VPN Security Suite

Version:
v3.4.0

Date:
18.11.2025

Contents

1 Introduction

This document intends to provide information and instruction on using a VPN Security Suite which is part of 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

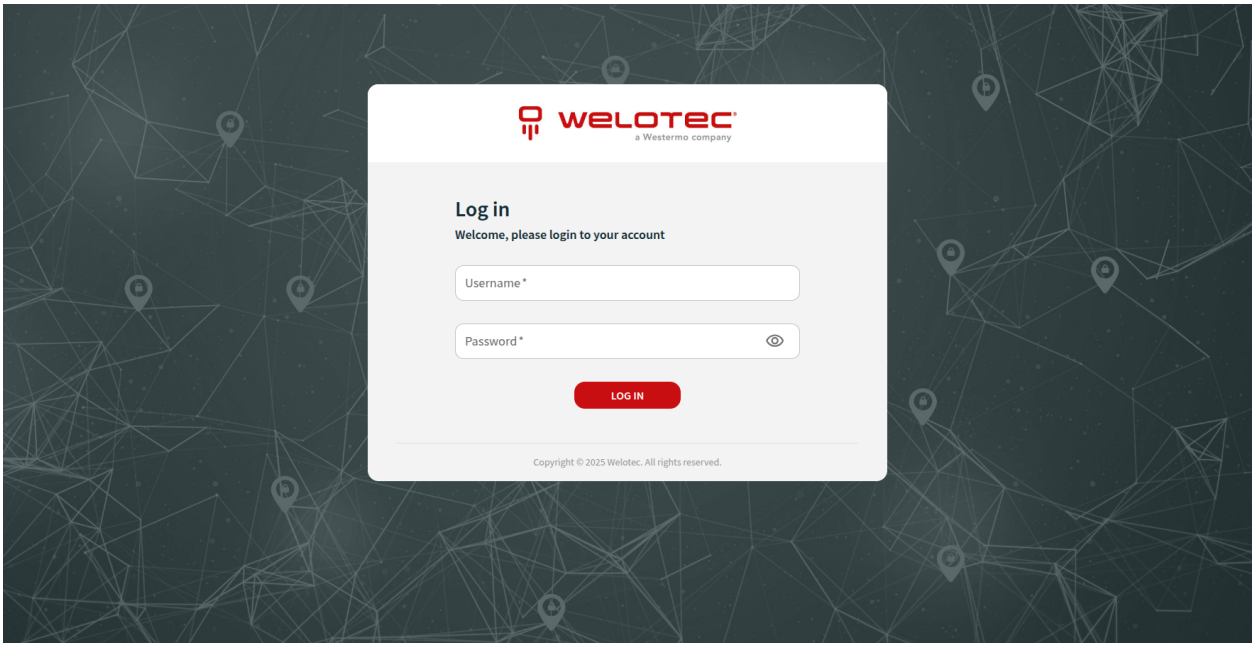
Website: www.welotec.com

2 Changelog

Version	Date	Log
v3.4.0	18.11.2025	Added hardware files functionality. Added firmware update path functionality. Device variables type casting added. Extended HTTPS server SSL certificates to support RSA and Elliptic Curve (EC) keys. Update PHP to 8.4.14.
v3.3.7	22.09.2025	Added mariadb server validation flag.
v3.3.6	09.09.2025	Update PHP to 8.4.11. Fix PHP license version information. Fix RCE vulnerability.
v3.3.5	14.08.2025	Fix invalid serialization of Edge Gateway config using plain format. Fix REST API documentation missing some properties in response schemas. Extend custom redirect URL functionality for Microsoft Entra ID using OpenID Connect (Single Sign-On) with additional endpoint. Add possibility to configure CORS related headers. Register login attempt when successfully logged in using Microsoft Entra ID using OpenID Connect (Single Sign-On). Update default branding. Add visible columns search bar. Add configuration that allows VPN users created by SSO to have technician VPN certificate generated.
v3.3.4	01.04.2025	Added possibility to enable endpoint with a custom redirect URL for Microsoft Entra ID using OpenID Connect (Single Sign-On). Added force device secret renewal on next device communication functionality. VPN Container Client communication used with Edge gateway with VPN Container Client communication procedure will not generate or renew device secrets anymore.
v3.3.3	26.02.2025	Restructure logs to increase performance for databases with large amount of logs. Group logs sent by VPN Container Client into a single log entry to increase readability. Obfuscate sensitive data on UI by default with a possibility to reveal them. Remove automatic version fill up for devices that are not routers. Fix edge case when changing VPN subnet configuration. Fix REST API documentation for user with VPN permissions. Add support for selecting labels on import devices screen.
v3.3.2	17.12.2024	Improve migration performance
v3.3.1	12.11.2024	Update default branding. Extend users that have VPN permission with option to manage endpoint devices
v3.3.0	19.08.2024	Lower number of layers in docker image. Upgrade to PHP 8.3 and Symfony 6.4. Add audit logs and device secrets. Add device secrets authentication and device x509 authentication. Updated firmware download URL format.
v3.2.1	19.06.2024	Certificate type functionality added, Updated VPN IP handling
v3.1.4	11.04.2024	Improve performance of database queries for logs. Add configurable Content-Security-Policy header. Fix invalid OpenVPN client CSC handling during SSL certificate autorenewal. TK500v3 device type added
v3.1.3	20.02.2024	Allow router commmunication 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.



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.

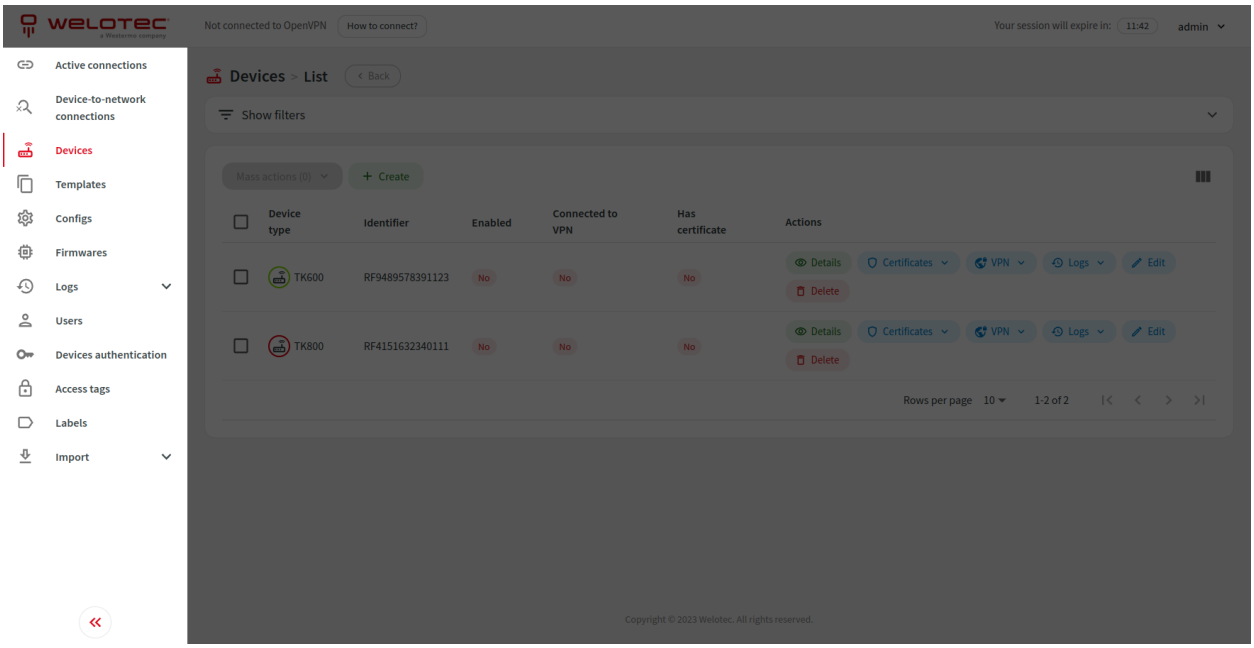
4.1 Branding

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

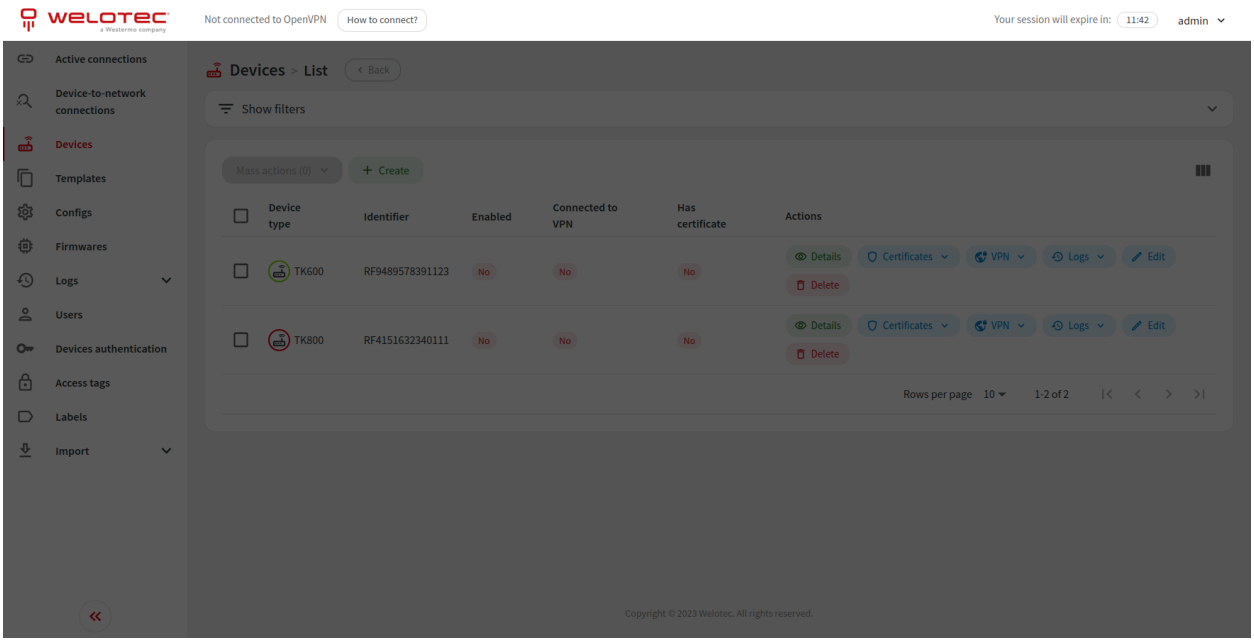
4.2.1 Sidebar

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.

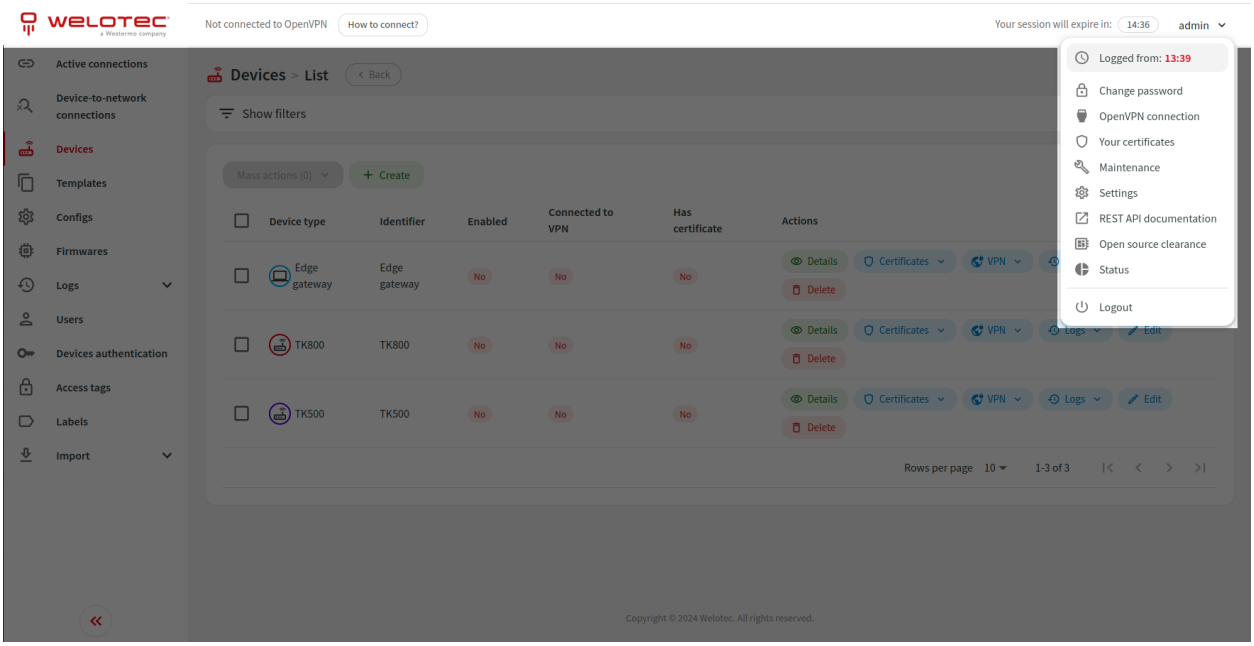


4.2.2 Navbar

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

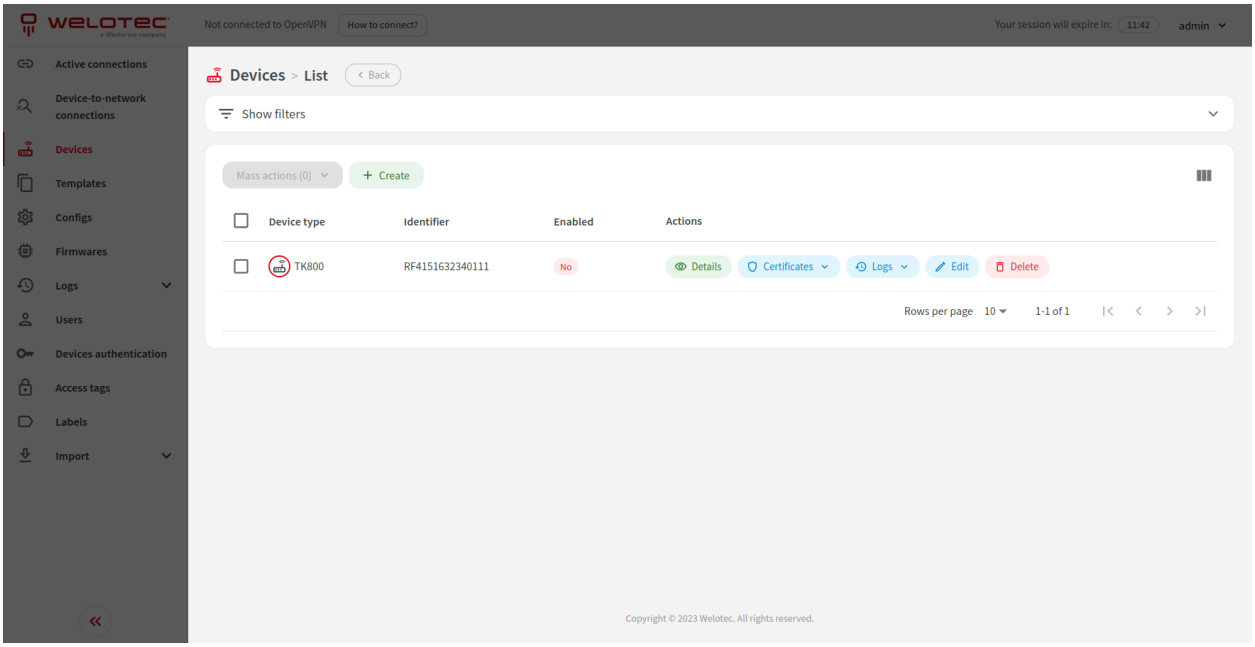


An expandable menu with additional options is available after clicking on the username.



