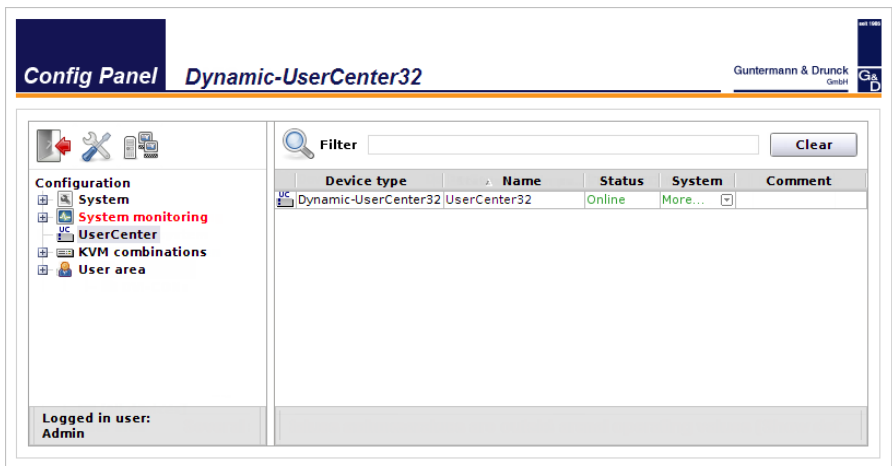


Dynamic-UserCenter 32



EN

Web Application »Config Panel«
Configuring the expansion

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.

Imprint

© Guntermann & Drunck GmbH 2015. All rights reserved.

Version 1.20 – 13/01/2015

Version: 1.11.7

Guntermann & Drunck GmbH
Dortmunder Str. 4a
57234 Wilnsdorf

Germany

Phone +49 2739 8901-100

Fax +49 2739 8901-120

<http://www.GDsys.de>

sales@GDsys.de

Table of contents

Introduction	4
System requirements	5
Supported web browsers	5
Java Runtime Environment	5
Configuring the network settings	6
Getting started	7
Starting the web application	7
Security instructions of the web browser	7
User login at the web application	8
Operating the web application	8
User interface	8
User logout	10
Selecting the default language of the web application	10
Choosing the hash algorithm to store passwords	10
Showing the version number of the web application	11
Administering »Dynamic Ports«	11
Configuring »Dynamic Ports«	11
Changing the view modes of the »Dynamic Port« LEDs	13
Allowing or denying the direct connection of user modules	14
Basic configuration of the web application	15
Network settings	15
Configuring the network settings	15
Configuring the global network settings	16
Increasing the reliability of network connections through link aggregation	17
Reading out the status of the network interfaces	19
Creating and administering netfilter rules	19
Creating new netfilter rules	19
Editing existing netfilter rules	20
Deleting existing netfilter rules	22
Changing the order/priority of existing netfilter rules	22
Creating an SSL certificate	23
Special features for complex KVM systems	23
Creating a Certificate Authority	23
Creating any certificate	24
Creating and signing the X509 certificate	25
Creating a PEM file	26
Selecting an SSL certificate	26
Firmware update	27
Restoring the default settings	28
Restarting the device	28

Network functions of the devices	29
NTP server	29
Time sync with an NTP server	29
Setting time and date manually	30
Logging syslog messages	31
Locally logging the syslog messages	31
Sending syslog messages to a server	32
Viewing and saving local syslog messages	33
User authentication with directory services	34
Monitoring functions	36
Viewing monitoring values	37
Listing values by applying monitoring sets	37
Listing individual values of critical devices	37
Disabling monitoring values	37
Advanced function regarding the administration of critical devices	38
Messages regarding critical statuses of devices	38
Viewing the list of critical devices	39
Marking messages from critical devices as read	39
Administrating monitor groups	39
Adding monitoring groups	40
Changing name and/or comment of monitoring groups	40
Assigning members to monitoring groups	41
Duplicating monitoring groups	41
Deleting monitoring groups	42
Administrating monitoring sets	42
Adding monitoring sets	43
Changing name and/or comment of monitoring sets	43
Assigning members to monitoring sets	43
Selecting a monitoring set in the folder configuration	44
Duplicating monitoring sets	44
Deleting monitoring sets	45
Device monitoring via SNMP	46
Practical use of the SNMP protocol	46
Configuring the SNMP agent	46
Configuring SNMP traps	48
Logbook	51
The dialogue entries of the logbook	51
The »Logbook configuration« window	51
Viewing a logbook entry in detail	52
Basic logbook functions	52
Creating a new logbook entry	52
Changing a logbook entry	53
Deleting a logbook entry	54

Advanced functions	54
Printing logbook entries	54
Exporting logbook entries	55
Copying the logbook entries	56
Shared editing	57
Users and Groups	58
Efficient rights administration	58
The effective right	58
Efficient user group administration	59
Administering user accounts	59
Creating a new user account	60
Renaming the user account	61
Changing the user account password	61
Changing the user account rights	62
Changing a user account's group membership	62
Enabling/Disabling a user account	62
Deleting a user account	63
Administering user groups	63
Creating a new user group	63
Renaming a user group	64
Changing the user group rights	64
Administering user group members	64
(De)activating a user group	65
Deleting a user group	65
System rights	65
Rights for full access (Superuser)	65
Changing the login right to the web application	66
Rights to change your own password	66
The »KVM combinations« folder	67
Folder administration	67
Creating new folders	67
Assigning a device to a folder	68
Deleting a device from a folder	68
Renaming a folder	69
Deleting a folder	69
Advanced functions of the KVM system	70
Temporarily (de)activating SNMP traps (Maintenance mode)	70
(De)activating the maintenance mode	70
Viewing a list of devices in maintenance mode	70
Identifying a device by activating the Identification LED	70
Saving and restoring the data of the KVM system	71
Overview of the monitoring values	72

Introduction

The *Config Panel* 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
- Easy operation through the drag & drop function
- Monitoring of various system features
- Advanced network functions (netfilter, syslog, ...)
- Backup and restore function

System requirements

The *Config Panel* web application is an application that runs on the Java platform. It can be applied on a computer with installed *Java Runtime Environment*. Use one of the supported web browsers to run this application.

IMPORTANT: Before operating the web application via web browser, connect the device on which the web application is operated to the local network (see installation guide).

Now adjust the network settings as described on page 6.

Supported web browsers

The following web browsers support the web application:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Mozilla Firefox 35

Java Runtime Environment

The web application runs on *Java Runtime Environment* (JRE). Starting the web application requires the installation of version 6 (update 19).

A free download of this version is available at the following website:

<http://www.oracle.com/technetwork/java/>

NOTE: Mind the special instructions for running *Java Runtime Environment* on a 64-bit browser for Windows:

http://www.java.com/en/download/faq/java_win64bit.xml

Configuring 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 15 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 describes how to operate the web application.

NOTE: The following chapters give a detailed overview of all functions and configuration settings.

Starting the web application

The web application can be operated on a computer with installed *Java Runtime Environment*. Use one of the supported web browsers to run this application.

NOTE: Information regarding the system requirements of the web application are provided on page 5.

How to start the web application:

1. Enter the following address to call the web application:

https://[ip address of the device]

NOTE: You can also start the web application via http connection (port 80). In this case it is not possible to authenticate the opposite side via certificate.

Security instructions of the web browser

The device, on which the web application is operated, stores an SSL certificate that enables the user or the web browser to authenticate the opposite site.

IMPORTANT: Replace the certificate that is included in the defaults of the device with an individual certificate, which is related to the device. Information on how to create such a certificate is given on page 26.

User login at the web application

After the certificates are authenticated, the login window opens.

How to log in to the web application:

1. Enter the following data in the login box:

Username:	Enter your username.
Password:	Enter your user account password.
Select language:	Select the language to be displayed on the user interface: <ul style="list-style-type: none"> ▪ (Default): apply default setting ▪ German ▪ English

2. Click the **Login** button.

IMPORTANT: Change the preset password of the administrator account immediately.

Use the administrator account to log in to the web application and change the password (see page 61).

These are the *preset* access data for the administrator account:

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

Operating the web application

User interface

The user interface of the web application consists of four main sections:

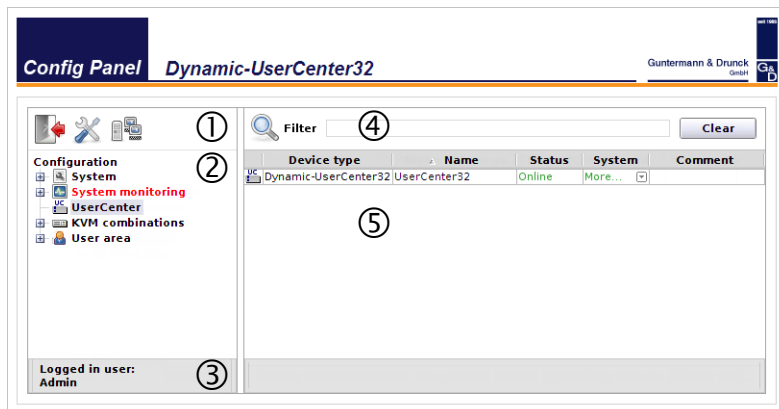


Figure 1: User interface

The different sectors of the user interface perform various tasks. The following table lists the intended use of each sector:

Toolbar ①:	The toolbar allows you to exit the active session and access the basic configuration of the web application.
Tree view ②:	The tree view shows the setting options.
User name ③:	Name of user logged in to the web application
Filter function ④:	<p>The filter function can be used to limit the elements that are displayed in the main view.</p> <p>Enter a part of the name of the searched element into the text field. Now, the main view only displays names that contain this particular text.</p> <p>Click Delete to cancel the filtering.</p>
Main view ⑤:	After you selected an element in the tree view ②, the main view displays the superior elements.

ADVICE: In the main view of **UserCenter** and **KVM combinations**, you can switch between the *Monitoring* and the *Info mode*.

