Application note

FESTO

Quick help

Documentation Festo Dashboards

100273

Title ..... Quick help
Version 1.30
Document number 100273
Original ..... de
Author ..... Festo

Last saved 04.05.2020

Copyright notice

Legal information

Hardware, software, operating systems and drivers may only be used for the applications described and only in conjunction with the components recommended by Festo SE & Co. KG.

Festo SE & Co. KG does not accept any liability for damages arising from the use of any incorrect or incomplete information contained in this documentation or any information missing therefrom.

Defects resulting from the improper handling of devices and modules are excluded from the warranty.

The data and information specified in this document should not be used for the implementation of safety functions related to the protection of personnel and machinery.

No liability is accepted for claims for consequential damages arising from failure or malfunction. Otherwise, the clauses concerning liability included in the terms and conditions of delivery, payment and use of software of Festo SE & Co. KG shall apply, which can be found at www.festo.com or provided upon request.

None of the information contained in this document is a guarantee of product features in the legal sense, in particular with regard to functionality, condition or quality.

The information in this document serves only as basic information for the implementation of a specific, hypothetical application and is in no way intended as a substitute for the operating instructions of the respective manufacturers and the design and testing of the respective application by the user.

The respective operating instructions for Festo products can be found at www.festo.com/sp .

Users of this document (function and application) must themselves verify that all functions described herein also work correctly in their own applications. Even after examining this document and while using the specifications contained herein, users nevertheless remain solely responsible for their own applications.

Table of contents

1 General information

1.1 What are Festo Dashboards?

Festo Dashboards reliably monitor and display the condition of Festo components in a web-based cloud application. Dashboards are available for the following Festo components:

- Valve terminal CPX/MPA
- Service unit combination (type/ID1) MSE6-E2M-5000-FB36-AGD in conjunction with FB36 bus node (Modbus®, TCP-IP) TN 3990296

The available components are connected to the cloud via an IoT gateway, the CPX-IOT. The CPX-IOT gateway thus serves as an interface between the local fieldbus and the cloud.

1.2 Where can I find Festo Dashboards?

As a cloud application, the dashboards can be accessed via a URL in a web browser (e.g. Google Chrome).
The URL is: https://dashboards.festo.com.

1.3 What do I need in order to use Festo Dashboards?

The use of Festo Dashboards requires an Internet connection and the use of a modern web browser such as Mozilla Firefox, Google Chrome, Apple Safari or Microsoft Edge. The browser should be kept up to date in order to ensure trouble-free operation.

1.3.1 Required hardware, CPX-MPA

In addition to a Festo valve CPX/MPA terminal, the CPX-IOT gateway is also required in order to use the CPX/MPA Dashboards. We offer this in the following configurations:

M18 power connector: 50E-T70GCQS-Z
⅞" power connector: 50E-T70GCQP-Z
IP20 power connector: 53E-T70GCQE-Z

A dashboard licence makes it possible to use the dashboards for a Festo CPX/MPA valve terminal. Licences can be obtained from the Festo App World (www.festo.com/appworld). Two different licence packages are available:

- 1-month dashboards licence
- 1-year dashboards licence

A 4-week trial licence is available in both cases. Furthermore, the CPX-IOT gateway must be connected to the same field network as the CPX/MPA. A list of all CPX/MPA modules which are recognised by Festo Dashboards and displayed in the cloud application is available here: https://www.festo.com/net/de_de/SupportPortal/Details/565962/Document.aspx

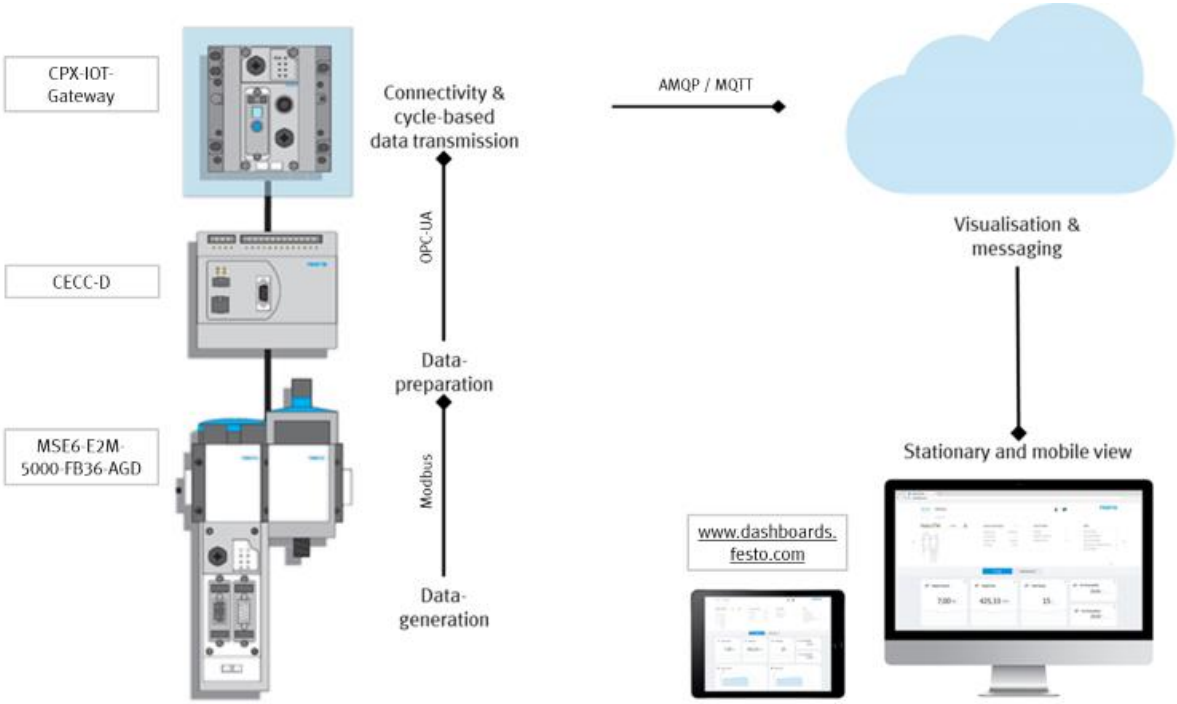
1.3.2 Required hardware, MSE6-E2M

The CPX-IOT gateway and a service unit combination (type/ID1) MSE6-E2M-5000-FB36-AGD are required in order to use the E2M Dashboard for monitoring the compressed air consumption of a system. We offer this in the following configurations:

M18 power connector: 50E-T70GCQS-Z
⅞" power connector: 50E-T70GCQP-Z
IP20 power connector: 53E-T70GCQE-Z

Festo's controller CECC-D is required in order to run the CM-Lib (Condition Monitoring Library). The CM-Lib converts big data to smart data. The CPX-IOT gateway ensures the necessary communication between the field level and the cloud. The CPX-IOT must be connected to the same field network as the E2M. Furthermore, a Festo controller CECC-D must be connected to the same network and equipped with the Condition Monitoring Library ("CM-Lib"), available from the Support Portal (https://www.festo.com/net/de_de/SupportPortal/Downloads/565418/617938/CECC-D_E2M-CM_V37.cecc_bak).

A detailed description of the CM-Lib installation process can be found here: "Getting started with E2M_CM cloud connectivity software for service unit combination MSE6-E2M-5000-FB36-AGD" https://www.festo.com/net/de_de/SupportPortal/Downloads/565963/618809/Getting%20started%20with%20E2M_CM.pdf.



Licences can be obtained from the Festo App World (www.festo.com/appworld). There are two different licence packages available for our SaaS (Software as a Service):

- 1-month dashboards licence
- 1-year dashboards licence

A 4-week trial licence is available in both cases.

1.1.1 Required hardware, CMMT-AS and CMMT ST

In addition to Festo's motor controller CMMT, the Gateway CPX-IOT is also required in order to use the CMMT dashboard. We offer this in the following configurations:

M18 power connector: 50E-T70GCQS-Z
⅞" power connector: 50E-T70GCQP-Z
IP20 power connector: 53E-T70GCQE-Z

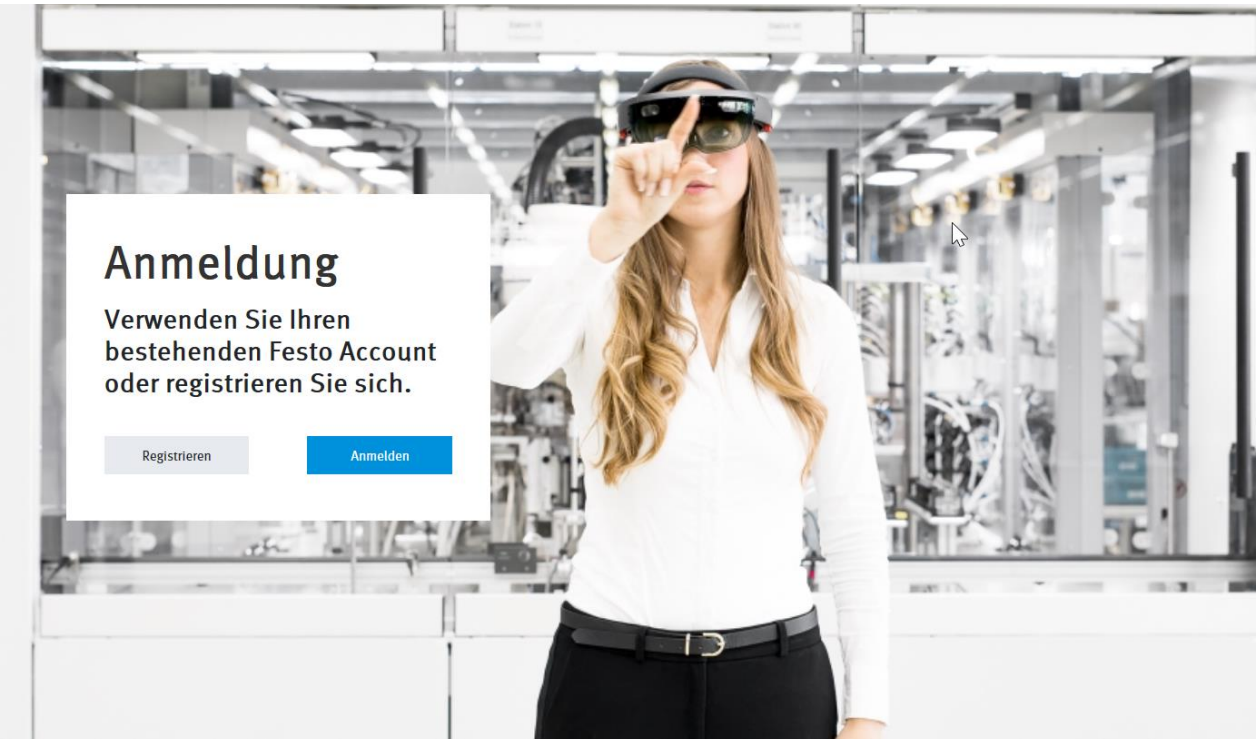
A dashboard licence makes it possible to use a dashboard for a Festo motor controller CMMT. Licences can be obtained from the Festo App World (www.festo.com/appworld). Two different licence packages are available:

- 1-month dashboards licence
- 1-year dashboards licence

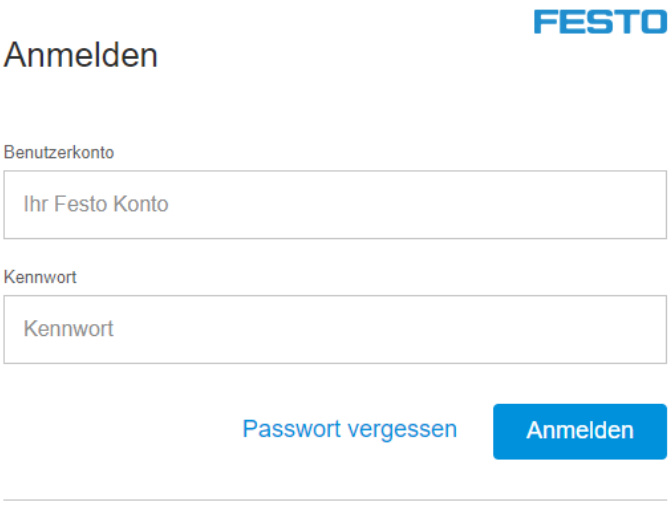
A 4-week trial licence is available in both cases. The gateway CPX-IOT must also be connected to the motor controller via a standard X18 Ethernet port. Detailed commissioning instructions can be accessed at the following link: https://dummy.de.

2 Registration, migration and login

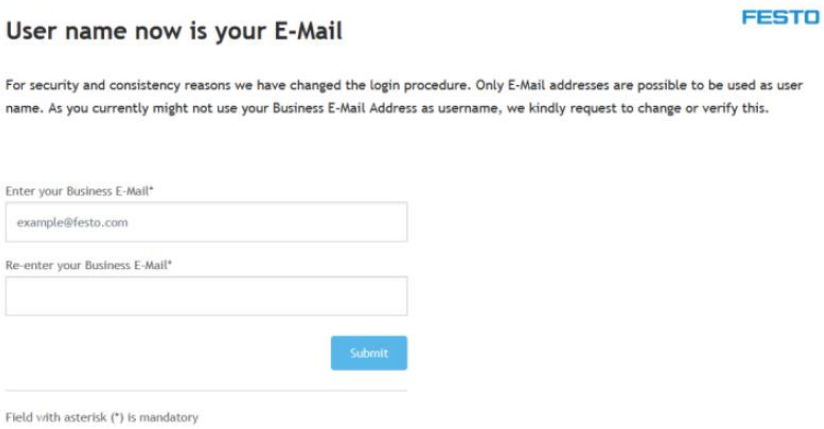
You can use the login data from your Festo Online Shop account in order to log in to Festo Dashboards. If you already have a Festo Online Shop account, just click on “Login”. If you do not yet have log-in data, register below: https://dashboards.festo.com.



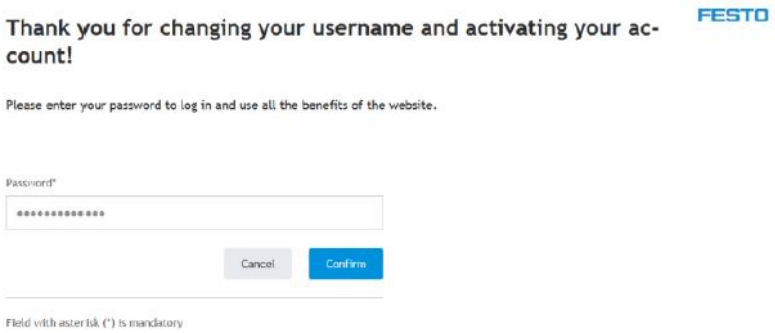
In order to use Festo Dashboards or Projects, one-time migration of your Online Shop user is required (* migration is a switchover process in a data processing system). Log in via the Dashboards or Projects log-in page with your current user data from your Festo Online Shop account. Then click on “Login”.



You are forwarded to the migration page. Enter your e-mail address to both fields. The entered e-mail address is used as the username (User) when logging in to Dashboards and Projects. The same e-mail address can be used as for the Festo Online Shop. Click on “Submit” after entering the e-mail address.



An e-mail is then sent to the e-mail address specified in the migration process. Click on the link in the e-mail. A window then appears to which the password must be entered once again. The migration process is completed by selecting “Confirm”. Dashboards and Projects can now be used.



Note:

Dashboards and Projects use the same migration process. If migration has been completed for one of the two, no additional migration is required for the other.

Dashboards and Projects support single sign-on (SSO). If you are logged in to one of these applications, you do not need to log in to the other applications as well. In addition, all web applications can be used with the same Festo Shop user.

3 Onboarding the gateway and components

3.1 Prerequisites for onboarding

In order to display data in a dashboard, a component (such as a valve terminal CPX/MPA or an energy efficiency module MSE6-E2M) must be physically connected to an IOT gateway CPX-IOT (hereinafter referred to as “gateway”) from Festo.

To ensure a smooth commissioning process (referred to below as “boarding”), make sure you have the product key of the gateway and components to hand. A valid licence is required in order to complete the boarding of the components. When boarding components for the first time, it is not necessary to purchase a licence via the Festo App World. A one-time trial licence (valid for 30 days) is available free of charge. After the trial licence has expired, a regular licence can be purchased from the Festo App World. It is also possible to visit the Festo App World when licencing is prompted during the boarding process.

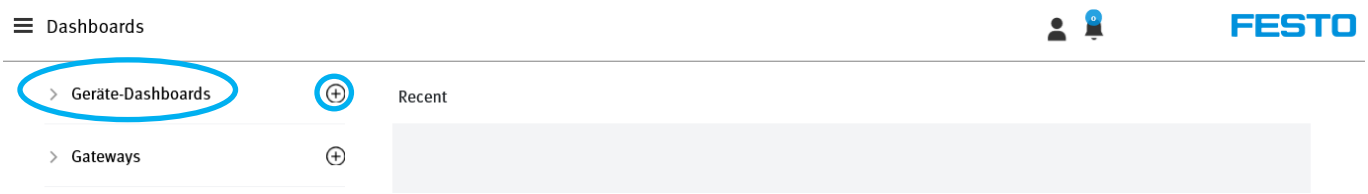
In order to guarantee a smooth boarding process, make sure you use the correct product keys. The product key for the gateway appears on the top of the device. The product key for the components appears on the left-hand side of the housing. It consists of an alphanumerical character string such as “SWRL9SB4T9T”.

Boarding the gateway is started and you are guided through the procedure in Festo Dashboards (https://dashboards.festo.com). The gateway is boarded digitally in the application as well as physically at the gateway. However, the procedure can also be completed at a remote location away from the gateway, as long as someone can manually select the appropriate switch settings at the gateway. This procedure ensures that only the actual owner of the gateway can complete boarding. The user who boards the gateway is the owner and is assigned the role of “Owner”. Only the user with the “Owner” role receives unrestricted authorisation and can delete the gateway again.

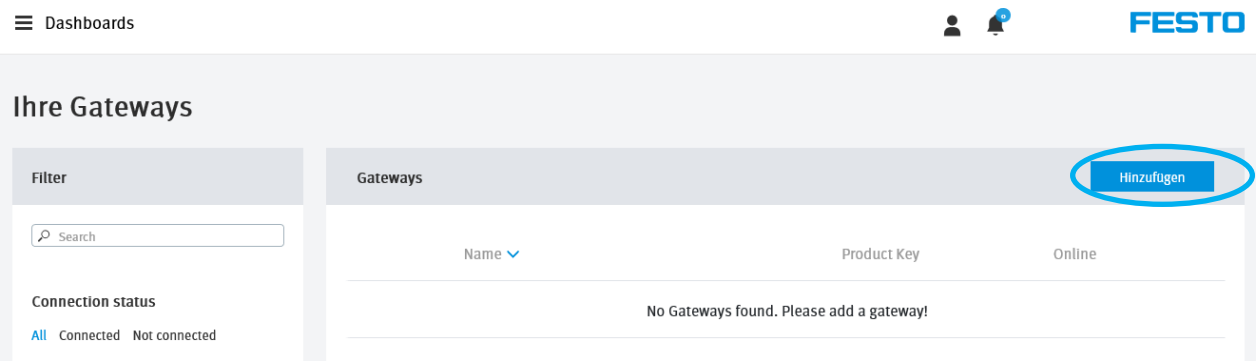
The boarding of components can be carried out autonomously and completely in the digital application. As a prerequisite, that the gateway must be set to switch position 3 = Read/Write and must already have been boarded. As is also the case with the gateway, the user who boards the component is its owner.

3.2 Gateway boarding

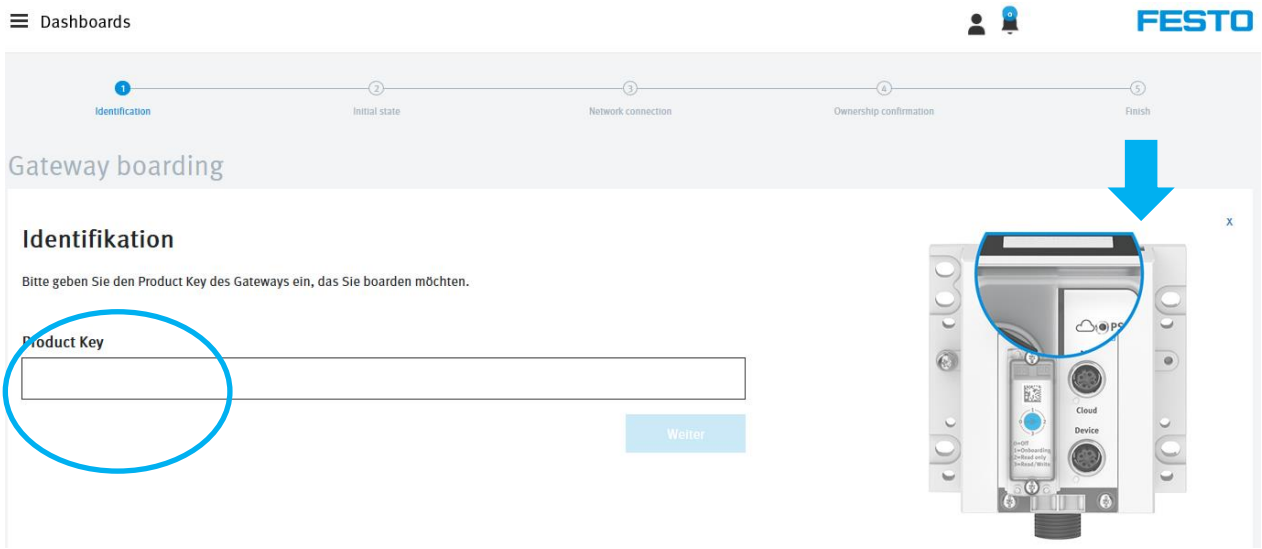
Boarding can start as soon as the gateway is connected to the network at the field level and an Internet connection has been established on the cloud side. Click on “Gateways” or on the (+) symbol in the “Dashboards” navigation menu to start gateway boarding.



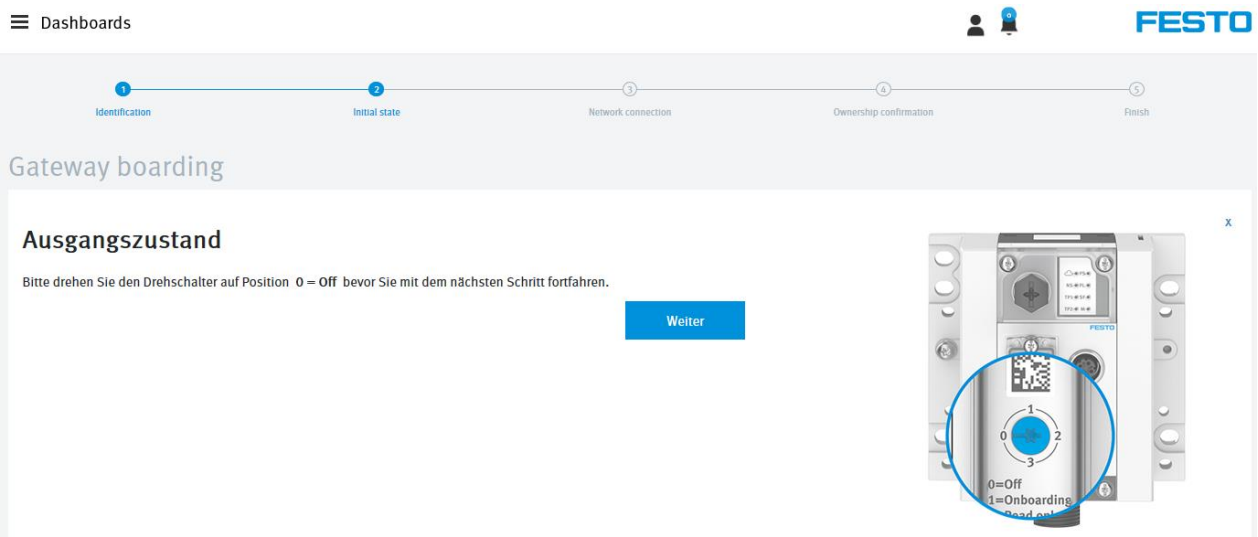
If you clicked on “Gateways,” you can access gateway boarding via the “Add” button.



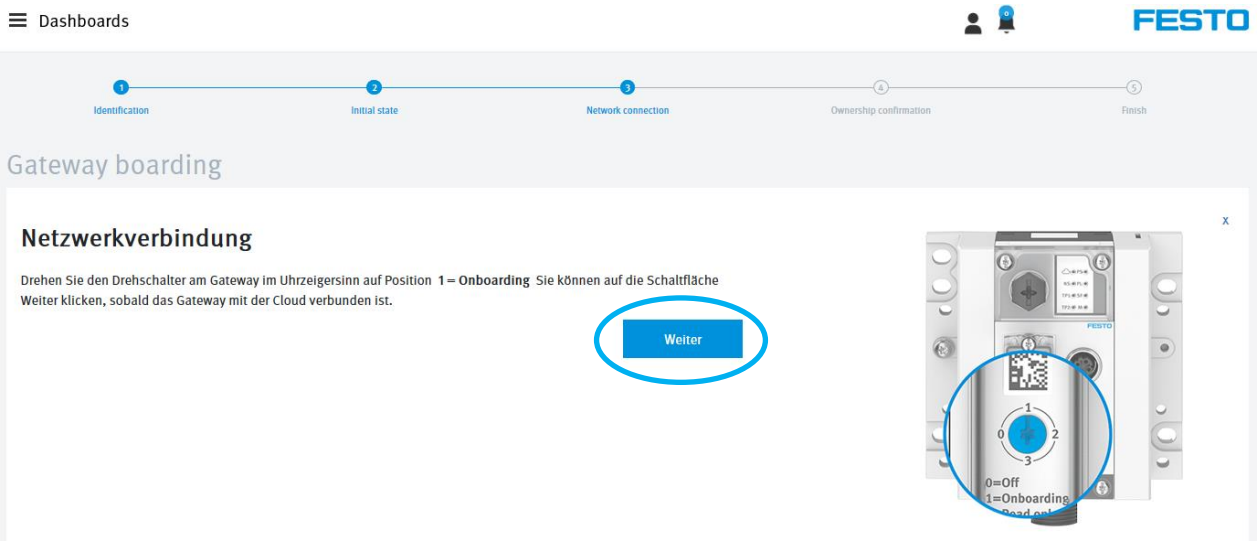
Now enter the product key for the gateway in the specified field. Product keys for gateways appear on the top of the device (see diagram on the right).



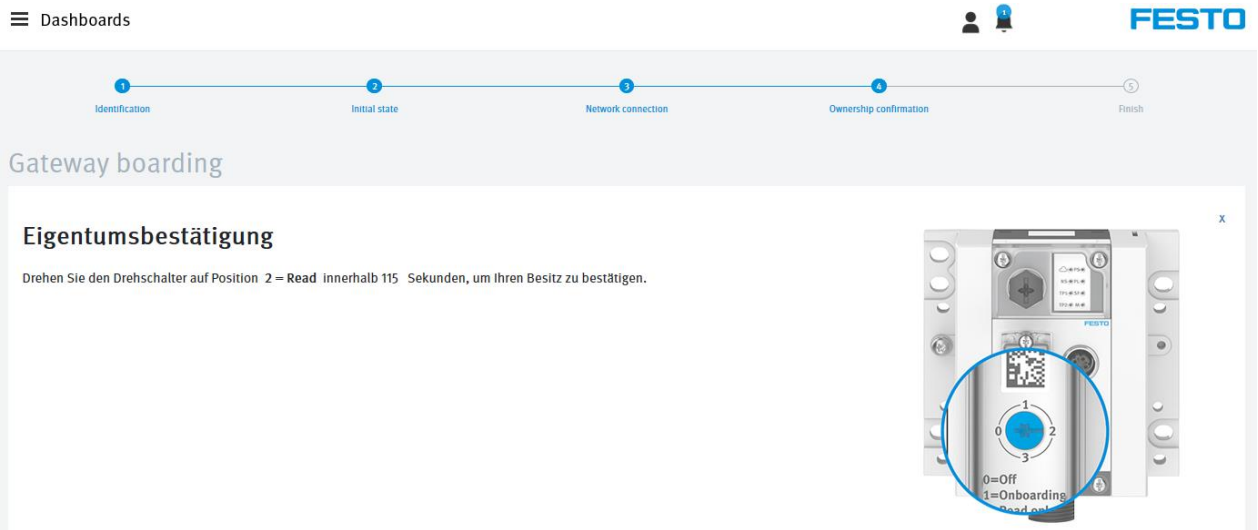
Then you can continue with the next step of boarding. Set the switch at the gateway to 0 = Off, after which the “Next” button is enabled. Now click on “Next”.



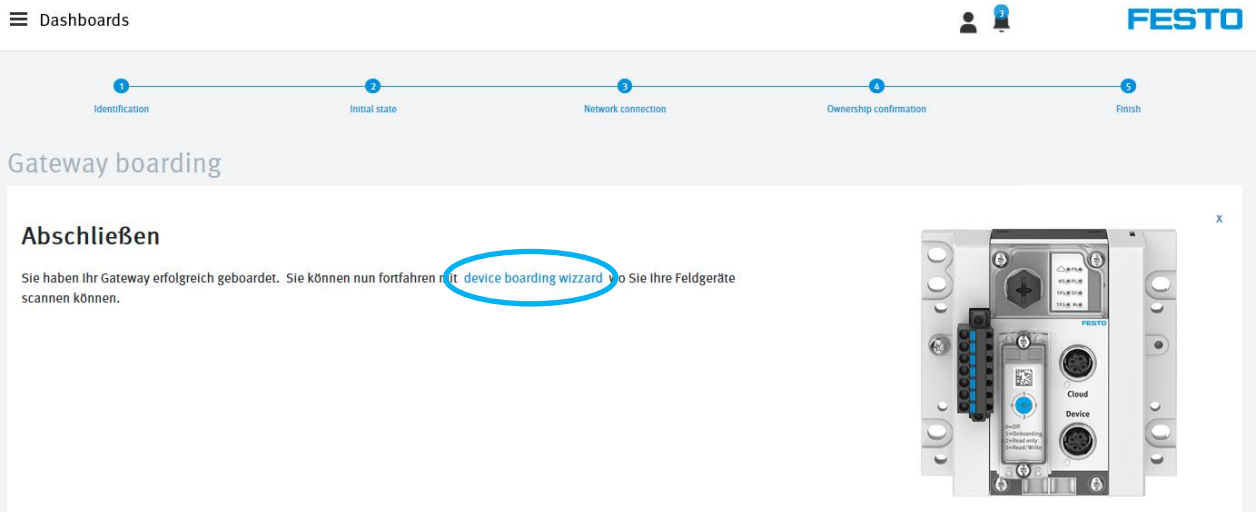
In the next step of the boarding process, turn the switch at the gateway clockwise to position 1 = Onboarding. A connection is now established between the gateway and the cloud. As soon as the connection has been established, the “Next” button is enabled Click on “Next”.



