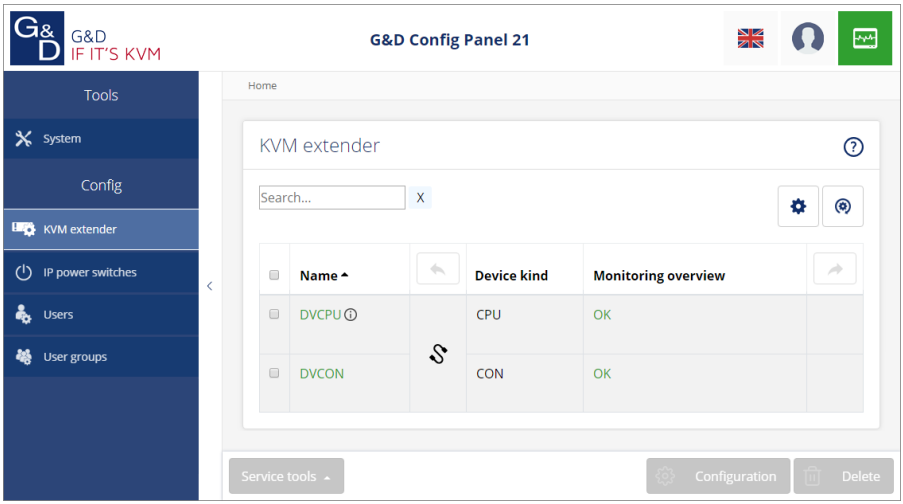
G&D DP1.2-VisionXG



EN

Web Application »Config Panel«

Configuring the KVM extender

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.

Version 2.00 – 10/05/2019
Config Panel 21 version: 1.1.001

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

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

http://www.gdsys.de
sales@gdsys.de

Table of contents

Chapter 1: Basic functions

Chapter 2: KVM extenders

1 Basic functions

The *ConfigPanel* web application provides a graphical user interface to configure the matrix switches of the KVM system. The application can be operated from any supported web browser (see page 5).

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 the web application can be started via the web browser of a computer, the device from which the web application is loaded must first be connected to the local network (see installation instructions).

If not already done, adjust the network settings described on page 6.

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

- Apple Safari 12
- Google Chrome 74
- Internet Explorer 11
- Microsoft Edge 44
- Mozilla Firefox 66

Supported operating systems

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

Recommended resolutions

- A minimum resolution of 1366 × 768 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 **DHCP**
- global network settings: settings obtained using **DHCP**

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 13 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 5.

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:

Username:	Enter a username.
Password:	Enter a password for your user account.

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 47).

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

- **Username:** Admin
- **Password:** 4658

3. Click on **Login**.

Operating the web application

User interface

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

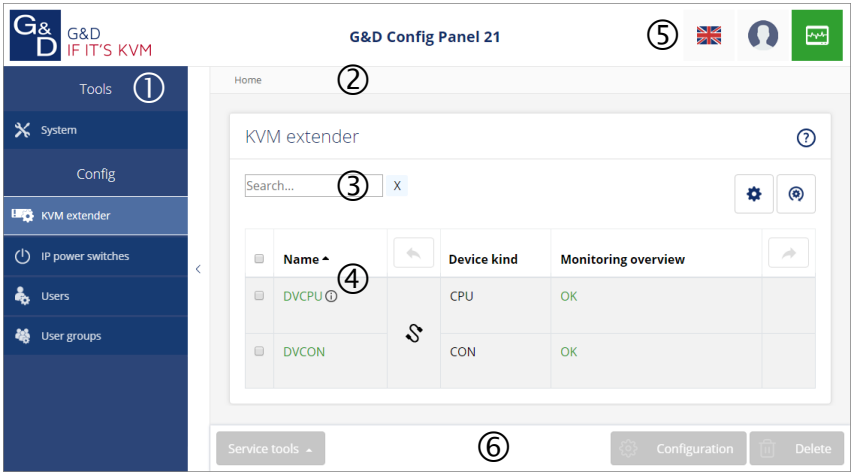


Figure 1: User interface of the web application

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 country flag shows the language currently active in the web application. Click on the country flag to switch between languages (*German/English*). A submenu opens displaying all supported languages in the form of flags. Switch the language by clicking on the desired flag. **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, ...)
Switch:	When selecting a KVM switch in the main view, you can use this submenu to switch the active KVM channel.
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 **KVM extender** and **Users** to your requirements.

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

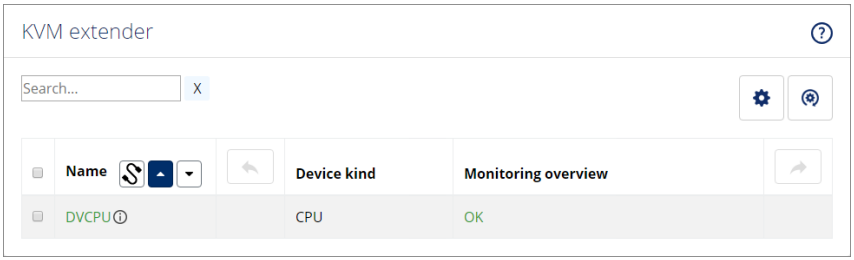


Figure 2: Table columns (default) of a KVM extender

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**.

Selecting the language of the web application

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.