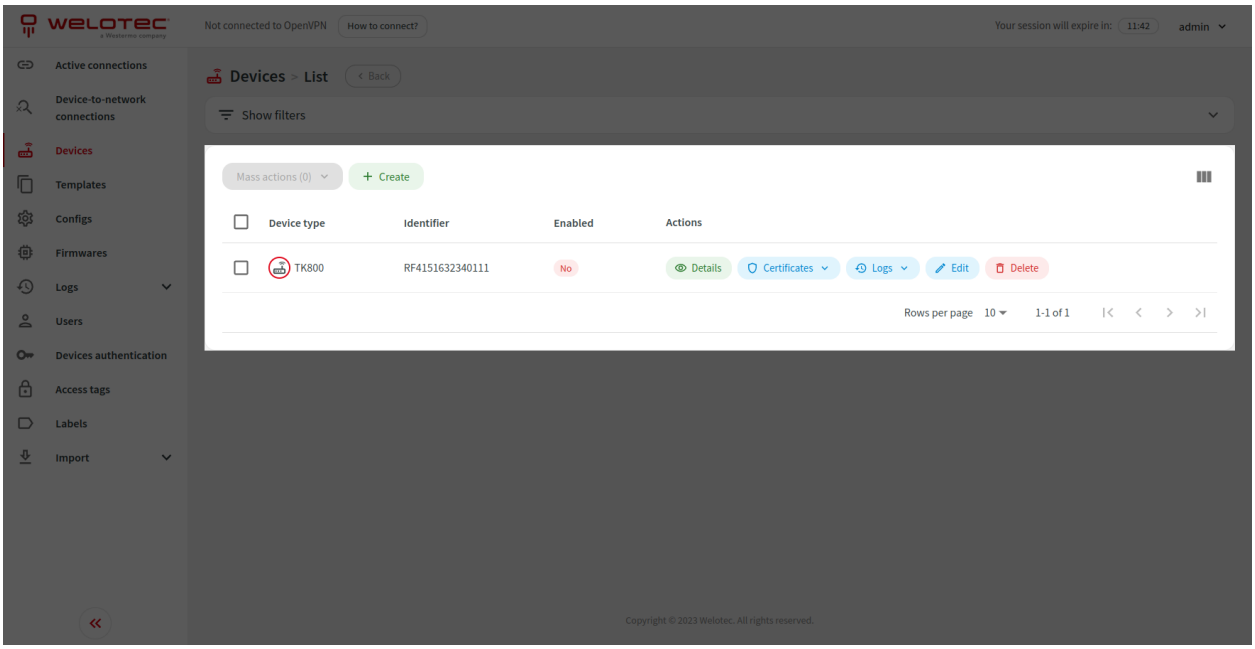
4.2.3 Content

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



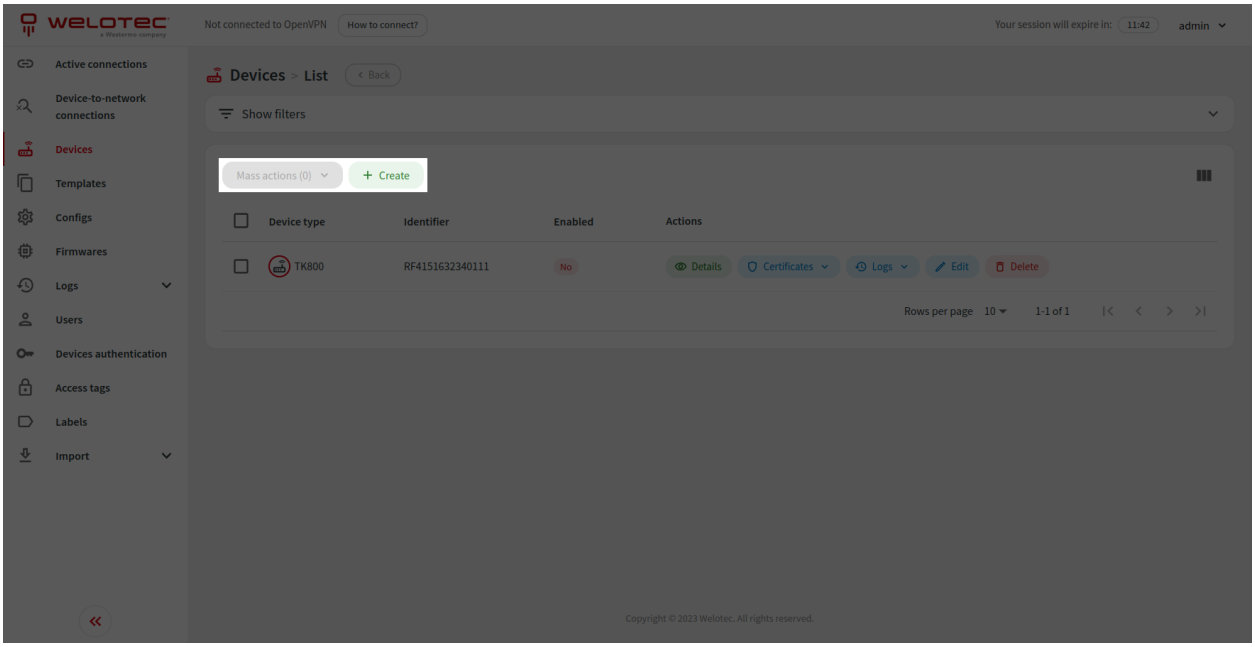
4.3 List view

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



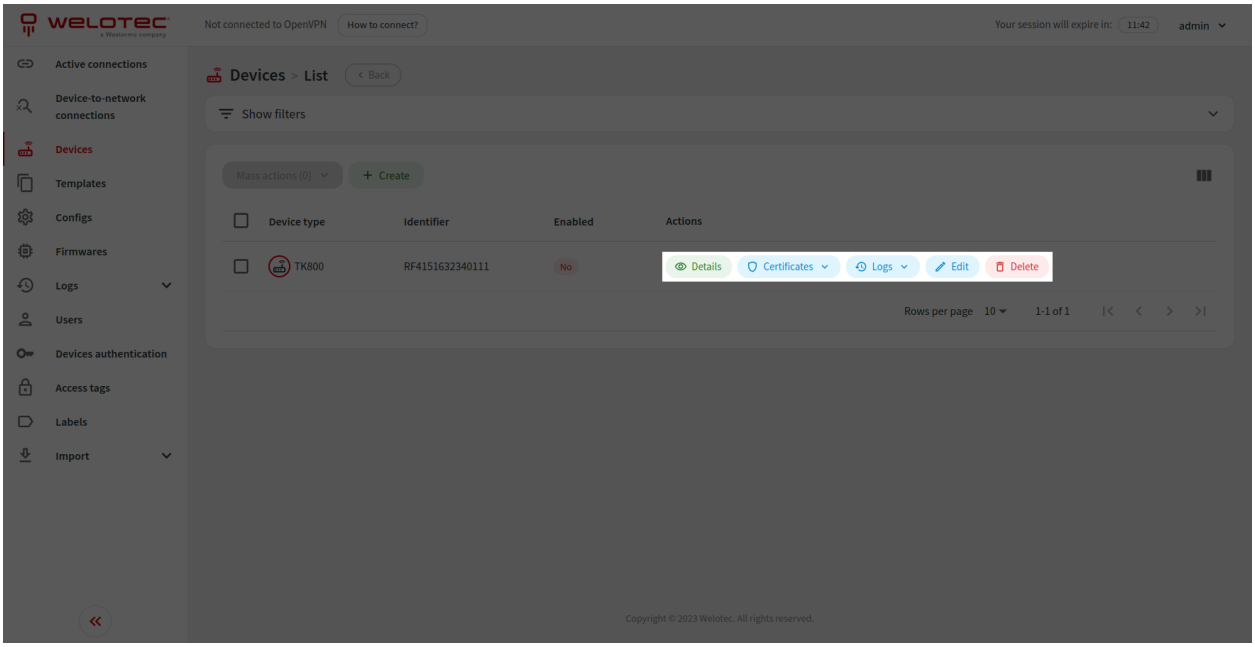
4.3.1 List actions

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



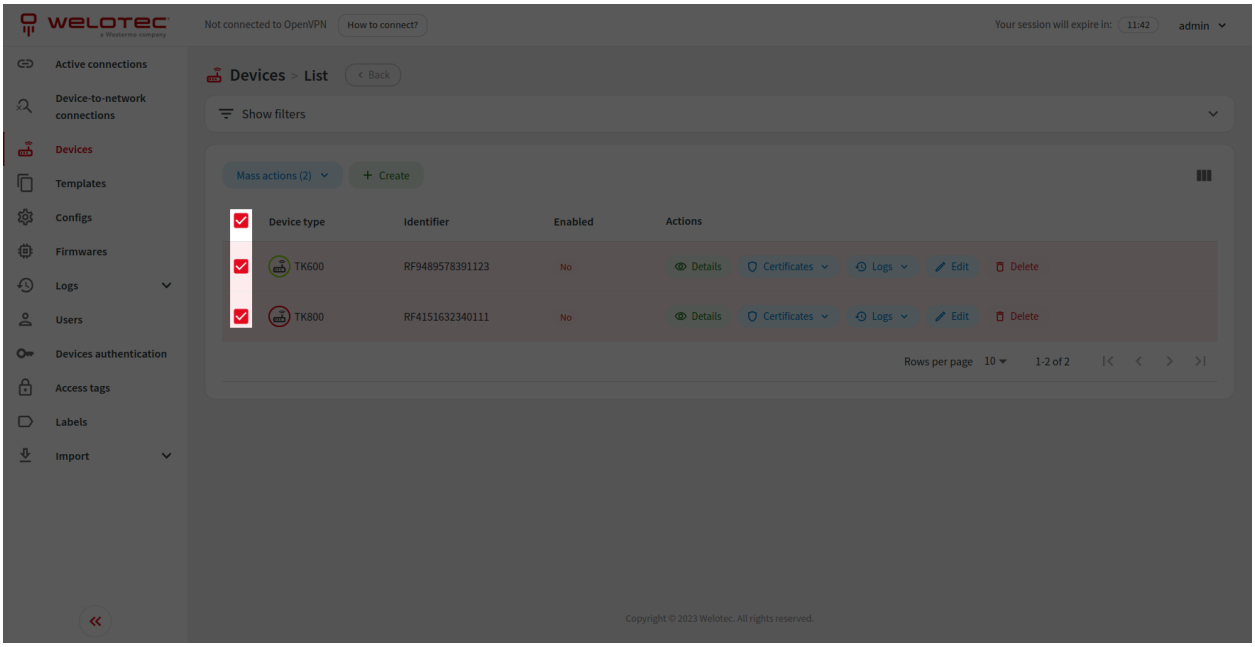
4.3.2 Row actions

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.

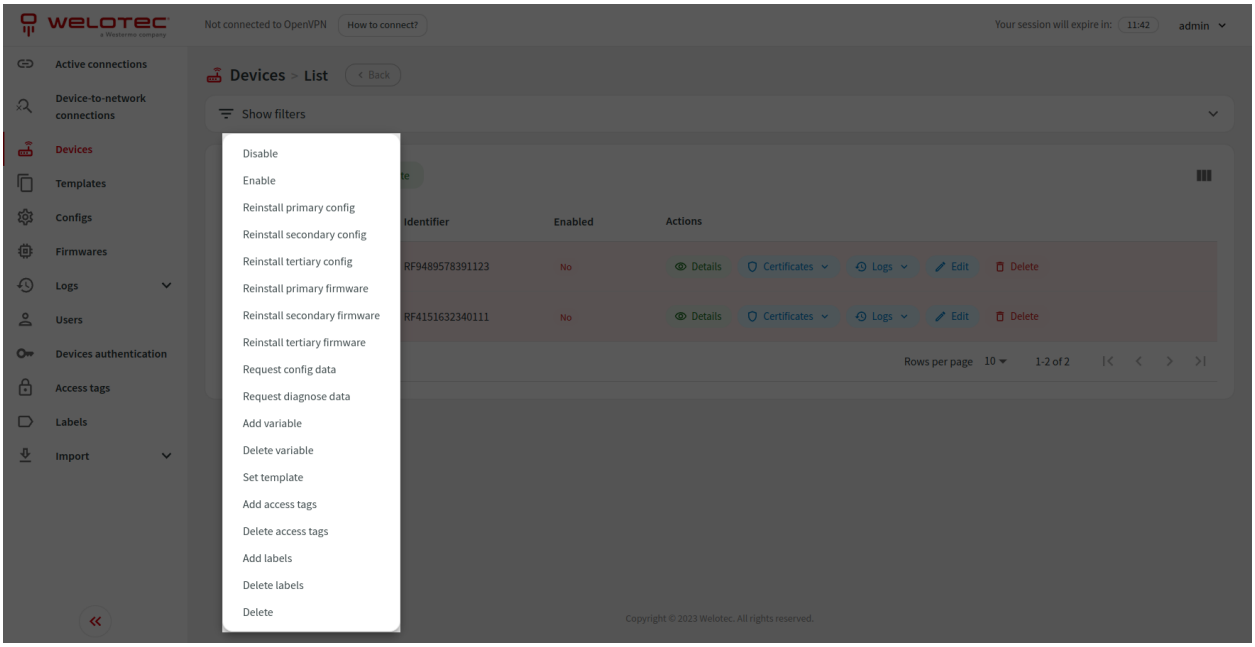


4.3.3 Mass actions

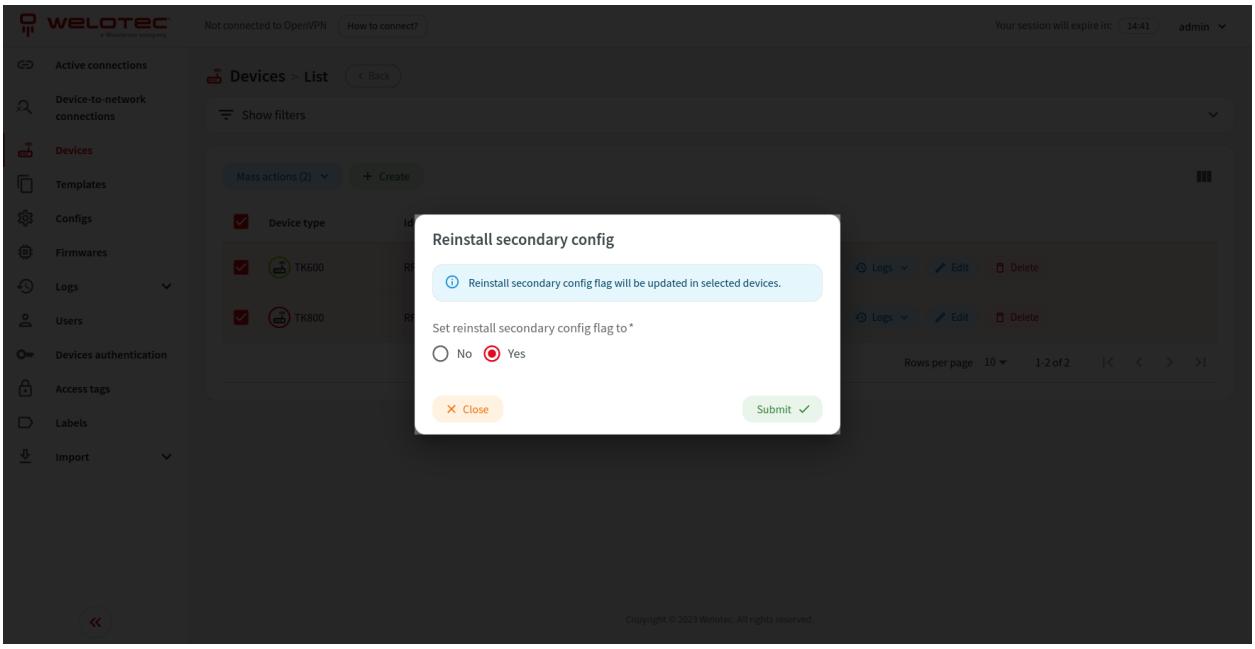
Mass actions give you the possibility to perform an operation on multiple selected rows (i.e. multiple devices). You can select rows using checkboxes in the first column in the table. You can also use the checkbox in the header of a table to select all visible rows.