In the final step, you need to confirm ownership of the gateway. To do so, set the switch to position 2 = Read. It is important that switching takes place within 120 seconds. This is a security mechanism by means of which both physical and digital confirmation is obtained from the owner of the gateway. If switching does not take place within 120 seconds, the boarding process must be restarted.



You have now successfully boarded the gateway. You can now start boarding the devices/components. Select the “device boarding wizard” to this end.

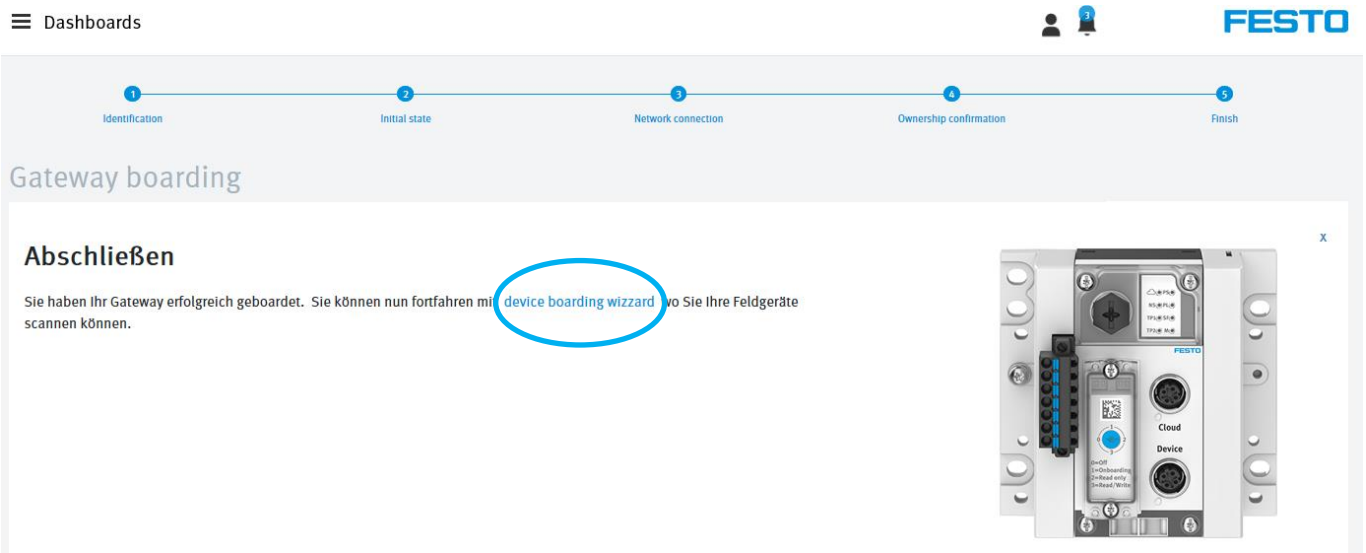


3.3 Device boarding process

Prerequisite: The gateway to which the desired device is connected must already have been successfully boarded. Connection must also have been established between the CPX-IOT gateway and the components at the field level, as well as between the CPX-IOT gateway and the cloud. If this is assured, you can start boarding the devices. There are three different boarding procedures.

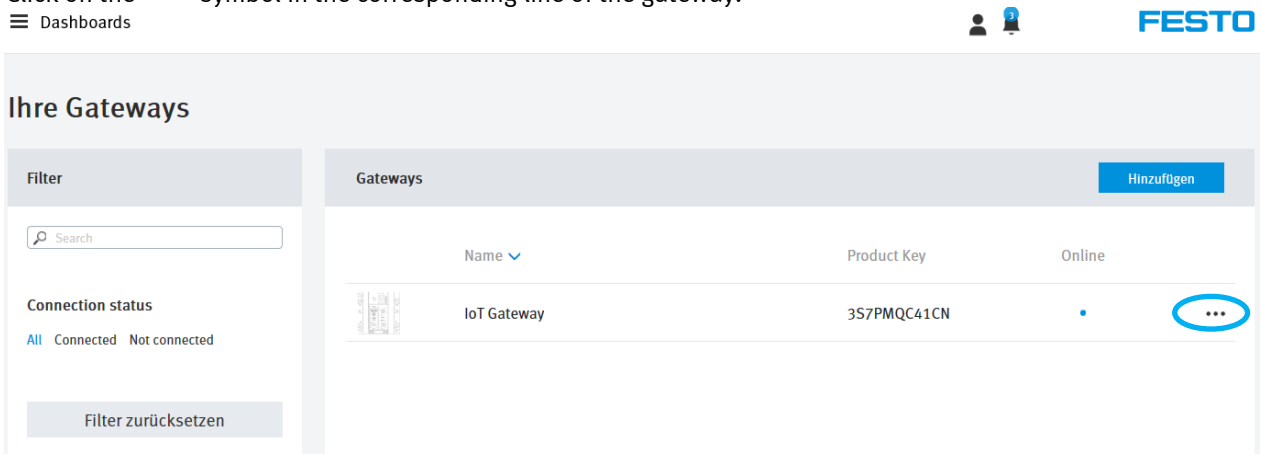
Procedure 1:

During the last step of gateway boarding, click on the “device boarding wizard” box. In this case you proceed directly to device boarding.

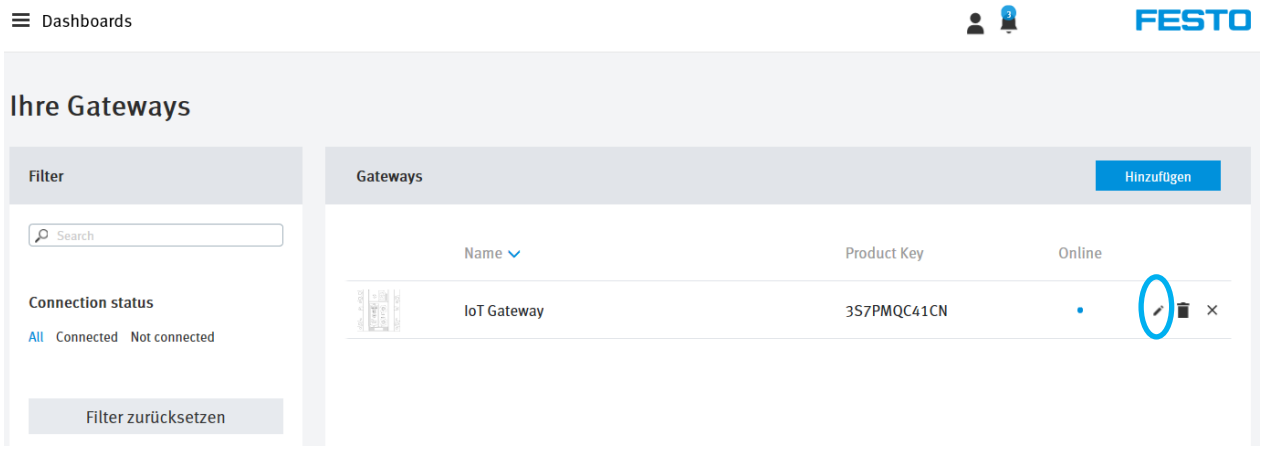


Procedure 2:

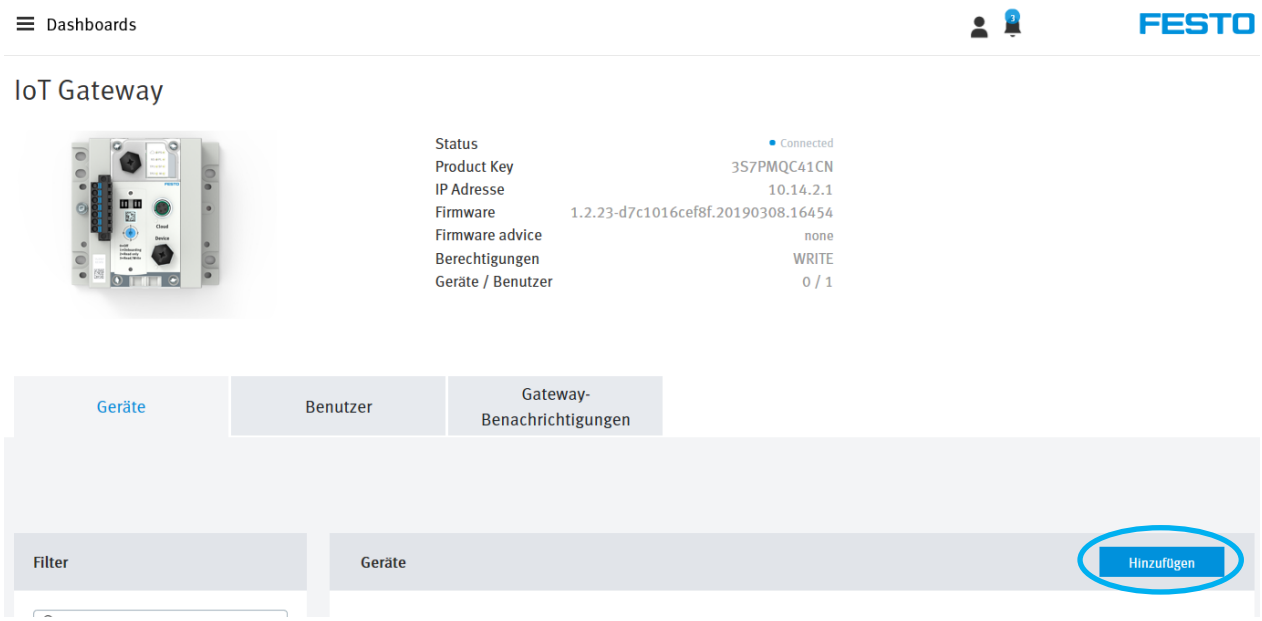
Click on “Gateways” in the “Dashboards” navigation menu. Here you can select the desired gateway to which the devices will be connected.
Click on the ••• symbol in the corresponding line of the gateway.



The toolbar now opens and you can click on the pencil icon to open the gateway’s dashboard.

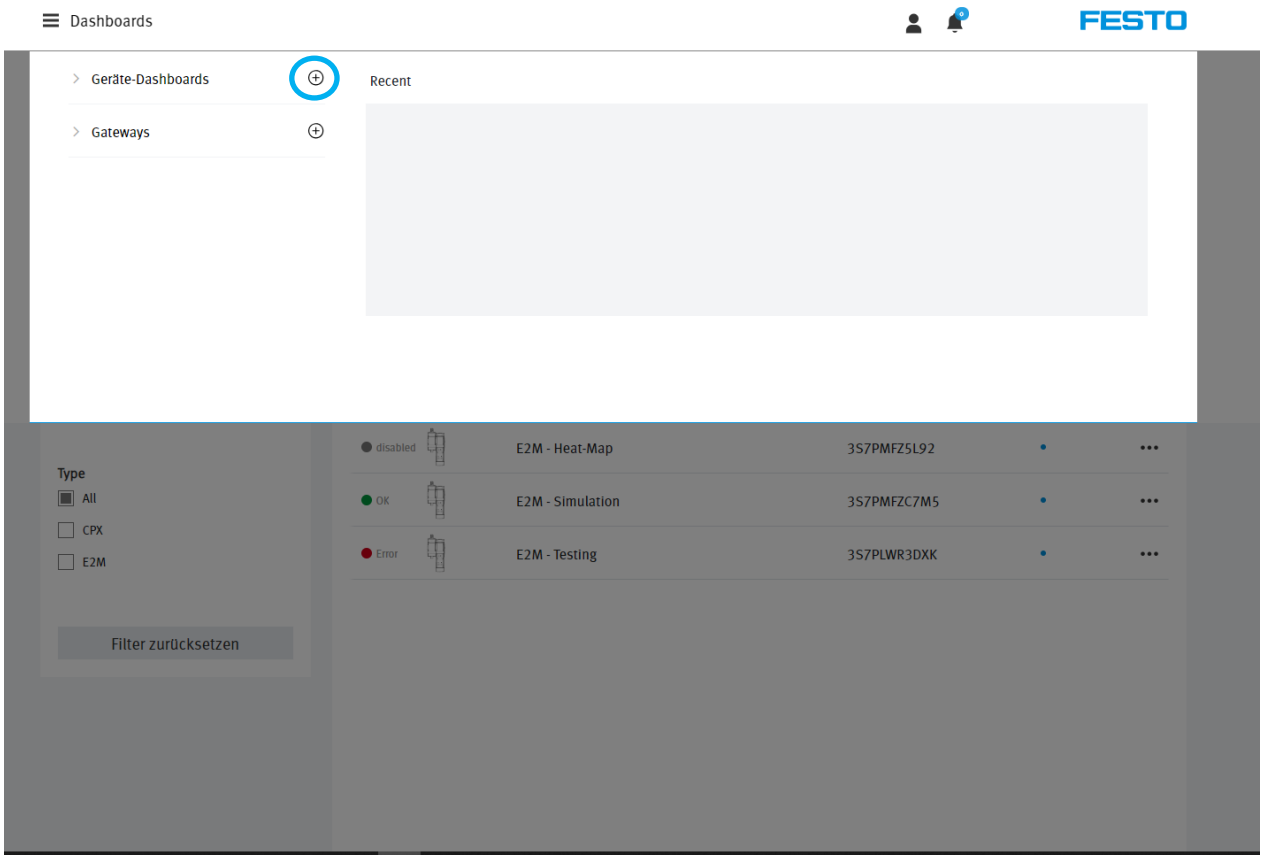


You can start scanning the connected components via the “Add” button in the gateway’s dashboard.

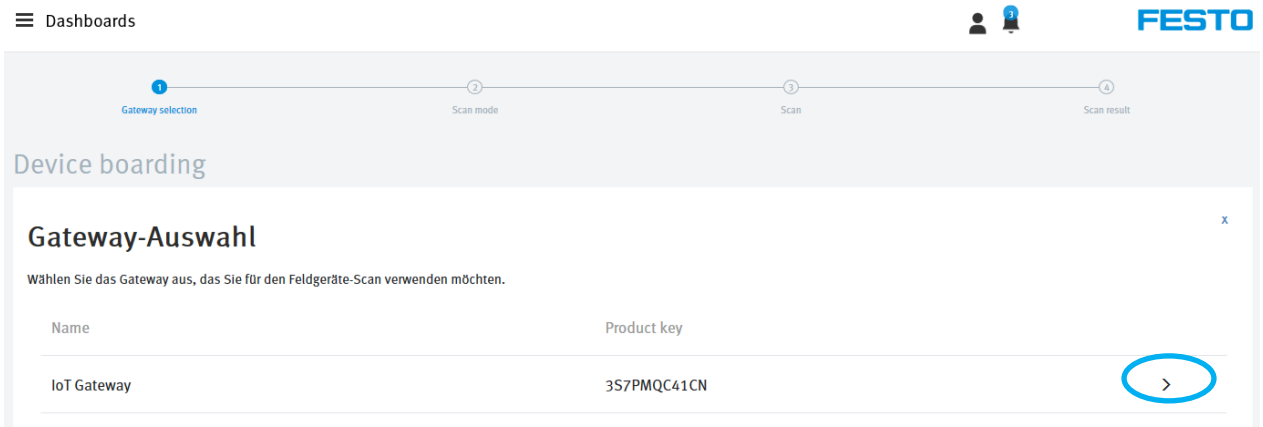


Procedure 3:

You can jump directly to device boarding by selecting (+) from the hamburger menu (the 3 thick bars on the left side of the application's screen).

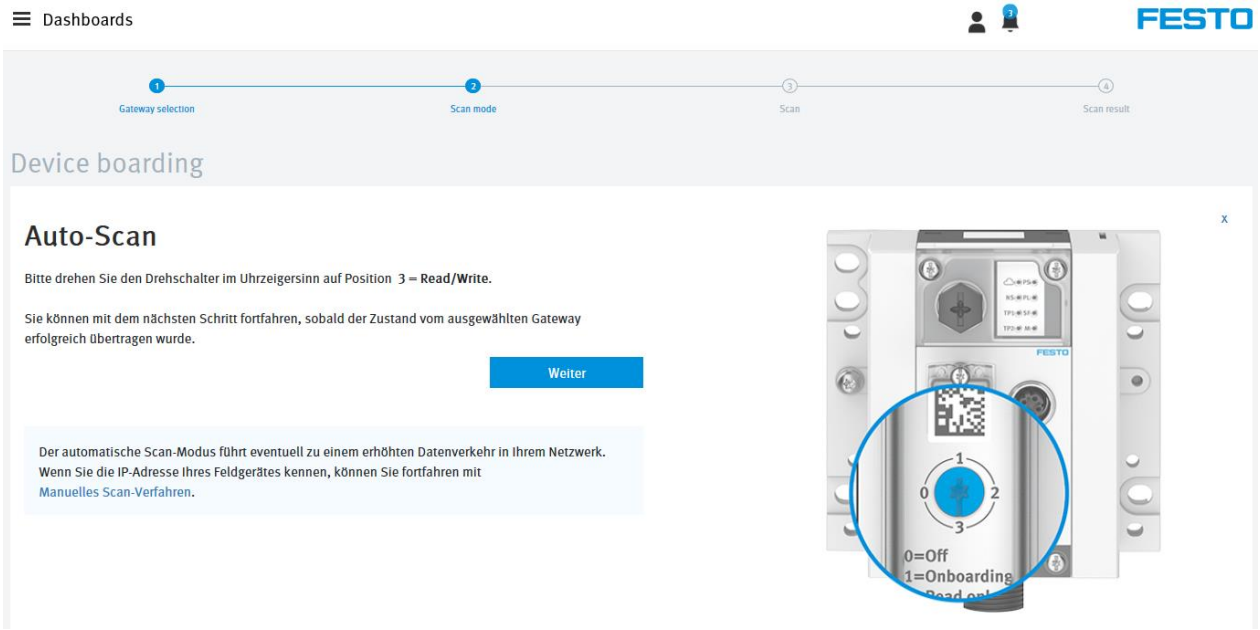


Whichever variant you choose, you will reach the first step of device boarding. Here, you have to select the gateway via which the devices are to be boarded. When this is done, you can jump directly to the next step.



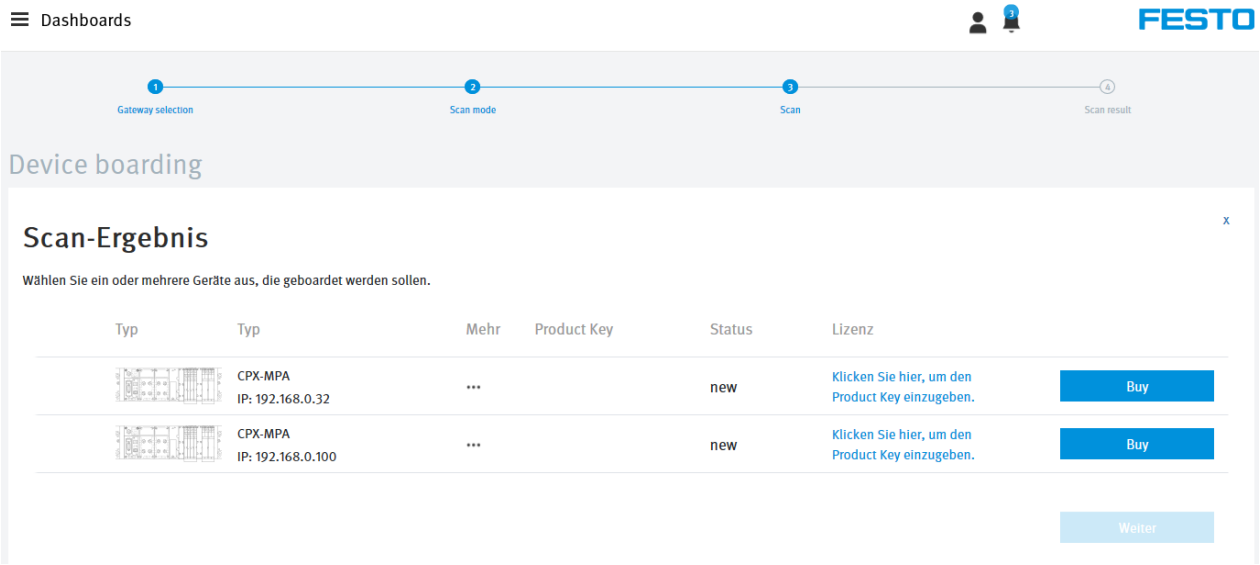
Here, you can now choose between two scanning procedures. During auto-scan, the gateway scans the field level and then lists all devices that can be boarded. By scanning manually, you can search for a specific device when the IP addresses are known. Basically, no distinction is made between the boarding statuses of the two scanning methods. The devices which are compatible with the dashboards are listed.

To carry out a scanning method, the rotary switch setting of the IoT gateway has to be sensed in advance. To do this, it must be set to position 3 = Read/Write. This is necessary in order to ensure that the appropriate boarding files can be created on the gateway during subsequent steps (write permission).



3.3.1 Auto-scan

The auto-scan method provides you with a list of all scanned devices for which a dashboard is available. All scanning results are displayed regardless of the boarding status.

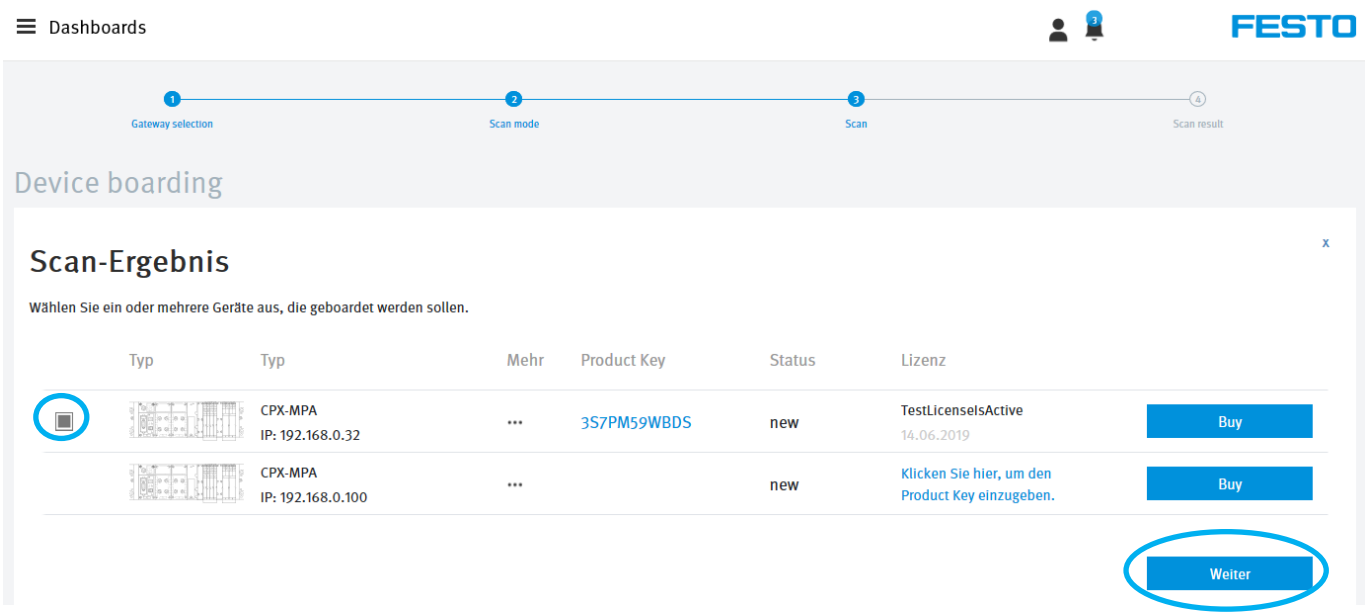


Note:

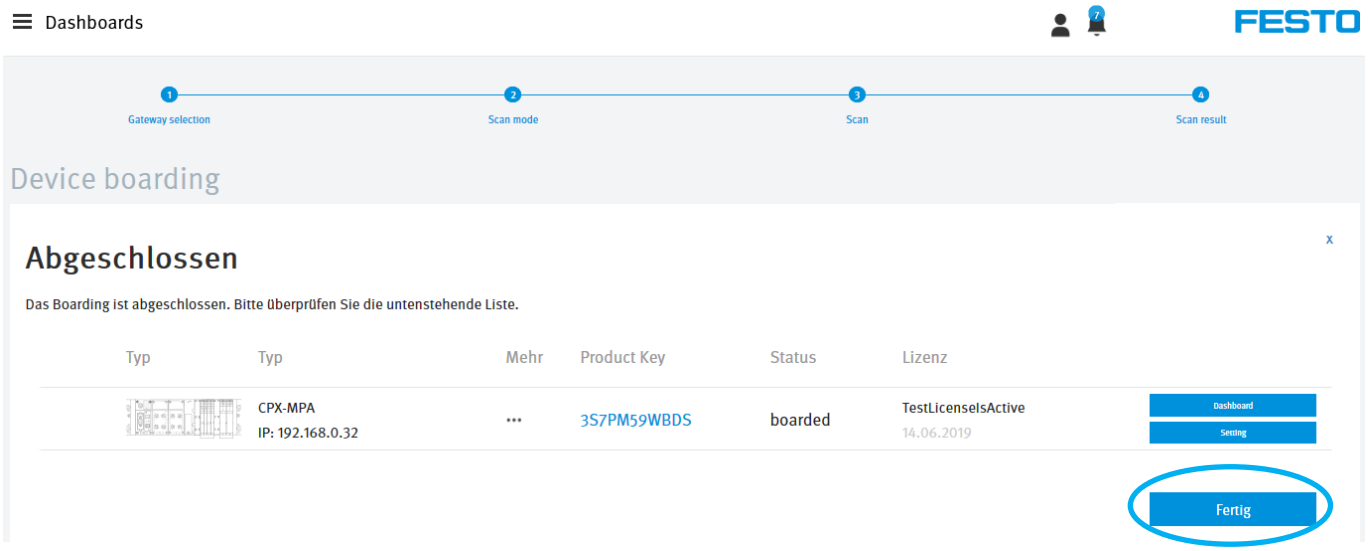
If no devices are found or if they are missing, a manual scan can be carried out when the IP address is known. If manual scans still do not yield a list of devices, checks must be carried out to determine whether they are in the same IP address space as the IoT gateway. The subnet mask must also be checked.

A valid product key (PK) must be entered in order to complete the boarding of a component. In the case of an MSE6-E2M, it is not necessary to enter a product key in the cloud. This is already done when commissioning the Condition Monitoring Library, where the PK is saved and subsequently read out. In the case of a CPX-MPA, the PK must be entered. The licences are examined after entering the product key.

If a valid licence and a product key are available, and the device has not been boarded, it is available for boarding. Select the devices to be boarded.



Click on “Ready” in order to successfully complete device boarding.

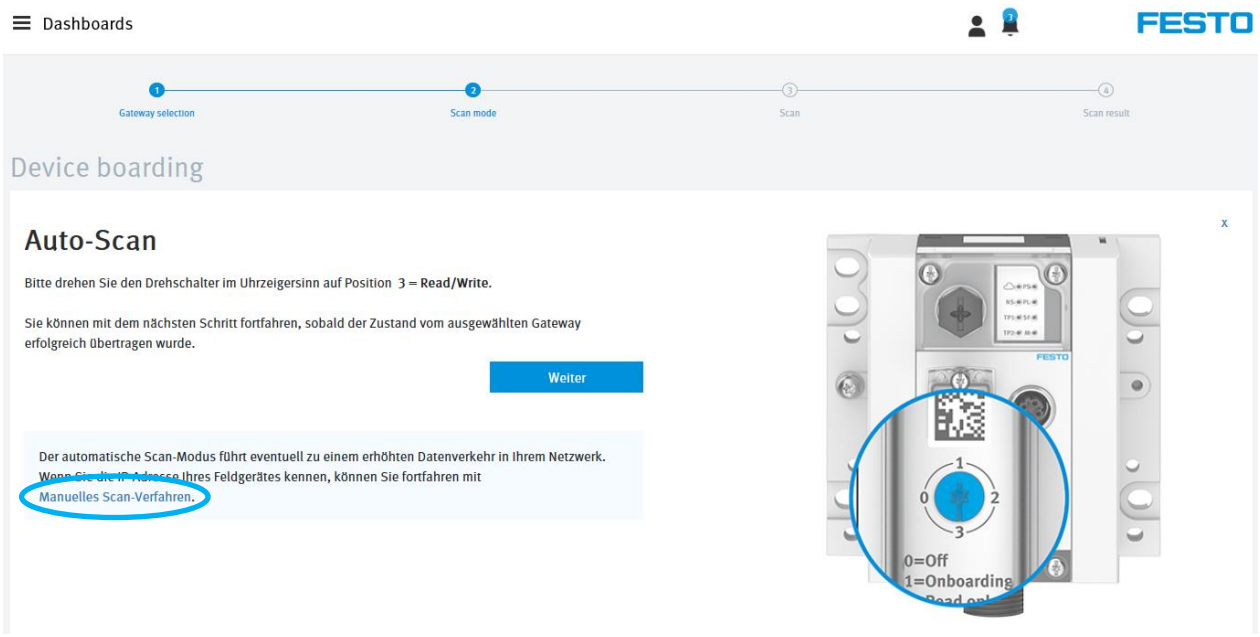


Note:
If a device has already been boarded, it cannot be selected for boarding again. This applies as well in the event that a device’s licence has expired or no licence is available. The status of the licence can be seen in the “Licence” tab. If an incorrect product key is entered, an appropriate error message is read out and boarding cannot be completed.

3.3.2 Manual scan

After selecting the gateway on which the devices are to be boarded, you can choose between auto-scan and manual scan. If the manual scanning process is selected, the IoT gateway will search for entered network

participants. This allows the search to be carried out more quickly with known IP addresses, because a complete network scan is not necessary. In addition, manual scanning reduces network utilisation at the field level.



If manual scanning has been selected, an IP address must be entered in step 2, “Scan Mode”. Once this has been done, you can click on “Next”. Now the gateway searches for the network participant with the entered IP address.

3.4 Deleting a gateway

The following two options are available for deleting a gateway:

- Delete gateway
- Forced gateway deletion

Prerequisite:

Only end users with the “Owner” role are authorised to delete a gateway.

Please also note that when deleting a gateway, all devices connected to are also be deleted. There is no need to connect the devices to the gateway. The “Delete gateway” function is recommended.