How to change the default language of the web application:

1. Click on the **country flag** at the top right.

   A submenu opens displaying all supported languages in the form of flags.

2. Change the language by clicking on the desired **flag**.

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

Showing the version number of the web application

How to show the version number of the web application:

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

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 6.

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 *network interface A*:
  192.168.0.1
- IP address of *network interface B*:
  Obtain address via **DHCP**
- Global network settings:
  Obtain settings via **DHCP**

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.

1. In the menu, click on **KVM extender**.
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**:

Operating mode:	Select the operational mode of **Interface A** or **Interface B**: ▪ **Off:** Disable network interface. ▪ **Static:** A static IP address is assigned. ▪ **DHCP:** ▪Obtain IP 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«.
IP address:	Enter the IP address of the interface (only when operating mode *Static* is selected).
Netmask:	Enter the netmask of the network (only when operating mode *Static* is selected).

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 **KVM extender**.
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 settings**.

5. Enter the following values:

Operating mode:	Select the operating mode: ▪ **Static:** Use static settings. ▪ **DHCP:** Obtain settings from a DHCP server. When selecting the *DHCP* mode, the following settings are applied automatically. It is not possible to enter any vlaues.
Hostname:	Enter the device's hostname.
Domain:	Enter the domain to which the device should belong.
Gateway:	Enter the gateway's IP address.
DNS server 1:	Enter the IP address of the DNS server.
DNS server 2:	Optionally, enter the IP address of another DNS server.

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* überwacht. 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 **KVM extender**.
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**:

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.* ▪ **Static:** A static IP address is assigned. ▪ **DHCP:** Obtain IP address from a DHCP server.
IP address:	Enter the IP address of the interface (only when operating mode *Static* is selected).
Netmask:	Enter the netmask of the network (only when operating mode *Static* is selected).

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

Primary slave:	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 **KVM extender**.
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:

Link detected:	Connection to the network established (**yes**) or disconnected (**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.

Creating new netfilter rules

How to create a new netfilter rule:

1. In the menu, click on **KVM extender**.
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/ Netmask::	Enter the IP address of the data packets or - by using the **Netmask** field - the address space of the IP addresses. **Examples:** ▪ **192.168.150.187:** for IP address 192.168.150.187 ▪ **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 IP addresses **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.
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 **KVM extender**.
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**
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/ Netmask::	Enter the IP address of the data packets or - by using the **Netmask** field - the address space of the IP addresses. **Examples:** ▪ **192.168.150.187:** for IP address 192.168.150.187 ▪ **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 IP addresses **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.
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 **KVM extender**.
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 **KVM extender**.
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.

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 how to create an SSL certificate.

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 23) must be used when creating certificates for these devices.

Alternatively, the identical PEM file (see page 26) 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:

Feld	Beispiel
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 x509 -req -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*.

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 23).

How to select the SSL certificate you want to use:

> **IMPORTANT:** Selecting and activating another certificate terminates all active sessions of the web application.

1. In the menu, click on **KVM extender**.
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. **ADVICE:** Older devices do *not* support **certificate #1**. In this case use **certificate #2** or a **user certificate** within the KVM system.
G&D certificate #2:	This certificate is supported by all 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: 1. 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. 2. Click on **Upload and activate** to store and activate the imported certificate for the device.

3. Click on **OK** to close the window.

Firmware update

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

Firmware update of a single KVM extender

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 KVM extender:

1. In the menu, click on **KVM extender**.
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 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 **target version** of the devices, if you selected more than one firmware files in step 5. 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**.

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**.

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 **target version** of the devices, if you selected more than one firmware files in step 5. 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**.

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 **KVM extender**.
2. Click on the desired device.
3. Open the menu **Service tools** and select the entry **Restart**.
4. Confirm the confirmation prompt with **Yes**.

Network functions of the devices

The different devices within the KVM system (e.g. *KVM extenders* and *KVM matrix switches*) 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, TACACS+)
- 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 41 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 **KVM extender**.
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:

NTP time sync:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the the time synchronization: ▪ **Disabled** ▪ **Enabled**
NTP server 1:	Enter the IP address of a time server.
NTP server 2:	O*ptionally* enter the IP address of a second time server.
Time zone:	Use the pull-down menu to select the time zone of your location.

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 **KVM extender**.
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.

Local logging of syslog messages

How to locally log syslog messages:

1. In the menu, click on **KVM extender**.
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**
Log level:	In this pull-down menu, select the severity from which a log message is to be logged. 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 **KVM extender**.
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** ▪ **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 name of the server to which the syslog messages are to be sent.
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 **KVM extender**.
2. Click on the device you want to configure.
3. Open the menu **Service untility** 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 (see page 35) 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.

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 **KVM extender**.
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 server**:

Auth. 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 directory service, select the corresponding entry from the pull-down menu:

- **LDAP**
- **Active Directory**
- **Radius**
- **TACACS+**

ADVICE: After selecting a directory service, enter the settings of the directory service server in the *Server Settings* section of the dialog box.

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.

