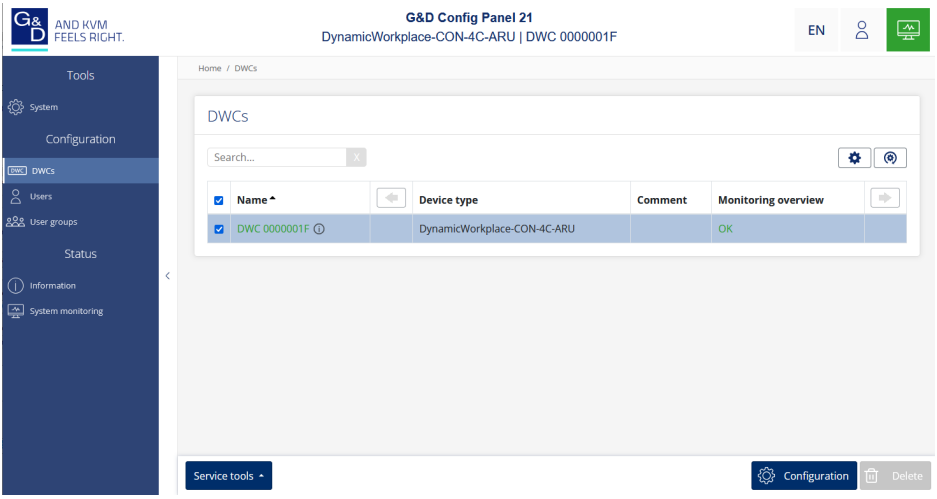
G&D DynamicWorkplace-CON series

EN »Config Panel« Web Application
Configuring the dynamic console



A9200166-1.10

About this manual

This manual has been carefully compiled and examined to the state-of-the-art.

G&D neither explicitly nor implicitly takes guarantee or responsibility for the quality, efficiency and marketability of the product when used for a certain purpose that differs from the scope of service covered by this manual.

For damages which directly or indirectly result from the use of this manual as well as for incidental damages or consequential damages, G&D is liable only in cases of intent or gross negligence.

Caveat Emptor

G&D will not provide warranty for devices that:

- Are not used as intended.
- Are repaired or modified by unauthorized personnel.
- Show severe external damages that was not reported on the receipt of goods.
- Have been damaged by non G&D accessories.

G&D will not be liable for any consequential damages that could occur from using the products.

Proof of trademark

All product and company names mentioned in this manual, and other documents you have received alongside your G&D product, are trademarks or registered trademarks of the holder of rights.

© Guntermann & Drunck GmbH 2026. All rights reserved.

Version 1.10 – 10/04/2026
Config Panel 21 version: 1.7.300

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

Phone +49 (0) 271 23872-0
Fax +49 (0) 271 23872-120

www.gdsys.com
sales@gdsys.com

Table of contents

Chapter 1: Basic functions

Introduction **1**

System requirements **2**
Supported operating systems 2
Recommended resolutions 2

Initial configuration of the network settings **3**

Getting started **4**
Starting the web application 4
Operating the web application 6
User interface 6
Frequently used buttons 8
Configuring table columns 8
Language settings 10
Selecting the language of the web application 10
Selecting the system language 10
Automatic logout 11
Showing terms of use 12
Password complexity 13
Login options 14
Showing the version number of the web application and general information 15
Closing the web application 15

Basic configuration of the web application **16**
Network settings 16
Configuring the network interfaces 16
Configuring global network settings 18
Increasing the reliability of network connections by link aggregation 20
Reading out the status of the network interfaces 23
Creating and administrating netfilter rules 24
Creating new netfilter rules 24
Editing existing netfilter rules 26
Deleting existing netfilter rules 29
Changing the order or priority of existing netfilter rules 29
Creating an SSL certificate 30
Special features for complex KVM systems 31
Creating a Certificate Authority 31
Creating any certificate 33
Creating and signing an X509 certificate 34
Creating a PEM file 35
Selecting an SSL certificate 36

Firmware update 38
Firmware update of a single device 38
Firmware update of multiple KVM system devices 39
Restoring the system defaults 40
Restarting the device 40

Network functions of the devices 41
NTP server 41
Time sync with an NTP server 41
Manual setting of time and date 43
Logging syslog messages 44
Local logging of syslog messages 45
Sending syslog messages to a server 46
Viewing and saving local syslog messages 47
User authentication with directory services 47
Setting up two-factor authentication on the device (optional) 50

Monitoring functions 52
Viewing all monitoring values 52
Enabling/disabling monitoring values 53
Advanced features for managing critical devices 54
Displaying the list of critical monitoring values 54
Confirm the alarm of a critical device 54

Monitoring devices via SNMP 55
Practical use of the SNMP protocol 55
Configuring an SNMP agent 55
Adding and Configuring SNMP traps 58

Users and groups 61
Efficient rights administration 61
The effective right 61
Efficient user group administration 62
Administrating user accounts 63
Creating a new user account 64
Activating two-factor authentication 65
Renaming a user account 68
Changing the password of a user account 69
Changing the user account rights 70
Overview of user-related settings (Personal profile) 71
Changing a user account's group membership 72
Enabling or disabling a user account 73
Deleting a user account 73

Administrating user groups 74
Creating a new user group 74
Renaming a user group 75
Changing the user group rights 76
Administrating user group members 77
(De)activating a user group 77
Deleting a user group 77
System rights 78
Rights for unrestricted access to the system (Superuser) 78
Changing the login right to the web application 78
Rights to change your own password 79
Authorization to confirm a monitoring alarm 79

Advanced functions of the KVM system 80
Identifying a device by activating the Identification LED 80
Saving the configurations 80
Saving the configurations with auto backup function 81
Restoring the configurations 84
Activating premium functions 85

Chapter 2: DWCs

Basic configuration of DWCs 86
Changing the name of a DWC 86
Changing the comment of a DWC 86

Configuration settings of DWCs 87
Device configuration 87
Selecting the active counterpart 87
Adding counterparts manually 87
Removing counterparts 87

Advanced features for DWCs 88
Copying the config settings (Replace device) 88
Configuring monitoring values 89
Selecting the values to be monitored 89
Viewing status information of a DWC 90

1 Basic functions

Introduction

The *ConfigPanel* web application provides a graphical user interface to configure the KVM system. The application can be operated from any supported web browser (see page 2).

ADVICE: The web application can be used in the entire network independently from the locations of the devices and consoles connected to the KVM system.

Thanks to its enhanced functions, the graphical user interface provides the following features for easy operation:

- Clearly arranged user interface
- Monitoring of various system features
- Advanced network functions (netfilter, syslog, …)
- Backup and restore function

System requirements

IMPORTANT: Before starting the web application via web browser, connect the device from which you want to load the web application to the local network. The *Installation* manual of the device provides more information.

If not already done, adjust the network settings as described on page 3.

The web application *ConfigPanel* has been successfully tested with the following web browsers:

- Apple Safari 26
- Google Chrome 142
- Microsoft Edge 144
- Mozilla Firefox 147

Supported operating systems

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

Recommended resolutions

- A minimum resolution of 1280 × 800 pixels is recommended.
- The web application is optimized to display the content in landscape mode.
- Portrait mode is supported. In this mode, not all contents may be visible.

Initial configuration of the network settings

NOTE: In the defaults, the following settings are pre-selected:

- IP address of *network interface A*: **192.168.0.1**
- IP address of *network interface B*: address obtained using **DHCPv4**
- Global network settings: obtain settings dynamically

To access the web application, the network settings of the device on which the web application is operated need to be configured.

How to configure the network settings before integrating the device into the local network:

1. Use a category 5 (or better) twisted pair cable to connect the network interface of any computer to the device's *Network A* interface.
2. Ensure that the IP address of the computer's network interface is part of the subnet to which the device's IP address belongs to.

   NOTE: Use the IP address *192.168.0.100,* for example.
3. Switch on the device.
4. Start the computer's web browser and enter **192.168.0.1** in the address bar.
5. Configure the network interface(s) and the global network settings as described in the paragraph *Network settings* on page 16 f.

   IMPORTANT: It is not possible to operate both network interfaces within one subnet!
6. Remove the twisted pair cable connection between computer and device.
7. Implement the device in the local network.

Getting started

This chapter introduces you to the basic operation of the web application.

NOTE: For a detailed explanation of the functions and configuration settings, refer to the following chapters of this manual.

Starting the web application

NOTE: Information on the system requirements of the web application can be found on page 2.

How to start the web application

1. Enter the following URL in the address line:

   https://[IP address of the device]

2. Enter the following data in the login mask:

Agree to the terms of use:	Click on the text to read the terms of use. Click on the checkbox to accept the terms of use.
	NOTE: The terms of use only appear if a corresponding configuration has been made (see *Showing terms of use* on page 12 ff.).
Username:	Enter a username.
Password:	Enter a password for your user account.
2-Factor Auth Code (TOTP):	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.
	NOTE: The 2-Factor Auth Code (TOTP) is only requested if two-factor authentication has been configured (see page 50 f.) and activated (see page 65 ff.).

IMPORTANT: Change the administrator account's default password.

To do this, log into the web application with the administrator account and then change the password (see page 69).

The *default* access data to the administrator account are:

- **Username:** Admin
- **Password:** see *login* information on the label on the bottom of the device

3. Click on **Login**.

Operating the web application

User interface

The user interface of the web application consists of several areas:

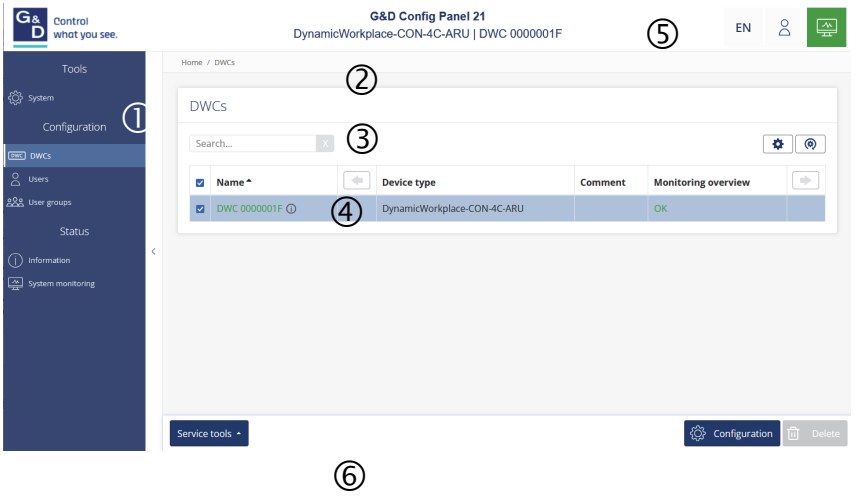


Figure 1: User interface of the web application

The different areas of the user interface serve different tasks. The following table lists the purpose of each area:

Menu ①:	In the menu the different functions of the web application are summarised in various topics.
Breadcrumb navigation ②:	The breadcrumb navigation shows you the path to the currently opened dialog. To quickly return to a higher-level dialog, you can click on it in the breadcrumb navigation.
Filter function ③:	You can use the filter function to narrow down the items displayed in the main view. In the text box, enter part of the name of the element you want to find. Only elements that contain this text in one of the *displayed* columns are displayed in the main view. The names are not case-sensitive during filtering. To delete the filter, click on the **[X]** icon.
Main view ④:	After selecting a topic in the menu, the contents of this topic are displayed here.

