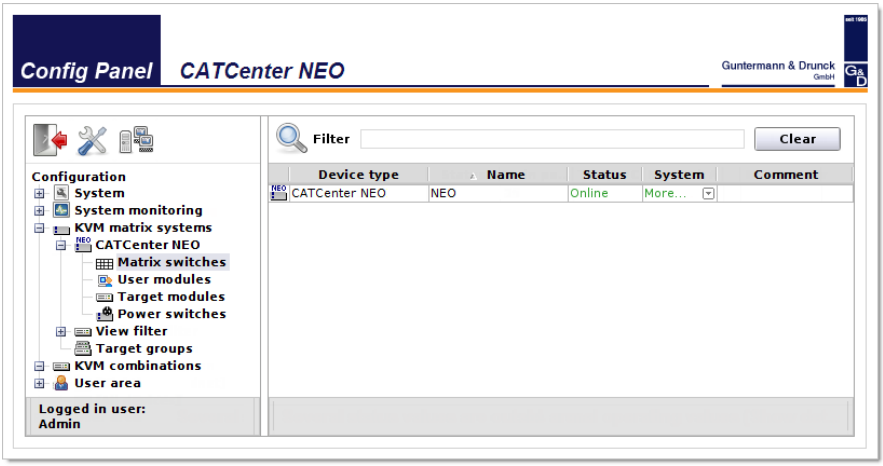
G&D CATCenter NEO



EN

Web Application »Config Panel«

Configuring the matrix switch

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

Version 2.40 – 24/07/2014
Version: 1.11.6

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

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

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

Table of contents

Chapter 1: Basic functions

System requirements **9**
Supported web browsers 9
Java Runtime Environment 9

Configuring the network settings **10**

Getting started **11**
Starting the web application 11
Security instructions of the web browser 11
User login at the web application 12
Operating the web application 12
User interface 12
Frequently used buttons 14
User logout 14
Selecting the default language of the web application 15
Selecting the hash algorithm for storing passwords 15
Showing the version number of the web application 15

Basic configuration of the web application **16**
Network settings 16
Configuring the network settings 16
Configuring the global network settings 17
Increasing the reliability of network connections through link aggregation 18
Reading out the status of the network interfaces 20
Creating and administrating netfilter rules 20
Creating new netfilter rules 20
Editing existing netfilter rules 21
Deleting existing netfilter rules 23
Changing the order/priority of existing netfilter rules 23
Creating an SSL certificate 24
Special features for complex KVM systems 24
Creating a Certificate Authority 24
Creating any certificate 25
Creating and signing the X509 certificate 26
Creating a PEM file 27
Selecting an SSL certificate 27
Firmware update 28
Restoring the default settings 29

Network functions of the devices **30**
NTP server 30
Time sync with an NTP server 30
Setting time and date manually 31

Logging syslog messages ... 32
Locally logging the syslog messages ... 32
Sending syslog messages to a server ... 33
Viewing and saving local syslog messages ... 34
User authentication with directory services ... 35

Monitoring functions ... **37**
Viewing monitoring values ... 38
Listing values by applying monitoring sets ... 38
Listing individual values of critical devices ... 38
Disabling monitoring values ... 38
Advanced function regarding the administration of critical devices ... 39
Messages regarding critical statuses of devices ... 39
Viewing the list of critical devices ... 39
Marking messages from critical devices as read ... 40
Administrating monitor groups ... 40
Adding monitoring groups ... 41
Changing name and/or comment of monitoring groups ... 41
Assigning members to monitoring groups ... 42
Duplicating monitoring groups ... 42
Deleting monitoring groups ... 43
Administrating monitoring sets ... 43
Adding monitoring sets ... 44
Changing name and/or comment of monitoring sets ... 44
Assigning members to monitoring sets ... 44
Selecting a monitoring set in the folder configuration ... 45
Duplicating monitoring sets ... 45
Deleting monitoring sets ... 46

Device monitoring via SNMP ... **47**
Practical use of the SNMP protocol ... 47
Configuring the SNMP agent ... 47
Configuring SNMP traps ... 49

Logbook ... **52**
The dialogue entries of the logbook ... 52
The »Logbook configuration« window ... 52
Viewing a logbook entry in detail ... 53
Basic logbook functions ... 53
Creating a new logbook entry ... 53
Changing a logbook entry ... 54
Deleting a logbook entry ... 55
Advanced functions ... 55
Printing logbook entries ... 55
Exporting logbook entries ... 56
Copying the logbook entries ... 57

Shared editing ... **58**

Users and Groups **59**
Efficient rights administration 59
The effective right 59
Efficient user group administration 60
Administrating user accounts 60
Creating a new user account 61
Renaming the user account 62
Changing the user account password 62
Changing the user account rights 63
Changing a user account's group membership 64
Enabling/Disabling a user account 64
Deleting a user account 65
Administrating user groups 65
Creating a new user group 65
Renaming a user group 66
Changing the user group rights 66
Administrating user group members 67
(De)activating a user group 67
Deleting a user group 67
System rights 68
Rights for full access (Superuser) 68
Changing the login right to the web application 68
Rights to change your own password 69

The »KVM combinations« folder **70**
Folder administration 70
Creating new folders 70
Assigning a device to a folder 71
Deleting a device from a folder 71
Renaming a folder 72
Deleting a folder 72

Advanced functions of the KVM system **73**
Temporarily (de)activating SNMP traps (Maintenance mode) 73
(De)activating the maintenance mode 73
Viewing a list of devices in maintenance mode 73
Identifying a device by activating the Identification LED 73
Saving and restoring the data of the KVM system 74
Activating the premium functions 75

Overview of the monitoring values **76**
»CATCenter NEO« matrix switch 76

Chapter 2: Matrix Systems

Target modules **77**
Adjusting access and configuration rights 77
Accessing a target module 77
Accessing a target group 78
Access mode if a target computer is accessed by several users 79
Changing the rights to configure the target modules 81
Changing the rights to reset or reactivate a PS/2 mouse 81
Basic configuration of the target modules 82
Renaming a target module 82
Changing the comment of a target module 82
Deleting a target module from the KVM matrix system 82
Copying the target module config settings 83
Settings for special hardware 84
Keymode for Apple computers 84
Keymode for USB multimedia keyboards 84
Support for servers of IBM's RS/6000 series 85
Enhanced functions 85
»Multiuser« display 85
Adjusting the power management of the target module 86
Viewing the status information of a target module 86
Viewing the cascade information 87

User consoles **88**
Operating modes of user consoles 88
Standard operating mode 88
Open Access operating mode 88
Video operating mode 88
Selecting the user console's operating mode 89
Basic configuration of user consoles 89
Changing the name or the comment of a user console 89
(De)activating the user console 90
Copying the console config settings 90
Deleting a user console from the KVM matrix system 91
Settings for special hardware 91
Adjusting the scancode set of a PS/2 keyboard 91
Activating the support for special PS/2 keyboards 92
Advanced functions 92
Setting the automatic user logout 92
Automatically disconnecting the access to a target module 93
Viewing the status information of a user module 93
Remembering the username in the login box 94
Setting the hold time for the screensaver 94
Viewing the cascade information 95

Target groups and view filters **96**
Difference between target groups and view filters 96
Intended use of target groups 96
Intended use of view filters 96
Administrating target groups 96
The »New Targets« target group 96
Creating a new target group 97
Changing the name or comment of a target group 97
Administrating target group members 97
Deleting a target group 98
Administrating view filters 99
Creating a new view filter 99
Assigning a target module to a view filter 99
Cancelling a target module's assignment to a view filter 99
Renaming a view filter 100
Deleting a view filter 100

Accessing the target modules via select keys **101**
Changing the select key modifier or the valid keys 101
Administrating select key sets 102
Creating a select key set 102
Changing name, comment or global allocation of a select key set 102
Defining select keys for the target modules 103
Assigning a select key set to a user account 104
Deleting a select key set 104

Automatically or manually switching the target modules **105**
Auto scanning all target modules (Autoscan) 105
Applying the *Autoscan* function 105
Configuring the scantime of the *Autoscan* function 105
Auto scanning all active target modules (Autoskip) 106
Applying the *Autoskip* function 106
Configuring the scantime of the *Autoskip* function 106
Scanning the target modules manually (Stepscan) 107
Starting and stopping the *Stepscan* function 107
Configuring keys to scan the targets manually 107
Administrating scanmode sets 108
Creating a scanmode set 108
Changing a scanmode set's name, comment or global assignment 109
Assigning the target modules to a scanmode set 109
Assigning a scanmode set to a user account 110
Deleting a scanmode set 111

Configuring the On-Screen Display (OSD) **112**
Configuration 112
Changing the hotkey to call the OSD 112
Opening the on-screen display via double keypress 113
Adjusting the information display 113
Changing the colour of the information display 114
Defining a standard view filter 115
Selecting the mode for OSD synchronisation 115
Selecting a keyboard layout for OSD entries 116
Operating the on-screen display by mouse 117
Enabling/disabling the on-screen display 117

Video tuning **118**
Rights administration 118
Changing the right to configure video profiles 118

Power switch **119**
Rights administration 119
Rights to switch the power outlets of a target module 119
Rights to switch the power outlets of a target group 120
Configuration 120
Assigning a power switch power outlet to the target module 120
Changing the name or the comment of a power switch 121
Deleting a power switch from the KVM matrix system 121
Viewing the status information of a target module 122

Special functions for cascaded KVM matrix systems **123**
Basic functions 123
Changing the name or comment of a matrix switch 123
Deleting a slave matrix switch from the system 123
Configuration settings 124
Defining the cascade mode of a matrix switch 124
Forwarding target names to the slave matrix switches 124
Viewing the status information of a matrix switch 125
Viewing cascade information 126
Copying the config settings of a matrix switch 127

Replicating the database of a KVM matrix switch **128**
Overview of the data to be replicated 128
Replicating the database 130
Adding a destination 131
Changing the address settings of a destination 131
Deleting a destination 131

Advanced functions of the KVM matrix switch **132**
Adjusting the RS232 mode and the baud rate of the service port 132
Rights administration 133
Right to change the personal profile 133
Optional functions 134

Push-Get function (option) **135**
Changing the right for carrying out the Push-Get function 135

IP-Control-API (option) **136**
C++class library functions 136
Configuring accesses for text-based control 137

Tradeswitch function (option) **138**
Basic configuration 138
Creating Tradeswitch workplaces 138
Changing the name and comment of a Tradeswitch workplace 139
Deleting a Tradeswitch workplace 139
Changing the Tradeswitch key and the valid keys 139
Detailed configuration of a Tradeswitch workplace 141
Assigning devices to a Tradeswitch workplace 141
Defining the master workplace of the Tradeswitch workplace 142
Enhanced functions 143
(De)activating the Tradeswitching information display 143
Starting the user module without keyboard 143

1 Basic functions

+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 9).

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
- comprehensive target administration
- 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 10.

Supported web browsers

The following web browsers support the web application:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Mozilla Firefox 31

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.java.com/de/download/

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

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

ADVICE: As an alternative to the steps described below, the initial configuration of the network interfaces of a matrix switch can be carried out via on-screen display.

The following table lists the default settings of the *Network A* network interface:

IP allocation:	Static
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Connection type:	Auto

NOTE: In the default, the *Network B* interface is deactivated.

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

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

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

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

Getting started

This chapter 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 9.

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.

The certificate contains the following features:

MD5 fingerprint:

47:F0:FF:87:96:84:D7:C8:63:43:6D:77:26:64:59:CD

SHA1 fingerprint:

68:92:9F:83:04:CD:7A:12:ED:2B:FE:34:0F:DF:BA:4B:0C:EF:47:30

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: ▪ **(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 62).

