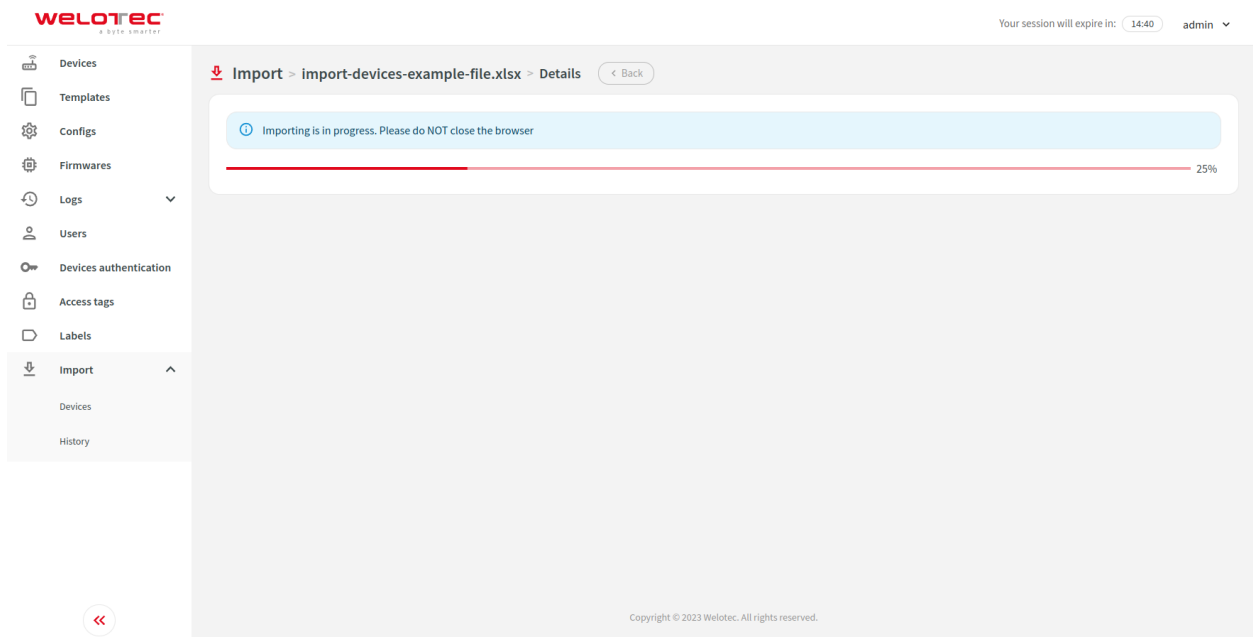
Mass actions (0)

<input type="checkbox"/>	Row	Status	Device type	Name	Serial number	IMSI	Model	Registration ID	Endorsement key	Hardware version	Template
<input type="checkbox"/>	1	✓	TK500	Example router 1	SN12345						Template
<input type="checkbox"/>	2	⚠	Edge gateway	Example router 2	9901001337						Template
<input type="checkbox"/>	3	❗	TK800	Example edge gateway 1	SN23456						Template
<input type="checkbox"/>	4	❗		Example edge gateway 1	SN234156	2.93E+29					

Copyright © 2023 Welotec. All rights reserved.

Step 3

This step informs you about import progress. As soon as it finishes you will be redirected to the next step.