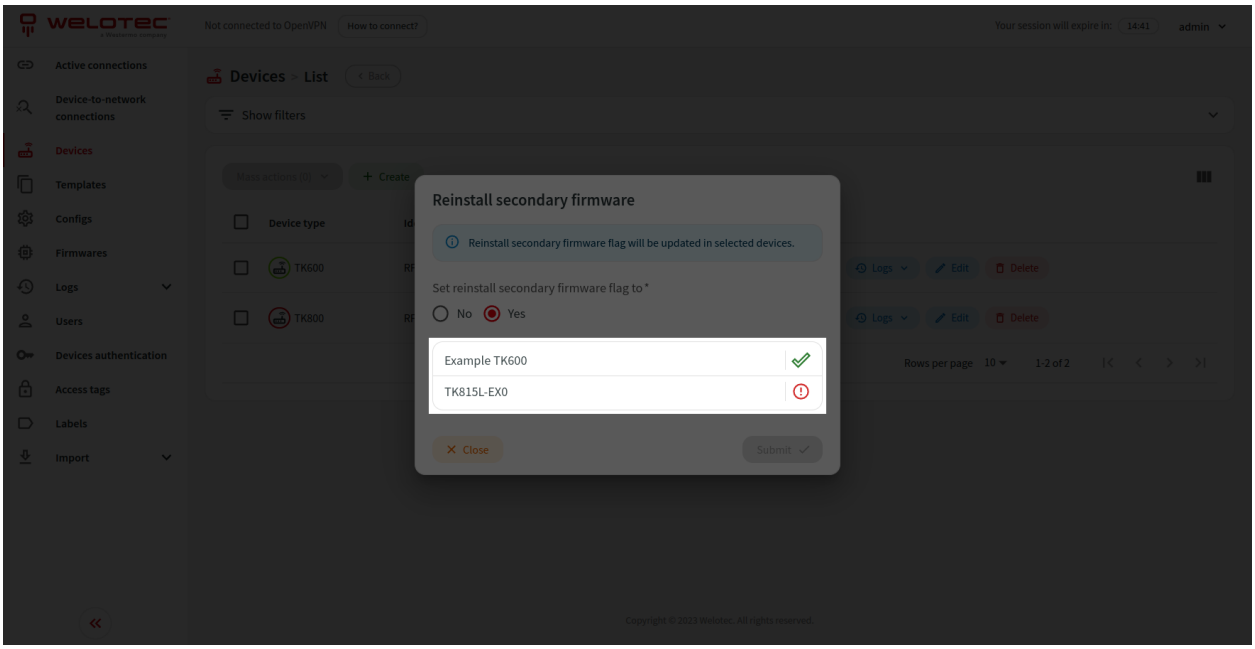
When at least one row is selected “Mass actions” button becomes usable. Clicking on the “Mass actions” button will expand possible mass actions.



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.

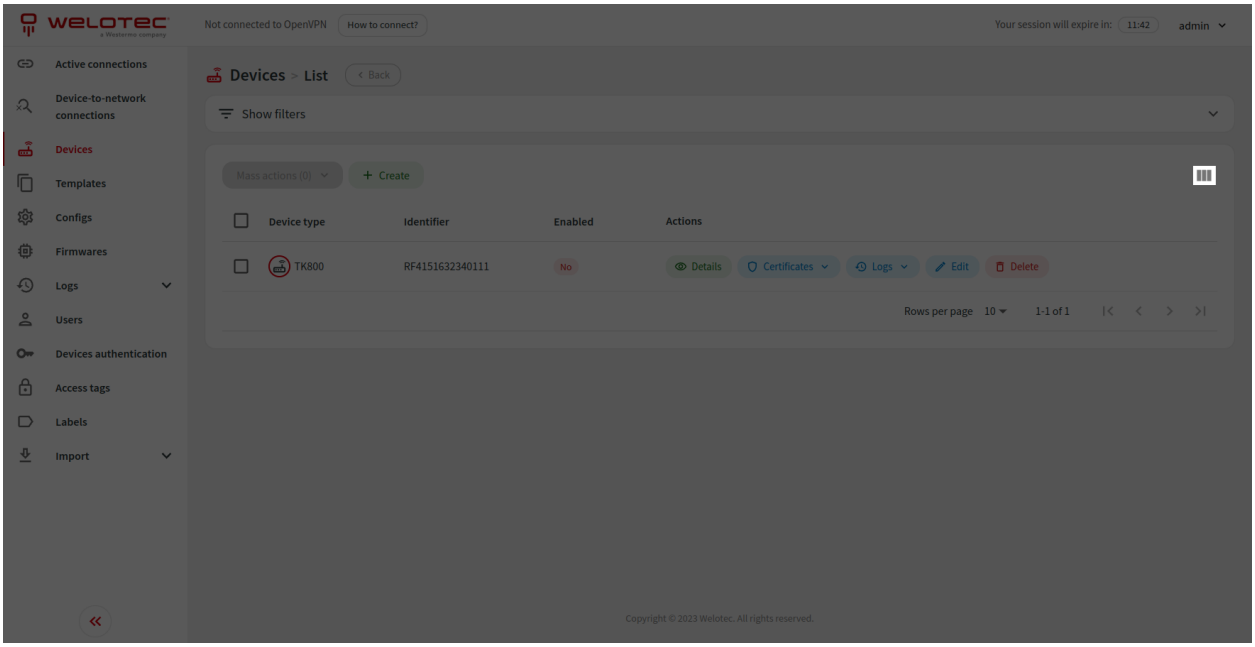


You will get feedback from the system about the status of executed action for each row. Each action can be executed successfully, executed with warnings, executed with errors or skipped. You can hover over the status icon to get a tooltip with detailed information.

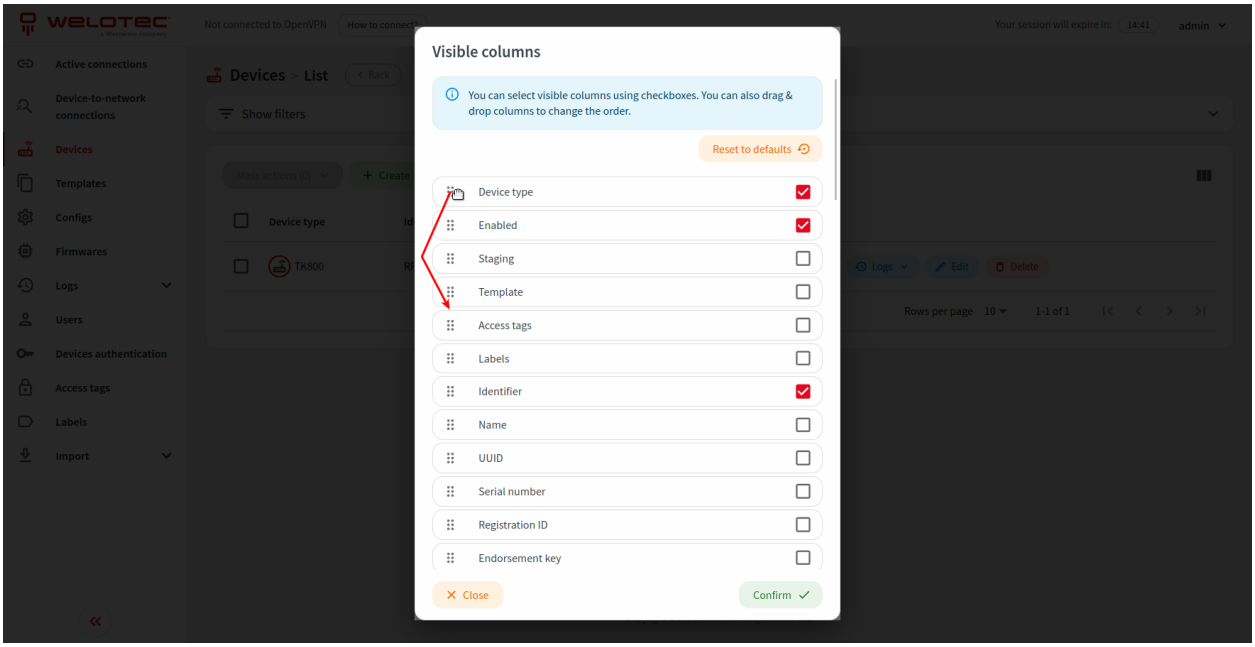


4.3.4 Visible columns

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

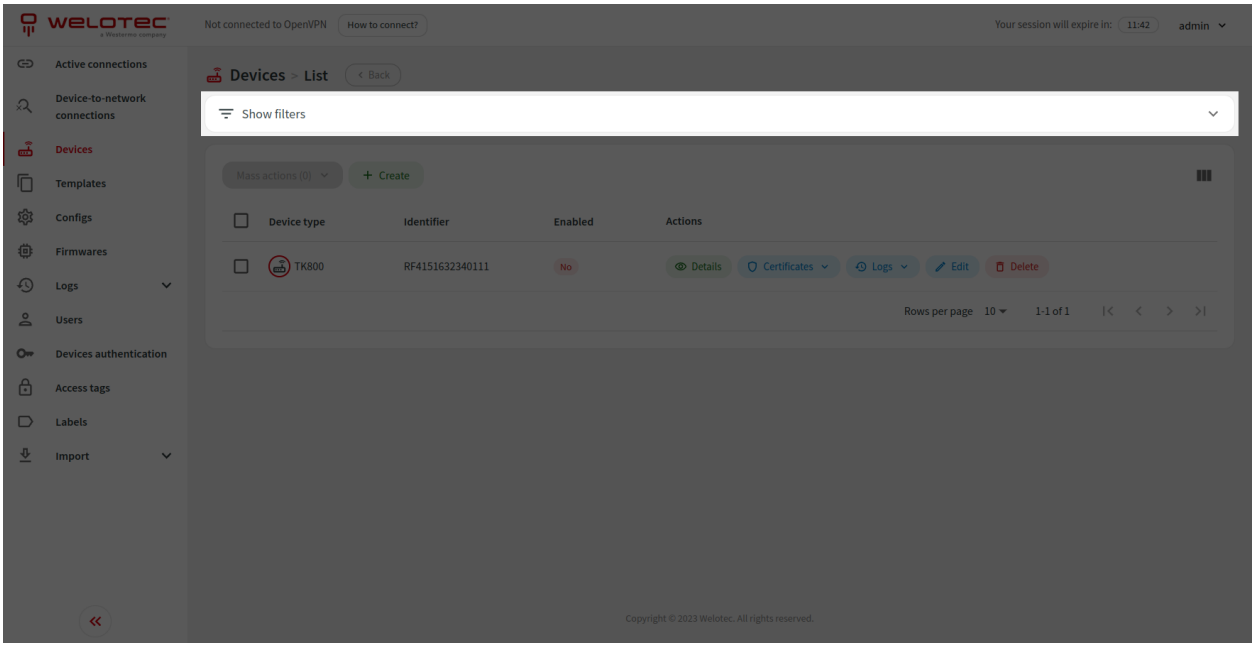


Visible columns dialog will be shown. It will allow you to select visible columns and adjust their order by using the drag & drop technique. Afterward please the changes by clicking the “Confirm” button. You can also reset visible columns to defaults by clicking the “Reset to defaults” button.

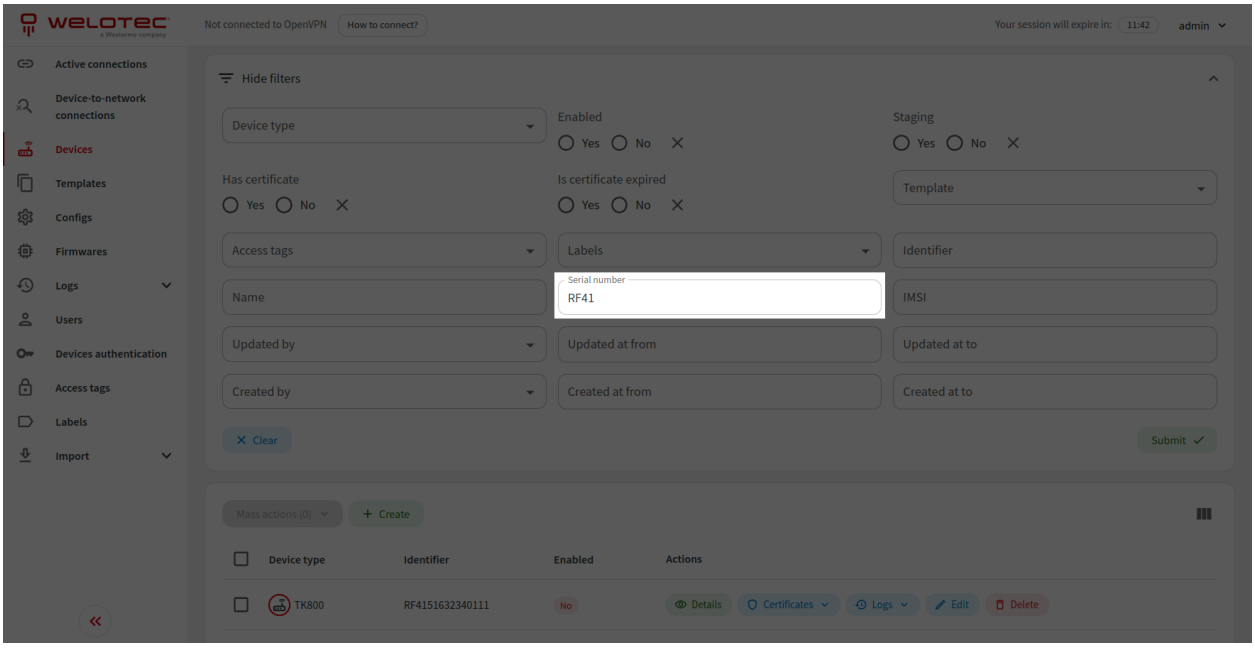


4.3.5 Filtering list results

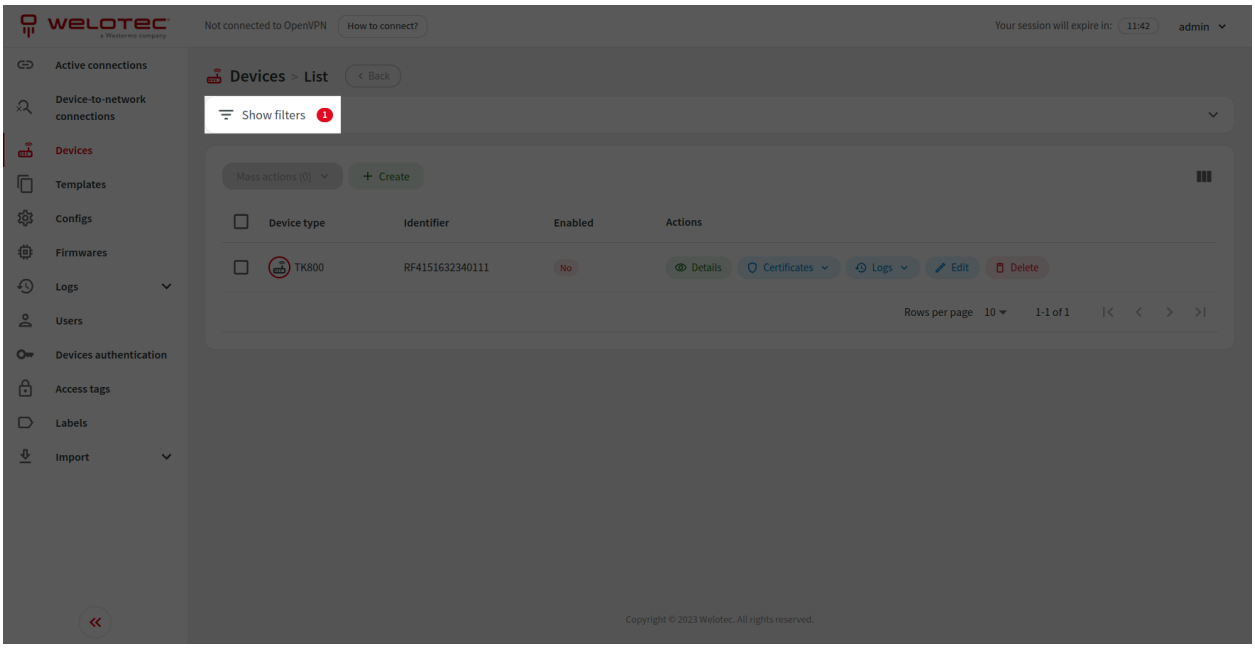
Visible results on the list can be filtered according to available filters. You can find an expandable “Show filters” section.



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”.