Shortcuts ⑤:	**Language selection:** The language identifier (for example **EN** for *English*) shows the currently active language in the web application. To switch the language, click the language identifier. This opens a submenu that shows the supported languages and the corresponding identifiers. Switch the language by clicking on the desired language. **User:** A click on the user icon opens a submenu: ▪ The name of the active user is displayed in the submenu. ▪ Click on *User* to access the user settings of the active user. ▪ Click on *Logout* to exit the active session. **Monitoring status:** This icon shows you at a glance whether all monitoring values are within the normal range (green icon) or if at least one monitoring value is outside the normal range (yellow or red icon). The *Monitoring status* icon always takes the colour of the *most critical* monitoring value If the icon is displayed in yellow or red, you can access the *Active alarms* dialog by clicking on the icon.
Buttons ⑥:	Depending on the dialog shown, different buttons are displayed in this area.

Frequently used buttons

The user interface uses various buttons to perform operations. The following table informs you about the names and functions of the buttons used in many dialog masks:

Configuration:	Show configuration settings of the selected element (device, user, ...)
Service tools:	If you select a device in the main view, you can use the service tools to perform certain tasks (for example, update, backup, show syslog).
Save:	Saving of the entered data. The opened dialog is still displayed.
Cancel:	The data you have entered will be discarded and the dialog will be closed.
Close:	The entered data is cached and the dialog is closed. Only after clicking on **Save** or **Cancel** the data is permanently stored or discarded.

Configuring table columns

You can adapt the table columns to be displayed under **DWCs** and **Users** to your requirements.

By default, the columns *Name*, *Device type*, *Comment* and *Monitoring overview* are shown under **DWCs**:

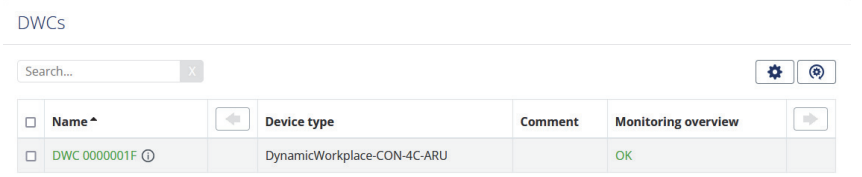


Figure 2: Table columns (selection) of a DWC

How to change the columns to be displayed:

> **NOTE:** The **Name** column is *always* shown as the first column of the table.

1. Click on the gears icon ( ) above the table.

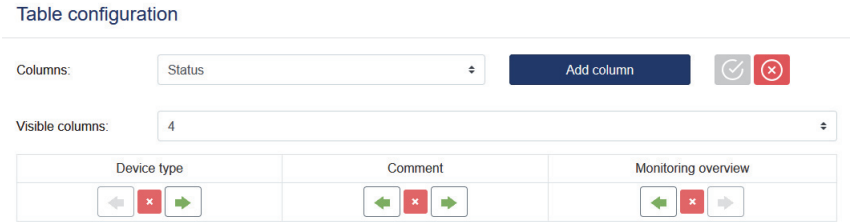


Figure 3: Table configuration

2. To add a column, select it from the **Columns** drop-down box and click on **Add column**.
3. To delete a column, click on the red button ( ) below the column header.
4. Click on the green **check mark** ( ) to save your settings or klick on the red **Discard** button ( ).

How to change the column order:

> **NOTE:** The **Name** column is *always* shown as the first column of the table.

1. Click on the gears icon above the table.
2. To move a column to the left, click on the **arrow left** icon ( ) of this column.
3. To move a column to the right, click on the **arrow right** icon ( ) of this column.
4. Click on the green **check mark** ( ) to save your settings or click on the red **Discard** button ( ).

How to reset the table configuration to the default settings

1. Click on the **Table configuration reset** icon ( ) above the table.
2. Confirm the security prompt by clicking on **Yes**.

Language settings

Selecting the language of the web application

How to change the language of the web application:



1. Click the language identifier of the current language in the upper right corner.
2. Switch the language to be used by clicking on the desired language.

NOTE: The selected language is saved in the user settings of the active user. The next time this user logs on, the previously selected language setting is applied.

Selecting the system language

The specified system language is assigned to all user accounts by default.

How to set the system language:

1. Click **System** on the menu.
2. Click **System language**.
3. Select the desired language.
4. Click **Save**.

Automatic logout

The Automatic logout function is used to automatically log out the user of the web application if no activity is detected for a certain period of time.

It is also possible to select whether the user is shown a timer (time counting down in minutes:seconds until automatic logout).

Define this period by entering a value between **1** and **60** minutes.

> **NOTE:** To disable the function, enter the value **0**.

How to (de)activate the Auto logout function:

1. Click **System** on the menu.
2. Click **Automatic logout**.
3. In the **Automatic logout of the Config Panel (0-60 minutes)** field, you can define the time of inactivity before automatic logout between **1** and **60** minutes (*default*: 15 minutes).

   > **NOTE:** If user activity is detected, the timer is reset.
   >
   > When an update process is started via the web application, the timer is also reset and only runs again once the update process has been completed.

4. In the **Show timer** field, you can select between the following options:

On:	The timer is displayed to the user at the top right of the web application if the entry in the **Automatic logout of the Config Panel (0-60 minutes)** is not **0**.
Off:	No timer is displayed to the user.

5. Click **Save**.

Showing terms of use

If the terms of use are displayed, they must be accepted before each (new) device access.

How to configure the display of terms of use:

1. Click **System** on the menu.
2. Click **Terms of use**.
3. In the **Show terms of use** field, you can select between the following options:

Off:	*No* terms of use are displayed during log in (*default*).
User defined:	*Individual* terms of use are displayed during log in.

4. If you selected *User defined* in the previous step, go to the **Short text** field and enter the text that a user is shown before accepting the terms of use (**example**: *I have read the terms of use and hereby agree to them*).
   This text field is limited to 70 characters.
5. Now enter the desired terms of use in the **Long text** field.
   This field is limited to 1,500 characters.
6. Click **Save**.

Password complexity

You can configure password complexity to comply with your individual password guidelines and improve security.

IMPORTANT: Changes in the section of password complexity have **no** effect on existing passwords, but are only taken into account when a password is changed (see *Changing the password of a user account* on page 69 ff.) and a new user account is created (see *Creating a new user account* on page 64). You should therefore configure the password complexity as early as possible.

IMPORTANT: Changes in the section of password complexity have **no** effect on user authentication with external directory services. The directory services have their own configuration options.

How to configure the password complexity:

1. Click **System** on the menu.
2. Click **Password complexity**.
3. In the **Minimum password length** field, enter the desired minimum password lenght (*Default*: 3)
4. In the **Minimum number of capital letters (e.g. ABCDEF)** field, enter the desired minimum number of capital letters within a password (*Default*: 0)
5. In the **Minimum number of lowercase letters (e.g. abcdef)** field, enter the desired minimum number of lowercases within a password (*Default*: 0)
6. In the **Minimum number of digits (e.g. 012345)** field, enter the desired minimum number of digits within a password (*Default*: 0)
7. In the **Minimum number of special characters (e.g. !#%&?@)** field, enter the desired minimum number of special characters within a password (*Default*: 0)
8. In the **Minimum number of characters of the previous password to be changed** field, enter the desired minimum number of characters that must be differnt compared with the previous password (*Default*: 0)

   NOTE: The minimum number of different characters compared with the previous password must not be higher than the minimum password length.

9. Click **Save**.

Login options

To improve security, further configuration options are available in the login options area.

You can specify how many failed attempts are accepted when entering a password and how long a user is locked out after exceeding the maximum number of failed attempts.

How to configure the Login options:

1. Click **System** on the menu.
2. Click **Login optionsy**.
3. In the **Number of consecutive invalid login attempts up to the time of blocking (0=off)** field, enter the desired maximum number of failed attempts when entering the password (*Default*: 0 = off/unlimited number of failed attempts, max. 1,000)
4. In the **Locking time (in minutes)** field, enter the desired locking time in minutes for which a user is locked after exceeding the maximum number of failed password entry attempts (*Default*: 1 (if max. failed attempts > 0), max. 1,440 minutes)
5. In the **Limit the number of simultaneous sessions with superuser rights** field, enter the desired number of maximum simultaneous superuser sessions (*Default*: 0 = off/unlimited number of superuser sessions, max. 1,024)

   NOTE: The maximum number of simultaneous superuser sessions is effectiv per interface (device/OSD and ConfigPanel).

6. Click **Save**.

Showing the version number of the web application and general information

How to show the version number of the web application and general information:

1. In the menu, click on **Information**.
2. The **General** tab provides you with information about the *ConfigPanel* version.

Closing the web application

Use the *Close* button to end the active session of the web application.

IMPORTANT: To protect the web application against unauthorised access, always use the *Logout* function after finishing your work with the web application.

How to close the web application:

1. Click on the **user icon** at the top right.



- Click on **Logout** to exit the active session.

Basic configuration of the web application

Network settings

The device provides two network interfaces (*Network A* and *Network B*). The network interfaces lets you integrate a device into up to two separate networks.

IMPORTANT: Note the separate instructions about the *Initial configuration of the network settings* on page 3.

Configuring the network interfaces

To connect the device to a local network, you need to configure the settings of the network.

NOTE: These are the default settings:

- IP address of the *network interface A*: **192.168.0.1**
- IP address of *network interface B*: Obtain address via **DHCPv4**
- Global network settings: Obtain settings dynamically

How to configure the settings of a network interface:

IMPORTANT: It is not possible to use both network interfaces within the same subnet.

NOTE: The *Link Local* address space 169.254.0.0/16 is reserved for internal communication between devices in accordance with RFC 3330. It is not possible to assign an IP address of this address space.

IMPORTANT: Configuration of **IPv6** should only be performed **by technically experienced users**. While IPv6 offers advanced features and a larger address space, it also introduces **more complex requirements regarding network structure, security, and compatibility**. Incorrect settings may lead to **connectivity issues or unexpected network behavior**. If you are **not familiar** with the IP addressing and network topology specific to IPv6, we recommend that you thoroughly **inform yourself about the implications** before enabling IPv6, or consult with your network administration.

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Interfaces**.

5. Enter the following values under **Interface A** or **Interface B**:

> **NOTE:** Each network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

Operating mode:	Select the operational mode of **Interface A** or **Interface B**: ▪ **Off:** Disable network interface. ▪ **Static IPv4:** A static IPv4 address is assigned. ▪ **DHCPv4:** Obtain IPv4 address from a DHCP server The drop-down list shows the text **Link aggregation active** if the interface has been added to a network interface group. In this case, configure the network interfaces under »Link aggregation«.
IPv4 address:	Enter the IPv4 address of the interface (only when operating mode *Static IPv4* is selected).
Netmask:	Enter the netmask of the network (only when operating mode *Static IPv4* is selected).
IPv6:	Click the toggle switch to enable IPv6 (green/right = enabled). **NOTE:** When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user. Click the toggle switch to disable IPv6 (grey/left = disabled (*default*)).
IPv6 address:	Enter the static IPv6 address of the interface.
Subnet prefix length:	Specify the prefix length (*default*: 64) for the interface according to the notation rules defined in RFC 5952.