Import > import-devices-example-file.xlsx > Details < Back

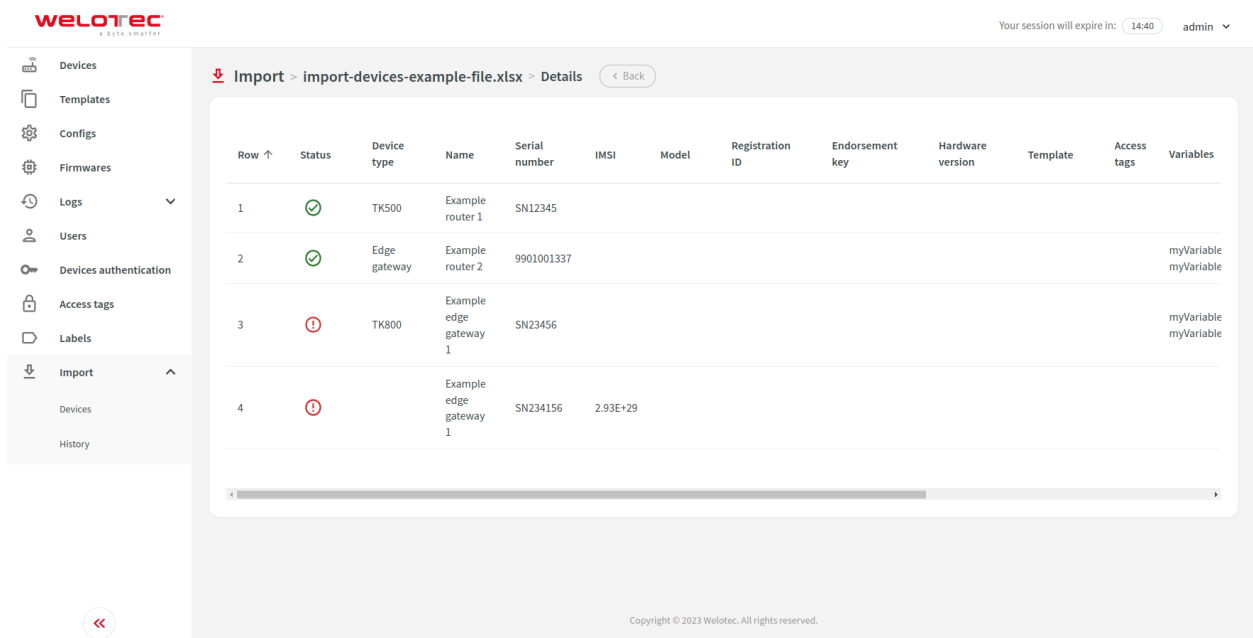
Importing is in progress. Please do NOT close the browser

25%

Copyright © 2023 Welotec. All rights reserved.

Step 4

You can view details about imported rows for this specific import.



Import > import-devices-example-file.xlsx > Details < Back

Row ↑	Status	Device type	Name	Serial number	IMSI	Model	Registration ID	Endorsement key	Hardware version	Template	Access tags	Variables
1	✓	TK500	Example router 1	SN12345								
2	✓	Edge gateway	Example router 2	9901001337								myVariable myVariable
3	⚠	TK800	Example edge gateway 1	SN23456								myVariable myVariable
4	⚠		Example edge gateway 1	SN234156	2.93E+29							

Copyright © 2023 Welotec. All rights reserved.

5.10.2 History

This section allows you to view a list of imports.

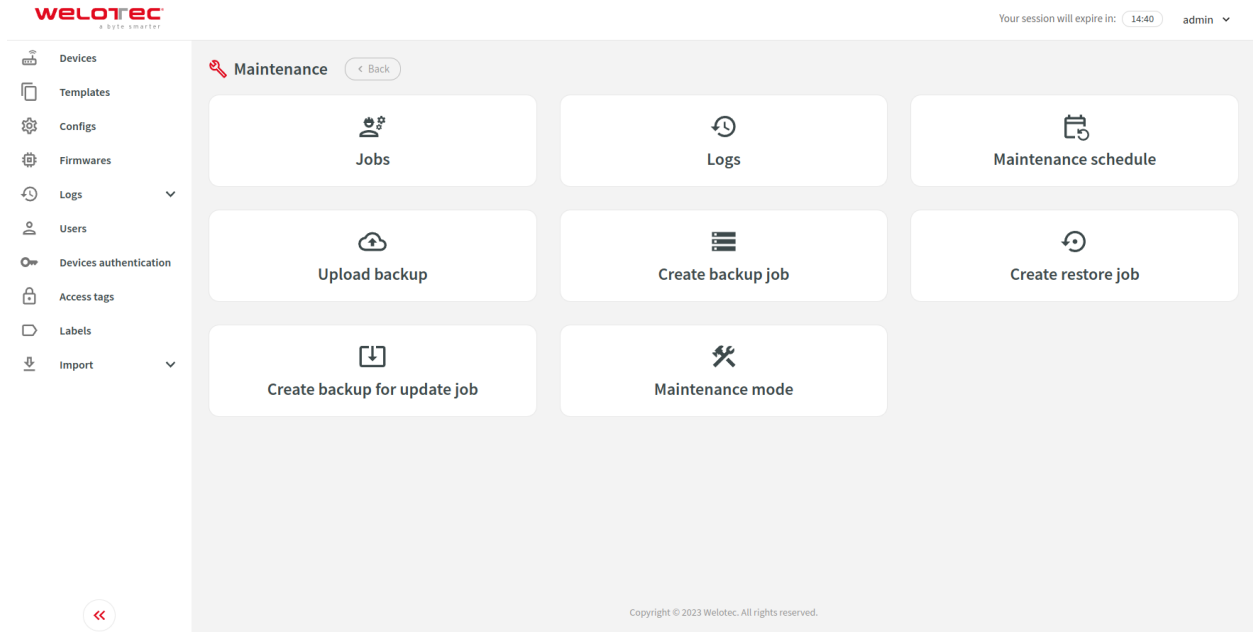
5.10.3 Row actions

You can perform the following extra actions on a single row:

1. Details - Open details about an import. Depending on the status it will redirect you to a proper step.
2. Continue - Continue importing rows. It will redirect you to step 3.