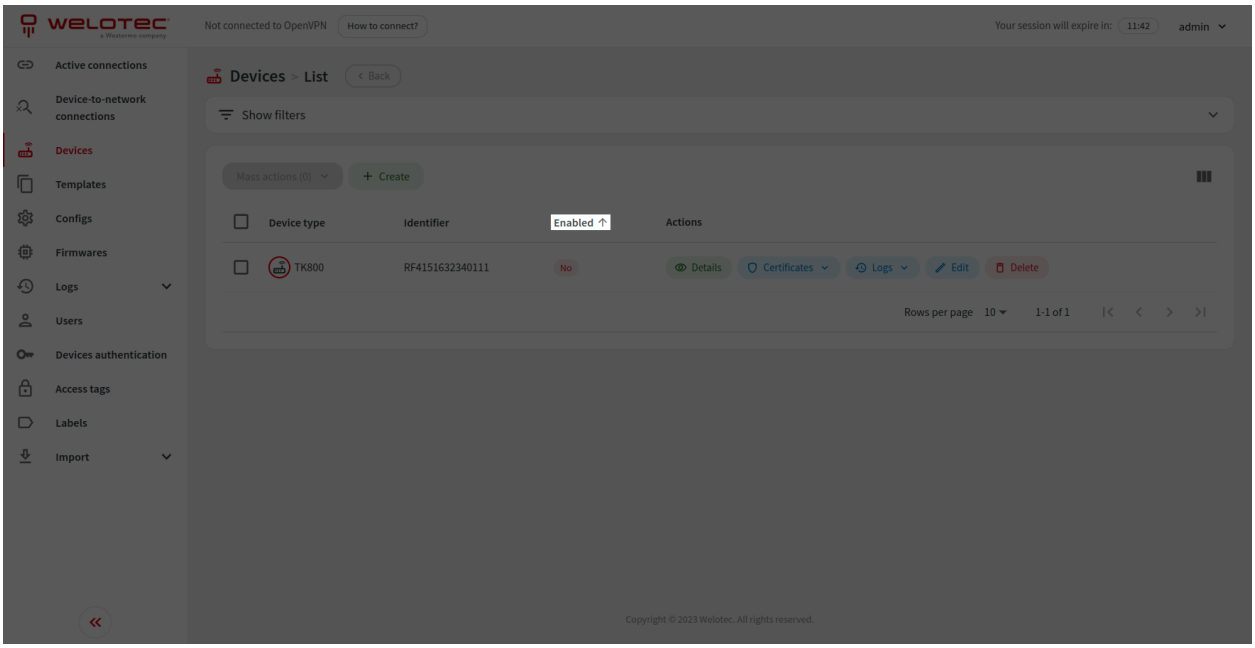


There is an additional indicator (a badge) on the “Show filters” section in case any of the available filters are currently active.



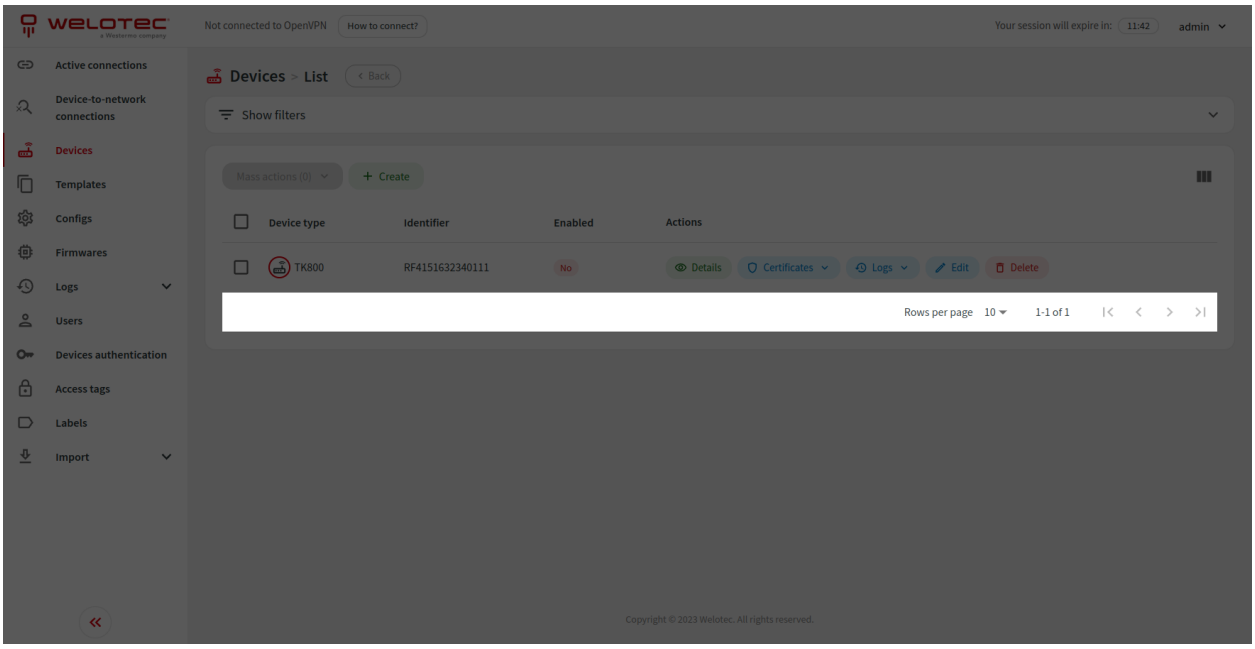
4.3.6 Sorting list results

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



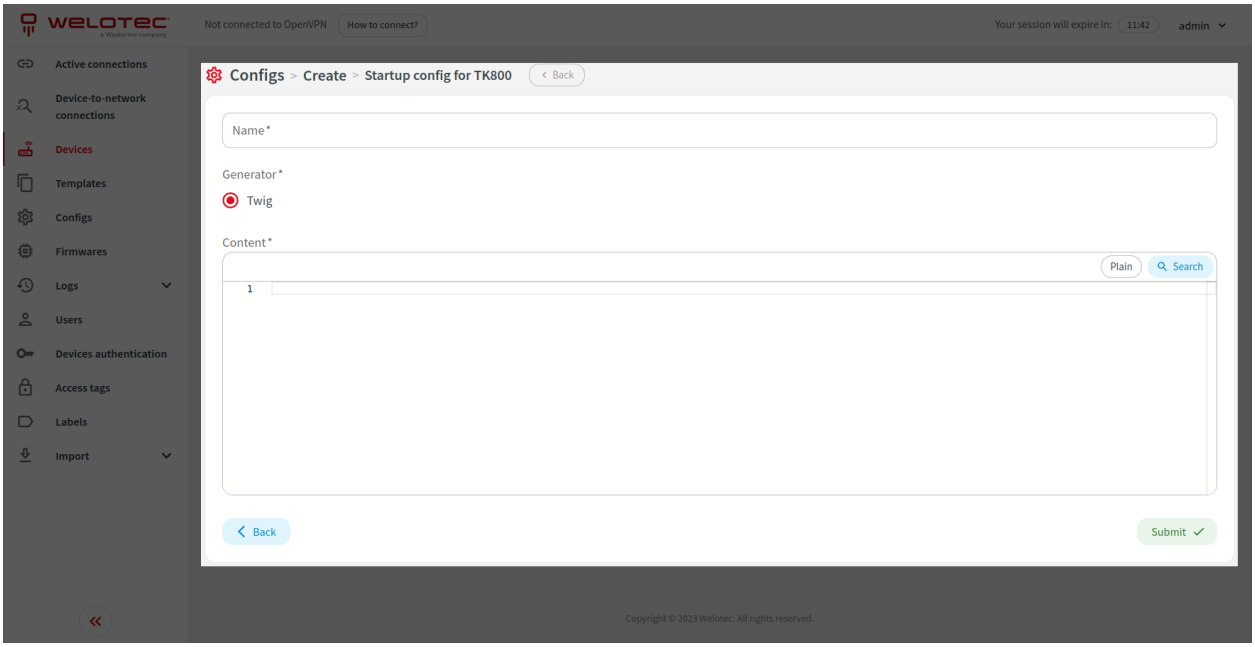
4.3.7 List pagination

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



4.4 Forms

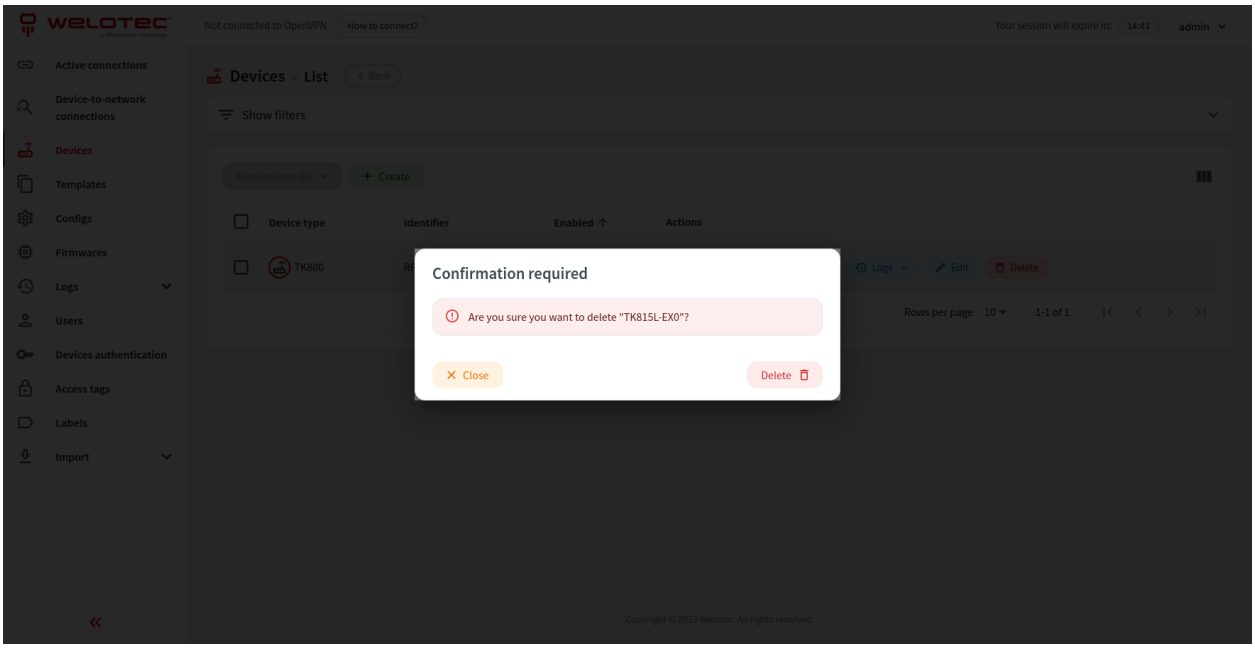
In order to input or change data you will use forms (i.e. to edit or create a device). Such a form consists of inputs that may need filling. When you edit or create information you can click “Submit” to store or update them in our system.



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 VPN Security Suite

5.1 Active connections

This section allows you to view and manage all active connections between users and devices. In order to connect to a device please refer to *OpenVPN connection* chapter.

5.1.1 Row actions

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

1. Close connection - Close the selected active connection between the user and the device.

5.2 Device-to-network connections

This section allows you to view and manage all active device-to-network connections. Device-to-network connections do not expire and are managed by enabled devices that support device-to-network connection functionality (i.e. Monitoring system device). In order to close them, please disable the connected device.

5.3 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.

5.3.1 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 the *Applying a template* section for more information
14. Add access tags
15. Delete access tags

16. Add labels
17. Delete labels
18. Delete

5.3.2 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 of the selected device. Visible only for devices that support certificate types.
    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. Generate certificate - Generate certificate using PKI Server. Available only for certificate types that support PKI certificates.
    5. Revoke certificate - Revoke certificate using PKI Server. Available only for certificate types that support PKI certificates.
    6. Download certificate - Download public key as .crt file.
    7. Download private key - Download private key as .key file.
    8. Download CA certificate - Download CA certificate as .crt file.
    9. Download .p12 - Download PKCS #12 file containing public key, private key and CA certificate.
3. VPN - Expandable group of actions connected with VPN functionalities. You can read more about connections and OpenVPN in the *OpenVPN connection* chapter. Visible only for devices that support VPN.
    1. Connect - Establish a connection between the currently logged-in user and the selected device.
    2. Connect to all - Establish a connection between the currently logged-in user, the selected device and all its endpoint devices. Available only for devices that have at least one endpoint device.
    3. Close my connection - Close the connection between the currently logged-in user and the selected device.
    4. Close multiple connections - Close multiple connections for the selected device. Opens a dialog that allows you to select multiple connections to close.
    5. Download OpenVPN configuration - Download OpenVPN configuration file for the selected device.
4. 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. VPN logs - View VPN logs for the selected device

5.3.3 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
- Overwrite endpoint devices and virtual subnet size
- Variables
- Overwrite masquerading
- 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. A similar pattern applies to overwriting endpoint devices.

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.

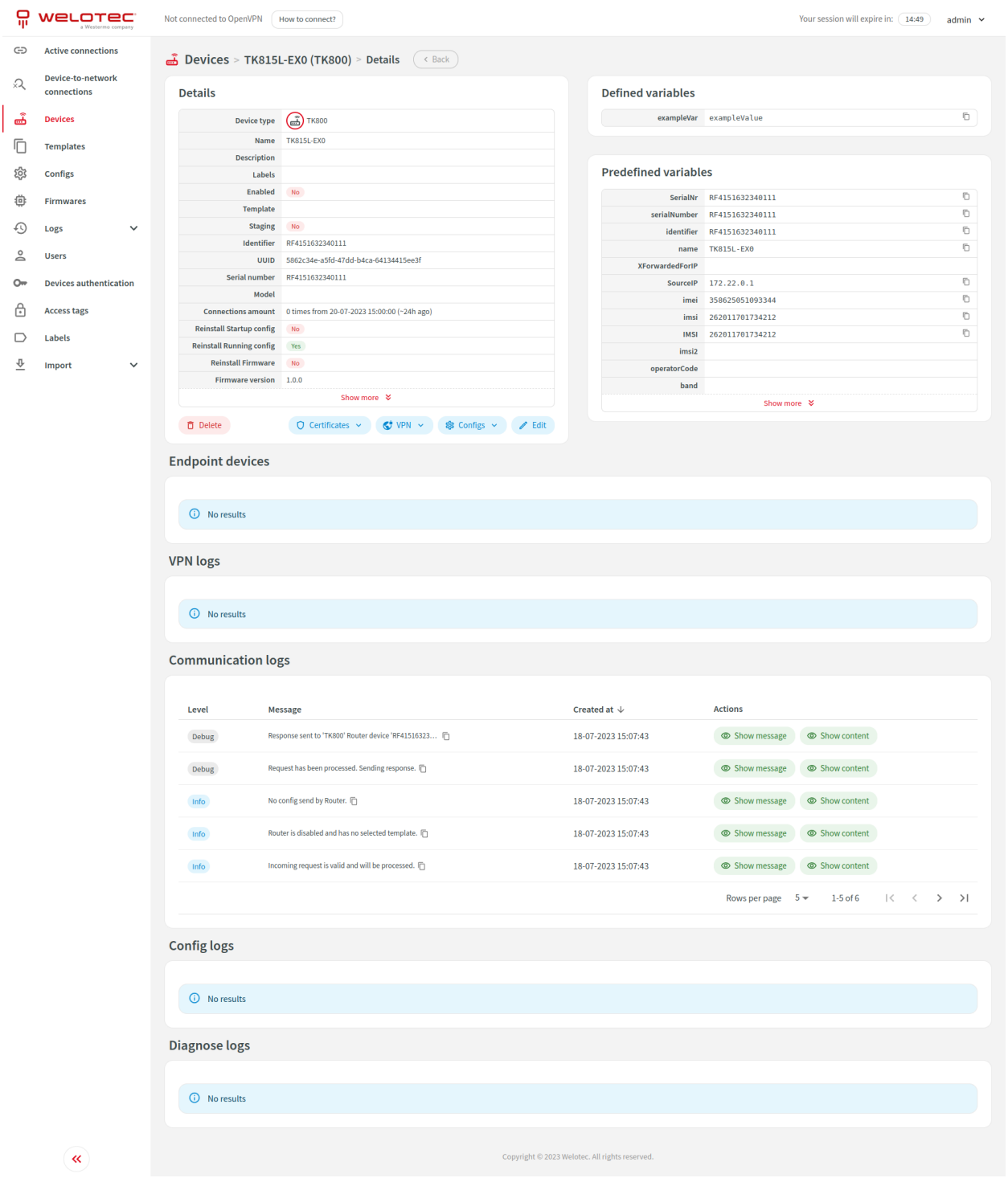
After applying a template to a device, you can change the device description, endpoint devices, virtual subnet size, variables, masquerading, access tags and labels. This will not affect the template itself or other devices using the same template. The same rule applies from the template perspective. You can change device description, endpoint devices, virtual subnet size, variables, masquerading, 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.