The main view of the *Monitoring mode* shows the values of the monitored features. The *Info mode* shows important information like the firmware version, or the device's IP and MAC address(es).

Right-click the table, and select **Column view > Monitoring** or **Information** to activate the desired mode.

Frequently used buttons

The user interface uses different buttons to carry out certain functions. The following table provides information on the names and functions of the buttons that are used in many interfaces.

Reload:	Reload window values from the system's database. Changes that have been carried out by the user are overwritten.
OK:	<p>Save your settings.</p> <p><i>Afterwards, the window closes.</i></p>
Apply:	<p>Save your settings.</p> <p><i>The window remains open.</i></p>
Cancel:	Cancel your settings and close window.
Print:	<p>Call print interface to select printer, page orientation and further settings.</p> <p>After the settings have been selected, the interface information (e.g., the <i>cascade information</i>) can be printed.</p>
Close:	Close windows.

User logout

Use the *Logout* button to exit the current session within the web application.

IMPORTANT: Always use the *Logout* function to exit your session to protect the web application against unauthorised access.

How to exit an active session in the web application:

1. Click the **Logout** button (see figure on the right) to exit the active session in the web application.



After your logout, the login box is displayed.

Selecting the default language of the web application

How to change the default language of the web application:

1. In the directory tree, click on **System**.
2. Double-click on **Configuration** in the main view.
3. Click the **System** tab.
4. Use the **Language** entry to select the default language to be displayed to all users of the web application:

- German
- English

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

Choosing the hash algorithm to store passwords

By default, the database stores user passwords as MD5 hash values.

If desired, you can change the hash algorithm to **bcrypt**.

1. Click the **System** entry in the tree view.
2. Double-click on **Configuration** in the main view.
3. Click the **System** tab.
4. Choose the algorithm from the **Hash algorithm** context menu:

- MD5
- bcrypt

5. Click **OK** to save the settings.

Showing the version number of the web application

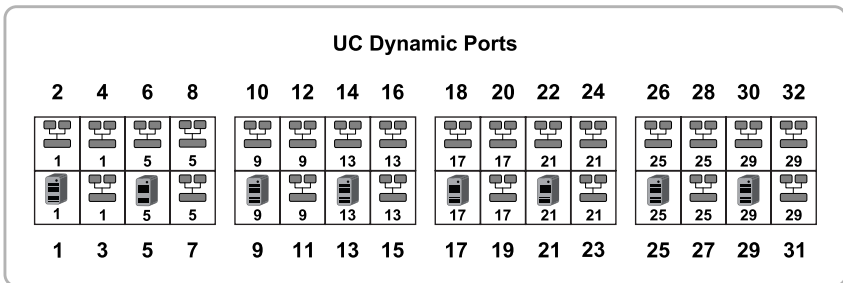
How to show the version number of the web application:

1. In the directory tree, click on **System > Information**.
2. Double-click on **General**.
3. Click on **Close** to close the window.

Administrating »Dynamic Ports«

In the default setting, the Dynamic Ports are divided into 8 groups. Each group lets you connect one target module and three matrix switches.

The following screenshot shows the default port configuration:



The following information are shown for each port:



The computer icon highlights *CPU* ports.
Connect a target module of the *DVI-CPU* series to these ports.



The cluster icon highlights *Cluster* ports.
Connect a matrix switch of the *DVICenter* series to these ports.




Every assigned port belongs to a group. The group number is shown below the computer and cluster icons.
The numbers result from the number of the group's *CPU port*.

Configuring »Dynamic Ports«




The ports of the *Dynamic-UserCenter 32* expansion can be grouped and assigned according to your personal preferences. Each group consists of a *CPU port* to which you can connect a target module. In addition, you can add at least two *Cluster ports* to the group. Connect the matrix switches that can access the target module to these ports.

How to configure »Dynamic Ports«:

1. Click the **Dynamic Port** icon (see figure on the right) in the tool bar of the web application. 
2. The configuration dialog shows the setting **Graph below table** (default) in the tool-bar of the web application
 You can also choose between the options: **Table only**, **Graph next to table** or **Graph only**.
3. If desired, click on **Predefined configurations**.
 Here, you can choose one of the frequently used configurations (**1:3**, **1:7** or **1:15**), or you can reset the assignment of all ports (**Unassigned**).
4. You can also adjust the current port layout or one of the frequently used configurations as shown in the table below.


NOTE: Select several ports by simultaneously pressing the left mouse key and Shift or Ctrl.

NOTE: You can also carry out the actions via drag & drop.

Carry out action in graph	Carry out action in table
TO CREATE A NEW PORT GROUP	
<ul style="list-style-type: none"> ▪ Right-click an unassigned port that you want to use as <i>CPU port</i> of the new group. ▪ Select New group from the context menu. 	<ul style="list-style-type: none"> ▪ In the left column, click the <i>CPU port</i> you want to create for the new port group. ▪ Click .
TO ASSIGN A CLUSTER PORT TO A PORT GROUP	
<ul style="list-style-type: none"> ▪ Right-click an unassigned port that you want to add as <i>Cluster port</i> of a group. ▪ Select Assign from the context menu. ▪ Select the <i>CPU port</i> in whose group you want to add the <i>Cluster port</i>. 	<ul style="list-style-type: none"> ▪ In the left column, click the <i>Cluster port</i> you want to add. ▪ In the right column, click the group name or a port of the group to which you want to add the <i>Cluster port</i>. ▪ Click .
TO DELETE A CLUSTER PORT FROM A PORT GROUP	
<ul style="list-style-type: none"> ▪ Right-click the <i>Cluster port</i> you want to delete from the group. ▪ Select Delete from group from the context menu. 	<ul style="list-style-type: none"> ▪ In the right column, click the <i>Cluster port</i> you want to delete from the group. ▪ Click .

TO DELETE A GROUP

▸ Warning: All ports of a port group are deleted.

- Right-click the *CPU port* whose group you want to delete.
- Select **Delete group** from the context menu.
- In the right column, click the *CPU port* whose group you want to delete.
- Click .

NOTE: Click **Print** to print a detailed list of all ports.

5. Click **Ok** to save any changes.

IMPORTANT: After you change the port assignment, the device reboots.

6. Click the **Logout** icon (see figure on the right) to leave the active sessions of the web application.



Changing the view modes of the »Dynamic Port« LEDs

In the device's default settings, the LEDs of the *Dynamic Ports* show the interface's status.

To facilitate the installation, you can switch the LEDs of the *Dynamic Ports* into *Port mode*. In Port mode, the *Dynamic Ports* to connect the matrix switches or the user modules are highlighted by green or yellow LEDs.

How to enable the Port mode of *Dynamic Ports*:

1. In the tree view, click **UserCenter**.
2. Right-click the device, and select **Dynamic Port LEDs > Show port type** from the menu.
3. Choose **System** to show the port modes of all ports, or choose the port group to which you want to limit the highlighting LEDs to.

The LEDs of the *Dynamic Ports* highlight the current port mode:

LED	Port mode
Yellow	Connection of matrix switches
Green	Connection of target modules

NOTE: If the port modes are active, the *Identification* LEDs on the device's front and back side are blinking.

How to enable the interface status of *Dynamic Ports*:

1. In the tree view, click **UserCenter**.
2. Right-click the device, and select **Dynamic Port LEDs > Show status** from the menu.
3. Choose **System** to show the port modes of all ports, or choose the port group to which you want to limit the highlighting LEDs to.

The LEDs of the *Dynamic Ports* now highlight the current status of the single ports (see Installation manual).

Allowing or denying the direct connection of user modules

The device's default settings allow you to connect user modules of the *DVI-CON* series instead of matrix switches to the *Cluster ports*.

You can change this setting under **Direct consoles** in the context menu.

How to allow or deny the direct connection of user modules:

1. In the tree view, click **UserCenter**.
2. Right-click the device you want to configure and select **Configuration** from the context menu.
3. Select one of the following options under **Direct consoles**:

Allowed:	You are allowed to connect user modules of the <i>DVI-CON</i> series to the <i>Cluster ports</i> . It is possible to access a user module.
Denied:	You are denied to connect user modules of the <i>DVI-CON</i> series to the <i>Cluster ports</i> . Trying to access a user module triggers the message that a matrix switch could not be found.

4. Click **Ok** to close the window.

Basic configuration of the web application

The tool symbol in the toolbar can be used to access the basic configuration of the web application.

Network settings

The devices with integrated web application are provided with two network interfaces (*Network A* and *Network B*). These network interfaces enable you to integrate the device into up to two separate networks.

IMPORTANT: Please mind the separate instructions regarding *Configuring the network settings* on page 6.

Configuring 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**

Configure the network settings to connect the device to a local network.

How to configure the settings of a network interface:

IMPORTANT: It is not possible to operate both network interfaces within one subnet.

NOTE: According to RFC 3330, the *Link Local* address space 169.254.0.0/16 is reserved for the internal communication between devices. An IP address of this address space cannot be assigned.

1. Click the tools symbol in the toolbar.
2. Click the **Network > Interfaces** tabs.
3. Use **Interface A** or **Interface B** paragraphs to enter the following data:

Operational mode:	<p>Use the pull-down menu to select the operating mode of Interface A or Interface B:</p> <ul style="list-style-type: none"> ▪ Off: switches off network interface. ▪ Static: uses static settings. ▪ DHCP: obtains the settings from a DHCP server. ▪ Link aggregation active: This interface was added to a group of network interfaces. <p><i>Use the »Link aggregation« tab to configure the network interfaces.</i></p>
--------------------------	--

IP address:	Only if the <i>Static</i> operating mode is selected: Enter the interface IP address.
Netmask:	Only if the <i>Static</i> operating mode is selected: Enter the network netmask.
Connection type:	Select if the network interface and the remote station are to negotiate the connection type automatically (Auto) or if one of the available types is to be applied.

- Click **OK** to save the data.