6 Maintenance

You can access the maintenance screen in the navbar menu.



6.1 Jobs

This section allows you to view a list of existing maintenance jobs. Maintenance jobs are executed roughly every minute.

6.1.1 Row actions

You can perform the following extra actions on a single row:

1. Download - Download the backup file. Available only for successful backup maintenance jobs.
2. Logs - View maintenance logs for the selected maintenance job.

6.2 Logs

This section allows you to view a list of existing maintenance logs.

6.3 Maintenance schedules

This section allows you to manage maintenance schedules. Maintenance schedules allow you to define recurring backups.

6.4 Upload backup

This section allows you to upload a backup file. The uploaded backup will be placed in the “backup/” folder located in “/var/www/application/archive” which is by default on the “smartems-volume-archive” volume.

6.5 Create backup job

This section allows you to create a single backup job. After submitting the form, a backup maintenance job will be created.

6.6 Restore backup job

This section allows you to restore a backup from a file. The list of archives to restore is loaded from “backup/” folder located in “/var/www/application/archive” which is by default on “smartems-volume-archive” volume. After submitting the form, a restore maintenance job will be created.

Be careful! Restoring a corrupted or invalid version of a backup will cause the application to malfunction.

6.7 Create backup for update job

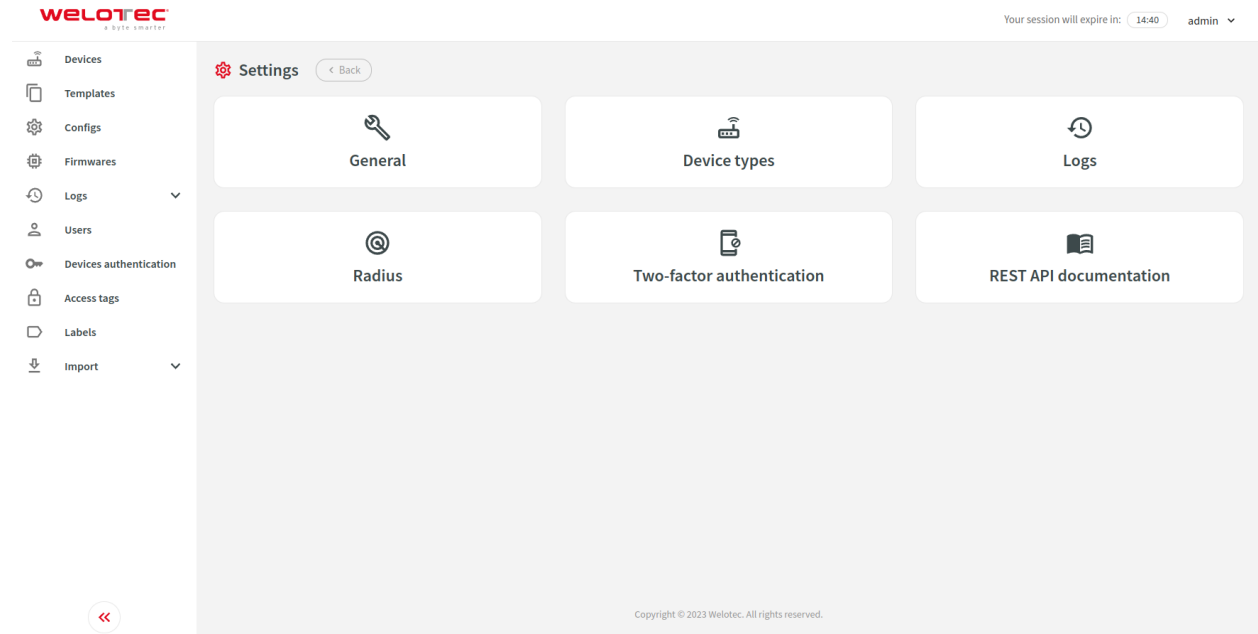
This section allows you to create a backup for update job. It is recommended to activate maintenance mode before preparing a backup for update. After submitting the form, a backup for update maintenance job will be created.

6.8 Maintenance mode

This section allows you to enable or disable maintenance mode. Enabling maintenance mode will reject device communication and disallow access to the application for every user except administrators.

7 Settings

You can access the settings screen in the navbar menu.



7.1 General

This section allows you to adjust general settings for the system i.e. router identifier, config generators, login and password restrictions.

7.2 Device types

This section allows you to manage existing device types.