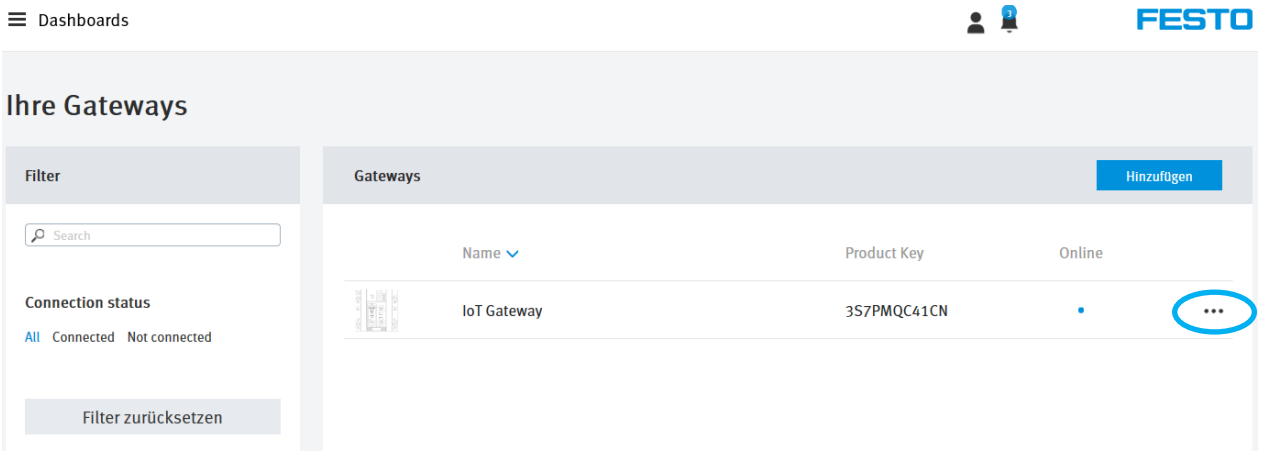
3.4.1 Delete gateway

As a prerequisite for deleting a gateway, the gateway must be connected and the rotary switch must be set to position 3 = Read/Write. If these prerequisites cannot be met or fulfilled, it is possible to force deletion of the dashboard via the cloud -› more in section 2.2.2, “Forced off-boarding”.

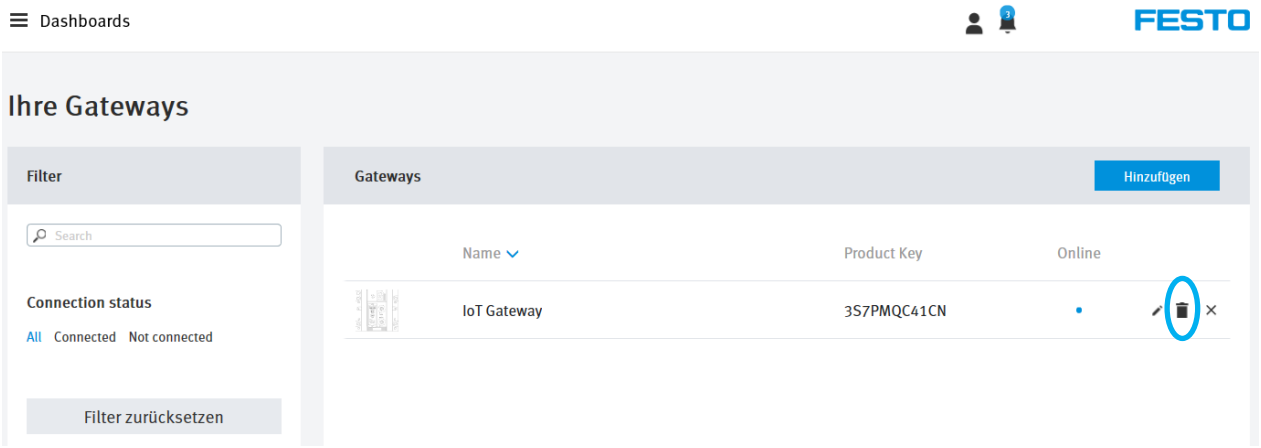
Attention:

Please note that when a gateway is deleted, all devices boarded on the respective gateway are also deleted.

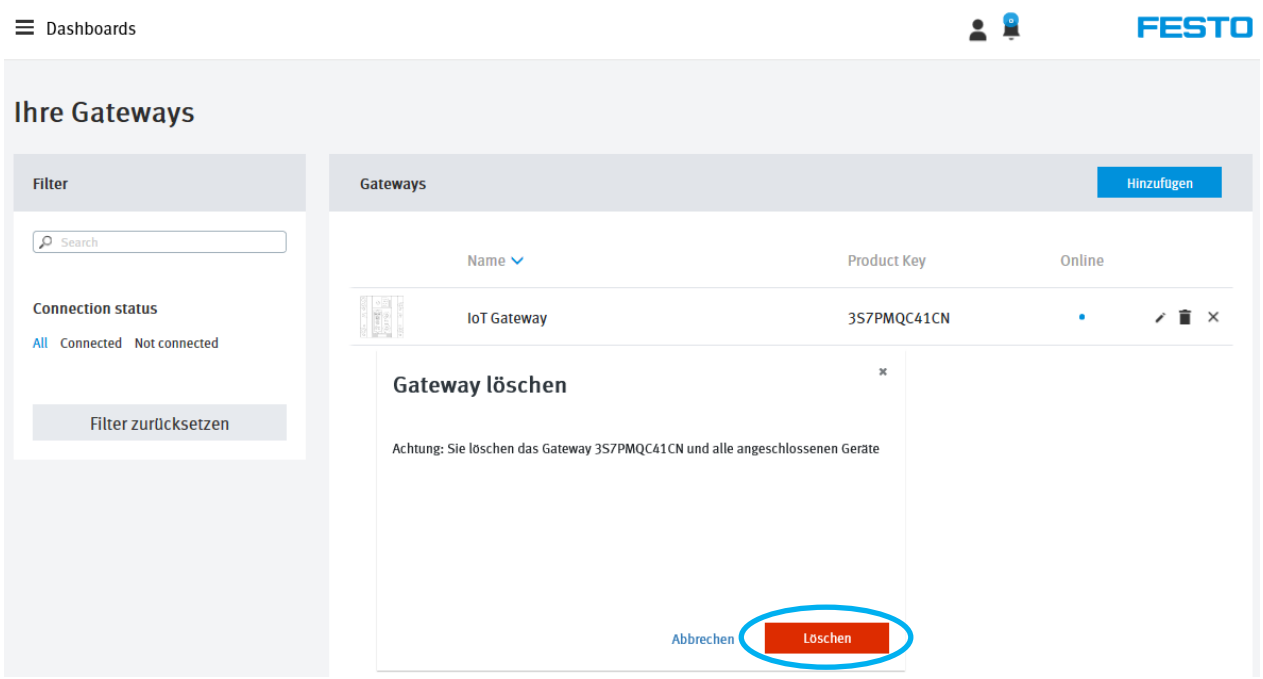
In order to delete a gateway, click on “Gateways” in the “Dashboard” navigation menu. Then select the required gateway by clicking on this symbol ••• in the corresponding line.



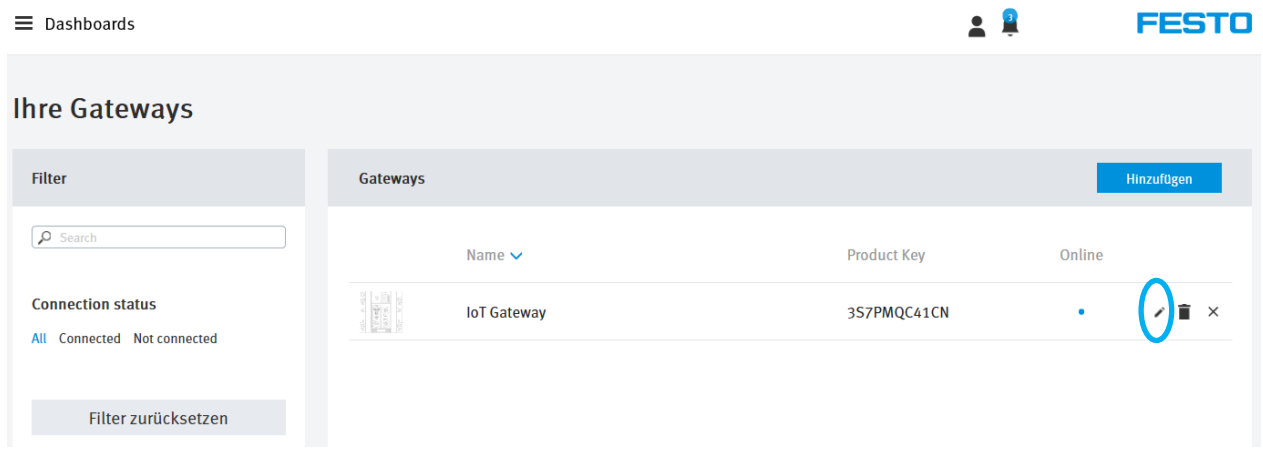
A toolbar appears. There are two ways to delete the gateway. The quickest way is to click on the “Recycle bin” icon.



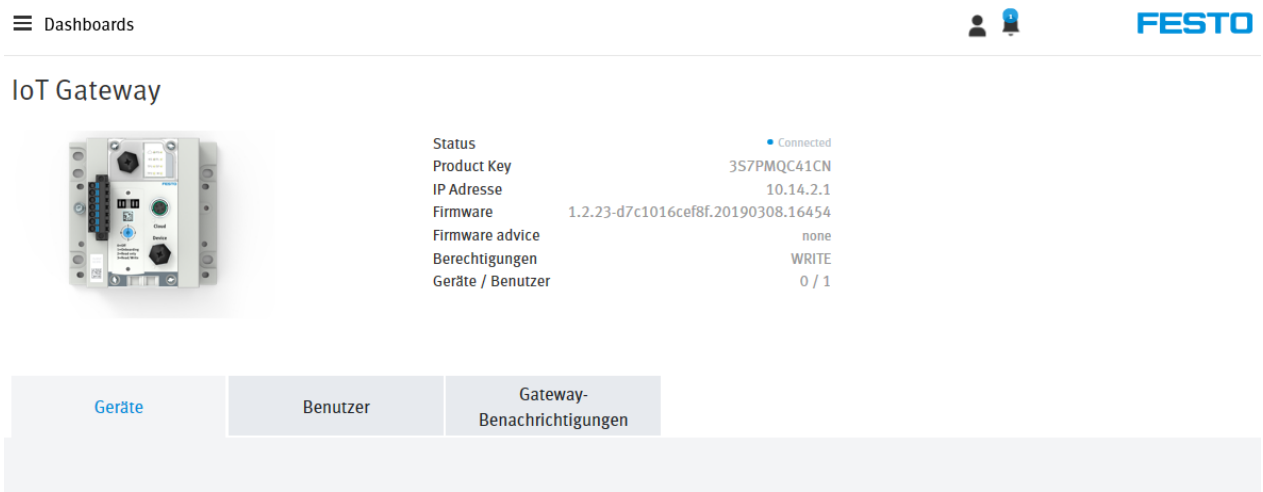
The gateway and all connected components are deleted by clicking on “Delete”.



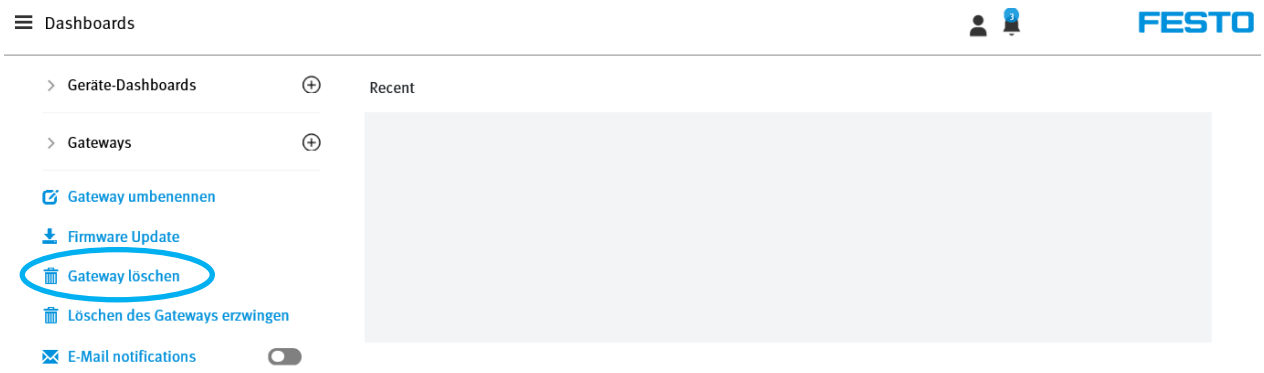
But you can also delete the gateway by clicking on the pencil icon.



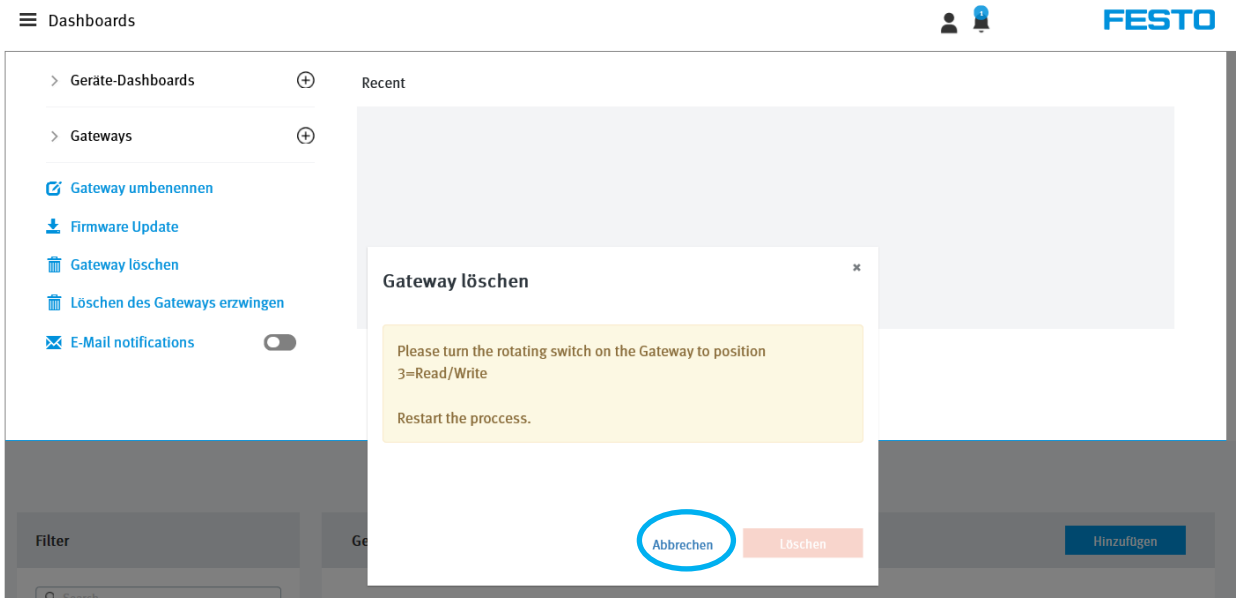
Clicking on the pencil icon first of all opens the gateway's dashboard. Amongst other things, you can see here which devices have been boarded for this gateway.



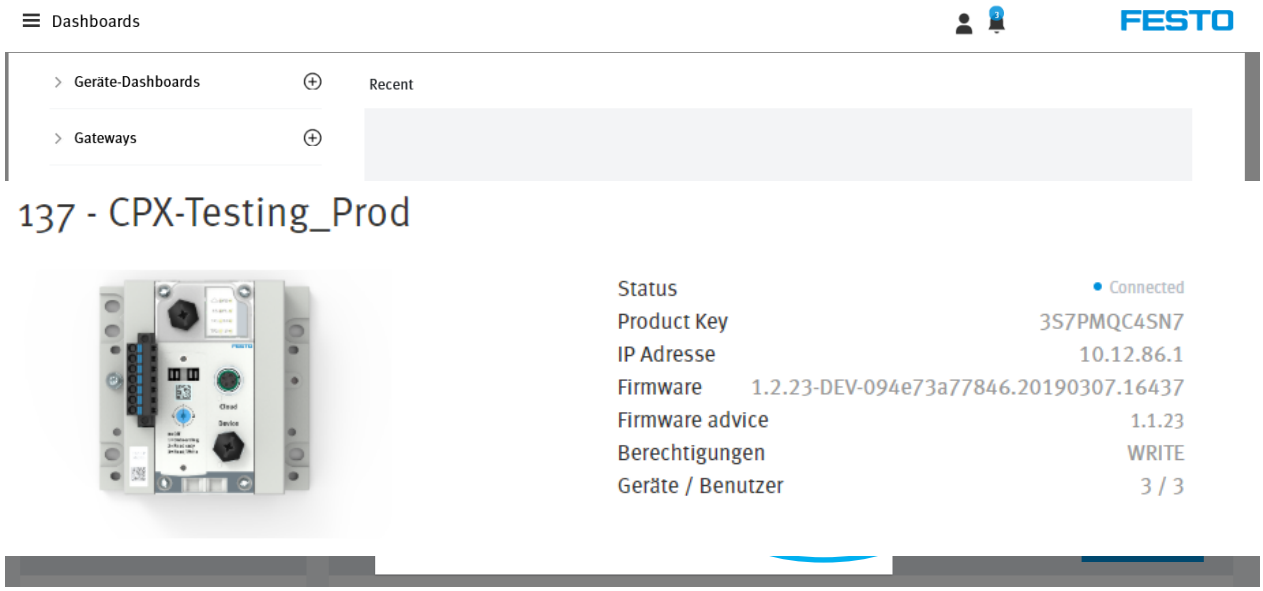
Now click on “Delete gateway” in the “Dashboard” navigation menu.



The “Delete gateway” window then appears and you are prompted to set the switch at the gateway to position 3 = Read/Write. When this is done, close the window by clicking on the “Cancel” button.



Then click once again on “Delete gateway” in the navigation menu on the left. The “Delete” button is now enabled and you can use it to complete deletion of the gateway.

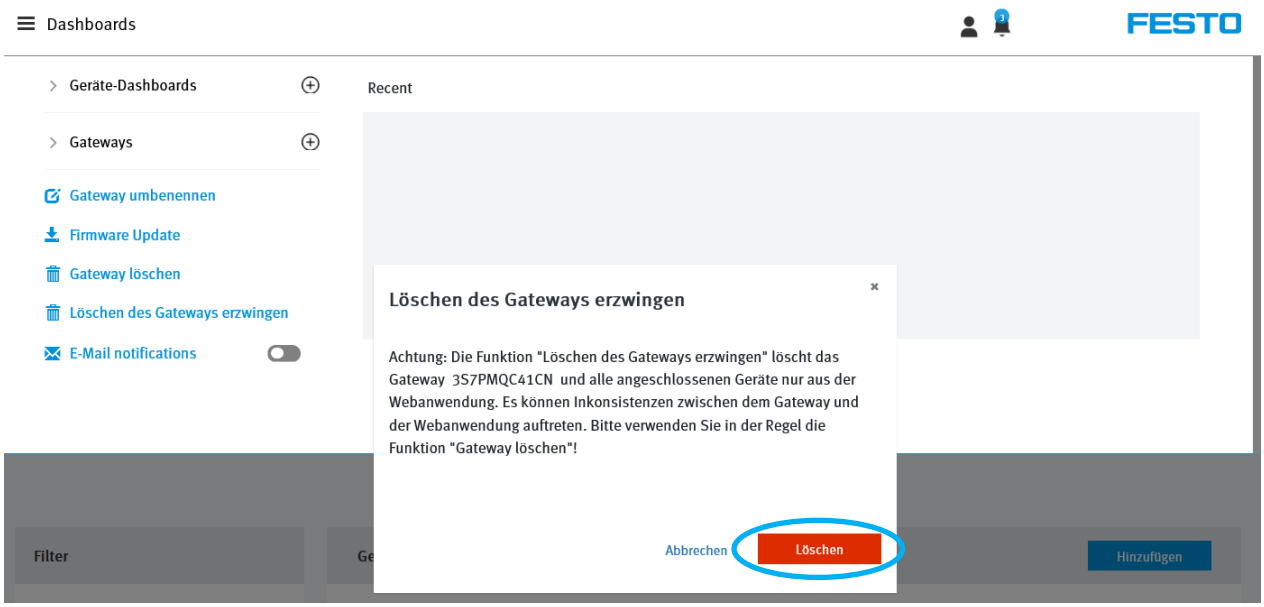


Note: If a gateway cannot be deleted, first determine whether or not the gateway is set to switch position 3 = Read/Write. This can be checked on the Gateway page. “WRITE” authority must be available here. If there is no

connection between the IoT gateway and the cloud, the gateway cannot be deleted. The connection status of the gateway can also be checked under “Status” on the Gateway page.

3.4.2 Forced gateway deletion

Only select this function if the gateway is no longer connected and you are no longer able to access it. Nevertheless, this function deletes the gateway and all connected devices on the cloud side only, which means that they are only deleted from the web application. All boarding files remain on the gateway. As a result, it is no longer possible to re-board the gateway together with the devices linked to it. However, it is possible to board the devices via a new gateway. In order to be able to use the gateway again, it must be set up by Festo Support.



3.5 Deleting devices

The following two options are available for deleting devices:

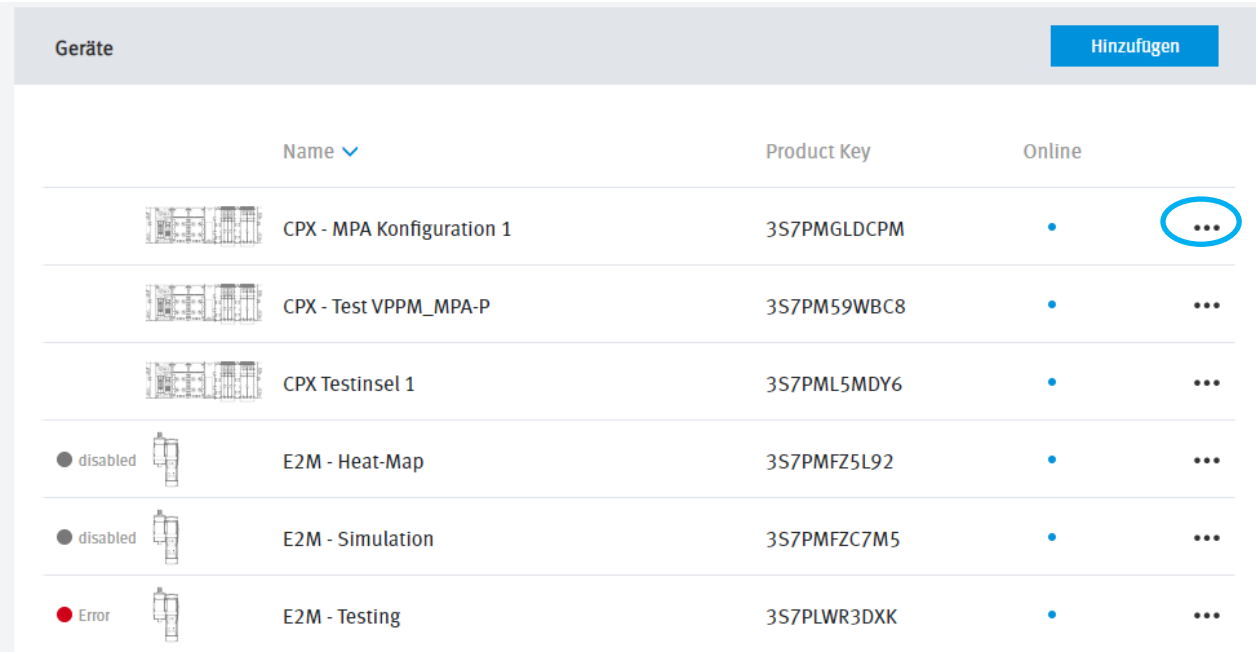
- Delete devices
- Forced device deletion

Prerequisite:
Only users with the “Owner” role are authorised to delete a gateway.

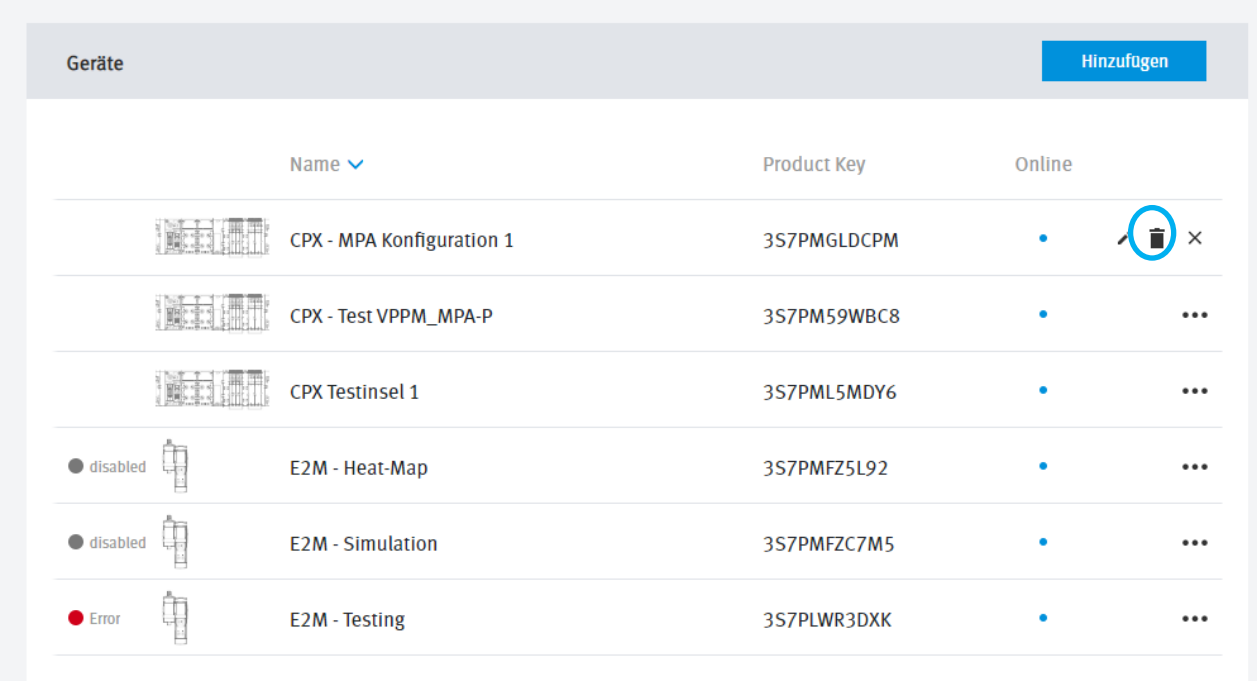
Please also note that data retention cannot be assured when deleting a device. There is no need to connect the devices to the gateway. We generally recommend the “Delete device” function.

3.5.1 Delete device

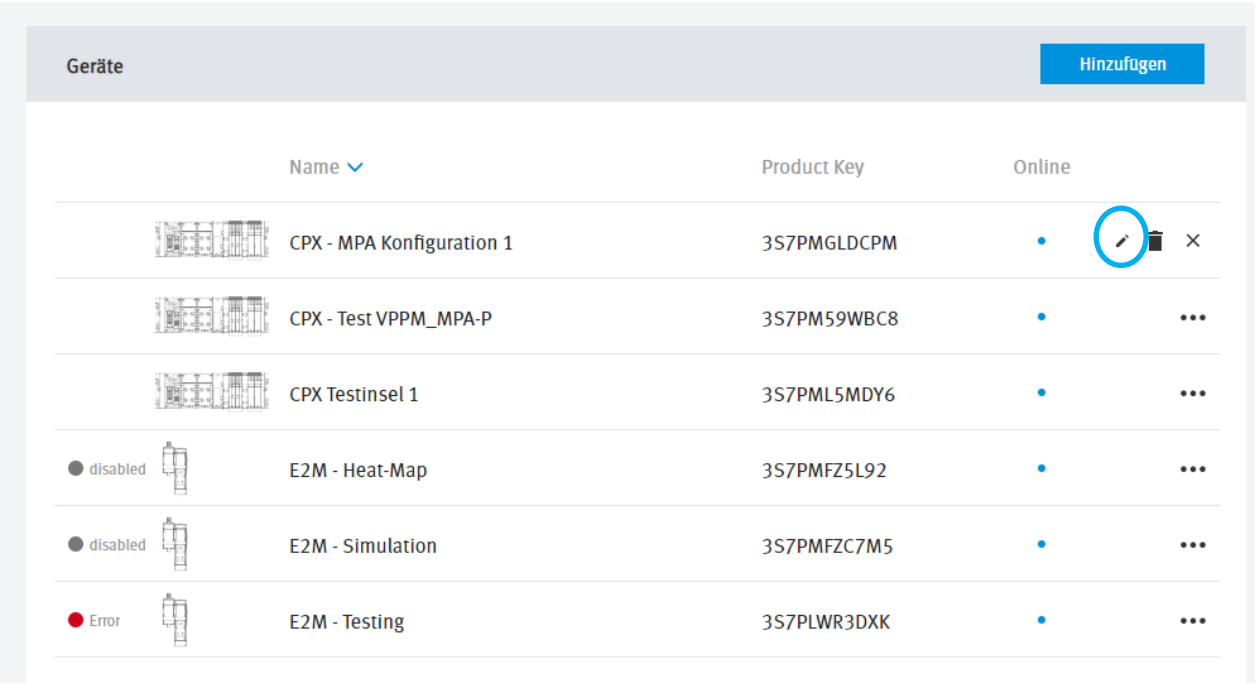
As a prerequisite for deleting a device, the gateway must be connected to the cloud and the rotary switch must be set to position 3 = Read/Write. If these prerequisites cannot be met or fulfilled, cloud-side hard deletion of the dashboards is also possible -› more in section 2.3.2, “Forced device deletion” (forced off-boarding). In order to delete a device, click on “Gateways” in the “Dashboards” navigation menu. Then select the required gateway by clicking on the ••• symbol in the corresponding line.



The toolbar then opens. There are two ways to delete the device. The quickest way is to click on the “Recycle bin” icon.