5.3.4 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.


welotec
Not connected to OpenVPN
How to connect?
Your session will expire in: 14:49
admin
Active connections
Device-to-network connections
Devices
Templates
Configs
Firmwares
Logs
Users
Devices authentication
Access tags
Labels
Import
Devices > TK815L-EX0 (TK800) > Details
Back
Details
Device type TK800
Name TK815L-EX0
Description
Labels
Enabled No
Template
Staging No
Identifier RF4151632340111
UUID 5862c34e-a5fd-47dd-b4ca-64134415ee3f
Serial number RF4151632340111
Model
Connections amount 0 times from 20-07-2023 15:00:00 (~24h ago)
Reinstall Startup config No
Reinstall Running config Yes
Reinstall Firmware No
Firmware version 1.0.0
Show more
Delete
Certificates
VPN
Configs
Edit
Defined variables
exampleVar exampleValue
Predefined variables
SerialNr RF4151632340111
serialNumber RF4151632340111
identifier RF4151632340111
name TK815L-EX0
XForwardedForIP
SourceIP 172.22.0.1
imei 358625051093344
imsi 262011701734212
IMSI 262011701734212
imsi2
operatorCode
band
Show more
Endpoint devices
No results
VPN logs
No results
Communication logs
Level
Message
Created at
Actions
Debug Response sent to 'TK800' Router device 'RF41516323... 18-07-2023 15:07:43 Show message Show content
Debug Request has been processed. Sending response. 18-07-2023 15:07:43 Show message Show content
Info No config send by Router. 18-07-2023 15:07:43 Show message Show content
Info Router is disabled and has no selected template. 18-07-2023 15:07:43 Show message Show content
Info Incoming request is valid and will be processed. 18-07-2023 15:07:43 Show message Show content
Rows per page 5
1-5 of 6
Config logs
No results
Diagnose logs
No results
Copyright © 2023 Welotec. All rights reserved.

5.4 Templates

This section allows you to manage existing templates.

5.4.1 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.

5.4.2 Details

The screen provides detailed information about a single template.

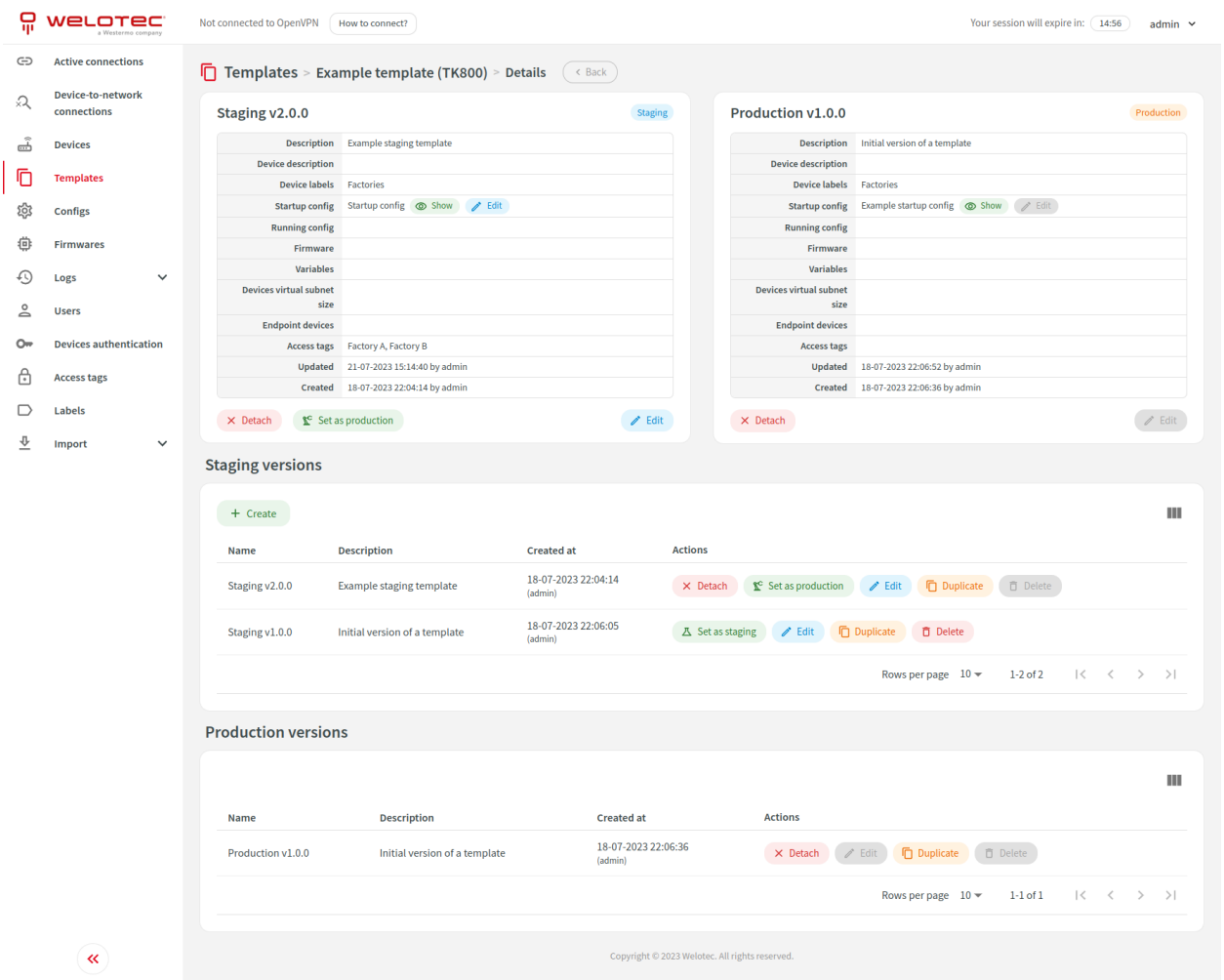
Templates can have multiple versions. Each template can have one version assigned as “Staging” and one version assigned as “Production”. Please refer to the *Applying a template* section for more information about using a template with a device.

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.



5.5 Configs

This section allows you to manage existing configs.

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.6 Firmwares

5.6.1 List actions

Exported CSV and Excel files will include additional rows for every hardware file existing in a firmware. For hardware file rows columns “Source”, “File name”, “MD5”, “Created at”, “Updated at”, “Created by”, “Updated by” will refer to hardware file instead of firmware.

You can perform the following extra list actions:

1. Create with hardware files - Create firmware with hardware files support. You will be presented with a list of device types that support hardware. You can enable hardware support for a device type on its’ edit screen.

5.6.2 Row actions

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

1. Hardware files - Redirects to a list of hardware files for selected firmware. Available only for firmwares that support hardware files.
2. Download - Download uploaded firmware.
3. Show URL - Open a dialog with the external URL of the selected firmware.
4. Show update path - Open a dialog with the update path of the selected firmware.
5. Duplicate - Duplicate selected firmware.

5.7 Firmwares hardware files

This section allows you to view a manage existing hardware files for a single firmware.

5.7.1 Row actions

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

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

5.8 Logs

5.8.1 Login attempts

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

5.8.2 Device failed login attempts

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

5.8.3 Secret logs

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

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 secret log.
2. Show updated secret - Open a dialog with the updated device secret value of the selected secret log.
3. Show previous secret - Open a dialog with the previous device secret value of the selected secret log.

5.8.4 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.

5.8.5 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.

5.8.6 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.

5.8.7 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.

5.8.8 Audit logs

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

Row actions

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

1. Show values - Open a dialog with the logged values. Depending on type of change dialog will show:
    - New values for create
    - New and old values for update. You can choose way of presenting those values: full difference, only changes, old values or new values.
    - Old values for delete

5.8.9 VPN logs

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

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 for the selected VPN log.

5.9 Users

This section allows you to manage existing users.

5.9.1 Row actions

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

1. Certificates - Expandable group of actions connected to certificate management of the selected user. Visible only for supported certificate types.
    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. Generate certificate - Generate certificate using PKI Server. Available only for certificate types that support PKI certificates.
    5. Revoke certificate - Revoke certificate using PKI Server. Available only for certificate types that support PKI certificates.

6. Download certificate - Download public key as .crt file.
7. Download private key - Download private key as .key file.
8. Download CA certificate - Download CA certificate as .crt file.
9. Download .p12 - Download PKCS #12 file containing public key, private key and CA certificate.

2. Download OpenVPN configuration - Download OpenVPN configuration file for the selected user.
3. Enable - Allows you to enable the selected user.
4. Disable - Allows you to disable the selected user.
5. Change password - Allows you to change password for the selected user.
6. Reset secret - Allows you to reset secret for the selected user. Only available when two-factor authentication is enabled in the system.
7. 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.

5.9.2 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.

VPN permissions

Users with VPN permissions are restricted to the following screens:

1. Active connections
2. Devices
3. Logs
    1. VPN logs

Users with VPN permissions has limited access to devices and their endpoint devices based on access tags. Having access to a device means that at least one access tag that user has assigned is also assigned to a device. The same logic applies to endpoint devices.

Users with VPN permissions have following access to a device:

- View - when user has access to an endpoint device that is assigned to a device without access.
- Edit - when user is not allowed to manage endpoint device and has access to a device. Allows to modify labels and description.
- Edit with managing endpoint devices - when user is allowed to manage endpoint devices and has access to a device. Allows to modify labels, description and endpoint devices. Endpoint devices are visible according to user access to them. This access level also allows creating endpoint devices.

Users with VPN permissions have following access to an endpoint device:

- Edit - when user is not allowed to manage endpoint devices and has access to an endpoint device. Allows to modify description.
- Edit with managing endpoint devices - when user is allowed to manage endpoint devices and has access to an endpoint device. Allows to fully modify endpoint device or delete it.

Logs are also limited to only those that are connected to visible devices. Active connections are limited only to his connections.

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.

5.10 Device authentication

This section allows you to manage existing devices authentication.

5.10.1 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.

5.11 Access tags

This section allows you to manage existing access tags.

Access tags are used to restrict access for users with SMART EMS permissions and VPN permissions. Please refer to *SMART EMS permissions* and *VPN permissions* sections for more information.

5.12 Labels

This section allows you to manage existing labels.

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

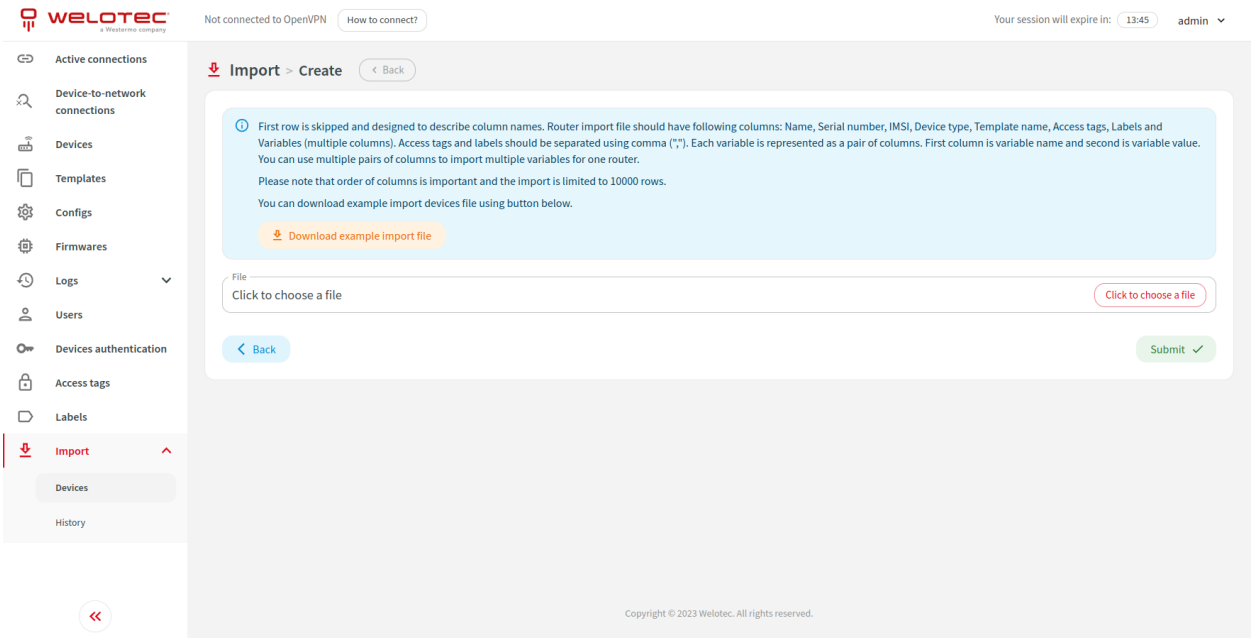
5.13 Import

5.13.1 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.

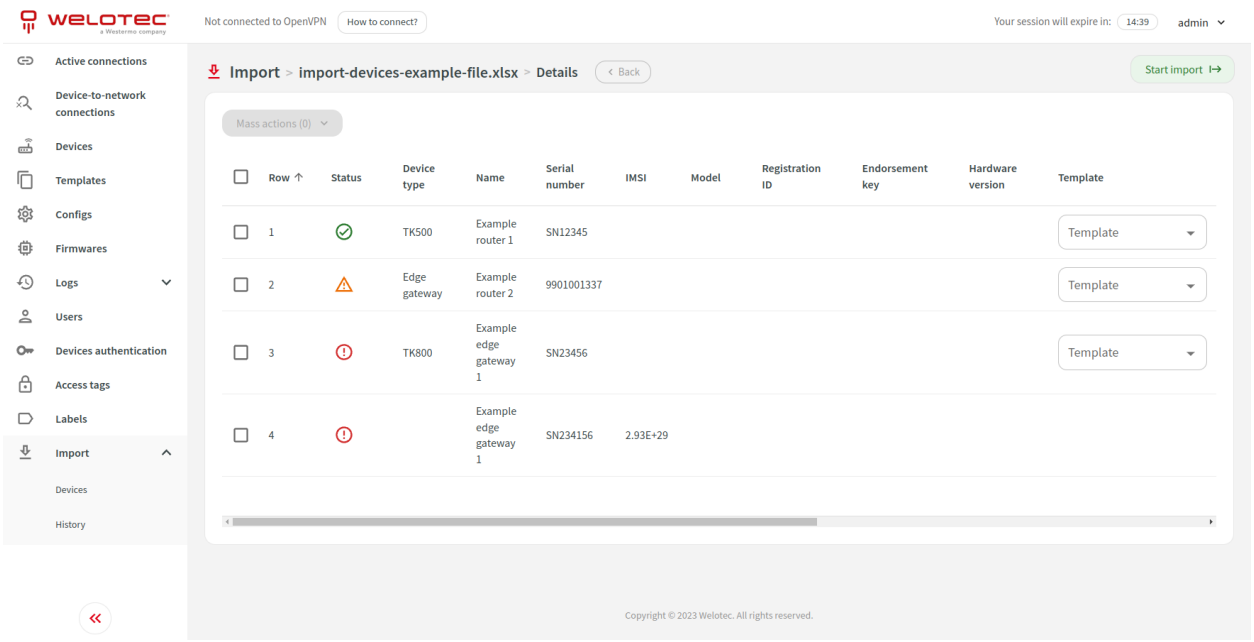


Step 2

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.

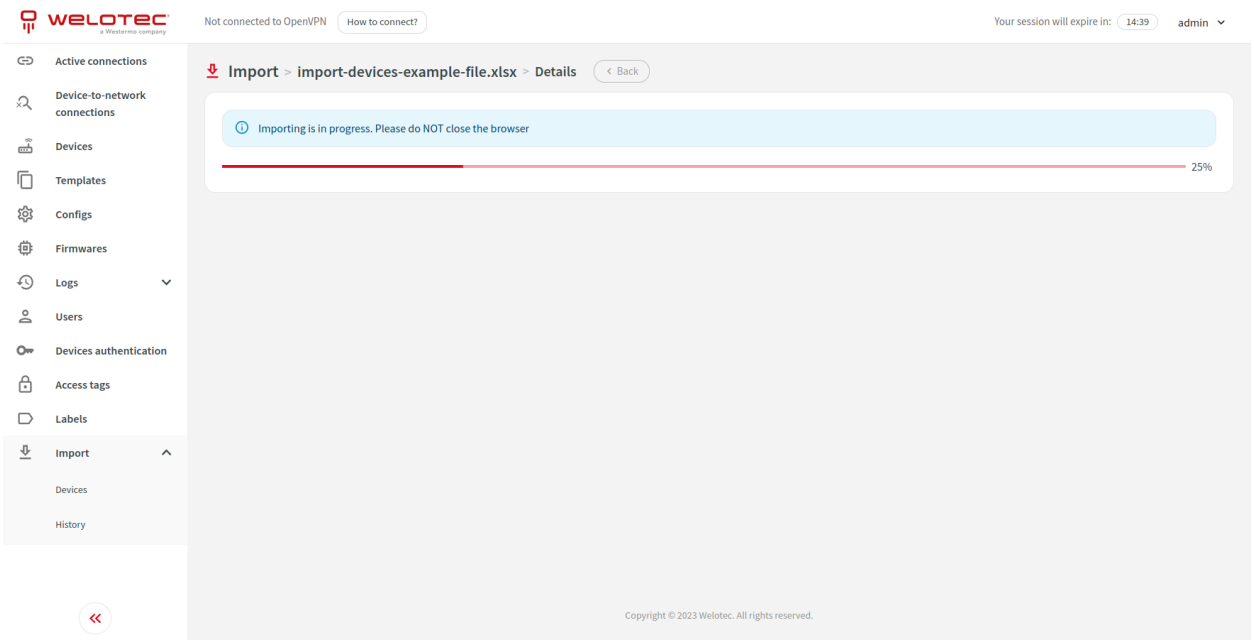
You can adjust imported rows by changing the data using inputs in columns or using mass actions.