6. Click on **Save**.

Monitoring functions

Under **KVM extender** 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:

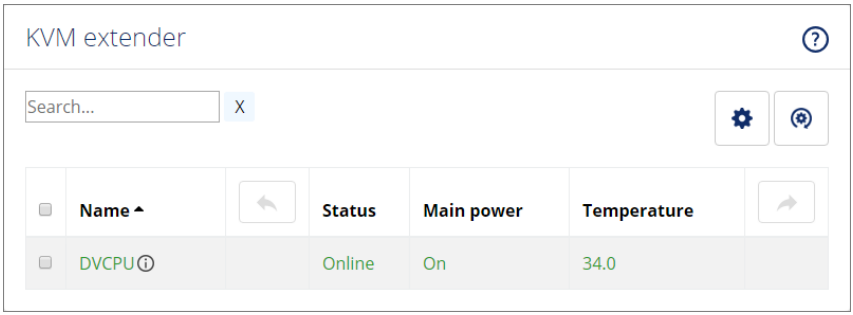


Figure 4: Detailed view of an exemplary monitoring table

The values configured for the table view (see *Configuring table columns* on page 10) 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 KVM extender.

How to show a list of all monitoring values:

1. In the menu, click on **KVM extender**.
2. Click on the device you want to configure 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 **Save**.

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 **KVM extender**.
2. Click on the KVM switch 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 **KVM extender**.
2. Click on the KVM switch 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 8) 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.

Acknowledging 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 acknowledge 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 **Acknowledge**.

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.

> **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 **KVM extender**.
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 followng values under *Global*:

Status:	Select the particular entry to either switch the SNMP agent off (**Off**) 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:	Enter the IP address or the address space of the addresses of incoming SNMP packets. **Examples:** ▪ **192.168.150.187:** 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**), write access (**Full**) 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 (**MD5** or **SHA**) which has been activated in the *Network Management System*.
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 (**DES** or **AES**) which has been activated in the *Network Management System*.
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**.

Configuring SNMP traps

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

1. In the menu, click on **KVM extender**.
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 (**MD5** or **SHA**) which has been activated in the *Network Management System*.
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 (**DES** or **AES**) which has been activated in the *Network Management System*.
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 **KVM extender**.
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

By using user accounts it is possible to assign users with individual rights.

IMPORTANT: The administrator and all users assigned with *superuser* rights are authorized to create and delete users and to edit rights as well as user-related settings.

Creating a new user account

The web application manages up to 256 user accounts. Each user account has individual login data, rights and user-specific settings for the KVM system.

How to create a new user account:

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

Name:	Enter the username.
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.

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.

Renaming a user account

How to change the name of a user account:

1. On the menu, click on **Users**.
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**.

Changing the password of a user account

How to change the password of a user account:

1. On 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:

New password:	Enter the new password.
Confirm password:	Repeat the new password.
Clear text:	Mark this entry to view and check both entered passwords.

4. 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. On 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. On 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**.

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. On the menu, click on **Users**.
2. Click on the user account 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:

Yes:	Allow full access to the KVM system and the connected devices
No:	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. On the menu, click on **Users**.
2. Click on the user account 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:

Yes:	Allow access to web application
No:	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. On the menu, click on **Users**.
2. Click on the user account 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:

Yes:	Allow users to change their own password
No:	Deny users the right to change their own password

5. Click on **Save**.

Advanced functions of the KVM system

Identifying a device by activating the Identification LED

Some devices provide an *Identification* LED on the front panel.

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 **KVM extender**.
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 and restoring the data of the KVM system

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**.

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.

7. Click **Restore**.

2 KVM extenders

You can configure the settings of the KVM extender and view the device's status information in the web application's *KVM extender* menu,.

Basic configuration of KVM extenders

Changing the name of a KVM extender

How to change the name of a KVM extender:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU** or **CON**.
4. Enter the name of the KVM extender in the **Name** field of the **Device** section.
5. Click on **Save**.

Changing the comment of a KVM extender

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

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

How to change the comment of a KVM extender:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU** or **CON**.
4. Enter a comment in the **Comment** field of the **Device** section.
5. Click on **Save**.

Deleting a KVM extender from the KVM system

When the system is not able to find a KVM extender that has previously been integrated into the KVM system, the system assumes that the device is switched off.

When a KVM extender has been permanently removed from the system, you can manually delete it from the list of KVM extenders.

NOTE: You can delete only KVM extenders that have been *switched off*.

How to delete a KVM extender that is switched off or disconnected from the system:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Delete**.
3. Confirm the security prompt by clicking on **Yes** or cancel the process by clicking on **No**.

Configuration settings of KVM extenders

Device configuration

Operating modes of the KVM extender

Depending on the application of the KVM extender, you can select one of the following operating modes:

- **Open Access:** In this mode, access to the KVM extender is *not* protected by authentication.

NOTE: This operating mode is set by default.

You can configure the same access rights for both a KVM extender and a user account.

IMPORTANT: The configured access rights apply to all users working with this KVM extender.

- **Standard:** The standard operating mode allows access to the KVM extender only after users have been authenticated with their username and password.

User rights can be configured in the individual user account.

How to select the operating mode of the KVM extender:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CON**.
4. Under **Operational mode**, you can select between the following options:

Open access console:	Open access mode (*default)*
Standard:	Standard operational mode

5. Click on **OK** to save your settings.

Changing the hotkey modifier key

The hotkey to open the OSD consists of at least one hotkey modifier key and an additional hotkey that you can freely select within a given frame.

NOTE: The default hotkey modifier is set to **Ctrl**.