Configuring the global network settings

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

How to configure the global network settings:

- Click the tools symbol in the toolbar.
- Click the **Network > Interfaces** tabs.
- Enter the following data in the **Global network settings** section:

Global preferences:	Use the pull-down menu to select the operating mode: <ul style="list-style-type: none"> ▪ Static: uses static settings. ▪ DHCP: obtains the settings from a DHCP server. <div> The following settings are automatically obtained in the <i>DHCP</i> operating mode. Inputs are not possible. </div>
Hostname:	Enter the device hostname.
Domain:	Enter the domain the device is to belong to.
Gateway:	Enter the gateway IP address.
DNS Server 1:	Enter the DNS server IP address.
DNS Server 2:	Optionally, enter the IP address of another DNS server.

- Click **OK** to save your data.

Increasing the reliability of network connections through link aggregation

In the default settings, you can use both network interfaces at the same time to access the web application from two different network segments, for example.

To increase the reliability, the network interfaces can be grouped through *link aggregation*. Only one interface is active within the group. Another interface only becomes active if the active interface fails.

We provide two different modes to monitor the interfaces:

- **MII mode:** The carrier status of the network interface is monitored through the *Media Independent Interface*. This mode only checks the function of the network interface.
- **ARP mode:** The *address resolution protocol* sends requests to an ARP target within the network. The answer of the ARP target confirms both the functionality of the network interface and the proper network connection to the ARP target.

If the ARP target is connected to the network but is temporarily offline, requests cannot be answered. Define multiple ARP targets to receive an answer from at least one target if an ARP target fails.

NOTE: MII and ARP mode cannot be combined.

How to configure the settings of grouped network interfaces:

NOTE: According to RFC 3330, the *Link Local* address space 169.254.0.0/16 is reserved for the internal communication between devices. An IP address of this address space cannot be assigned.

1. Click the tools symbol in the toolbar.
2. Click the **Network > Link aggregation** tab.
3. Enter the following data into the **Network** paragraph:

Name:	Enter a name for the group of network interfaces.
Operational mode:	Choose the operational mode for the grouped network interfaces: <ul style="list-style-type: none"> ▪ Off: disables link aggregation. <i>Use the »Interfaces« tab to configure the network interfaces.</i> ▪ 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 if you have selected the <i>Static</i> operational mode).
Netmask:	Enter the netmask of the network (only if you have selected the <i>Static</i> operational mode).

4. Enter the following data in the **Parameter** paragraph:

Primary slave:	<p>Choose if the data traffic should run via <i>Network A (Interface A)</i> or <i>Network B (Interface B)</i>. As soon as the selected interface is available, the data traffic is sent via this interface.</p> <p>If you choose the option None, the data traffic is sent via any interface. The interface only changes if the active interface is down.</p>
Link monitoring:	<p>Choose if you want the MII or ARP mode (description see below) to be used to monitor the interface.</p>
MII down delay:	<p>Time delay in milliseconds before a failed network interface is disabled.</p> <p>The value must be a multiple of 100 ms (the MII link monitoring frequency).</p>
MII up delay:	<p>Time delay in milliseconds before a reset network interface is enabled.</p> <p>The value must be a multiple of 100 ms (the MII link monitoring frequency).</p>
ARP interval:	<p>Enter the interval (100 to 10,000 milliseconds) according to which the incoming ARP packets of the network interfaces are to be checked.</p>
ARP validate:	<p>The validation ensures that the ARP packet for a particular network interface is generated by one of the listed ARP targets.</p> <p>Choose if or what incoming ARP packets are to be validated:</p> <ul style="list-style-type: none">▪ 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 within the group are validated.
ARP target:	<p>The table lists all configured ARP targets.</p> <p>Use the New, Edit, and Delete buttons to administrate the ARP targets.</p>

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

Reading out the status of the network interfaces

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

How to detect the status of the network interfaces:

1. Click the tools symbol in the toolbar.
2. Click the **Network > Link status** tab.
3. The **Interface A** and **Interface B** paragraph provides you with the following data:

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

4. Click **OK** to close the window.

Creating and administrating netfilter rules

In the default settings of the devices, all network computers have access to the *Config Panel* web application (open system access).

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

If you create a netfilter rule, the open system access is deactivated and all incoming data packets are compared to the netfilter rules. The list of the netfilter rules is processed according to the stored order. As soon as a rule applies, it is carried out and the following rules are ignored.

Creating new netfilter rules

How to create new netfilter rules:

1. Click the tools symbol in the toolbar.
2. Click the **Network > Netfilter** tabs.
3. Enter the data described below.

Interface:	Use the pull-down menu to select on which network interfaces the data packets are to be trapped and manipulated: <ul style="list-style-type: none"> ▪ All ▪ Interface A ▪ Interface B ▪ [Name of a group of network interfaces]
-------------------	---

Option:	<p>Use the pull-down menu to select how the rule's sender information are to be interpreted:</p> <ul style="list-style-type: none"> ▪ Normal: The rule applies for data packets whose sender information does comply with the indicated IP address or MAC address. ▪ Inverted: The rule applies for data packets whose sender information does <i>not</i> comply with the indicated IP address or MAC address.
IP address/ Netmask:	<p>Enter the data packet IP address or use the Netmask entry to enter the address space of the IP addresses.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ 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 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p> </div>
MAC address:	<p>Enter the MAC address to be considered in this filter rule.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p> </div>
Filter rule:	<ul style="list-style-type: none"> ▪ Drop: Data packets whose sender information comply with the IP address or MAC address are <i>not</i> processed. ▪ Accept: Data packets whose sender information comply with the IP address or MAC address are processed.

4. Click **Add** to save the data in a new filter rule.

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

5. Click **OK** to close the window.

NOTE: The new netfilter rule does not apply for active connections. Restart the device to disconnect any active connections. Afterwards, all rules apply.

Editing existing netfilter rules

How to edit an existing netfilter rule:

1. Click the tools symbol in the toolbar.
2. Click the **Network > Netfilter** tabs.
3. Mark the rule to be changed in the list of the existing netfilter rules.

4. The current rule settings are displayed in the upper part of the window. Check and change the data described on the following page.

Interface:	Use the pull-down menu to select on which network interfaces the data packets are to be trapped and manipulated: <ul style="list-style-type: none"> ▪ All ▪ Interface A ▪ Interface B
Option:	Use the pull-down menu to select how the rule's sender information are to be interpreted: <ul style="list-style-type: none"> ▪ Normal: The rule applies for data packets whose sender information does comply with the indicated IP address or MAC address. ▪ Inverted: The rule applies for data packets whose sender information does <i>not</i> comply with the indicated IP address or MAC address.
IP address/Netmask:	Enter the data packet IP address or – using the Netmask entry – the address space of the IP addresses. Examples: <ul style="list-style-type: none"> ▪ 192.168.150.187: for the 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 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> The <i>IP address</i> and/or a <i>MAC address</i> can be indicated within a rule. </div>
MAC address:	Enter the MAC address to be considered in this filter rule. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule. </div>
Filter rule:	<ul style="list-style-type: none"> ▪ Drop: Data packets whose sender information comply with the IP address or MAC address are <i>not</i> processed. ▪ Accept: Data packets whose sender information comply with the IP address or MAC address are processed.

5. Click **Change** to save the changed data.
6. Click **OK** to close the window.

NOTE: The changed network rule does not apply for active connections. Restart the device to disconnect any active connections. Afterwards, all rules apply.

Deleting existing netfilter rules

How to delete existing netfilter rules:



1. Click the tools symbol in the toolbar.
2. Click the **Network > Netfilter** tabs.
3. Mark the rule to be deleted in the list of the existing netfilter rules.
4. Click **Remove**.
5. Confirm the confirmation prompt by pressing **Yes** or cancel the process by clicking **No**.
6. Click **OK** to close the window.

Changing the order/priority of existing netfilter rules

The netfilter rules are processed in the order they are stored. If a rule does apply, the respective action is carried out and all following rules are ignored.

IMPORTANT: Please mind the order or priority of the single rules, especially when adding new rules.

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

1. Click the tools symbol in the toolbar.
2. Click the **Network > Netfilter** tabs.
3. Mark the rule whose order/priority is to be changed in the list of the existing netfilter rules.
4. Click the  button (*arrow up*) to increase the priority or the  button (*arrow down*) to decrease the priority.
5. Click **OK** to close the window.

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: <http://www.openssl.org/>
- Win32 OpenSSL: <http://www.slproweb.com/products/Win32OpenSSL.html>

IMPORTANT: Creating an X509 certificate requires the software OpenSSL. If necessary, follow the instructions on the websites mentioned above to install the software.

The following pages give information on creating an X509 certificate.

Special features for complex KVM systems

If you want different devices to communicate within a KVM system, use the identical *Certificate Authority* (see page 23) to create certificates for those devices.

The identical PEM file (see page 26) can also be used for all devices. In this case, all certificate features are identical.