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.



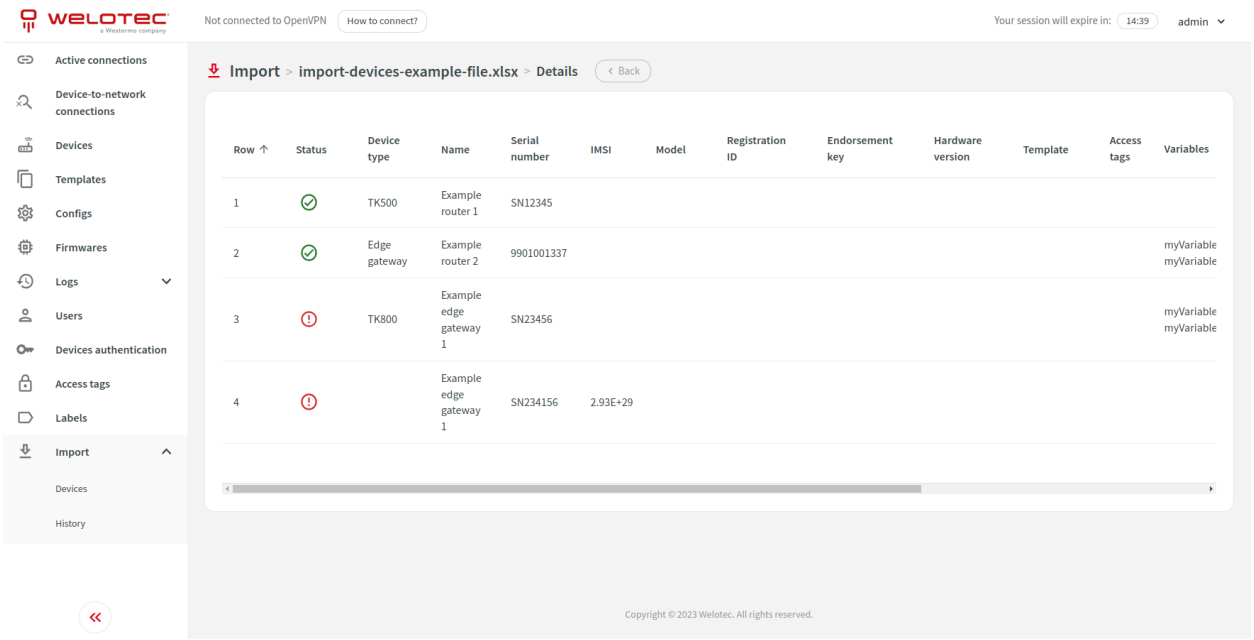
Step 3

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



Step 4

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



5.13.2 History

This section allows you to view a list of imports.

5.13.3 Row actions

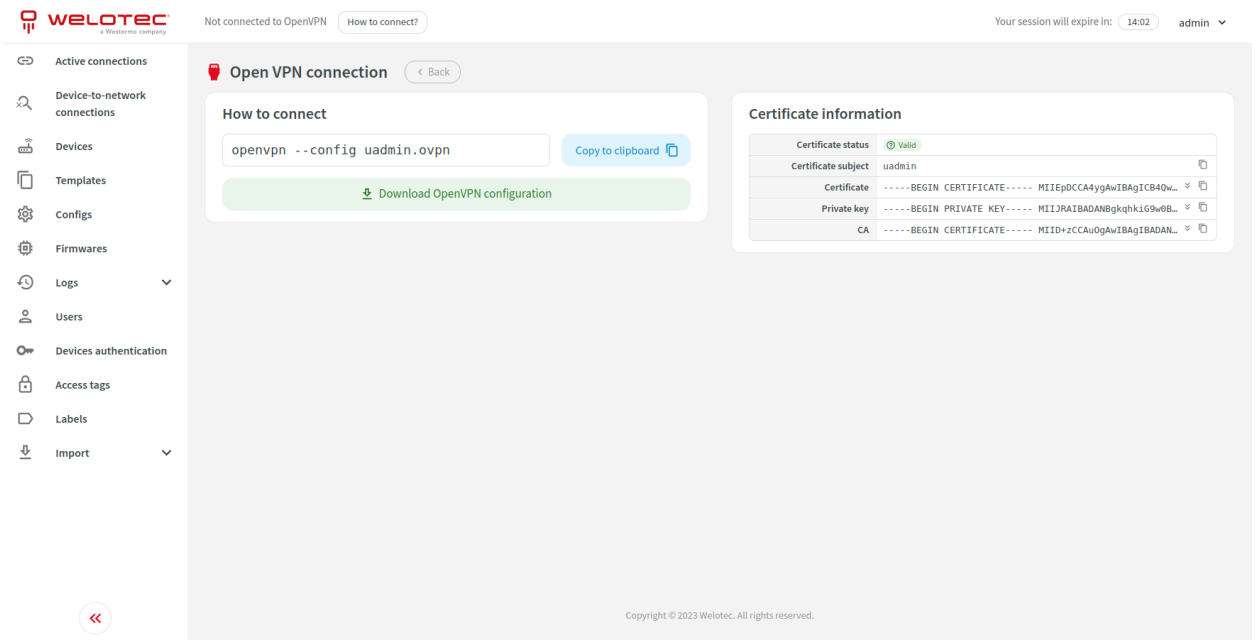
You can perform the following extra actions on a single row:

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 OpenVPN connection

You can access the OpenVPN connection screen in the navbar menu.

This screen allows you to download the OpenVPN configuration and view the technician VPN certificate for currently logged-in user.



6.1 Establishing OpenVPN connection

OpenVPN is an open-source software that allows you to create secure point-to-point or site-to-site connections.

6.1.1 Installing software

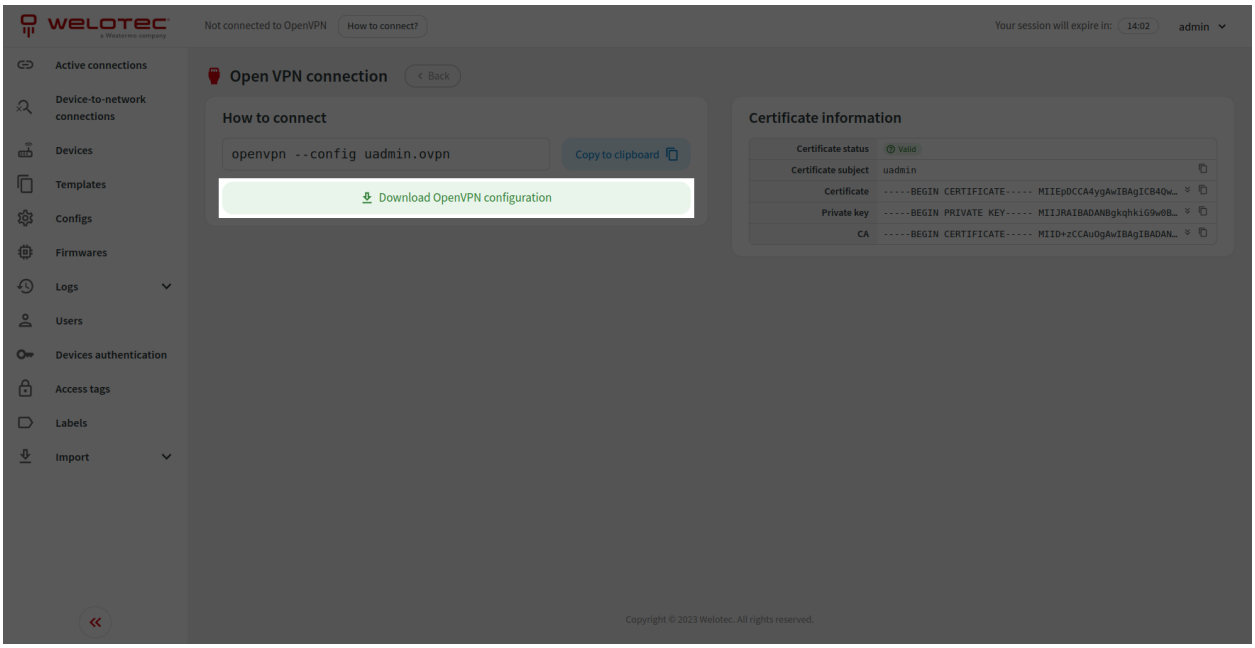
Please follow the instructions under this link to install OpenVPN software.

Installing OpenVPN

6.1.2 Downloading OpenVPN configuration file

To make a successful connection you need a valid technician VPN certificate. If you do not have one please ask your VPN Security Suite administrator to provide you one.

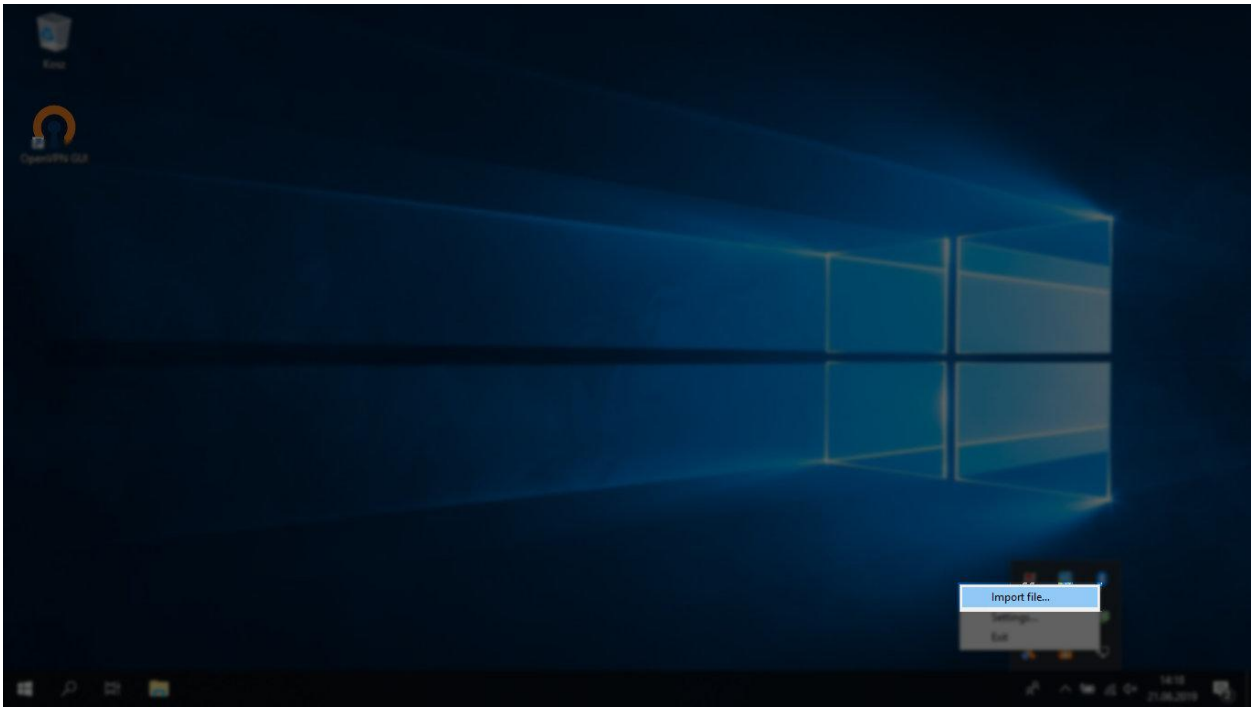
Please click “Download OpenVPN Configuration” to download the OpenVPN configuration file.

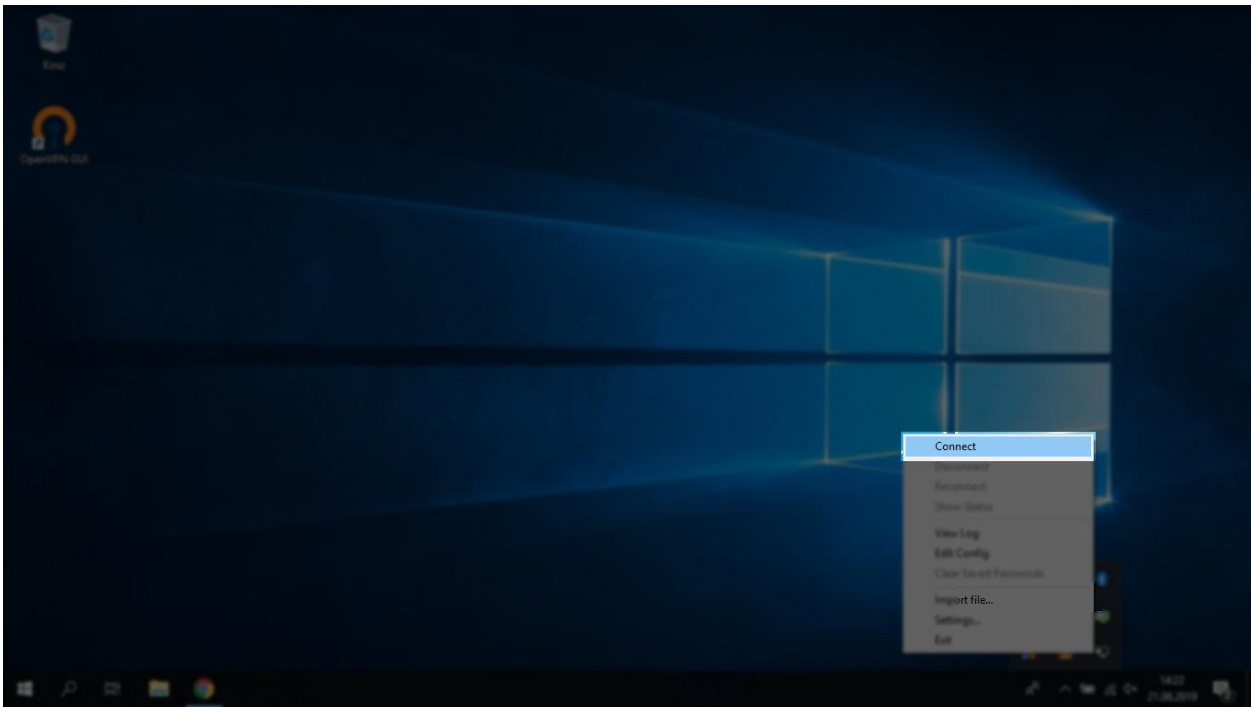


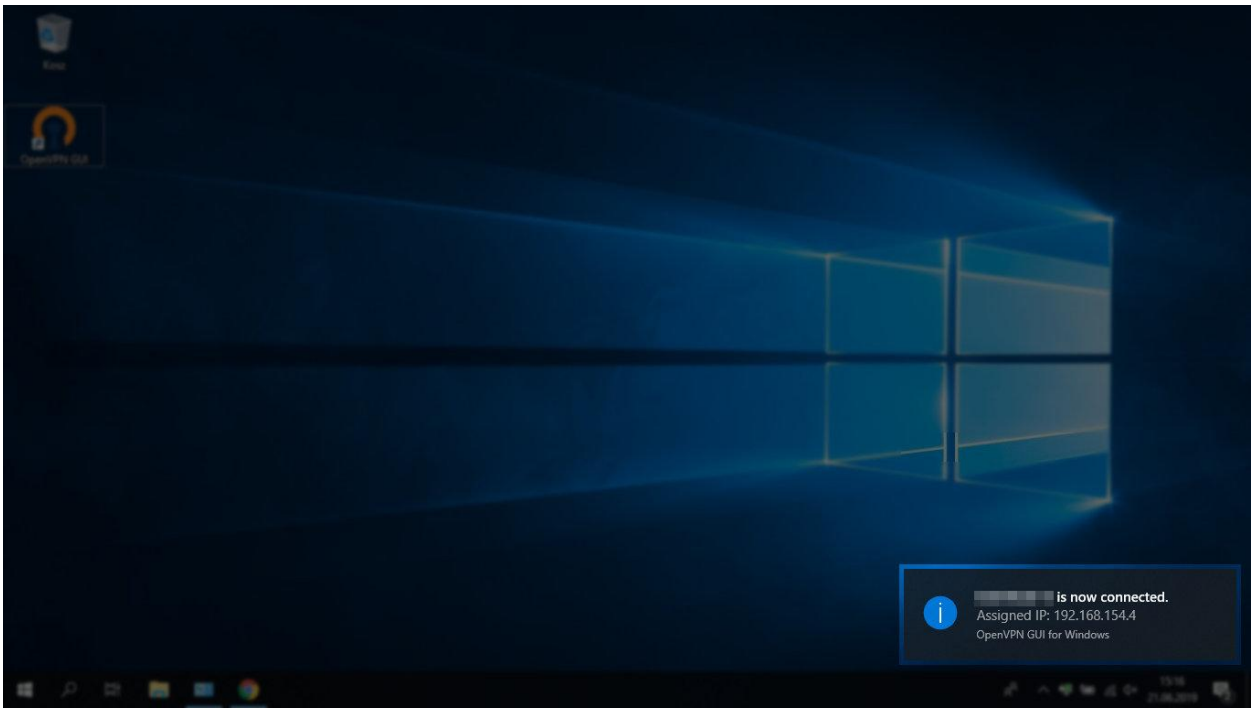
6.1.3 Connecting to OpenVPN on Windows

In order to connect on Windows please click the right mouse button on the OpenVPN icon and choose “Import file…”. Please pick the configuration file that you downloaded in the previous step. Afterwards please again click the right mouse button on the OpenVPN icon and choose “Connect”. You should see confirmation that OpenVPN is connected.