7.2.1 Row actions

You can perform the following extra actions on a single row:

1. Details - Open details about the selected device type.
2. Duplicate - Duplicate the selected device type.
3. Enable - Allows you to enable the selected device type.
4. Disable - Allows you to disable the selected device type.

7.2.2 Communication procedure

Devices communicate with SMART EMS to deliver many functionalities including managing configuration, updating firmwares, gathering diagnose data, sending logs and managing secure VPN connection. Some communication procedures are tailored to a specific device, while others (i.e. edge gateway communication procedure) are designed to be easily integrated with third-party devices. Communication procedures can require some functionalities to be enabled in a device type to be able to support designed functionalities.

Please contact Welotec directly to get guidance and detailed information about working with communication procedures or integrating third-party devices.

7.2.3 Edit form

When editing a device type that already has some devices created, this form will be limited only to fields that can be modified without creating dangerous inconsistencies in existing devices.

7.3 Logs

This section allows you to adjust settings for cleanup duration and size of different types of logs.

7.4 Radius

This section allows you to adjust settings for radius authentication.

7.5 Two-factor authentication

This section allows you to adjust settings for two-factor authentication (TOTP).

7.6 Single Sign-on (SSO)

This section allows you to adjust settings for single sign-on (SSO).

7.6.1 Microsoft Entra ID with OpenID Connect

You can configure SMART EMS to use OpenID Connect to sign-in users via Azure portal App.

You can find “Application (client) ID” and “Directory (tenant) ID” in your Azure Application under “Overview”. You can read more about “Credential” options below. Please refer to “Roles” section under “Azure Application configuration” and fill “Role mappings”.

After clicking “Submit”, a new button “Log in using Microsoft” will be visible on SMART EMS login screen.

Client secret credential

On your Azure Application please navigate to “Certificates & secrets” (“Manage” section), click “New client secret”, fill the form according to your needs and click “Add”. Value in “Value” of created client secret will be needed to configure SMART EMS.

Uploaded certificate credential

Please upload public and private key. Public key should be uploaded to your Azure Application on “Certificates” tab in “Certificates & secrets” (“Manage” section).

Generated certificate credential

You can generate public and private key by checking “Generate public and private key” and saving the form. You will be able to view or download generated public key afterwards. It should be uploaded to your Azure Application on “Certificates” tab in “Certificates & secrets” (“Manage” section).

Azure Application configuration

Please navigate to “App registrations”, select your application and navigate to “Authentication” (“Manage” section). Please add platform for “Web” and add to “Redirect URIs” your SMART EMS URL followed by /authentication/sso/microsoftoidc/login (i.e. <https://example.com/authentication/sso/microsoftoidc/login>).

Please navigate to “Certificates & secrets” (“Manage” section) and configure it according to selected “Credential” in SMART EMS.

preferred_username claim can be used to have human readable username for the user. In order to use it please navigate to “Token configuration” (“Manage” section) and click “Add optional claim”. Select “Token type” ID, check preferred_username claim and click “Add” to apply the changes.

In order to support front-channel logout (recommended) please also configure “Front-channel logout URL”. Use your SMART EMS URL followed by /web/api/authentication/sso/microsoftoidc/logout (i.e. <https://example.com/web/api/authentication/sso/microsoftoidc/logout>). You also need to adjust token configuration. Please navigate to “Token configuration” (“Manage” section) and click “Add optional claim”. Select “Token type” ID, check sid claim and click “Add” to apply the changes.

Roles

In order to assign roles to specific groups or users please navigate to “App roles” (“Manage” section). Please click “Create app role” and fill the form according to your needs. Please take into consideration that value set in “Value” field is used by SMART EMS to map roles in the application.

In order to map roles in SMART EMS please navigate to “Settings” (click on your username in top right corner) and “Single sign-on (SSO)”. Under “Role mappings” you can set user permissions for each role that has been created in “App roles”.