Creating a Certificate Authority

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

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)	Wilnsdorf
Organization Name (e.g., company)	Guntermann & Drunck GmbH
Organizational Unit Name (e.g., section)	
Common Name (e.g., YOUR name)	Guntermann & Drunck GmbH
Email Address	

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

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

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

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

Creating any certificate

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

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

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

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

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

How to create the certificate request:

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

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

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

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

Field	Example
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (e.g., city)	Wilnsdorf
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 the 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 > gdc.d.pem
cat server.key >> gdc.d.pem
cat ca.crt >> gdc.d.pem
```

b. Windows

```
copy server.crt + server.key + ca.crt gdc.d.pem
```

2. The *gdc.d.pem* file is created during the 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. Click the tools symbol in the toolbar.
2. Click the **Certificate** tab.
3. 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 **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 **Upload and activate** to store and activate the imported certificate for the device.

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

Firmware update

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

IMPORTANT: This function only updates the firmware of the device on which the web application has been started!

How to update the firmware:

1. Open the web application of the device whose firmware you want to update.
2. Click the tools symbol in the toolbar.
3. Click the **Tools > Firmware update** tabs.

4. Enter the storage location and the name of the backup file into the **Path** entry.

IMPORTANT: Use the information provided in the *Device* and *Comment* entries to check if you selected the correct device file.

ADVICE: Use the file dialog to select the location and the name of the update file.

5. Click on **Update now**.
6. Click **OK** to leave the interface.

Restoring the default settings

This function enables the user to restore the default settings of the device on which the web application is operated.

How to restore the default settings:

IMPORTANT: All settings are reset.

1. Click the tools symbol in the toolbar.
2. Click the **Tools > System defaults** tabs.

IMPORTANT: Use the information provided in the *Date* and *Comment* entries to check if you have selected the correct backup file.

3. Disable the **Reset network config** option to maintain the configuration of the network interfaces.
4. Click on **System Defaults** to reset the current configuration.

Restarting the device

This function enables you to restart the KVM switch. Before restarting the device you are requested to confirm your action to prevent accidental restarts.

How to restart the KVM switch via web application:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device. Now click the **Restart** on the context menu.
3. Confirm the safety request with **Yes**.

ADVICE: You can also restart the device using the **tools icon** of the web application. For this, click **Tools > Restart** to carry out the restart.

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 function 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 52 ff.)

NTP server

The device's time and date settings can either adjust be adjusted manually or automatically by synchronizing the settings with an NTP server (*Network Time Protocol*).

Time sync with an NTP server

How to change the NTP time sync settings:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network** tab.
4. Click the **NTP server** tab and enter the following data:

NTP time sync:	Select the respective entry from the pull-down menu to (de)activate the time sync: <ul style="list-style-type: none"> ▪ Disabled ▪ Enabled
NTP server 1:	Enter the IP address of a time server.
NTP server 2:	<i>Optionally</i> 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 **OK** to close the window.

Setting time and date manually

How to manually set the time and date of the KVM matrix system:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network > NTP server** tabs.
4. If necessary, disable the **NTP time sync** option. Otherwise, you might not be able to set time and date manually.
5. Use the **Time** entry to enter the current time (*hh:mm:ss*).
6. Use the **Date** entry to enter the current time (*DD.MM.YYYY*).

ADVICE: Click on **Accept local date** to accept the current system date of the computer on which the *Config Panel* web application has been started.

7. Click **OK**.

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 | ▪ 3: Error | ▪ 6: Info |
| ▪ 1: Alert | ▪ 4: Warning | ▪ 7: Debug |
| ▪ 2: Critical | ▪ 5: Note | |

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

Locally logging the syslog messages

How to locally log the syslog messages:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network** tab.
4. Click the **Syslog** tab and enter the following data in the **Syslog local** section:

Syslog server:	Select the respective entry from the pull-down menu to define whether syslog messages are to be sent to a server: <ul style="list-style-type: none"> ▪ Disabled ▪ Enabled
Log Level:	Use the pull-down menu to select from which severity code on a log message is to be logged. The selected severity code and all lower severity codes are logged. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> If you selected the severity code <i>2 - Critical</i>, messages for this code as well as for the severity codes <i>1 - Alert</i> and <i>0 - Emergency</i> are logged. </div>

5. Click **OK** to close the window.

Sending syslog messages to a server

How to send syslog messages to a server:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network** tab.
4. Click the **Syslog** tab and enter the following data in the **Syslog server 1** or **Syslog server 2** section:

Syslog server:	Select the respective entry from the pull-down menu to define whether syslog messages are to be sent to a server or not: <ul style="list-style-type: none"> ▪ Disabled ▪ Enabled
Log Level:	Use the pull-down menu to select from which severity code on a log message is to be logged. The selected severity code and all lower severity codes are logged. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>If you select severity code <i>2 - Critical</i>, messages for this code and for the severity codes <i>1 - Alert</i> and <i>0 - Emergency</i> are logged.</p> </div>
IP address/ DNS name:	Enter the IP address or the server name to which the syslog messages are to be sent.
Port:	Enter the port – usually 514 – on which the server receives the incoming messages.
Protocol:	Select the protocol – usually UDP – on which the server receives the incoming messages: <ul style="list-style-type: none"> ▪ TCP ▪ UDP

5. Click **OK** to close the window.

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 window.

How to view and store the local syslog messages:

1. Click on **System > Information** in the tree view.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Double-click on **Syslog** in the main view.
4. Click the **Fetch syslogs** tab.

The matrix switch calls the local syslog messages, which are now displayed in the text field.

ADVICE: If necessary, click **Save** to save these messages in a text file. The opening file window enables you to select the location and a file name.
Afterwards, click **Save**.

5. Click **OK** to close the window.

User authentication with directory services

In in-house networks, the user accounts of different users are often administrated by a directory service. The device can access such a directory service and authenticate users against the directory service.

NOTE: If the *Admin* user account cannot be authenticated by the directory service, the user account is authenticated by the device's data base.

The directory service is exclusively used to authenticate a user. The user rights are assigned within a database of the KVM system. The following paragraphs describe the different scenarios:

- **The user account exists within the directory service and the KVM system**

The user can log in with the password stored in the directory service. After the login, the user is assigned with the rights of the correspondent account in the KVM system.

NOTE: The password which the user used to log in, is taken over into the database of the KVM system.

- **The user account exists within the directory service, but not within the KVM system**

A user that has been successfully authenticated against the directory service, but does not have an account of the same name within the database of the KVM system, is assigned with the rights of the *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 in to the KVM system.

- **The user account exists within the KVM system, but not within the directory service**

If the directory service is available, it reports that the user account does not exist. The access to the KVM system is denied to the user.

If the server is not available, but the fallback system is active (see below), the user can log in with the password that is stored within the KVM system.

IMPORTANT: Mind the following safety instructions to prevent a locked or deactivated user from logging in to the system in case the connection to the directory service fails:

- If a user account is deactivated or deleted in the directory service, this action can also be carried out within the user database of the KVM system.
- Only activate the fallback system in reasonable exceptional cases.

How to configure the user account authentication:

NOTE: If no directory service is applied, the user accounts are administered by the device.

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now, click the **Configuration** entry in the context menu.
3. Click the **Network > Authentication** tabs and enter the following data:

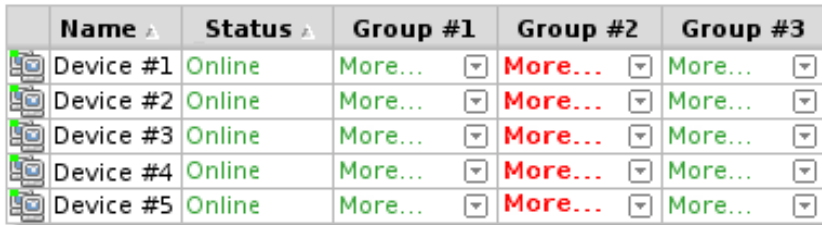
Auth. Server:	<p>Select the Local option if the user administration is to be carried out by the KVM system.</p> <p>If a particular directory service is to be applied, select the respective entry from the pull-down menu:</p> <ul style="list-style-type: none"> ▪ LDAP ▪ Active Directory ▪ Radius ▪ TACACS+
<p>ADVICE: After the directory service has been selected, collect the settings of the directory service server in the Server settings.</p>	
Fallback:	<p>Activate this option if the local user administration of the KVM system is to be applied in case the directory service is temporarily not available.</p>
<p>IMPORTANT: Mind the following safety instructions to prevent a locked or deactivated user from logging in to the system in case the connection to the directory service fails:</p> <ul style="list-style-type: none"> ▪ If a user account is disabled or deleted in the directory service, this action can also be carried out within the user database of the KVM system. ▪ Only activate the fallback system in reasonable exceptional cases. 	

4. Click **OK** to close the window.

Monitoring functions

The current monitoring values of all devices within the KVM system can be viewed in the device-specific branches (e.g. *KVM matrix systems*) as well as in the *KVM Combinations* and *Critical Devices* branches of the tree view.

The various information regarding a device can either be displayed in individual values or in monitoring groups, which are sorted according to topic. The following exemplary figure shows the *Status* values and three different monitoring groups:



Name ▲	Status ▲	Group #1	Group #2	Group #3
Device #1	Online	More... ▾	More... ▾	More... ▾
Device #2	Online	More... ▾	More... ▾	More... ▾
Device #3	Online	More... ▾	More... ▾	More... ▾