6. Click on **Save**.

Configuring global network settings

Even in complex networks global network settings ensure that the web application is available from all subnetworks.

How to configure global network settings:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Now go to **Global network settings**.
5. Enter the following values:

Operating mode:	Enter the desired operating mode: ▪ **Static:** Use of static settings. ▪ **Dynamic:** Partial automatic retrieval of the settings described below from a DHCP server (IPv4) or via SLAAC (IPv6).
Hostname:	Enter the hostname of the device.
Domain:	Enter the domain to which the device should belong.
Gateway IPv4:	Enter the IPv4 address of the gateway.
Gateway IPv6:	Enter the IPv6 address of the gateway.
DNS server 1:	Enter the IP address of the DNS server..
	NOTE: If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**.
DNS server 2:	*Optionally*, enter the IP address of another DNS server..
	NOTE: If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**.
Prioritization of IPv6:	Click the toggle switch if IPv6 should be preferred when a destination has both an IPv6 and an IPv4 address (green/right = IPv6 is preferred). Click the toggle switch if IPv6 should not be preferred (grey/left = IPv6 is not preferred, *default*).
Use IPv6 Stateless Address Auto-configuration (SLAAC):	Click the toggle switch if SLAAC should be used (green/right = SLAAC is used, *default*). Click the toggle switch if SLAAC should not be used (grey/left = SLAAC is not used).

Send ICMP Echo Reply to Echo Request from a Multicast/anycast address (IPv6):	Click the toggle switch if ICMPv6 Echo Requests should be answered (green/right = Echo Requests are answered, *default*). Click the toggle switch if ICMPv6 Echo Requests should not be answered (grey/left = Echo Requests are not answered).
Send ICMP destination unreachable messages (IPv6):	Click the toggle switch if an ICMPv6 error message should be sent to the sender when a packet cannot be delivered (green/right = error message is sent, *default*). Click the toggle switch if no ICMPv6 error messages should be sent (grey/left = error message is not sent).
Process redirect messages (IPv6):	Click the toggle switch if redirect messages should be accepted and processed (green/right = redirect messages are processed, *default*). Click the toggle switch if redirect messages should not be processed (grey/left = redirect messages are not processed).
Duplicate Address Detection (IPv6):	Click the toggle switch if a check for duplicate IPv6 addresses should be performed before an address is used (green/right = duplicate address check is performed, *default*). Click the toggle switch if no check for duplicate IPv6 addresses should be performed (grey/left = no duplicate address check is performed).

6. Click on **Save**.

Increasing the reliability of network connections by link aggregation

By default, you can use both network interfaces at the same time to acees the web application from two different network segments, for example

To increase reliability, the entwork interfaces can be grouped via *link aggregation*. Within a group, only one interface is active at a time. Another interface only becomes active if the active interface fails.

Two different modes are available for monitoring the interfaces:

- **MII mode:** The carrier status of the network interface is monitored via the *media independent interface*. In this mode, only the functionality of the network is tested.
- **ARP mode:** Using the *address resolution protocol*, requests are sent to an ARP target on the network. The response from the ARP target confirms both the functionality of the network interface and a proper network connection to the ARP target.

If the ARP target is connected to the network but temporarily offline, the requests cannot be answered. For this reason, you should determine several ARP targets in order to obtain a response from at least one target even if an ARP target fails.

NOTE: It is not possible to combine **MII** and **ARP mode**.

How to configure the settings of grouped network interfaces:

NOTE: The *Link Local* address space 169.254.0.0/16 is reserved for internal communication between devices in accordance with RFC 3330. It is not possible to assign an IP address of this address space.

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Link aggregation**.

5. Enter the following values under **Network**:

> **NOTE:** The network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

Name:	Enter the name of the network interface group.
Operating mode:	Select the operating mode for grouped network interfaces: ▪ **Off:** Disable link aggregation. *Go to »Interfaces« to configure the network interfaces (see Configuring the network interfaces on page 16 ff.).* ▪ **Static IPv4:** A static IPv4 address is assigned. ▪ **DHCPv4:** Obtain IPv4 address from a DHCP server.
IPv4 address:	Enter the IPv4 address of the interface (only when operating mode *Static IPv4* is selected).
Netmask:	Enter the netmask of the network (only when operating mode *Static IPv4* is selected).
IPv6:	Click the toggle switch to enable IPv6 (green/right = enabled). **NOTE:** When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user. Click the toggle switch to disable IPv6 (grey/left = disabled (*default*)).
IPv6 address:	Enter the static IPv6 address of the interface.
Subnet prefix length:	Specify the prefix length (*default*: 64) for the interface according to the notation rules defined in RFC 5952.

6. Enter the following values under **Parameter**:

Primary Follower:	Select whether data traffic should preferably be transmitted via the interface *Network A* (**Interface A**) or the interface *Network B* (**Interface B**). As soon as the selected interface is available, this interface is used for data traffic. If you select the option **None**, the data traffic is sent via any interface. A switch-over occurs only if the active interface fails.
Link monitoring:	Select whether you want to use the **MII** or the **ARP** mode (see explanation above) to monitor the interface.
MII down delay:	Waiting period in milliseconds before a failed network interface is disabled. The entered value must be a multiple of 100 ms (the MII link monitoring frequency).
MII up delay:	Waiting period in milliseconds before a reset network interface is activated. The entered value must be a multiple of 100 ms (the MII link monitoring frequency).
ARP interval:	Enter the interval (100 to 10,000 milliseconds) after which the system checks for incoming ARP packets of the network interfaces.
ARP validate:	The validation ensures that the ARP packet for a particular network interface has been generated by one of the specified ARP targets. Select whether or which of the incoming ARP packets should be validated: ▪ **None:** ARP packets are not validated (default). ▪ **Active:** Only the ARP packets of the active network interface are validated. ▪ **Backup:** Only the ARP packets of the inactive network interface are validated ▪ **All:** The ARP packets of all network interfaces of the group are validated.
ARP target:	The table contains a list of all configured ARP targets. Use the buttons **New**, **Edit** and **Delete** to manage the ARP targets.

7. Click on **Save**.

Reading out the status of the network interfaces

The current status of both network interfaces can be read out in the web application.

How to detect the status of the network interfaces:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Information**.
4. Go to the paragraph **Link status**.
5. The paragraphs **Interface A** and **Interface B** include the following values:

> **NOTE:** The network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

Link detected:	Connection to the network established (**yes**) or interrupted (**no**).
Auto-negotiation:	Both the transmission speed and the duplex method have been configured automatically (**yes**) or manually by the administrator (**no**).
Speed:	Transmission speed
Duplex:	Duplex mode (**full** or **half**)

6. Click on **Save**.

Creating and administrating netfilter rules

By default, all network computers have access to the web application *ConfigPanel* (open system access).

NOTE: The open system access allows unrestricted connections via ports 80/TCP (HTTP), 443/TCP (HTTPS) and 161/UDP (SNMP).

Once a netfilter rule has been created, open system access is disabled and all incoming data packets are compared with the netfilter rules. The list of netfilter rules is processed in the stored order. As soon as a rule applies, the corresponding action is executed and the following rules are ignored.

NOTE: As soon as a netfilter rule is used, the *Default DROP policy* takes effect.

If *certain* IP addresses are to be accepted, it is sufficient to assign the *Accept* filter rule to them. Data packets via *all* other IP addresses are not processed (*"dropped"*) due to the *Default DROP policy*.

IMPORTANT: If data packets are only not to be processed (*"dropped"*) via *certain* IP addresses, the *Drop* filter rule must be assigned to these IP addresses. The *Accept* filter rule must then be assigned to the IP addresses that are to be accepted, as further data packets via other IP addresses will otherwise also not be processed (*"dropped"*) due to the *Default DROP policy*. If all other IP addresses are to be accepted, the *Accept* rule can be applied to *all* IP addresses (**0.0.0.0/0**).

Creating new netfilter rules

How to create a new netfilter rule:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Netfilter**.

5. Enter the following values:

Interface:	In the pull-down menu, select on which network interfaces the data packets are to be intercepted and manipulated: ▪ **All** ▪ **Interface A** ▪ **Interface B** ▪ **Link-Aggregation group**
Option:	In the pull-down menu, select how to interpret the sender information of the rule: ▪ **Normal:** The rule applies to data packets whose sender information corresponds to the IP address or MAC address specified in the rule. ▪ **Inverted:** The rule applies to data packets whose sender information does *not* correspond to the IP address or MAC address specified in the rule.
IP address/ Prefix length:	Enter the IP address of the host or, by specifying the **Prefix length**, define the network segment. **Examples IPv4:** ▪ **192.168.150.187/32:** for IP address 192.168.150.187 If only an IP address is entered without specifying a prefix length, the system will automatically apply / **32** as the prefix in the background. ▪ **192.168.150.0/24:** IP addresses of section 192.168.150.x ▪ **192.168.0.0/16:** IP addresses of section 192.168.x.x ▪ **192.0.0.0/8:** IP addresses of section 192.x.x.x ▪ **0.0.0.0/0:** all IPv4 addresses **Examples IPv6:** ▪ **2001:db8::222:4dff:fe84:3cb6/128:** Only this IP address If only an IP address is entered without specific a prefix length, the system will automatically apply / **128** as the prefix in the background. ▪ **fe80::/64:** all link local IP addresses ▪ **2001:db8::/64:** IP addresses of space 2001:db8::/64 ▪ **::/0:** all IPv6 addresses **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule. **NOTE:** Enter link local IPv6 addresses here without a zone ID, if applicable.
MAC address:	Enter the MAC address to be considered in this filter rule. **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.

Filter rule:	▪ **Drop:** Data packets whose sender information matches the IP address or MAC address are not processed. ▪ **Accept:** Data packets whose sender information matches the IP address or MAC address are processed.
Service:	Select a specific service for which this rule is used exclusively, or choose (**All**).

6. Click on **Add** to save the values in a new filter rule.

   The new filter rule is added to the end of the list of existing filter rules.

7. Click on **Save**.

NOTE: The new nefilter rule is not applied to active connections. Restart the device if you want to disconnect the active connections and then apply all the rules.

Editing existing netfilter rules

How to edit an existing netfilter rule:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Netfilter**.
5. In the list of existing netfilter rules, select the rule you want to change.

6. The current rule settings are displayed in the upper part of the dialog. Check and change the following settings.

Interface:	In the pull-down menu, select on which network interfaces the data packets are to be intercepted and manipulated: ▪ **All** ▪ **Interface A** ▪ **Interface B** ▪ **Link-Aggregation group**
Option:	In the pull-down menu, select how to interpret the sender information of the rule: ▪ **Normal:** The rule applies to data packets whose sender information corresponds to the IP address or MAC address specified in the rule. ▪ **Inverted:** The rule applies to data packets whose sender information does *not* correspond to the IP address or MAC address specified in the rule.
IP address/ Prefix length:	Enter the IP address of the host or, by specifying the **Prefix length**, define the network segment. **Examples IPv4:** ▪ **192.168.150.187/32:** for IP address 192.168.150.187 If only an IP address is entered without specifying a prefix length, the system will automatically apply **/32** as the prefix in the background. ▪ **192.168.150.0/24:** IP addresses of section 192.168.150.x ▪ **192.168.0.0/16:** IP addresses of section 192.168.x.x ▪ **192.0.0.0/8:** IP addresses of section 192.x.x.x ▪ **0.0.0.0/0:** all IPv4 addresses **Examples IPv6:** ▪ **2001:db8::222:4dff:fe84:3cb6/128:** Only this IP address If only an IP address is entered without specific a prefix length, the system will automatically apply **/128** as the prefix in the background. ▪ **fe80::/64:** all link local IP addresses ▪ **2001:db8::/64:** IP addresses of space 2001:db8::/64 ▪ **::/0:** all IPv6 addresses **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule. **NOTE:** Enter link local IPv6 addresses here without a zone ID, if applicable.
MAC address:	Enter the MAC address to be considered in this filter rule. **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.