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:

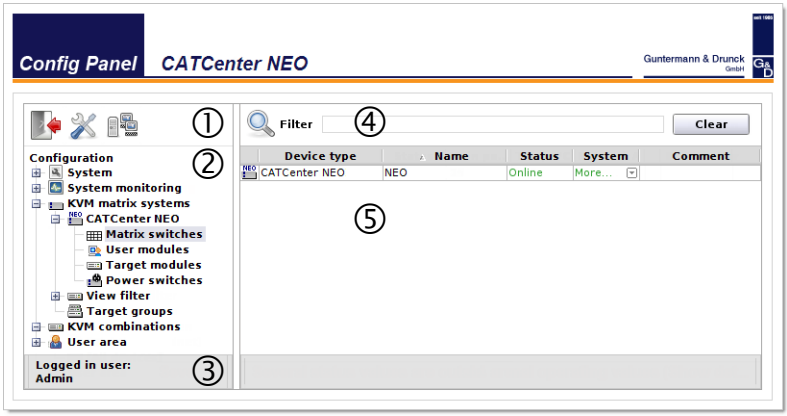


Figure 1: User interface

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:	The filter function can be used to limit the elements that are displayed in the main view. 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. Click **Delete** to cancel the filtering.
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 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:	Save your settings. *Afterwards, the window closes.*
Apply:	Save your settings. *The window remains open.*
Cancel:	Cancel your settings and close window.
Print:	Call print interface to select printer, page orientation and further settings. After the settings have been selected, the interface information (e.g., the *cascade information*) can be printed.
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.

Selecting the hash algorithm for storing passwords

By default, user passwords are stored as MD5 hash values in the database.

You can also change the hash algorithm to **bcyrpt**.

NOTE: The hash algorithm **bcrypt** is supported from version 1.3.000.

Update the firmware of one of the devices before resetting a backup containing **bcrypt** hash values.

How to change the hash algorithm to store passwords:

1. In the directory tree, click on **System**.
2. Double-click on **Configuration** in the main view.
3. Click the **System** tab.
4. Chosse the algorithm from the **Hash algorithm** options:

   - **MD5**
   - **bcrypt**

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

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 10.

Configuring the network settings

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:	Use the pull-down menu to select the operating mode of **Interface A** or **Interface B**: ▪ **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. *Use the »Link aggregation« tab to configure the network interfaces.*
IP address:	Only if the *Static* operating mode is selected: Enter the interface IP address.

Netmask:	Only if the *Static* 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.

4. 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:

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

Global preferences:	Use the pull-down menu to select the operating mode: ▪ **Static:** uses static settings. ▪ **DHCP:** obtains the settings from a DHCP server.
	The following settings are automatically obtained in the *DHCP* operating mode. Inputs are not possible.
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.

4. 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 addres 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: - **Off:** disables link aggregation. *Use the »Interfaces« tab to configure the network interfaces.* - **Static:** A static IP address is assigned. - **DHCP:** obtain IP address from a DHCP server.
IP address:	Enter the IP address of the interface (only if you have selected the *Static* operational mode).
Netmask:	Enter the netmask of the network (only if you have selected the *Static* operational mode).

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

Primary slave:	Choose if the data traffic should run via *Network A* (**Interface A**) or *Network B* (**Interface B**). As soon as the selected interface is available, the data traffic is sent via this interface. If you choose the option **None**, the data traffic is sent via any interface. The interface only changes if the active interface is down.
Link monitoring:	Choose if you want the **MII** or **ARP mode** (description see below) to be used to monitor the interface.
MII down delay:	Time delay in milliseconds before a failed network interface is disabled. The value must be a multiple of 100 ms (the MII link monitoring frequency).
MII up delay:	Time delay in milliseconds before a reset network interface is enabled. The value must be a multiple of 100 ms (the MII link monitoring frequency).
ARP interval:	Enter the interval (100 to 10,000 milliseconds) according to which the incoming ARP packets of the network interfaces are to be checked.
ARP validate:	The validation ensures that the ARP packet for a particular network interface is generated by one of the listed ARP targets. Choose if or what incoming ARP packets are to be validated: ▪ **None:** ARP packets are not validated (default). ▪ **Active:** Only the ARP packets of the active network interface are validated. ▪ **Backup:** Only the ARP packets of the inactive network interface are validated. ▪ **All:** The ARP packets of all network interfaces within the group are validated.
ARP target:	The table lists all configured ARP targets. Use the **New**, **Edit,** and **Delete** buttons to administrate the ARP targets.

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: ▪ **All** ▪ **Interface A** ▪ **Interface B** ▪ **[Name of a group of network interfaces]**

Option:	Use the pull-down menu to select how the rule's sender information are to be interpreted: ▪ **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 *not* comply with the indicated IP address or MAC address.
IP address/ Netmask:	Enter the data packet IP address or use the **Netmask** entry to enter the address space of the IP addresses. **Examples:** ▪ **192.168.150.187:** for IP address 192.168.150.187 ▪ **192.168.150.0/24:** IP addresses of section 192.168.150.x ▪ **192.168.0.0/16:** IP addresses of section 192.168.x.x ▪ **192.0.0.0/8:** IP addresses of section 192.x.x.x ▪ **0.0.0.0/0:** all IP addresses **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.
MAC address:	Enter the MAC address to be considered in this filter rule. **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.
Filter rule:	▪ **Drop:** Data packets whose sender information comply with the IP address or MAC address are *not* 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: ▪ **All** ▪ **Interface A** ▪ **Interface B**
Option:	Use the pull-down menu to select how the rule's sender information are to be interpreted: ▪ **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 *not* 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:** ▪ **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 The *IP address* and/or a *MAC address* can be indicated within a rule.
MAC address:	Enter the MAC address to be considered in this filter rule. **NOTE:** The *IP address* and/or a *MAC address* can be specified within a rule.
Filter rule:	▪ **Drop:** Data packets whose sender information comply with the IP address or MAC address are *not* 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 24) to create certificates for those devices.

The identical PEM file (see page 27) 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 *CATCenter NEO*).

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

   b. Windows

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

2. The *gdcd.pem* file is created 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 24).

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.

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 50 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 **KVM Matrix systems > [System name] > Matrix switches**.
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: ▪ **Disabled** ▪ **Enabled**
NTP server 1:	Enter the IP address of a time server.
NTP server 2:	O*ptionally* enter the IP address of a second time server.
Time zone:	Use the pull-down menu to select the time zone of your location.

5. Click **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 **KVM Matrix systems > [System name] > Matrix switches**.
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
- **1:** Alert
- **2:** Critical
- **3:** Error
- **4:** Warning
- **5:** Note
- **6:** Info
- **7:** Debug

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

Locally logging the syslog messages

How to locally log the syslog messages:

1. Use the tree view to click on **KVM Matrix systems > [System name] > Matrix switches**.
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: ▪ **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.

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

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 **KVM Matrix systems > [System name] > Matrix switches**.
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: ▪ **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. If you select severity code *2 - Critical*, messages for this code and for the severity codes *1 - Alert* and *0 - Emergency* are logged.
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: ▪ **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 **KVM Matrix systems > [System name] > Matrix switches**.
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: Select the **Local** option if the user administration is to be carried out by the KVM system.

If a particular directory service is to be applied, select the respective entry from the pull-down menu:

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

ADVICE: After the directory service has been selected, collect the settings of the directory service server in the **Server settings**.

Fallback: 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.

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:

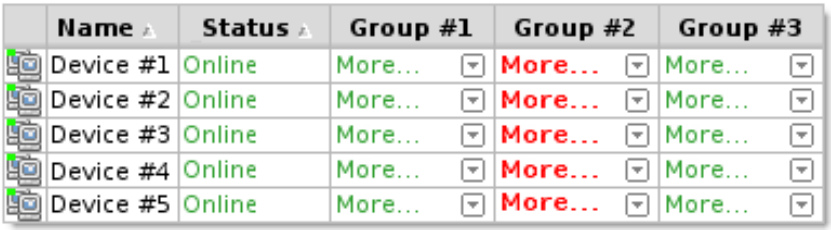
- If a user account is disabled or deleted in the directory service, this action can also be carried out within the user database of the KVM system.
- Only activate the fallback system in reasonable exceptional cases.

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 123 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 **KVM Matrix systems > [System name] > Matrix switches**.
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 45 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

IMPORTANT: The device-specific *KVM matrix systems* branch exclusively displays the individual values.

It is therefore not possible to create and administer monitoring groups.

How to add a new monitoring group:

1. Right-click 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 *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 *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 *not* 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 *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 *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 be 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:

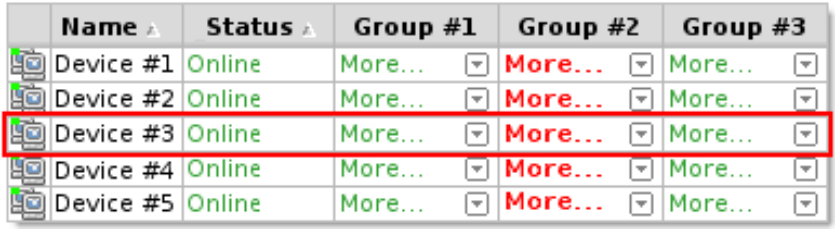


Figure 4: Status of the individual *Status* value and three groups of a monitoring set

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:

> **IMPORTANT:** The device-specific *KVM matrix systems* branch exclusively displays the individual values.
>
> It is therefore not possible to create and administer monitoring groups.

1. Right-click 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 *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 40 ff.) before creating a monitoring set.

How to assign members to a monitoring set:

1. Right-click 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 the 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 *not* 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 a *subfolder* of 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 *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 *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 be 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 **KVM Matrix systems > [System name] > Matrix switches**.
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 *incoming* 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 *View* access (**View**) or deny the access (**No**) via *SNMPv2c* protocol.
Source:	Enter the IP address or the address space of the addresses of incoming SNMP packets. **Examples:** ▪ **192.168.150.187:** Only IP address 192.168.150.187 ▪ **192.168.150.0/24:** IP addresses of space 192.168.150.x ▪ **192.168.0.0/16:** IP addresses of space 192.168.x.x ▪ **192.0.0.0/8:** IP addresses of space 192.x.x.x
Read-only community:	Enter the name of the *Community* which has also been selected in the *Network Management System*.

IMPORTANT: The 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 *Securitiy 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 *View* access (**View**) or deny the access (**No**) via *SNMPv3* protocol.
User:	Enter the username for the communication with the *Network Management System*.
Authentication protocol	Select the authentication protocol (**MD5** or **SHA**) which has been activated in the *Network Management System*.
Authentication passphrase	Enter the authentication passphrase for the communication with the *Network Management System*.
Security level	Select between one of the following options: ▪ **NoAuthNoPriv:** user authentication and *Privacy* protocol deactivated ▪ **AuthNoPriv:** user authentication activated, *Privacy* protocol deactivated ▪ **AuthPriv:** user authentication and *Privacy* protocol activated
Privacy protocol:	Select the Privacy protocol (**DES** or **AES**) which has been activated in the *Network Management System*.
Privacy passphrase:	Enter the privacy passphrase for secure communication with the *Network Management System*.

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

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 **KVM Matrix systems > [System name] > Matrix switches**.
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 *Network Management Servers*.
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 *outgoing* SNMP packets are to be accepted.
Retries:	Enter the number of retries to send an *SNMP Inform*.
	NOTE: Inputs are only possible if the *Inform* option has been selected in the *Notification type* entry.
Timeout:	Enter the time (in seconds) after which an *SNMP Inform* is to be sent again if you have received no confirmation.
	NOTE: Inputs are only possible if the *Inform* option has been selected in the *Notification type* 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 *Network Management System* an.
Authentication protocol	Select the authentication protocol (**MD5** or **SHA**) which has been activated in the *Network Management System*.
Authentication passphrase	Enter the authentication passphrase for the communication with the *Network Management System*.
Security level	Select between one of the following options: ▪ **NoAuthNoPriv:** deactivated user authentication and *Privacy* protocol ▪ **AuthNoPriv:** activated user authentication, deactivated *Privacy* protocol ▪ **AuthPriv:** activated user authentication and *Privacy* protocol
Privacy protocol:	Select the privacy protocol (**DES** or **AES**) which has been activated in the *Network Management System*.

Privacy passphrase:	Enter the privacy passphrase for secure communication with the *Network Management System*.
Engine ID:	Enter an *Engine ID* 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 **KVM Matrix systems > [System name] > Matrix switches**.
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 **KVM Matrix systems > [System name] > Matrix switches**.
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 (*Subject*, *Body*, …) 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 *JDoe*	Group *Office*	Group *TargetConfig*	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: Creat 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.