Device #4	Online	More... ▾	More... ▾	More... ▾
Device #5	Online	More... ▾	More... ▾	More... ▾

Figure 2: Detailed view of an exemplary monitoring table

Individual values (the *Status* value in the figure above) immediately show if the status is correct (green) or deviating from the normal operating value (red). The text in the column also provides information about the current status.

Monitoring groups allow you to group various individual values. The column of a monitoring group shows if all values are within range (*green*) or if at least one value is deviating from the normal operating values (*red*).

Clicking the arrow in the column opens a separate window, which displays the individual values of the group.

Viewing monitoring values

NOTE: An overview of the possible monitoring values of all different device types is given on page 72 ff.

By applying different monitoring sets, the monitoring values are displayed in the different branches of the tree view.

Several branches (e.g. *Critical devices*) provide another view to enable the user to detect critical monitoring values as fast as possible.

Listing values by applying monitoring sets

A monitoring set defines which individual values and groups are to be displayed.

The column, which shows the *individual values*, enables you to read the status and check whether it is deviating from the normal operating values.

Monitoring groups allow you to group various individual values. The column of a monitoring group shows if all values are within range (*green*) or if at least one value is deviating from the normal operating values (*red*).

Clicking the arrow in the column opens a window, which contains detailed information regarding the individual values of the group.

ADVICE: The following pages of this chapter provide detailed information regarding monitoring groups and monitoring sets.

Listing individual values of critical devices

If a device shows a value that deviates from the normal operating values, the device is additionally listed in the *Critical devices* branch. This branch displays all deviating (red) values in tabular form. This way, deviating values can be detected as fast as possible.

NOTE: To be able to find deviant values as fast as possible, monitoring sets are not applied here.

Disabling monitoring values

Any monitoring value can be disabled. After disabling, the monitoring values are no longer shown in the web application.

IMPORTANT: The web application does not show any warnings about disabled values. No SNMP traps are sent regarding these values.

How to enable/disable the monitoring values:



1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now, click the **Configuration** entry in the context menu.

3. Click the **Monitoring** tab.

Two tables list the monitoring values of the KVM system:

Enabled:	lists all active monitoring values.
Disabled:	lists all inactive monitoring values.

To give you a faster overview, the values are grouped in both columns.

4. Mark the monitoring values to be enabled/disabled.
5. Click the  button (*right arrow key*) to disable the monitoring value or  (*left arrow key*) for enabling.
6. Click **OK** to save your settings.

Advanced function regarding the administration of critical devices

The *Critical Devices* branch lists the devices that show at least one value that exceeds the normal operating values.

NOTE: A sub-branch is displayed for each device class in the KVM system (e. g. *KVM matrix systems*).

Messages regarding critical statuses of devices

If one value exceeds the normal operating values, the branch is marked red. A blinking message under the main view points to this condition.

ADVICE: If the blinking message appears on your screen, press **Ctrl + Space** to open the *Critical devices* branch.

Click on the blinking message to show the list of the deviating values in a separate window.

Viewing the list of critical devices

How to view the list of critical devices:

1. Click on the **System monitoring > Critical Devices** folders in the tree view.

The main view lists all affected devices. The critical values are displayed in the table.

ADVICE: Click a sub-branch of the folder in order to only list the devices of a particular device class.

Marking messages from critical devices as read

Many messages require immediate actions from the administrator. Other messages (e.g. the break-down of the redundant power supply), however, point to possibly uncritical conditions.

In such a case, all peculiar values of a device can be marked as read, which causes the following:

- A device whose deviating values have been marked as read shows no blinking status bar.
- The cells, info dialogues and monitoring windows of all “read” devices are highlighted in yellow.
- If a monitoring group contains critical values, which have been marked as read, the column displays *Error*. In addition, the cell is highlighted in yellow.

NOTE: The system only highlights values that have been deviating from the normal operating values at the time the function has been executed. The web application shows if another monitoring value of such a device deviates from the normal operating values.

How to mark the Monitoring messages of a device as read:

1. Click on the **System monitoring > Critical Devices** folders in the tree view.
2. Right-click the desired device. Now click the **Acknowledge** entry of the context menu.

Administrating monitor groups

IMPORTANT: Any recently created monitoring groups are only available in the branch in which they were created.

If a monitoring group was created in a device-specific branch, it is no longer available in the *KVM combinations* branch.

The *Config Panel* web application already provides several default monitoring groups. Those groups can neither be edited nor deleted, but they can be duplicated and individually adjusted to your wishes.

All groups that were preconfigured or created are shown in the monitoring table as long as they are contained in the applied monitoring set (see page 44 ff.):






	Name ▲	Status ▲	Group #1	Group #2	Group #3
	Device #1	Online	More... ▼	More... ▼	More... ▼
	Device #2	Online	More... ▼	More... ▼	More... ▼
	Device #3	Online	More... ▼	More... ▼	More... ▼
	Device #4	Online	More... ▼	More... ▼	More... ▼
	Device #5	Online	More... ▼	More... ▼	More... ▼

Figure 3: Status of different devices in the »Group #1« monitoring group

ADVICE: Due to the high amount of individual values, it is recommended to display the most important values as individual values and group the rest in groups according to topic.

This provides a quick overview and the values are displayed in a space-saving way.

Adding monitoring groups

How to add a new monitoring group:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring groups** entry in the context menu.
3. Click **New**.
4. Enter the name and an optional comment for the new group.
5. Click **OK** to create the group.

Changing name and/or comment of monitoring groups

How to change the name and/or comment of a monitoring group:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring groups** entry in the context menu.
3. Select the group to be edited and click **Edit**.
4. Change the name and/or the optional comment of the group.
5. Click **OK** to save your settings.

Assigning members to monitoring groups


How to assign members to a monitoring group:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring groups** entry in the context menu.
3. Select the group to be edited and click **Edit**.
4. Click the **Member** tab.

Now you have the possibility to add members to or delete them from a monitoring group.

The window consists of two tables, which list the monitoring values of the KVM system:

Unassigned:	lists monitoring values that are <i>not</i> assigned to this group
Assigned:	lists monitoring values that are assigned to this group

5. Mark the monitoring value you want to add to or delete from the group.
6. Click  (*right arrow*) to add the monitoring value to the group or  (*left arrow*) to delete it from the member list.
7. Click **OK** to save your settings.

Duplicating monitoring groups

The *KVM combinations* branch as well as many other device-specific branches contain several default groups. These groups are displayed in light grey.

IMPORTANT: It is *not* possible to edit or delete a default monitoring group.

If you want to create a new group based on an already existing group, simply duplicate the existing group and edit the duplicate.

How to duplicate a monitoring group:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring groups** entry in the context menu.
3. Select the group to be duplicated and click **Edit**.
4. Enter the name and an optional comment for the group.
5. Click **Duplicate** to duplicate the existing group.
6. Edit the new group as described on the previous page or click **Close** to close the window.

Deleting monitoring groups

The *KVM combinations* branch as well as many other device-specific branches contain several default groups. These groups are displayed in light grey.

IMPORTANT: It is *not* possible to edit or delete a default monitoring group.

How to delete a monitoring group:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring groups** entry in the context menu.
3. Select the group to be deleted and click **Delete**.
4. Confirm the confirmation prompt by clicking **Yes** or cancel the task by clicking **No**.
5. Click **Close** to save your settings.

Administrating monitoring sets

A monitoring set defines the individual values and the groups to be displayed in a subfolder of the *KVM combinations* branch or a device-specific branch:

	Name ▲	Status ▲	Group #1	Group #2	Group #3
	Device #1	Online	More... ▼	More... ▼	More... ▼
	Device #2	Online	More... ▼	More... ▼	More... ▼
	Device #3	Online	More... ▼	More... ▼	More... ▼
	Device #4	Online	More... ▼	More... ▼	More... ▼
	Device #5	Online	More... ▼	More... ▼	More... ▼

Figure 4: Status of the individual **Status** value and three groups of a monitoring set

The *Config Panel* web application already provides several default monitoring groups. The groups can neither be edited nor deleted, but they can be duplicated and individually adjusted to your wishes.

It is also possible to create and configure a new group.

IMPORTANT: The created monitoring sets are only displayed in the branch in which they have been created.

If a monitoring set has been created in a device-specific branch, it is no longer displayed in the *KVM combinations* branch!

Adding monitoring sets

How to add a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring set** entry in the context menu.
3. Click **New**.
4. Enter the name and an optional comment for the new set.
5. Click **OK** to create the set.

Changing name and/or comment of monitoring sets

How to change the name and/or comment of a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring sets** entry in the context menu.
3. Select the set to be edited and click **Edit**.
4. Enter the name and an optional comment for the set.
5. Click **OK** to save your settings.

Assigning members to monitoring sets

IMPORTANT: It is important to define your desired monitoring groups (see page 39 ff.) before creating a monitoring set.

How to assign members to a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring sets** entry in the context menu.
3. Select the set to be edited and click **Edit**.
4. Click the **Member** tab.



Now you have the possibility to add members to or delete them from a monitoring set.

The entry consists of two tables which list the monitoring values of the KVM system. The values are divided into the sub categories *Individual values* and *Groups (Columns)*.

NOTE: Click on the [-] in the category header to hide the content of this category. Clicking on [+] shows the contents.

The different values are either listed in the left or the right-hand table:

Unassigned:	lists monitoring values that are <i>not</i> assigned to this set
Assigned:	lists monitoring values that are assigned to this set

5. Mark the monitoring value you want to add to or delete from the group.
6. Click  (*right arrow*) to add the monitoring value to the set or  (*left arrow*) to delete it from the member list.
7. Click **OK** to save your settings.

Selecting a monitoring set in the folder configuration