Filter rule:	▪ **Drop:** Data packets whose sender information matches the IP address or MAC address are not processed. ▪ **Accept:** Data packets whose sender information matches the IP address or MAC address are processed.
Service:	Select a specific service for which this rule is used exclusively, or choose (**All**).

7. Click on **Apply** to save your settings.
8. Click on **Save**.

NOTE: The new nefilter rule is not applied to active connections. Restart the device if you want to disconnect the active connections and then apply all the rules.

Deleting existing netfilter rules

How to delete existing netfilter rules:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Netfilter**.
5. In the list of existing netfilter rules, select the rule you want to delete.
6. Click on **Delete**.
7. Confirm the confirmation prompt by clicking on **Yes** or cancel the process by clicking on **No**.
8. Click on **Save**.

Changing the order or priority of existing netfilter rules

The list of netfilter rules is processed in the stored order. As soon as a rule applies, the corresponding action is executed and the following rules are ignored.

IMPORTANT: Pay attention to the order or priority of the individual rules, especially when adding new rules.

How to change the order or priority of existing netfilter rules:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Netfilter**.
5. In the list of existing netfilter rules, select the rule whose order/priority you want to change.
6. Click the button **Arrow up** to increase the priority or the button **Arrow down** to decrease the priority.
7. Click on **Save**.

Creating an SSL certificate

Use the free implementation of the SSL/TLS protocol *OpenSSL* to create an SSL certificate.

IMPORTANT: For security reasons, network certificates for the web application (see page 30 ff.) and, if used, additional user certificates for the KVM connection are **not** included in a backup and may have to be stored again after a restore.

The following websites provide detailed information about operating OpenSSL:

- OpenSSL project: **https://www.openssl.org/**
- Win32 OpenSSL: **http://www.slproweb.com/products/Win32OpenSSL.html**

IMPORTANT: Creating an SSL certificate requires the software OpenSSL. If necessary, follow the instructions on the websites mentioned above to install the software.

The instructions on the following pages explain *exemplarily* how to create an SSL certificate.

In principle, a certificate is created in 5 steps:

1. Creating a Private Key
2. Creating a Certificate Signing Request (CSR)
3. Submitting the CSR to the CA
4. Receiving the certificate from the CA
5. Creating the PEM file

Special features for complex KVM systems

If different G&D devices are to communicate with each other within a KVM system, the identical *Certificate Authority* (see page 31) must be used when creating certificates for these devices.

Alternatively, the identical PEM file (see page 35) can also be used for all devices. Inthis case, all characteristics of the certificates are identical.

Creating a Certificate Authority

A *Certificate Authority* enables the owner to create digital certificates (e. g. for a matrix switch.

How to create a key for the Certificate Authority:

> **IMPORTANT:** The following steps describe how to create keys that are not coded. If necessary, read the OpenSSL manual to learn how to create a coded key.

1. Enter the following command into the command prompt and press **Enter**:

```
openssl genrsa -out ca.key 4096
```

2. OpenSSL creates the key and stores it in a file named *ca.key*.

How to create the Certificate Authority:

1. Enter the following command into the command prompt and press **Enter**:

```
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

2. Now, OpenSSL queries the data to be integrated into the certificate.

   The following table shows the different fields and an exemplary entry:

Field	Example
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (e.g., city)	Siegen
Organization Name (e.g., company)	Guntermann & Drunck GmbH
Organizational Unit Name (e.g., section)	
Common Name (e.g., YOUR name)	Guntermann & Drunck GmbH
Email Address	

IMPORTANT: The device's IP address must not be entered under *Common Name*.

   Enter the data you want to state, and confirm each entry by pressing **Enter**.

3. OpenSSL creates the key and stores it in a file named *ca.crt*.

IMPORTANT: Distribute the certificate *ca.crt* to the web browsers using the web application. The certificate checks the validity and the trust of the certificate stored in the device.

Creating any certificate

How to create a key for the certificate to be created:

> **IMPORTANT:** The following steps describe how to create keys that are not coded. If necessary, read the OpenSSL manual to learn how to create a coded key.

1. Enter the following command into the command prompt and press **Enter**:

```
openssl genrsa -out server.key 4096
```

2. OpenSSL creates the key and stores it in a file named *server.key*.

How to create the certificate request:

1. Enter the following command into the command prompt and press **Enter**:

```
openssl req -new -key server.key -out server.csr
```

2. Now, OpenSSL queries the data to be integrated into the certificate.

   The following table shows the different fields and an exemplary entry:

Field	Example
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (e.g., city)	Siegen
Organization Name (e.g., company)	Guntermann & Drunck GmbH
Organizational Unit Name (e.g., section)	
Common Name (e.g., YOUR name)	192.168.0.10
Email Address	

> **IMPORTANT:** Enter the IP address of the device on which the certificate is to be installed into the row *Common Name*.

   Enter the data you want to state, and confirm each entry by pressing **Enter**.

3. If desired, the *Challenge Password* can be defined. This password is needed if you have lost the secret key and the certificate needs to be recalled.

4. Now, the certificate is created and stored in a file named *server.csr*.

Creating and signing an X509 certificate

1. Enter the following command into the command prompt and press **Enter**:

```
openssl req -x509 -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
```

2. OpenSSL creates the certificate and stores it in a file named *server.crt*.

IMPORTANT: If you do not create the certificats as explained in the previous sections, but use your own certificates with certificate extensions, the command to be entered must be adapted or extended accordingly.

EXAMPLE: If you use *Extended Key Usage* to restrict the permitted use of the key, at least the *serverAuth* and *clientAuth* extensions must be activated or taken into account:

```
openssl req -x509 -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt -addext 'extendedKeyUsage = serverAuth, clientAuth'
```

ADVICE: To check which certificate extensions are used, use:

```
openssl x509 -text -in ca.crt
```

Creating a PEM file

NOTE: The *.pem* file contains the following three components:

- server certificate
- private server key
- certificate of the certification authority

If these three components are available separately, enter them successively to the *Clear text* entry before updating the certificate stored in the device.

1. Enter the following command(s) into the prompt and press **Enter**:

   a. Linux

   ```
   cat server.crt > gdcd.pem
   cat server.key >> gdcd.pem
   cat ca.crt >> gdcd.pem
   ```

   b. Windows

   ```
   copy server.crt + server.key + ca.crt gdcd.pem
   ```

2. The *gdcd.pem* file is created while copying. It contains the created certificate and its key as well as the *Certificate Authority*.

Selecting an SSL certificate

By default, each G&D device with integrated web application stores at least one SSL certificate. The certificate has two functions:

- The connection between web browser and web application can be established via an SSL-secured connection. In this case, the SSL certificate allows the user to authenticate the opposite side.

  If the device's IP address does not match the IP address stored in the certificate, the web browser sends a warning message.

  ADVICE: You can import a user certificate so that the device's IP address matches the IP address stored in the certificate.

- The communication between G&D devices within a system is secured via the devices' certificates.

  IMPORTANT: Communication between devices is possible only if all devices within a KVM system use certificates of the same *Certificate Authority* (see page 31).

How to select the SSL certificate you want to use:

IMPORTANT: After activating *another* certificate, close the currently active »Config Panel« sessions and start new sessions.

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Certificate**.

5. Select the certificate you want to use:

G&D certificate #1:	This certificate is enabled for *new* devices. **NOTE:** Make sure that you use the same certificate for all devices within the KVM system.
G&D certificate #2:	This certificate is supported by some older G&D devices with integrated web application.
User certificate:	Select this option if you want to use a certificate purchased from a certificate authority or if you want to use a user certificate. Now you can import and upload the certificate: ▪ Click on **Import certificate from file** and use the file dialog to select the .pem file you want to import. You can also copy the plain text of the server certificate, the server's private key and the certificate of the certificate authority to the text box. ▪ Click on **Upload and activate** to store and activate the imported certificate for the device.

6. Click on **Save**.

IMPORTANT: For security reasons, network certificates for the web application (see page 30 ff.) and, if used, additional user certificates for the KVM connection are **not** included in a backup and may have to be stored again after a restore.

Firmware update

The firmware of each device of the KVM system can be updated via the web application.

Firmware update of a single device

IMPORTANT: This function only updates the firmware of the device on which the web application was started.

How to execute a firmware update of a single device:

1. In the menu, click on **DWCs**.
2. Click on the device you want to update.
3. Open the menu **Service tools** and select the entry **Firmware update**.
4. Click on **Supply firmware image files**.

   NOTE: If the firmware file is already available in the internal storage, you can skip this step.

   Select the firmware file on your local disk and click on **Open**.

   NOTE: Multiple selection of firmware files is possible by simultaneously pressing the **Shift** or **Ctrl** key and the left mouse button.

   The firmware file is transferred to the internal storage and can then be selected for the update.
5. Select the firmware files to be used from the internal storage and click on **Continue**.
6. Select the **Intended version** of the devices if you selected more than one firmware files for one device.
7. Move the **Update** slider to the right (green) in the rows of all devices to be updated.
8. Click on **Start update**.

IMPORTANT: Do **not** close the browser session while the device is being updated! Do **not** turn off the product or disconnect it from the power supply during the update.

Firmware update of multiple KVM system devices

How to execute a firmware update of multiple KVM system devices:

1. In the menu, click on **System**.
2. Click on **System update**.
3. Select the devices whose firmware you want to update and click **Firmware update**.

   NOTE: For devices for which a firmware update is currently not possible, the reason for this is displayed in the **Status** field.

4. Click on **Supply firmware image files**.

   NOTE: If the firmware file is already in the internal storage, you can skip this step.

   Select the firmware file on your local disk and click **Open**.

   NOTE: Multiple selection of firmware files is possible by simultaneously pressing the **Shift** or **Ctrl** key and the left mouse button.

   The firmware file is transferred to the internal storage and can then be selected for the update.
5. Select the firmware files to be used from the internal storage and click **Continue**.
6. Select the **Intended version** of the devices if you selected more than one firmware files for one device.
7. Move the **Update** slider to the right (green) in the rows of all devices to be updated.
8. Click on **Start update**.

NOTE: In order to ensure the transfer of updates to the end devices for larger data volumes, the end devices are updated in groups as required.

IMPORTANT: Do **not** close the browser session while the devices are being updated! Do **not** turn off the products or disconnect them from the power supply during the update.

Restoring the system defaults

With this function, the system defaults of the device on which the web application is operated can be restored.

How to restore the system defaults:

1. In the menu, click on **System**.
2. Click on **System defaults**.
3. Select the scope of the recovery:

Reset all settings:	Reset all settings of the device.
Reset only local network settings:	Reset only local network settings.
Reset only KVM application settings:	Reset all settings except the local network settings.

4. Click on **Set system defaults**.

Restarting the device

This function restarts the device. Before restarting, you will be prompted for confirmation to prevent an accidental restart.

How to restart the device using the web application:

1. In the menu, click on **DWCs**.
2. Click on the desired device.
3. Open the menu **Service tools** and select the entry **Restart**.
4. Confirm the confirmation prompt with **Restart**.

Network functions of the devices

The devices within the KVM system provide *separate* network functions.

The following functions can be configured for each device within the KVM system:

- Authentication against directory services (LDAP, Active Directory, RADIUS)
- Time synchronisation via NTP server
- Forwarding of log messages to syslog servers
- Monitoring and control of computers and network devices via *Simple Network Management Protocol* (see page 55 ff.)

NTP server

The date and time of a device can be set either automatically by time synchronization with an NTP server (*Network Time Protocol*) or manually.

Time sync with an NTP server

How to change the NTP time sync settings:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.

4. Go to the paragraph **NTP server** and enter the following values:

General	
NTP time sync:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the time synchronization: ▪ **Disabled** (*default*) ▪ **Enabled**
Time zone:	Use the pull-down menu to select the time zone of your location.
NTP server 1	
Address:	Enter the IP address of a time server.
Authentication:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the authentication: ▪ **Disabled** (*default*) ▪ **SHA1**
Key ID:	After enabling the authentication, enter the key ID that can be used for key authentication with the NTP server.
Key:	Enter the key in the form of up to 40 hex digits.
NTP server 2	
Address:	O*ptionally* enter the IP address of a second time server.
Authentication:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the authentication: ▪ **Disabled** (*default*) ▪ **SHA1**
Key ID:	After enabling the authentication, enter the key ID that can be used for key authentication with the NTP server.
Key:	Enter the key in the form of up to 40 hex digits.

5. Click on **Save**.

Manual setting of time and date

How to manually set the time and date of the device:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **NTP server**.

> **IMPORTANT:** If necessary, disable the **NTP time sync** option. Otherwise, you might not be able to set time and date manually.

5. Go to the entry **Time** under **Time/date** to enter the current time (*hh:mm:ss*).
6. Go to the entry **Date** under **Time/date** to enter the current time (*DD.MM.YYYY)*.

> **ADVICE:** Click on **Accept local date** to copy the current system date of the computer on which the web application was opened to the *Time* and *Date* fields.

7. Click on **Save**.

Logging syslog messages

The syslog protocol is used to transmit log messages in networks. The log messages are transmitted to a syslog server that logs the log messages of many devices in the computer network.

Among other things, eight different severity codes have been defined to classify the log messages:

- **0:** Emergency
- **1:** Alert
- **2:** Critical
- **3:** Error
- **4:** Warning
- **5:** Note
- **6:** Info
- **7:** Debug

The web application enables you to configure whether the syslog messages are to be locally logged or sent to up to two syslog servers.

EXAMPLE: When using severity code 6 (*default*), the following events are logged with time stamp (ISO8601) and other information, for example:

- User login: Which user has logged on to which device and is the user already logged on to another device (usercount N)
- Login failure: An incorrect login attempt was made on which device (even when using severity level 5)
- User rights change: Which user has made a change to rights via which device
- (Auto)backup failure: For which device has an (auto)backup failed (even when using severity level 3)

NOTE: The selected severity and all lower severity levels are logged.

Local logging of syslog messages

How to locally log syslog messages:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Syslog** enter the following data under **Syslog local**:

Syslog local:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the local logging of syslog messages: ▪ **Disabled** ▪ **Enabled** (*default*)
Log level:	In this pull-down menu, select the severity from which a log message is to be logged (*Default*: 6 - Info). The selected severity and all lower severity levels are logged.

If you select the severity *2 - Critical*, messages for this code as well as for the severity levels *1 - Alert* and *0 - Emergency* are logged.

5. Click on **Save**.

Sending syslog messages to a server

How to send syslog messages to a server:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Syslog** and enter the following values under **Syslog server 1** or **Syslog server 2**:

Syslog server:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the sending of syslog messages to a server: ▪ **Disabled** (*default*) ▪ **Enabled**
Log level:	In this pull-down menu, select the severity level from which a log message is to be logged. The selected severity level and all lower severity levels are logged. If you select the severity *2 - Critical*, messages for this code as well as for the severity levels *1 - Alert* and *0 - Emergency* are logged.
IP address/ DNS name:	Enter the IP address or the FQDN of the destination server for the syslog messages.
Port:	Enter the port - usually 514 - on which the syslog server accepts incoming messages.
Protocol:	Select the protocol - usually UDP - on which the syslog server accepts incoming messages: ▪ **TCP** ▪ **UDP**

5. Click on **Save**.

Viewing and saving local syslog messages

If the function to log the local syslog messages is activated, these syslog messages can be viewed and, if necessary, stored in the information dailog.

How to view and store local syslog messages:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure.
3. Open the menu **Service tools** and select the entry **Syslog**.
4. Click on **Retrieve syslog**.

   The local syslog messages are now retrieved and displayed in the text field.

   ADVICE: Click on **Save syslog** to save the messages in a text file.

5. Click on the red **[X]** to close the window.

User authentication with directory services

In internal corporate networks, user accounts are often managed centrally by a directory service. The device can access such a directory service and authenticate users against the directory service.

NOTE: If the directory service fails to authenticate the user account *Admin*, the user account is authenticated against the database of the device.

The directory service is used exclusively to authenticate a user. Rights are granted by the database of the KVM system. The following paragraphs describe the different scenarios:

- **The user account exists in the directory service and in the KVM system**
  The user can log on with the password stored in the directory service. After a successful login, the rights of the account with the same name are assigned to the user in the KVM system.

  NOTE: The password with which the user has successfully logged on is transferred to the database of the KVM system.

- **The user account exists in the directory service, but not in the KVM system**
  A user who has been successfully authenticated against the directory service but does not have an account of the same name in the KVM system's database will be granted the rights of a *RemoteAuth* user.
  If required, change the rights of this particular user account to set the rights for users without a user account.

> **ADVICE:** Deactivate the *RemoteAuth* user to prevent users without user accounts to log on to the KVM system.

- **The user account exists in the KVM system, but not in the directory service**
  If the directory service is available, it reports that the user account does not exist. Access to the KVM system is denied to the user.
  If the server is not available but the fallback mechanism is activated, the user can log on with the password stored in the KVM system.

> **IMPORTANT:** In order to prevent the logon of a user locked or deactivated in the directory service when the connection to the directory service fails, please observe the following security rules:
> - If a user account is deactivated or deleted in the directory service, this action must also be carried out in the user database of the KVM system!
> - Activate the fallback mechanism only in exceptional cases.

> **IMPORTANT:** When using two-factor authentication
> (see *Setting up two-factor authentication on the device (optional)* on page 50),
> the fallback mechanism **cannot** be used.

How to configure the authentication of user accounts:

> **NOTE:** If no directory service is used, the user accounts are managed by the device.