Administrating 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 63).

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 69
Mouse reset	Reset or reactivate PS/2 mouse	page 81
Multi access	Access type when a target computer is simultaneously accessed	page 79
Personal profile	Change personal user settings	page 133
Push-Get rights	Carry out *Push-Get function*	page 135
Superuser right	Unrestricted access to the configuration of the system	page 68
Target access rights	Access to a target module	page 77
Target config	Configuration of target modules	page 81
Target group access rights	Access to a target group	page 78
Target power group rights	Switch power outlets of a target group	page 120
Target power rights	Switch power outlets of a target module	page 119
WebIf login	Login to the *Config Panel* web application	page 68

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 *not* 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.
3. 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

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

Deleting a user account

How to delete 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 delete and click the **Delete** entry in the context menu.
3. 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:

1. Click on the **User area > User groups** entries in the tree view.
2. Right-click the display range and click the **New** entry in the context menu.
3. 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.

4. 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 69
Mouse reset	Reset or reactivate PS/2 mouse	page 81
Multi access	Access type when a target computer is simultaneously accessed	page 79
Personal profile	Change personal user settings	page 133
Push-Get rights	Carry out *Push-Get function*	page 135
Superuser right	Unrestricted access to the configuration of the system	page 68
Target access rights	Access to a target module	page 77
Target config	Configuration of target modules	page 81
Target group access rights	Access to a target group	page 78
Target power group rights	Switch power outlets of a target group	page 120
Target power rights	Switch power outlets of a target module	page 119
WebIf login	Login to the *Config Panel* web application	page 68

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 *not* 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 49), 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 **KVM Matrix systems > [System name] > Matrix switches**.
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 **KVM Matrix systems > [System name] > Matrix switches**.
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.

Activating the premium functions

After a premium function has been purchased, the user receives a *feature key*. This file contains a key to activate the purchased function(s).

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

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

1. Use the tree view to click on **KVM Matrix systems > [System name] > Matrix switches**.
2. Right-click the device whose *feature key* is to be imported.
3. Click the **Configuration** entry in the context menu.
4. Click the **Features** tab.
5. Click on **Import feature key from file...** and import the feature key (file) via the file interface.

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

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

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

Overview of the monitoring values

The device-specific branches as well as the *KVM combinations* and the *Critical devices* branch of the tree view enable you to view information on the current status of the different devices in the KVM system.

The following pages list the various monitoring values of different devices.

»CATCenter NEO« matrix switch

Feature	Status	Meaning
Fan speed	Numerical value	Fan speed (rpm)
Main power	Off	»Main power« power pack does not supply power.
	On	Power supply via »Main power« power pack
Network A	Down	No connection to network
	Up	Connection to network has been established
Network B	Down	No connection to network
	Up	Connection to network has been established
Redundant power	On	Power is supplied via »Red. power« power pack
	Off	No power is supplied via »Red. power« power pack
Temperature	Numerical value	Current temperature in the device

2 Matrix Systems

The *KVM Matrix systems* in the tree view of the web application can be used to configure various settings of the matrix switches and the connected devices.

The following pages provide a detailed description of these settings.

Target modules

Target modules connect target computers to the KVM matrix system. They can be accessed with user modules.

Adjusting access and configuration rights

Accessing a target module

> **ADVICE:** It is generally recommended to use target groups to help assign all target access rights (see page 66).
>
> This way, you are able to keep an overview of the KVM matrix system. It also benefits the operating performance within the system's on-screen display.

In order to execute particular user settings which deviate from the existing target groups, you can assign a user with individual access rights in addition to the group rights.

How to change the target access rights:

1. Click **User area > Users** in the tree view to change this right.

   If you want to change the rights for a user group, click **User area > User groups**.

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 **Matrix systems > Individual Device Rights** tabs.
4. Choose the desired target module in the list on the left side of the window.

   > **ADVICE:** Use the drop-down menu to choose the target module to be displayed in the selection window.

You can choose between the following options:

[All targets]	Lists all target modules within the system
[Unassigned]	Only lists *[Unassigned]* target modules
Search...	After you have chosen this option, another window opens. Choose the desired *View filter* in the tree to only display the devices which are assigned to this view filter.

5. The **Access** field on the right side of the window enables you to choose between the following options:

No:	Denies access to the computer that is connected to the target module
View:	Allows the user to view the screen content of the computer that is connected to the target module
Full:	Allows full access to the computer connected to the target module

6. Repeat steps 4 and 5 if you want to change the access rights for other target modules.
7. Click **OK** to save your settings.

Accessing a target group

How to change the target group access right:

1. Click the tree view entries **User area > Users** to change this right.

   If you want to change the rights for a user group, click **User area > User groups**.
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 tabs **Matrix systems > Device Group Rights**.
4. Choose the desired target module in the list on the left side of the window.
5. The **Access** field on the right side of the window enables you to choose between the following options:

No:	Denies access to a target computer which is already accessed by another user
View:	Screen contents of a target computer that is already accessed by another user can be viewed; inputs are *not* possible
Full:	Allows full access to a target computer that is already accessed by another user

6. Repeat steps 4 and 5 to change the access rights for further target modules.
7. Click **OK** to save your settings.

Access mode if a target computer is accessed by several users

Only one user can access each target computer in the default settings of a *CATCenter NEO* system.

This restriction can be lifted by changing the access rights for a user account or a user group.

You can either change the global settings to allow several users to access a target computer at the same time (for all target computers a user or a user group has access to) *or* you can change the rights for particular target computers or target groups only.

> **NOTE:** The right for simultaneous access depends on the user's effective right (see page 59). The effective right is the highest right which results from the individual right of the user accounts and the rights of the assigned group(s).

How to change the rights to access *all* target computers at the same time:

1. Click **User area > Users** in the tree view to change this right.

   If you want to change the rights for a user group, click **User area > User groups**.

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 **Matrix systems** and **Global Device Rights** tabs.
4. Use the **Multi Access** field in the **Access Rights** column to choose between the following options:

No:	Denies access to a target computer which is already accessed by another user
View:	Screen contents of a target computer that is already accessed by another user can be viewed; inputs are *not* possible
Full:	Allows full access to a target computer that is already accessed by another user

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

How to change the rights to access a *certain* target module or group at the same time:

NOTE: Several users are only allowed to access the target at the same time if the user account or the user group hold the *general access rights* (see page 77 f.) for the target computer!

1. In order to change this right for a user account, click **User area > User** in the tree.

   In case you want to change the right for a user group, click **User area > User groups**.

2. Right-click the user account or user group to be configured and click **Configuration** in the context menu.

3. Click the **Matrix systems** tab.

4. If you want to change the access rigths for a certain target module, click on **Individual Group Rights**.
   If the rights should apply for a target group, click on **Device Group Rights.**

5. Choose your desired target module or target group from the list on the left side.

   ADVICE: Use the drop-down menu to choose the target modules to be displayed in the selection screen:
   - **[All targets]:** Lists all target modules within the system
   - **[Unassigned]:** Only lists *[Unassigned]* target modules
   - **Search...** After you have chosen this option, a new window opens. Choose the desired *View filter* in the tree to display only the devices which are assigned to this view filter.

6. Use the **Multi access rights** field on the right side of the window to choose between the following options:

No:	Denies access to a target computer (of a group) which is already accessed by another user
View:	Screen contents of a target computer (of a group) that is already accessed by another user can be viewed; inputs are *not* possible
Full:	Allows full access to a target computer (of a group) that is already accessed by another user

7. Click **Ok** to save you settings.

Changing the rights to configure the target modules

How to change the rights to view and edit the configuration of the target modules:

1. Click the tree view entries **User area > Users** to change this right.

   If you want to change the rights for a user group, click **User area > User groups**.

2. Double-click the user account or the user group to be configured.
3. Click the **Matrix systems > Global Device Rights** tabs.
4. Use the **Target config** field to choose between the following options:

Yes:	Allows the user to view and edit the target module config
No:	Denies the user to view and edit the target module config

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

Changing the rights to reset or reactivate a PS/2 mouse

Unlike USB mouse devices, PS/2 mouse devices do not support the hot plug technology. It is therefore possible to insert the PS/2 plug during operation but the target module or the connected computer might not detect the input device.

In order to activate or reset the PS/2 mouse, a special command can be sent from the KVM matrix system to the computer connected to the target module.

How to change the rights to reset or reactivate the PS/2 mouse:

1. Click the **User area > Users** tree view entries to change this right.

   In case of a user group, click the entries **User area > User groups**.

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 **Matrix systems > Global Device Rights** tabs.
4. Use the **Mouse reset** field to choose between the following options:

Yes:	Allows the user to reset or reactivate the PS/2 mouse interface of a target computer
No:	Denies the user to reset or reactivate the PS/2 mouse interface of a target computer

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

Basic configuration of the target modules

Renaming a target module

While the KVM matrix system is initiated, the target modules are automatically named.

How to rename a target module:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module and click the **Configuration** entry in the context menu.
3. Enter the name of the target module into the **Name** field.
4. Press **OK** to save your settings.

Changing the comment of a target module

In addition to the target module name, the list field of the web application also displays a comment regarding this target module.

ADVICE: Use the comment to write the location of the target module down, for example.

How to change the comment of a target module:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module and click the **Configuration** entry in the context menu.
3. Enter any comment into the **Comment** field.
4. Press **OK** to save your settings.

Deleting a target module from the KVM matrix system

If the KVM matrix system is not able to detect an already known target module, the system defines the device as being switched off. Therefore, you have to manually delete the list entry of the target module you want to permanently remove from the system.

NOTE: Only switched-off target modules can be deleted.

How to delete a target module that is switched off or disconnected from the system:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module 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.**

Copying the target module config settings

If a target module of the KVM matrix system is replaced by another device, the previous config settings can be copied to the new device. After the config settings have been copied to the new device, it can be operated immediately.

IMPORTANT: After this task has been carried out the target module whose settings you want to copy is deleted from the KVM matrix system.

How to copy the target module config settings:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the new target module and click the **Get config from ...** entry in the context menu.

   A new window shows a list of all target modules that are switched-off or deleted from the KVM matrix system.
3. Choose the target module whose configuration settings you want to copy.
4. Click **OK** to copy the configuration settings.

Settings for special hardware

Keymode for Apple computers

NOTE: This setting can only be edited with USB versions of the target modules.

If the Apple computer that is connected to the target module does not (properly) react to keypresses of multimedia keys, the special keymode for Apple computers can be enabled.

How to (de)activate the special keymode for Apple computers:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module you want to configure and click the **Configuration** entry in the context menu.
3. Use the **Apple Mode** field to choose between the following options:

Yes:	Enables keymode for Apple computers
No:	Enabels standard mode

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

Keymode for USB multimedia keyboards

NOTE: This setting can only be edited with USB versions of the target modules.

Various manufacturers have added special keys to some USB keyboards. Use the configuration settings of the target modules to activate or deactivate the support of such keys.

How to (de)activate the support for the multimedia keys of a USB keyboard:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module you want to configure and click the **Configuration** entry in the context menu.
3. Use the **Multimedia special keys of the USB keyboard** field to choose between the following options:

Yes:	Support for multimedia keys of a USB keyboard is enabled
No:	Support for multimedia keys of a USB keyboard is disabled

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

Support for servers of IBM's RS/6000 series

NOTE: This setting can only be edited with PS/2 versions of the target modules.

Enable the support for UNIX servers of IBM's RS/6000 series if the target computer is such a server.

How to (de)activate the special support for servers of IBM's RS/6000 series:

1. Click the **KVM matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module you want to configure and click the **Configuration** entry in the context menu.
3. Use the **IBM RS/6000 support** field to choose between the following options:

yes:	Support for servers of IBM's RS/6000 series is activated
no:	Support for servers of IBM's RS/6000 series is deactivated

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

Enhanced functions

»Multiuser« display

If several users are accessing a target computer (Multiuser mode), the *»Multiuser«* information can be activated. This way, all accessing users are provided with the information that at least one other user is currently accessing the target computer.

NOTE: The setting to display this information is usually configured for the entire system and individually for each user account.

Both options are described on this page.