After a monitoring set has been created, it can be activated in the configuration of one (or more) folders of the tree view.

How to activate a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Configuration** entry in the context menu.
3. Use the **Monitoring set** entry to select the desired set.

IMPORTANT: The created monitoring sets are only displayed in the branch in which they have been created.

If a monitoring set has been created in the *KVM extenders* branch, it is no longer displayed in the *KVM combinations* branch!

4. Click **OK** to activate the selected set.

Duplicating monitoring sets

The *KVM combinations* branch as well as many other device-specific branches contain several default groups. Those groups are displayed in light grey.

IMPORTANT: It is *not* possible to edit or delete those groups.

If you want to create a new set based on an already existing set, simply duplicate the existing set and edit the duplicate.

How to duplicate a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring sets** entry in the context menu.
3. Select the set to be duplicated and click **Edit**.
4. Enter the name and an optional comment for the set.

5. Click **Duplicate** to duplicate the existing set.
6. Edit the new set as described on the previous page or click **Close** to close the window.

Deleting monitoring sets

The *KVM combinations* branch as well as many other device-specific branches contain several default groups. These groups are displayed in light grey.

IMPORTANT: These groups *cannot* be edited or deleted.

How to delete a monitoring set:

1. Right-click the top level of a device-specific branch (e.g. *UserCenter*) or the *KVM combinations* branch in the tree view.
2. Click the **Monitoring sets** entry in the context menu.
3. Select the set to be deleted and click **Delete**.
4. Confirm the confirmation prompt by clicking **Yes** or cancel the task by clicking **No**.
5. Click **Close** to save your settings.

Device monitoring 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, which runs on the monitored device and detects its status. Via SNMP, the detected data are transmitted to the *Network Management System*.

If an *Agent* detects a severe failure within the device, it can send a *Trap* packet to the *Network Management System*. This way, the administrator is directly informed about such occurrences.

Configuring the SNMP agent

How to configure the SNMP agent:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network > SNMP Agent** tabs.
4. Enter the following data in the *Global* paragraph:

Status:	Select the particular entry to either switch the SNMP agent off (Off) or on (Enabled).
Protocol:	Select the protocol (TCP or UDP) – normally UDP – via which the SNMP packets are to be transmitted.
Port:	Define the port – normally 161 – on which the <i>incoming</i> SNMP packets are to be accepted.
SysContact:	Enter the admin's contact data (e.g. direct dial or email address).
SysName:	Enter the device name.
SysLocation:	Enter the location of the device.

5. If you want to process the packets of the **SNMPv2c** protocol version, enter the following data in the paragraph of the same name:

Access:	Activate the <i>View</i> access (View) or deny the access (No) via <i>SNMPv2c</i> protocol.
Source:	Enter the IP address or the address space of the addresses of incoming SNMP packets. Examples: <ul style="list-style-type: none"> ▪ 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 <i>Community</i> which has also been selected in the <i>Network Management System</i> .

IMPORTANT: The transfer of the packet password (*Community*) of the *SNMPv2c* protocol version is not encrypted. Therefore, it can be easily tapped!

If required, use the *SNMPv3* protocol version (see below) and a high *Security level* to ensure a secure data transfer.

6. If you want to process the packets of the **SNMPv3** protocol version, enter the following data in the respective paragraph:

Access:	Activate the <i>View</i> access (View) or deny the access (No) via <i>SNMPv3</i> protocol.
User:	Enter the username for the communication with the <i>Network Management System</i> .
Authentication protocol	Select the authentication protocol (MD5 or SHA) which has been activated in the <i>Network Management System</i> .
Authentication passphrase	Enter the authentication passphrase for the communication with the <i>Network Management System</i> .
Security level	Select between one of the following options: <ul style="list-style-type: none"> ▪ NoAuthNoPriv: user authentication and <i>Privacy</i> protocol deactivated ▪ AuthNoPriv: user authentication activated, <i>Privacy</i> protocol deactivated ▪ AuthPriv: user authentication and <i>Privacy</i> protocol activated
Privacy protocol:	Select the Privacy protocol (DES or AES) which has been activated in the <i>Network Management System</i> .
Privacy passphrase:	Enter the privacy passphrase for secure communication with the <i>Network Management System</i> .

Engine ID method:	Select how the SnmpEngineID should be assigned: <ul style="list-style-type: none"> ▪ Random: The <i>SnmpEngineID</i> is re-assigned with every restart of the device. ▪ Fix: The <i>SnmpEngineID</i> is the same as the MAC address of the device's network interface. ▪ User: The string entered under <i>Engine ID</i> is used as <i>SnmpEngineID</i>.
Engine ID:	When using the <i>Engine ID method</i> User , enter a string that is used as <i>Engine ID</i> .

7. Click **OK** to save your settings and to leave the window.

Configuring SNMP traps

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

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network > SNMP trap** tabs.
4. Click **Add** or **Edit**.
5. Enter the following data in the **Global** paragraph:

Server:	Enter the IP address of the <i>Network Management Servers</i> .
Protocol:	Select the protocol (TCP or UDP) – normally UDP – via which the SNMP packets are to be transmitted.
Port:	Define the port – normally 162 – on which the <i>outgoing</i> SNMP packets are to be accepted.
Retries:	Enter the number of retries to send an <i>SNMP Inform</i> .
NOTE: Inputs are only possible if the <i>Inform</i> option has been selected in the <i>Notification type</i> entry.	
Timeout:	Enter the time (in seconds) after which an <i>SNMP Inform</i> is to be sent again if you have received no confirmation.
NOTE: Inputs are only possible if the <i>Inform</i> option has been selected in the <i>Notification type</i> entry.	

Log level: Select from which severity level an SNMP trap is to be sent.
The selected severity level and all lower severity levels are logged.

NOTE: If you select the *2 - Critical*, severity level SNMP traps are sent for occurrences from this level and from the *1 - Alarm* and *0 - Emergency* severity levels.

Version: Select if the traps are to be created and sent according to the *SNMPv2c (v2c)* or *SNMPv3 (v3)* protocol.

Notification type: Select if the occurrences are sent as *Trap* or *Inform* packet.

NOTE: *Inform* packets require a confirmation of the *Network Management System*. If this confirmation is not available, the transmission is repeated.

6. If you use the **SNMPv2c** protocol version, use the respective paragraph to enter the same *Community* name as selected in the *Network Management System*.

IMPORTANT: The transfer of the packet password (*Community*) of the *SNMPv2c* protocol version is not encrypted. Therefore, it can be easily tapped!

If required, use the *SNMPv3* protocol version (see below) and a high *Security level* to ensure a secure data transfer.

7. If you decided to use the **SNMPv3** protocol version, use the respective paragraph to enter the following data:

User:	Enter the username for communication with the <i>Network Management System</i> an.
Authentication protocol	Select the authentication protocol (MD5 or SHA) which has been activated in the <i>Network Management System</i> .
Authentication passphrase	Enter the authentication passphrase for the communication with the <i>Network Management System</i> .
Security level	Select between one of the following options: <ul style="list-style-type: none"> ▪ NoAuthNoPriv: deactivated user authentication and <i>Privacy</i> protocol ▪ AuthNoPriv: activated user authentication, deactivated <i>Privacy</i> protocol ▪ AuthPriv: activated user authentication and <i>Privacy</i> protocol
Privacy protocol:	Select the privacy protocol (DES or AES) which has been activated in the <i>Network Management System</i> .

Privacy passphrase:	Enter the privacy passphrase for secure communication with the <i>Network Management System</i> .
Engine ID:	Enter an <i>Engine ID</i> which clearly identifies the SNMP agent within the network.

8. Click **OK** to save your settings and to leave the window.

How to delete existing traps:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network > SNMP trap** tabs.
4. Select the receiver to be deleted and click **Delete**.
5. Click **OK** to save your settings and to leave the window.

How to generate a test event:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Network > SNMP trap** tabs.
4. Click on **Generate test event**.
5. Click **OK** to save your settings and to leave the window.

NOTE: If properly configured, the *Trap* message is displayed within your *Network Management System*.

Logbook

The *Logbook* of a device of the KVM system allows you to collect any information.

ADVICE: Write down if you plan on changing the configuration of the device and assign the entry with a status («Open»).

After these changes have been carried out, assign the «Closed» status to the logbook entry. This way you can refer to the logbook to look up the times at which the changes have been made.

If you want to save the logbooks or edit them with other programs, the logbooks of the different devices can be printed, copied to the clipboard, or exported to a file.

The dialogue entries of the logbook

After the logbook has been called up, the «Logbook configuration» dialog shows an overview of all logbook entries that have been saved so far.

All details regarding the entry are shown by double-clicking.

The «Logbook configuration» window

The *Logbook configuration* window shows a table with all logbook entries that have been made until then.

The table displays the *Subject* and *Status* («Open» or «Closed») and the *Date* the entry has been last edited.

NOTE: By default, the table is sorted in descending order according to the contents of the «Status» column. This order is indicated by a small triangle in the column header.

If you want to sort the entries according to the contents of another column, click the header of the desired column. Another click reverses the sort sequence.

The following actions can be carried out in the logbook:



- **New:** create a new logbook entry
- **Edit:** update an existing logbook entry
- **Delete:** delete a logbook entry
- **Print:** print a logbook entry
- **Export:** export the data of the logbook entry to csv file
- **Copy:** copy the details of the logbook entry to the clipboard

Viewing a logbook entry in detail

Double-click a logbook entry to show its details. The overview provides the following information:

Subject:	short description (max. 128 characters) that allows a quick overview in the table and on the print-out
Body:	detailed description (max. 1.024 characters)
Status:	current status (»Open« or »Closed«)
Creator:	user name of the person who created the logbook entry
Created:	date and time the entry has been originally created
Last editor:	user name of the person who last changed the entry
Last edited:	date and time the entry has been last changed

The upper part of the window shows several buttons that provide the following functions:

-  (**left arrow**): shows the previous logbook entry (if available)
- **Print**: print logbook entry
- **Export**: export the data of the logbook entry to csv file
- **Copy**: copy the details of the logbook entry to the clipboard
-  (**right arrow**): shows the last logbook entry (if available)

NOTE: The functions of the *Print*, *Export* and *Copy* buttons correspond to the entries of the same name in the context menu of the logbook entries.

These functions are described on the following pages.

Basic logbook functions

The basic logbook functions enable you to create new or edit and delete the existing logbook entries.