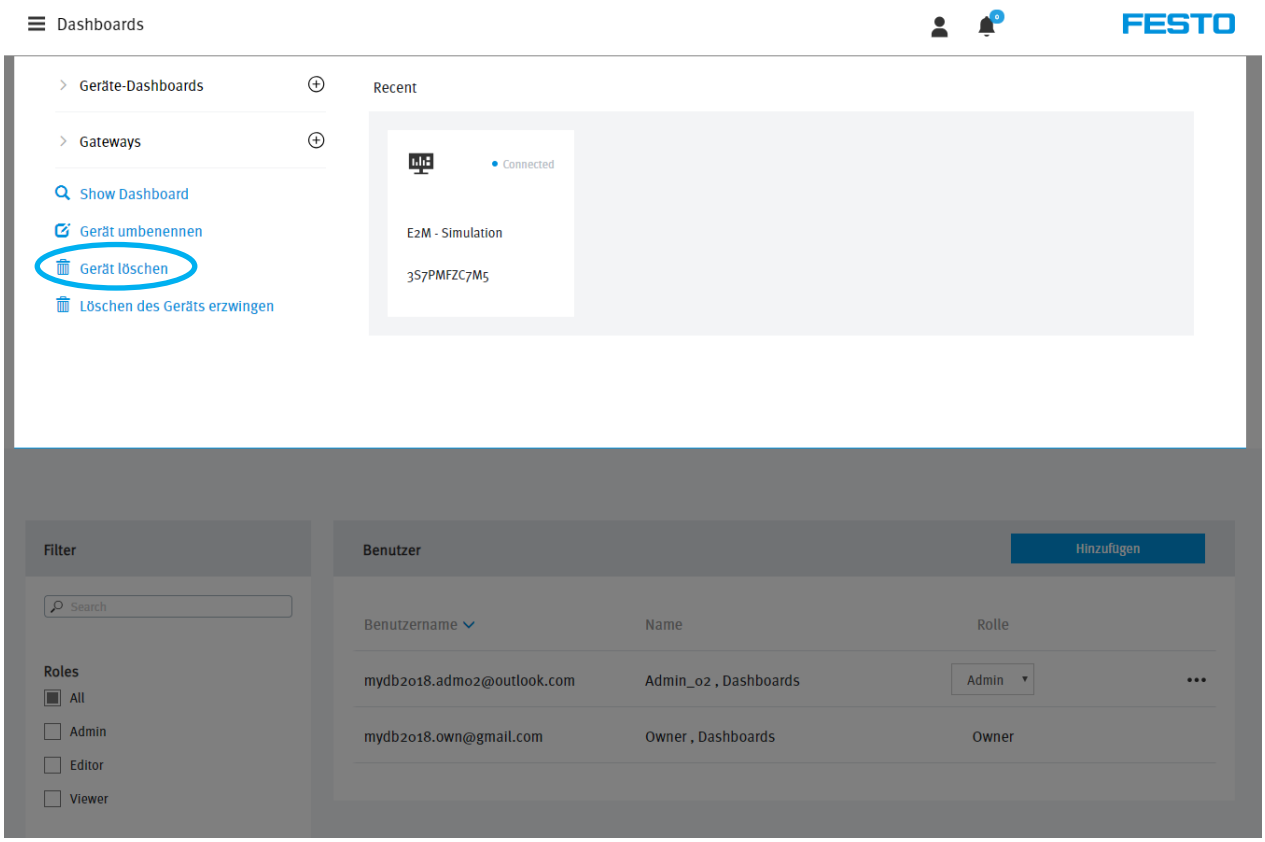


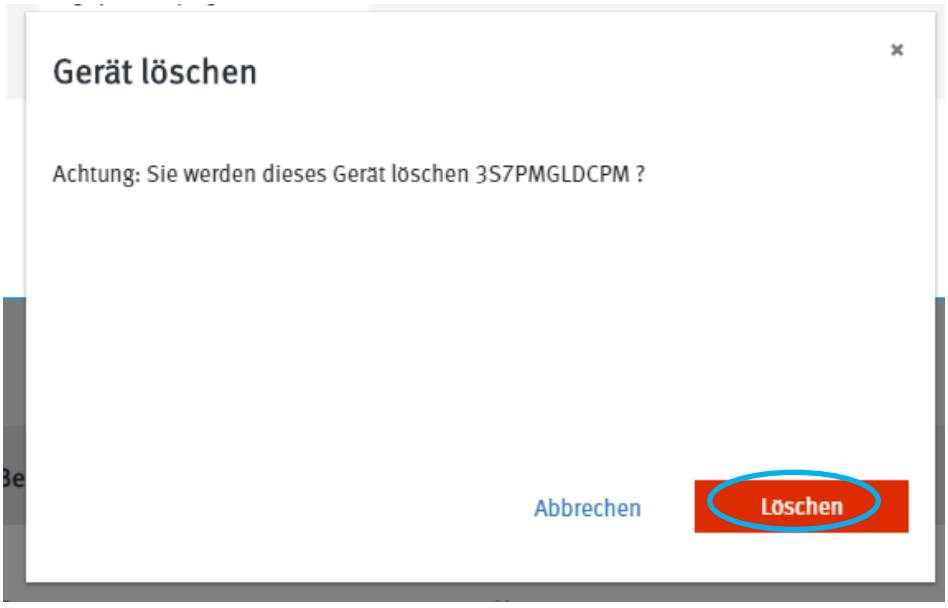
Clicking on “Delete” clears the devices from the cloud as well as the corresponding device files on the gateway. But you can also delete the device by selecting the pencil icon.



The dashboard page for the device appears. If the hamburger menu is opened in the dashboard, you can remove the components via the “Delete device” entry.

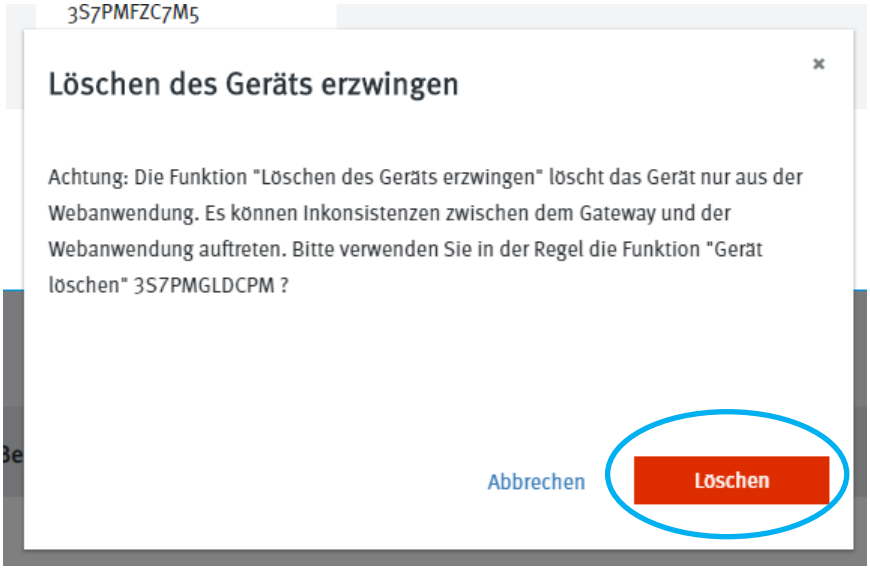
In either case, the “Delete device” window appears. The delete button is only enabled if the gateway is set to switch position 3 = Read/Write. If this is not the case, an appropriate message appears in the window.





3.5.2 Forced device deletion

Only select this function if the gateway is no longer connected and you are no longer able to access it. Nevertheless, this function deletes the devices on one side only, which means they are only deleted from the web application. The device's board files remain on the gateway. As a result, it is no longer possible to re-board the device in combination with the gateway. However, it is possible to board the devices via a new gateway. In order to be able to board the devices again via the gateway, it must be set up by Festo Support.



4 Dashboards

4.1 Gateway dashboard

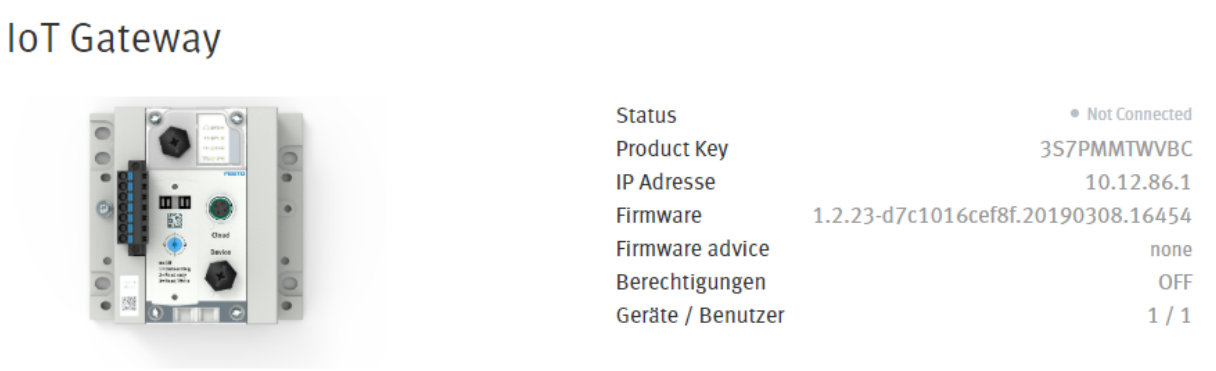
The gateway dashboard includes the gateway's asset information, a device list with the devices connected to it, user management and a notification centre. All data is available in a structured form. The gateway dashboard can also be used to start the boarding process to add additional components to the gateway.

4.1.1 Asset information

The gateway's asset information displays the connection status of the component, the gateway's product key and the cloud-side IP address. And thus the gateway can be uniquely assigned using an individual identifier. Furthermore, the current firmware status and a firmware recommendation are also read out. If the gateway already has the latest firmware, "none" is read out as the suggested firmware.

Information concerning write and read rights for the gateway can also be viewed in the authorisations window. If gateway authorisation is set to **Off**, the cloud interface is physically deactivated. This means there is no way to access the gateway or send data from the gateway to the cloud. The status of the gateway is thus **disconnected** and all connected devices are offline. With the **Read** authorisation level, data can only be sent from the gateway to the cloud. Write access from the cloud to the gateway is not possible. In addition, the boarding process cannot be started with this authorisation. This is only possible if the gateway has **Write** authorisation. Authorisation is set via the rotary switch on the gateway.

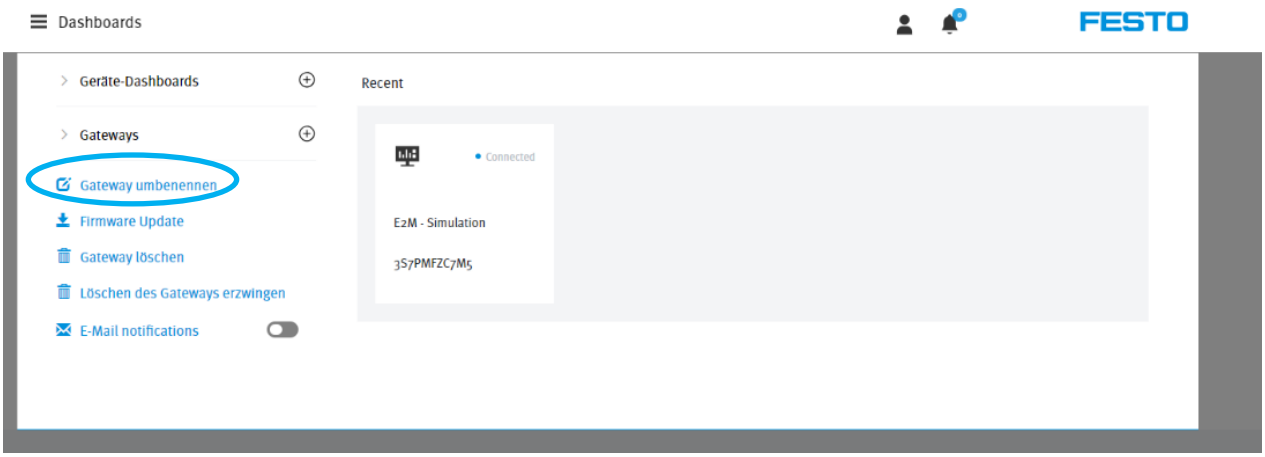
Device/user information displays the number of devices boarded on the gateway and the end users authorised to use the gateway. For detailed information on the connected devices, the device list can be viewed under the "Devices" tab. User management can be accessed in the "Users" tab in order to manage users.



4.1.2 Renaming the gateway

The gateway's name can be changed on the gateway dashboard page by clicking on the hamburger menu and selecting "Rename gateway". The name of the gateway can be used to uniquely identify the gateway to a system. For example, "Gateway name" is used in the "Gateway list" when selecting the gateway for boarding devices.

When naming the gateway and devices, any given name can only be assigned once. This applies to both the gateway and the device. If a name is entered that has already been assigned, a message appears indicating that renaming has failed. A gateway could be named, for example, "GW – Test". If a name is entered that has already been assigned, a message is displayed indicating that renaming has failed. Unequivocal assignment of names ensures that the dashboards are clear and easy to use.



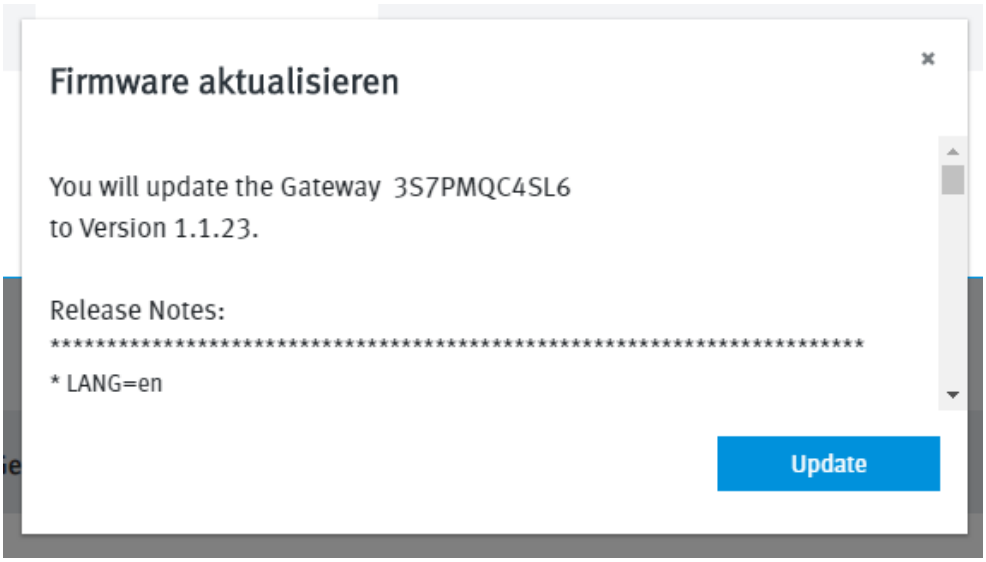
4.1.3 Firmware update

A firmware update for the gateway can be executed autonomously from the cloud. Local access to the gateway is not required. As a basic prerequisite for updating from the cloud, gateway authorisation must be set to “Onboarding”, “Read” or “Write”. Furthermore, the Internet connection between the gateway and the cloud must be stable. During the firmware update, the rotary switch position at the gateway may not be changed and the network connection must not be interrupted.

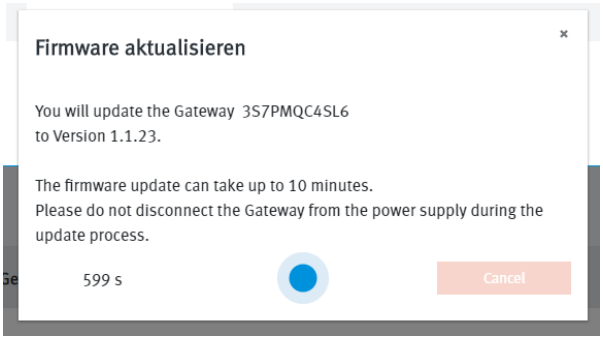
If, despite everything, a firmware update from the cloud fails, you can alternatively use the Festo Field Device Tool (FFT). You can enter the link from the Support Portal (SuP) to the FFT in order to download the firmware manually. The firmware is available from the Support Portal.

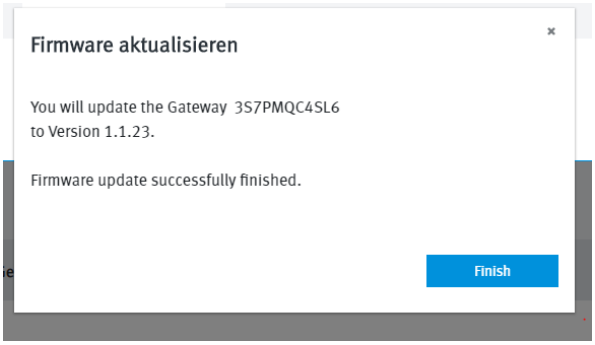
To start the firmware update, open the menu using the hamburger menu and select the “Firmware Update” entry. If the gateway is set to 0 = Off, there is no connection between the cloud and the gateway. This means that the boarding process cannot be started and a corresponding message is displayed. If, despite everything, a firmware update must be carried out, the rotary switch must be set to 0 = Onboarding, 1 = Read or 2 = Read/Write. Alternatively, you can also download a firmware update manually via the Festo Field Device Tool.

After selected “Firmware update”, an information window opens. This is where changes and bug fixes included in the new firmware release are shown.



The update process is started by clicking on “Update”. The update process can take up to 600 seconds (10 minutes). Connection between the gateway and the cloud must be assured during this time. After the update has been completed, the gateway is restarted. The “Gateway connection lost” message appears and, after re-connecting, the “Gateway connection established” message appears. Since the gateway must be rebooted, connection between the devices and the cloud is also interrupted. However, the connection is automatically restored after the gateway is restarted. As a result of the firmware update, the gateway and the devices boarded onto it cannot be accessed for as long as 10 minutes. And thus data which accumulates during this period cannot be processed.

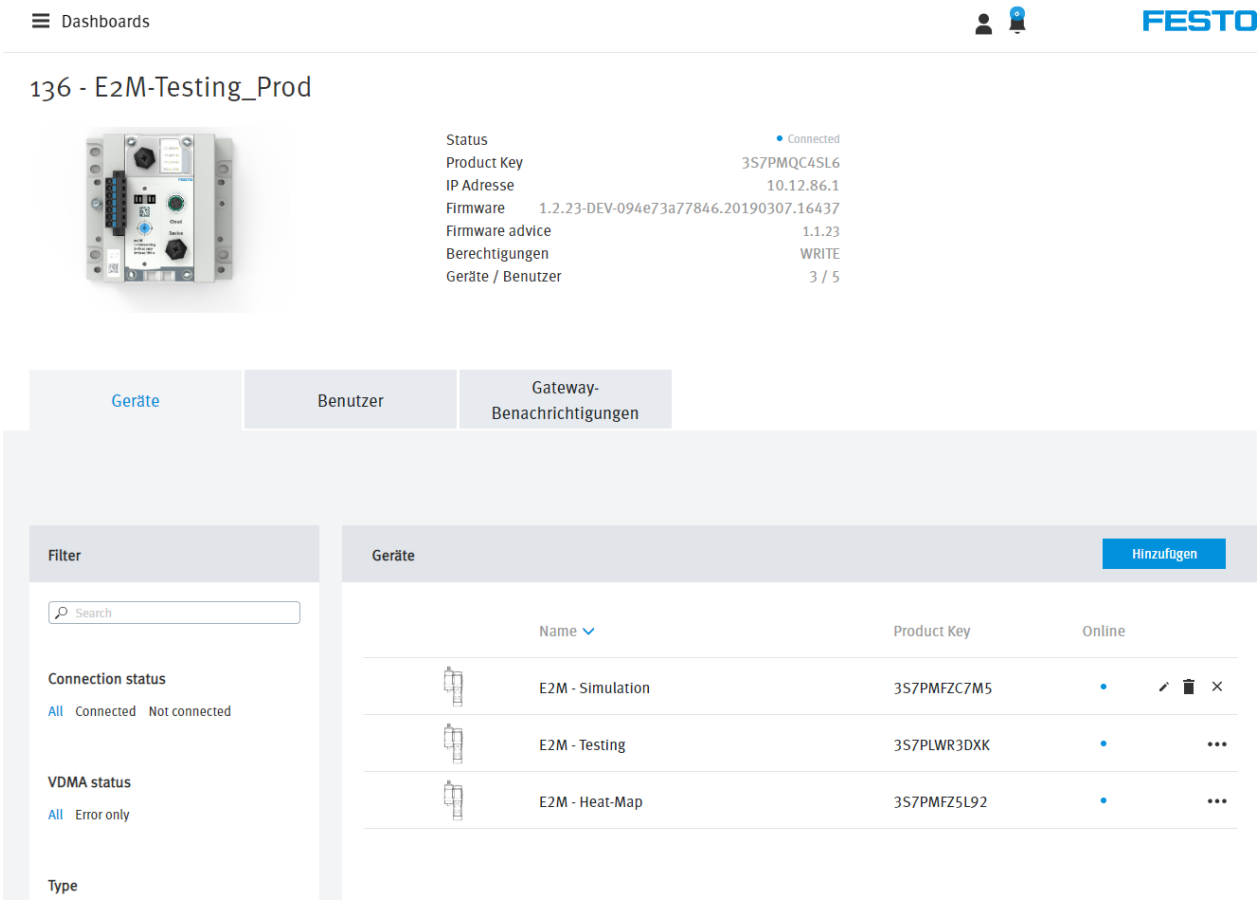




4.1.4 Device list

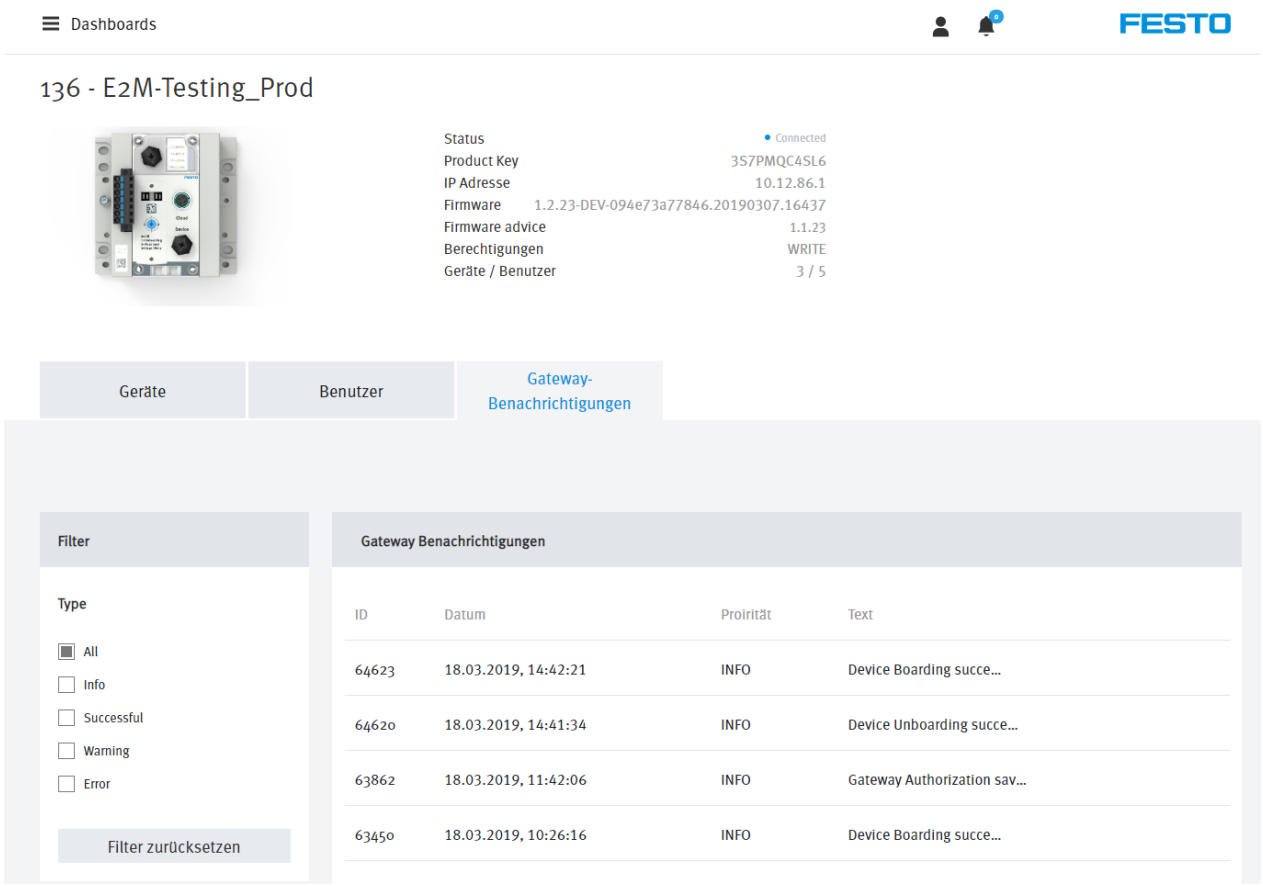
All of the devices that are boarded onto the gateway are listed in the device list. You can also board new devices via the device list. To do this, select the “Add” button. This allows you to directly access device boarding.

If a device is selected in the device list, this will take you directly to the dashboard. You can also jump to the “Device settings” page via the menu. Furthermore, a device on the gateway can also be deleted.



4.1.5 Gateway notifications

All notifications assigned to a gateway are listed under “Gateway notifications”. This is where notifications such as “Gateway connection lost”, “Gateway connection established” or “Device boarding successful” are listed. Further notifications can be found in section 9, “Notifications”.

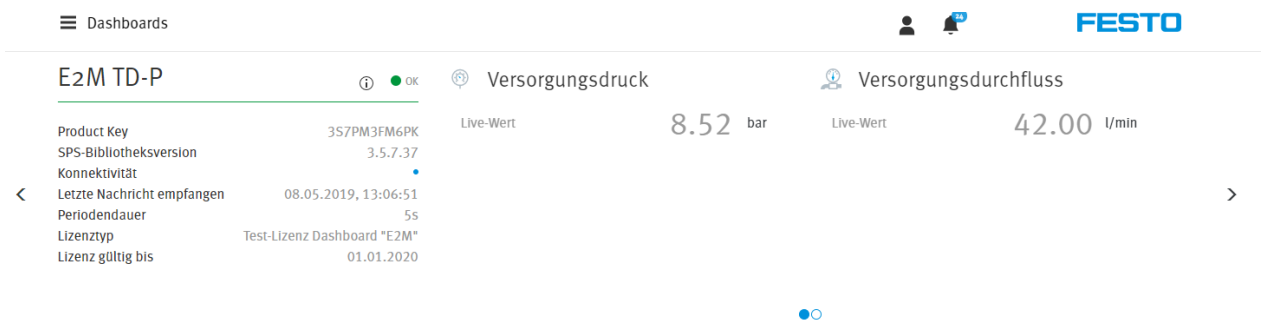


4.2 MSE6-E2M dashboard

4.2.1 Asset information

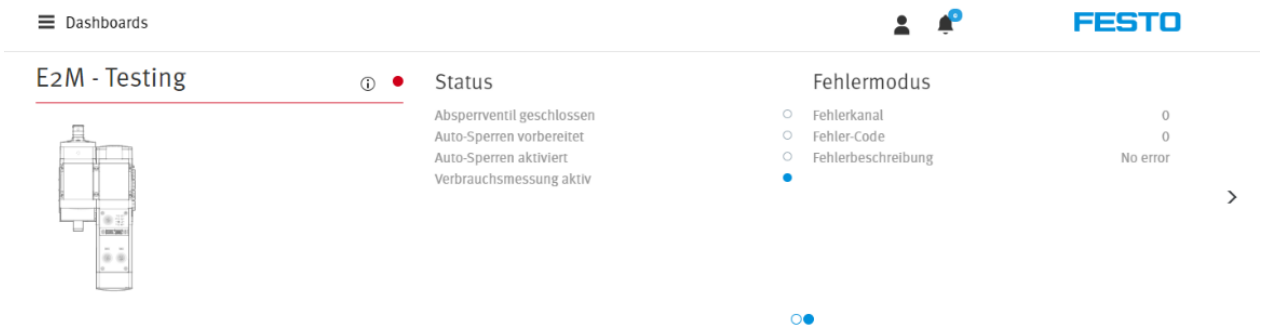
E2M asset information can be found in the top part of the dashboard or in the “Dashboard settings” page. Asset information includes information about the product key, the library version and connectivity, as well as the time period and timestamp of the last received message. The type of licence available for the dashboard and the duration of the licence term are specified as well.

Select the “Info” icon next to the dashboard name to switch to asset information.



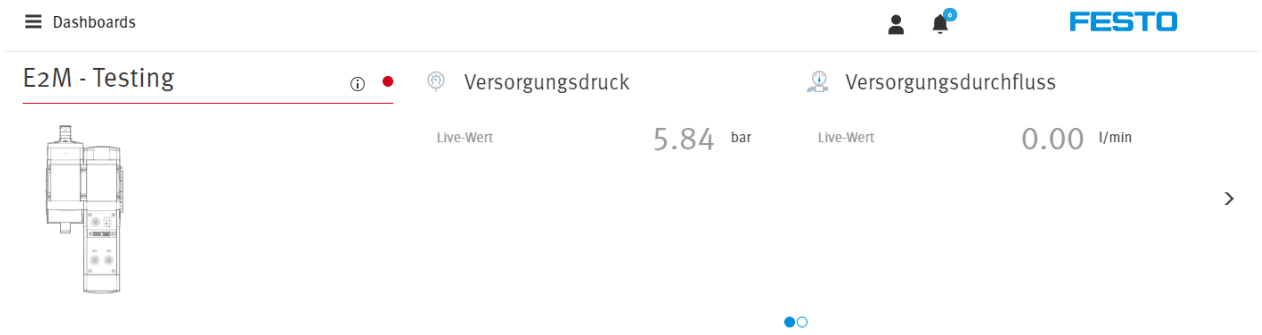
4.2.2 Error mode and status messages

The MSE6-E2M includes internal diagnosis messages. These can be sent to a higher-level controller or read out via the Festo Maintenance Tool (https://www.festo.com/net/de_de/SupportPortal/Details/348136/Document.aspx). These messages are also displayed at the dashboard. This makes it possible to obtain information about the error channel, the error code and the error description (please refer to the relevant manual for further information). There are also status messages. This allows you to quickly check whether or not the consumption measurement is active, the shut-off function is activated/deactivated and whether or not the E2M is currently in shut-off mode (“Shut-off valve closed” and “Auto shut-off activated” LEDs are on). The “Auto lock prepared” LED indicates that the value has not reached the device’s defined critical limit for automatic locking of the valve and that the E2M is performing a shut-off measurement.



4.2.3 Live data

Above the widget area, you can switch between the error mode and status messages (see section 3.2.2, “Error mode and status messages”) or live data. Live data is transmitted to the cloud once every second. These data are not saved. Pressure and flow rate at the component can be monitored visually on the E2M dashboard.



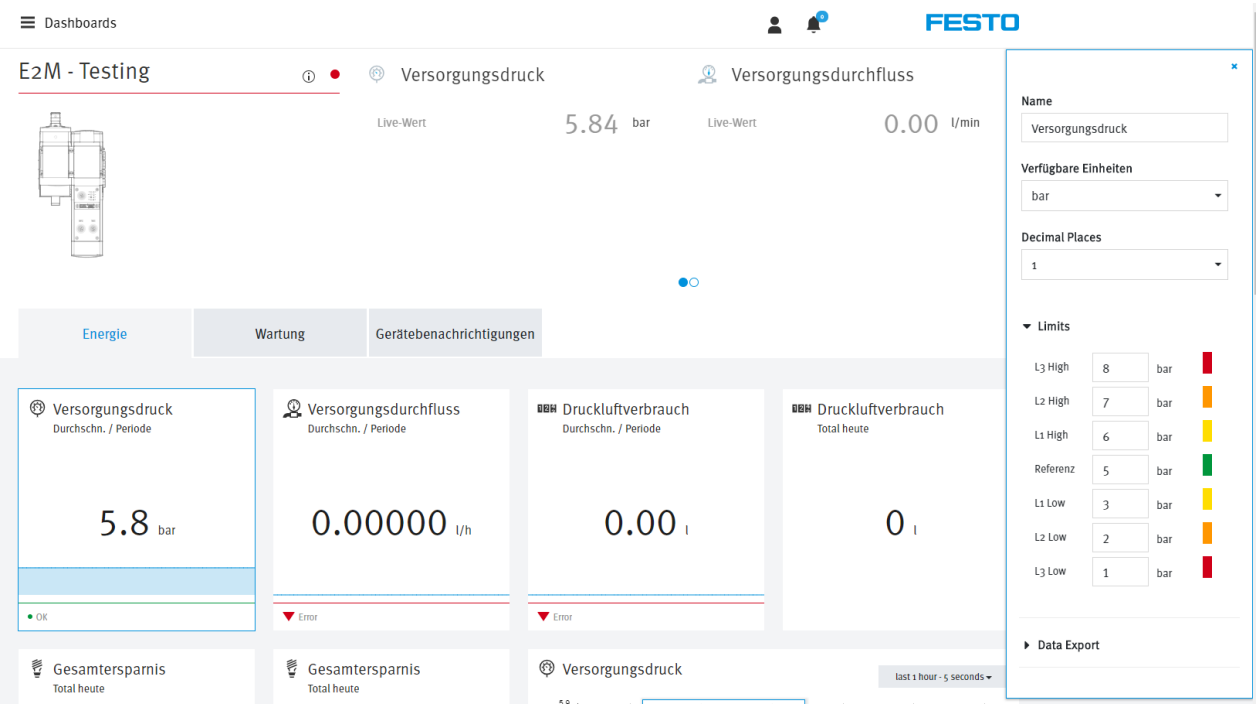
4.2.4 Energy widget area

In the energy widget area, all relevant data for the energy category are aggregated and visualised in the form of KPIs (key performance indicators) and historical data using mathematical methods. In addition, the relevant KPIs can be monitored for critical limits according to VDMA Standard Sheet 24582 (see section 10, VDMA monitoring in accordance with Standard Sheet 24582).