7.7 REST API documentation

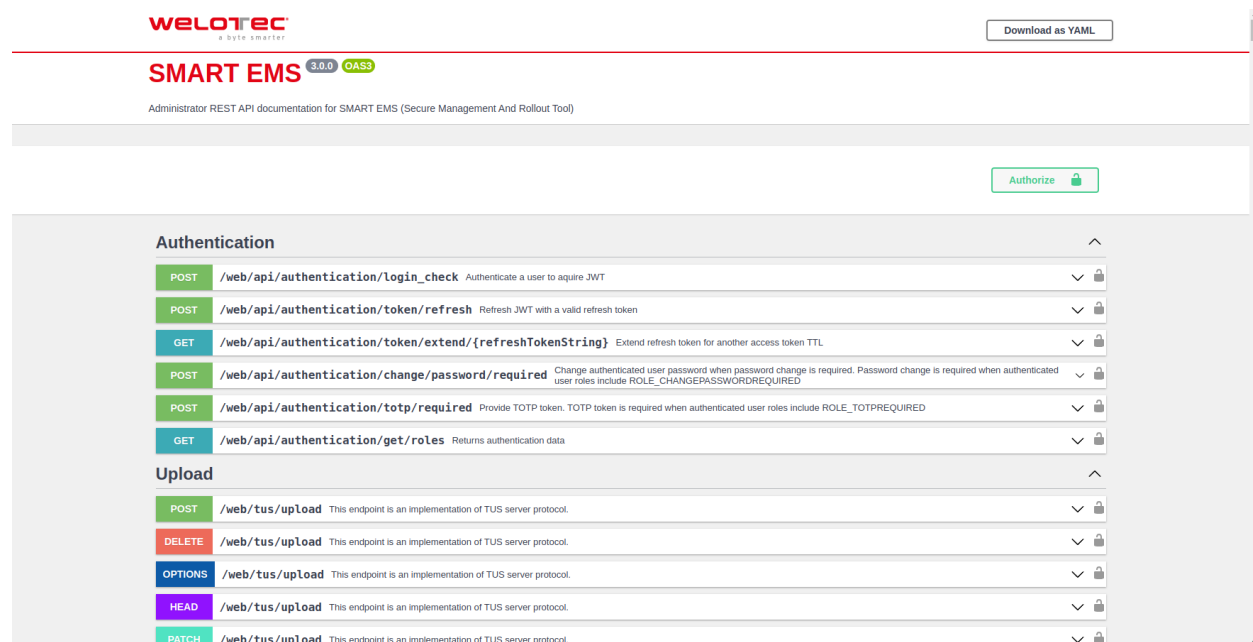
This section allows you to enable or disable REST API documentation for specific users.

8 REST API Documentation

You can access REST API documentation in the navbar menu. This option might be disabled by the Administrator.

REST API documentations are limited to user permissions. Users with administrator permissions and SMART EMS permissions have separate REST API documentation.

This screen allows you to read through REST API documentation described using OpenAPI 3.0 (OAS 3.0) standard and visualised by Swagger UI. You can also download the OpenAPI specification as a YAML file by clicking the “Download as YAML” button in the top right corner.



SMART EMS 3.0.0 OAS3

Administrator REST API documentation for SMART EMS (Secure Management And Rollout Tool)

[Download as YAML](#)

[Authorize](#)

Authentication

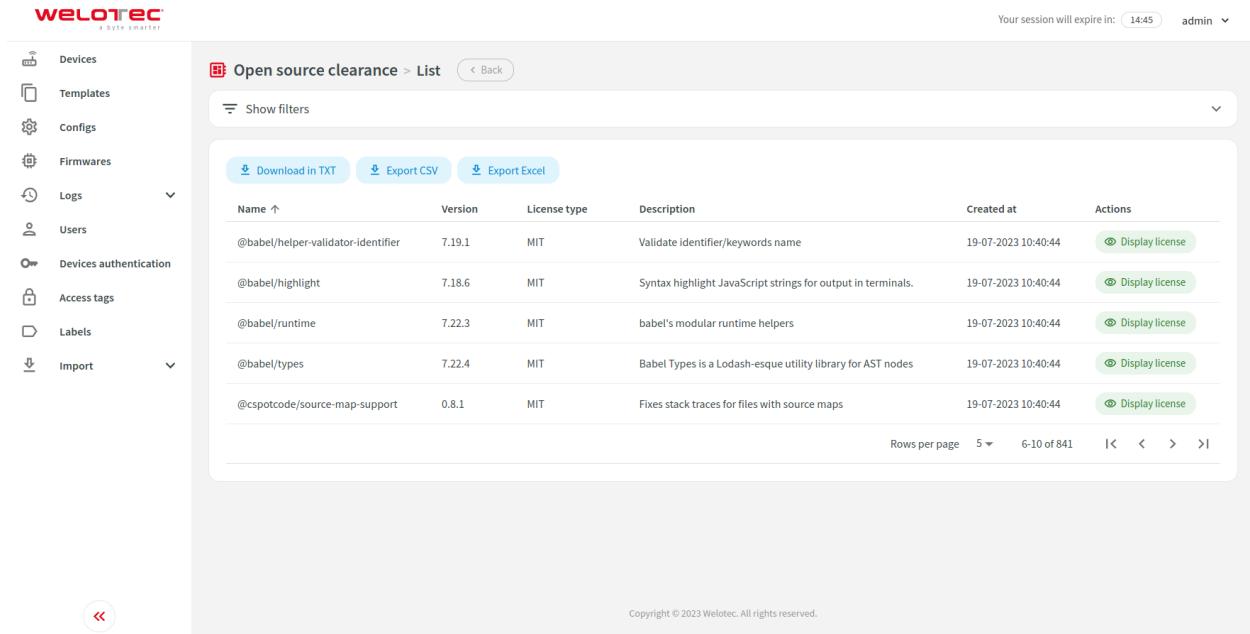
Method	Endpoint	Description
POST	/web/api/authentication/login_check	Authenticate a user to acquire JWT
POST	/web/api/authentication/token/refresh	Refresh JWT with a valid refresh token
GET	/web/api/authentication/token/extend/{refreshTokenString}	Extend refresh token for another access token TTL
POST	/web/api/authentication/change/password/required	Change authenticated user password when password change is required. Password change is required when authenticated user roles include ROLE_CHANGEPASSWORDREQUIRED
POST	/web/api/authentication/totp/required	Provide TOTP token. TOTP token is required when authenticated user roles include ROLE_TOTPREQUIRED
GET	/web/api/authentication/get/roles	Returns authentication data