How to (de)activate the »Multiuser« information *for the entire system*:

1. Click the **KVM matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the master matrix switch and click the **Configuration** entry in the context menu.
3. Use the **Multiuser display** field in the **Configuration** column to choose between the following options:

yes:	Enables the »Multiuser« display
no:	Disables the »Multiuser« display

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

How to (de)activate the »Multiuser« information for a particular *user account*:

1. Click the **User area > User** tree view entries.
2. Right-click the user account you want to configure and click the **Configuration** entry in the context menu.
3. Click the **Matrix system > Personal Profile > Matrix switch** tabs and use the **Multiuser display** field to choose between the following options:

system:	Global system settings apply (see above)
on:	Displays »Multiuser« information
off:	Does *not* display »Multiuser« information

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

Adjusting the power management of the target module

IMPORTANT: This setting can only be edited for USB versions of the target modules.

The target modules of the *CATpro2-USB series* are usually switched on as soon as the USB controller provides the target module with the required voltage.

Disable the USB Power Management setting if no screen content is being displayed on the monitor of the accessing user module while the target computer is booting.

How to change the power management setting of the target module:

1. Click the **KVM Matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module you want to configure and click the **Configuration** entry in the context menu.
3. Use the **USB power management** field to choose between the following options:

Enabled:	The target module of the *CATpro2-USB series* is switched on as soon as the USB controller provides the target module with the required voltage.
Disabled:	The target module of the *CATpro2-USB series* is directly switched on.

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

Viewing the status information of a target module

The context menu of a target module enables you to call an interface with various status information of the target module. In addition to the name and the storage location, information regarding the firmware version is displayed.

How to view the status information of a target module:

1. Click the **KVM Matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the target module whose status information you want to view and click the **Information** entry in the context menu.
3. This interface provides the following information:

Name:	target module name
Device ID:	physical ID of the target module
Status:	current status (*on* or *off*) of the target modules
Folder:	folder to which the target module is assigned to
Comment:	user comment regarding the target module
Firmware name:	firmware name
Firmware revision:	firmware version

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

Viewing the cascade information

The cascade information provides you with an overview of the physical connections of the KVM matrix system. In addition to the master device, the connected slave devices as well as the user modules and target modules are displayed.

The cascade information also displays the physical device ID, the connection port at the KVM matrix system and the status.

How to view the cascade information:

1. Click the **KVM Matrix systems > Name > Targets** entries in the tree view.
2. Right-click the target module and click the **Cascade info** entry in the context menu to view the cascade tree directory:

> **NOTE:** The matrix switch via whose context menu the cascade information has been called is highlighted in red.

3. The cascade information provides the following information:

- Name, port and status of the connected user modules
- Name, port and status of the connected target modules
- Name and ports of slave devices

4. Click **Close** to close the cascade view.

User consoles

The target computers connected to the system are operated at the user consoles of the KVM matrix system.

Operating modes of user consoles

Depending on the intended use of the user console, the console's operating mode can be selected from the following options:

Standard operating mode

NOTE: This operating mode is preset in the default.

The standard operating mode only permits the access to the KVM matrix system after you have entered your username and your password.

The user rights can be individually adjusted in the settings of the user accounts.

Open Access operating mode

The access to the KVM matrix system is not password-protected.

For this user console, you can configure the same access rights as for a user account.

IMPORTANT: The configured access rights do apply for *all* users at this user console.

Video operating mode

A video console (only possible when combined with the optional *Push-Get function*) is especially suited when used with a projector since mouse and keyboard do not have to be connected.

If the video console is provided with mouse and keyboard, you can only make entries at the on-screen display.

For this user console, you can configure the same access rights as for a user account.

IMPORTANT: The configured access rights apply for *all* users at this user console.

NOTE: A video console is not displayed.

As a result, an accessing video console is not highlighted to other accessing users. A user without Multiuser rights can therefore access the user console simultaneously to the video console.

Selecting the user console's operating mode

How to select the user console's operating mode:

1. Click on **KVM Matrix systems > Name > Consoles** in the tree view.
2. Right-click the user console you want to configure and click the **Configuration** entry in the context menu.
3. Click on the **General** tab.
4. Use the **Operating mode** entry to select between the following options:

Standard:	standard operating mode
Open Access:	open access operating mode
Video:	video operating mode

> **NOTE:** Selecting the *Open Access* or *Video* options activates further submenus to configure the access rights.
>
> These settings are explained in the chapter *Changing the user account rights* on page 63 ff.

5. Press **F2** to save your settings.

Basic configuration of user consoles

Changing the name or the comment of a user console

How to change the name or comment of a user console:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the console you want to configure and click the **Configuration** entry in the context menu.
3. Click on the **General** tab.
4. Use the **Name** entry to rename the user console.
5. Use the **Comment** entry to change or collect a comment regarding the user console.
6. Click **OK** to save your settings.

(De)activating the user console

If you want to deny a user console access to the KVM matrix system, the user console can be deactivated.

NOTE: If the user console is deactivated, the monitor displays the message »*This console has been disabled*«. It is therefore not possible to call the on-screen display or the login box.

If a user is accessing this user console, the access is *immediately* withdrawn.

How to (de)activate the user console:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure and click the **Configuration** entry in the context menu.
3. Click on the **General** tab
4. Use the **Enabled** entry to select between the following options:

Enabled:	user console activated
Disabled:	user console deactivated

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

Copying the console config settings

If a user console of the KVM matrix system is replaced by another device, the previous config settings can be copied to the new device.

Afterwards the new device can be immediately operated.

IMPORTANT: After the settings of a user console have been copied, the use console is deleted from the KVM matrix system.

How to copy the user console config settings:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the new console and click on **Get config from ...** in the context menu.

   A new window provides a list with all inactive or deleted user consoles.
3. Select the user console whose configuration settings you want to copy.
4. Click **OK** to copy the configuration settings.

Deleting a user console from the KVM matrix system

If the KVM matrix system is not able to detect a user console that already has been connected to the system, the console is considered inactive.

Delete the list entry of the console that is to be permanently removed from the system.

> **NOTE:** Only inactive user consolescan be deleted by the administrator and all users with the *Superuser* right.

How to delete a user console that is switched off or disconnected from the system:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to delete and click **Delete** in the context menu.
3. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Settings for special hardware

Adjusting the scancode set of a PS/2 keyboard

If a key is pressed on the PS/2 keyboard, the keyboard processor sends a data packet that is called scan code. The two common scan code sets (sets 2 and 3) contain different scan codes.

The KVM switch interprets all inputs of the PS/2 keyboard with scan code set 2.

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

How to select the scancode set of the PS/2 keyboard:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now click on **Configuration** in the context menu.
3. Click on the **General** tab
4. Use the **Scancode Set** entry to select between the following options:

Set 2:	activates scancode set 2
Set 3:	activates scancode set 3

5. Click **OK** to save your settings.
6. Restart the user console to apply your changes.

Activating the support for special PS/2 keyboards

How to activate the support for a special PS/2 keyboard:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now click on **Configuration** in the context menu.
3. Click the **General** tab
4. Use the **Enh. Keyboard** entry to select between the following options:

default:	standard keyboard
PixelPower Clarity (blue):	special »*PixelPower Clarity (blue)*« keyboard
PixelPower Rapid Action:	special »*PixelPower Rapid Action*« keyboard
SKIDATA1:	special »*SKIDATA1*« keyboard

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

Advanced functions

Setting the automatic user logout

A user console can be configured so that the access to the target module is automatically disconnected after a user has been inactive for a certain amount of time. This way, the inactive user is automatically logged out of the KVM matrix system.

How to set the automatic user logout:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now, click on **Configuration** in the context menu.
3. Click on the **General** tab.
4. Use the **Auto logout (minutes)** entry to set the time (**1** to **99** minutes) for the automatic logout.

> **NOTE:** The value »0« deactivates the automatic user logout.

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

Automatically disconnecting the access to a target module

The user console can be configured in a way that the active access to a target module is automatically disconnected after the user has been inactive for a certain amount of time.

If the OSD is opened at the moment of disconnection, it remains on the screen even after it has been automatically disconnected.

If the OSD is closed at the moment of disconnection, the message, which is displayed on the right-hand side, is shown on the screen of the user console.

```
CON-Admin
Not connected
```

How to automatically disconnect the access to a target module:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now click on **Configuration** in the context menu.
3. Click on the **General** tab.
4. Use the **Auto disconnect (min)** entry to set the time (1 to 99 minutes) for automatically disconnecting the access to a target module.

   NOTE: The value »0« deactivates the automatic disconnection when a target module is accessed.

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

Viewing the status information of a user module

The context menu of a user module enables you to call an interface with various status information of the user module. This interface displays the name and also information regarding the firmware version.

How to view the status information of a user module:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console and click on **Information** in the context menu.
3. The interface, which now opens, provides the following information:

Name:	user module name
Device ID:	physical ID of the user module
Status:	current status (**on** or **off**) of the user module
Comment:	user comment regarding the target module
Firmware name:	firmware name
Firmware revision:	firmware version

4. Click **Close** to close this interface.

Remembering the username in the login box

If the same user often works at a certain user console, his login can be used as default in the login box of the KVM matrix system.

After a user has logged out of the system, the login mask automatically remembers the username of the last active user.

How to remember the username in the login mask:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now, click **Configuration** in the context menu.
3. Click on the **General** tab.
4. Use the **Remember last user** entry to select between the following options:

yes:	the system remembers the last user
no:	the system does not remember the last user

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

Setting the hold time for the screensaver

The screensaver deactivates the screen display at the user console after the user has been inactive for an amount of time you can adjust.

NOTE: This setting operates independently from the screensaver settings of the target computer.

How to set the hold time of the screensaver:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click the user console you want to configure. Now click on **Configuration** in the context menu.
3. Click on the **General** tab.
4. Use the **Screensaver (min)** entry to set the holding time (**1** to **99** minutes) for activating the screensaver.

   NOTE: The value »0« deactivates the screensaver of the user console.

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

Viewing the cascade information

The cascade information provides you with an overview of the physical connections of the KVM matrix system. In addition to the master device, the connected slave devices, user consoles, and target modules.

The cascade information also displays the physical device ID, the connection port at the KVM matrix system, and the status.

How to view the cascade information:

1. Click on **KVM Matrix systems > [Name] > Consoles** in the tree view.
2. Right-click on the desired user console. Now click on the **Cascade information** entry in the context menu to view the cascade tree directory:

   NOTE: The user console, via whose context menu the cascade information has been called, is highlighted in red.

3. The cascade information provides the following information:

   - Name, port and status of the connected user consoles
   - Name, port and status of the connected target modules
   - Name and ports of slave devices

4. Click **Close** to close the cascade view.

Target groups and view filters

Difference between target groups and view filters

The target modules of the KVM matrix system can be arranged in target groups and view filters.

Intended use of target groups

The creation of target groups enables the administrator to quickly assign the rights of a user or a user group for all target modules within a group.

NOTE: The different target modules can be members of *several* target groups.

Intended use of view filters

View filters enable the users of a KVM matrix system to organise the different target modules into views. Especially in large KVM matrix systems, the creation of view filters provides better orientation.

You can group the target modules according to their location (e.g. the server room) or to other features (e.g. to the operating system of the connected computer).

Administrating target groups

The »New Targets« target group

By default, the *New dig.Targets* target group is created in the KVM matrix system. This group automatically contains all target modules as soon as they are first connected to the KVM matrix system. For this, the computer connected to the module has to be switched on.

If you want to provide a user or a user group with particular rights to all recently connected target modules, change the device group rights (see page 77) of either the user account or the user group.

Creating a new target group

How to create a new target group:

1. Click on **KVM Matrix systems > Target groups** in the tree view.
2. Right-click the display range. Now click on **New > Target group** in the context menu.
3. Use the **Name** entry to name the target group.
4. *Optional:* Use the **Comment** entry to change or enter any comment regarding the matrix switch.
5. Click **OK** to save your settings.

NOTE: The rights for this target group can be assigned when the device group rights (see page 66) of either the user account or the user group are changed.