In case of connection problems please re-check the OpenVPN version that you downloaded and installed. You can also try installing older versions of OpenVPN.




Connect
Import file...


is now connected.
Assigned IP: 192.168.154.4
OpenVPN GUI for Windows

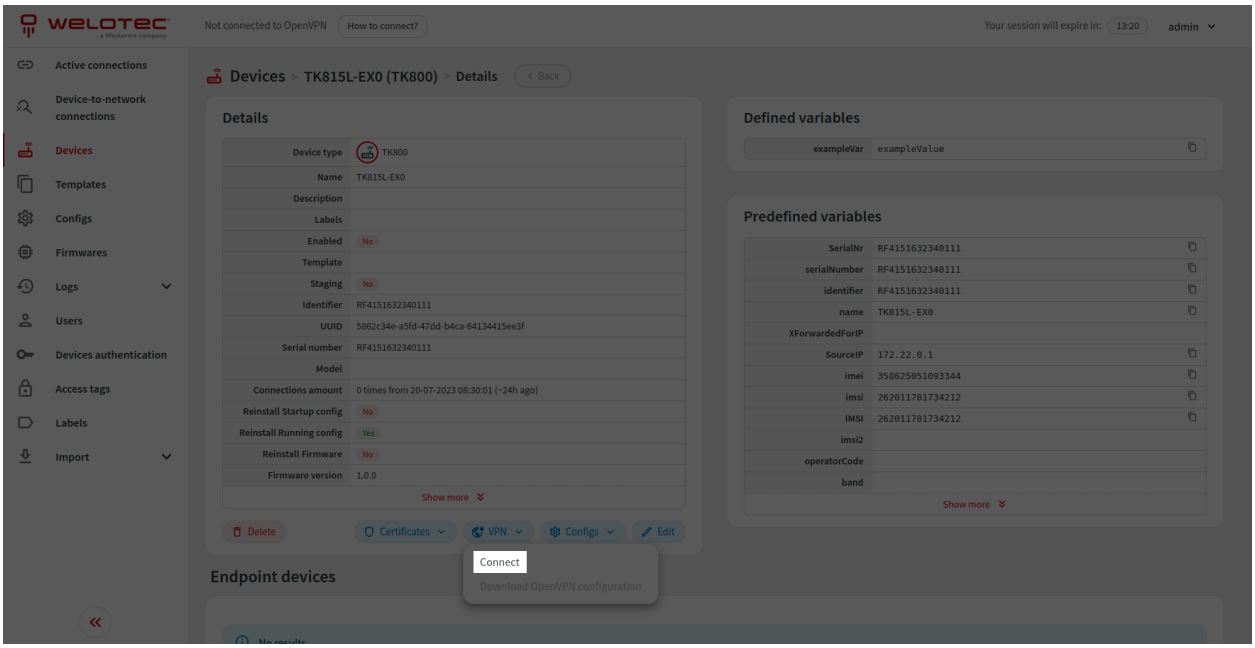
6.1.4 Connecting to OpenVPN on Linux

In order to connect on Linux please use the command visible under “How to connect?”. The file used in the visible command is the one downloaded via the “OpenVPN Configuration” button. You might need to use super user privileges to establish an OpenVPN connection (sudo).

6.1.5 Connecting to a device

In order to connect to a device currently logged in user needs to be connected to OpenVPN.

Please find the desired device on the device list or navigate to the details screen. You will find the “VPN” expandable button, please select “Connect”. After making a successful connection you will be able to connect to the chosen device by using his VPN IP address. You can find this address on the device details screen in the “Details” section. When a device includes endpoint devices, it is also possible to connect to this device and all endpoint devices at once using the “Connect to all” option (also under the “VPN” expandable button).



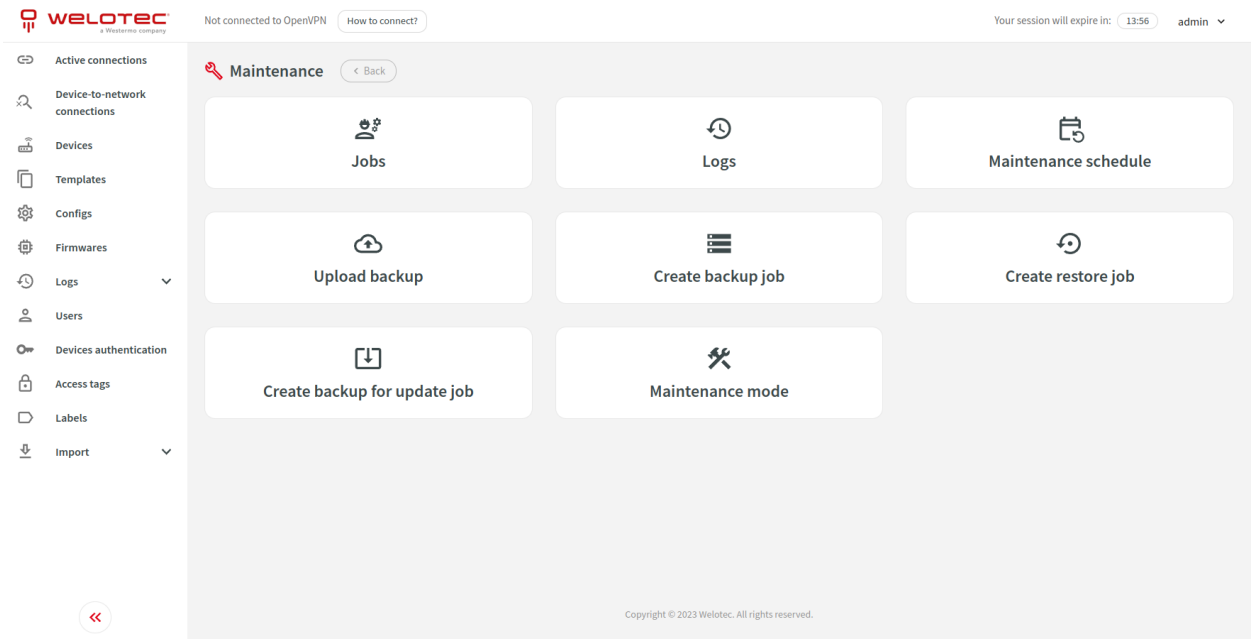
6.1.6 Closing connection

After finishing your work with a device please close the connection. You can do that on the active connections screen. It is also possible to close the connection on the device list or device details screen by clicking the “VPN” expandable button and selecting “Close my connection”. In case of multiple connections being open to this device (or its endpoint devices) additional option “Close multiple connections” is available (also under the “VPN” expandable button) which opens a dialog that allows you to select multiple connections to close.

Please remember that your connection might be automatically closed after a certain time (by default 4 hours).

7 Maintenance

You can access the maintenance screen in the navbar menu.



7.1 Jobs

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

7.1.1 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.

7.2 Logs

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

7.3 Maintenance schedules

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

7.4 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.

7.5 Create backup job

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

7.6 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.

7.7 Create backup for update job

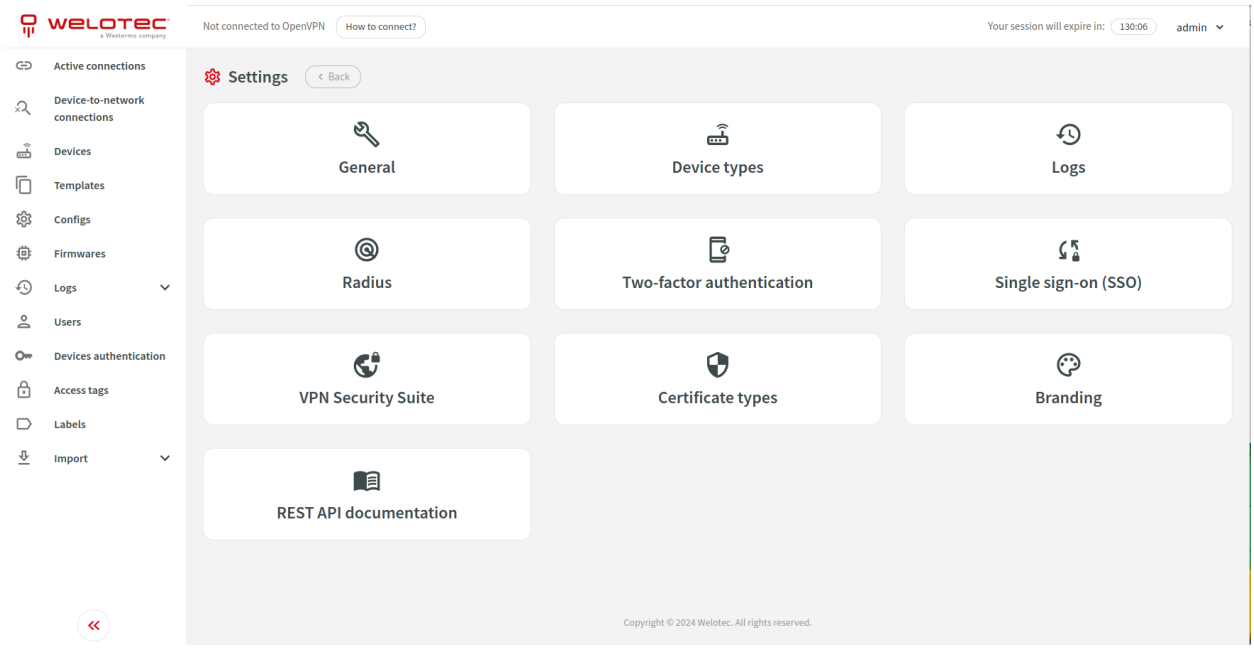
This section allows you to create a backup for update job. It is recommended to activate maintenance mode before preparing a backup for update. After submitting the form, a backup for update maintenance job will be created.

7.8 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.

8 Settings

You can access the settings screen in the navbar menu.



8.1 General

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

8.2 Device types

This section allows you to manage existing device types.

8.2.1 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.
5. Secrets - Allows you to manage device secrets settings for devices in selected device type.
6. Hardwares - Allows you to manage device hardwares for the selected device type.

8.2.2 Communication procedure

Devices communicate with SMART EMS to deliver many functionalities including managing configuration, updating firmwares, gathering diagnose data, sending logs, managing certificate types, 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.

8.2.3 Firmware update paths

When the communication procedure supports firmware functionality, you have two main options for managing firmware updates:

1. **Any Schema (anySchema)**: If you leave the firmware schema as `anySchema`, the system will automatically install the firmware from the template whenever the device reports a different firmware version than what's defined in the template.
2. **Firmware Schema (e.g., semanticVersioning)**: When using a specific firmware schema like `semanticVersioning`, you can:
   - Define a sequence of firmwares in the system
   - Add the latest firmware version to the template
   - During device communication, based on the device's reported `firmwareVersion`, the system will automatically update to the next higher firmware version from the sequence that is greater than the device's current version
   - `semanticVersioning` supports pre-release tags. Allowed prefixes are: `stable`, `beta` (or `b`), `RC`, `alpha` (or `a`), `patch` (or `pl`/`p`).

Additional options:

- **allowDowngradeFirmware flag**: When enabled, this flag allows the installation of firmware from the template (highest version) even if the device reports having a higher version than what's available in the template. This is useful for forcing downgrades when necessary.

8.2.4 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.

8.3 Device secrets

Device secrets functionality allows you to safely manage sensitive information like passwords, keys and credentials for a specific device.

Functionality includes:

1. Device type secrets - Allows you to manage device secrets settings for devices in selected device type.
2. Device secrets - Allows users to show, edit and delete values of device secret
3. Secret log - Allows you to audit who, when and how used device secrets
4. Device secret variables - System automatically prepares additional predefined device variables to use in device configs

8.3.1 Manage device type secrets

Accessible from device type screen. It allows you to manage device secrets settings in selected device type.

Secret have following properties:

1. Device type - The device type associated with the secret.
2. Name - A human-readable name of the secret (used in logs and device details)
3. Description - A human-readable explanation of the secret's purpose and usage (shown in device details).
4. Use secret as device variable - Whether the system should automatically generate variables based on this secret.
5. Variable name prefix - (Only applicable if "Use as Device Variable" is enabled) Prefix for system-generated device variables.
6. Secret value behaviour - How secret value should behave during device communication.
7. Allow users to manually edit secret value - Whether users can manually edit the secret value.
    - Administrators - Can edit/clear all device secrets.
    - SMART EMS users - Can edit/clear specific device secrets if they have:
        - Access to the device.
        - At least one access tag from the defined access tag list.
    - VPN users - cannot edit/clear device secrets.
8. Enable reminder for manual secret value renewal - Reminder will be visible on device details screen in device secret section. You can specify number of days after which reminder should appear.
9. Access tags - A list of access tags required for SMART EMS users to access device secrets (users must also have device access).
10. Secret value requirements - Minimum length and character type requirements (lowercase, uppercase, special characters, digits) for the secret value. Automatically renewed secrets will meet these requirements.

8.3.2 Device secrets

Accessible from device detail screen. SMART EMS users have access to device secrets only when they have access to this device. List of device secrets is also limited based on access tags (at least one access tag that SMART EMS user has assigned is also assigned to device secret). VPN users do not have access to this functionality.

List of device secrets also include last renewed at column which includes informative icons when:

1. Secret value will be automatically generated during next device communication.
2. Secret value will be automatically renewed during device communication.
3. Secret value will be automatically renewed during device communication, but it is already expired.
4. Secret value should be renewed manually as soon as possible.

Users can:

1. Show secret value - A dialog will be shown with secret value and device secret variables.
2. Edit - Possible when device secret allows users to manually edit secret value.
3. Clear secret value - Possible when device secret allows users to manually edit secret value.

8.3.3 Secret log

The secret log allows you to audit any:

- Showing or changing of device secret value by a user
- Showing or changing of device secret value by a device authentication user during device communication
- Showing content of communication logs, config logs, and diagnose logs by user
- Showing previous or updated device secret value of secret log by user

SMART EMS users can access the content of communication, configuration, and diagnostic logs only if:

- They have access to the specific device.
- They have access to all the device's secrets with "Use secret as device variable" enabled.

8.3.4 Device secret variables

The system automatically generates a list of device secret variables for each device secret with "Use secret as device variable" enabled. These variables are constructed by combining the "Variable name prefix" with an encoding algorithm.

Available Variables:

- prefixPlain: **Warning**: Stores the device secret value in plain text. **Do not use** except for exceptional circumstances.
- prefixBase64: **Warning**: Stores the device secret value encoded with Base64, which is reversible. **Not recommended** for most use cases.
- prefixCryptMd5: Uses the Crypt MD5 algorithm for encoding. **Considered less secure** for modern password storage. Use with caution. (Example: $1$0YyPL6hr$8evKweYo5.YdqCTUT6YVi0)
- prefixCrypBlowFish: Uses the Crypt BlowFish algorithm for encoding. (Example: $2y$10$tVKxnUo5cgYXFGriRLaPNuf0iRQEhOm4gGvmMPEgWFqVJAnNL3heu)
- prefixCrypSha256: Uses the Crypt SHA-256 algorithm for encoding. (Example: 5s6EGldrZmqN3MaeL$xa4pZVRJE8yBgdFlRVKN.dr.M1ZVp249H0wuz/nGVH2)
- prefixCrypSha512: Uses the Crypt SHA-512 algorithm for encoding. (Example: 6Vw0KA4YXj1LZIkSG$jlhIiH6BqhC2Rb5yEse5JyZu65QPzgCqef0rRpsNDuny5hEKYUMTuGcEU5rnvRciG01//sPCYwo5NYCidXhYw

Important Notes:

- When used in device configs, the values will be obscured within the web interface.
- During device communication, the unobscured values are used.
- Due to this, communication, config, and diagnostic logs that might contain these secrets. Accessing them is logged in the secret log.
- To access the content of these logs, users must have permission to all the device's secrets with "Use secret as device variable" enabled.
- If defined or predefined variable with same name exists, device secret variable will override value in generated config

8.4 Logs

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

8.5 Radius

This section allows you to adjust settings for radius authentication.