Cyclic KPIs

KPIs including supply pressure, flow and compressed air consumption are pre-aggregated cyclically (every 5 seconds) by the Condition Monitoring Library and sent to the cloud for visualisation. VDMA monitoring can be carried out for these KPIs in accordance with Standard Sheet 24582.

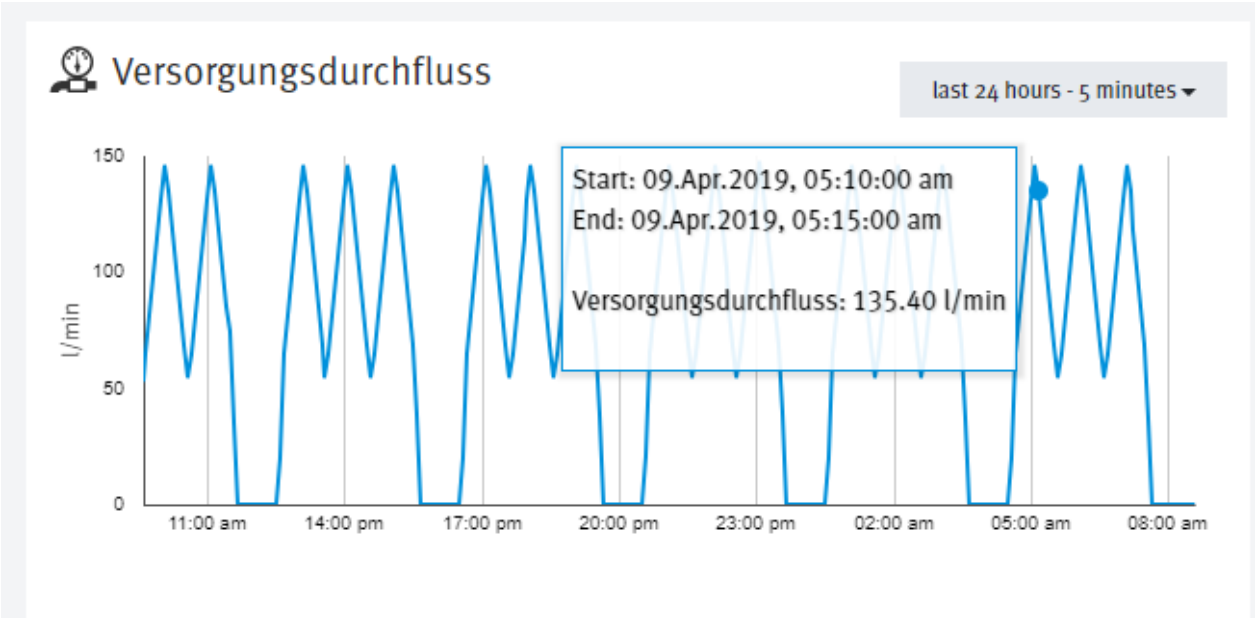
The critical limits are defined via the edit mode. To do this, enable the edit mode and select the desired widget. The limit values can then be defined under “Limits”. Refer to section 10 for more information.



A KPI with a aggregated “Daily total” is now also available for compressed air consumption. This is continuously added up over the course of the day (time zone: UTC1). Aggregation is restarted at the beginning of each day.

Historical data

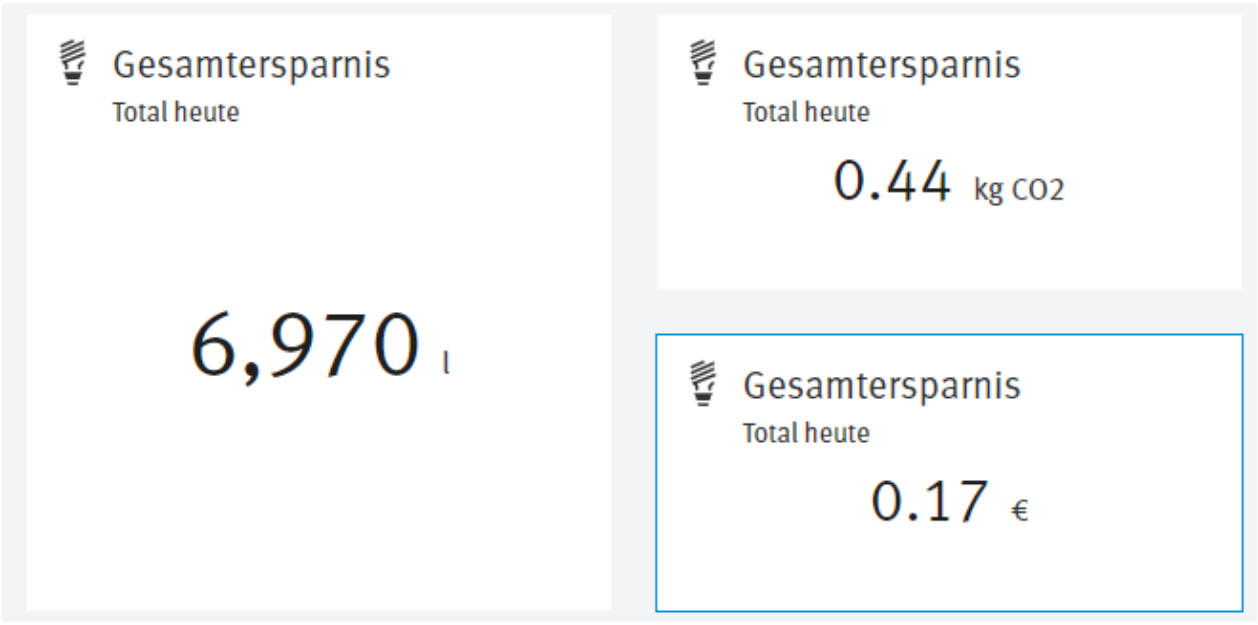
Historical data are also available for the above-mentioned widgets. These are visualised in a line chart for supply pressure and supply flow and in a bar chart for compressed air consumption and total savings. The display can be configured to show time periods ranging from the last 24 hours to the entire last year. If a data point is also selected in the charts, further information is read out such as the beginning and end of the aggregation interval, as well as the value and the selected unit of measure.



Widgets’ total savings

The widgets’ total savings are calculated in the cloud. The leakage measurements at the E2M form the basis for this calculation. The E2M is automatically switched to the shut-off state if the value does not reach the critical limit defined for the component for the specific time period. For further information, refer to the documentation for the service unit combination E2M. During this process, the E2M measures the leakage. This leakage measurement and the duration for which the E2M is shut off form the basis for the calculation of total compressed air savings. The status LEDs “Auto lock activated” and “Shut-off valve closed” can be used to check whether or not the E2M is in shut-off mode.

Furthermore, by specifying the compressed air index [Wh/Nm^3] and CO_2 emission factor [g/kWh] via the edit mode, CO_2 consumption savings can be calculated. If the energy costs for generating compressed air are known and can be specified [€/kWh], energy costs savings can be calculated.



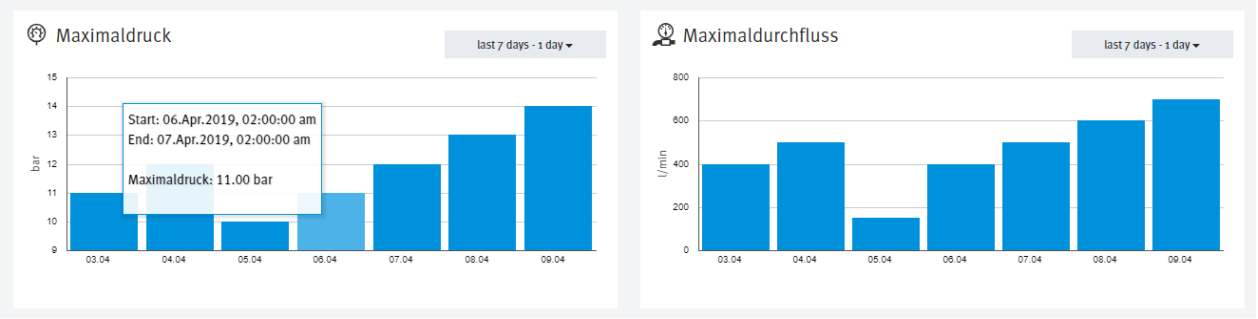
4.2.5 Widget area service

The “Service” tab contains all relevant information for planning service tasks on a machine (only with regard to compressed air). Information on maximum flow and pressure, as well as leakage within the system, is thus made available. The switching cycles of the E2M can be used to check how often the system has been shut off.

Maximum pressure and maximum flow

Maximum pressure and maximum flow are the maximum values per day that occurred at the E2M. The maximum value is determined in the condition monitoring library. The sensor system is scanned for 100 ms Switch-on peaks can also be reliably detected in this way.

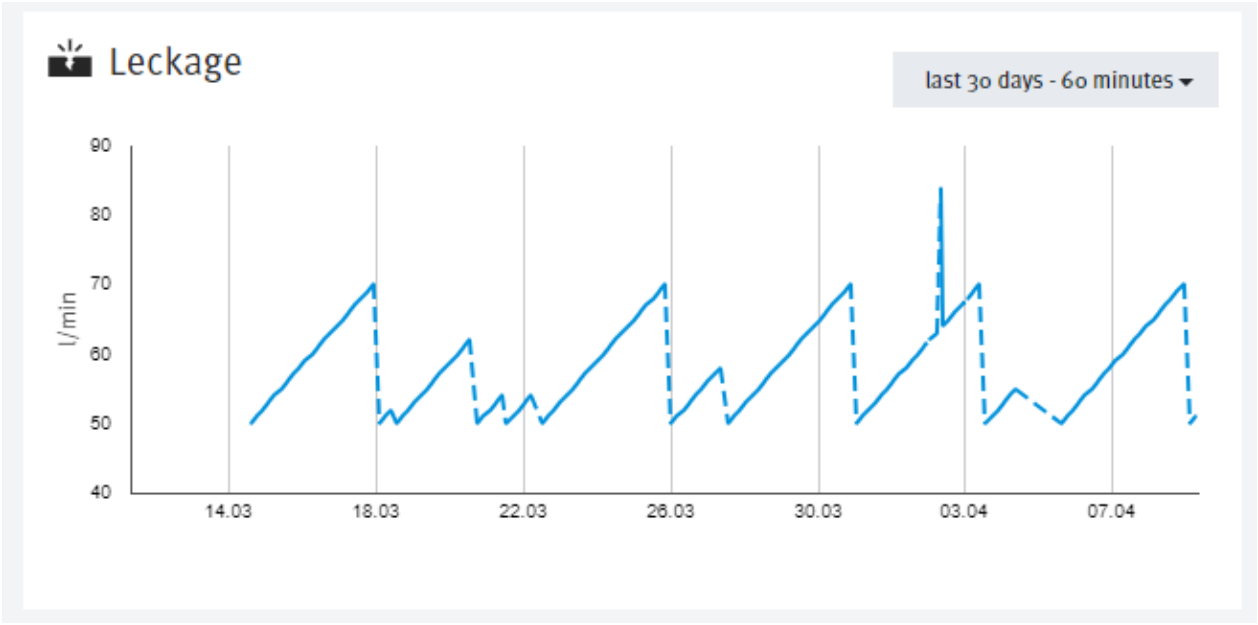
Historical data in the form of bar charts is also available for both values. Depending on the selected display interval, the global maximum value is read out.



Leakage

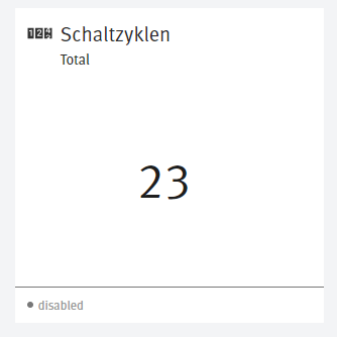
The E2M determines leakage within the system while performing shut-off measurements. If the E2M then switches to the shut-off state, the determined leakage value is transmitted to the cloud and displayed in the leakage widget. A line chart can also be used to check the leakage curve and, if drift is too great, remedial measures can be taken at an early stage.

Note: Since leakage is only determined and transmitted at certain points in time, it is only valid for these points in time. Thus the line chart only shows the individual data points at which a leakage measurement has been performed. Since no assumption can be made about leakage between measurements, the measuring points are connected with dashed lines. This is only to make visualisation easier.



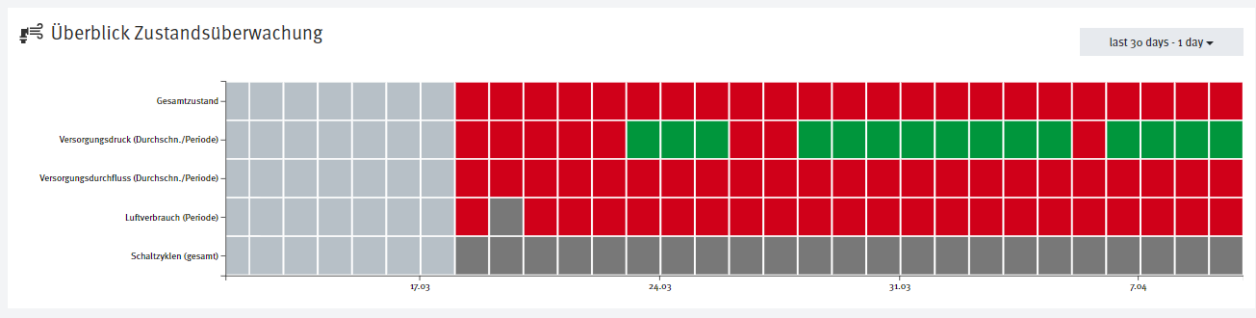
Switching cycles

The E2M has an internal switching cycle counter for the shut-off valve. This counter increases if the E2M switches to the shut-off state or if the shut-off valve is closed manually. The counter reading is displayed in the Total Switching Cycles widget. The absolute value of the switching cycle over the entire service life of the E2M is read out here. Additional critical limits can also be stored for this value. If the critical limits are exceeded, maintenance measures can be planned at an early stage.



Condition monitoring overview

Condition monitoring provides a historical progression which can be used to check when which VDMA status is created for which variable. This makes it possible to search specifically for cyclic malfunctions in the system, or for drift over time. The worst VDMA status over aggregation time is displayed.



Further information on VDMA status according to Standard Sheet 24582 can be found in section 8.

4.2.6 Device notifications

The “Device notifications” tab lists all notifications that belong to the E2M dashboard. A filter function can be used to select from amongst priorities including Info, Successful, Warning and Error. For further information concerning notifications, refer to section 9, “Notifications”.

4.2.7 Hamburger menu

The dashboard can be renamed via the hamburger menu. You can also enable or disable e-mail notifications. In addition, the edit mode can be opened to adjust the widgets. The Settings entry takes you to user management for the dashboard.

4.3 CPX-MPA dashboard

The CPX-MPA dashboard is divided into two parts. In the top part you will find the device overview, and in the lower part the widget area. The device overview contains the valve terminal configuration (digital image) and the

asset information. The widget area also contains historical data as well as cyclic data for the individual modules. The widget area is only available for analogue input and output modules, and for all modules with sensors in the pneumatic section of the CPX.

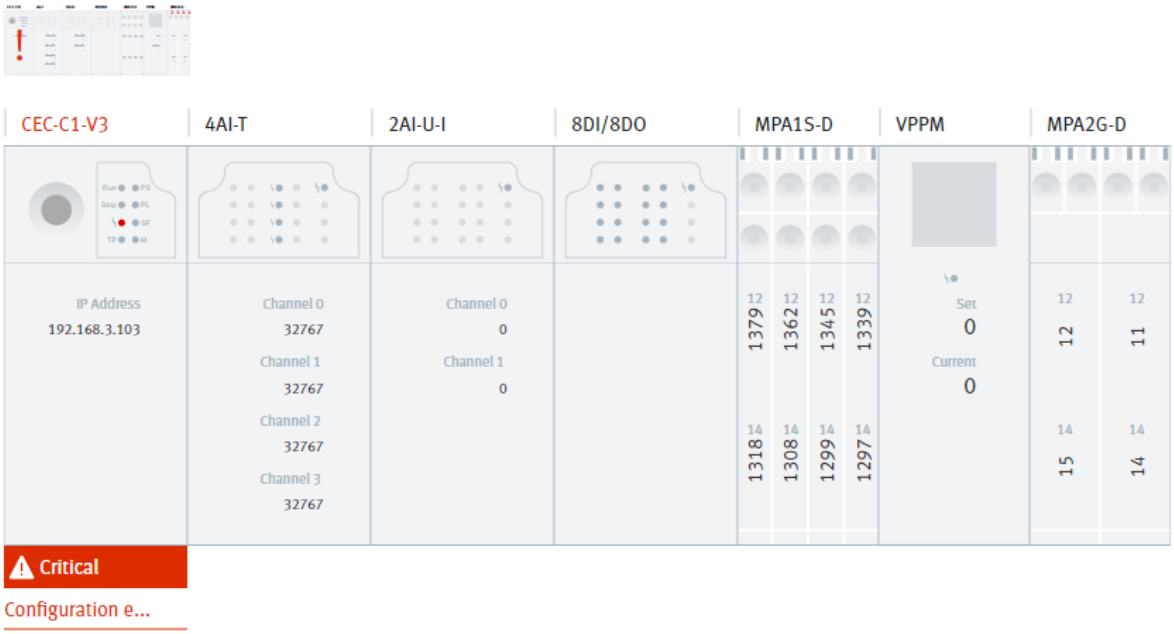
4.3.1 Device overview

The device overview shows an image of the valve terminal configuration. The image corresponds to the physical component. All information about the hardware that can be ascertained visually is displayed here. The image is supplemented with asset information such as analogue input/output, switching clearance of the valves and the actual measured value from the sensors (pressure plate, proportional pressure regulator).

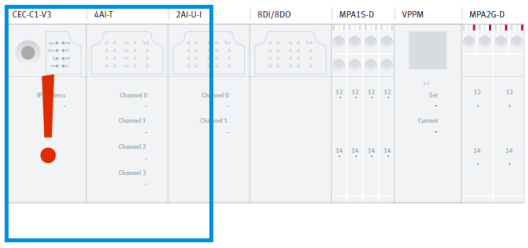
If module-specific errors occur, an error message is displayed below the corresponding module. The error messages are identical to those read out via the Festo Maintenance Tool.

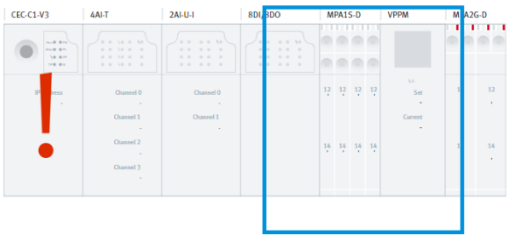
Note:

The CPX generates a diagnosis message. This accomplished via activated limit value monitoring and the stored limit values at the device. The CPX can be activated and set for diagnosis messages and limit values for individual modules via the Festo Maintenance Tool or programming environments such as CODESYS or the TIA portal.



A thumbnail view can be seen above the illustration. This displays the area of the valve terminal in which you are currently located. This is necessary if large CPX configurations are available and the display range is insufficient. This thumbnail view can also be used to move the displayed area. A red exclamation mark also identifies the module at which an error has occurred (e.g. critical limit violation, parameterisation error etc.).



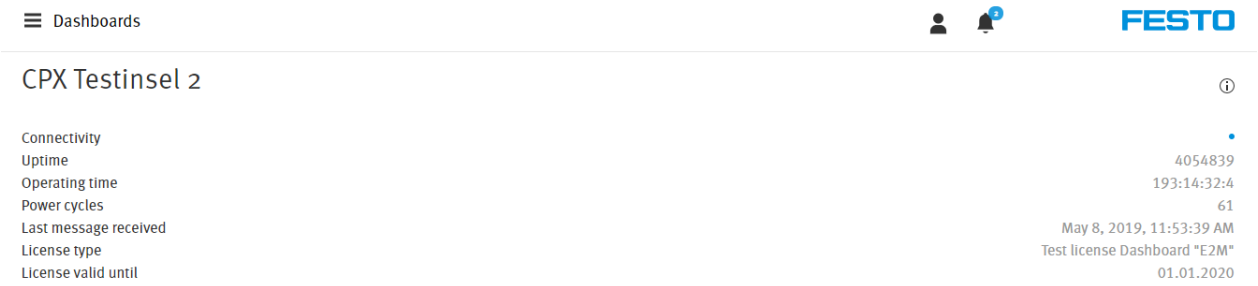


4.3.2 Asset information

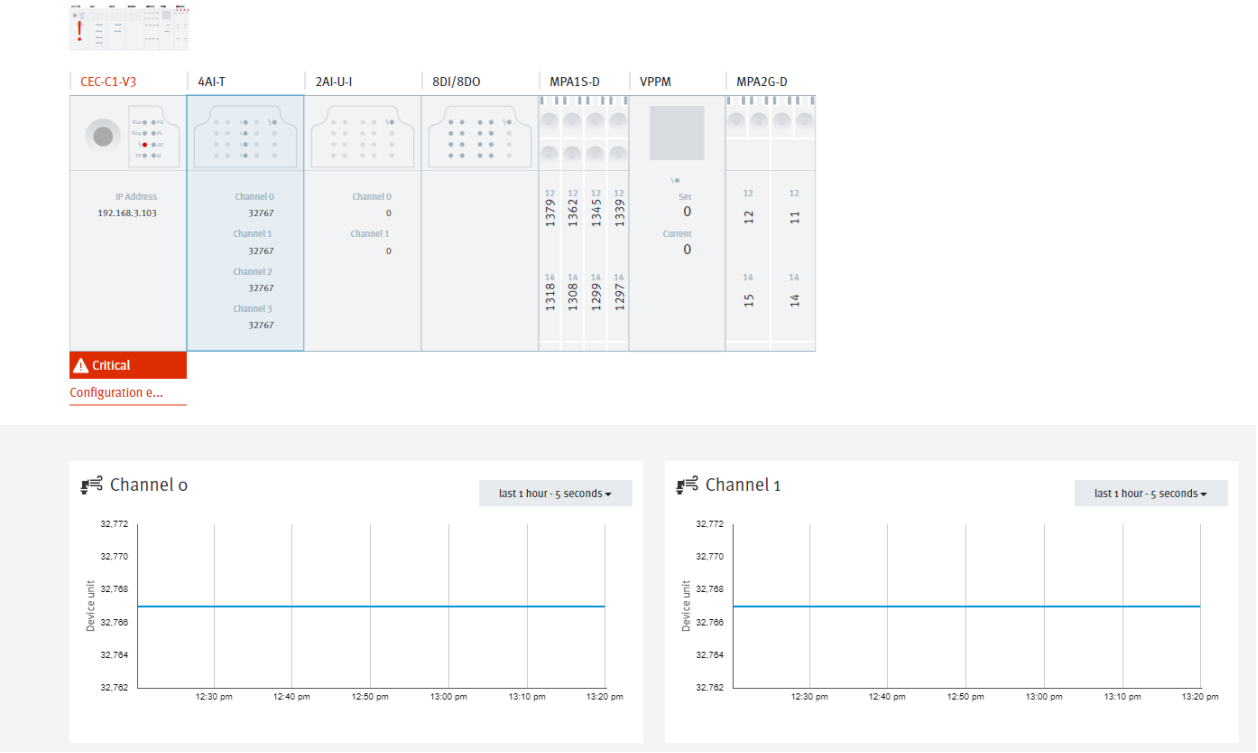
To view the asset information of a CPX Dashboard, click on the information icon in the device overview or on the “Dashboard settings” page. Asset information includes information about the product key and connectivity, as

well as the period and timestamp of the last message received. Licence duration and type of licence are also displayed.

The Runtime entry in the asset information indicates how long the CPX has been in operation since the last switch-on process. Total runtime provides information on total operating time of the CPX valve terminal over the product lifecycle. The “Power cycles” provide information on how often the CPX has been switched off and on. This information should not be mistaken for information about the runtimes of the CPX connection to the cloud.
Widget area



Module-specific widgets are also available for modules such as analogue input or output modules, pressure plates and proportional pressure regulators. Select the corresponding module in the device overview. Once this is done, the widget area opens.



In addition to the parameters summarised in the widget area, historical data is available for CSV export. The data is read out without unit of measure. The measured values displayed here are raw values and correspond to those of the unit of measure selected in the module. If the selected unit of measure is known in the hardware, the data can be interpreted clearly.

4.3.3 Module information

The widget area of the CPX Dashboard also displays the module information for each module. The meaning of the individual entries is broken down below:

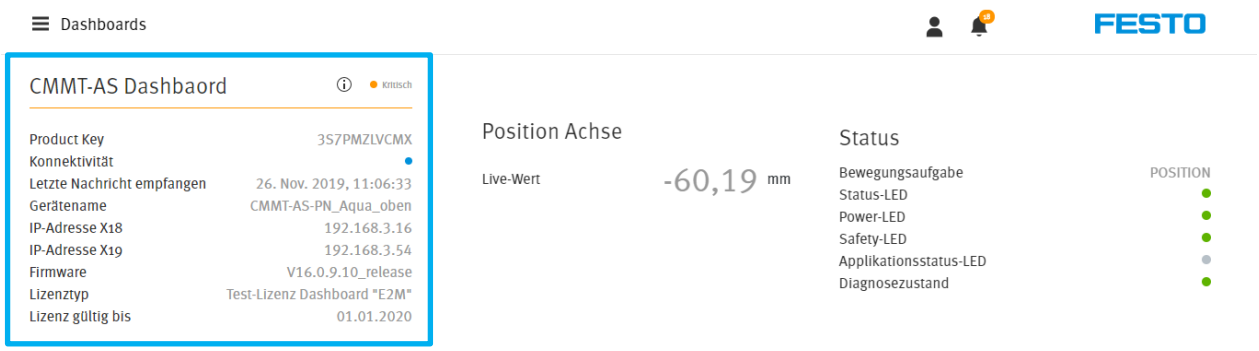
- The index, also called the module slot, indicates the position of the module in the CPX string. For example, if there is a 3, this is the fourth module in the CPX. It should be noted that counting begins with zero.
- Serial number: The serial number is used for traceability of the batch/... of the respective module.
- The IP addresses and subnet masks specify the IP addresses assigned to a bus node or a controller.
- Any revision is based on the firmware version of the CPX and the hardware used. The revision is particularly relevant if an entire CPX or an individual module has been exchanged.

4.4 CMMT-AS and CMMT-ST dashboard

4.4.1 Asset information

The asset information for the CMMT can be found in the top part of the dashboard or in the “Dashboard settings” page. Asset information includes information concerning the product key, the CMMT firmware, the IP addresses selected for the real-time Ethernet (RTE), port X19 (EtherCAT, PROFINET etc.), as well as the standard

Ethernet X18 interface, the device name in the field and information concerning the last received message. Furthermore, the type of licence available for the dashboard and the duration of the licence term are specified. The overall status of the component can also be viewed via the asset information.

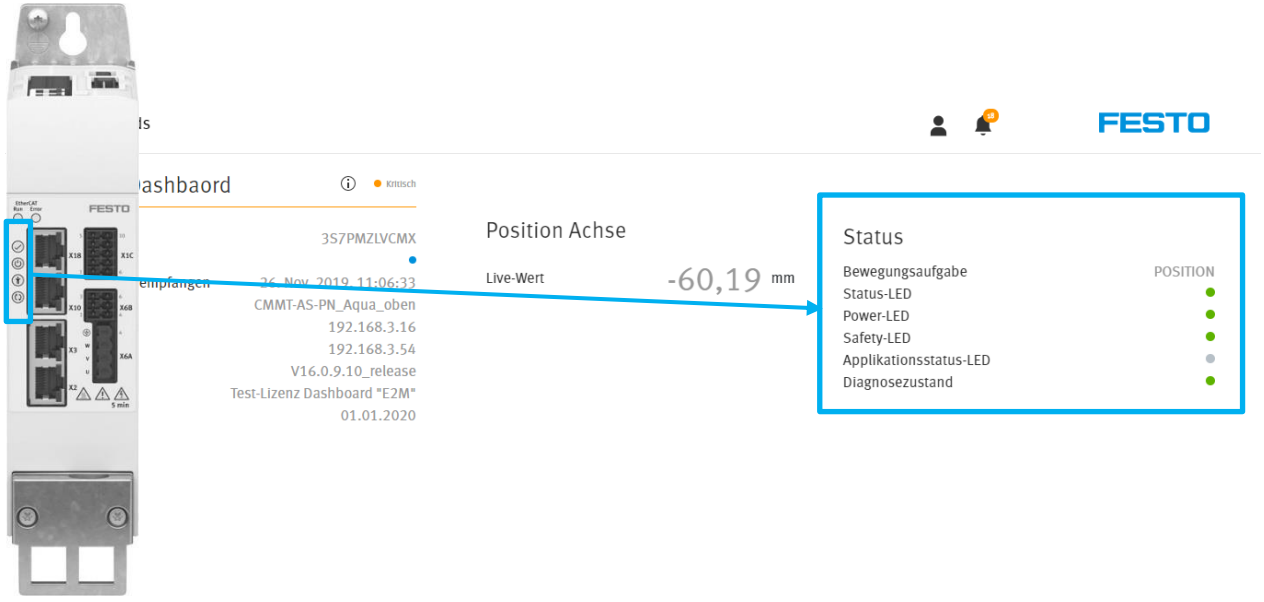


Note:

The status “LEDs” located under “Status” in the dashboard’s header influence overall aggregation of the dashboards overall status. If an error in the CMMT appears in the field, the corresponding LED turns green (OK), yellow (warning) or red (error) (see section 4.4.2, “Error mode and status messages”). Based on aggregation in accordance with VMDA Standard Sheet 24582, a corresponding overall status is ascertained for the dashboard.