Changing the name or comment of a target group

How to change the name or comment of a target group:

1. Click on **KVM Matrix systems > Target groups** in the tree view.
2. Right-click the target group to be edited. Now click on the **Configuration** entry in the context menu.
3. Use the **Name** entry to name the target group.
4. *Optional:* Use the **Comment** entry to change or enter a comment regarding the matrix switch.
5. Click **OK** to save your settings.

Administrating target group members

NOTE: Up to 20 target modules can be assigned to each target group of the KVM matrix system.

How to administrate the members of a target group:

1. Click on **KVM Matrix systems > Target groups** in the tree view.
2. Right-click the target group to be configured. Now click on the **Configuration** entry in the context menu.
3. Click the **Members** tab to add members to or delete them from the target group.

The dialog consists of two tables that list the target modules of the KVM matrix system:

Unassigned:	lists the target modules that are *not* assigned to this group
Assigned group members:	lists the target modules that are assigned to this group

4. Use the drop-down menu to select the type of target modules to be displayed. You can select between the following options:

[All targets]	lists all target modules of the system.
[Unassigned]	only lists the target modules of the *[Unassigned]* view.
Search...	After this option has been selected, another window opens. Select the desired *View filter* in the tree view to display only the therein contained devices.

5. Mark the target module you want to add to or delete from the group.
6. Now, click the button (*right arrow*) to add the target module to the group or the button (*left arrow*) to delete it.
7. Click **OK** to save your changes.

Deleting a target group

How to delete a target group:

1. Click on **KVM Matrix systems > Target groups** in the tree view.
2. Right-click the target group to be deleted. Now, click on the **Delete** entry in the context menu.
3. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Administrating view filters

Creating a new view filter

How to create a new view filter:

1. Click on **KVM Matrix systems > View filter** in the tree view. Now click on **New folder** entry in the context menu.
2. Use the **Name** entry to enter a name.
3. *Optional:* Use the **Comment** entry to enter a comment.
4. Click **OK** to save your inputs.

NOTE: The folders can be interlaced in any way.

Assigning a target module to a view filter

Directly after a new target module is connected to the KVM matrix system, it is assigned to the *[Unassigned]* group. By assigning the target module to another group, the existing assignment is cancelled.

How to assign a view filter to a target module:

1. Click the **KVM Matrix systems > View filter** entries in the tree view.
2. Click the folder of the view filter to which the target module is assigned to.

   NOTE: The *[All targets]* folder lists all target modules within the system.
3. Right-click the target module to be assigned and click on **Copy device**.
4. Open the folder to which the target module is to be assigned to.
5. Right-click the main view and click **Paste device** in the context menu.

Cancelling a target module's assignment to a view filter

The assignment can be cancelled by moving the target module to the *[Unassigned]* folder or by selecting the **Remove from folder** entry in the context menu.

How to cancel a target module's assignment to a view filter:

1. Click the **KVM Matrix systems > View filter** entries in the tree view.
2. Click the folder of the view filter to which the target module is currently assigned to.

   NOTE: The *[All targets]* folder lists all target modules within the system.
3. Right-click the target module whose assignment you want to delete. Now click on **Remove from folder** in the context menu.

   The target computer is now moved to the *[Unassigned]* group.

Renaming a view filter

How to rename a view filter:

1. Click the **KVM Matrix systems > View filter** entries in the tree view.
2. Right-click the view filter you want to rename and click **Rename folder** in the context menu.
3. Edit the name and press **Enter**.

Deleting a view filter

The created view filter can be deleted at any time. The target modules assigned to this view filter are automatically moved to the *[Unassigned]* folder.

> **NOTE:** The *[Unassigned]* and *[All targets]* view filters are administrated by the web application and therefore cannot be deleted.

How to delete a view filter:

1. Click the **KVM Matrix systems > View filter** entries in the tree view.
2. Right-click the view filter you want to delete. Now click **Delete folder** in the context menu.
3. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Accessing the target modules via select keys

After the select key modifier(s) and a select key set have been adjusted and a select key set has been activated in the user account, the target module can be accessed with key combinations.

Changing the select key modifier or the valid keys

The select keys enable you to quickly access a particular target computer with a key combination. For this, *select key sets* can be created in the KVM matrix system.

In combination with the select key modifier, a select key set defines the key combination to be pressed to access a particular target computer.

In addition to the select key modifier, you are also enabled to define the valid keys for the select keys.

How to change the select key modifier or the valid keys:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the master matrix switch and click the **Configuration** entry in the context menu.
3. Select at least one of the listed modifiers in the **Select key modifier** entry by marking the respective entry:

▪ **Ctrl**	▪ **Win**
▪ **Alt**	▪ **Shift**
▪ **Alt Gr**	

4. Use the **Valid keys** entry to select one of the following options:

Only numbers:	*only numerical keys* are interpreted as select keys when pressed in combination with the select key modifier
Only characters:	*only alphabetic keys* are interpreted as select keys when pressed in combination with the select key modifier
Numbers and characters:	*alphabetical and numerical keys* are interpreted as select keys when pressed in combination with the select key modifier

IMPORTANT: The selected valid keys and the select key modifier are *no longer* provided as key combinations to the operating system and the applications on the target computer.

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

Administrating select key sets

The KVM matrix system allows you to create 20 global select key sets or ten individual select key sets for each user.

A select key set can be used to define the select key sets for the target modules you would like to access.

NOTE: Global select key sets are displayed in the personal profile of all users of the KVM matrix system.

Creating a select key set

How to create a select key set:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Click on the **[+]** button in the *Select key set* entry and enter the following data:

Name:	Enter the name of the select key set.
Comment:	Enter a comment regarding the select key set.
Global:	Mark this entry if you want the select key set in the personal profile to be available for all users of the KVM matrix system.

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

Changing name, comment or global allocation of a select key set

How to change the name, comment and/or *Global* setting of a select key set:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Select key set** entry to select the select key set to be activated and click **Change.**

5. Change the desired data of the select key set:

Name:	Enter the name of the select key set.
Comment:	Enter any comment regarding the select key set.
Global:	Mark this entry if you want the select key set in the personal profile to be available for all users of the KVM matrix system.

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

Defining select keys for the target modules

NOTE: Global select key sets can only be edited by users with activated *Superuser* right (see page 68).

Without this right, only the select keys, which are assigned to the target modules, can be viewed.

How to define the select keys for target modules:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Select key set** entry to choose the select key set to be edited and click **Edit.**
5. Click the **Assigned targets** tab.
6. Use the drop down menu to select the type of target modules to be displayed in the select window. The following options are available:

[All targets]	displays all target modules within the KVM matrix system
[Not assigned]	only displays the target modules that are *[Not assigned]* to the view filter
Search...	This option opens another window. Select the desired view filter in the tree view to display only the herein contained devices in the select window.

7. Use the **Keys** column to select the device whose select key you want to change and then enter the desired character(s).
8. Click **OK** to save your changes.

Assigning a select key set to a user account

By assigning a select key set to a user account, the select keys defined in a set are interpreted and the particular target module is accessed.

How to assign a select key set to a user account or cancel the existing assignment:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Select key set** entry to choose the select key set to be activated.
5. Click **OK** to save your settings.

Deleting a select key set

NOTE: Only users with the *Superuser* right (see page 68) are allowed to delete a global select key set.

How to delete a select key set:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Select key set** entry to choose the select key set to be deleted and click **Delete**.
5. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Automatically or manually switching the target modules

Auto scanning all target modules (Autoscan)

The *Autoscan* function successively accesses all target modules that are mentioned in the active scancode set and available to the user.

The *Scantime* setting (see page 105) enables you to define how long a target module is to be accessed.

When accessing the target modules, the workplace name, the name of the currently accessed target module, and a note regarding the *Autoscan* function are displayed.

NOTE: If the *Autoscan* function is active, the keyboard and mouse inputs are transmitted to the currently accessed target module.

During your inputs, the *Autoscan* function stops and continues after you finished your inputs.

Applying the *Autoscan* function

Requirements for using this function:

- *Creating a scanmode set* (see page 108)
- *Assigning a scanmode set to a user account* (see page 110)

Configuring the scantime of the *Autoscan* function

By default, a target module is accessed for five seconds. After that, the target module is disconnected and the next target module is accessed.

Select a time span between 1 and 99 seconds to define how long the target module is to be accessed.

How to change the scantime:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Scantime** entry to enter a time span between **1** and **99** seconds.
5. Click **OK** to save your settings.

Auto scanning all active target modules (Autoskip)

The *Autoskip* function successively accesses any target module that is included into the active scancode set and available to the user.

The connected computer must be active to carry out this function.

The *Scantime* setting (see page 105) enables you to define how long each target module is to be accessed.

When accessing the target modules, the workplace name, the name of the currently accessed target module, and a note regarding the *Autoscan* function are displayed.

NOTE: If the *Autoskip* function is activated, all keyboard and mouse inputs are transmitted to the currently accessed target module.

The *Autoskip* function stops during the user's imputs and continues after all inputs are finished.

Applying the *Autoskip* function

Requirements for using this function:

- *Creating a scanmode set* (see page 108)
- *Assigning a scanmode set to a user account* (see page 110)

Configuring the scantime of the *Autoskip* function

By default, each target module is accessed for five seconds. After that, the target module gets disconnected and the next target module is accessed.

Select a time span between 1 and 99 seconds in order to define how long the target module is to be accessed.

How to change the scantime:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Scantime** entry to enter a duration between **1** and **99** seconds.
5. Click **OK** to save your settings.

Scanning the target modules manually (Stepscan)

By pressing a key, the *Stepscan* function successively accesses all target modules that are indicated in the scanmode set and approved for the user.

When accessing the target modules, the workplace name, the name of the currently accessed target module, and a note regarding the *Stepscan* function are displayed.

Starting and stopping the *Stepscan* function

Requirements for using this function:

- *Creating a scanmode set* (see page 108)
- *Assigning a scanmode set to a user account* (see page 110)
- *Configuring keys to scan the targets manually* (see page 107)

Configuring keys to scan the targets manually

By pressing a key, the *Stepscan* function successively switches to all target modules that are available to the user.

You can select different keys to access the next (default **Up**) or the previous (default **Down**) target module.

How to select the keys for using the *Stepscan* function:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Stepkeys** entry to select between the following options:

Up/Down:	arrow keys *Up* and *Down*
PgUp/PgDn:	*page*↑ and *page*↓ keys
Num Up/Down:	arrow keys *Up* and *Down* of the numeric keypad
Num PgUp/PgDn:	*page*↑ and *page*↓ keys of the numeric keypad
Num +/-	*plus* and *minus* keys of the numeric keypad

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

Administrating scanmode sets

The matrix system enables you to create 20 global select key sets or ten individual scanmode sets for each user.

The select key sets allow you to define the computers to be accessed when performing the *Autoscan*, *Autoskip* or *Stepscan* function.

NOTE: The global scanmode sets are displayed in the *Personal Profile* menu of all users of the matrix system.

Creating a scanmode set

How to create a scanmode set:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **[+]** button in the **Scanmode set** row to collect the following data:

Name:	Enter the name of the scanmode set.
Comment:	Enter a comment regarding the sscanmode set.
Global:	Mark this entry if you want the scanmode set in the *Personal Profile* to be available for all users of the KVM matrix system.

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

Changing a scanmode set's name, comment or global assignment

How to change a scamode set's name, comment and/or *Global* setting:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Select the scanmode set to be edited in the *Scanmode set* row and click **Change.**
5. If required, change the following data:

Name:	Enter the name of the scanmode set.
Comment:	Enter any comment regarding the scanmode set.
Global:	Mark this entry if you want the scanmode set in the *Personal Profile* to be available for all users of the KVM matrix system.

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

Assigning the target modules to a scanmode set

NOTE: Global scanmode sets can only be edited by users with activated *Superuser* right (see page 68).

Without this right, only the assigned target modules can be viewed.

How to define the select keys for target modules:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Select the scanmode set to be edited in the *Scanmode set* row and click **Edit.**
5. Click the **Member** tab.

6. Use the drop down menu to select the type of target modules to be displayed in the select window. The following options are available:

[All targets]	Displays all target modules within the system.
[Not assigned]	Only displays the target module that are *[Not assigned]* to the view filter.
Search...	This option opens another window. Select the desired *View filter* in the tree view to only display the herein contained devices in the select window.