If many application programs on a computer are operated with key combinations or different KVM devices are used in a cascade, the number of available key combinations may be limited.

If an application program or another device within the cascade uses the same hotkey, you can change the hotkey.

NOTE: Hotkey modifiers can be one key or a combination of the keys *Ctrl*, *Alt*, *Alt Gr*, *Win* or *Shift.*

How to change the hotkey modifier:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU**.

4. In the **Hotkey modifier** field of the **Configuration** section, select *at least* one of the listed modifier keys by marking the corresponding check box:

   - **Ctrl**
   - **Alt**
   - **Alt Gr**
   - **Win**
   - **Shift**

   NOTE: If you selected multiple modifier keys, press them together to trigger the hotkey.

5. Click on **Save**.

Changing the OSD key

The hotkey to open the OSD consists of at least one hotkey modifier key and an additional hotkey that you can freely select within a given frame.

You can change both the hotkey modifier key **Ctrl** and the OSD key **Num**.

How to change the OSD key:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU**.
4. In the **Hotkey** field, select the OSD key to open the on-screen display when pressed together with the hotkey modifier key(s).

   You can choose between the keys *Num, Pause*, *Copy*, *Delete*, *Home*, *End, PgUp*, *PgDn and Space.*

5. Click on **Save**.

Opening the on-screen display by pressing a key twice

As an alternative to opening the on-screen display (OSD) with the key combination **Hotkey+Num** or **Double hotkey+Num**, you can open the OSD by pressing a specific key twice.

How to enable/disable opening the on-screen display by pressing a key twice:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU**.
4. In the **OSD via double keypress** field, you can select between the following options:

Off:	Opening the on-screen display by pressing a key twice disabled (*default*)
Ctrl:	Open OSD by pressing the *Ctrl* key twice
Alt:	Open OSD by pressing the *Alt* key twice
Alt Gr:	Open OSD by pressing the *Alt Gr* key twice
Win:	Open OSD by pressing the *Windows* key twice
Shift:	Open OSD by pressing the *Shift* key twice
Print:	Open OSD by pressing the *Print* key twice
Arrow left	Open OSD by pressing the *Arrow left* key twice
Arrow right	Open OSD by pressing the *Arrow right* key twice
Arrow down	Open OSD by pressing the *Arrow down* key twice
Arrow up	Open OSD by pressing the *Arrow up* key twice

5. Click on **Save**.

Selecting the USB HID mode

The KVM extender supports various USB input devices. Some USB input devices provide special features that you can use after selecting the respective USB keyboard mode.

As an alternative to specific USB keyboard modes, you can use the **Generic HID** mode. In this mode, data from the USB device connected to the upper **Keyb./Mouse** socket of the user module is transferred unchanged to the computer module.

IMPORTANT: The **Generic HID** mode supports many of the HID devices available on the market. However, it is not possible to guarantee the operation of a particular HID device in Generic HID mode.

IMPORTANT: When connecting a USB hub or USB device equipped with multiple USB devices, only the first of the connected HID devices can be used in **Generic HID** mode.

▪ **USB keyboards:** The preset USB keyboard mode **PC Standard** supports the standard keyboard layout.

When using *Apple* or *Sun* keyboards, special keyboard modes let you use the special keys of these keyboards.

The following table lists the supported USB keyboards:

INPUT DEVICE	SETTING
PC keyboard with standard keyboard layout	› PC Standard:
PC keyboard with additional multimedia keys	› Multimedia
Apple keyboard with numeric keypad (A1243)	› Apple A1243

▪ **Displays and tablets:** You can operate the computer connected to the KVM extender with one of the supported *displays* or*tablets*:

INPUT DEVICE	SETTING
HP 2310tk	› HP 2310t
iiyama T1931	› iiyama T1931
NOTTROT N170 KGE	› NOTTROT N170 KGE
Wacom Cintiq 21UX	› Wacom Cintiq 21US
Wacom Intuos3	› Wacom Intuos 3
Wacom Intuos4 S	› Wacom Intuos 4 S
Wacom Intuos4 M	› Wacom Intuos 4 M
Wacom Intuos4 L	› Wacom Intuos 4 L
Wacom Intuos4 XL	› Wacom Intuos 4 XL
Wacom Intuos5 S	› Wacom Intuos 5 S
Wacom Intuos5 M	› Wacom Intuos 5 M
Wacom Intuos5 L	› Wacom Intuos 5 L

▪ **Generic HID mode:** In this mode the data from the USB device connected to the upper **Keyb./Mouse** socket of the user module is transferred unchanged to the computer module.

INPUT DEVICE	SETTING
any USB device	› Generic HID

IMPORTANT: The **Generic HID** mode supports many of the HID devices available on the market. However, it is not possible to guarantee the operation of a particular HID device in Generic HID mode.

- **Controller:** The **ShuttlePRO v2** multimedia controller is used to control various audio and video programs. With a special USB keyboard mode, you can use the controller to operate the computer connected to the target module:

INPUT DEVICE	SETTING
Contour ShuttlePRO v2	‣ Contour Shuttle Pro 2

- **LK463-compatible keyboard:** You can connect an LK463-compatible keyboard to the user module. The arrangement of the 108 keys of such keyboards corresponds to the OpenVMS keyboard layout.