IMPORTANT: Any device within a KVM system provides a separate logbook.

Creating a new logbook entry

How to create a new logbook entry for a device:

1. Click on the folder that contains the device whose logbook you want to open.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Click on **New**.

4. Enter the **Status** (max. 128 characters) of the logbook entry.

ADVICE: The subject is shown in the overview of the logbook entries and allows a quick overview of the entries.

5. If necessary, use the **Body** entry to change the detailed description (max. 1.024 characters) of the logbook entry.
6. Click **OK** to save the logbook entry.

Changing a logbook entry

How to change the logbook entry of a device:

1. Click on the folder that contains the device whose logbook entry you want to change.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Click the entry to be edited and click on **Edit**.
4. If necessary, change the **Subject** (max. 128 characters) of the logbook entry.

ADVICE: The subject is shown in the overview of the logbook entries and allows a quick overview of the entries.

5. If necessary, use the **Body** entry to change the detailed description (max. 1.024 characters) of the logbook entry.
6. Use the **Status** button to select between the »Open« and »Closed« options.
7. The following information are provided in this dialog:

Creator:	user name of the person that created the logbook entry
Created:	date and time the entry has been originally created
Last editor:	user name of the person that last changed the entry
Last edited:	date and time the entry has been last changed

8. Click **OK** to save the logbook entry.

Deleting a logbook entry

How to delete the logbook entry of a device:

1. Click on the folder that contains the device whose logbook entry you want to delete.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Click the entry to be deleted and click on **Delete**.
4. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Advanced functions

The advanced functions allow you to print or export the logbook entries. The data of a logbook entry can also be copied to the clipboard.

The advanced functions can either be called up via the buttons in the detail dialog of the logbook or the context menu of the »Logbook configuration« dialog.

NOTE: The functions of several logbook entries can only be applied if they have been called up via the context menu.

Printing logbook entries

How to print one or several logbook entries:

1. Click on the folder that contains the device whose logbook entry you want to change.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Mark one or several existing logbook entries.

NOTE: To select several logbook entries, press the **Ctrl** key and select the different entries by mouse.

4. Right-click one of the marked entries and click on **Print**.
5. Select the **Printer** on which the document is to be printed.

NOTE: If desired, you can also adjust the headline, the number of copies, the page layout and the frame settings.

6. Click on **Print**.

Exporting logbook entries

Use the export function to export the data of a logbook entry to a CSV file.

This file format is usually used for exchanging data between different programs. A CSV file that has been created with the *Config Panel* web application can be read with all common spreadsheet programs, for example.

NOTE: CSV is short for *Comma-Separated Values*.

How to export one or several logbook entries:

1. Click on the folder that contains the device whose logbook entry you want to change.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Mark one or several existing logbook entries.

NOTE: To select several logbook entries, press the **Ctrl** key and select the different entries by mouse.

4. Right-click one of the marked entries and click on **Export**.
5. Use the **File Name** section to select the location and the file name of the file to be created.
6. The configuration section offers the following settings:

Column headings:	Select if the column headings (<i>Subject, Body, ...</i>) are to be output in the CSV file. Options: Yes, No
Delimiter:	Select the desired delimiter between the different data fields in the CSV file. Options: Tabulator, Semicolon, Comma, Space

7. Click on **Export**.

Copying the logbook entries

As an alternative to the export function, which creates a CSV file, the copy function can be used to copy logbook entries to the clipboard of the operating system.

The copied data can be pasted to any application that has access to the clipboard.

How to copy one or several logbook entries:

1. Click on the folder that contains the device whose logbook entry you want to change.
2. Right-click on the desired device and click on **Logbook** in the context menu.
3. Mark one or several existing logbook entries.

NOTE: To select several logbook entries, press the **Ctrl** key and select the different entries by mouse.

4. Right-click one of the marked entries and click on **Copy**.
5. Open a document in the application to which you want to copy the data and press **Ctrl+V**.

Shared editing

The web application enables two users with the respective rights to edit settings at the same time.

For example, if two users simultaneously change the user account settings, the web application informs the other user about these changes:

- A message in purple appears in the upper row of the footer and highlights the other user's changes.
- The changed setting or the menu item in the submenu, which contains this setting, is displayed in green.

The following options are provided to process the collected data:

Discard data:	1. Click on Reload to read the current values of the dialogue from the database.
Overwrite all data:	1. Click on Accept . 2. Click on Overwrite all data .
Only save own changes:	1. Click on Accept . 2. Click on Only save own changes .

Users and Groups

Efficient rights administration

The web application administrates up to 256 user accounts as well as the same amount of user groups. Any user within the system can be a member of up to 20 groups.

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

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

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

The effective right

The effective right determines the right for a particular operation.

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

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

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

Right	User <i>JDoe</i>	Group <i>Office</i>	Group <i>TargetConfig</i>	Effective right
Target config	No	No	Yes	Yes
Change own password	No	Yes	No	Yes
Target access	Full	View	No	Full

The settings of the *Target config* and *Change own password* rights result from the rights assigned to the user groups. The *Target access* right which, in this case, enables full access, was given directly in the user account.

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

ADVICE: Click the **Details** button to get a list of the groups and rights that are assigned to the user account.

Efficient user group administration

User groups enable the creation of a shared right profile for several users with identical rights. Furthermore, the user accounts that are included in the member list can be grouped and therefore no longer have to be individually configured. This facilitates the rights administration within the matrix system.

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

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

EXAMPLE: Create more groups if the user rights are to be further divided. If, for example, some users of the »Office« group are to be provided with the *multi-access* right, a respective user group can be created:

- Create a user group (e. g., »Office_MultiAccess«) with identical settings for the »Office« group. The *multi-access* right is set to *full*. Assign the respective user accounts to this group.
- Create a user group (e. g., »MultiAccess«) and only set the *multi-access* right to *Yes*. In addition to the »Office« group, also assign the respective user accounts to this group.

In both cases, the user is provided with the *full* effective right for *multi-access*.

ADVICE: The user profile offers the possibility to provide extended rights to a group member.

Administering user accounts

User accounts enable you to define individual rights for every user. The personal profile also provides the possibility to define several user-related settings.

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

Creating a new user account

The web application administrates up to 256 user accounts. Any user account is provided with individual login data, rights and user-related settings for the KVM system.

How to create a new user account:

1. Click on **User area > User** in the tree view.
2. Right-click the display range and afterwards the **New** entry in the context menu.
3. Enter the following information within the interface:

Name:	Enter the desired username.
Password:	Enter the user account password.
Repeat password:	Repeat the password.
Clear text:	If necessary, mark this entry to view and control both passwords.
Full name:	If desired, enter the user's full name.
Comment:	If desired, enter a comment regarding the user account.
Enabled:	Click this entry to activate the user account.

If the user account is deactivated, the user is not able to access the KVM system.

4. Click **OK** to save the entered data.

IMPORTANT: After the user account has been created, it is assigned with no rights. Add the user account to an existing user group or provide it with individual rights (see page 62).

Renaming the user account

How to rename a user account:

1. Click on **User area > User** in the tree view.
2. Right-click the user account to be edited and click the **Configuration** entry in the context menu.
3. Enter the new username in the **Name** entry.
4. *Optional:* Enter the user's full name in the **Full name** entry
5. Click **OK** to save your settings.

Changing the user account password

How to change the user account password:

1. Click on **User area > User**.
2. Right-click the user account to be edited and click the **Configuration** entry in the context menu.
3. Click on **Change password**.
4. Change the following data within the entry mask:

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

5. Click **OK** to save the new password.
6. Click **OK** to save your settings.

Changing the user account rights

Any user account can be assigned with different rights.

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

Name	Right	Page
Change own password	Change own password	page 66
Superuser right	Unrestricted access to the configuration of the system	page 65
WebIf login	Login to the <i>Config Panel</i> web application	page 66

Changing a user account's group membership

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



How to change a user account's group membership:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user group to be edited and click the **Configuration** entry in the context menu.
3. Click the **Members** tab.

Now you can easily add members to or delete them from any user group.

The window consists of two tables. These tables list the user accounts of the KVM matrix system:

Unassigned:	lists all user accounts that are <i>not</i> assigned to this group
Assigned group members:	lists all user accounts that are assigned to this group

4. Mark the user account you want to add to or delete from the group.
5. Click the  button (*right arrow*) to add the user account to the group or the  button (*left arrow*) to delete it from the list.

Enabling/Disabling a user account

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

How to enable/disable a user account:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user account you want to enable/disable and click the **Configuration** entry in the context menu.

- Click the **Enabled** entry to enable the user account.

Disable the entry if you want to lock the access to the system for this user account

- Click the **OK** button to save your settings.

Deleting a user account

How to delete a user account:

- Click on the **User area > User groups** entries in the tree view.