4.4.2 Error mode and status messages

All relevant CMMT status messages are read out in the dashboard. They appear in the dashboard header. The status LEDs depict the status LEDs on the CMMT and are made available in the dashboard for quick viewing. Information concerning the various LED colours and blinking statuses can be found in the corresponding CMMT manuals.



The motion task makes it possible to draw conclusions about the CMMT’s current operating mode (position, torque, speed etc.). The status LED indicates the overall status at the component side of the CMMT. The power LED indicates the status of the power supply (power stage and logic voltage). The safety LED indicates the status of the safety functions. The utilised safety functions (STO, SS1, SBC etc.) are relevant when interpreting the safety LED. The diagnostic status is linked to the internal CMMT diagnosis messages. If a diagnosis message is pending in the CMMT, the LED in the dashboard is switched in accordance with its severity. The following severity levels are possible for all status LEDs in the CMMT dashboard: OK (green), warning (yellow) and error (red). Various blinking speeds are also possible.

Status LED

✓ Status-LED, Anzeige des Gerätestatus

LED	Bedeutung
 blinkt rot	Es liegt ein Fehler vor.
 blinkt gelb	Es liegt eine Warnung vor, oder der Servoantriebsregler führt gerade ein Firmware-Update durch.
 leuchtet gelb	Der Servoantriebsregler befindet sich in der Initialisierungsphase.
 blinkt grün	Der Servoantriebsregler ist bereit und die Endstufe ist ausgeschaltet (Ready).

LED	Bedeutung
 leuchtet grün	Die Endstufe und der Regler sind freigegeben.

Power LED

The power LED indicates the status of the CMMT's power supply. Amongst other things, DC link voltage status is displayed here. Limit values can be specified for DC link voltage in the CMMT. If the limit values are fallen short of or exceeded, the motor controller is switched to an error state. The LEDs on the CMMT and in the dashboard are switched accordingly.

⏻ Power-LED, Status der Spannungsversorgung

LED	Bedeutung
 blinkt gelb	Die Logikspannungs- und die AC-Versorgung sind vorhanden. Der Zwischenkreis wird geladen.
 leuchtet gelb	Die Logikspannungsversorgung ist vorhanden aber die AC-Versorgung fehlt.
 leuchtet grün	Die Logikspannungsversorgung ist vorhanden und der Zwischenkreis ist geladen.

Safety LED

Malfunctions of the safety sub-functions are detected and displayed in the functional device. The following are detected:

– Safety sub-functions requested via 1 channel (discrepancy monitoring)

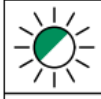
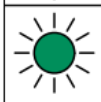
– Internal device errors that lead to pulse monitoring not being switched off or only switched off on one channel

– Errors in the brake outputs or the external wiring that result in voltage being present on the brake output even though safety sub-function SBC has been requested Malfunctions are also reported externally by the functional part via the additional communication interfaces (bus, commissioning software).

LED	Bedeutung
 blinkt rot	Fehler im Sicherheitsteil oder eine Sicherheitsbedingung ist verletzt.
 blinkt gelb	Die Sicherheits-Teilfunktion ist angefordert, aber noch nicht aktiv.
 leuch-tet gelb	Die Sicherheits-Teilfunktion ist angefordert und aktiv.
 blinkt grün	Endstufe, Bremsenausgänge und Safety-Diagnoseausgänge sind gesperrt (Safety-Parametrierung läuft).

LED	Bedeutung
 leuch-tet grün	Ready, es ist keine Sicherheits-Teilfunktion angefordert.

Application LED

LED	Bedeutung
 blinkt im Wechsel rot, gelb, grün	Identifikationssequenz aktiv (zur optischen Identifikation des Geräts in einem Netzwerk), aktivierbar über die Parametriersoftware
 blinkt gelb	reserviert für zukünftige Erweiterungen
 leuchtet gelb	
 blinkt grün	
 leuchtet grün	

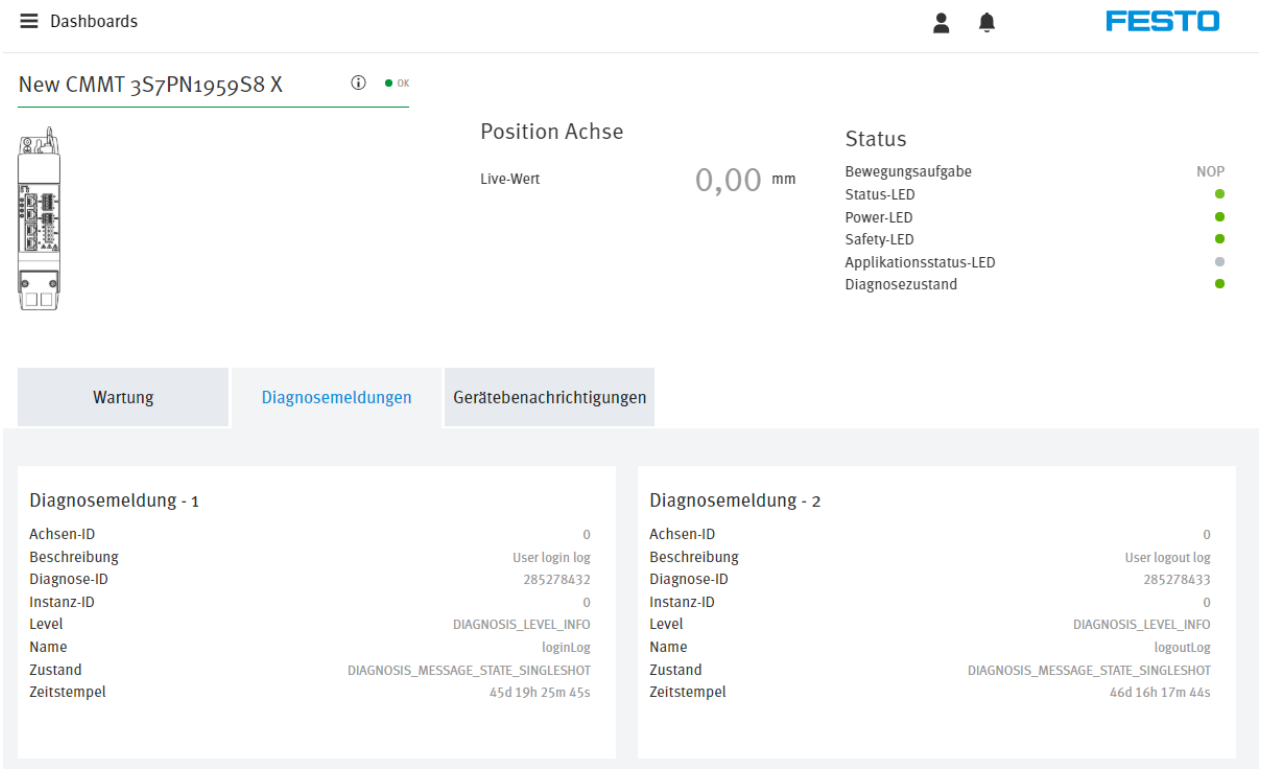
Diagnostics status

The diagnostics status of the CMMT is determined as follows:

LED colour	Brief description of the error	Error description	Corrective action	Power stage activated
Green	Info	Message with minimal degree of severity, for information only	None	Yes
Yellow	Warning	Message with medium degree of severity, indicates impending error states	None	Yes
Red	Stop category 2	Error with a high degree of severity and execution of a specified corrective action.	The drive is decelerated using a specified braking ramp immediately after the error occurs. The drive is kept in a controlled state.	Yes
Red	Stop category 1	Error with a high degree of severity and execution of a specified corrective action.	The drive is decelerated using a specified braking ramp immediately after the error occurs. The power stage is subsequently shut down.	No
Red	Stop category 1a	Error with a high degree of severity and execution of a specified corrective action.	- Deceleration with motor short-circuit and adjustable braking current - If position detection is still possible: braking is activated when speed falls below an adjustable threshold value. - If position detection is not possible (defective encoder):	No

			brake is activated immediately. - The power stage is shut down after braking delay time has expired. Applications: - Encoder error - Loss of correct commutation position	
Red	Stop category 0	Error with a high degree of severity and execution of a specified corrective action.	The power stage is shut down immediately after the error occurs.	No

In the case of the CMMT-ST, complete descriptions concerning the diagnostics status can be viewed in the “Diagnosis message” tab. Here you can see which error has resulted in which status. Further information can be found in section 5.4.4, ”Widget area diagnosis messages”.



Note:
In order to obtain detailed information concerning the diagnostic status in the case of the CMMT-AS, log in to the CMMT-AS via the Festo Automation Suite. Complete information can be viewed under “Diagnostics”.

4.4.3 Widget maintenance area

All of the KPIs required for planning maintenance-relevant tasks at the CMMT and the associated components (axis, gear unit etc.) are located in the widget maintenance area. On the one hand, absolute and instantaneous values can be monitored with the help of the limit value settings in the respective widgets. Historical data are also available as widgets or as CSV export files for the temperature and torque monitoring widgets.

Intermediate circuit voltage

TDC link voltage is continuously monitored by the device's firmware. The switching thresholds can be parameterised. The device can therefore be adapted to different supply voltages. If the selected limit values are exceeded, the power stage is switched off with the message "Overload in DC link circuit". For example, the limit values are set as follows for the CMMT-AS drives listed below:

Default switching thresholds on delivery, CMMT-AS-C2-... and CMMT-AS-C4-...:

- Undervoltage: 250 V
- Overvoltage: 400 V

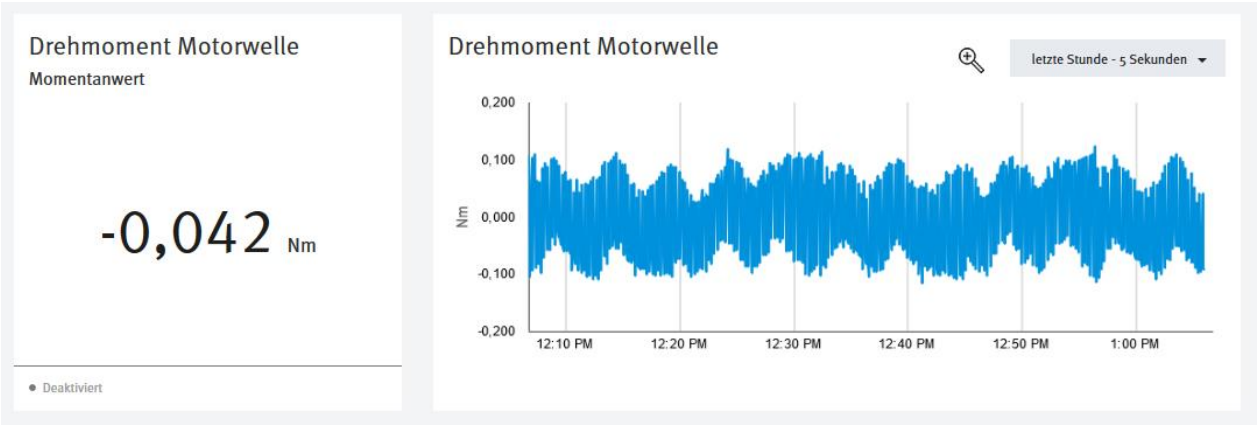
Default switching thresholds on delivery, CMMT-AS-C3-... und CMMT-AS-C5-...:

- Undervoltage: 450 V
- Overvoltage: 800 V

The cut-off voltages of the CMMT-AS and the CMMT-ST can be found in the respective data sheets available from the Support Portal.

Motor shaft torque

Torque applied to the motor shaft is displayed in the motor shaft torque widget as an instantaneous value. This value can be monitored by setting limit values. The limit values to be defined must be set in accordance with the application. A torque analysis over any desired period of time can be performed by displaying historical data.

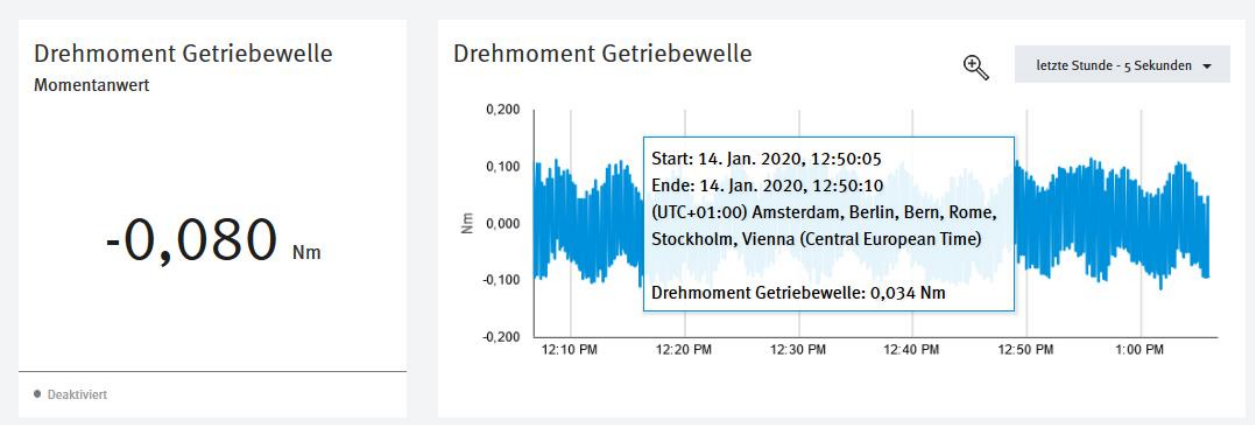


Maximum permissible torque values for the utilised motors can be found in their respective data sheets. Maximum permissible torque for the application can be found in the specifications and data sheets for the respective application.

Gear shaft torque

Torque applied to the motor shaft is displayed in the gear shaft torque widget as an instantaneous value. This value can be monitored by setting limit values. The limit values to be defined must be set in accordance with the gear unit. A torque analysis over any desired period of time can be performed by displaying historical data.

Maximum permissible torque values for the utilised gear unit can be found in its respective data sheet. Maximum permissible torque for the application can be found in the specifications and data sheets for the respective application.



Load change counter

The load change counter records how many reversals the utilised axis has completed. The value is displayed as an absolute value in the dashboard. Two limit values can be specified for the load change counter in the device. A warning is read out when the first limit value is exceeded, and an error is read out when the second limit value is exceeded. Error states can be detected at an early stage by setting limit values in the dashboard. The maximum number of load changes for the respectively connected axis can be found in the corresponding data sheet.

Runtime

CMMT runtime is read out here as an absolute value. Monitoring of the CMMT's service life is made possible by defining limit values.

Running performance

Running performance is the overall distance travelled by the connected axis. The value shown in the dashboard is an absolute value, i.e. total axis running performance. Limit values can be specified in the CMMT's parameters registry, which determine running performance as of which a warning or an error will be read out. These values can be used as reference points for defining the limit values in the dashboard. Monitoring of running performance in the dashboard can be used to generate an early warning for pending axis failure or wear.

Maximum running performance of the respectively connected axis can be found in the corresponding data sheets of the respectively utilised axis.

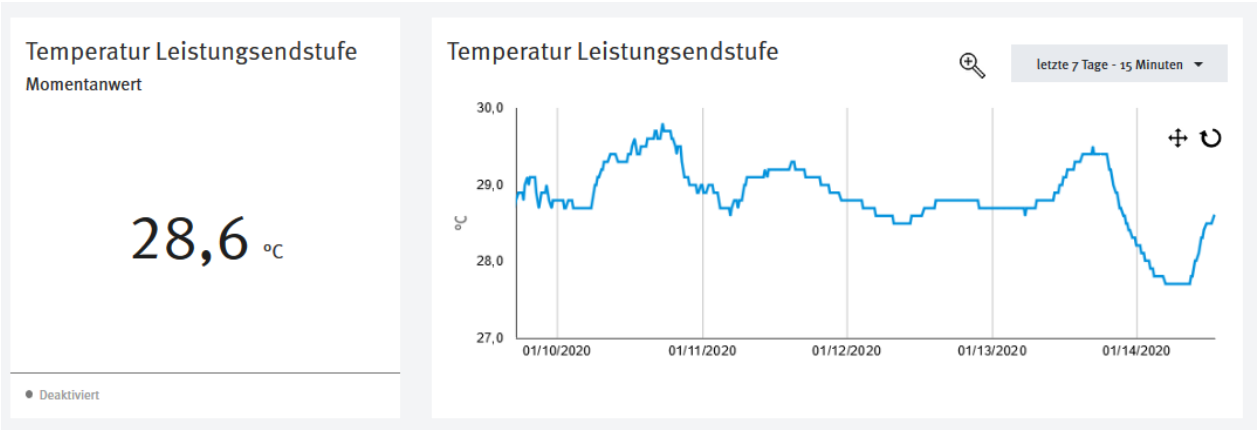
Power stage temperature

The temperature of the power stage is displayed here as an instantaneous value. The CMMT is shut down automatically in the event of excessive temperature. Early detection of temperature rises is made possible by setting limit values and displaying historical data at the dashboard.

The cut-off temperatures of the CMMT-AS and the CMMT-ST can be found in the respective data sheets available from the Support Portal.

A warning is triggered by the CMMT at temperatures of greater than 80° C in the case of the CMMT-AS-C2-11A-P3 and the CMMT-AS-C5-11A-P3, and at temperatures of greater than 100° C in the case of the CMMT-AS-C3-

11A-Pr. The cut-off temperature (error state) is, for example, greater than 85° C for the CMMT-AS-C2-11A-P3 and the CMMT-AS-C5-11A-P3 and greater than 105° C for the CMMT-AS-C3-11A-Pr.

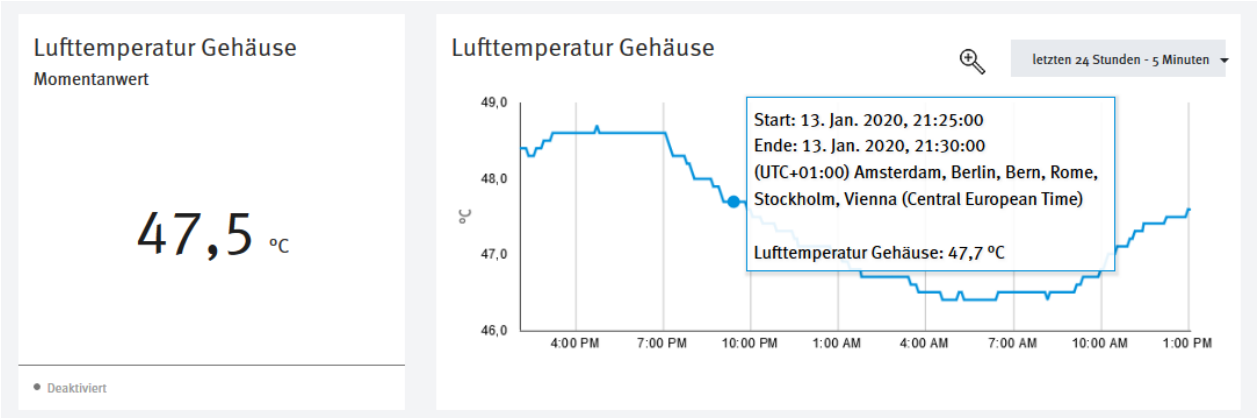


Air/housing temperature

The housing or air temperature of the CMMT is displayed here as an instantaneous value. The CMMT is shut down automatically in the event of excessive temperature. Early detection of temperature rises is made possible by setting limit values and displaying historical data in the cloud.

The cut-off temperatures of the CMMT-AS and the CMMT-ST can be found in the respective data sheets available from the Support Portal.

The cut-off temperature is, for example, greater than 75° C for the CMMT-AS-C2-11A-P3, the CMMT-AS-C5-11A-P3 and the CMMT-AS-C3-11A-Pr. A warning is triggered at temperatures of greater than 75° C for the CMMT-AS-C2-11A-P3, the CMMT-AS-C5-11A-P3 and the CMMT-AS-C3-11A-Pr.



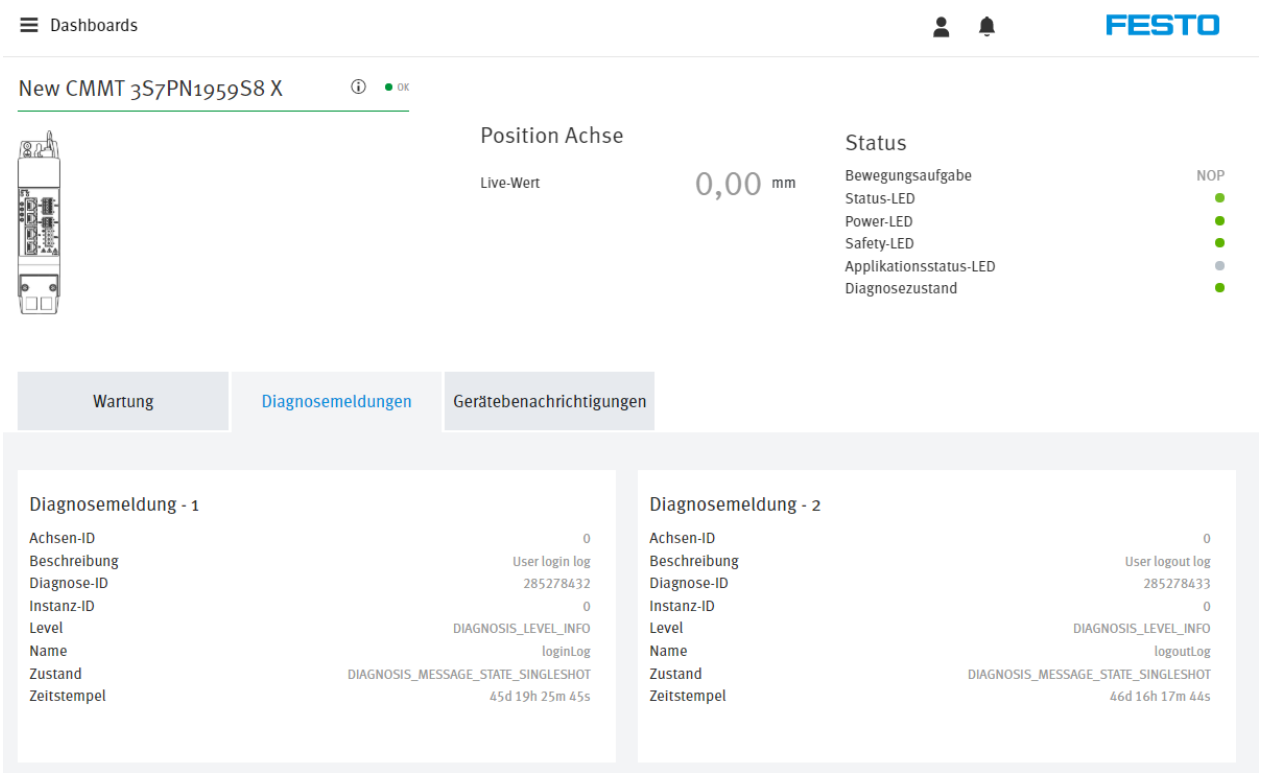
Motor temperature (CMMT-AS only)

The temperature of the connected motor is displayed here as an instantaneous value. If the motor is not equipped with an integrated temperature sensor, no value is read out. If the motor is equipped with a temperature sensor, motor temperature can be monitored in the cloud by setting limit values, thus permitting early detection of temperature rises.

The cut-off temperatures for the utilised motors can be found in their respective data sheets.

4.4.4 Widget area diagnosis messages (CMMT-ST only)

Currently pending diagnosis messages from the CMMT-ST are displayed here. If the diagnosis messages are acknowledged at the device (e.g. via FAS), they are no longer displayed in the cloud. The following section explains how the diagnosis messages have to be interpreted.



Axis ID:

The axis ID indicates whether a diagnosis message involves a system message or a drive message. The ID is broken down as follows:

- Axis ID 0: system message
- Axis ID 1: drive 1 message
-

Description:

The description shows the action, status or error in the CMMT which has triggered a diagnosis message. The description makes it possible to quickly allocate the diagnosis message and the action or cause of error in the CMMT.

Diagnostics ID:

Each CMM diagnosis message has its own unique diagnostics ID, via which all information associated with a diagnosis message can be retrieved.

Level:

The level indicates the severity of the diagnosis message. Depending on the level of the diagnostics message, the CMMT reacts correspondingly. Levels, corrective actions and how the power stage is affected (drive standstill) are listed below:

Level	Diagnostics level	Corrective action	Power stage activated
Info	Message with minimal degree of severity, for information only	None	Yes

Warning	Message with medium degree of severity, indicates impending error states	None	Yes
Stop category 2	Error with a high degree of severity and execution of a specified corrective action.	The drive is decelerated using a specified braking ramp immediately after the error occurs. The drive is kept in a controlled state.	Yes
Stop category 1	Error with a high degree of severity and execution of a specified corrective action.	The drive is decelerated using a specified braking ramp immediately after the error occurs. The power stage is subsequently shut down.	No
Stop category 1a	Error with a high degree of severity and execution of a specified corrective action.	- Deceleration with motor short-circuit and adjustable braking current - If position detection is still possible: braking is activated when speed falls below an adjustable threshold value. - If position detection is not possible (defective encoder): brake is activated immediately. - The power stage is shut down after braking delay time has expired. Applications: - Encoder error - Loss of correct commutation position	No
Stop category 0	Error with a high degree of severity and execution of a specified corrective action.	The power stage is shut down immediately after the error occurs.	No

Name:

If an action or a cause of error occurs in the CMMT, the name indicates which follow-up action has been implemented by the CMMT. For example, the name “jobignored_because_deviceControllerIsDisabled” might appear here. It can be deduced that the CMMT’s power stage has been deactivated and that no further motion tasks will be accepted.

Status:

Fundamentally, a diagnosis message can have different statuses. Various statuses are broken down below:

- DIAGNOSIS_MESSAGE_STATE_TRIGGERED: Cause of error active.
- DIAGNOSIS_MESSAGE_STATE_RESOLVED: Cause of error eliminated (e.g. DC link voltage has returned to target range), no need to acknowledge the message.
- DIAGNOSIS_MESSAGE_STATE_SINGLESHOT: Triggered by detected error, message must be acknowledged.

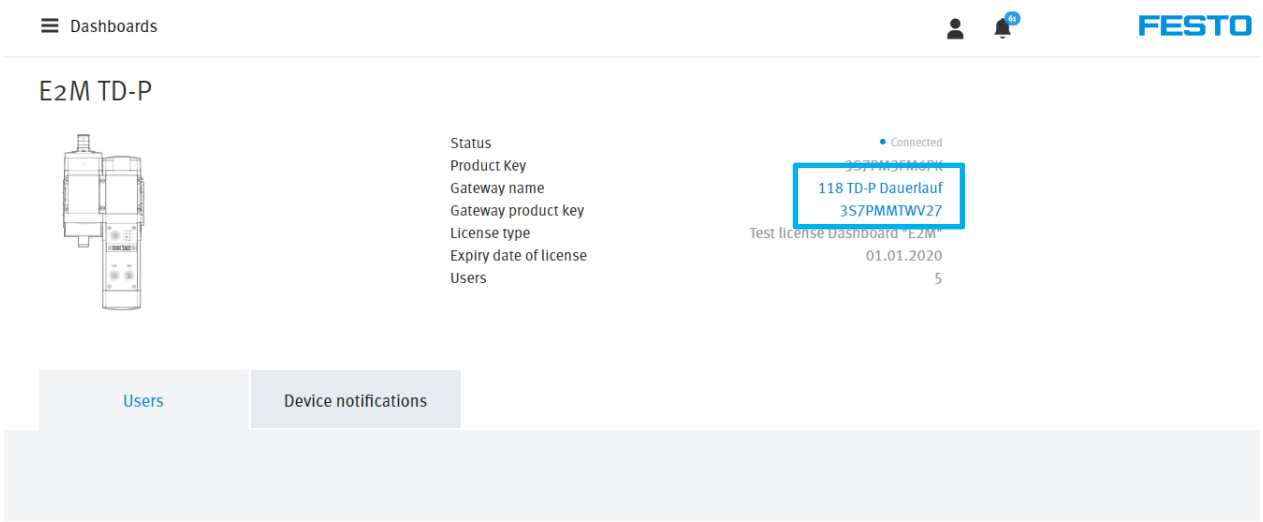
Timestamp:

The timestamp indicates the point in time at which the diagnosis message was triggered. The timestamp makes it possible to determine when an action has taken place in the CMMT or how long a status has already been pending.

4.5 Jump from the dashboard to the IoT gateway

To return from a dashboard to the gateway on which the device is boarded, you must first open the “Dashboard settings” page.

The asset information of the device in question can be found in the top part of the “Settings” page. This is where, amongst other things, the gateway name and the product key of the corresponding gateway are stored. In order to jump to the “Gateway” page, select either the gateway name with blue background or the product key. If these are not highlighted in blue, they cannot be selected and jumping is not possible. Jumping is only possible if the user has an Owner or Admin account on the gateway to which the jump is made.



5 Data retention and data export

5.1 General remarks on data retention

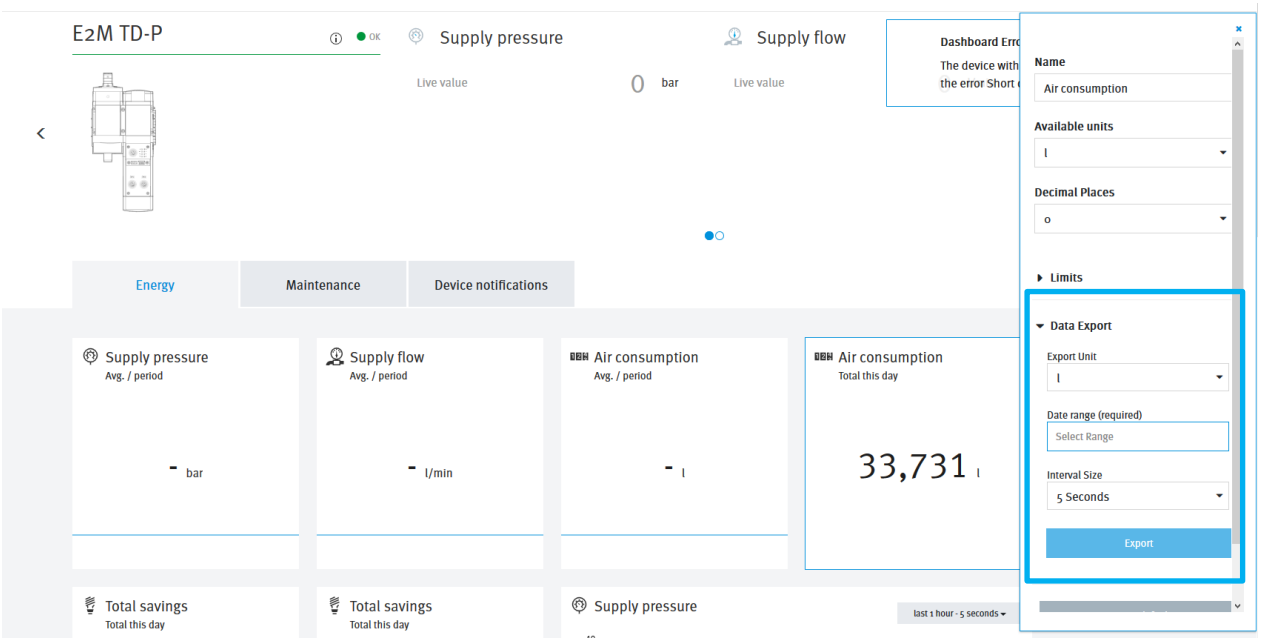
Periodic data transmitted via the gateway are stored in the cloud. Data for the visualisation of processes and trends are made available in this way. The data are stored for one year, after which old data is successively overwritten with new data (“ring buffer”).