A special USB keyboard mode ensures that the pressing of a special key on this keyboard is transmitted to the target computer:

INPUT DEVICE	SETTING
LK463-compatible keyboard	‣ LK463

How to select a USB HID mode:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU**.
4. Select the desired option under **USB HID mode**.
5. Click on **Save**.

Changing the scancode set of a PS/2 keyboard

When a key on the PS/2 keyboard is pressed, the keyboard processor sends a data packet called scancode. There are two common scancode sets (sets 2 and 3) that contain different scancodes.

By default, the KVM extender interprets all entries of a PS/2 keyboard with scancode set 2.

ADVICE: If the *pipe* ("|") cannot be entered or the arrow keys of the keyboard do not work as expected, it is recommended to switch to scan code set 3.

How to change the setting of the scancode set:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU** if you want to configure the setting of the local workstation (on the **CPU** module).

   Click on the tab **CON** if you want to configure the setting of the remote workstation (on the **CON** module).
5. In the **Scancode set** field of the **Configuration** section, select one of the following options:

Set 2:	Activates scancode set 2 for PS/2 keyboard inputs
Set 3:	Activates scancode set 3 for PS/2 keyboard inputs

6. Click on **Save**.
7. Turn the KVM extender off and back on again.

NOTE: After a restart, the keyboard is initialised and the selected scancode set is applied.

Selecting a keyboard layout for OSD inputs

If the characters displayed on the on-screen display are different from the characters entered on the workstation keyboard, the selected keyboard layout is not correct.

In this case, find out the keyboard layout of the connected keyboard and then configure it in the user module settings.

How to select the keyboard layout of the keyboard connected to the user module:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CON**.

4. In the **Keyboard layout** field, select between the following options:

German (*default*)
English (USA)
English (United Kingdom)
French
Spanish
Lat. American
Portuguese:

5. Click on **Save**.

Reinitialising USB input devices

Once you connect a USB keyboard or mouse to the KVM extender, the input device is initialised and can be used without restrictions.

The USB connection of some USB input devices needs to be reinitialised after a certain time. Activate the automatic reinitialisation of the USB input devices if a USB keyboard or mouse no longer reacts to your inputs during operation.

How to enable/disable reinitialisation of USB input devices:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU** if you want to configure the setting of the local workstation (on the **CPU** module).

   Click on the tab **CON** if you want to configure the setting of the remote workstation (on the **CON** module).
5. In the **USB auto refresh** field, select one of the options listed under **Configuration**:

Off:	The connected USB input devices do not need to be reinitialised.
All devices:	All USB devices are reinitialised regularly.
Only faulty devices:	The status of the USB devices is monitored. If communication to a USB device is disturbed, this device is reinitialised (*default*).

6. Click on **Save**.

Setting the waiting time of the screensaver

You can define a period after which the screensaver switches off the screen display at the workplace when the user is inactive.

NOTE: This setting is independent of the screensaver settings of the computer connected to the computer module.

How to set the waiting time of the screensaver:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU** if you want to configure the screensaver of the local workstation (on the **CPU** module).

   Click on the tab **CON** if you want to configure the screensaver of the remote workstation (on the **CON** module).
5. In the **Screensaver time (minutes)** row, enter the waiting time (1 to 999 minutes) of the screensaver.

   NOTE: Entering the value **0** disables the screensaver.
6. Click on **Save**.

Turn »Fallback compression« on or off

Activate *Fallback compression* if, in the event of a fibre failure, you want to transmit the image data compressed over the remaining active fibres.

How to turn »Fallback compression« on or off:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU**.
5. In the field **Fallback compression**, select one of the following options:

Enabled:	In the event of a fibre failure, the image data is compressed and transmitted via the still active fibers (*default*)
Disabled:	The transmission of the image data is *always* uncompressed.

6. Click on **Save**.

Permission for exclusive access to the workstation

If the user does not make an entry at the active workstation within the specified time period of the automatic input lock (default: 1 second), the KVM extender also allows the other workstation to operate the extender.

If the right for exclusive access to the workstation is activated in the web application, users at this workstation can use the key combination **Hotkey+Print** (default: **Ctrl+Print**) to exclusively operate the KVM extender.

After pressing this key combination, the input devices of the concurrent workstation are deactivated. By pressing the key combination again on the active workstation, both workstations can operate the KVM extender again.

NOTE: After activating the exclusive operation of the KVM extender at a workstation, the *Caps Lock* and the *Num* and *Scroll Lock* LEDs on the keyboard of the locked workstation flash alternately.

The active workstation indicates the exclusive operation of the KVM Extender by the blinking *Scroll Lock* LED.

How to select the right for the exclusive operation of a workstation:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU** if you want to configure the access to the local workstation (on the **CPU** module).

   Click on the tab **CON** if you want to configure the access to the remote workstation (on the **CON** module).
5. In the field **Permanent access mode**, select one of the following options:

Enabled:	Exclusive access permitted (*default*)
Disabled:	Exclusive access denied

6. Click on **Save**.

Changing the video operating mode of workstation

In the standard configuration of the KVM extender, the image of the computer is displayed both on the monitor of the active and on the monitor of the concurrent workstation.

You can also specify that the image of the other workstation is switched off as soon as an entry is made at the other workstation.

The image is displayed again on the other workstation as soon as the user's entries have been completed at the workstation.