7. The interface consists of two tables that list the user accounts of the KVM matrix system:

Not assigned	Lists the target modules that are *not* assigned to the scan-mode set
Assigned targets	Lists the target modules that are assigned to the scanmode set

8. Mark the target module you want to add to or delete from the scanmode set.
9. Click the button (*right arrow*) to add the target module to the scanmode set or the button (*left arrow*) to delete it from the scanmode set.
10. Click **OK** to save your changes.

Assigning a scanmode set to a user account

By assigning a scanmode set to a user account, the target modules selected in the set are accessed when performing the *Autoscan*, *Autoskip* or *Stepscan* function.

How to assign a scanmode set to the user account or cancel the existing assignment:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Select the scanmode set to be activated in the **Scanmode set** entry.
5. Click **OK** to save your settings.

Deleting a scanmode set

NOTE: Only users with activated *Superuser* right (see page 68) can delete a global scanmode set.

How to delete a scanmode set:

1. Click on the **User area > User** entries in the tree view.
2. Right-click on the user account to be configured and click **Configuration** in the context menu.
3. Click the **Matrix systems > Personal Profile > Matrix switch** tabs.
4. Use the **Scanmode Set** entry in the *Matrix switch user configuration* to select the scanmode set to be deleted and click the **Delete.**
5. Confirm the confirmation prompt by clicking **Yes** or cancel this process by clicking **No**.

Configuring the On-Screen Display (OSD)

The on-screen display of the KVM matrix system enables the user to operate and configure the system. By default, the on-screen display is provided at all user consoles.

Configuration

Many of the on-screen display's basic functions can be adjusted to your demands.

You can define the hotkey as well as the position and font size of the on-screen display.

Any settings that can be adjusted to your needs are described on the following pages.

Changing the hotkey to call the OSD

The hotkey to call the on-screen display (OSD) is used at all consoles within the KVM matrix system. This hotkey enables you to open the OSD in order to operate and configure the system.

NOTE: In the default, the hotkey **Ctrl** is preset.

The hotkey consists of at least one hotkey modifier key and an additional hotkey, which you can freely select.

Both the **Ctrl** hotkey modifier key and the **Num** hotkey can be configured by the user.

How to change the hotkey to call the on-screen display:

1. Click on **KVM Matrix systems > [Name] > Matrix switches** in the tree view.
2. Right-click the display range of the master matrix switch and click the **Configuration** entry in the context menu.
3. Select at least one of the listed modifiers in the **Hotkey modifier** entry by marking the entry:

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

4. Use the **Hotkey scancode** entry to select one of the following options:

Num	*Num* key
Pause	*Pause* key
Insert	*Insert* key
Delete	*Delete* key
Home	*Home* key
End	*End* key
PgUp	*Page Up* key
PgDn	*Page Down* key
Space	*Space* key

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

Opening the on-screen display via double keypress

In addition to opening the on-screen display (OSD) via hotkey (see above), you can open the OSD by pressing a previously selected key twice (**Ctrl**, **Alt**, **Alt Gr**, **Win**, **Shift** or **Print**).

How to enable/disable opening the on-screen display via double keypress:

1. In the directory tree, click on **KVM matrix systems > [Name] > Matrix switches**.
2. Right-click the master matrix switch and click **Configuration** on the context menu.
3. Under **OSD via double keypress,** select one of the following options:

Off	The OSD can be opened only by pressing the hotkey.
Ctrl, **Alt**, **Alt Gr**, **Win**, **Shift** or **Print**	The OSD can also be opened by pressing the selected key twice.

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

Adjusting the information display

When switching to a target module, a temporary information display (5 seconds) opens. The display informs you about the console name, the name of the currently accessed target module and provides further information.

The information display can also be permanently displayed or deactivated. The selected setting is assigned to your user account and stored in your *Personal Profile*.

ADVICE: When active, the temporary information can be recalled by pressing **Ctrl**+**Caps Lock**.

How to change the settings of the information display:

1. In the directory tree, click on **User area > User**.
2. Right-click the user account you want to edit. Now click on **Configuration** on the context menu.
3. Click on **Matrix systems > Personal Profile > Matrix switch**.
4. Under **Display mode**, select between the following options:

Temp:	Show temporary information display (5 seconds)
Perm:	Permanent information display
Off:	Disable information display

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

Changing the colour of the information display

By default, information displays (like when accessing a target module) are shownin light green. In their peronal profiles, users can change the colour of the information display.

How to change the colour of the information display:

1. In the directory tree, click on **User area > User**.
2. Right-click the user account to be edited. Now click on **Configuration** on the context menu.
3. Click on **Matrix systems > Personal profile > Matrix switch**.
4. Under **Display color,** you can choose between the following options:

Light green:	Show information display in light greendefault)
Black, dark red, dark yellow, dark blue, purple dark turquoise, silver, yellow, blue, fuchsia, light turquoise or **white**	Show information display in the selected colour

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

Defining a standard view filter

After the user login, the *Select* menu is displayed. The default setting of the *Select* menu displays all target modules. By applying the view filter, the display of the target modules can be filtered.

If you want to activate a certain view filter directly after accessing the *Select* menu, you can configure the user account accordingly.

> **NOTE:** The preset view filter is applied directly after your login at the matrix system.
>
> By applying the view filter, you can change the default and therefore activate another filter.

How to select a standard view filter for the Select menu:

1. In the directory tree, click on **User area > User**.
2. Right-click the user account you want to edit and click on **Configuration** in the context menu.
3. Click on **Matrix systems > Personal Profile > Matrix switch**.
4. Under **Def. view filter,** you can select between the following options:

ALL:	Displays all target modules
LAST:	The view filter that was used by the last user is applied when the *Select* menu is called in the OSD.
View filter name:	The selected view filter is applied if the *Select* menu is called in the OSD.

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

> **IMPORTANT:** When the *LAST* option has been selected and the user account is shared by two persons at the same time, the view filter of the last active person is stored.

Selecting the mode for OSD synchronisation

If both the synchronisation signal and the colour information are transmitted through one cable, the on-screen display is displayed in a slightly deviating, palish colour.

In this case you can select several synchronisation modes for the graphics signal of the target computer.

How to select a mode for the OSD synchronisation:

1. Click on **KVM Matrix systems > [Name] > Targets**.
2. Right-click the target module and click **Configuration** on the context menu.
3. Under **RGB synchronisation for OSD** in the *Target module configuration* paragraph, you can select one of the following options:

Standard:	RGB mode for OSD sync is active
Green:	RGsB mode for OSD sync is active
All:	RsGsBs mode for OSD sync is active

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

Selecting a keyboard layout for OSD entries

If the characters entered at the console keyboard deviate from the characters displayed on the on-screen display, the selected keyboard layout does not fit the keyboard.

In this case, please ascertain which keyboard layout does apply to the connected keyboard and select the layout in the console settings.

How to select the keyboard layout for the user console keyboard:

1. Click on **KVM Matrix systems > [Name] > Consoles**.
2. Right-click the console to be configured and click **Configuration** on the context menu.
3. Use the **Keyboard layout** entry under *User console config* to select one of the following options:

- **German**
- **English (US)**
- **English (UK)**
- **French**
- **Spanish**
- **Lat. American**
- **Portuguese**

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

Operating the on-screen display by mouse

In the default settings of the KVM matrix system, the on-screen display (OSD) can only be called with a configured key combination.

If a Microsoft »IntelliMouse Explorer« or another compatible mouse with five keys is connected to the user console, you can call the on-screen display through the mouse keys four and five at the side of the mouse

How to enable/disablethe mouse support to operate the on-screen display:

1. Click on **KVM Matrix systems > [Name] > Consoles**.
2. Right-click the console to be configured. Now, click the **Configuration** button on the context menu.
3. Use the **OSD by Mouse** entry under *User console config* to select one of the following options:

Yes:	Opens the OSD via mouse key 4 and 5 of a compatible mouse
No:	Disables the possibility to call the OSD by mouse

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

Enabling/disabling the on-screen display

This function defines if the users at the user module are enabled to activate the on-screen display or if they are only allowed use select keys for the switching.

How to enable/disable the on-screen display:

1. Click on **KVM Matrix systems > [Name] > Consoles**.
2. Right-click the console to be configured. Now, click the **Configuration** button on the context menu.
3. Use the **OSD blocked** entry under *User console config* to select one of the following options:

Yes:	On-screen display blocked
No:	On-screen display available

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

Video tuning

When a user console accesses a target module for the first time, a video profile is automatically created for this connection.

This video profile stores information about the different cable parameters. This information ensures that the video image is displayed perfectly at the user console.

The video profile can be recalculated at any time or manually adjusted by the user.

NOTE: Changing the cable length between a console and the matrix switch or between the target module and the matrix switch has an influence on the image quality.

When the cabling has been changed, it is recommended to carry out the automatic video tuning (see below).

Deleting the existing video profile has the effect that the video tuning is automatically performed when a user console accesses a target module for the first time (after the profile has been deleted).

Rights administration

Changing the right to configure video profiles

How to change the right to configure the video profiles:

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

   In case of a user group, click the entries **User area > User groups**.

2. Right-click the user account or the user group you want to configure. Now, click the **Configuration** entry in the context menu.

3. Click the **Matrix systems > Global device rights** tab.

4. Use the **Video Configuration** entry to select one of the following options:

yes:	allows configuration of video profiles.
no:	denies configuration of video profiles.

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

Power switch

Integrating a power switch (*G&D Hardboot CCX*) into the KVM matrix system allows you to use the system for (de)activating the power supply of the devices.

For this purpose, one or several power outlets are assigned to a target module. Afterwards these outlets can be switched in the *Operation* menu.

Rights administration

Rights to switch the power outlets of a target module

How to change the rights to switch the power outlet(s) assigned to a target:

1. Click on the **User area > Users** entries in the tree view to change this right.

   If you want to change this right for a user group, click on **User area > User groups**.

2. Right-click the user account or the user group you want to configure and click the **Configuration** entry in the context menu.

3. Now click the **Matrix systems > Individual device rights** tabs.

4. Select the desired target module in the list field on the left-hand side.

   Use the drop-down menu to select the target module to be displayed in the selection window.

   Select between the following options:

[All targets]	lists all target modules of the system.
[Unassigned]	only lists the target modules of the *[Unassigned]* view.
Search...	After this option has been selected, another window opens. Select the desired *View filter* in the tree view to display only the therein contained devices.

5. Use the **Target Power** entry to select between the following options:

yes:	Allow the switching of the power outlets that are assigned to the selected target module.
no:	Deny the switching of the power outlets that are assigned to the selected target module.

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

Rights to switch the power outlets of a target group

How to change the right to switch the power outlet(s) assigned to the target modules of the group:

1. Click on the **User area > Users** entries in the tree view to change this right.

   If you want to change this right for a user group, click on **User area > User groups**.

2. Right-click the user account or the user group you want to configure and click the **Configuration** entry in the context menu.

3. Now click the **Matrix system > Device group rights** tabs.

4. Select the desired target module in the list field on the left-hand side.

5. Use the **Target Power** entry to select between the following options:

yes:	Allow the switching of the power outlets that are assigned to the target modules of the selected group.
no:	Deny the switching of the power outlets that are assigned to the target modules of the selected group.

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

Configuration

Assigning a power switch power outlet to the target module

If at least one *G&D Hardboot CCX* power switch is provided to the system, one or more power outlets can be assigned to a target module.

Afterwards the assigned power outlets can be switched in the *Operation* menu of the consoles' on-screen display.

How to change the assigned power switch outlets:

1. Click the **KVM Matrix systems > [Name] > Targets** entries in the tree view.

2. Right-click the target module and click the **Assign power outlet…** entry in the context menu.

   A new window provides a list of all available and already assigned power switch power outlets. Here, you can assign power outlets to the target module or delete existing assignments.

   The interface consists of two tables, which list the power switch power outlets of the KVM matrix system:

Available power outlet(s):	lists the power outlets that are *not* assigned to this target module
Assigned power outlet(s):	lists the power outlets that are assigned to this target module

3. Mark the outlet you want to assign to the target module or whose assignment you want to delete.
4. Click the button (*right arrow*) to assign this outlet or the button (*left arrow*) to delete the assignment.