5.2 Data export

Furthermore, data can also be exported as a comma-separated file (.csv). You select the interval and the period:

1. Click on “Enable editing mode” in the menu.
2. Select the widget you want to export.
3. Select the desired period (up to one year).
4. Select the required aggregation level (mean value generation ranging from 5 seconds to 24 hours is possible).
5. Finish the export procedure by selecting “Export”.

The CSV export is sent to the e-mail address for the Festo account that has been stored. Transmission of e-mails is independent of the settings for e-mail notifications in the dashboard. To fully complete CSV export, select “Open” in the e-mail that has been received. This will trigger a download.



6 User roles and rights management

The Festo Dashboards application has various user roles:

- Owner
- Admin
- Editor
- Viewer

The user who boards a gateway or a device for the first time is the “Owner” of the gateway device. The Owner must also authorise other users to access a gateway or device. If an administrator has access to a device or gateway, he can add additional users to the corresponding dashboards.

6.1 Overview of rights management

Rights management determines with which role a user can execute which actions in the dashboards. Rights management for the gateway and the devices is broken down according to the various user roles in the following table.

	Gateway					
Role	Delete gateway	Call up gateway overview page	Change gateway settings	Board devices on the gateway	Execute firmware update	Force off-boarding
Owner	x	x	x	x	x	x
Admin		x	x	x	x	
Editor						
Viewer						

	Device						
Role	Delete device	Call up device overview page	Change device settings	Set critical limits	Download a CSV	Force off-boarding	View device dashboard
Owner	x	x	x	x	x	x	x
Admin		x	x	x	x		x
Editor				x	x		x
Viewer							x

The following table shows who can authorise new users with which user roles for a gateway or a component, or delete users.

Role	Admin user role	Editor user role	Viewer user role
Owner	x	x	x
Admin	x	x	x
Editor			
Viewer			

6.2 User management

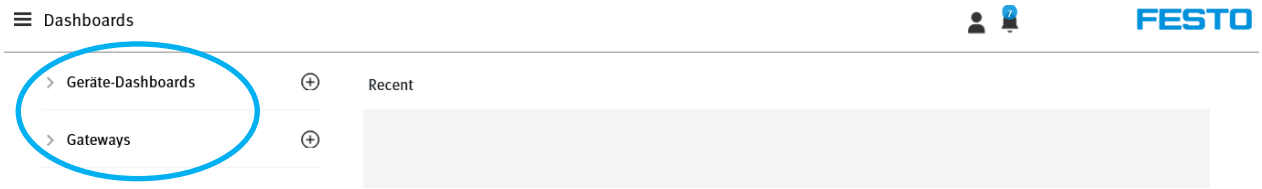
All users who are authorised to access a gateway or dashboard are listed in user management. In addition, the authorisation level of the user is displayed. Users can be created and deleted, and their authorisation levels can be changed in user management. However, this necessitates Admin or Owner rights for the gateway or dashboard. The user rights for each gateway or dashboard can thus be assigned individually according to the “Rights management” table.

6.2.1 Creating a new user

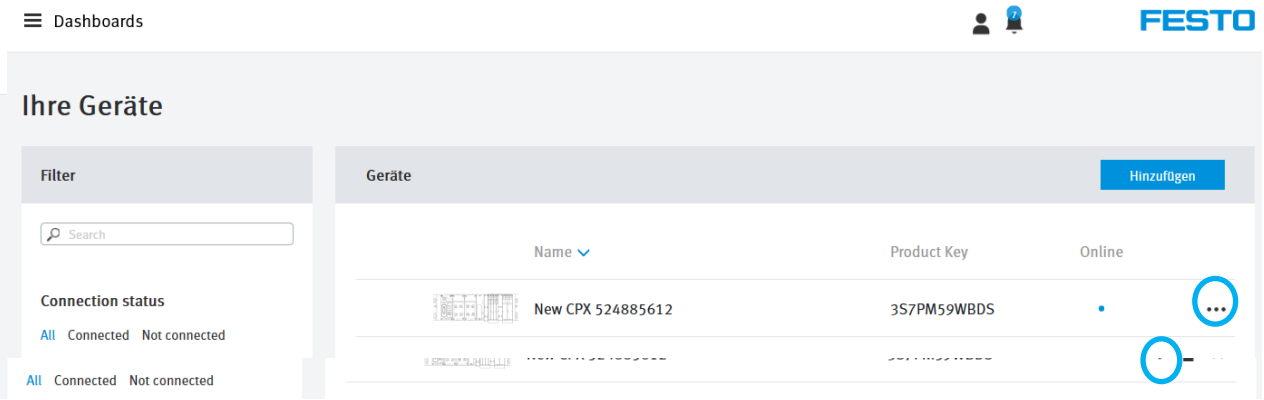
New users can be individually created and assigned a role for each gateway and dashboard. The procedure is the same for each type of dashboard and for each gateway. Access to a dashboard can be granted for any valid e-mail address.

Note:
Users who do not have a Festo shop account can be also invited. However, these users must register on the Festo homepage before they can access a dashboard. Once this is done, they are granted access to the relevant dashboard. Invited users also receive an e-mail notification. This contains a link to the dashboard to which they have been granted access.

In order to create a new user, use the “Dashboards” menu to go to the desired category, i.e. “Device Dashboard” or “Gateway”.

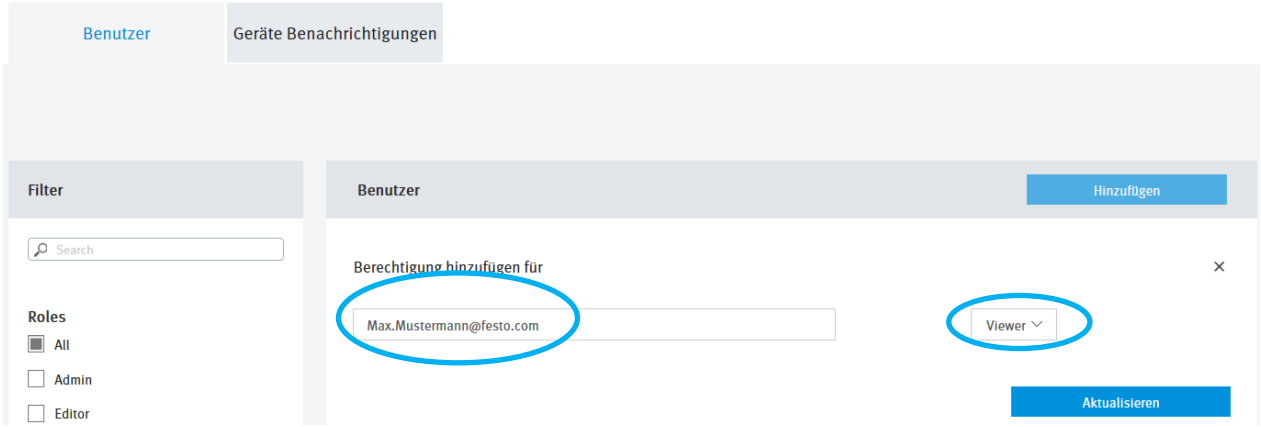


Then click on the 3 dots for the dashboard or gateway for which you want to create a new user.



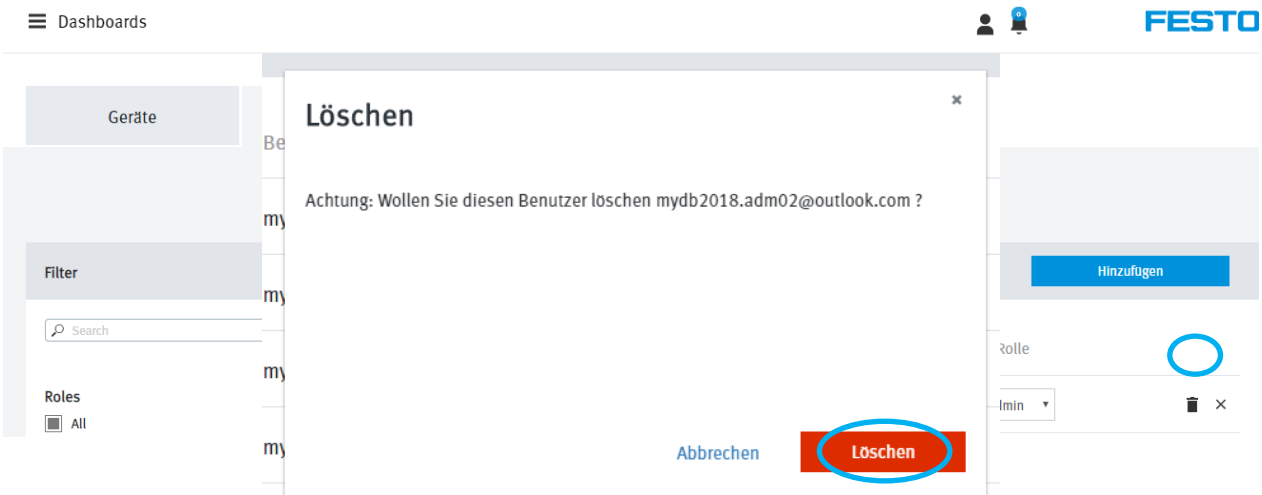
Then click on the pencil icon.

Click on the “Add” button to create a new user. This is where you can enter the relevant e-mail address and the user’s authorisation level. The authorisation level is assigned via the drop-down menu next to the input field for the e-mail address. Click on the “Update” button to finish creating the user. Note: If a valid e-mail address is not entered (syntax is checked), creation of the user cannot be completed.



6.2.2 Deleting a user

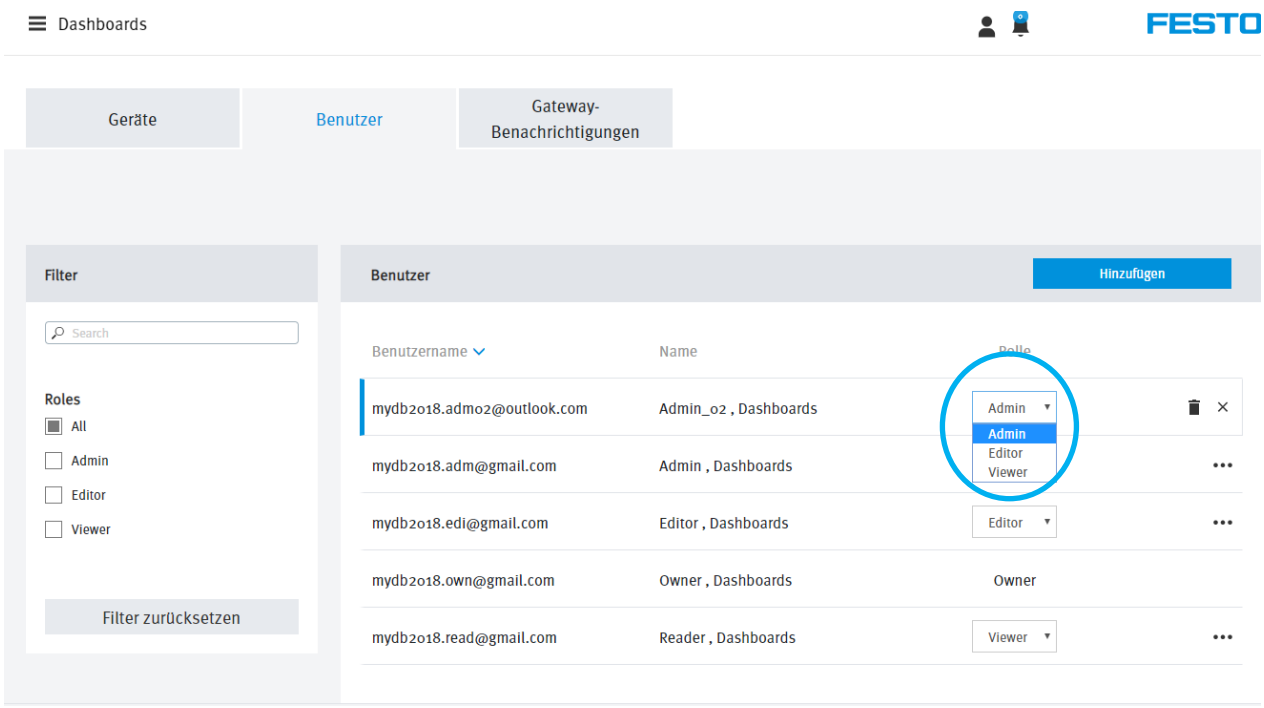
In order to delete a user, open user management for the dashboard or gateway. User management is then accessed from the “User” tab. All users authorised for the dashboard or gateway are listed here. To delete a user, open the menu at the corresponding user entry and click on the “rubbish bin” icon. This function is only available for users with Owner or Admin authorisation.



Then click on the “Delete” button in the delete window.

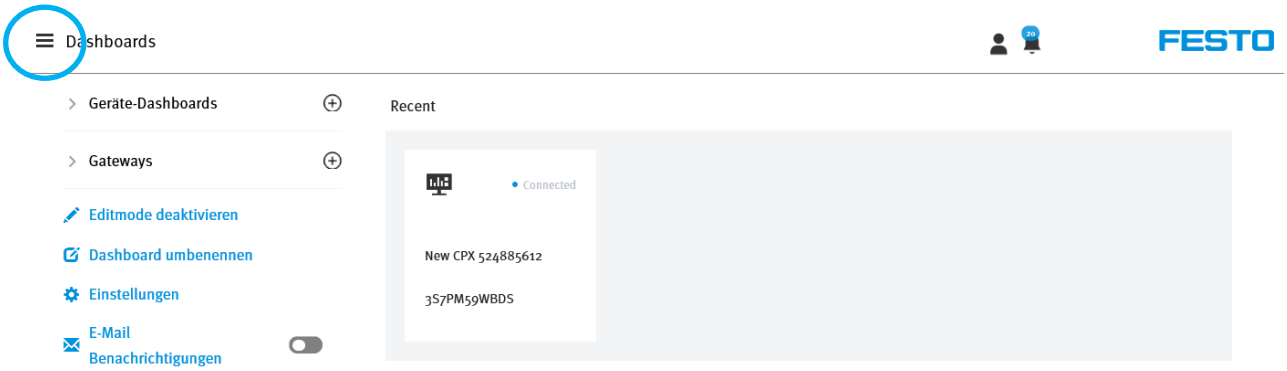
6.2.3 Changing user rights

In order to change the rights of a user, open the drop-down menu in the “Role” tab. You can assign the Admin, Editor or Reviewer role to a user here. Note: The rights of the “Owner user” cannot be changed. To change the Owner of a gateway, the gateway must be deleted and then re-boarded with another user.



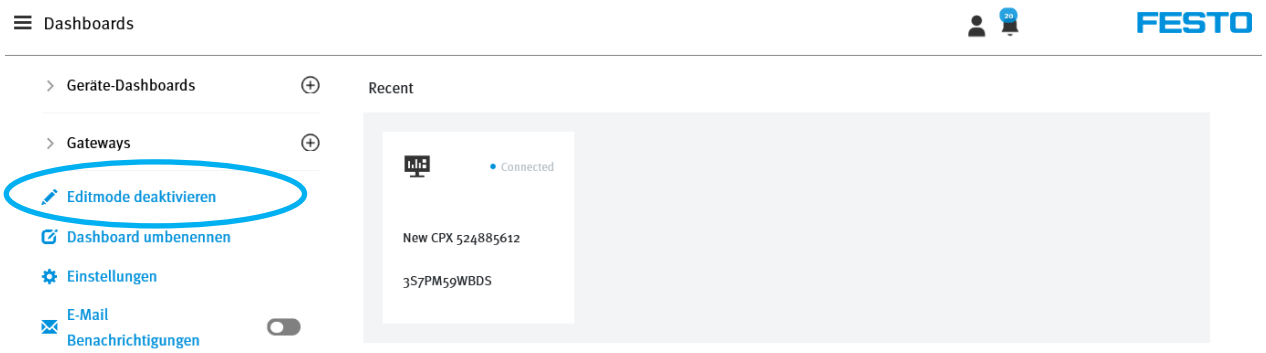
7 Dashboard settings

In order to access the dashboard settings, you must first open a dashboard page. Then click on the hamburger menu (see figure). Further options can be found under the “Dashboards” menu item. Depending on your user role, this is where you can enable/disable the editing mode, rename the dashboard, switch to settings and enable/disable e-mail notifications. It is important to note that these settings must always be entered for each dashboard. In this view you can also see the “Recent” function to the right of the navigation bar.

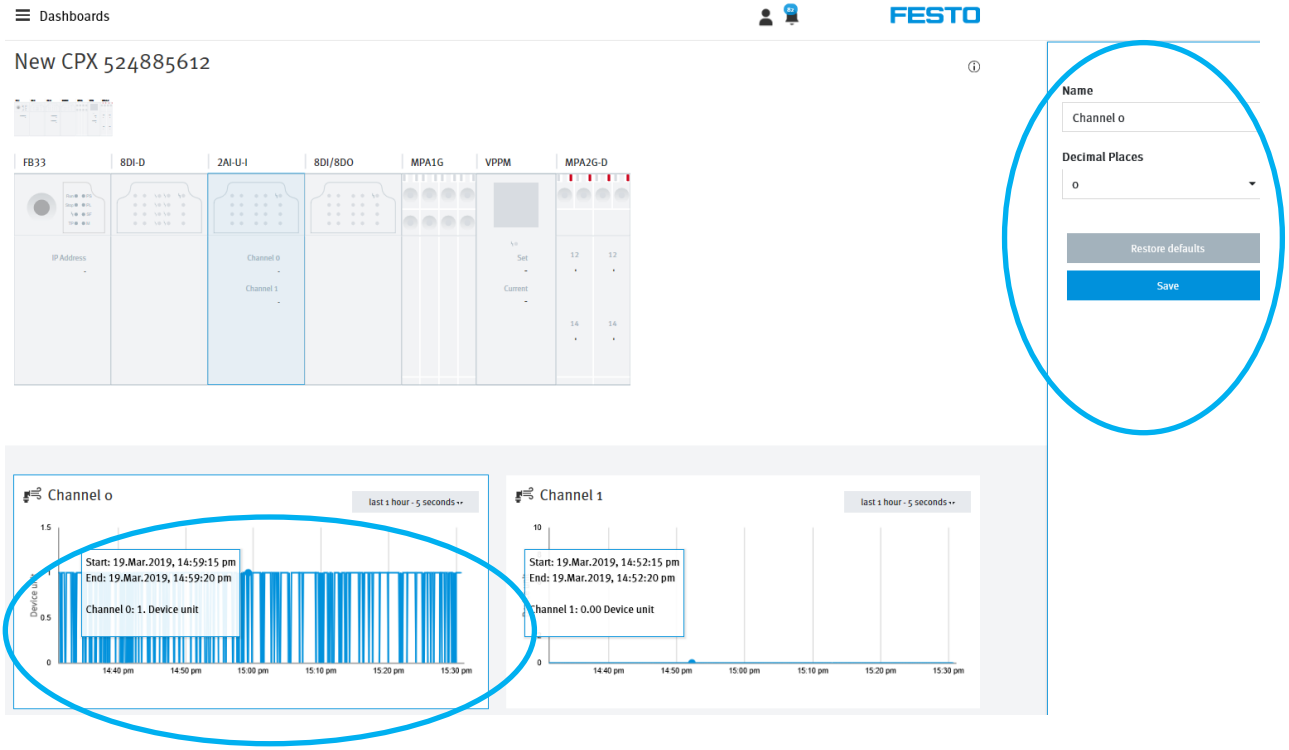


7.1 Enabling/disabling the editing mode

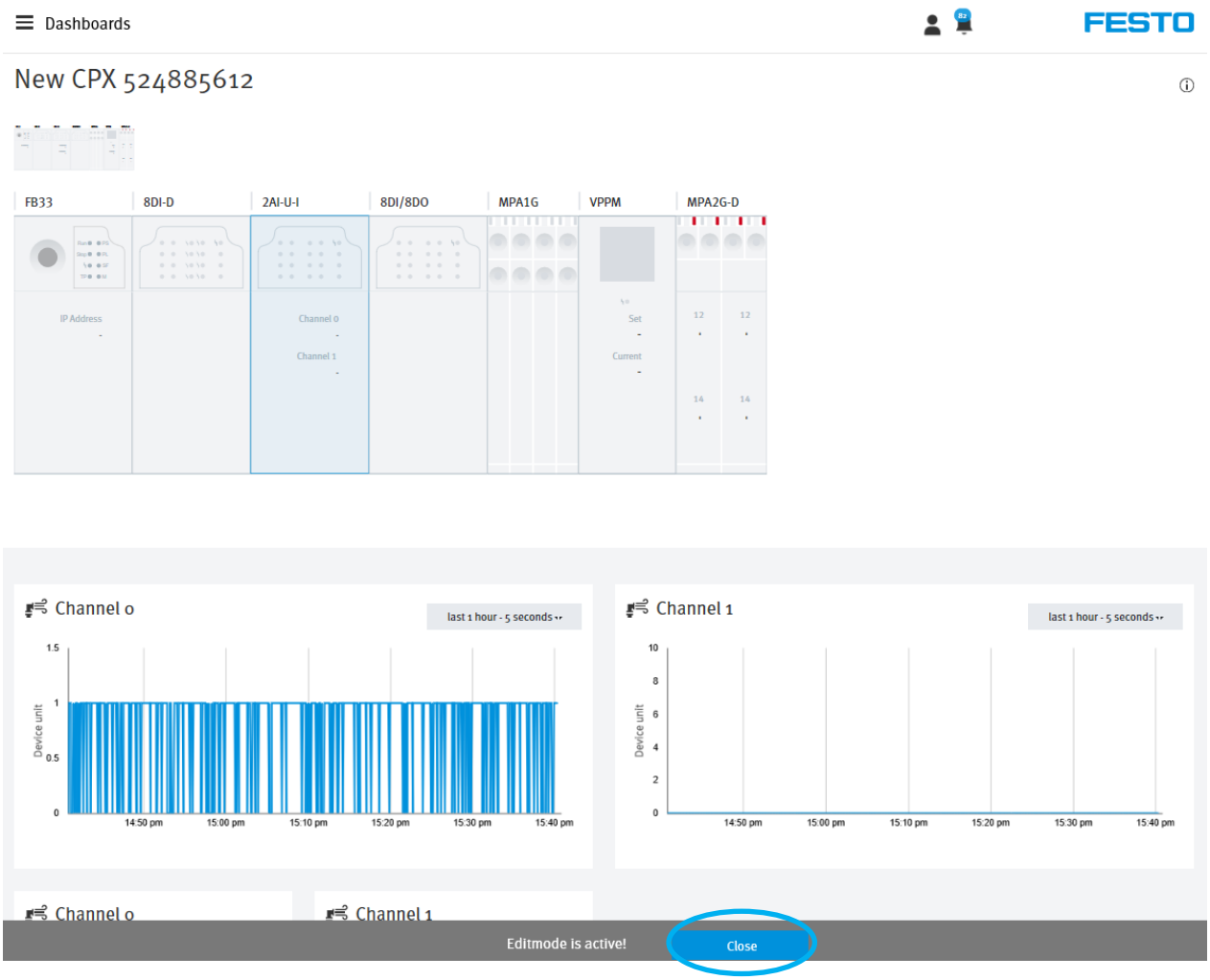
You can enable or disable the editing mode via the dashboard settings in the “Dashboards” menu.



After enabling the widget, simply click on the appropriate widget (see screenshot, bottom left). An input field opens on the right-hand side. Here you can edit the relevant parameters of the widgets.

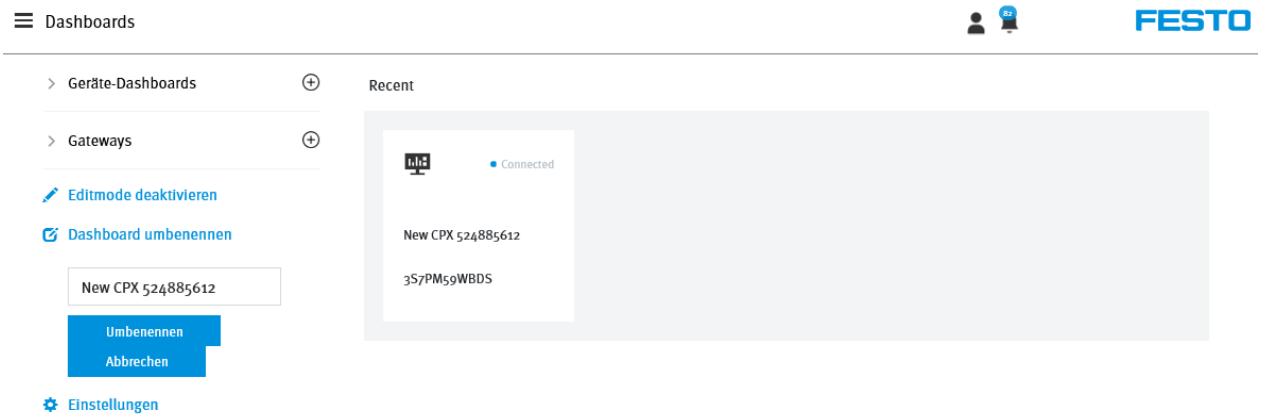


To disable the edit function again, simply click on the “Close” button in the bar at the bottom.



7.2 Renaming a dashboard

The dashboard can be renamed in the “Dashboard” menu by clicking on “Rename dashboard”. It is important to note that the name must be changed separately for each dashboard.



7.3 Settings

The “Dashboard settings” page or the “Gateway settings” page can be accessed via the “Settings” menu item. Notifications, asset information and user management can be viewed here.

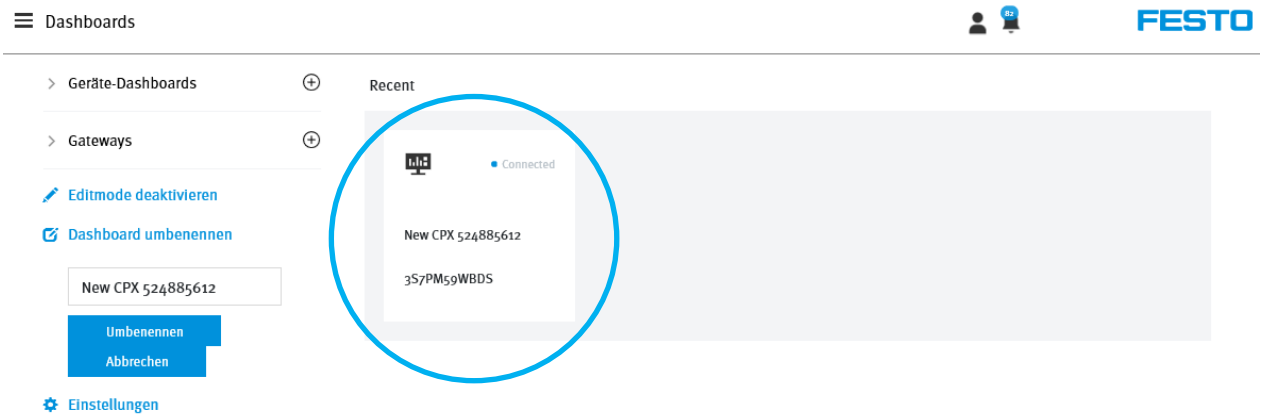
7.4 E-mail notifications

E-mail distribution can be switched on or off for each dashboard under the “E-mail notifications” menu item. This setting must be made for each dashboard and is user-dependent. Push notifications and logbook entries are not affected by this setting. E-mail notifications do not have to be enabled for CSV exports.

Please refer to section 9, “Notifications”, to find out which notifications are sent by e-mail.

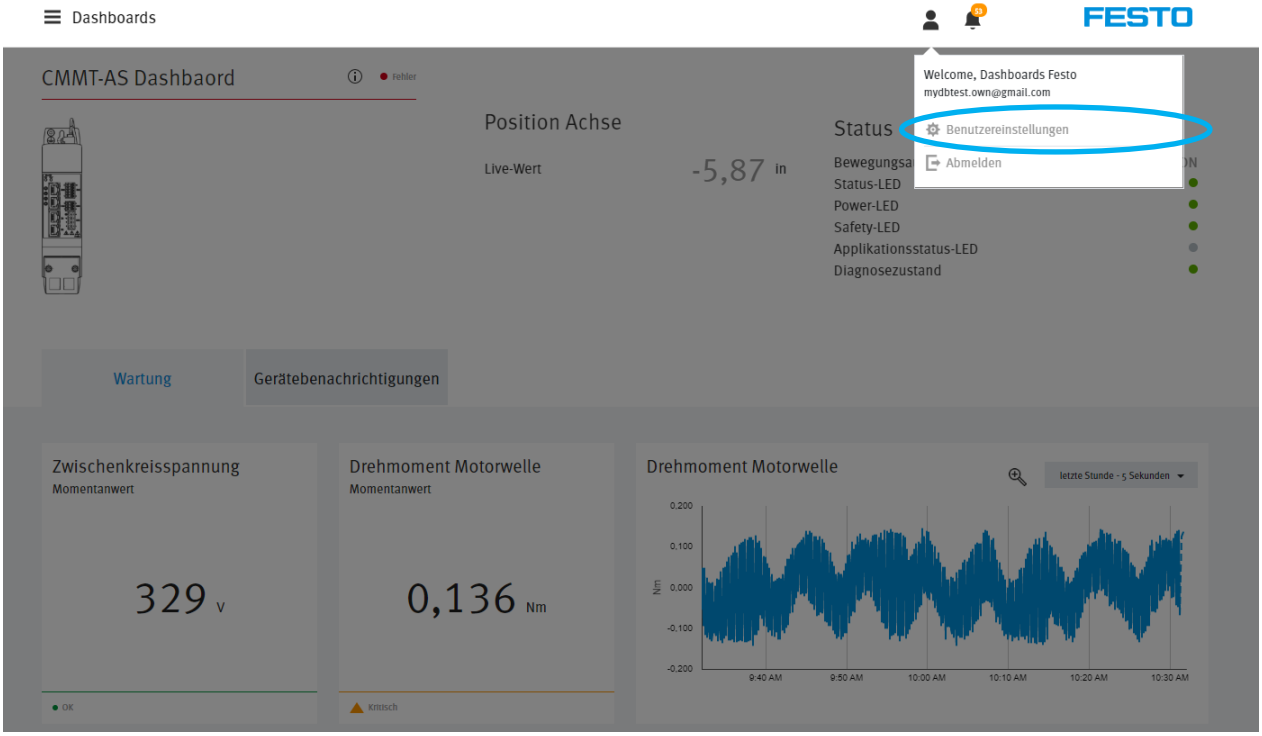
7.5 Last viewed

The three most recently visited dashboards are displayed after clicking on the hamburger menu.