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **Authentication**.

5. Enter the following values under **Authentication service**:

Authentication server: Select the **Local** option if the user administration is to be carried out by the KVM system.

If you want to use a certain external directory service, select the corresponding entry from the pull-down menu:

- **LDAP**
- **Active Directory**
- **Radius**

After selecting a external directory service, enter the settings of the directory service server in the corresponding dialog box.

NOTE: User names can be subject to a naming convention when using external directory services (see *Creating a new user account* on page 64).

ADVICE: When using *LDAP* or *Active Directory*, enter the path from which the respective search should be started in the **Base DN/SearchScope** field. This saves time and prevents an unnecessarily long search.

Fallback: Activate this option if you want to use the local user administration of the KVM system if the directory service is temporarily unavailable.

IMPORTANT: In order to prevent the logon of a user locked or deactivated in the directory service when the connection to the directory service fails, please observe the following security rules:

- If a user account is deactivated or deleted in the directory service, this action must also be carried out in the user database of the KVM system!
- Activate the fallback mechanism only in exceptional cases.

IMPORTANT: When using two-factor authentication, the fallback mechanism **cannot** be used
(see *Setting up two-factor authentication on the device (optional)* on page 50).

6. Click on **Save**.

Setting up two-factor authentication on the device (optional)

Standard user authentication involves querying a password. To provide a greater level of security, optional two-factor authentication (2FA) can be used to query a second factor based on a device in the user's possession. 2FA makes use of a time-based one-time password (TOTP). Authenticator apps or hardware tokens can be used.

To enable use of 2FA, support for it must first be activated on the relevant device.

IMPORTANT: If you no longer have access to your possession-based factor or if it is broken, you will lose access to the system. Take precautions by, for example, keeping the emergency codes in a safe place if you are using the internal OTP server and configuring settings that will minimise the risk of losing access (see *Activating two-factor authentication* on page 65).

How to activate 2FA on the device:

1. In the menu, click on **DWCs**.
2. Double-click the device that is to be configured.
3. Click on the tab **Network**.
4. Select the section **2-factor authentication (2FA)**.

5. In the sector 2-factor authentication, enter the following data:

2FA support:	▪ **Disabled** (*default*) ▪ **Enabled**
OTP server:	Select the option **Internal** (*default*), if you will be using an authentication server that is provided in the device. If you want to use a specific external directory service, select the corresponding entry from the pull-down menu: ▪ **LDAP** ▪ **Active Directory** ▪ **Radius** Once you have selected a directory service, enter the settings for the directory service server in the dialogue screen that opens.
Login only for users with configured 2FA:	If the internal OTP server is used, you can specify whether login for users without activated 2FA will permitted (*default*) or prevented. This option can be used to set up a transition period for setting up the OTPs, for example. ▪ **No** (*default*) ▪ **Yes**

NOTE: Note that usernames may be subject to a naming convention if a directory service is used (see *Creating a new user account* on page 64).

IMPORTANT: If an external directory service is used, the second factor will be required for **every** user profile on login.

6. Click on **Save**.

IMPORTANT: Use time sync with an NTP server (see page 41). Alternatively, you can set the time and date manually (see page 43).

Information on activating two-factor authentication is provided on page 65.

Monitoring functions

Under **DWCs** and **System monitoring** you can view the monitoring values of any devices connected to the KVM system.

The following exemplary figure shows the monitoring values *Status*, *Main power* and *Temperature* of a device:

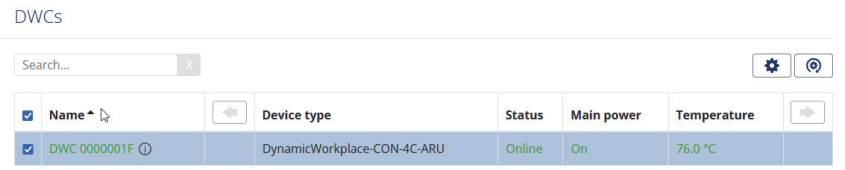


Figure 4: Detailed view of an exemplary monitoring table

The values configured for the table view (see *Configuring table columns* on page 8) are listed in the table.

You can see immediately from the colour whether the status is correct (green) or critical (red). The text displayed in the column also provides information about the current status.

Viewing all monitoring values

You can see the list of all monitoring values under **DWCs**.

How to show a list of all monitoring values:

1. In the menu, click on **DWCs**.
2. Click on the device you want to check and then click on **Configuration**.
3. Click on the tab **Monitoring**.

   The displayed table contains a list of all available monitoring values.
4. Click on **Close**.

Enabling/disabling monitoring values

You can switch each monitoring value on and off *separately* or you can switch all monitoring values on or off *together*.

Deactivated monitoring values are *not* displayed in the web application.

IMPORTANT: The web application does *not* give any warnings about deactivated monitoring values and does also *not* send any SNMP traps for these values.

How to enable/disable an *individual* monitoring value:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Monitoring**.
4. Turn the slider in the column **Enabled** of the desired monitoring value to the right (enabled) or to the left (disabled).
5. Click on **Save**.

How to enable/disable *all* monitoring values:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Monitoring**.
4. Mark or unmark the **Enabled** checkbox in the column header to switch all values on or off.
5. Click on **Save**.

Advanced features for managing critical devices

The **Monitoring status** icon (see *User interface* on page 6) shows you at a glance whether all monitoring values are within the normal range (green icon) or if at least one monitoring value is outside the normal range (yellow or red icon).

The *Monitoring status* icon always takes the colour of the *most critical* monitoring value

Displaying the list of critical monitoring values

If the **Monitoring status** icon is displayed in yellow or red, you can access the **Active alarms** dialog by clicking on the icon.

The *Active alarms* dialog shows any critical values.

Confirm the alarm of a critical device

Many alarm messages require immediate action by the administrator. Other alarms (for example, the failure of the redundant power supply), on the other hand, indicate possibly uncritical circumstances.

In such a case, you can confirm the alarm message of a value. The value is thus downgraded from **Alarm** (red) to **Warning** (yellow).

How to acknowledge the monitoring message of a device:

1. Click on the red **Monitoring status** icon at the top right.
2. Select the alarm you want to acknowledge.
3. Click on **Confirm**.

Monitoring devices via SNMP

The *Simple Network Management Protocol* (SNMP) is used to monitor and control computers and network devices.

Practical use of the SNMP protocol

A *Network Management System* (NMS) is used to monitor and control computers and network devices. The system queries and collects data from the *agents* of the monitored devices.

IMPORTANT: Chinese and Cyrillic characters are not supported by many network management systems.

Therefore, make sure that the passwords you use do not contain such characters!

NOTE: An *agent* is a program that runs on the monitored device and determines its status. The determined data is transmitted to the *Network Management System* via SNMP.

If an *agent* detects a serious event on the device, it can automatically send a *trap* packet to the *Network Management System*. This ensures that the administrator is informed about the event at short notice.

Configuring an SNMP agent

How to configure an SNMP agent:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **SNMP agent**.

5. Enter the following values under *Global*:

Status:	Select the particular entry to either switch the SNMP agent off (**Disabled**) or on (**Enabled**).
Protocol:	Select the protocol (**TCP** or **UDP**) – usually UDP – to be used to transmit the SNMP packets.
Port:	Define the port – usually 161 – on which the *incoming* SNMP packets are to be accepted.
SysContact:	Enter the admin's contact data (e.g. direct dial or e-mail address).
SysName:	Enter the device name.
SysLocation:	Enter the location of the device.

6. If you want to process packets of protocol version **SNMPv2c,** enter the data listed on the following page in the section with the same name.

Access:	Activate read access (**View**), write access (**Full**) or deny access (**No**) via the *SNMPv2c* protocol.
Source IPv4:	Enter the IP address of the host or the network segment from which SNMP packets should be received. **Examples:** ▪ **192.168.150.187/32:** Only IP address 192.168.150.187 ▪ **192.168.150.0/24:** IP addresses of space 192.168.150.x ▪ **192.168.0.0/16:** IP addresses of space 192.168.x.x ▪ **192.0.0.0/8:** IP addresses of space 192.x.x.x
Read-only community:	Enter the name of the *Community* which has also been selected in the *Network Management System*.

IMPORTANT: The password (*Community*) of the packages of protocol version *SNMPv2c* is transmitted unencrypted and can therefore be easily tapped.

If necessary, use the protocol version *SNMPv3* (see below) and a high *security level* to ensure secure data transmission.

7. If you want to process packets of protocol version **SNMPv3c,** enter the data in the section with the same name:

Access:	Activate read access (**View**) or deny access (**No**) via the *SNMPv3c* protocol.
User:	Enter the username for the communication with the *Network Management System*.
Authentication protocol:	Select the authentication protocol which has been activated in the *Network Management System*: ▪ **SHA-1** ▪ **SHA-224** ▪ **SHA-256** ▪ **SHA-384** ▪ **SHA-512** (*default*) ▪ **MD5** **NOTE:** As it is now known that **MD5** does not offer collision resistance it is not recommended to use it.
Authentication passphrase:	Enter the authentication passphrase for the communication with the *Network Management System*.
Security level:	Select one of the following options: ▪ **NoAuthNoPriv:** user authentication and *Privacy* protocol deactivated ▪ **AuthNoPriv:** user authentication activated, *Privacy* protocol deactivated ▪ **AuthPriv:** user authentication and *Privacy* protocol activated
Privacy protocol:	Select the privacy protocol which has been activated in the *Network Management System*: ▪ **AES128** ▪ **AES192** ▪ **AES256** (*default*) ▪ **DES.** **NOTE:** Due to the short key length of **DES**, its use is not recommended.
Privacy passphrase:	Enter the privacy passphrase for secure communication with the *Network Management System*.

Engine ID method:	Select how the **SnmpEngineID** should be assigned: ▪ **Random:** The *SnmpEngineID* is re-assigned with every restart of the device. ▪ **Fix:** The *SnmpEngineID* is the same as the MAC address of the device's network interface. ▪ **User:** The string entered under *Engine ID* is used as *SnmpEngineID*.
Engine ID:	When using the *Engine ID method* **User**, enter the string that is used as *Engine ID*.

8. Click on **Save**.

Adding and Configuring SNMP traps

How to add a new trap or edit an existing trap:

1. In the menu, click on **DWCs**.
2. Click on the tab **Network**.
3. Go to the paragraph **SNMP trap**.
4. Click on **Add** or on **Edit**.
5. Enter the followng values under **Global**:

Server:	Enter the IP address of the *Network Management Server*.
Protocol:	Select the protocol (**TCP** or **UDP**) – usually UDP – to be used to transmit the SNMP packets.
Port:	Enter the port – usually 162 – on which *outgoing* SNMP packets are transmitted.
Retries:	Enter the number of retries to send an *SNMP Inform*. **NOTE:** Inputs are only possible if the *Inform* option is selected in the *Notification type* field.
Timeout:	Enter the timeout (in seconds) after which an *SNMP Inform* will be resent if no confirmation is received. **NOTE:** Inputs are only possible if the *Inform* option is selected in the field *Notification type*.

Log level:	Select the severity of an event from which an SNMP trap is to be sent. The selected severity and all lower severity levels are logged. **NOTE:** If you select the severity *2 - Critical*, SNMP traps will be sent for events of this severity level as well as for events of the severity levels *1 - Alert* and *0 - Emergency*.
Version:	Select if the traps are to be created and sent according to the *SNMPv2c* (**v2c**) or *SNMPv3* (**v3**) protocol.
Notification type:	Select if events are sent as *Trap* or *Inform* packet. **NOTE:** Inform packets require a confirmation of the Network Management System. If this confirmation is not available, transmission is repeated.

6. If you selected protocol version **SNMPv2c** in the last step, enter the name of the *Community*, which was also selected in the *Network Management System*.

IMPORTANT: The password (*Community*) of the packages of protocol version *SNMPv2c* is transmitted unencrypted and can therefore be easily tapped.

If necessary, use the protocol version *SNMPv3* (see below) and a high *security level* to ensure secure data transmission.

7. If you selected protocol version **SNMPv3** in step 5, enter the following data in the section with the same name:

Username:	Enter the username for the communication with the *Network Management System*.
Authentication protocol:	Select the authentication protocol which has been activated in the *Network Management System*: ▪ **SHA-1** ▪ **SHA-224** ▪ **SHA-256** ▪ **SHA-384** ▪ **SHA-512** ▪ **MD5** (*default*) **NOTE:** As it is now known that **MD5** does not offer collision resistance it is not recommended to use it.
Authentication passphrase:	Enter the authentication passphrase for secure communication with the *Network Management System*.

Security level:	Select one of the following options: ▪ **NoAuthNoPriv:** user authentication and *Privacy* protocol deactivated ▪ **AuthNoPriv:** user authentication activated, *Privacy* protocol deactivated ▪ **AuthPriv:** user authentication and *Privacy* protocol activated
Privacy protocol:	Select the privacy protocol which has been activated in the *Network Management System*: ▪ **AES128** ▪ **AES192** ▪ **AES256** ▪ **DES** (*default*). **NOTE:** Due to the short key length of **DES**, its use is not recommended.
Privacy passphrase:	Enter the privacy passphrase for secure communication with the *Network Management System*.
Engine ID:	Enter the *Engine ID* of the trap receiver.

8. Click on **Save**.

How to delete an existing trap:

1. In the menu, click on **DWCs**.
2. Click on the tab **Network**.
3. Go to the paragraph **SNMP trap**.
4. In the row of the receiver you want to delete, click on **Delete**.
5. Click on **Save**.

Users and groups

Efficient rights administration

The web application administrates up to 1,024 user accounts as well as the same amount of user groups. Any user within the system can be a member of up to 20 groups.