Upload

Method	Endpoint	Description
POST	/web/tus/upload	This endpoint is an implementation of TUS server protocol.
DELETE	/web/tus/upload	This endpoint is an implementation of TUS server protocol.
OPTIONS	/web/tus/upload	This endpoint is an implementation of TUS server protocol.
HEAD	/web/tus/upload	This endpoint is an implementation of TUS server protocol.
PATCH	/web/tus/upload	This endpoint is an implementation of TUS server protocol.

9 Open source clearance

You can access the open source clearance screen in the navbar menu.



Open source clearance > List [Back](#)

Show filters

Download in TXT Export CSV Export Excel

Name ↑	Version	License type	Description	Created at	Actions
@babel/helper-validator-identifier	7.19.1	MIT	Validate identifier/keywords name	19-07-2023 10:40:44	Display license
@babel/highlight	7.18.6	MIT	Syntax highlight JavaScript strings for output in terminals.	19-07-2023 10:40:44	Display license
@babel/runtime	7.22.3	MIT	babel's modular runtime helpers	19-07-2023 10:40:44	Display license
@babel/types	7.22.4	MIT	Babel Types is a Lodash-esque utility library for AST nodes	19-07-2023 10:40:44	Display license
@cspotcode/source-map-support	0.8.1	MIT	Fixes stack traces for files with source maps	19-07-2023 10:40:44	Display license

Rows per page: 5 6-10 of 841 |< < > >|

Copyright © 2023 Welotec. All rights reserved.

9.1 List actions

You can perform the following extra list actions:

1. Download in TXT - Download open source clearance as a TXT file.

9.2 Row actions

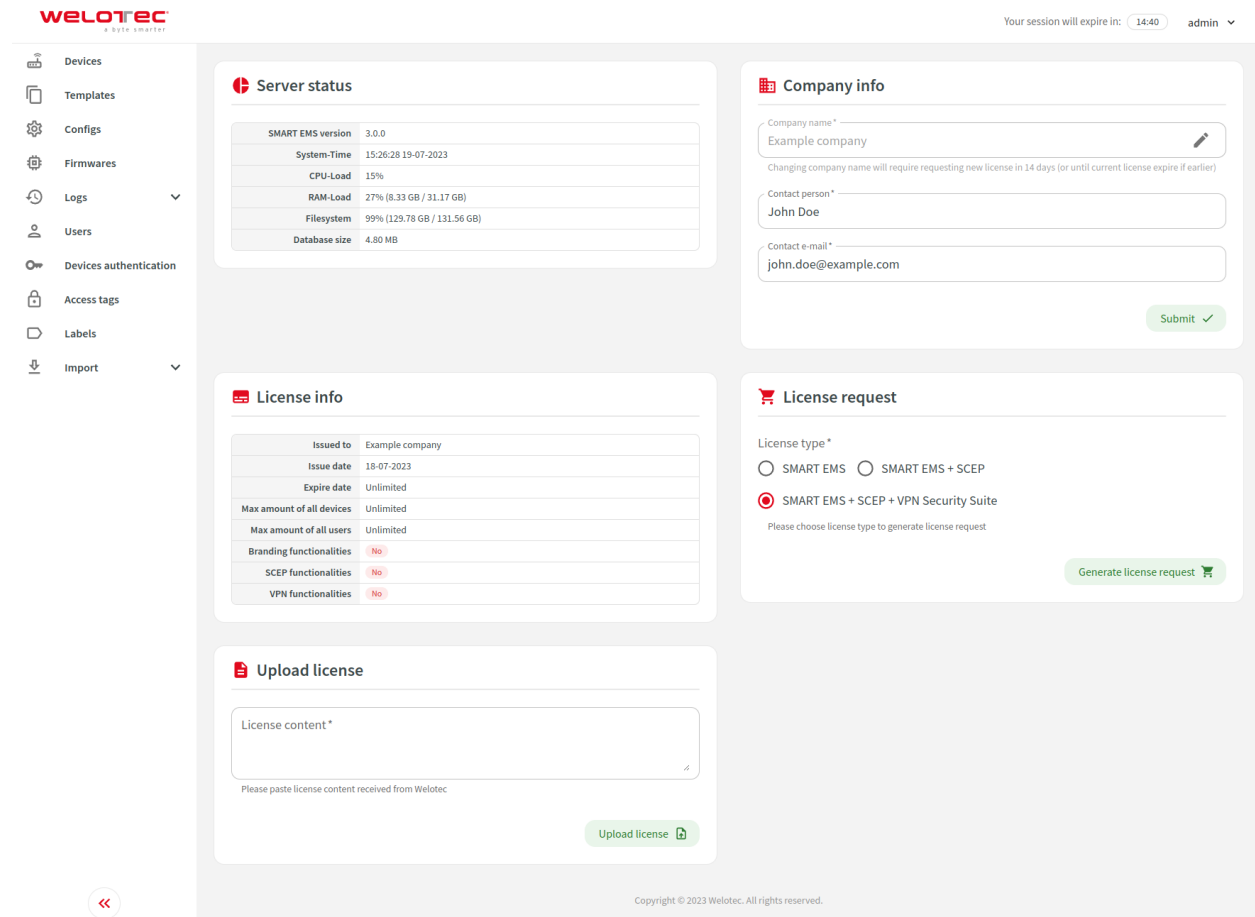
You can perform the following extra actions on a single row:

1. Display license - Open a dialog with the license.

10 Status and license

You can access the status and license screen in the navbar menu.

This screen allows you to see server status, license status, adjust company information, generate license request and upload license.



The screenshot shows the Welotec web interface for managing status and licenses. The top navigation bar includes the Welotec logo, a session timer (14:40), and a user dropdown (admin). The left sidebar contains a menu with items: Devices, Templates, Configs, Firmwares, Logs, Users, Devices authentication, Access tags, Labels, and Import. The main content area is divided into four panels:

- Server status:** A table showing system metrics:

SMART EMS version	3.0.0
System-Time	15:26:28 19-07-2023
CPU-Load	15%
RAM-Load	27% (8.33 GB / 31.17 GB)
Filesystem	99% (129.78 GB / 131.56 GB)
Database size	4.80 MB
- Company info:** A form for company details. Fields include Company name (Example company), Contact person (John Doe), and Contact e-mail (john.doe@example.com). A green 'Submit' button is at the bottom right.
- License info:** A table showing license details:

Issued to	Example company
Issue date	18-07-2023
Expire date	Unlimited
Max amount of all devices	Unlimited
Max amount of all users	Unlimited
Branding functionalities	No
SCEP functionalities	No
VPN functionalities	No
- License request:** A form for requesting a license. It has a 'License type' section with three radio buttons: SMART EMS, SMART EMS + SCEP, and SMART EMS + SCEP + VPN Security Suite (which is selected). A green 'Generate license request' button is at the bottom right.