How to select the video operating mode of the KVM extender:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General**.
4. Click on the tab **CPU** if you want to configure the video operating mode of the local workstation (on the **CPU** module).

   Click on the tab **CON** if you want to configure the video operating mode of the remote workstation (on the **CON** module).
5. In the field **Image display**, select one of the following options:

Always on (*default*)
Off for action at the remote/local console

6. Click on **Save**.

Changing the time period of the input lock

If input is made at a workstation using the keyboard or mouse, the KVM extender automatically locks the input devices of the concurrent workstation. The lock is released if no further input is made at the active workstation within the set time period of the input lock (default: 1 second).

After the time span of the input lock has expired, the computer can be operated again at both workstations.

You can set the time period of the input lock within the range of 0 to 90 seconds.

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

How to change the time period of the input lock:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **General** and then on the tab **CPU**.
4. Enter the desired time period of the input lock (0 to 90 seconds) in the field **Multiuser input lock**.

   NOTE: Entering the value **0** deactivates the input lock.

5. Click on **Save**.

Changing the exclusive mode action key

After pressing the key combination for the exclusive operation of the extender, the input devices of the concurrent workstation are disabled. By pressing the key combination again on the keyboard of the active workstation, both workstations can operate the KVM extender again.

The shortcut for the exclusive operation consists of at least one hotkey modifier key (see *Changing the OSD key* on page 55) and an additional *exclusive* key that you can freely select within a given frame. You can change both the hotkey modifier key **Ctrl** and the exclusive key **Print**.

How to change the exclusive key:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
1. Click on the tab **General** and then on the tab **CPU**.
2. In the **Exclusive mode actionkey** field, you can select a key:

   You can choose between the keys *Backspace*, *Print*, *Scroll*, *Num*, *Pause*, *Copy*, *Delete*, *Home*, *End*, *PgUp*, *PgDn* and *Space.*

3. Click on **Save**.

Video channel configuration

Reading the EDID profile of a monitor

The EDID information (*Extended Display Identification Data*) of a monitor informs the graphics card of the connected computer about various technical features of the device. The KVM extender usually forwards this information unaltered to the computer via Enhanced-DDC (*Enhanced Display Data Channel*).

However, the EDID profile of a monitor can also be imported and transmitted to one (or more) of the connected computers via the KVM extender.

NOTE: You can import an EDID profile directly from a monitor connected to the KVM extender or from a bin file.

How to import the EDID profile of a connected monitor:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. Click on **New EDID profile**.
6. Click in the **Learn** list box and select the monitor whose EDID information you want to read in.

   NOTE: The **Name** and **Comment** fields of the profile are automatically prefilled and the contents of the EDID information are displayed.

7. Click on **Ok**.
8. If desired, change the information in the fields **Name** and/or **Comment**.
9. Click on **Save**.

How to import the EDID profile of a monitor from a file:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. Click on **New EDID profile**.
6. Click on **Select file**.
7. Select the bin file to be imported from the file dialog and click on **Open**.

> **NOTE:** The **Name** and **Comment** fields of the profile are automatically prefilled and the contents of the EDID information are displayed.

8. If desired, change the information in the fields **Name** and/or **Comment**.
9. Click on **Save**.

Defining the EDID profile of a channel

How to select the EDID profile:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. In the **EDID profile** field of the **Video channel** section, select between the following options:

[Auto]:	automatic handling of EDID data (default)
Profile name:	Selection of an EDID profile previously imported by a user

6. Click on **Save**.

Reducing the colour depth of the image data to be transmitted

By default, the KVM extender transmits the image information to the user module with a maximum colour depth of 24 bit.

When using a high image resolution and displaying moving images, it may happen in exceptional cases that some images are "skipped" at the user module.

In this case, reduce the colour depth of the image data to be transmitted to 18 bit. This can reduce the data volume to be transmitted.

NOTE: Depending on the content of the image, slight colour gradations may occur when reducing the colour depth.

How to reduce the colour depth of image data to be transmitted

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. Select one of the options given under **Color depth**:

24 Bit:	Image data is transmitted with a maximum colour depth of 24 Bit (*default*)
18 Bit:	Colour depth of the image data is reduced to 18 bit.

6. Click on **Save**.

Enabling/disabling DDC/CI support

The computer and user modules supported by the KVM extender is ready to support monitors with **DDC/CI** function.

After the function has been activated, the **DDC/CI**information is transparently forwarded to the monitor to support as many monitors as possible. However, support *cannot* be guaranteed for all monitors.

How to configure DDC/CI transmission of a user module:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.

5. Select one of the options given under **DDC/CI monitor**:

Disabled:	The transmission of DDC/CI signals is disabled (default).
CPU > monitor:	The transmission of DDC/CI signals is exclusively carried out from computer to monitor.
Bidirectional:	The transmission of DDC/CI signals is bidirectional.

6. Click on **Save**.

Use of the Freeze mode

If the cable connection between the computer module and the user module is interrupted during operation, no image is displayed on the monitor of the remote workstation in the standard setting of the KVM Extender.

Activate the *Freeze* mode if you want to display the last image received at the user module in the event of a disconnection until the connection is restored.

In order to visibly signal the disconnection, the last image received is displayed either with a coloured frame and/or the display **Frozen** and the time elapsed since the disconnection.