User accounts and user groups can be provided with different rights to operate the system.

ADVICE: Rights administration can be carried out almost completely through user groups. Therefore, user groups and the assigned rights have to be planned and implemented beforehand.

This way, user rights can be changed quickly and efficiently.

The effective right

The effective right determines the right for a particular operation.

IMPORTANT: The effective right is the maximum right, which consists of the user account's individual right and the rights of the assigned group(s).

EXAMPLE: The user *JDoe* is member of the groups *Office* and *ComputerModuleConfig*.

The following table shows the user account rights, the rights of the assigned groups and the resulting effective right:

Right	User *JDoe*	Group *Office*	Group *ComputerModuleConfig*	Effective right
Config Panel Login	No	No	**Yes**	**Yes**
Change own password	No	**Yes**	No	**Yes**
Confirm monitoring alert	**Yes**	No	No	**Yes**

The settings of the *Config Panel Login* and *Change own password* rights result from the rights assigned to the user groups. The *Confirm monitoring alert* right is given directly in the user account.

The dialogue windows of the web application additionally display the effective right for every setting.

ADVICE: Click on the **i** button to get a list of the groups and rights assigned to the user account.

Efficient user group administration

User groups let you create a shared right profile for multiple users with identical rights. Furthermore, any user accounts included in the member list can be grouped and therefore no longer have to be individually configured. This facilitates the rights administration within the system.

If the rights administration takes place within user groups, the user profile only stores general data and user-related settings (key combinations, language settings, …).

When initiating the system, it is recommended to create different groups for users with different rights (e. g. »*Office*« and »*IT*«) and assign the respective user accounts to these groups.

EXAMPLE: Create more groups if you want to divide the user rights even further. If, for example, you want to provide some users of the »*Office*« group with the *Confirm monitoring alert* right, you can create a user group for these users:

- Create a user group (e. g., »*Office_monitoring*«) with identical settings for the »*Office*« group. The *Confirm monitoring alert* right is set to *Yes*. Assign the respective user accounts to this group.
- Create a user group (e. g., »*Monitoring*«) and set only the *Confirm monitoring alert* right to *Yes*. In addition to the »*Office*« group, also assign the respective user accounts to this group.

In both cases, the user is provided with the *Yes* effective right for *Confirm monitoring alert*.

ADVICE: The user profile lets you provide extended rights to a group member.

Administrating user accounts

User accounts let you define individual rights for every user. The personal profile also provides the possibility to define user-related settings (see *Overview of user-related settings (Personal profile)* on page 71).

IMPORTANT: The administrator and any user assigned with the *Superuser* right are permitted to create and delete user accounts and edit rights and user-related settings.

Creating a new user account

The web application manages up to 1,024 user accounts. Each user account has individual login data, rights and user-specific settings for the KVM system.

IMPORTANT: If an individual password policy is to be taken into account, you must configure the password complexity (see *Password complexity* on page 13) before creating a new user account.

How to create a new user account:

1. In the menu, click on **User**.
2. Click on **Add user**.
3. Enter the following values in the dialog box:

Name:	Enter a user name.
	NOTE: User names can be subject to a naming convention when using external directory services (see *User authentication with directory services* on page 47 ff.).
Password:	Enter the user account password.
Confirm password:	Repeat the password.
Clear text:	If necessary, mark this entry to view and check both passwords.
Full name:	If desired, enter the user's full name.
Comment:	If desired, enter a comment regarding the user account.
Enabled:	Mark this checkbox to activate the user account.
	NOTE: If the user account is deactivated, the user is not able to access the KVM system.

4. Click on **Save**.

IMPORTANT: After the user account has been created, it does not have any rights within the KVM system.

5. If two-factor authentication is activated on the device (see page 50), the settings for the user account must be made in the next step (see page 65).

Activating two-factor authentication

NOTE: To use two-factor authentication, it first needs to be set up on the device (see page 50).

If the internal OTP server is used for 2FA, it can be activated for almost any user profile (exception: user *RemoteAuth*). To generate the security key for activation, various controlling parameters are used in addition to the key itself, which can be generated automatically. The key and the controlling parameters can be modified by the user. This is necessary for setting up hardware tokens. If authenticator apps are used, the parameters do not generally need to be modified.

IMPORTANT: If an external directory service is used (see *Setting up two-factor authentication on the device (optional)* on page 50 ff.), 2FA is activated automatically for each user profile in the database. This means that login from the device is only possible if the external OTP server has identical user profiles and the second factor is validated successfully.

IMPORTANT: To activate or deactivate 2FA for a user profile, the user needs superuser rights (see page 78), or the user must be logged in with the corresponding user profile (see page 78) and have the right *Change own password* (see page 79).

IMPORTANT: Use time sync with an NTP server (see page 41). Alternatively, you can set the time and date manually (see page 43).

NOTE: 2FA can be activated for almost all user profiles. The only exception is the user *RemoteAuth*.

How to activate 2FA in the user account:

1. In the menu, click on **User**.
2. Click on the user account that is to be configured and then click on **Configuration**.
3. Click on **Edit** in the line **2-factor authentication**.
4. Select **Enabled** in the section **2FA for this user**.
5. Enter the following data in the menu:

Encryption key:	When the parameter **2FA for this user** is changed from **Disabled** to **Enabled**, a encryption key is generated and displayed automatically. **IMPORTANT: Base32 format** must be used for the entry. Click on **Generate** to obtain a new encryption key.
Hash algorithm:	▪ **SHA1** ▪ **SHA256** (*default*) ▪ **SHA512**
Validity period (secs):	Enter how long the 2-Factor Auth Code (TOTP) should remain valid. The value entered must be between **10** and **200** seconds (*default*: 30 seconds). **ADVICE:** It is a good idea to avoid selecting a validity period that is too short, as access problems could otherwise occur if the time is not synchronised correctly.
Length of 2-Factor Auth Code (TOTP):	▪ **6 digits** (*default*) ▪ **8 digits**
2-Factor Auth Code (TOTP) window width:	The window width specifies how many previous 2-Factor Auth Codes (TOTP) are valid in addition to the current one. It is **not** possible to allow future 2-Factor Auth Codes (TOTP). The value entered must be between **1** and **20** (*default*: 1). **ADVICE:** To avoid access problems from occurring as the result of the time not being synchronised correctly, it can be a good idea to permit several previous 2-Factor Auth Codes (TOTP).
Show QR code & copy security key:	Clicking the button validates the entries that have been made. A security key is generated and a QR code is displayed that contains the generated security key and that can be used to scan in with an authenticator app. The security key is copied to the clipboard.
Verification code:	Enter a verification code here that you receive from a hardware token or an authenticator app that you are using. Only numbers can be entered in this field.

6. Click on **Save**.

IMPORTANT: Following successful activation of 2FA, it the internal OTP server is used, the additional button **Emergency codes** is displayed in the line **2-factor authentication**. If you click this button, five emergency codes will be displayed. Each of these emergency codes enables a user account to be accessed **once** only. These codes are **not** limited to a specific time period. The codes should be kept in a safe place. The emergency codes can be used, for example, if a hardware token is lost to enable continued access to the system.

Click on **Get new codes** to create five new codes.

NOTE: A user who has been successfully authenticated against the directory service but who does not have an account with the same name in the database of the KVM system will be given the rights of the user *RemoteAuth*.

The 2-Factor Auth Code (TOTP) is validated by the configured external OTP server.

Change the rights of this special user account to configure the rights of users without their own account (see *Changing the user account rights* on page 70).

Deactivate the user *RemoteAuth* to prevent users from logging in to the KVM system without their own user acoount (see *Enabling or disabling a user account* on page 73).

Once 2FA has been activated in the user acoount, the 2-Factor Auth Code (TOTP) will be queried in addition to the username and password on login (see *Starting the web application* on page 4).

Renaming a user account

How to change the name of a user account:

1. In the menu, click on **User**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Enter the username under **Name**.
4. *Optional:* Enter the user's full name under **Full name**
5. Click on **Save**.

NOTE: User names can be subject to a naming convention when using external directory services (see *User authentication with directory services* on page 47 ff.).

Changing the password of a user account

NOTE: The activated *Superuser* right
(see *Rights for unrestricted access to the system (Superuser)* on page 78 ff.)
or the right *Change own password*
(see *Rights to change your own password* on page 79 ff.)
are prerequisite for changing the password of a user account.

NOTE: When changing the password, any defined password policies
(see *Password complexity* on page 13) are taken into account.

How to change the password of a user account:

1. In the menu, click on **Users**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Change the following values in the dialog box:

Current password:	Enter the current password.
	NOTE: No entry is required in this field for users with activated superuser rights (see page 78 ff.).
New password:	Enter the new password.
Confirm new password:	Repeat the new password.
Clear text:	Mark this entry to view and check entered passwords.
Verification code:	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.
	NOTE: The 2-Factor Auth Code (TOTP) is only requested if two-factor authentication has been configured (see page 50 f.) and activated (see page 65 ff.).

4. Click on **Save**.

Changing the user account rights

Any user account can be assigned with different rights.

The following table lists the different user rights. Further information on the rights can be found on the indicated pages.

System rights

Name	Right	Page
Superuser right	Unrestricted access to the configuration of the system	page 78
Config Panel Login	Login to the *ConfigPanel* web application	page 78
Change own password	Change own password	page 79
Confirm monitoring alert	Confirmation of a monitoring alarm	page 79

Overview of user-related settings (Personal profile)

The following table provides an overview of the user-related settings. It additionally lists the *default* settings and references to detailed descriptions of the functions.

Personal profile	Field name	Page
Changing the password of a user account	New password	69
Language settings	Language	10

Changing a user account's group membership

NOTE: Any user within the system can be a member of up to 20 user groups.

How to change a user account's group membership:

1. In the menu, click on **User**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Click on the **Membership** tab.
4. In the **Members** column, turn the slider of the group to which you want to add the user to the right (enabled).

   ADVICE: If necessary, use the *Search* field to limit the number of user groups to be displayed in the selection window.

5. In the **Members** column, turn the slider of the group from which the user is to be removed to the left in the (disabled).

   ADVICE: If necessary, use the *Search* field to limit the number of user groups to be displayed in the selection window.

6. Click on **Save**.

Enabling or disabling a user account

IMPORTANT: If a user account is disabled, the user has no access to the KVM system.

How to enable or disable a user account:

1. In the menu, click on **User**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Mark the check box **Enabled** to activate the user account.

   If you want to block access to the system with this user account, unmark the checkbox.
4. Click on **Save**.

Deleting a user account

How to delete a user account:

1. In the menu, click on **User**.
2. Click on the user account you want to delete and then click on **Delete**.
3. Confirm the confirmation prompt by clicking on **Yes** or cancel the process by clicking on **No**.

Administrating user groups

User groups enable the user to create a common rights profile for several users with the same rights and to add user accounts as members of this group.

This way, the rights of these user accounts do not have to be individually configured, which facilitates the rights administration within the KVM system.

NOTE: The administrator and any user with the *Superuser* right are authorised to create and delete user groups as well as edit the rights and the member list.

Creating a new user group

The user can create up to 1,024 user groups within the system.

How to create a new user group:

1. In the menu, click on **User groups**.
2. Click on **Add user group**.
3. Enter the following values in the dialog box:

Name:	Enter the username.
Comment:	If desired, enter a comment regarding the user account.
Enabled:	Mark this checkbox to activate the user account.

NOTE: If the user group is disabled, the group rights do *not* apply to the assigned members.

4. Click on **Save**.

IMPORTANT: Directly after the new user group has been created, it contains no rights within the system

Renaming a user group

How to rename a user group:

1. In the menu, click on **User groups**.
2. Click on the user group you want to configure and then click on **Configuration**.
3. Enter the group name under **Name**.
4. Click on **Save**.

Changing the user group rights

The various user groups can be assigned with different rights.

The following table lists the different user rights. Further information about the rights is given on the indicated pages.

System rights

Name	Right	Page
Superuser right	Unrestricted access to the configuration of the system	page 78