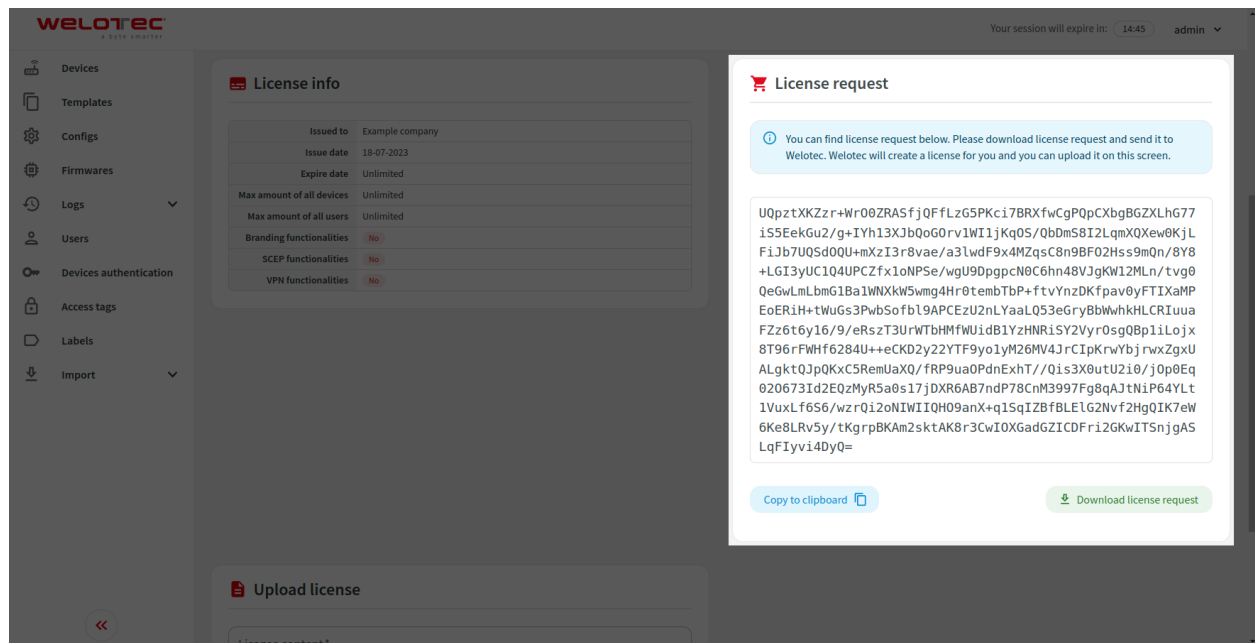
At the bottom of the main content area is an 'Upload license' panel with a text area for 'License content' and a green 'Upload license' button. A footer note at the bottom center reads 'Copyright © 2023 Welotec. All rights reserved.'

10.1 Requesting license

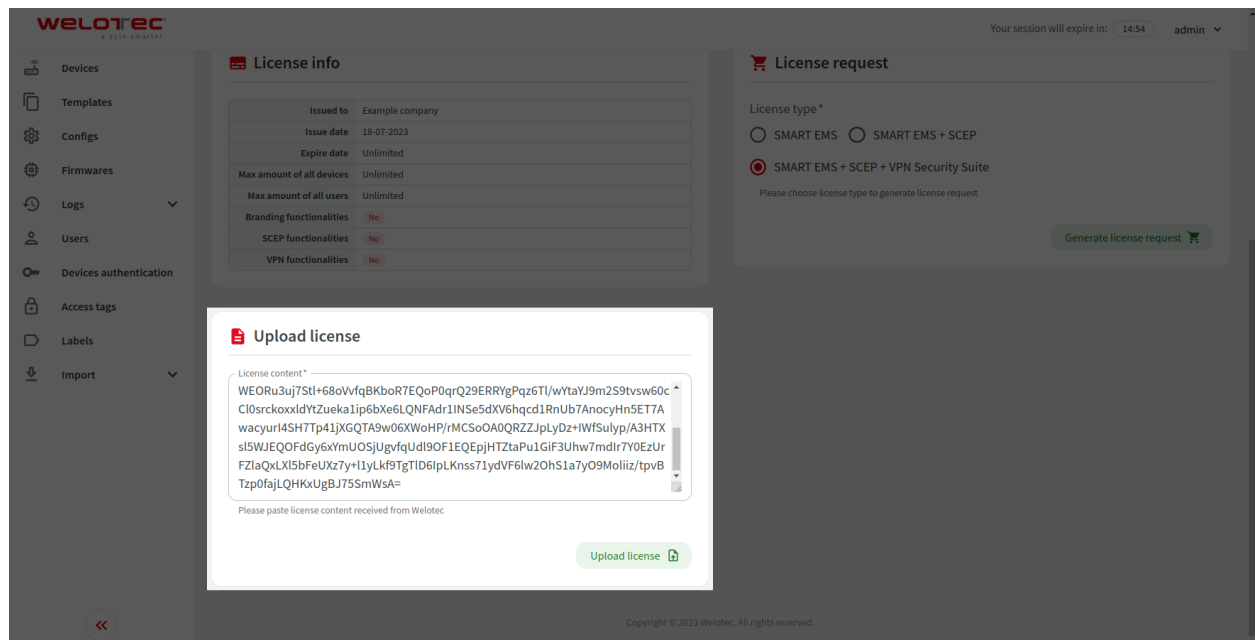
You can request a license of a specific type:

- SMART EMS
- SMART EMS + SCEP
- SMART EMS + SCEP + VPN Security Suite

Please select license type and click “Generate license request”.



License request will be shown. You can copy it to a clipboard or download it to a file. Please send generated license request to Welotec so we can generate an appropriate license for you. The generated license should be uploaded to the system using the “Upload license” form.



10.2 License expiration

In case of license expiry, the system will switch back to the demo license. When the demo license expires, the system will run in maintenance mode.