Changing the name or the comment of a power switch

How to change the name or the comment of a user module:

1. Click on **KVM Matrix systems > [Name] > Power switches** in the tree view.
2. Right-click the power switch you want to configure. Now click the **Configuration** entry in the context menu.
3. Click on the **General** tab.
4. Use the **Name** entry to rename the power switch.
5. Use the **Comment** entry to change or collect any comment regarding the power switch.
6. Click **OK** to save your settings.

Deleting a power switch from the KVM matrix system

If the KVM matrix system is not able to detect a power switch, which already had been connected to the system, the system defines the device as being switched off.

It is therefore necessary to manually delete the list entry of the power switch to be permanently removed from the system.

NOTE: Only inactive power switches can be deleted.

How to delete a power switch that is inactive or disconnected from the system:

1. Click on **KVM Matrix systems > [Name] > Power switches** in the tree view.
2. Right-click the power switch you want to delete and click **Delete** in the context menu.
3. Confirm the confirmation prompt by pressing **Yes** or cancel the process by pressing **No**.

Viewing the status information of a target module

Use the context menu of a target module to call an interface with various status information of the target module.

1. Click the **KVM Matrix systems > [Name] > Power switches** entries in the tree view.
2. Right-click on the power switch. Now click the **Information** entry in the context menu.
3. The opening interface provides the following information:

Name:	displays the power switch name
Status:	shows status of the power switch (*on* or *off*)
Comment:	user comment regarding the power switch
Name:	name of the matrix switch the power switch is connected to
Device ID:	device ID of the matrix switch to which the power switch is connected to
Class:	device class of the matrix switch to which the power switch is connected to

NOTE: The *Outlets* paragraph lists all channels of the power switches. The table also lists which target module is assigned to the power switch.

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

Special functions for cascaded KVM matrix systems

Cascading increases the number of target computers that can be connected to the KVM matrix system. For this, several matrix switches are integrated into the system.

The configuration settings for a KVM matrix switch are described in this chapter.

Basic functions

Changing the name or comment of a matrix switch

How to change the name or comment of a matrix switch:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the matrix switch you want to configure. Now click the **Configuration** entry in the context menu.
3. Rename the matrix switch using the **Name** entry.
4. *Optional:* Use the **Comment** entry to change or enter a comment regarding the matrix switch.
5. Click **OK** to save your settings.

Deleting a slave matrix switch from the system

If the KVM matrix system is not able to detect a matrix switch, which already had been connected to the system, the device is considered inactive.

Delete the list entry of a matrix switch that you want to permanently remove from the system.

> **NOTE:** Only inactive matrix switches can be deleted by the administrator and all users with the *Superuser* right.

How to delete inactive or disconnected matrix switches:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the matrix switch you want to delete and click **Delete** in the context menu.
3. Confirm the confirmation prompt by pressing **Yes** or cancel the process by pressing **No**.

Configuration settings

Defining the cascade mode of a matrix switch

In a cascaded KVM matrix system, the single matrix switches auto detect if they have been installed as master or as slave device within the cascaded system.

NOTE: Applying the *Auto* setting in the cascade mode may change the matrix switch's operating mode if the devices' cabling has been accidentally changed.

To avoid this, the operating mode of each matrix switch can be separately adjusted.

IMPORTANT: The settings regarding the cascade mode are to be carried out in the web application of the matrix switch whose setting you want to change.

How to change the cascade mode of a matrix switch:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the matrix switch you want to configure. Now click the **Configuration** entry in the context menu.
3. Click on the **General** tab.
4. Use the **Cascade mode** entry to select between the following options:

Auto:	The matrix switch decides whether it is operating in the master or slave mode.
Master:	In this operating mode, only user consoles can be connected to the *Console* ports. The names of the connected target modules can be edited. The edited names are automatically updated at the slave devices within the cascade.
Slave:	In this operating mode, the connected target modules cannot be renamed. The target modules are automatically named by the master device.

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

Forwarding target names to the slave matrix switches

Within a cascaded KVM matrix system, the target module names from the superior matrix switch are forwarded to the connected matrix switch(es). This way, the target modules named identically within the system.

If you want to define different target module names within the different matrix switches of the cascaded system, deactivate the *Forward target names* function.

IMPORTANT: Deactivating the function to forward target names in the *first level* of the matrix switch only affects the directly connected matrix switches of the *second level*.

If the *third level* also includes slave matrix switches, this function has to be deactivated in the matrix switches of the second level!

How to (de)activate the forwarding of target names to the slave matrix switches:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the user module you want to configure. Afterwards click the **Configuration** entry in the context menu.
3. Click on the **General** tab.
4. Use the **Forward target names** entry to select between the following options:

On:	The target module names are forwarded from the superior matrix switch to the connected matrix switch(es).
Off:	The target module names are not forwarded from the superior matrix switch to the connected matrix switch(es).

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

Viewing the status information of a matrix switch

The context menu of the matrix switch enables you to call an interface, which provides various status information of the device. Besides technical data, the name, the status and the MAC address are displayed.

How to view the status information of a matrix switch:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the desired matrix switch. Now click the **Information** entry in the context menu.

3. The display lists the following information:

Name:	matrix switch name
Device ID:	physical ID of the matrix switch
Status:	the current status (**On** or **Off**) of the matrix switch
Comment:	user comment regarding the matrix switch
CPU hardware revision:	hardware revision of the matrix switch
Console ports:	number of console ports at the matrix switch
FPGA revision:	revision of the FPGA module
Firmware name:	firmware name
Firmware revision:	firmware version
MAC address A:	MAC address of *network interface A*
MAC address B:	MAC address of *network interface B*
Serial number:	serial number of the matrix switch
Target ports:	number of target ports at the matrix switch

4. Click **OK** to leave the interface.

Viewing cascade information

The cascade information provides you with an overview of the physical connections of the KVM matrix system. In addition to the master device, the connected slave devices as well as the user modules and target modules are displayed.

The cascade information also displays the physical device ID, the connection port at the KVM matrix system and the status.

How to view the cascade information:

1. Click on **KVM Matrix systems > Name > Matrix switches** in the tree view.
2. Right-click the desired matrix switch. Now, click on **Cascade information** to view the cascade tree directory.

> **NOTE:** The user console, via whose context menu the cascade information has been called, is highlighted in red.

3. The cascade information (see figure above) provides the following information:

- Name, port and status of the connected user modules
- Name, port and status of the connected target modules
- Name and ports of slave devices

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

Copying the config settings of a matrix switch

If a matrix switch of the KVM matrix system is replaced by another device, the settings of the old device can be copied to the new one.

After the config settings have been copied, the new device is immediately ready for operation.

IMPORTANT: The matrix switch whose settings are copied is afterwards deleted from the KVM matrix system.

How to copy the configuration settings of a matrix switch:

1. Click on **KVM Matrix systems > [Name] > Matrix switches** in the tree view.
2. Right-click the new matrix switch. Now click on **Get config from ...** in the context menu.

   A new window now lists all inactive matrix switches.
3. Select the matrix switch whose configuration settings you want to copy.
4. Click **OK** to copy the config settings.

Replicating the database of a KVM matrix switch

Certain target modules(e.g. *CATpro2-DVI-Audio-UC-USB*) can be connected to two separate KVM matrix switches.

In such cases it is useful to replicate the database of a matrix switch (*Master*) to the other matrix switch (*Destination*). The following paragraphs list the configuration settings of the master matrix switch that can be replicated to one or several destinations.

Overview of the data to be replicated

The web application defines the scope of data to be replicated. In the following, the data to be replicated are listed according to topic.

Matrix switch

The following configuration settings are copied from the master device to a destination:

▪ Hotkey modifier	▪ Hotkey
▪ Select key modifier	▪ Permitted select keys
▪ Multiuser display	▪ Forwarding of target names
▪ RS232 mode	▪ RS232 bit rate

Tradeswitch function

The following configuration settings are copied if the tradeswitch function is enabled on both the master device and the destination:

▪ Tradeswitch key modifier	▪ Permitted tradeswitch keys

Target modules

The following data and settings of target modules are transmitted for all target modules that are connected to both master device and destination:

▪ Name	▪ Comment
▪ Configuration settings	

NOTE: If the destination already contains a local target with the same name, it is renamed to »Name (local)«.

Target groups

The following data and settings of the target groups are copied from the master device to a destination:

- Name
- Comment

NOTE: Only target modules that are connected to the destination are listed as members in the target group of the destination.

Global scan sets

The following data and settings of the global scan sets are copied from the master device to a destination:

- Name
- Comment

NOTE: Only target modules that are connected to the destination are listed as members in the scan set of the destination.

IMPORTANT: If the destination already contains a local scan set with the same name, it is renamed to »Name (<user name>)«.

Global select key sets

The following data and settings of the global select key sets are copied from the master device to a destination:

- Name
- Comment

NOTE: Only target modules that are connected to the destination are listed as members in the select key set of the destination.

IMPORTANT: If the destination already contains a local select key set with the same name, it is renamed to »Name (<user name>)«.

Replicating the database

IMPORTANT: The user account from which you accessed the web application of the master matrix switch is automatically used to log in to the destinations.

Please make sure that the user account exists on all destinations and holds the superuser right!

How to replicate the database:

1. Click **System > Tools** in the tree view.
2. Double-click **Replicate data**.

   The **Replicate database** window lists the installed destinations to which the database of the master matrix switch is replicated.

   NOTE: When establishing the connection to the devices, a symbol with a red dot is displayed next to the destinations.

   If the connection has been established, the device symbol and device name are shown in brackets.

3. Under **Port configuration**, you can define if you want to replicate the port configuration on the source devices.

   NOTE: If the number of ports differs between source device and target device, the corresponding settings are not replicated.

4. *Optional:* Add or delete a destination or change its address settings if required (see page 131).
5. Click **Continue**.

   The configuration settings are subsequently copied to the different devices. All status information are displayed and updated during the replication.

   IMPORTANT: A message alerts you about any problems that might occur during the replication of target groups, global scan sets and/or global select key sets.

   Please choose between the following options:

   - **All on this matrix switch:** overwrite all existing target data of this type (target groups, global scan sets or global select key sets) on this device
   - **All on all matrix switches:** overwrite all existing target data of this type on all devices
   - **Yes:** overwrite target data
   - **No:** skip target data

6. Click **Close**.

Adding a destination

How to add a new destination:

1. Click **System** in the tree.
2. Right-click **System** and click **Replicate database** in the context menu.
3. Click **Add**.
4. Enter the desired **IP address** or **DNS name**.
5. Add more destinations (steps 2 through 5) if necessary.
6. Click **Ok**.

Changing the address settings of a destination

How to change the IP address or DNS name of a destination:

1. Click **System** in the tree.
2. Right-click **System** and click **Replicate database** in the context menu.
3. Mark the device whose address settings you want to change.
4. Click **Change**.
5. Enter the desired **IP address** or **DNS name**.
6. Click **Ok**.

Deleting a destination

How to delete a destination:

1. Click **System** in the tree.
2. Right-click **System** and click **Replicate database** in the context menu.
3. Mark the device to be deleted.
4. Click **Delete**.
5. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Advanced functions of the KVM matrix switch

Restarting the matrix switch

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

How to restart the matrix switch via web application:

1. In the directory tree, click **KVM Matrix systems > [name] > Matrix switches**.
2. Right-click the device. Now click the **Restart** on the context menu.

Confirm the safety request with **Yes.**

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

Adjusting the RS232 mode and the baud rate of the service port

The RS232 interface of the matrix switch can be used for different applications. In addition to controlling a powerswitch, the interface can be used by the customer support team for service diagnoses.

Depending on the interface application, the interface mode and, if necessary, the baud rate have to be selected.

How to change the mode and/or the baud rate of the RS232 interface:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the master matrix switch. Now click the **Configuration** entry in the context menu.
3. Use the **RS232 mode** entry to select between the following options:

G&D Hardboot:	control of the Powerswitch (G&D Hardboot).
Debug:	diagnose mode (for support team)

4. Use the **RS232 baud rate** entry to select between the following options:

9600
19200
38400
57600
115200

NOTE: Depending on the interface operating mode, the baud rate is possibly preset.