Config Panel Login	Login to the *ConfigPanel* web application	page 78
Change own password	Change own password	page 79
Confirm monitoring alert	Confirmation of a monitoring alarm	page 79

Administrating user group members

How to administrate user group members:

1. In the menu, click on **User groups**.
2. Click on the user group you want to configure and then click on **Configuration**.
3. Click on the **Members** tab.
4. In the **Members** column, click on the slider of the users you want to add to the group (enabled).

   ADVICE: If necessary, use the *Search* field to limit the number of users to be displayed in the selection window.

5. In the **Members** column, click on the slider of the users you want to delete from the group (disabled).

   ADVICE: If necessary, use the *Search* field to limit the number of users to be displayed in the selection window.

6. Click on **Save**.

(De)activating a user group

How to (de)activate a user group:

1. In the menu, click on **User groups**.
2. Click on the user group you want to configure and then click on **Configuration**.
3. Activate the **Enabled** slider to activate the user group.

   If you want to lock the access to the KVM system for members of this user group, deactivate the checkbox.

4. Click on **Save**.

Deleting a user group

How to delete a user group:

1. In the menu, click on **User groups**.
2. Click on the user group you want to delete and then click on **Delete**.
3. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

System rights

Rights for unrestricted access to the system (Superuser)

The *Superuser* right allows a user unrestricted access to the configuration of the KVM system.

NOTE: The information about the user's previously assigned rights remains stored when the *Superuser* right is activated and is reactivated when the right is revoked.

How to assign a user account with unrestricted access to the system:

1. In the menu, click on **User** or **User groups**.
2. Click on the user account or the user group you want to configure and then click on **Configuration**.
3. Click on the tab **System rights**.
4. Under **Superuser right**, select between the following options:

Activated:	Allow full access to the KVM system and the connected devices
Deactivated:	Deny full access to the KVM system and the connected devices

5. Click on **Save**.

Changing the login right to the web application

How to change the login right to the web application:

1. In the menu, click on **User** or **User groups**.
2. Click on the user account or the user group you want to configure and then click on **Configuration**.
3. Click on the tab **System rights.**
4. Under **Config Panel Login**, select between the following options:

Activated:	Allow access to web application
Deactivated:	Deny access to web application

5. Click on **Save**.

Rights to change your own password

How to change the right to change your own password:

1. In the menu, click on **User** or **User groups**.
2. Click on the user account or the user group you want to configure and then click on **Configuration**.
3. Click on the tab **System rights**.
4. Under **Change own password**, select between the following options:

Activated:	Allow users to change their own password
Deactivated:	Deny users the right to change their own password

5. Click on **Save**.

Authorization to confirm a monitoring alarm

How to change the authorization to confirm a monitoring alarm:

1. In the menu, click on **User** or **User groups**.
2. Click on the user account or the user group you want to configure and then click on **Configuration**.
3. Click on the tab **System rights**.
4. Under Confirm monitoring alert, select between the following options:

Activated:	Confirmation of monitoring alarms allowed
Deactivated:	Confirmation of monitoring alarms denied

5. Click on **Save**.

Advanced functions of the KVM system

Identifying a device by activating the Identification LED

Some devices provide an *Identification* LED.

Use the web application to switch the device LEDs on or off in order to identify the devices in a rack, for example.

How to (de)activate the *Identification* LED of a device:

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure.
3. Open the menu **Service tools** and select the entry **Ident LED**.
4. Click on **LED on** or **LED off**.
5. Click on the red **[X]** to close the window.

Saving the configurations

The backup function lets you save your configurations. You can reset your configurations with the restore function.

How to save the configuration of the KVM system:

1. In the menu, click on **System**.
2. Click on **Backup & restore**.
3. Click the **Backup** tab.
4. *Optional:* Enter a **Password** to secure the backup file or a **Comment**.
5. Select the scope of data you want to back up: You can back up either the **network settings** and/or the **application settings**.
6. Click **Backup**.

IMPORTANT: For security reasons, network certificates for the web application and, if used, additional user certificates for the KVM connection are **not** included in a backup and may have to be stored again after a restore.

Saving the configurations with auto backup function

The device can save an automatic backup on a network drive at a defined interval. This means that you do not have to make a manual backup after a configuration option has been changed. You can reset your configurations with the restore function.

How to use the auto backup function:

1. In the menu, click on **System**.
2. Click on **Auto Backup**.
3. Enter the following data:

Auto Backup:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the auto backup function: ▪ **Disabled** (*default*) ▪ **Enabled**
Filename prefix:	Enter the filename prefix. **ADVICE:** When the auto backup function is enabled, the filename prefix field is automatically filled with the **UID** of the device. You can change this entry. **IMPORTANT:** Only letters (upper and lower case), numbers (*0* to *9*) and the characters - and _ are permitted. The prefix may contain a maximum of 25 characters.
Backup password:	*Optional*: Enter a password to secure the backup file. **IMPORTANT:** Double inverted commas („ and “) cannot be used here.
Backup scope:	Select the scope of data you want to back up: You can back up either the **network settings** and/or the **application settings**.

Path:	Enter the path for the backup files. **IMPORTANT:** The syntax of the path depends on the selected protocol. When using the **NFS** protocol, the URL format defined in RFC 2224 must be used – taking into account the general URL notation specified in RFC 3986. When using the **CIFS** protocol, the URL format must follow RFC 3986. Contrary to the specifications in RFC 2224 and RFC 3986, the protocol, port, username, and password must not be included in the path parameter. These values are taken exclusively from the separate parameters: **Protocol**, **Port**, **User**, and **Password**. **Examples:** ▪ **NFS:** *name:/directory1/directory2* ▪ **CIFS:** *//name/directory1/directory2*
Protocol:	Choose between the following protocols: ▪ **NFS** (*default*) ▪ **CIFS**
Port:	Enter the port. This field is filled automatically depending on the selection in the *protocol* field: ▪ **2049** (when selected *NFS*) ▪ **445** (when selected *CIFS*)
User:	*Optional:* Enter the name of the user.
Password:	*Optional:* Enter a password to secure the share.
Time:	Enter the following data: ▪ **Hour** (numbers *0* to *23*) ▪ **Minute** (numbers *0* to *59*)
Selection of the day:	You can choose between the following options: ▪ **1.** to **31. day of the month** ▪ **Select all** (every day of the month)

4. Click on **Save & Test** or **Save**.

> **ADVICE:** Use **Save & Test** and check whether a backup was successfully saved with the desired parameters.

> **IMPORTANT:** You can see whether the test was successful in the syslog messages (see *Logging syslog messages* on page 44 ff.).

IMPORTANT: For security reasons, network certificates for the web application and, if used, additional user certificates for the KVM connection are **not** included in a backup and may have to be stored again after a restore.

Restoring the configurations

How to restore the configuration of the KVM system:

1. In the menu, click on **System**.
2. Click on **Backup & restore**.
3. Click on **Restore** tab.
4. Click **Select file** and open a previously created backup file.
5. Use the information given under **Creation date** and **Comment** to check if you selected the right backup file.
6. Select the scope of data you want to restore: You can restore either the **network settings** and/or the **Application settings**.

   NOTE: If one of these options cannot be selected, the data for this option was not stored.

   NOTE: If a password was entered when the data was saved, it is requested here.

7. Click **Restore**.

IMPORTANT: For security reasons, network certificates for the web application and, if used, additional user certificates for the KVM connection are **not** included in a backup and may have to be stored again after a restore.

Activating premium functions

With every purchase of a premium function, you receive a feature key. This file contains a key to activate the purchased function(s).

The premium function(s) is/are activated by importing this key to the web application.

How to import a feature key to activate the purchased function(s):

1. In the menu, click on **DWCs**.
2. Click on the device you want to configure.
3. Open the menu **Service tools** and select the entry **Features**.
4. Click on **Import feature key from file...** and import the feature key (file) via the file interface.

   After the file is loaded, the clear text of the feature key is displayed in the text field.

   NOTE: The clear text of the feature key can also be copied into the text field.

5. Click on **Save**.

2 DWCs

You can configure the settings of the DynamicWorkplace-CONs (DWC) and view the device's status information in the web application's *DynamicWorkplace-CONs* menu.

Basic configuration of DWCs

Changing the name of a DWC

How to change the name of a DWC:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. Enter the name of the DWC in the **Name** field of the **Device** section.
4. Click on **Save**.

Changing the comment of a DWC

The list field of the web application displays the name of a DWC as well as the comment entered.

> **ADVICE:** For example, use the comment field to note the location of the DWC.

How to change the comment of a DWC:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. Enter a comment in the **Comment** field of the **Device** section.
4. Click on **Save**.

Configuration settings of DWCs

Device configuration

Selecting the active counterpart

How to select the active counpterpart:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. The table in the *Possible counterparts* section lists the possible devices. Select the device by sliding the slider to the *right* (**on**).
4. Click on **Save**.

Adding counterparts manually

How to add counterparts manually:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. Click on **Add manually** in the *Possible counterparts* section.
4. Enter the UID of the device to be added.
5. Click on the green **check mark** ( ) to save your settings or click on the red **Discard** button ( ).

Removing counterparts

How to remove manually added counterparts:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. In the *Possible counterparts* section, click on the UID of the device you want to remove.
4. Click on **Remove**.

Advanced features for DWCs

Copying the config settings (Replace device)

If a DWC is replaced by another DWC, the previous config settings can be copied to the new device. After the config settings have been copied to the new device, it can be operated immediately.

IMPORTANT: After this task is carried out, the DWC whose settings you want to copy is deleted from the KVM system.

How to copy target module config settings:

1. In the menu, click on **DWCs**.
2. Click on the *new* device.
3. Open the menu **Service tools** and select the entry **Replace device**.
4. Choose the *old* device whose configuration settings you want to copy.
5. Click on **Save**.

Configuring monitoring values

In the *Monitoring* section, you can define values to be monitored and check the status of these values.

Selecting the values to be monitored

By default, the KVM system monitors a variety of DWCs values. If required, you can limit the evaluation and monitoring of properties.

How to manage the values to be monitored:

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. Click on the tab **Monitoring**.
4. Enable or disable individual monitoring values by sliding the slider to the *left* (**off**) or to the *right* (**on**).

   ADVICE: In order to enable or disable *all* values you can use the check box in the header of the **Enabled** column.

5. Click on **Save**.

Viewing status information of a DWC

Using the configuration menu of a DWC, you can open a window displaying different status information.

How to view the status information of a DWC

1. In the menu, click on **DWCs**.
2. Click on the DWC and then click on **Configuration**.
3. Click on **Information**.
4. The following information is displayed in the dialog box that opens now:

DynamicWorkplace-CON	
Name:	Name of the DWC
Device ID:	Physical ID of the DWC
Status:	Current status (**online** or **offline**) of the DWC
Class:	Device class of the DWC

Hardware information	
Firmware name:	Firmware name
Firmware rev.:	Firmware version
Hardware rev.:	Hardware revision
IP address A:	IP address of *Network A* interface
IP address B:	IP address of *Network B* interface
MAC A:	MAC address of *Network A* interface
MAC B:	MAC address of *Network B* interface
Serial number	Serial number of the DWC

Link status Interface A	
Link detected:	Connection to the network established (**yes**) or interrupted (**no**).
	NOTE: The following information is only displayed for CAT variants.
Auto-negotiation:	The transmission speed and the duplex method have been configured automatically (**yes**) or manually by the administrator(**no**).
Speed:	Transmission speed
Duplex	Duplex method (**full** or **half**)

Link status Interface B	
Link detected:	Connection to the network established (**yes**) or interrupted (**no**).
	NOTE: The following information is only displayed for CAT variants.
Auto-negotiation:	The transmission speed and the duplex method have been configured automatically (**yes**) or manually by the administrator(**no**).
Speed:	Transmission speed
Duplex	Duplex method (**full** or **half**)

NOTE: In addition, the *monitoring* information of the device is displayed.

5. Click on **Close** to close the window.

NOTES

NOTES

NOTES

G&D. Control what you see.

Headquarters | Hauptsitz

Guntermann & Drunck GmbH Systementwicklung

Obere Leimbach 9 | D-57074 Siegen | Phone +49 271 23872-0
sales@gdsys.com | www.gdsys.com

US Office

G&D North America Inc.
4540 Kendrick Plaza Drive | Suite 100
Houston, TX 77032 | United States
Phone +1-346-620-4362
sales.us@gdsys.com

Middle East Office

Guntermann & Drunck GmbH
Dubai Studio City | DSC Tower
12th Floor, Office 1208 | Dubai, UAE
Phone +971 4 5586178
sales.me@gdsys.com

APAC Office

Guntermann & Drunck GmbH
60 Anson Road #17-01
Singapore 079914
Phone +65 9685 8807
sales.apac@gdsys.com