8.6 Two-factor authentication

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

8.7 Single Sign-on (SSO)

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

8.7.1 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”.

8.8 VPN Security Suite

This section allows you to adjust settings for VPN Security Suite which includes configuring connection to OPNsense, OpenVPN configuration, devices OpenVPN and virtual networks, technicians OpenVPN networks.

8.9 Certificate types

This section allows you to manage certificate types and their configuration.

A certificate type defines various aspects of certificates used by devices. You can create and manage certificate types to suit the needs of your specific devices and PKI infrastructure.

8.9.1 Key Properties of a Certificate Type

- **Name**: A user-friendly name for the certificate type (e.g., “Device Authentication Certificate”).
- **Certificate entity**: Specifies which entity can use this certificate type.
- **Common Name Prefix**: A prefix used to automatically generate the Common Name field in certificates issued for this type (e.g., “eg-“).
- **Variable Name Prefix**: A prefix used to generate predefined variables containing device certificate related data to use in device config.
- **Enabled**: Allows to enable or disable certificate type
- **User available actions**: Download, upload, delete, generate and revoke using PKI - when enabled actions will be visible for users in device or user actions
- **Automatic behaviours**: Defines how system should handle certificate when device or user is being enabled or disabled
- **PKI Protocol**: Choose PKI protocol for handling generation and revocation of certificate
- **SCEP protocol settings**: (if PKI protocol is SCEP) Define SCEP protocol settings like URLs, credentials, etc.

8.10 REST API documentation

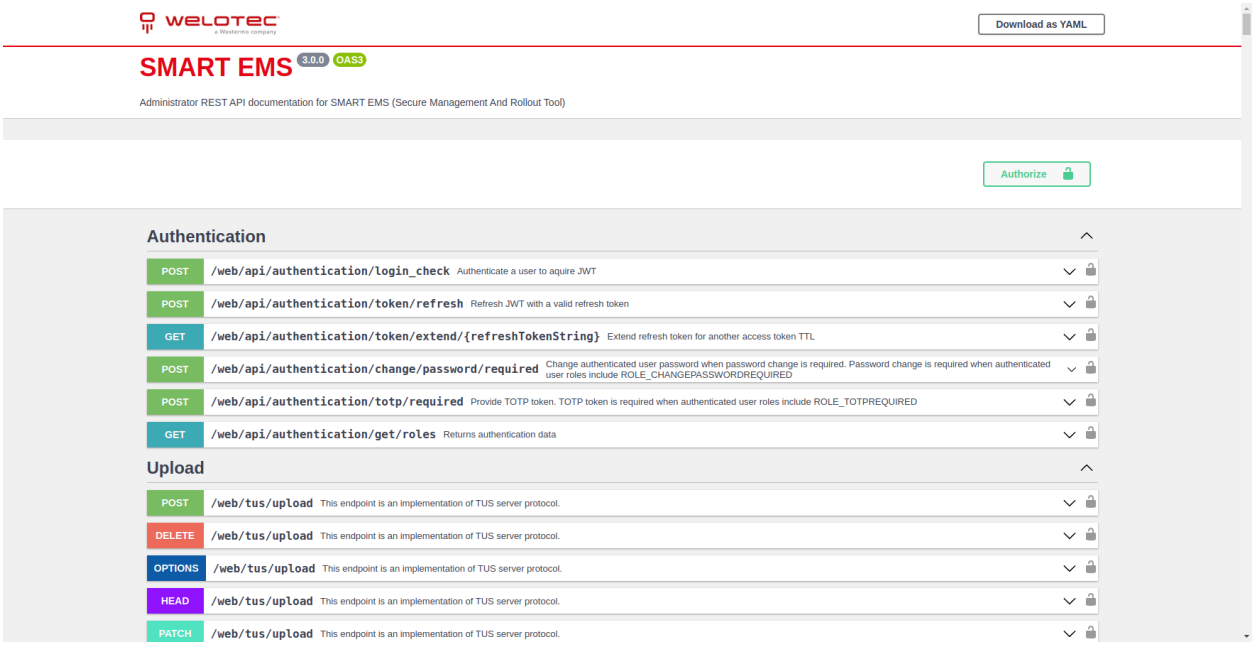
This section allows you to enable or disable REST API documentation for specific users.

9 REST API Documentation

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

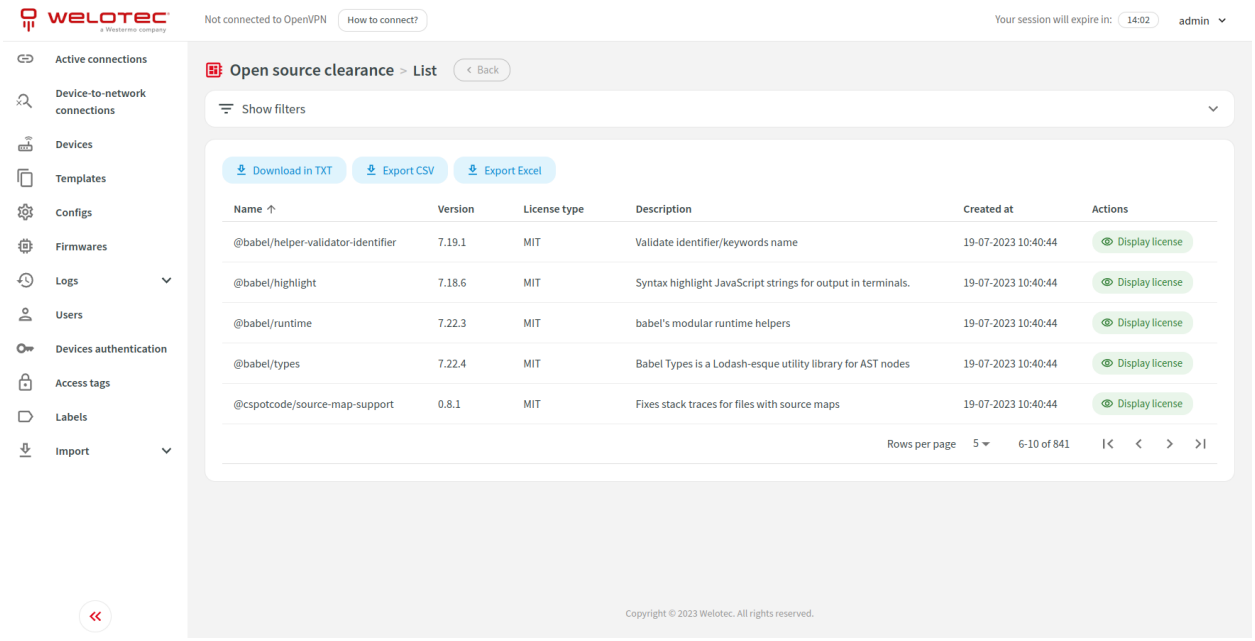
REST API documentations are limited to user permissions. Users with administrator permissions, SMART EMS permissions and VPN Security Suite permissions have separate REST API documentation.

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.



10 Open source clearance

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



10.1 List actions

You can perform the following extra list actions:

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

10.2 Row actions

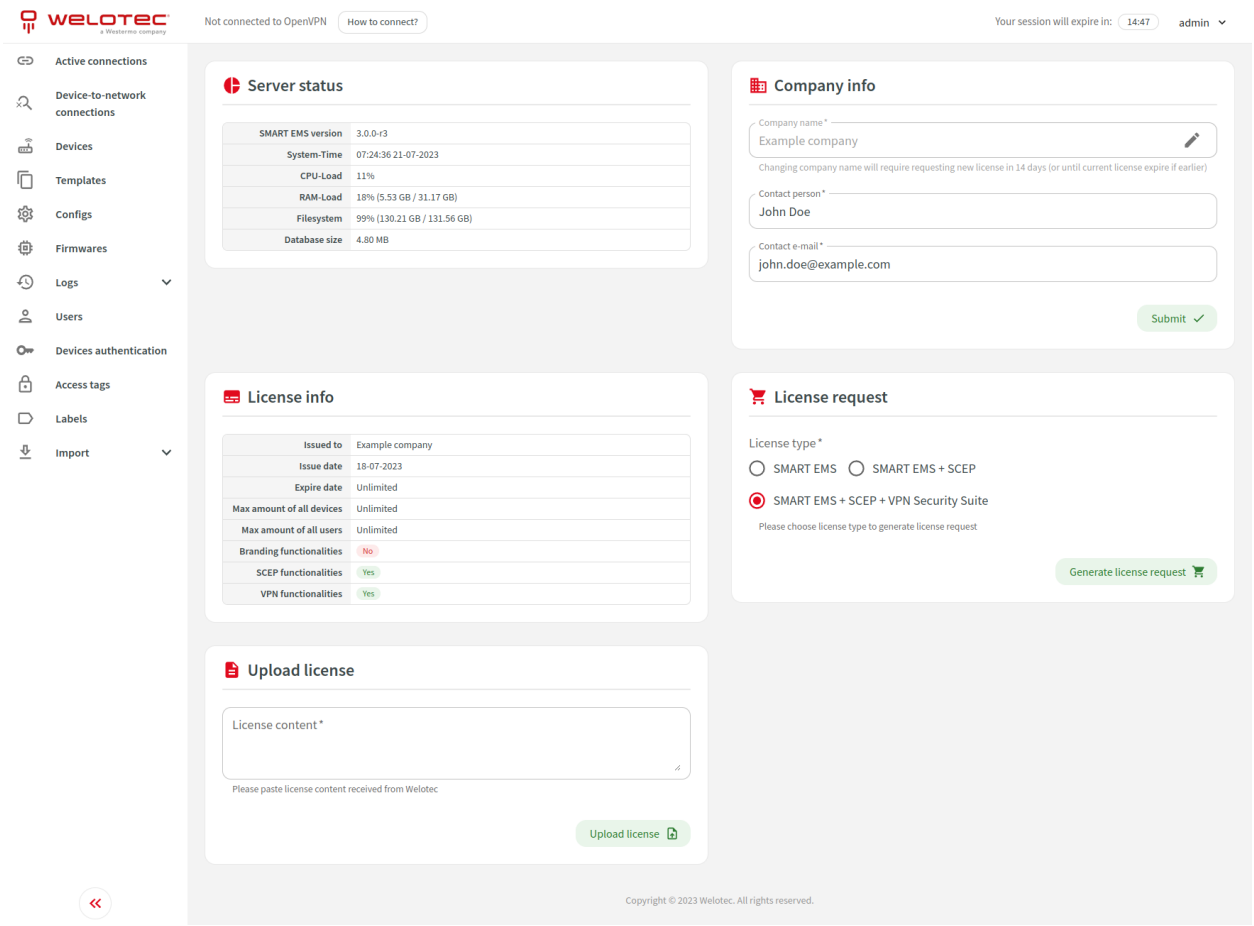
You can perform the following extra actions on a single row:

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

11 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.

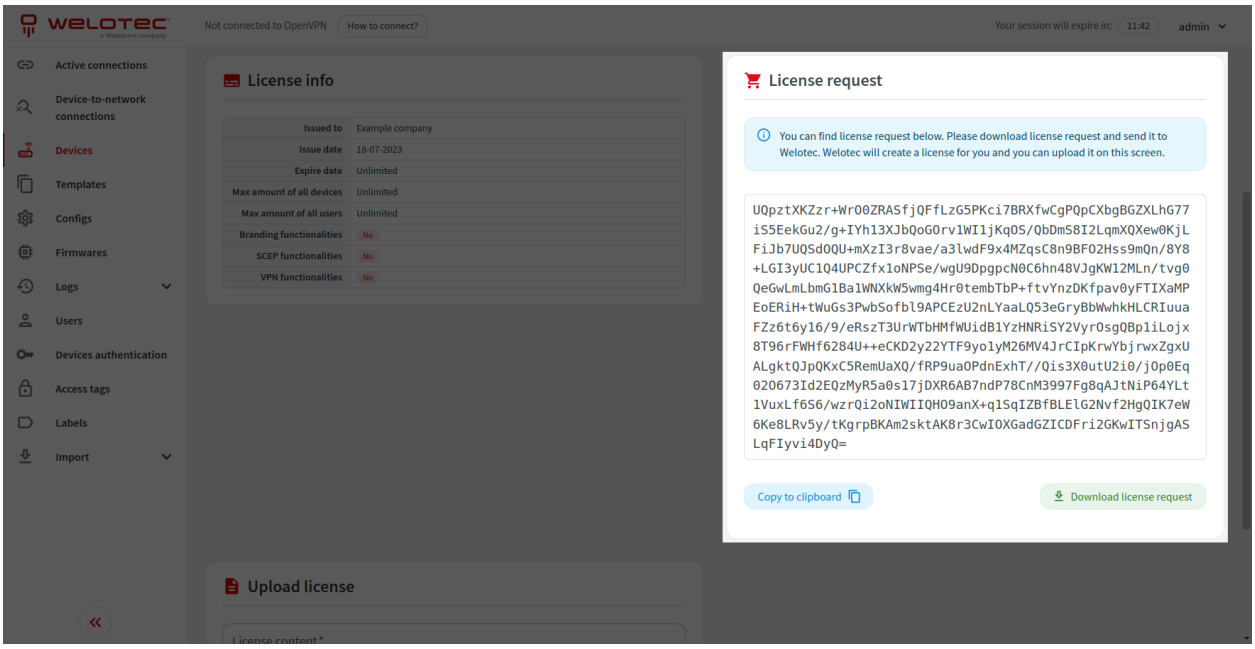


11.1 Requesting license

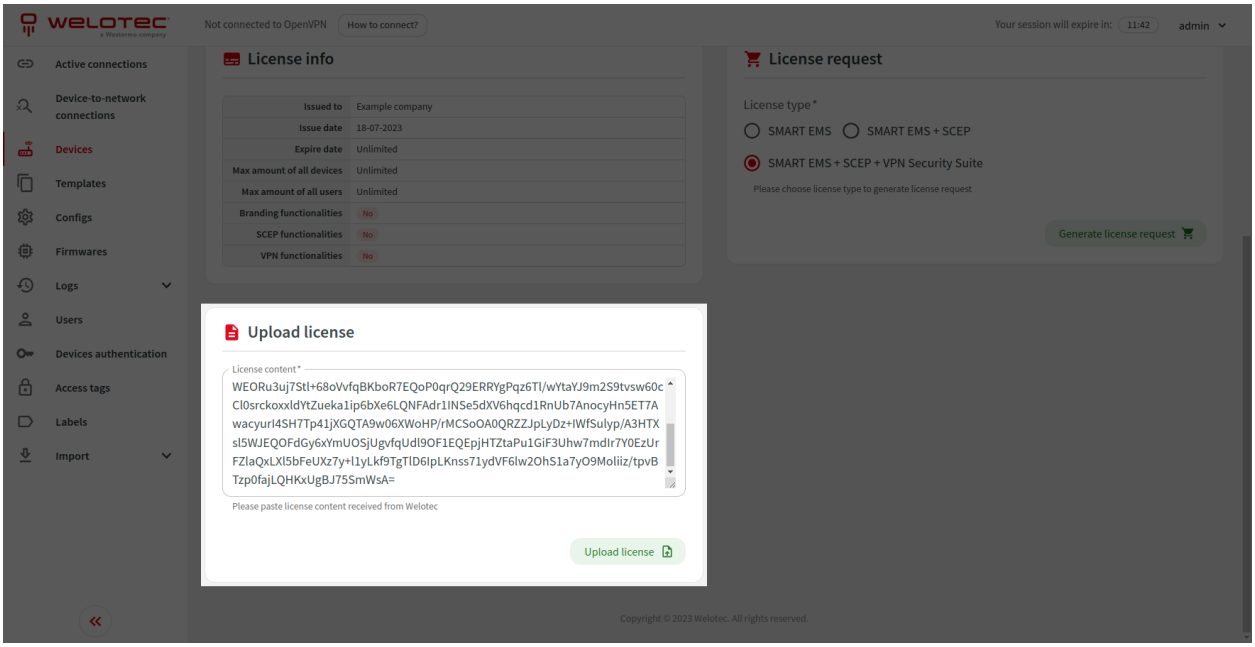
You can request a license of a specific type:

- 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.



11.2 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.

12 OSS clearings

You can find OSS clearings under following link: OSS Licenses