How to configure the Freeze mode:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. In the **Freeze mode** field, select one of the following options:

Off:	Show no image if the connection is lost (*default*).
On | OSD timer + frame:	Display of a coloured frame in case of a disconnection as well as display of the warning *Frozen* and the time elapsed since the disconnection.
On | OSD timer	Display of the warning *Frozen* and the time elapsed since the disconnection.
On | Frame:	A disconnection is indicated by a coloured frame.

6. Click on **Save**.

Enable/disable »Freeze mode buffer«

NOTE: By default, the *Freeze mode buffer* is enabled.

In *Freeze mode* (see previous section), the buffer ensures that the image is *fully* displayed even if the connection is interrupted. In this mode, the video outputs of various extenders or video channels *are not* synchronized.

If the buffer is **deactivated**, the image may not be *fully displayed* if the connection is interrupted. In this mode, the video outputs of various extenders or video channels are *synchronized*. Therefore, monitors placed in a row or split-screen monitors do not show any visible time lags.

How to turn the »Freeze mode buffer« on or off:

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on the tab **Video channels**.
4. When using a *multi-channel* device, click on the desired video channel and then click on **Configuration**.
5. In the **Freeze mode buffer** field, select one of the following options:

With buffer:	The buffer ensures that the image is *fully displayed* even if the connection is interrupted. In this mode, the video outputs of various extenders or video channels are *not* synchronized (see below).
Without buffer:	Without the buffer, the image may not be *fully displayed* if the connection is interrupted. In this mode, the video outputs of various extenders or video channels are synchronized. Therefore, monitors placed in a row or split-screen monitors do not show any visible time lags.

6. Click on **Save**.

Personal settings

Displaying an information overlay

You can display an information overlay temporarily (5 seconds) in the upper left corner.

ADVICE: If the temporary information overlay is active, you can show the information at any time by pressing the key combination **Ctrl+Caps Lock key**.

You can also set the information overlay to permanent or switch it off.

How to change the colour of the information overlay:

1. In the menu, click on **Users**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Click on the tab **KVM extender systems**.
4. In the **Show OSD info** field, select between the following options:

Off:	Switch off information overlay
Temporary:	Temporary information overlay (5 seconds, *default*)
Permanent:	Permanent information overlay

5. Click on **Save**.

Adjusting the transparency of the on-screen display

By default, the on-screen display (OSD) is displayed with medium transparency on top of the screen contents. The part of the screen that is covered by the OSD shines through the OSD.

You can adjust or disable the transparency level.

How to adjust the transparency level of the on-screen display:

1. In the menu, click on **Users**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Click on the tab **KVM extender systems**.

4. In the **OSD transparency** field, select between the following options:

High:	High transparency of screen contents
Average:	Average transparency of the screen contents (*default*)
Low:	Low transparency of screen contents
Off:	On-screen display covers screen contents

5. Click on **Save**.

Changing the colour of the information overlay

By default, information overlays are displayed in light green, but you can also change the colour.

How to change the colour of the information overlay:

1. In the menu, click on **Users**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Click on the tab **KVM extender systems**.
4. In the **OSD info colour** field, you can select between the following options:

light green:	Display information overlay in light green (default)
black, dark red, green, dark yellow, dark blue, purple, dark turquoise, silver, yellow, blue, magenta, light turquoise or **white**	Display information overlay in the selected colour

5. Click on **Save**.

Enable/disable an automatic OSD timeout

If desired, you can define that the OSD closes automatically after a period of inactivity.

Select a time span between **5** and **99**seconds to define a period of inactivity after which the OSD closes automatically.

> **NOTE:** Entering the value **0** disables the function.

How to change the period of inactivity after which the OSD closes:

1. In the menu, click on **Users**.
2. Click on the user account you want to configure and then click on **Configuration**.
3. Click on the tab **KVM extender systems**.
4. Under **Timeout OSD session**, enter a time span between **5** and **99**seconds.
5. Click on **Save**.

Rights

Right to change the personal profile

How to change the right to change the personal profile:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Change personal profile** field, select one of the following options:

Yes:	Viewing and editing of own user profile allowed
No:	Viewing and editing of own user profile denied

5. Click on **Save**.

Right to view and edit the device configuration

How to change the right to view and edit the device configuration:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Change device configuration** field, select one of the following options:

Yes:	Viewing and editing of device configuration allowed
No:	Viewing and editing of device configuration not allowed

5. Click on **Save**.

Access to USB devices

How to change USB access rights for *all* modules:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Access USB devices** field of the **Global extender rights** section, choose one of the following options:

Yes:	Access to USB devices allowed.
No:	Access to USB devices denied.

5. Click on **Save**.

How to change USB access rights for *a particular* module:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Access USB devices** field of the **Individual rights** section, choose an option for each module listed:

Yes:	Access to USB devices allowed.
No:	Access to USB devices denied.

5. Click on **Save**.

Access rights to a computer module

How to change the access rights to a computer module:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Access** field of the **Individual rights** section, choose an option for each module listed:

Full access (green tick):	Full access to the computer connected to the computer module allowed
No (red prohibition sign)	Access to the computer connected to the computer module denied
View (eye icon):	Screen contents of the computer connected to the computer module can be viewed

5. Click on **Save**.

Right to switch the power sockets of a computer module

How to change the right to switch the power socket(s) assigned to the computer module:

How to change the access rights to a computer module:

1. In the menu, click on **Users** or on **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 **KVM extender systems**.
4. In the **Target power** field of the **Individual rights** section, choose an option for each module listed:

Yes:	Switching of the sockets assigned to the selected computer module permitted
No:	Switching of the sockets assigned to the selected computer module not allowed

5. Click on **Save**.

Advanced features for KVM extenders

Copying the config settings (Replace device)

If a computer or a target module is replaced by another device, 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 target module 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 **KVM extender**.
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 KVM extender's 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 **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on **Monitoring**.