- Right-click the user account you want to delete and click the **Delete** entry in the context menu.
- Click **OK** to confirm the confirmation prompt.

Administrating user groups

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

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

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

Creating a new user group

The user can create up to 256 user groups within the system.

How to create a new user group:

- Click on the **User area > User groups** entries in the tree view.
- Right-click the display range and click the **New** entry in the context menu.
- Enter the following data in the entry mask:

Name: Enter the name of the user group.

Enabled: Activate this entry to enable the user group.

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

Comment: If necessary, enter a comment regarding the user group.

- Click **OK** to save your settings.

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

Renaming a user group

How to rename a user group:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user account you want to rename and click the **Configuration** entry in the context menu.
3. Use the **Name** entry to enter the new name of the user group.
4. Click **OK** to save your settings.

Changing the user group rights

The various user groups can be assigned with different rights.

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

Name	Right	Page
Change own password	Change own password	page 66
Superuser right	Unrestricted access to the configuration of the system	page 65
WebIf login	Login to the <i>Config Panel</i> web application	page 66

Administrating user group members



How to administrate user group members:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user group to be edited and click the **Configuration** entry in the context menu.
3. Click the **Members** tab.

Members can now easily be added to or deleted from the user groups.

The window consists of two tables. These tables list the user accounts of the KVM system:

Unassigned:	lists all user accounts that are <i>not</i> assigned to this group
Assigned group members:	lists all user accounts that are assigned to this group

4. Mark the user account you want to add to or delete from the group.
5. Mark the user account you want to add to or delete from the group. Now click the  button (*right arrow*) to add the user account to the group or the  button (*left arrow*) to delete it from the list.

(De)activating a user group

How to (de)activate a user group:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user group you want to (de)activate and click the **Configuration** entry in the context menu.
3. Activate the **Enabled** entry to activate the user group.

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

4. Click the **OK** button to save your settings.

Deleting a user group

How to delete a user group:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the user group you want to delete and click the **Delete** entry in the context menu.
3. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

System rights

Rights for full access (Superuser)

The *Superuser* right enables you to fully access and configure the KVM system.

NOTE: The information about the user rights, which have been assigned before, are still stored when the *Superuser* right is activated. After the *Superuser* right has been withdrawn, the saved rights do apply again.

How to change the *Superuser* right:

1. If you want to change this right of a user account, click the **User area > Users** entries in the tree view.
For changing the rights for a user group, click the **User area > User groups** entries.
2. Right-click the user account or the user group you want to configure and click the **Configuration** entry in the context menu.
3. Click the **System rights** tab.

4. Use the **Superuser** entry to select between the following options:

Yes:	allows full access to the KVM system and the connected devices
No:	denies full access to the KVM system and the connected devices

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

Changing the login right to the web application

How to change the login right to the web application:

1. If you want to change this right of a user account, click the **User area > Users** entries in the tree view.

For changing the rights for a user group, click the **User area > User groups** entries.

2. Right-click the user account or the user group you want to configure and click the **Configuration** entry in the context menu.
3. Click the **System rights** tab.
4. Use the **Web Interface Login** entry to select between the following options:

Yes:	enables access to web application
No:	denies access to web application

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

Rights to change your own password

How to change the right to change your own password:

1. If you want to change this right of a user account, click the **User area > Users** entries in the tree view.

For changing the rights for a user group, click the **User area > User groups** entries.

2. Right-click the user account or the user group you want to configure and click the **Configuration** entry in the context menu.
3. Click the **System rights** tab.
4. Use the **Change own password** entry to select between the following options:

Yes:	allows the user to change the user account password
No:	denies the user to change the user account password

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

The »KVM combinations« folder

The *KVM combinations* folder enables you to group different devices in any folders. Especially in larger system, this folder provides better orientation.

The devices can be grouped according to locations (e. g. server room) or other features (e. g. the operating system of the connected computer).

ADVICE: The devices of *different* classes – e.g. the target modules of a matrix system or an extender – can be grouped within one folder.

Folder administration

The *KVM combinations* folder provides the following system folders:

[Unassigned]:	This folder lists all devices that are not assigned to any KVM combination.
[All devices]:	This folder lists all devices of the KVM system.

NOTE: You cannot delete or rename system folders.

Creating new folders

How to create an empty folder:

1. Right-click on **KVM combination** in the tree view and click on **New folder** in the context menu.

ADVICE: If you want to create a subfolder, right-click the main directory and click on **New folder**.

2. Use the **Name** entry to enter the desired name.
3. *Optional:* Use the **Comment** entry to enter a comment.
4. Click **OK** to create the folder.

Assigning a device to a folder

NOTE: Each device can be listed in any number of subfolders.

How to group the *connected devices* in a new folder:

1. Click on **KVM combinations** > **[All devices]** in the tree view.
2. Right-click a connected device and click on **Group connected devices** in the context menu.
3. Use the **Name** entry to enter the desired name.
4. *Optional:* Use the **Comment** entry to enter a comment.
5. Click **OK** to group the devices in the new folder.

How to assign a device to an existing folder:

1. Click on **KVM combinations** > **[All devices]** in the tree view.
2. Right-click the device to be assigned and click on **Copy device** in the context menu.
3. Open the folder to which the device is to be assigned to.
4. Right-click the main view and click on **Paste device** in the context menu.

Deleting a device from a folder

A device can be deleted from the folder by moving it to the *[Unassigned]* group or by selecting the **Remove from folder** entry in the context menu.

How to cancel a target module's assignment to a folder:

1. Click on **KVM combinations** > **[All devices]** in the tree view.
2. Open the folder to which the device is assigned to.
Right-click the device whose assignment you want to delete and click on **Remove from folder** in the context menu.

Renaming a folder

How to rename a folder:

1. Click on **KVM combinations** > **[All devices]** in the tree view.
2. Right-click the folder to be renamed and click on **Rename folder** in the context menu.
3. Edit the name and press **Enter**.

Deleting a folder

Any created folders can be deleted at any time.

If a folder contains devices while it is deleted, these devices are automatically moved to the *[Unassigned]* group.

NOTE: The system folders *[Unassigned]* and *[All devices]* are administrated by the web application and cannot be deleted.

How to delete a folder:

1. Click on **KVM combinations** > **[All devices]** in the tree view.
2. Right-click the folder to be deleted and click on **Delete folder** in the context menu.

NOTE: You can select several folders by pressing **Shift**, **Ctrl** and the left mouse key at the same time.

3. Confirm the security request by clicking **Yes** or cancel the task by clicking **No**.

Advanced functions of the KVM system

Temporarily (de)activating SNMP traps (Maintenance mode)

By activating the maintenance mode, the user is enabled to deactivate SNMP traps (see page 48), e.g. for devices that are occupied for reasons of maintenance.

The status messages are displayed again after the maintenance mode has been deactivated.

(De)activating the maintenance mode

How to (de)activate a device's maintenance mode:

1. Use the tree view to click on **UserCenter**.
2. Right-click the device and click on **Maintenance > On** or **Maintenance > Off** in the context menu.

Viewing a list of devices in maintenance mode

How to display the list of devices in maintenance mode:

1. Click on the **System monitoring > Maintenance** folders in the tree view.

The main view lists the respective devices.

ADVICE: The devices in *Maintenance* mode are always displayed in yellow.

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. Use the tree view to click on **UserCenter**.
2. Right-click the device and click on **Identification LED > On** or **Identification LED > Off** in the context menu.

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.

NOTE: To save and restore your configuration, you can go to **System > Tools** in the directory tree or use the **Tools icon**.

How to save the configuration of the KVM system:

1. In the directory tree, click on **System > Tools**.
2. Click **Backup**.
3. Enter the location and the name of the backup file under **Path**.

ADVICE: Use the file button to select the name and the location of the backup file via the file dialog.

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 directory tree, click on **System > Tools**.
2. Click on **Restore**.
3. Enter the location and the name of the backup file under **Path**.

ADVICE: Use the file button to select the name and the location of the backup file via the file window.

4. Use the information given under **Creation date** and **Comment** to check if you selected the right backup file.
5. Select the scope of data you want to restore: You can restore either the **network settings** and/or the **Application settings**.

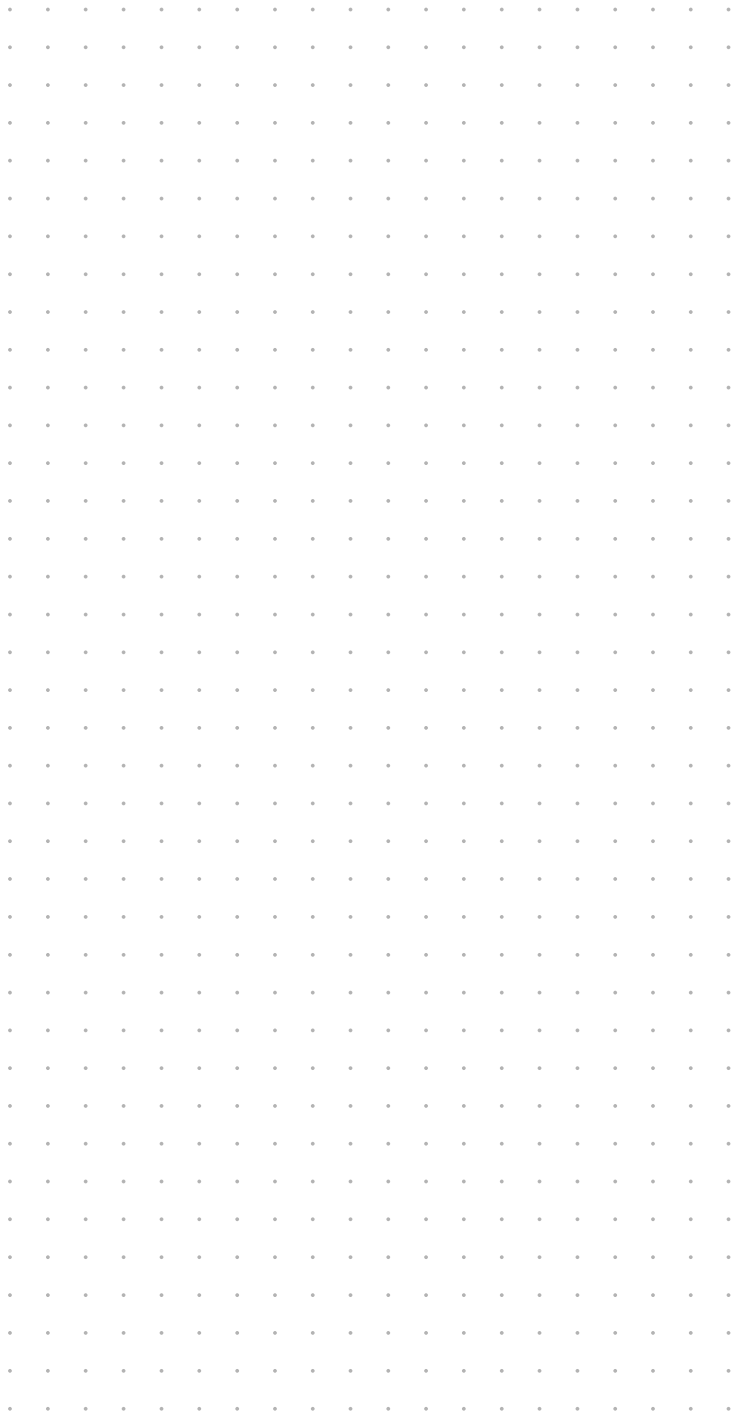
NOTE: If one of these options cannot be selected, the data for this option was not stored.

6. Click **Restore**.
7. Click **OK** to close the window.

Overview of the monitoring values

The device-specific branches and the *KVM combinations* and the *Critical devices* branch of the tree view let you view current status information about the device.

Feature	Status	Meaning
Fan speed	Numerical value	Fan speed (rpm)
Main power	On	The power supply has been established via the »Main power« power pack.
	Off	No power is supplied via the »Main power« power pack.
Network A	Down	No connection to network
	Up	The connection to the network has been established
Network B	Down	No connection to network
	Up	The connection to the network has been established
Redundant power	On	The power supply has been established via the »Red. power« power pack
	Off	No power is supplied via the »Red. power« power pack
Temperature	Numerical value	Current temperature in the device



NOTES



The manual is constantly updated and available on our website.

<http://gdsys.de/A9200124>

Guntermann & Drunck GmbH

Dortmunder Str. 4a
57234 Wilnsdorf

Germany

<http://www.GDsys.de>
sales@GDsys.de

Guntermann & Drunck
GmbH

seit 1985