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

Rights administration

Right to change the personal profile

How to change the right to change the personal profile:

1. Click on the **User area > Users** entries in the tree view to change this right.

   If you want to change this right for a user group, click on **User area > User groups**.

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 **Matrix systems > Global device rights** tabs.

4. Use the **Edit personal profile** entry in the *Access rights* paragraph to select between the following options:

Yes:	allows to view and edit own user profile
No:	denies to view and edit own user profile

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

Optional functions

The functional range of the KVM system can be expanded by purchasing additional functions.

Name	Function	Description
Push-Get function	The additional Push-Get function enables you to push the image to or get the image from any computer connected to the KVM matrix system to the display of another user console.	page 102
IP-Control-API	Use the C++ class library supplied with this function to access the KVM matrix system over a TCP/IP connection.	page 105
Tradeswitch function	The Tradeswitch function optimises the operation of user modules that monitor several computers over several monitors. Instead of connecting keyboard and mouse to each monitor, the Tradeswitch function provides a central keyboard/mouse for all operating tasks of the user console.	page 108

Push-Get function (option)

NOTE: The functions and settings described in this chapter are only available if the *Push-Get function* has been purchased.

The Push-Get function enables you to push the image to or get the image from any computer connected to the KVM matrix system to the display of another user console.

This way, you can exchange and edit display contents.

The addressed user console can be a standard console or a large screen projection, for example.

Changing the right for carrying out the Push-Get function

IMPORTANT: This setting is only available if the additional *Push-Get function* has been activated.

How to change the right for using the *Push-Get* function:

1. Click the **User area > Users** entries to change this right for a user account.

   If you want to change this right for a user group, click on **User area > User groups**.

2. Right-click the user account or the user group you want to configure. Now, click on **Configuration**.
3. Click the **Matrix systems > Individual device rights** tabs.
4. Select the **Consoles** option in the drop-down menu.
5. Choose the desired user module in the list field.
6. Use the **Push-Get** entry to select one of the following options:

yes:	enables the usage of the *Push-Get* function
no:	denies the usage of the *Push-Get* function

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

IP-Control-API (option)

After the »*IP-Control-API*« function has been activated, the supplied C++ class library can be used to control the KVM matrix system over a TCP/IP connection.

A touchscreen or a custom software can be integrated into the KVM matrix system. Use the self-developed touchscreen software or the custom software to access the *Application Programming Interface* of the class library.

The *Application Programming Interface* (API) enables you to execute the functions of the KVM matrix system that are listed at the bottom of this page.

ADVICE: As an alternative to programming own software solutions, the provided command line tool can be called out of script files, for example.

C++class library functions

The C++ class library provides the following functions:

- **Logon User:** user logon at user module
- **Logout User:** user logout at user module
- **Connect CPU:** accesses target module with user module

  NOTE: This function can only be carried out if a user with *ViewOnly* or *FullAccess* rights is logged in at the user module, or the console is an *OpenAccess* console that provides those rights.

- **Disconnect CPU:** disconnects active access
- **Get Connections:** queries connection data of »occupied« user modules
- **Get DVICenter:** queries known matrix switches
- **Get CPUs:** queries known target modules
- **Get Consoles:** queries known user modules

Configuring accesses for text-based control

Use the web application *Config Panel* to configure the service for text-based control. In the web application, you can define »remote control« accesses and their settings.

IMPORTANT: Text-based control is only possible with these accesses.

How to create a new access or edit existing accesses:

1. In the directory tree, click **KVM Matrix systems > [Name] > Matrix switches**.
2. Right-click the device you want to configure and click **Configuration** on the context menu.
3. Click on **Network> Remote Control**.
4. To create a new access, click **Add**.
   To adit an existing access, click **Edit**.
5. Enter or edit the following data:

Access:	Select the protocol (**TCP**) or (**UPD**) you want to use for text-based communication.
Port:	Enter the port you want to use for text-based communication.
Status:	Select if the access is **enabled** or **disabled**.
Encryption:	The following types of encryption are supported: ▪ **unencrypted:** Select **None** to transmit the data without encryption (default). ▪ **partly encrypted:** Select **Password: CBC-3DES**, to transmit only login passwords with encryption. ▪ **encrypted:** Select **CBC-3DES** to transmit date entirely encrypted.
Key:	After enabling an encryption method, enter the key. Some encryption modes require an additional initialisation vector. If necessary, enter the key followed by a colon (:) and the initialisation vector.

6. Click **OK** to save your settings and to close the window.

Tradeswitch function (option)

NOTE: The functions and settings described in this chapter are only available, if the purchased *Tradeswitch* function has been activated.

The Tradeswitch function optimises the operation of user modules that monitor several computers over several monitors.

Instead of connecting keyboard and mouse to each monitor, the Tradeswitch function provides a central keyboard/mouse for all operating tasks of the user module.

In order to enable this, up to eight user modules of a KVM matrix system are arranged into groups, which form the multi-monitor console.

Each user module within a group is provided with a monitor, but only one of the group's user modules is provided with keyboard and mouse. By using a hotkey, the user is now able to switch these two input devices to each monitor. Now, each computer of the group can be operated.

Further information:

- *Creating Tradeswitch workplaces* on page 138
- *Assigning devices to a Tradeswitch workplace* on page 141
- *Defining the master workplace of the Tradeswitch workplace* on page 142
- *Changing the Tradeswitch key and the valid keys* on page 139
- *Starting the user module without keyboard* on page 143

Basic configuration

Creating Tradeswitch workplaces

How to create a new Tradeswitch workplace:

1. Click on the **KVM Matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the matrix switch to be configured. Now click on **Configuration** in the context menu.
3. Click the **Workplaces** tab.
4. Click on **Add**.
5. Use the **Name** entry to enter the workplace name.
6. *Optional:* Use the **Comment** entry to enter a comment regarding the workplace.
7. Click **OK** to leave the interface.

Changing the name and comment of a Tradeswitch workplace

How to change the name and comment of a Tradeswitch workplace:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the matrix switch to be configured. Now click on **Configuration** in the context menu.
3. Click the **Workplaces** tab.
4. Mark the Tradeswitch workplace you want to edit and click on **Change**.
5. Use the **Name** entry to enter the workplace name.
6. *Optional:* Use the **Comment** entry to enter a comment regarding the workplace.
7. Click **OK** to leave the interface.

Deleting a Tradeswitch workplace

How to delete a Tradeswitch workplace:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the matrix switch to be configured. Now click **Configuration** in the context menu.
3. Click the **Workplaces** tab.
4. Mark the Tradeswitch workplace you want to delete and click **Delete.**
5. Confirm the confirmation prompt by clicking **Yes** or cancel the process by clicking **No**.

Changing the Tradeswitch key and the valid keys

The Tradeswitch keys enable you to switch the keyboard and mouse signals from one user module to another one or to a target computer by pressing a key combination.

In the *Tradeswitch function* section of the *Configuration* menu, several user modules and/or target computers can be grouped into a workplace. You can define the keys to be pressed in order to switch the keyboard and mouse signals to a particular user module or target computer.

In addition to defining the Tradeswitch key modifier, you can also define the valid keys for the Tradeswitch keys.

How to change the Tradeswitch key modifier or the valid keys:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the master matrix switch. Now click **Configuration** in the context menu.
3. Select *at least* one of the listed select key modifiers in the **Tradeswitch key modifier** row by marking the entry.

▪ **Ctrl**
▪ **Alt**
▪ **Alt Gr**
▪ **Win**
▪ **Shift**

4. Use the **Valid keys** row to select one of the following options:

Only numbers:	*only numerical keys* are interpreted as select keys when pressed in combination with the select key modifier
Only characters:	*only alphabetic keys* are interpreted as select keys when pressed in combination with the select key modifier
Numbers and characters:	*alphabetical and numerical keys* are interpreted as select keys when pressed in combination with the select key modifier

IMPORTANT: The selected keymode and tradeswitch key modifier(s) are *no longer* provided as key combinations to the operating system and the applications on the target computer.

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

Detailed configuration of a Tradeswitch workplace

Assigning devices to a Tradeswitch workplace

IMPORTANT: If no keyboard is connected to a user module, the user receives a message directly after the user module has been switched on. The booting process is cancelled.

Use the *Keyboard required* (see page 143) setting to boot the user module.

ADVICE: Giving the targets self-explanatory names that refer to the function or the location of the device simplifies the configuration of the Tradeswitch workplace.

Detailed information on how to rename the target modules can be found on page 82.

How to assign target or user modules to the Tradeswitch workplace:

IMPORTANT: Any computers that are locally connected to the *UCON-s* or *UCON-Audio-s* user modules cannot be operated through the Tradeswitch function if these user modules are added as slave devices to the Tradeswitch workplace.

If these workplaces are master workplaces (see page 142), the local devices can be operated without any restrictions.

1. Click on the **KVM Matrix systems > [Name] > Targets** entries in the tree view.
2. Right-click the matrix switch to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Workplaces** tab.
4. Mark the Tradeswitch workplace you want to edit and click **Change.**
5. Click the **Assigned workplace members** tab.
6. Use the drop down menu to select the type of devices to be displayed in the select window.

   Choose between the following options:

[All targets]	displays all target modules within the system
[Unassigned]	displays the target module that are *[Not assigned]* to the view filter
Workplaces	displays all user modules within the system
Search...	Selecting this option opens another window. Select the desired *View filter* in the tree view.

7. Use the **Key combination** column to select the device whose Tradeswitch key you want to change and enter the desired character(s).
8. Repeat step 7 if you want to change the Tradeswitch key of another device.
9. Click **OK** to save your changes.

Defining the master workplace of the Tradeswitch workplace

ADVICE: By giving the targets self-explanatory names that connect to the function or the location of the device, the configuration of the Tradeswitch workplace is highly simplified.

Detailed information on how to rename the target modules can is given on page 82.

Within a Tradeswitch workplace a workplace has to be defined to which keyboard and mouse are connected. This master workplace also provides information on accessing users.

How to define a master workplace of the Tradeswitch workplace:

1. Click on the **KVM Matrix systems > [Name] > Matrix switches** entries in the tree view.
2. Right-click the matrix switch to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **Workplaces** tab.
4. Mark the Tradeswitch workplace you want to edit and click **Change.**
5. Click the **Assigned workplace members** tab.
6. Use the drop down menu to select the type of devices to be displayed in the selection window.

   Choose between the following options:

[All targets]	all target modules within the system
[Unassigned]	target modules that are *[Not assigned]* to the view filter
Workplaces	all user modules within the system
Search...	This option opens another window. Select the desired *View filter* in the tree view to only display the herein contained devices in the select window.

7. Mark the entry in the **Master** column of the device that is to serve as master workplace.
8. Click **OK** to save your changes.

Enhanced functions

(De)activating the Tradeswitching information display

If you purchased the *Tradeswitch function*, the messages »*Forwarding to...*« (at the master workplace) or »*Forwarded*« (at the target workplace) can be displayed at the monitor.

How to (de)activate the Tradeswitching information display:

1. Click on the **KVM Matrix systems > [Name] > Consoles** entries in the tree view.
2. Right-click the user module to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **General** tab.
4. Use the **Display Tradeswitching** entry to select between the following options:

yes:	activated information display
no:	deactivated information display

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

Starting the user module without keyboard

If no keyboard is connected to a user module, the user receives an according message directly after the user module has been switched on. The booting process is cancelled.

NOTE: Use the *Keyboard required* setting to boot the user module.

How to (de)activate the booting of the user module without a keyboard:

1. Click the tree view entries **KVM Matrix systems > [Name] > Consoles**.

   A list of all workplaces is displayed.
2. Right-click the user module to be configured. Now click the **Configuration** entry in the context menu.
3. Click the **General** tab.
4. Use the **Keyboard required** entry to select between the following options:

yes:	user module only boots with connected keyboard
no:	user module boots without keyboard

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

NOTES

NOTES

The manual is constantly updated and available on our website.

http://gdsys.de/A9200066

Guntermann & Drunck GmbH

Obere Leimbach 9
57074 Siegen

Germany

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