8 Global user settings

Click on the user symbol to the left of the “notification bell” in order to access the user settings. Then select “User settings”.



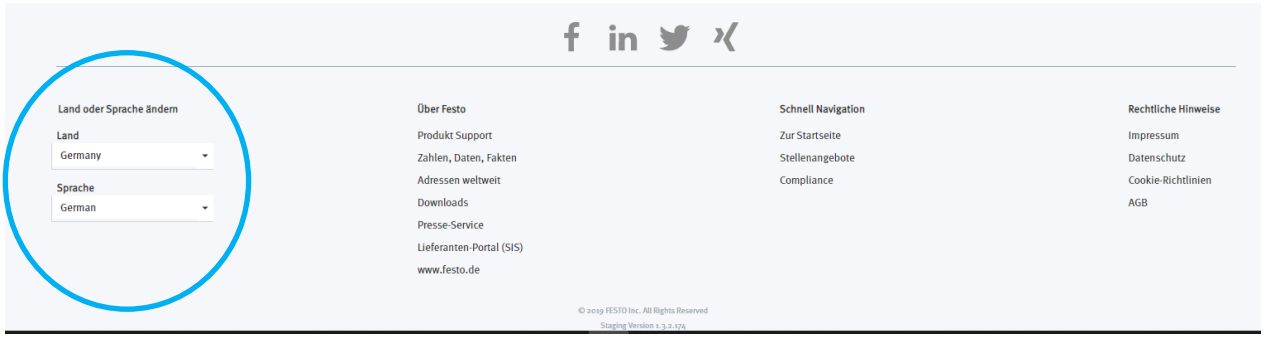
The following settings can be entered here:

- Country selection
- Language setting
- Time zone
- Point and comma separator

Note: When a country is chosen, the associated time zone is selected automatically. If the automatically selected time zone is not desired, it can be changed manually with the help of the time zone setting.

Entered user settings apply to the respective user only. They apply to all dashboards as well.

Note: Settings entered to the footer are only valid temporarily. When the dashboard is reloaded, language and country are set once again to the selections entered in the user settings.



9 Licence management

A dashboard licence enables use of a dashboard for a Festo device connected via the gateway. Up to 99 users can be created for each dashboard. Users are people who have access to the dashboard. Restricting user rights and roles ensures the required level of data security.

You can purchase a licence for the desired dashboard in the Festo App World.

www.festo.com/appworld

The purchase of dashboard licences is processed as a subscription. The amount due is invoiced at the beginning of the licence period. Subsequently, the contract term and the associated licence period are automatically extended by a further licence period.

9.1 Licence extension

A monthly licence can be upgraded to an annual licence at any time. The range of services provided by the new licence package is available immediately after an upgrade and you receive a debit note for the new invoice amount. The new 12-month contract term begins when the larger licence package has been purchased. Claims to the services of the previous licence package are lost when the upgrade is purchased. Outstanding payment obligations from the previous licence agreement expire after an upgrade.

9.2 Terminating the licence

A subscription can be terminated at any time and termination becomes effective at the end of the licence period.

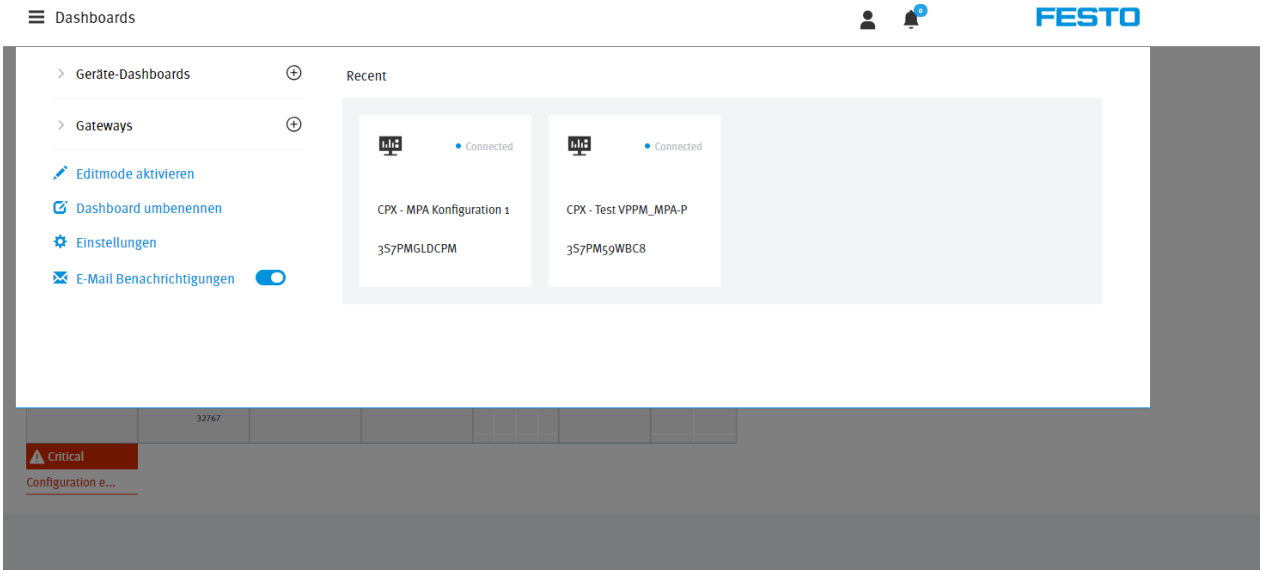
10 Notifications

Notifications are intended to provide quick information about all relevant events on the component side, as well as at the gateway. Push notifications, logbook entries e-mail transmission are provided. Transmission of e-mails can be switched on and off individually depending on the user and the dashboard. This does not affect the CSV export, as this is always sent by e-mail.

10.1 E-mail dispatch settings

E-mail can be enabled or disabled for each dashboard on a per-user basis. To do this, select the hamburger menu in the relevant dashboard. This setting can only be made on the “Dashboard” page and not on the “Settings” page. If you are on the “Settings” page, you can switch to the “Dashboard” page using the “Show dashboard” button.

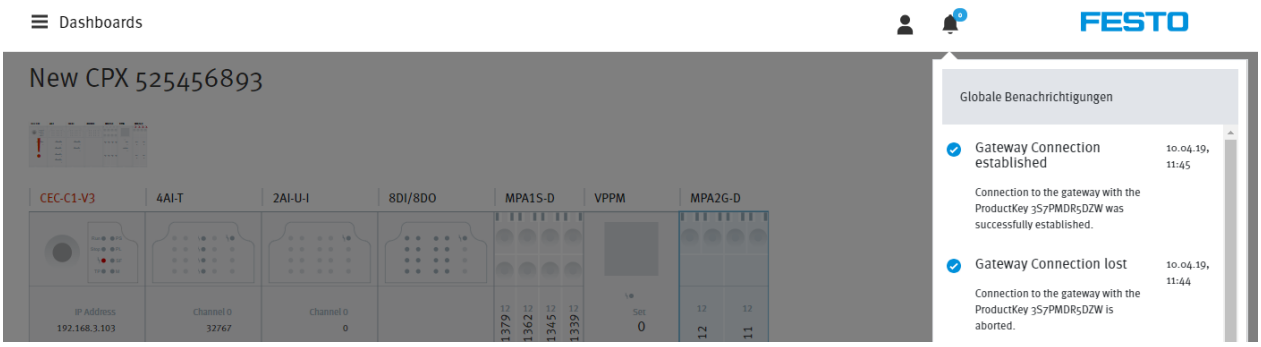
The “E-mail notifications” tab indicates whether e-mail is enabled (Blue) or disabled (Grey). Selecting the tab switches back and forth between enabled and disabled.



10.2 Push notifications

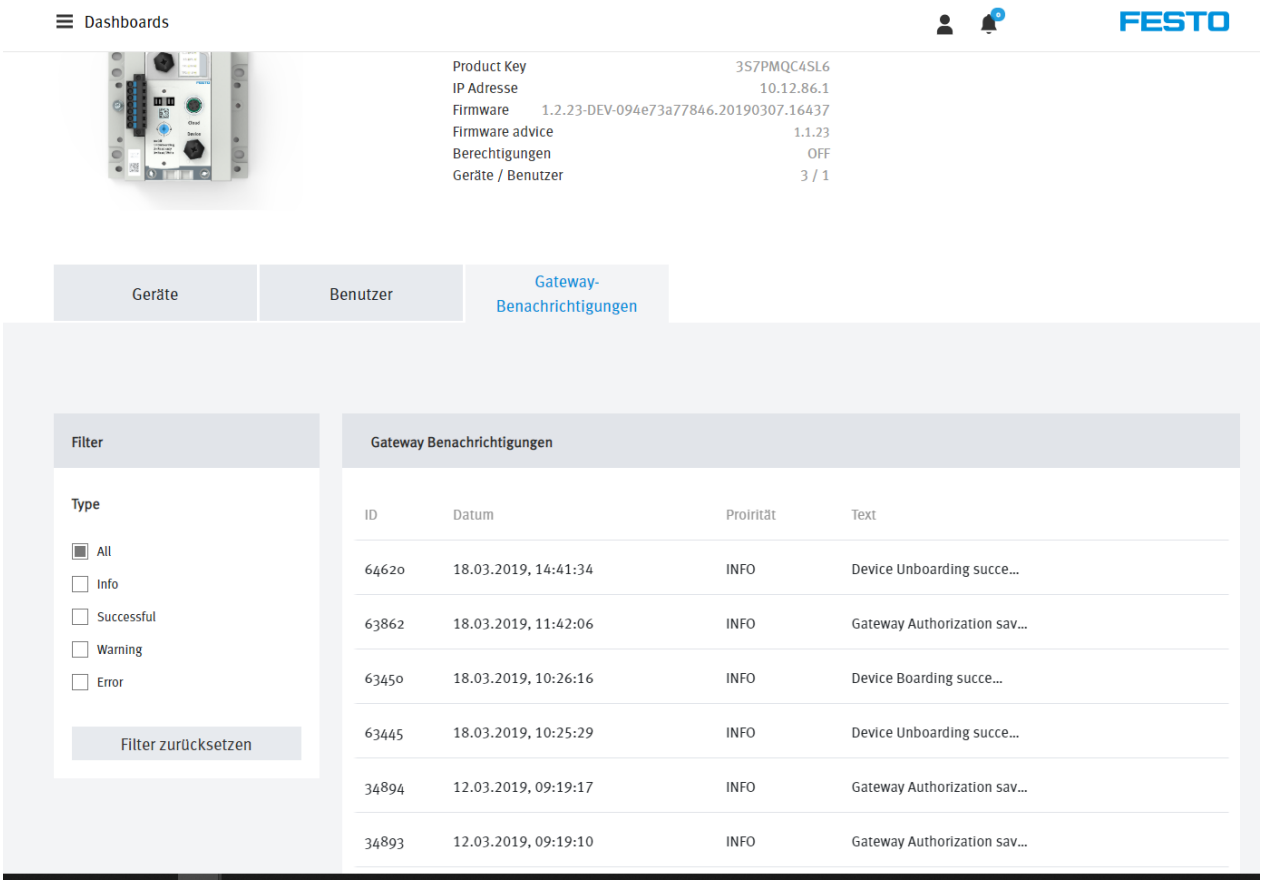
All notifications that have occurred are displayed as push notifications. Push notifications are deleted from the global notifications after refreshing the page, or by logging on and back off again. If the notifications should nevertheless be viewed, this can be done in the corresponding logbooks of the dashboards.

In order to make push notifications easy to manage, they are divided into categories including Information, Warning and Error. This is also indicated by the symbols. The push messages pop up on the one hand, and can be viewed via the “bell” icon on the other hand.



10.3 Notification centre

The notification centre can be found in the respective dashboards. This is where all notifications that can be assigned to a dashboard are stored. As with push notifications, these notifications are assigned different priorities with which they can be filtered.



10.4 CPX-IOT gateway

The CPX-IOT gateway has its own logbook. This is integrated in the IoT gateway dashboard. Notifications are categorised by means of priorities including Info, Successful, Warning and Error. The following notification may occur in the IoT gateway:

DEVICE_BOARDING_SUCCESS

Severity: INFO

Where: logbook gateway, toast

Example: The device MSE6-E2M with the product key 3S7PLWRRMH7 was successfully registered.

DEVICE_BOARDING_FAILED

Severity: ERROR

Where: logbook gateway, toast

Example: the device MSE6-E2M with the product key 3S7PLWRRMH7 could not be registered. Incorrect switch settings.

DEVICE_UNBOARDING_SUCCESS

Severity: INFO

Where: logbook gateway, toast

Example: The device MSE6-E2M with the product key 3S7PLWRRMH7 was successfully removed.

DEVICE_UNBOARDING_FAILED

Severity: ERROR

Where: logbook gateway, toast

Example: the device MSE6-E2M with the product key 3S7PLWRRMH7 could not be removed. Incorrect switch settings.

GATEWAY_BOARDING_SUCCESS

Severity: INFO

Where: logbook gateway, toast

Example: the gateway with the product key 3S7PLWRRMH7 was successfully registered.

GATEWAY_UNBOARDING_FAILED

Severity: ERROR

Where: logbook gateway, toast

Example: the gateway with the product key 3S7PLWRRMH7 could not be removed.

GATEWAY_CONNECTION_ESTABLISHED

Severity: INFO

Where: logbook gateway, toast

Example: connection to the gateway with the product key 3S7PLWRRMH7 was successfully established.

GATEWAY_CONNECTION_LOST

Severity: INFO

Where: logbook gateway, toast

Example: connection to the gateway with the product key 3S7PLWRRMH7 has been aborted.

GATEWAY_AUTHORIZATION_SAVED

Severity: INFO

Where: logbook gateway, toast

Example: the user ‹user› was authorised on the gateway with the product key 3S7PLWRRMH7 as Admin.

GATEWAY_AUTHORIZATION_SAVE_FAILED

Severity: INFO

Where: logbook gateway, toast

Example: the authorisation for the user max.mustermann@mail.de failed.

GATEWAY_NAME_CHANGED

Severity: INFO

Where: logbook gateway, toast

Example: for the gateway with the product key 3S7PLWRRMH7 the gateway name was changed from IoT-CNC to IoT-CNC Scharnhausen by user max.mustermann@mail.de.

10.5 E2M Dashboard

The E2M Dashboard has its own logbook. It can be listed in the IoT gateway dashboard. Notifications are categorised by means of priorities including Info, Successful, Warning and Error. The following notifications may occur in the E2M dashboard:

CSV_EXPORT_STARTED

Severity: INFO

Where. Logbook device, toast,

Example: the CSV data export has been started. Requested by user max.mustermann@mail.de.

CSV_EXPORT_AVAILABLE

Severity: INFO

Where: e-mail to user who requested CSV export

CSV_EXPORT_FAILED

Severity: ERROR

Where. Logbook device, toast

Example: the CSV data export was aborted.

DASHBOARD_LIMITS_CHANGED

Severity: INFO

Where. Logbook device, toast

Example: for the device with the product key 3S7PMFZ5L92 the limits of the size supply flow (avg/period)/Reference has changed from 10 to 20 by user max.mustermann@mail.de

DASHBOARD_SETTINGS_SAVED

Severity: INFO

Where: Logbook device, toast

Example: for the device with the product key 3S7PMFZ5L92 the parameter air consumption (period) was changed from l to m³ by user max.mustermann@mail.de.

DASHBOARD_SETTINGS_SAVE_FAILED

Severity: ERROR

Where: Logbook device, toast

Example: for the device with the product key 3S7PLWRRMH7 the parameter change failed.

DASHBOARD_STATE_CHANGED

Severity: WARNING

Where: Logbook device, toast, e-mail to all users

Example: for the device with the product key 3S7PLWRRMH7 the state of the size ‹monitored size› has changed from ‹state old› to ‹state new›.

DASHBOARD_NAME_CHANGED

Severity: INFO

Where: Logbook device, toast

Example: for the device with the product key 3S7PLWRRMH7 the device name was changed from ‹Name old› to ‹Name new› by user max.mustermann@mail.de.

DASHBOARD_NAME_CHANGE_FAILED

Severity: ERROR

Where: Logbook device, toast

Example: for the device with the product key 3S7PLWRRMH7 the device name change failed.

DEVICE_CONNECTION_ESTABLISHED

Severity: INFO

Where: Logbook device, toast

Example: connection to device MSE6-E2M with the product key 3S7PLWRRMH7 was successfully established.

DEVICE_CONNECTION_LOST

Severity: INFO

Where: Logbook device, toast

Example: connection to device MSE6-E2M with the product key 3S7PLWRRMH7 is aborted.

DEVICE_AUTHORIZATION_SAVED

Severity: INFO

Where: Logbook device, toast

Example: the user max.musterman@mail.de was authorised as Admin on the device MSE6-E2M with the product key 3S7PLWRRMH7.

DEVICE_AUTHORIZATION_SAVE_FAILED

Severity: ERROR

Where: Logbook device, toast

Example: the authorisation for the user max.mustermann@mail.de failed.

10.6 CPX-MPA dashboard

The CPX-MPA Dashboard has its own logbook. This can be listed in the IoT Gateway Dashboard. Notifications are categorised by means of priorities including Info, Successful, Warning and Error. The following notifications may occur in the CPX-MPA Dashboard:

DASHBOARD_NAME_CHANGED

Severity: INFO

Where: Logbook device, toast

Example: for the device with the product key 3S7PLWRRMH7 the device name was changed from CPX Production Plant 2 to CPX Production Plant 2 by user max.mustermann@mail.de.

DASHBOARD_NAME_CHANGE_FAILED

Severity: ERROR

Where: Logbook device, toast

Example: for the device with the product key 3S7PLWRRMH7 the device name change failed.

DEVICE_CONNECTION_ESTABLISHED

Severity: INFO

Where: Logbook device, toast

Example: connection to device MSE6-E2M with the product key 3S7PLWRRMH7 was successfully established.

DEVICE_CONNECTION_LOST

Severity: INFO

Where: Logbook device, toast

Example: connection to device MSE6-E2M with the product key 3S7PLWRRMH7 is aborted.

DEVICE_AUTHORIZATION_SAVED

Severity: INFO

Where: Logbook device, toast

Example: the user max.mustermann@mail.de was authorised as Admin on the device CPX with the product key 3S7PLWRRMH7.

DEVICE_AUTHORIZATION_SAVE_FAILED

Severity: ERROR

Where: Logbook device, toast

Example: the authorisation for the user max.mustermann@mail.de failed.

DASHBOARD_ERROR_DETECTED

Severity: ERROR

Where: Logbook device, toast, e-mail to all users

Example: the device with the product key 3S7PLWRRMH7 has the error short circuit.

DASHBOARD_ERROR_RELEASED

Severity: INFO

Where: Logbook device, toast, e-mail to all users

Example: for the device with the product key 3S7PLWRRMH7 the error Short circuit is no longer present.

11 VDMA monitoring according to Standard Sheet 24582

The VDMA fieldbus-neutral reference architecture for condition monitoring in factory automation forms the basis for the creation of communication profiles for condition monitoring and the integration of condition monitoring tools (dashboards). Dashboards answer the following questions:

- What needs to be monitored?
- How should I measure the variables?
- How do measured values have to be processed technically/mathematically?
- How can I visualise a status message?
- How will I be informed about status statements in the system?

In order to answer these questions, we use a CM-Lib for the MSE6-E2M that collects the measured values from the sensors, processes them and then sends them to the gateway. In combination with the setting of critical limits in the cloud, compressed air monitoring can be individually adapted to the system. By visualising the VDMA status as well as by clear notifications and e-mail alerts, you are always kept up to date on the condition and state of health of the components and the general pneumatics in the system.

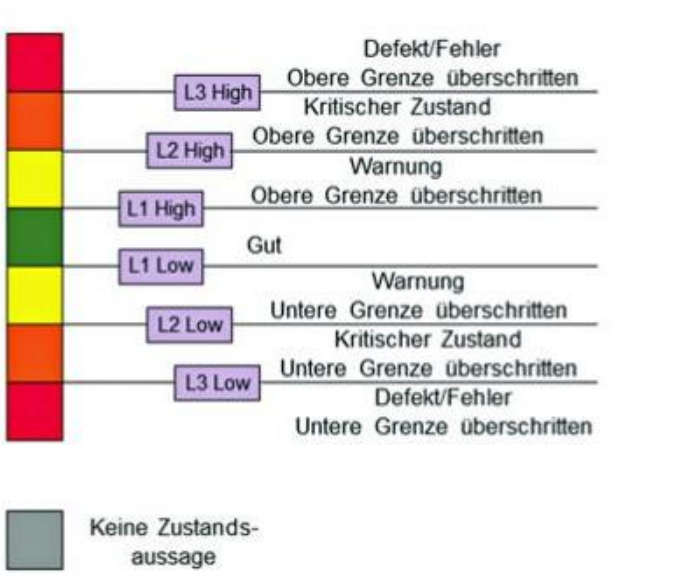
11.1 Aggregation hierarchy

The aggregation hierarchy of condition monitoring is defined in accordance with VDMA guidelines. And thus the most critical subsystem status is always read out as the overall statement for the component. This logic is also used in status monitoring.

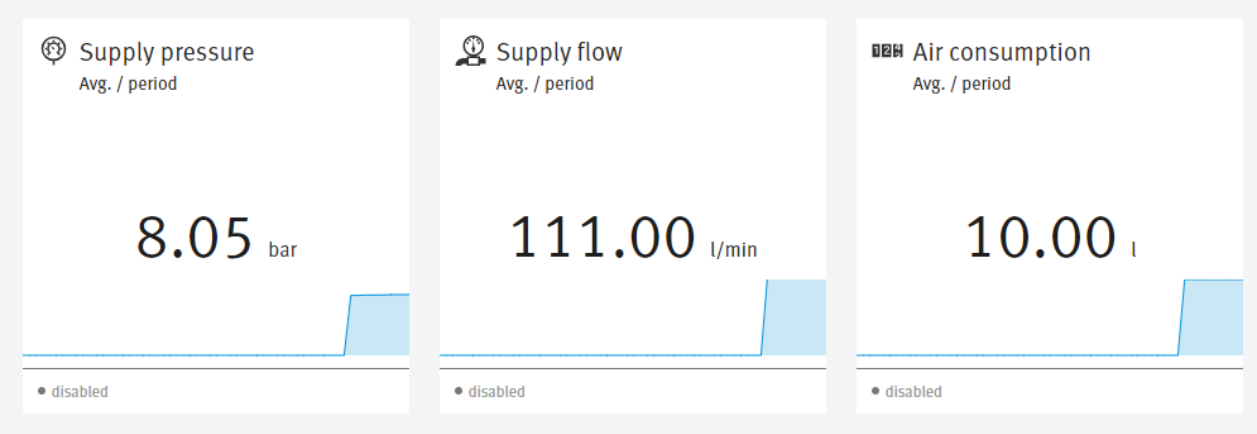
11.2 Setting critical limits

The limit values in the dashboard for monitoring transmitted data points and the definition of a status are defined in VDMA Standard Sheet 24582.

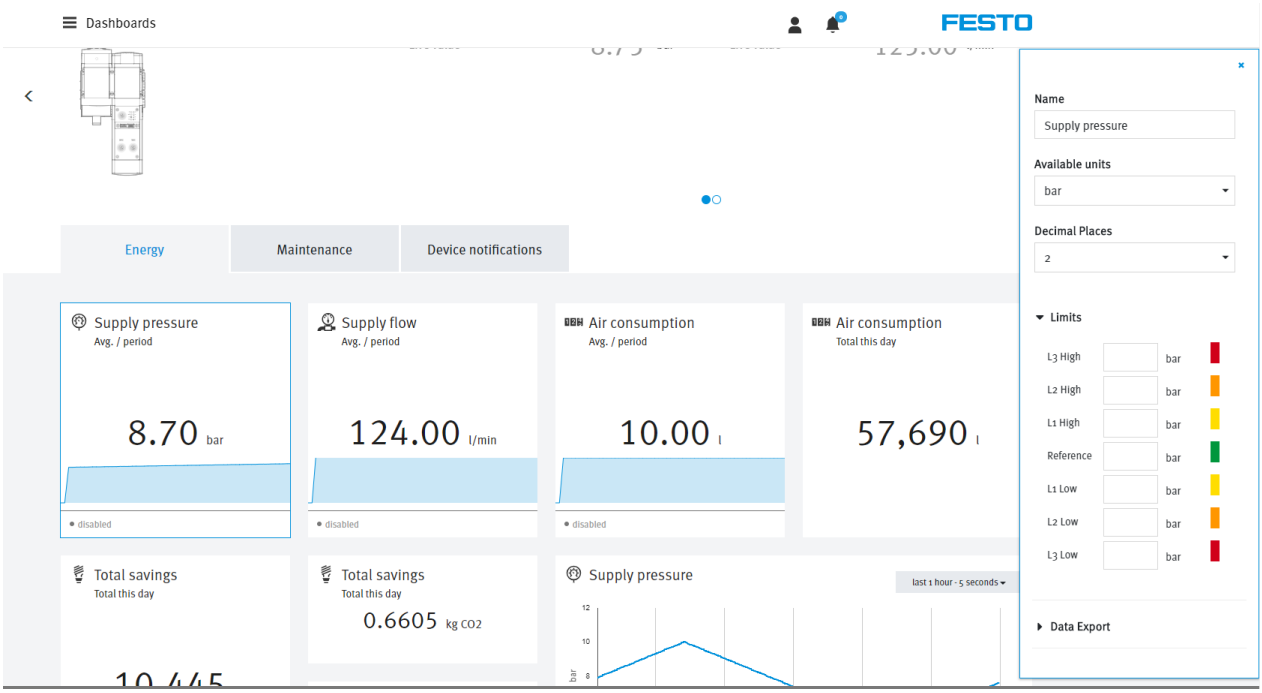
You can define critical limits for gradations L1-L3 High and L1-L3 Low yourself for a data point in the dashboard. The system then warns you by e-mail if the critical limits set in the dashboard are exceeded or fallen short of, and if the notification function is switched on.



By default, no critical limits are stored and thus the disabled state (grey) is read out in the widgets and as the overall status. All widgets in which limit values can be specified are thus displayed as disabled (grey) after boarding.



In order to be able to define the critical limits, the edit mode must be enabled via the hamburger menu. Then select the widget in which the critical limits will be set. Once the widget has been selected, a settings window opens. The critical limits can now be defined in the critical limits settings. Not all critical limits need to be specified. If a critical limit is missing, the corresponding status is not shown. If all fields are cleared, the widget switches back to the disabled state (grey). The selected critical limits are only accepted if they are saved in the edit mode via the “Save” button.

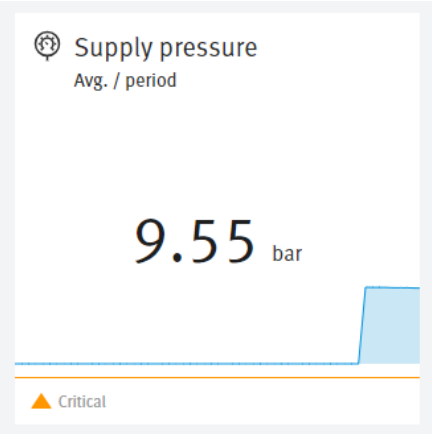


11.3 VDMA status display in the widget and in the device overview

The VDMA status is always displayed at the bottom of the relevant widgets. The gradations and colour codes are defined in accordance with the VDMA Standard Sheet. The following states are possible:

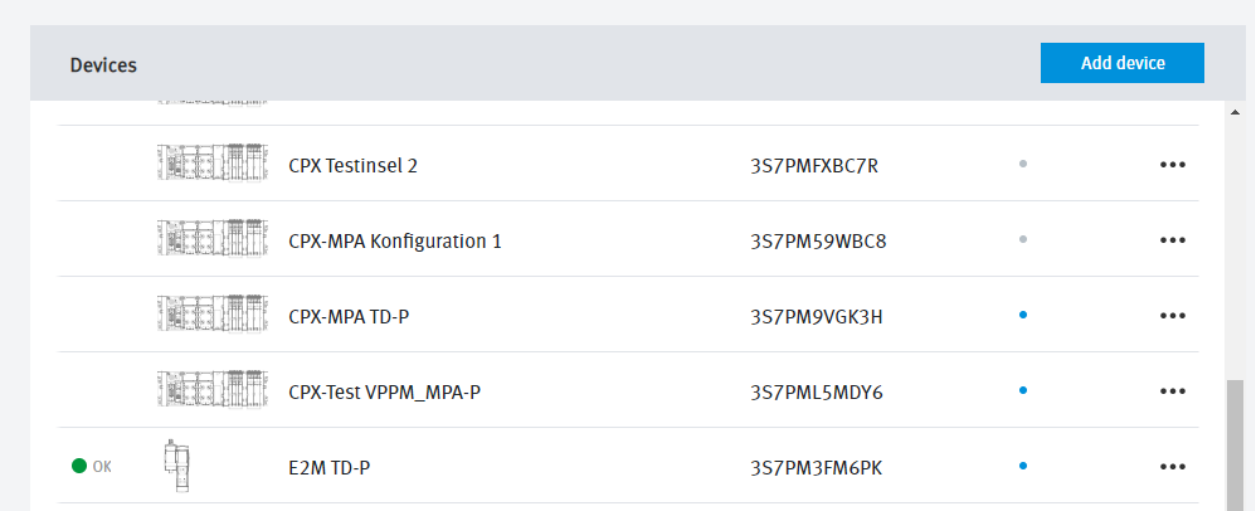
- OK (green)
- Warning (yellow)
- Critical (orange)
- Error (red)

An arrow also indicates visually whether the upper (arrow pointing upwards) or lower (arrow pointing downwards) critical limit has been exceeded or fallen short of. In the case of the component's overall VDMA status, there is no indication of critical limits which have been exceeded or fallen short of. The reason for this lies in the conflicting statements. The following screenshot depicts and exceeded VDMA L2 High status. A warning is read out. Since the upper critical limit has been exceeded, the arrow points upwards.



11.4 VDMA status in the device overview

The device overview displays the overall VDMA status of a component. The most critical status of the component is displayed according to the aggregation hierarchy as per VDMA Standard Sheet 24582. Critical limits which have been exceeded or fallen short of are not shown here.



11.5 How do I define a critical limit?

The critical limits are set specifically for the system. The user possesses the required system or component-specific know-how for the machine under test.

11.6 When is a VDMA status read out?

The VDMA status is read out whenever the component is actively connected to the cloud. No statement can be made about the status of a component when it is offline. In this case, the overall status and all relevant widgets are set to disabled. If no critical limits are defined, the corresponding widget is also set to disabled. If no critical limits are set in any of the relevant widgets, the overall status of the component and all relevant widgets are set to disabled. In the case of component-specific statuses for which no status statements can be made either, the corresponding widgets and the overall status are set to disabled. With the E2M, for example, this is the case when the component is in the shut-off state.