4. Enable or disable individual monitoring values by sliding the slider to the *left* (**off**) or to the *right* (**on**).

> **NOTE:** 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 KVM extender

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

How to view the status information of a KVM extender

1. In the menu, click on **KVM extender**.
2. Click on the KVM extender you want to configure and then click on **Configuration**.
3. Click on **Information**.
4. The following information is displayed in the dialog box that opens now:

KVM extenders	
Name:	Name of the KVM extender
Device ID:	Physical ID of the KVM extender
Status:	Current status (**online** or **offline**) of the KVM extender
Class:	Device class of the KVM extender
Comment:	Comment about the KVM switch entered by a user

Hardware information	
IP address A:	IP address of *Network A* interface
MAC A:	MAC address of *Network A* interface
IP address B:	IP address of *Network B* interface
MAC B:	MAC address of *Network B* interface
Firmware name:	Firmware name
Serial number	Serial number of the KVM switch
Firmware revision:	Firmware version
Hardware revision:	Hardware revision
FPGA revision:	FPGA revision

Link status	
Link detected:	Connection to the network established (**yes**) or interrupted (**no**).
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.

IP Power switch

Applying a compatible IP power switch (**ePowerSwitch 1G R2**, **4M+ R2** und **8M+ R2**) lets you switch the power supply of devices using the KVM extender.

First, connect the power switch to the **Network** interface. Before you can switch the power outlet using the OSD, use the web application to add the power switch to the KVM system. You can use the web application to configure the device, too.

Configuration

Adding a IP power switch to the KVM system

How to add a IP power switch to the KVM system:

1. In the menu, click on **IP power switches**.
1. Click on **Add IP power switch**.
2. Under **Name** you can enter a name for the power switch.
3. If desired, enter a comment for the power switch under **Comment**.
4. Click on **Save**.

Changing name or comment of a IP power switch

How to change the name or comment of a IP power switch:

1. In the menu, click on **IP power switches**.
2. Click on the IP power switch you want to configure and then click on **Configuration**.
3. Under **Name** you can change the default name of the power switch.
4. Change or enter a comment about the power switch under **Comment**.
5. Click on **Save**.

Configuring a IP power switch

To be able to control the power switch via KVM extender, enter the IP address and the access data of the *Hidden Page Account* (see installation guide of the power switch) of the power switch.

How to configure a IP power switch:

1. In the menu, click on **IP power switches**.
2. Click on the IP power switch you want to configure and then click on **Configuration**.
3. Fill in all fields under **Configuration**.
4. Click on **Save**.

Assigning a power switch power outlet to the KVM extender

If the system is provided with at least one power switch, you can assign one or more power outlets to the KVM extender.

Any assigned power outlets can be switched by using the on-screen display of the user module.

How to change the assignment of power switch power outlets:

1. In the menu, click on **IP power switches**.
2. Click on the IP power switch you want to configure and then click on **Configuration**.
3. Click on the tab **Outlets**.

   On the tab, all available power switch outlets are displayed in the left table (**Outlet index**). The table on the right shows all computer modules (**Targets**).

   NOTE: The **Assigned** mark in the left table indicates the power switch outlets to which a computer module is assigned.

4. In the table on the *left*, select the outlet that you want to assign to a computer module or whose assignment you want to remove.
5. (De)activate the assignment of a power outlet to a specific computer module in the right table by moving the **Assigned** controller of the computer module to the *right* (*assigned*) or to the *left* (*not assigned*).
6. Click on **Save**.

Deleting a IP power switch from the KVM system

If the KVM matrix system is not able to detect an existing power switch, the systems defines the device as being switched off.

Therefore, manually delete the list entry of the power switch you want to permanently delete from the system.

NOTE: Only power switches that are switched off can be deleted.

How to delete a IP power switch that is switched off or disconnected from the system:

1. In the menu, click on **IP power switches**.
2. Click on the IP power switch you want to delete and then click on **Delete**.
3. Confirm the security prompt by clicking on **Yes** or cancel the process by clicking on **No**.

Viewing status information of a IP power switch

The context menu a power switch allows you to open a window containing various status information.

How to view the status information of a IP power switch:

1. In the menu, click on **IP power switches**.
2. Click on the IP power switch you want to configure and then click on **Configuration**.
3. Click on the tab **Information**.

   The tab shows the following information:

Name:	Name of the power switch
Status:	Current status (*Online* or *Offline*) of the power switch

NOTE: The paragraph *Power outlets* shows a list containing all channels of the power switch. The table also shows the assigned computer module.

4. Click on **Save**.

NOTES

NOTES

NOTES

NOTES

The manual is constantly updated and available on our website.

https://gdsys.de/A9200145

Guntermann & Drunck GmbH

Obere Leimbach 9
57074 Siegen

Germany

http://www.gdsys.de
sales@gdsys.de